

Т.И.Алиев. Сети ЭВМ и телекоммуникации

Т.И. Алиев  
Сети ЭВМ и  
телекоммуникации

Учебное пособие



Редакционно-издательский отдел  
Санкт-Петербургского государственного  
университета информационных технологий,  
механики и оптики  
197101, Санкт-Петербург, Кронверкский пр., 49



Санкт-Петербург  
2011

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

**Т.И. Алиев**  
**СЕТИ ЭВМ И ТЕЛЕКОММУНИКАЦИИ**

**Учебное пособие**



**Санкт-Петербург**

**2011**

Алиев Т.И. Сети ЭВМ и телекоммуникации. – СПб: СПбГУ ИТМО, 2011. – с.400

В пособии излагаются общие принципы структурной и функциональной организации компьютерных сетей, приводятся основные понятия техники связи, анализируются методы модуляции и кодирования данных, рассматриваются кабельные и беспроводные системы связи, а также общие принципы организации телекоммуникационных сетей.

Один из разделов полностью посвящен локальным вычислительным сетям (ЛВС), в котором рассматриваются принципы организации ЛВС, подробно излагаются вопросы построения и функционирования локальных сетей Ethernet, включая высокоскоростные технологии, Token Ring, FDDI, а также беспроводных сетей. В разделе, посвящённом глобальным вычислительным сетям, рассматриваются методы и средства объединения локальных и территориальных сетей, принципы организации сетей с установлением соединений, таких как X.25, Frame Relay, ATM, а также сетей с маршрутизацией, при рассмотрении которых основное внимание уделяется сети Internet.

Пособие предназначено, прежде всего, для студентов, обучающихся по направлению 230100 – «Информатика и вычислительная техника» и 231000 – «Программная инженерия», изучающих дисциплину «Сети ЭВМ и телекоммуникации» и связанные с ней дисциплины. Пособие может быть полезным для выпускников (бакалавров, магистрантов и специалистов), подготавливающих выпускные квалификационные работы в области компьютерных сетей и технологий.

Рекомендовано к печати Советом факультета компьютерных технологий и управления 14 декабря 2010 г., протокол № 16



В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена Программа развития государственного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет информационных технологий, механики и оптики» на 2009–2018 годы.

© Санкт-Петербургский государственный университет информационных технологий, механики и оптики, 2011

© Алиев Т.И., 2011



В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена Программа развития государственного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет информационных технологий, механики и оптики» на 2009–2018 годы.

---

## КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Кафедра вычислительной техники (ВТ) Санкт-Петербургского государственного университета информационных технологий, механики и оптики является одной из авторитетнейших научно-педагогических школ России. Более 70 лет кафедра ведет подготовку высококвалифицированных специалистов в области информатики и вычислительной техники. За годы своего существования на кафедре подготовлено более 5000 высококвалифицированных специалистов, 950 преподавателей из разных вузов бывшего СССР окончили курсы повышения квалификации по вычислительной технике, подготовлено более 230 кандидатов наук и 36 докторов наук. Преподавателями и научными сотрудниками кафедры изданы 27 монографий и 6 учебников для вузов, десятки учебно-методических пособий. Сегодня кафедра вычислительной техники является одной из крупнейших в университете, имеющей высококвалифицированный состав преподавателей, среди которых 8 профессоров и 16 доцентов, обучающих более 500 студентов и аспирантов.

Традиционно на кафедре вычислительной техники основной упор в подготовке специалистов делается на фундаментальную базовую подготовку как в рамках общепрофессиональных дисциплин, так и специальных дисциплин, охватывающих все наиболее важные разделы вычислительной техники: функциональная схемотехника и микропроцессорная техника, алгоритмизация и программирование, информационные системы и базы данных, мультимедиатехнологии, вычислительные сети и средства телекоммуникации, защита информации и информационная безопасность. В то же время, кафедра считает необходимым предоставить студентам старших курсов возможность специализироваться в более узких профессиональных областях в соответствии с их интересами. Такими областями являются: 1) встраиваемые системы реального времени, 2) информационные системы и базы данных, 3) сети ЭВМ и корпоративные системы; 4) информационная безопасность вычислительных систем и сетей.

## **ВВЕДЕНИЕ**

Специалисты по вычислительной технике утверждают, что 50% знаний в области компьютерных и сетевых технологий устаревает за 5 лет. С этой оценкой можно не соглашаться, но факт остается фактом: базовые технологии, представления о перспективности или бесперспективности той или иной технологии, подходы и методы решения ключевых задач и даже понятия о том, какие задачи при создании сетей являются основными – всё это изменяется быстро и часто неожиданно.

Действительно, полностью осталась в прошлом традиционная модемная связь со скоростью передачи данных до 56 кбит/с, уступив место сначала ISDN-технологии, которая ещё лет 10 назад считалась основной технологией для доступа в Интернет по телефонным каналам и которая, так и не получив широкого распространения, в настоящее время практически полностью вытеснена ADSL-технологией. Точно так же ATM-технология, на которую возлагались большие надежды и которая считалась одной из наиболее перспективной для передачи мультимедийных данных, постепенно вытесняется технологией MPLS. И таких примеров можно привести достаточно много.

Всё это делает проблематичным написание качественного учебного пособия по сетевым технологиям, рассчитанного на несколько лет, которое должно отражать современное состояние компьютерных сетей и определять направления развития сетевых технологий, давая молодым специалистам многообразные и в то же время фундаментальные знания.

Какова же цель данного пособия? Для кого оно предназначено, на какой круг читателей ориентировано? Ответы на эти вопросы определяют содержание и стиль изложения материала.

Пособие ориентировано, в первую очередь, на студентов, начинающих изучать компьютерные сети. Конечно, можно попытаться заставить студентов изучить одну из перечисленных в списке литературы книг, объёмом около 1000 страниц. Однако вряд ли стоит рассчитывать на успех, если этот материал должен быть освоен в течение одного семестра, тем более студентами младших курсов. Трудно представить, как за 4 месяца можно не просто прочитать, а разобраться и выучить материал примерно 10 дисциплин, если по каждой дисциплине будет использоваться учебник по 1000 страниц. Кроме того, для студентов, специализирующихся в области компьютерных сетей, на старших курсах предусматриваются специальные дисциплины, в которых более детально изучаются те или иные разделы, например, протоколы различных сетевых технологий, технологии беспроводных сетей, сетевые операционные системы, методы и средства защиты информации в компьютерных сетях, программирование Интернет-приложений и т.д.

В связи с этим, одна из целей написания этого пособия, состояла в создании учебного пособия приемлемого объёма, которое охватывало бы большинство вопросов компьютерных сетей, включая исторические аспекты развития сетевых технологий и сравнительный качественный, а в некоторых случаях и количественный анализ методов и средств, используемых в разных сетевых технологиях. Исходя из этого, автор стремился изложить основные концепции по каждому из рассматриваемых вопросов, не вдаваясь в детали, полагая, что продвинутые студенты, заинтересовавшиеся тем или иным разделом, самостоятельно могут расширить свои знания, обратившись к солидным источникам или к Интернету.

Основная цель пособия – дать начальное представление об общих принципах структурно-функциональной организации современных компьютерных сетей и средств телекоммуникаций, ознакомить с основными терминами и понятиями в области сетевых технологий, рассмотреть наиболее популярные технологии построения и функционирования локальных и глобальных сетей, провести качественный, и, по-возможности, количественный сравнительный анализ различного сетевого оборудования и разных сетевых технологий без использования сложных математических выкладок. Уровень изложения материала предполагает знание основ вычислительной техники, принципов построения и функционирования компьютеров, принципов организации программных и информационных средств.

Сформулированные выше цели достигаются за счёт следующих решений.

1. Предпринята попытка сформулировать чёткие однозначные определения терминов и понятий, используемых в процессе изложения материала. Часто в литературных источниках некоторые термины либо не определены, либо определены нечетко и неоднозначно.

2. Материал пособия сопровождается многочисленными рисунками, количество которых в каждом разделе превышает полсотни. Автор считает, что рисунки позволяют более успешно усваивать излагаемый материал и благодаря своей наглядности способствуют более эффективному запоминанию материала.

Автор сознательно не использовал подрисуночных подписей, сопровождая все рисунки только номерами, которые необходимы для указания ссылок на рисунки в тексте пособия. Автор полагал, что отсутствие подрисуночных подписей при желании или необходимости (при подготовке к контрольным работам или тестовым испытаниям) узнать, что же изображено на рисунке, заставит читателя с большим интересом прочитать текст, который относится к этому рисунку. А, как известно, то, что изучается или добывается с заранее сформированным

интересом, усваивается более прочно и запоминается гораздо лучше, чем простое чтение текста, тем более по принуждению.

3. В пособии для более эффективного усвоения материала фрагменты, представляющие наибольший интерес, выделяются разными шрифтами, что позволяет акцентировать внимание читателя на тех или иных аспектах, которые, по мнению автора, являются важными для понимания излагаемого материала.

**Полужирный курсив** выделяет наиболее важные и часто используемые термины и понятия, для которых дается определение или подробное описание.

**Полужирным шрифтом** выделяются прочие общепринятые термины и понятия, часто встречающиеся в литературе и не имеющие чёткого определения, а также вспомогательные заголовки, названия и т.д.

**Курсив** выделяет в тексте ключевые слова и фразы, на которые следует обратить внимание и которые раскрывают смысл излагаемого материала или имеют важное значение. Кроме того курсивом могут быть выделены термины и понятия, которые определены в других разделах и значения которых можно найти, используя алфавитный указатель.

**Структура учебного пособия.** Пособие содержит 4 раздела, *Заключение*, *Вопросы и задания для самостоятельной работы*, *Используемые аббревиатуры*, *Список литературы* и *Алфавитный указатель*. Материал каждого раздела разбит на параграфы, которые имеют двойную нумерацию. Параграфы разбиты на пункты с тройной нумерацией, которые могут содержать подпункты с нумерацией из четырёх чисел.

*Заключение* содержит краткий обзор представленного в пособии материала, а также обсуждение некоторых проблемных вопросов, которые, по мнению автора, излагаются в литературе некорректно. По этим вопросам автор излагает свою точку зрения, надеясь на её понимание.

*Вопросы и задания для самостоятельной работы* охватывают практически весь излагаемый в пособии материал и позволяют читателю самостоятельно выполнить проверку степени усвоения изложенного материала, а также закрепить полученные знания в процессе решения предлагаемых задач. Для того чтобы можно было легко найти ответы, все вопросы и задания разбиты по разделам, а внутри каждого раздела (кроме первого) вопросы разбиты по параграфам.

*Используемые аббревиатуры* содержат кроме русскоязычных множество общепринятых англоязычных аббревиатур, широко используемых в различных публикациях по компьютерной и сетевой тематике. Для каждой англоязычной аббревиатуры даётся перевод на русский язык и в некоторых случаях – русскоязычный аналог.

В настоящее время имеется большое количество книг, не говоря уже о статьях и публикациях в Интернете, охватывающих практически все

вопросы компьютерных и телекоммуникационных технологий. Это, прежде всего, выдержавшее уже 4 издания книга Олиферов [1], в которой достаточно полно, последовательно и на хорошем уровне излагаются вопросы компьютерных сетей. Это и ряд переводных книг [2-4, 6, 7], в которых можно найти дополнительную информацию и ознакомиться с авторской трактовкой некоторых положений в области компьютерных и телекоммуникационных сетей.

Представленный в пособии *Список литературы* содержит минимальный перечень источников, которые автор рекомендует в первую очередь для получения более подробной информации по тем или иным вопросам [1-4] и материал из которых в той или иной степени был использован при написании данного пособия [1-8].

В конце пособия имеется *Алфавитный указатель* со ссылками на страницы, содержащие определения основных терминов и понятий, используемых в учебном пособии.

Учебное пособие предназначено, прежде всего, для студентов, обучающихся по направлению «Информатика и вычислительная техника» и «Программная инженерия», изучающих дисциплину «Сети ЭВМ и телекоммуникации» и связанные с ней дисциплины. Пособие может быть полезным для выпускников (бакалавров, магистрантов и специалистов), подготавливающих выпускные квалификационные работы в области компьютерных сетей и технологий.

# Раздел 1. ОБЩИЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ СЕТЕЙ ЭВМ

## 1.1. Основные понятия и терминология

В данном параграфе вводятся используемые при изложении материала понятия и определения, позволяющие систематизировать средства вычислительной техники и средства телекоммуникаций, являющиеся объектами изучения в дисциплине "Сети ЭВМ и телекоммуникации".

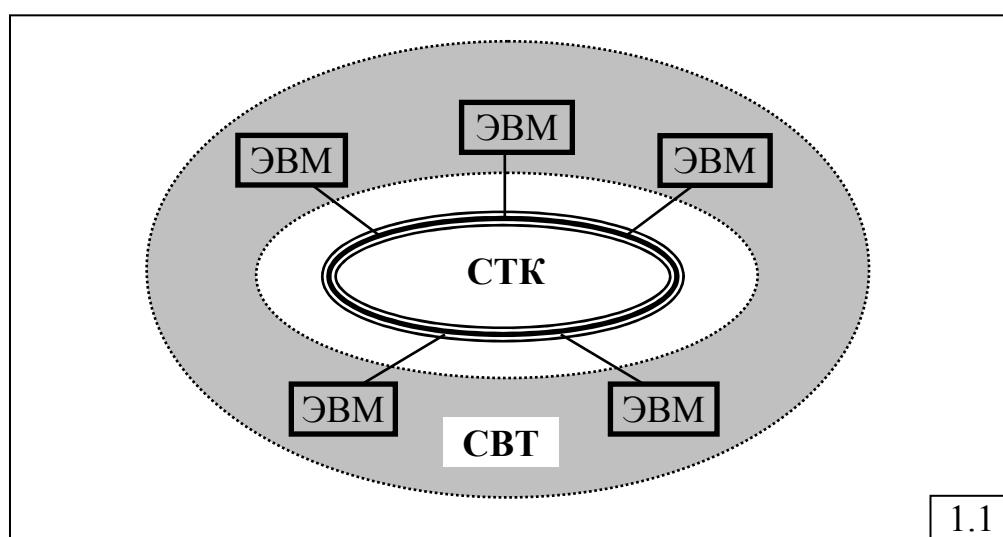
К сожалению, для вычислительной техники характерна терминологическая неоднозначность и неопределённость, что проявляется в различном толковании в разных литературных источниках одного и того же термина (например «вычислительная система» или «вычислительный комплекс»), либо в использовании разных терминов для обозначения одного и того же понятия (например «вычислительная сеть», «сеть ЭВМ», «компьютерная сеть»). Всё это зачастую усложняет восприятие и усвоение материала.

Целью излагаемого в данном разделе материала является устранение терминологической неоднозначности и уточнение используемых ниже терминов и понятий. Предлагаемая классификация различных систем и объектов вычислительной техники направлена на выявление классов систем, характеризующихся одинаковыми или близкими свойствами, что позволяет унифицировать процесс изучения и исследования вычислительных систем и сетей.

### 1.1.1. Понятие сети ЭВМ

**Сеть ЭВМ** (рис.1.1) – совокупность *средств вычислительной техники* (СВТ), представляющих собой множество ЭВМ, объединённых с помощью *средств телекоммуникаций* (СТК). Сеть ЭВМ реализует две основные функции:

- обработку данных;
- передачу данных.



1.1

Наряду с термином «сеть ЭВМ» широко используются близкие по смыслу термины «компьютерная сеть» и «вычислительная сеть», которые обычно рассматриваются как синонимы. Однако некоторые незначительные различия между указанными терминами мы будем иметь в виду при дальнейшем изложении материала.

Из данного выше определения (рис.1.1) следует, что «сеть ЭВМ» представляет собой множество ЭВМ (компьютеров), объединённых в единую сеть с помощью средств телекоммуникаций, образующих **базовую сеть передачи данных (СПД)**. Другими словами, «сеть ЭВМ» или «компьютерная сеть» – это объединение ЭВМ (компьютеров), в отличие, например, от телефонной сети, объединяющей автоматические телефонные станции (АТС). Поэтому эти два термина будем рассматривать и использовать ниже как эквивалентные. Термин же «вычислительная сеть» скорее характеризует назначение сети – выполнение вычислений, что отличает её, например, от «информационной сети», предоставляющей информационные услуги, или от «телекоммуникационной сети», предназначеннной для передачи данных.

Отдельные сети ЭВМ могут объединяться между собой, образуя большие компьютерные сети, которые в свою очередь могут объединяться и образовывать сверхбольшие глобальные сети. Такое объединение сетей приводит к иерархической структуре, в которой небольшие сети являются подсетями сетей более высокого ранга.

Итак, сеть ЭВМ реализует передачу и обработку *данных*. Однако часто можно услышать или прочитать, что в сети передаётся и обрабатывается *информация*. Так что же на самом деле передаётся и обрабатывается в сети: данные или информация? Для ответа на этот вопрос необходимо определить понятия «данные» и «информация».

Существуют различные подходы к определению понятий «данные» и «информация» в разных областях человеческой деятельности: в биологии, в кибернетике, в философии и т.д. Создана даже специальная научная дисциплина «Теория информации».

Среди всех существующих определений понятий «данные» и «информация» воспользуемся общепринятыми традиционными определениями, для чего обратимся к «Словарю русского языка» С.И.Ожегова, и попытаемся сформулировать разницу между этими двумя терминами.

### 1.1.2. Данные и информация

**«Данные** – сведения, необходимые для какого-нибудь вывода, решения.

**Информация** – сведения, осведомляющие о положении дел, о состоянии чёго-нибудь». (Ожегов С.И. Словарь русского языка).

Из этих определений следует, что данные – это любое множество сведений, а информация – это сведения, полученные с некоторой целью и несущие в себе новые знания для того, кто эту информацию получает.

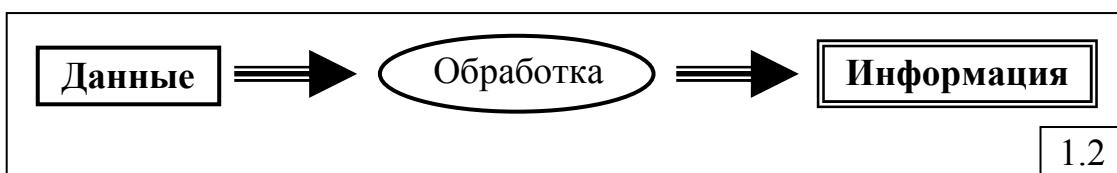
Например, телефонная книга содержит *данные* в виде множества телефонных номеров различных организаций. Извлекая же номер некоторой конкретной организации, в которую мы хотим позвонить, мы получаем *информацию* в виде телефонного номера (или нескольких телефонных номеров) этой организации. По этой же причине мы говорим «база *данных*» (а не «база *информации*»), но, формируя запрос к базе данных, мы получаем информацию в виде сведений, представляющих для нас определённый интерес.

«*Информация*» – понятие субъективное. Сведения, которые являются информацией для одного человека, могут не быть информацией для другого. Например, сведения типа «Париж – столица Франции, а Лондон – столица Англии» являются информацией для школьника, который впервые узнал об этом, и не являются информацией (чем-то новым и ранее не известным) для взрослого человека.

Следует также иметь в виду, что количественной мерой данных является **объём** – количество единиц данных, измеренных в байтах, словах, страницах, количестве телефонных номеров в телефонной книге и т.п. В то же время, количественной мерой информации является **энтропия** – мера неопределенности информации. Чем больше энтропия, тем более ценной является информация.

Таким образом, можно сказать, что в компьютерной сети передаются и данные, и информация.

Взаимосвязь понятий «*данные*» и «*информация*» в рассматриваемом контексте иллюстрируется рис.1.2, показывающим, что информация извлекается из множества данных в результате некоторых манипуляций (обработки данных).



### 1.1.3. Средства вычислительной техники

**Средства вычислительной техники** (СВТ) реализуют обработку данных и представляют собой совокупность ЭВМ, вычислительных комплексов и вычислительных систем различных классов.

Определим смысловое значение каждого из упомянутых терминов – «ЭВМ», «вычислительный комплекс», «вычислительная система» – и покажем существующую между ними разницу.

**ЭВМ (электронная вычислительная машина, компьютер)** – совокупность технических средств, предназначенных для организации ввода, хранения, автоматической обработки по заданной программе и вывода данных (информации).

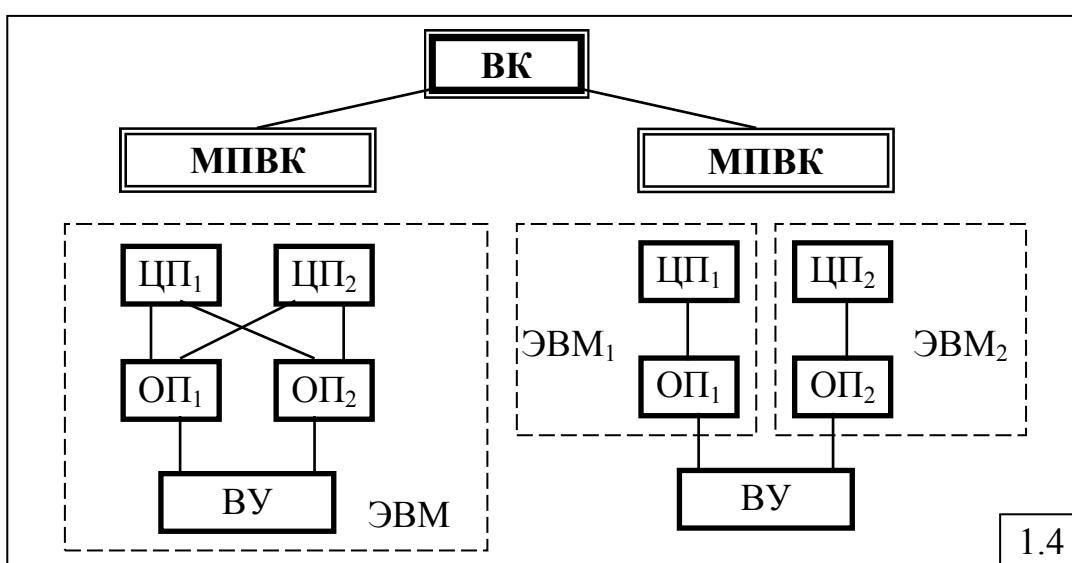
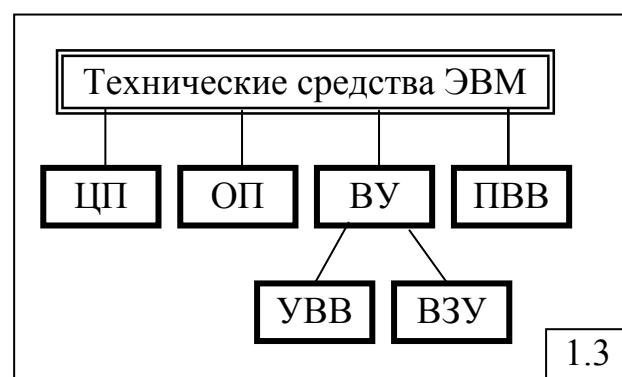
К техническим средствам относятся (рис.1.3):

- центральный процессор (ЦП);

- оперативная (основная) память (ОП);
- внешние устройства (ВУ), включающие устройства ввода-вывода (УВВ) и внешние запоминающие устройства (ВЗУ);
- процессоры (каналы) ввода-вывода (ПВВ, КВВ).

### **Вычислительный комплекс (ВК)**

(ВК) – совокупность технических средств, содержащая несколько центральных процессоров и представляющая собой одну ЭВМ с несколькими ЦП (**МПВК – многопроцессорный ВК**) или объединение нескольких однопроцессорных ЭВМ (**ММВК – многомашинный ВК**) (рис.1.4).



Основной целью построения ВК является обеспечение высокой надежности и/или производительности, не достижимой для однопроцессорных ЭВМ.

**Вычислительная система (ВС)** – совокупность технических и программных средств, ориентированных на решение определенной совокупности задач.

К программным средствам относятся (рис.1.5):

- **системное программное обеспечение**, представляющее собой совокупность стандартных программных средств, обеспечивающих функционирование ВС и включающих операционную систему (ОС), основными составляющими которой для организации эффективного функционирования ВС, являются **управляющие программы** (УП), а также трансляторы с алгоритмических языков и библиотеки математических и служебных программ;
- **прикладное программное обеспечение** в виде множества **прикладных программ** (ПП), обеспечивающих ориентацию ВС на решение задач конкретной области применения.



Понятие «вычислительная система» в рассматриваемом контексте полностью согласуется с понятием «система», сформулированным в общей теории систем, в соответствии с которым *система должна обладать структурной и функциональной организацией*, а также фундаментальными свойствами: *целостностью, связностью, организованностью и интегративностью*. Последнее означает, что система обладает свойствами (функциями), которые не присущи ни одному из элементов, входящих в состав системы.

Именно программные средства обеспечивают функциональную организацию ВС, реализуемую управляющими программами операционной системы и прикладными программами. Свойство интегративности в значительной степени обеспечивается прикладными программами. Действительно, элементы (устройства) ЭВМ обеспечивают функции обработки данных (ЦП), хранения данных (ОП, ВЗУ), ввода и вывода данных (УВВ). В то же время вычислительная система с соответствующим программным обеспечением может выполнять функции перевода с одного языка на другой, играть в шахматы и другие игры, воспроизводить звук, фото- и видеоизображения и т.д., то есть ВС обладает функциями, не присущими отдельным устройствам ЭВМ.

Таким образом, многопроцессорный (многомашинный) ВК, рассматриваемый в совокупности с программным обеспечением, можно называть **многопроцессорной (многомашинной) вычислительной системой** – МПВС (ММВС), а суперЭВМ с программным обеспечением – **высокопроизводительной ВС** (ВПВС).

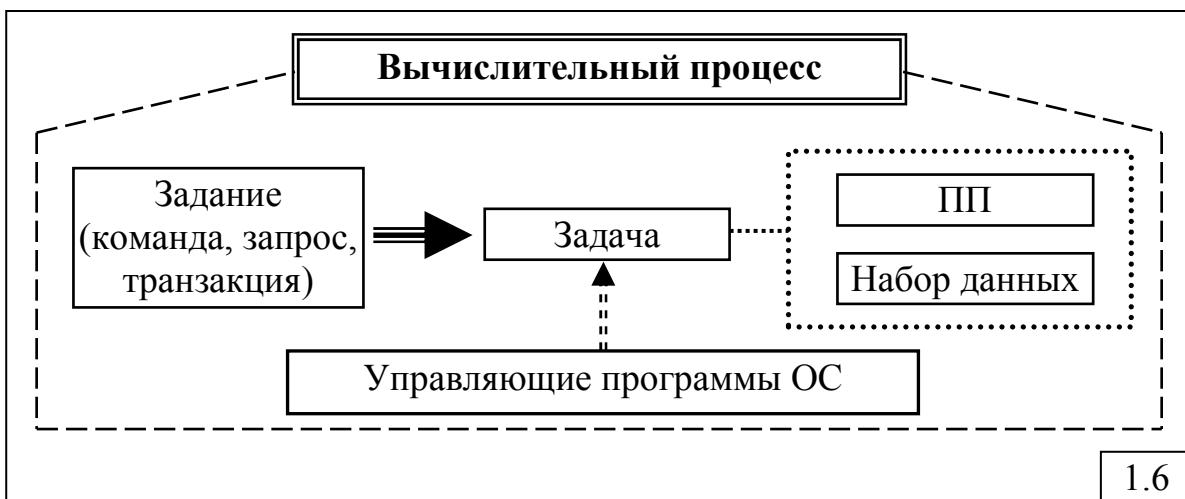
Ещё одной отличительной особенностью ЭВМ от ВС является единица измерения производительности. Производительность ЭВМ измеряется в MIPS (миллион инструкций, команд или операций в секунду) или в FLOPS (операций с плавающей точкой в секунду – для суперЭВМ), а производительность ВС – в количестве задач, выполняемых системой за единицу времени, называемой *системной производительностью*. Очевидно, что системная производительность зависит как от параметров технических средств ВС, так и от параметров программных средств, в частности, прикладных программ. Ясно, что количество «коротких» задач, выполняемых системой за единицу времени в ВС, всегда будет больше, чем «длинных» задач.

На системном уровне в качестве основной единицы работы ВС рассматривается **задача**, представляющая совокупность определенной прикладной программы с определенным набором данных (рис.1.6).

Причиной инициализации задачи может быть **задание (команда, запрос, транзакция)**.

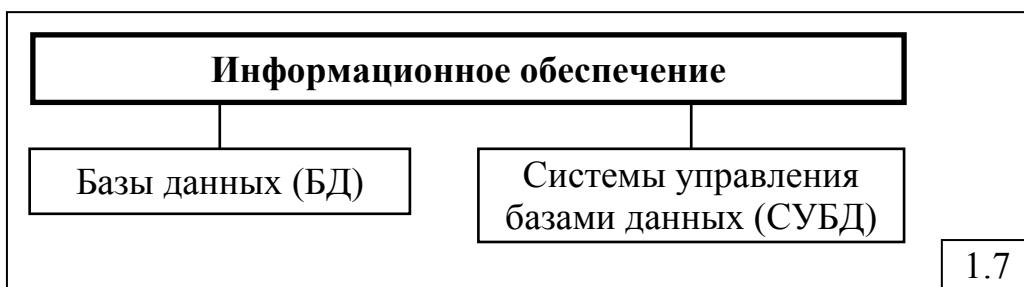
Выполнение задач в ВС называется **вычислительным процессом**.

Определенный порядок (последовательность) прохождения задач через систему, то есть управление вычислительным процессом, осуществляется *управляющими программами ОС*.



1.6

К программным средствам ВС тесно примыкают *базы данных* и *системы управления базами данных*, которые можно рассматривать как самостоятельную составляющую ВС – *информационное обеспечение* (рис.1.7).



1.7

**База данных** (БД) – упорядоченные наборы данных (файлы), имеющие определенную структуру.

**Системы управления базами данных (СУБД)** – специальные программные средства, предназначенные для формирования, модификации и выборки данных.

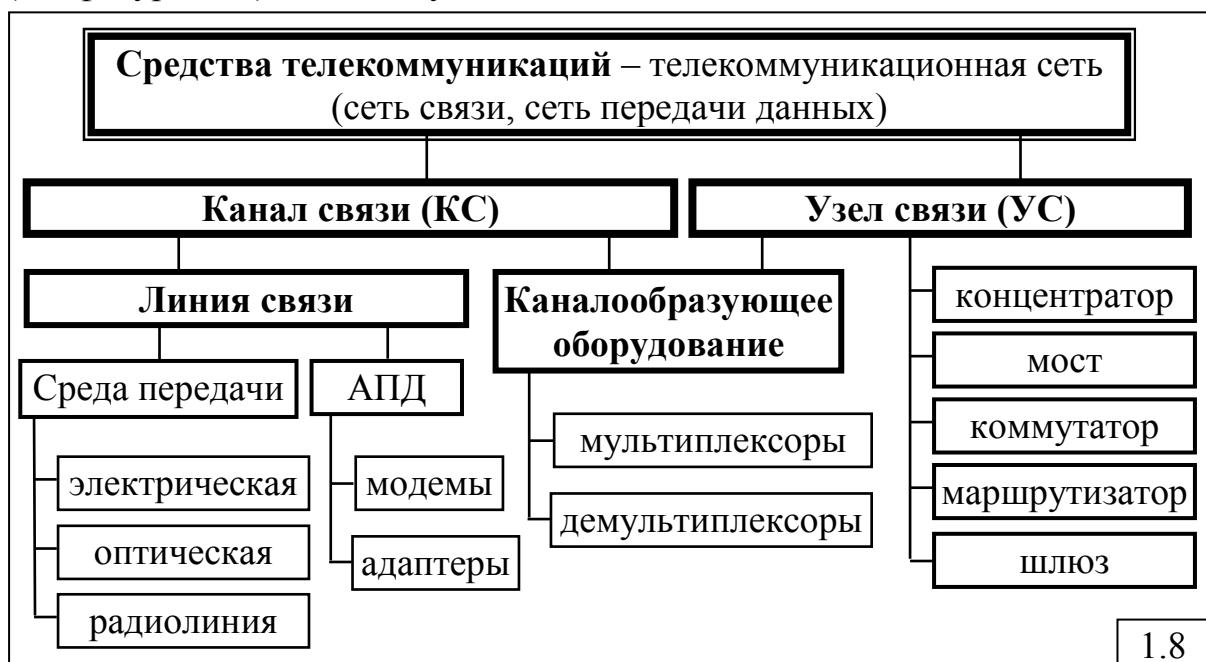
Часто термин "вычислительная система" используется в качестве обобщенного понятия. При этом предполагается, что ВС может быть построена на базе однопроцессорной ЭВМ, многомашинного или многопроцессорного вычислительного комплекса, а компьютерная сеть, представляющая собой объединение нескольких ВС, может рассматриваться как система более высокого уровня.

Компьютерная сеть кроме функций ввода, хранения, обработки и вывода данных реализует функции по передаче данных на значительные расстояния между абонентами сети, в качестве которых выступают ВС и пользователи сети, имеющие доступ к ресурсам сети с помощью удаленных терминалов.

#### 1.1.4. Средства телекоммуникаций

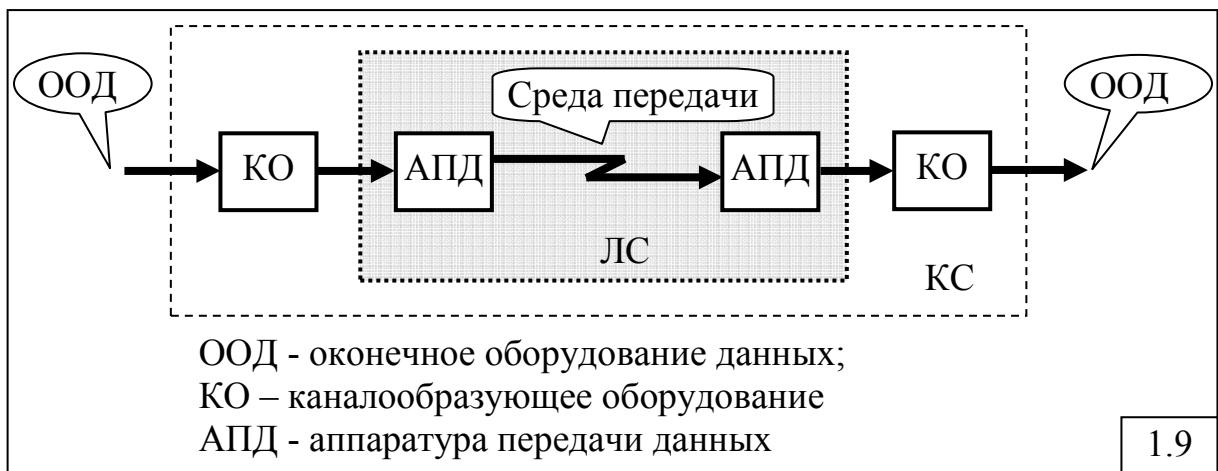
**Средства телекоммуникаций** (СТК) реализуют передачу данных и образуют *телекоммуникационную сеть* (*сеть связи, сеть передачи данных*), состоящую из узлов связи (УС), объединенных каналами связи (КС) для передачи данных (рис.1.8).

Способ объединения УС и КС определяет **топологию** (конфигурацию) телекоммуникационной сети.



**Канал связи (КС)** включает в себя *линию связи (ЛС)* и *каналообразующее оборудование*.

**Линия связи (ЛС)** представляет собой физическую среду передачи, по которой передаются сигналы, вместе с *аппаратурой передачи данных* (АПД), формирующей сигналы, соответствующие типу ЛС (рис.1.9).



**Аппаратура передачи данных (АПД)** осуществляет преобразование сигналов в соответствии с типом среды передачи (линии связи). К АПД относятся различного типа *модемы* (модуляторы-демодуляторы), используемые в телефонных и высокочастотных КС: телефонные, кабельные, радиомодемы, xDSL-модемы, адаптеры и т.д.

**Каналообразующее оборудование (КО)** предназначено для формирования канала передачи данных между двумя взаимодействующими абонентами, при этом в одной и той же линии связи одновременно может быть сформировано несколько каналов за счет использования различных методов уплотнения.

Технология уплотнения и формирования многоканальных систем передачи данных в компьютерных сетях называется *мультиплексированием* и реализуется мультиплексорами и демультиплексорами. Обычно каналообразующее оборудование входит в состав узлов телекоммуникационной сети.

Основными функциями узлов связи являются:

- *маршрутизация*, заключающаяся в выборе направления передачи (маршрута) данных;
- *коммутация*, заключающаяся в установлении физического или логического соединения между входными и выходными портами узла;
- *мультиплексирование*, заключающееся в объединении нескольких входящих в узел потоков данных в один выходящий из узла поток;
- *демультиплексирование*, заключающееся в разделении одного входящего в узел потока данных на несколько выходящих из узла потоков.

В качестве узлов связи в вычислительных сетях используются специализированные сетевые устройства: концентраторы, мосты, коммутаторы, маршрутизаторы и шлюзы.

В качестве оконечного оборудования данных (ООД) (рис.1.9) могут выступать компьютеры и сетевое оборудование (мосты, коммутаторы, маршрутизаторы), находящееся в узлах сети.

Состав ЭВМ, вычислительного комплекса, системы и сети, а также взаимосвязь между рассмотренными понятиями иллюстрируется рис.1.10.

### 1.1.5. Понятия архитектуры и технологии компьютерной сети

В широком смысле под *архитектурой компьютерной сети* будем понимать множество технических и инженерных решений по структурной и функциональной организации сети, обеспечивающих определенную совокупность ее свойств и характеристик, рассматриваемую с точки зрения пользователя сети и отличающую данную конкретную сеть от любой другой сети.

Под *технологией компьютерной сети* (сетевой технологией) будем понимать совокупность способов организации (реализации) передачи и обработки данных, обеспечивающих достижение определенных целей, формулируемых в виде требований к качеству (эффективности) обработки и передачи данных.

## **1.2. Состав и типы компьютерных сетей**

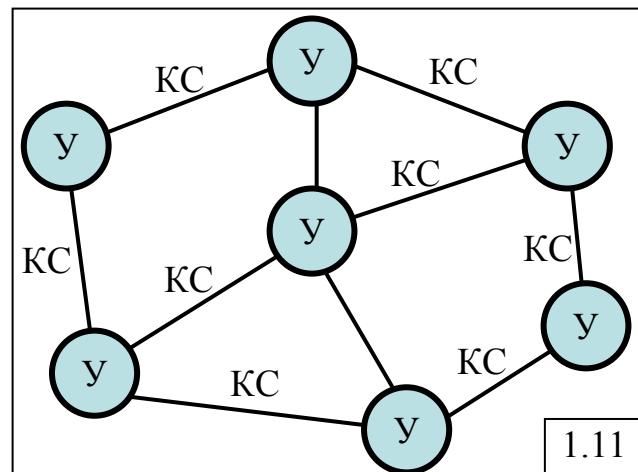
### **1.2.1. Состав компьютерной сети**

Концептуально компьютерную сеть можно представить как совокупность взаимосвязанных узлов (рис.1.11).

**Узел сети** – совокупность средств, объединенных каналами связи и реализующих функции:

- выбора направления и организации передачи данных (средства коммутации и маршрутизации); такие узлы называются *узлами связи* (*узлами коммутации, узлами передачи данных*);
  - обработки данных (средства обработки данных); такие узлы называются *узлами (центрами) обработки данных*.

В качестве узлов связи могут использоваться коммутаторы и маршрутизаторы, а в качестве узлов обработки данных – компьютеры, предоставляющие свои информационные и вычислительные ресурсы пользователям сети и называемые **хост-машинами** или просто **хостами** (host).



В сети Internet термин "хост-машина" трактуется более широко: *хост-машиной* называется любой пользовательский компьютер, подключенный к сети.

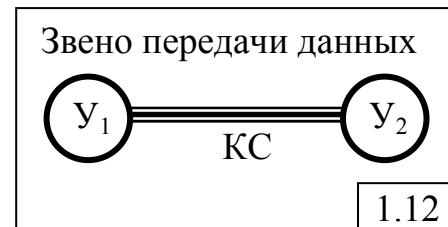
Совокупность средств коммуникаций (связи) для передачи данных, состоящая из каналов связи и узлов связи, образует *сеть связи*, называемую также *телекоммуникационной сетью* или *сетью передачи данных (СПД)*. Следует иметь в виду, что понятие «сеть передачи данных»

имеет более узкий смысл по сравнению с понятием «сеть связи». СПД предназначена для передачи компьютерных (цифровых) данных, в то время как в сети связи (или, что то же самое, телекоммуникационной сети) могут передаваться как цифровые (дискретные), так и непрерывные (аналоговые) данные, к которым относятся мультимедийные данные – речь, аудио и видео.

Два узла, связанные каналом связи, образуют звено передачи данных (рис.1.12).

Данные в компьютерной сети передаются в виде сообщений.

**Сообщение** представляет собой единицу данных, передаваемую между пользователями сети как *единое целое* и имеющую определённый смысл. В качестве сообщений могут выступать программные файлы, электронные письма, неподвижные изображения, видеофильмы и т.п. Сообщение представляется в определённом формате (рис.1.13), содержащем в общем случае заголовок и концевик. В заголовке указывается адрес получателя данного сообщения и адрес отправителя, а также дополнительная служебная информация (тип и длина сообщения, приоритет и т.д.), необходимая для эффективной передачи сообщения в сети. Концевик обычно содержит контрольную сумму, используемую для обнаружения ошибок, которые могут появиться при передаче сообщения по сети.



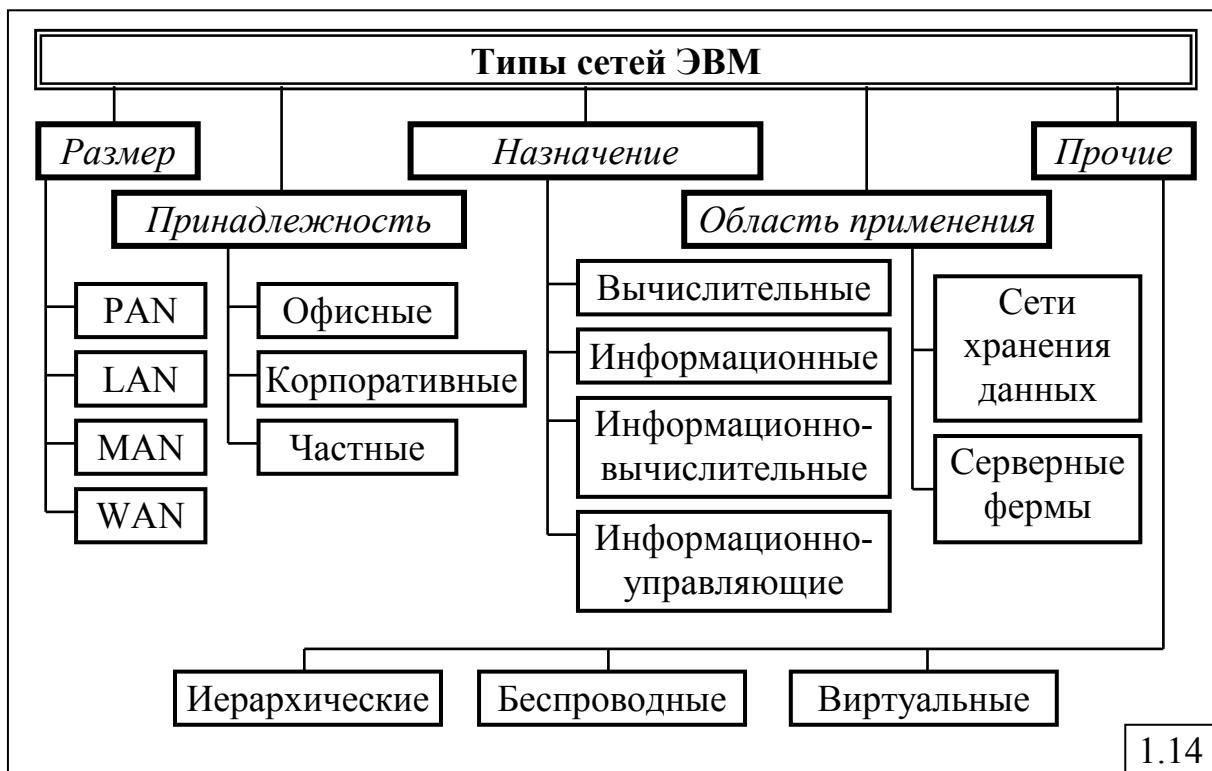
Сообщение при передаче через телекоммуникационную сеть может быть разбито на несколько блоков данных, каждый из которых представляется в формате, аналогичном сообщению (рис.1.13). Такой блок данных отличается от сообщения тем, что имеет ограниченную длину, в то время как длина сообщения в принципе не ограничена. Так, например, сообщение, представляющее собой видеофильм длиной в несколько гигабайт, при передаче через телекоммуникационную сеть может быть разбито на множество блоков данных, длина которых не будет превышать 1000 байт, причём каждый такой блок данных будет иметь заголовок с одинаковыми адресами отправителя и получателя.

### 1.2.2. Классификация сетей ЭВМ

Классификация сетей ЭВМ (компьютерных сетей), как любых больших и сложных систем, может быть выполнена на основе различных признаков, в качестве которых могут быть использованы (рис.1.14):

- размер (территориальный охват) сети;
- принадлежность;
- назначение;

- область применения.



1.14

### 1. По размеру (территориальному охвату) сети ЭВМ делятся на:

- персональные;
- локальные;
- городские (региональные).
- глобальные.

**Персональная сеть (Personal Area Network, PAN)** — это сеть, объединяющая персональные электронные устройства пользователя (телефоны, карманные персональные компьютеры, смартфоны, ноутбуки и т.п.) и характеризующаяся:

- небольшим числом абонентов;
- малым радиусом действия (до нескольких десятков метров);
- некритичностью к отказам.

К стандартам таких сетей в настоящее время относятся Bluetooth, Zigbee, Пиконет.

**Локальная вычислительная сеть (ЛВС) (Local Area Network, LAN)** — сеть со скоростью передачи данных, как правило, не менее 1 Мбит/с, обеспечивающая связь на небольших расстояниях — от нескольких десятков метров до нескольких километров. Оборудование, подключаемое к ЛВС, может находиться в одном или нескольких соседних зданиях.

Примеры ЛВС: Ethernet, Token Ring.

**Городская вычислительная сеть (Metropolitan Area Network, MAN)** — сеть, промежуточная по размеру между ЛВС и глобальной сетью. Протоколы и кабельная система для городской вычислительной сети описываются в стандартах комитета IEEE 802.6. MAN реализуется на основе протокола DQDB (Distributed Queue Dual Bus) — двойная шина с

распределенной очередью и использует волоконно-оптический кабель для передачи данных со скоростью 100 Мбит/с на территории до 100 км<sup>2</sup>. MAN может применяться для объединения в одну сеть группы сетей, расположенных в разных зданиях. Последние разработки, связанные с высокоскоростным беспроводным доступом в соответствии со стандартом IEEE 802.16, привели к созданию MAN в виде широкополосных беспроводных ЛВС.

**Глобальная сеть** (*Wide Area Network, WAN*) – в отличие от ЛВС охватывает большую территорию и представляет собой объединение нескольких ЛВС, связанных с помощью специального сетевого оборудования (маршрутизаторов, коммутаторов и шлюзов), образующих в случае использования высокоскоростных каналов магистральную сеть передачи данных (магистральную сеть связи). Наиболее широкое применение находят глобальные сети для нужд информационного обмена в коммерческих, научных и других профессиональных целях.

Для построения глобальных сетей могут использоваться различные сетевые технологии, в том числе TCP/IP, X.25, Frame Relay, ATM, MPLS.

Настоящей глобальной сетью, пожалуй, можно считать только сеть Интернет. Вряд ли глобальной можно считать сеть, объединяющую 2-3 ЛВС, находящиеся в разных городах, расположенных на расстоянии нескольких десятков или даже сотен километров друг от друга. Однако, поскольку для построения такой «простой» сети используются обычно те же сетевые технологии и технические средства, что и в сети Интернет, то такие сети обычно тоже относят к классу глобальных сетей.

## 2. По принадлежности сети ЭВМ делятся на:

- *офисные* – сети, расположенные на территории офиса компании, ограниченной обычно пределами одного здания, и построенные на технологиях LAN;
- *корпоративные (ведомственные)* – сети, представляющие собой объединение нескольких офисных сетей компании, расположенных в разных территориально разнесенных зданиях, находящихся возможно в разных городах и регионах, и построенные на технологиях MAN или WAN;
- *частные* – сети, построенные обычно на технологии **виртуальной частной сети** (*Virtual Private Network, VPN*), позволяющей обеспечить одно или несколько сетевых соединений, которые могут быть трёх видов: узел-узел, узел-сеть и сеть-сеть, образующих логическую сеть поверх другой сети (например, Интернет).

## 3. По назначению сети ЭВМ делятся на:

- *вычислительные*, предназначенные для решения задач пользователей, ориентированных, в основном, на вычисления;
- *информационные*, ориентированные на предоставление информационных услуг; примерами таких сетей могут служить сети, предоставляющие справочные и библиотечные услуги;

- *информационно-вычислительные*, предназначенные для решения задач пользователей и предоставления информационных услуг;
- *информационно-управляющие*, предназначенные для управления реальными объектами и процессами.

4. По области применения сети можно разделить на:

- сети хранения данных;
- серверные фермы.

**Сеть хранения данных (СХД)** (*Storage Area Network, SAN*) представляет собой множество внешних устройств хранения данных, таких как дисковые массивы, ленточные библиотеки, оптические накопители, подключённые к серверам, при этом операционная система рассматривает подключённые ресурсы, как локальные.

Следует не путать сеть хранения данных с **сетевой системой хранения данных** (*Network Attached Storage, NAS*), представляющей собой компьютер с дисковым массивом, подключенный обычно к локальной сети и поддерживающий работу по принятым в этой сети протоколам. Часто диски в NAS объединены в RAID массив. Несколько таких компьютеров могут быть объединены в одну систему, обеспечивая надёжность хранения данных, простой доступ для пользователей и хорошую масштабируемость.

**Серверная ферма** – это множество серверов, соединенных сетью передачи данных и работающих как единое целое. Серверная ферма обычно является ядром крупного центра обработки данных (ЦОД), обеспечивающего распределенную обработку данных.

К перечисленным типам сетей следует добавить:

- беспроводные ЛВС;
- виртуальные локальные вычислительные сети;
- иерархические сети;

**Беспроводная ЛВС** (*wireless LAN – WLAN*) – локальная сеть, использующая для передачи данных инфракрасное излучение или чаще всего радиоволны.

**Виртуальная локальная вычислительная сеть (ВЛВС)** (*virtual LAN – VLAN*) – логическое объединение узлов локальной сети, позволяющее выделить пользователей одной рабочей группы с общими интересами в отдельный сетевой сегмент. При этом объединяемые узлы могут принадлежать различным физическим сегментам.

**Иерархическая сеть** (*hierarchical network*) – сеть, в которой главным вычислительным центром является одна хост-машина, а терминалами – остальные сетевые устройства. Это традиционная архитектура, противоположная современной архитектуре распределенных вычислений, в которых интеллектуальные рабочие станции играют более активную роль в вычислительном процессе.

### **1.2.3. Администрирование компьютерных сетей**

Важным требованием к любой компьютерной сети, обеспечивающим эффективное функционирование, является её **управляемость**, заключающаяся в возможности:

- централизованного наблюдения и контроля состояния основных элементов сети, отдельных подсистем и сети в целом;
- выявления и устранения возникающих в процессе функционирования сети проблем, таких как сбои и отказы отдельных устройств сети, определение и устранение перегрузок и т.д.;
- сбора и анализа данных для оценки производительности сети и планирования развития сети;
- обеспечения информационной безопасности и защиты данных и т.п.

Для реализации перечисленных возможностей необходимо в сети иметь специальные автоматизированные средства администрирования, взаимодействующие с техническими и программными средствами сети с помощью коммуникационных протоколов.

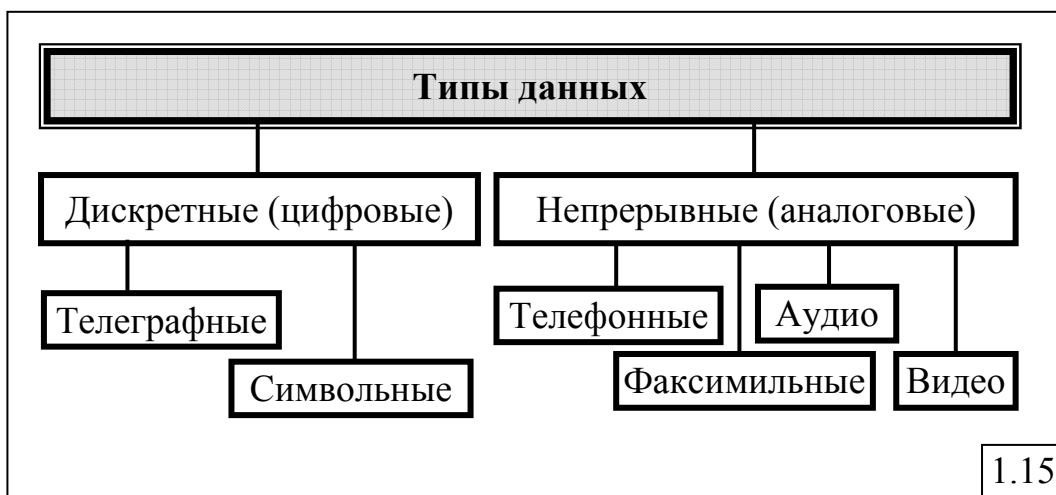
Поддержка и обеспечение эффективного функционирования компьютерной сети за счет принятия своевременных организационных решений по управлению сетью на основе анализа характеристик функционирования и текущего состояния сети реализуется в рамках **администрирования** компьютерной сети сетевым администратором.

К основным функциям администрирования сети относятся:

- наблюдение за потоками данных;
- установка новых версий программного обеспечения;
- создание и поддержание таблиц маршрутизации и коммутации;
- диагностика состояния компонентов сети;
- контроль ошибок и устранение простых отказов;
- замена отказавших узлов резервными;
- реконфигурация сети;
- поддержка отказоустойчивости компьютерной сети;
- добавление новых пользователей;
- определение прав пользователей сети при их обращении к разным ресурсам: файлам, каталогам, принтерам и т.д.;
- ограничение возможностей пользователей в выполнении тех или иных системных действий.

### **1.2.4. Типы данных**

Первоначально сети ЭВМ строились для обработки и передачи компьютерных данных, представляемых в цифровой (дискретной) форме. Современные компьютерные сети ориентированы на передачу и обработку самых разнообразных данных, которые могут быть разделены на следующие типы (рис.1.15).



1. **Телеграфные данные** – дискретные данные, представляемые в виде импульсов постоянного или переменного тока, передаваемые по телеграфным каналам связи (ТгКС).

2. **Телефонные (голосовые) данные** – речь в спектре частот от 80 до 12000 Гц, передаваемая по телефонным КС (ТфКС), называемым также *каналами тональной частоты* (ТЧ). Речь по таким каналам передаётся в ограниченной полосе частот от 300 Гц до 3400 Гц, что обеспечивает разборчивость фраз более 99%.

3. **Факсимильные данные** – неподвижные изображения.

4. **Аудиоданные** (звуковое вещание) – в отличие от телефонных, кроме речи передается музыка, пение и т.п. в спектре частот от 20 Гц до 20 кГц. Для качественной передачи аудио данных достаточна полоса частот от 30 Гц до 15 кГц.

5. **Видеоданные** (телевизионное вещание) – совокупность движущихся изображений и звукового сопровождения в спектре частот от 40 Гц до 6 МГц. В современных компьютерных сетях различают видеоданные трёх типов, отличающиеся требованиями к качеству передачи:

- **видеоконференцсвязь**, представляющая собой медленно изменяющиеся изображения и характеризующаяся *невысокими требованиями к качеству передачи*;
- **телеизионное вещание обычного качества**;
- **телеизионное вещание высокой чёткости**.

6. **Символьные (цифровые, компьютерные) данные** – совокупность символов, например двоичных символов в компьютерах.

Телеграфные и цифровые данные по своей природе относятся к *дискретным* данным, остальные – к *непрерывным* данным, но которые могут быть представлены (закодированы) в цифровой форме.

Телефонные, аудио- и видеоданные относятся к так называемым **мультимедийным** данным, к которым предъявляются специфические требования к качеству передачи по сравнению с обычными компьютерными (цифровыми) данными.

## 1.3. Многоуровневая организация вычислительных сетей

### 1.3.1. Требования к организации компьютерных сетей

Для обеспечения эффективного функционирования к компьютерным сетям предъявляются требования, основными среди которых являются (рис.1.16):

1) **открытость** – возможность добавления в сеть новых компонентов (узлов и каналов связи, средств обработки данных) без изменения существующих технических и программных средств;

2) **гибкость** – сохранение работоспособности при изменении структуры сети в результате сбоев и отказов отдельных компонентов сети или при замене оборудования;

3) **совместимость** – возможность работы в сети оборудования разного типа и разных производителей;

4) **масштабируемость** – способность сети увеличивать свою производительность при добавлении ресурсов (узлов и каналов связи);

5) **эффективность** – обеспечение требуемого качества обслуживания пользователей, задаваемого в виде показателей производительности, временных задержек, надежности и т.д., при минимальных затратах.



Указанные требования реализуются за счет *многоуровневой организации управления процессами* в сети, в основе которой лежат понятия **процесса, уровня, интерфейса и протокола** (рис.1.17).



### 1.3.2. Понятия процесса и уровня

Функционирование вычислительных систем и сетей удобно описывать в терминах процессов.

**Процесс** – динамический объект, реализующий целенаправленный акт обработки или передачи данных.

Процессы делятся на:

1) **прикладные** – обработка данных в ЭВМ и терминальном оборудовании, а также передача данных в СПД;

2) **системные** – обеспечение прикладных процессов (активизация терминала для прикладного процесса, организация связи между процессами и др.).

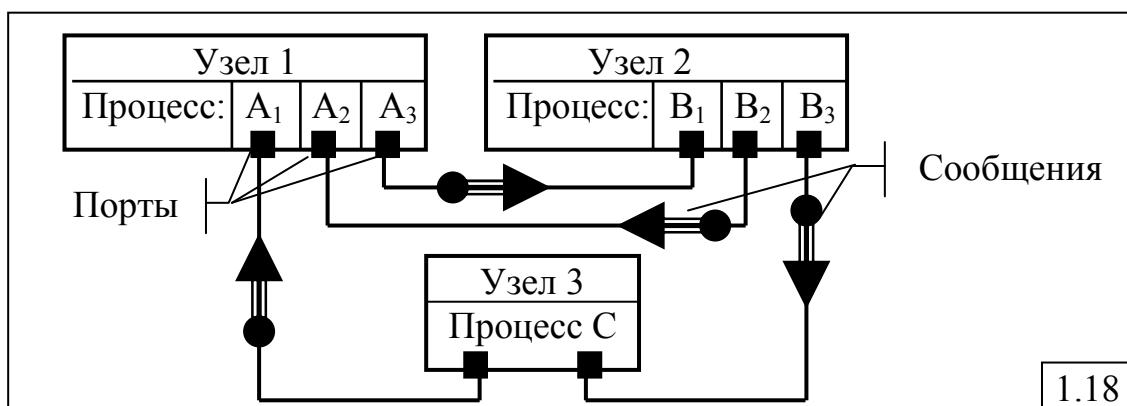
Данные между процессами передаются в виде сообщений через логические программно-организованные точки, называемые **портами**.

Порты разделяются на *входные* и *выходные*.

Промежуток времени, в течение которого взаимодействуют процессы, называется **сеснсом** или **сессией**.

В каждом узле обработки данных (компьютере) могут одновременно выполняться несколько независимых прикладных процессов, связанных, например, с обработкой данных (такие процессы называются вычислительными процессами). Эти процессы путём обмена сообщениями через соответствующие порты могут взаимодействовать с прикладными процессами, протекающими в других узлах вычислительной сети так, как это показано на рис.1.18.

Здесь в узле 1 и 2 выполняются по 3 прикладных процесса  $A_1, A_2, A_3$  и  $B_1, B_2, B_3$  соответственно, а в узле 3 выполняется один прикладной процесс  $C$ . Эти процессы через соответствующие порты обмениваются сообщениями, причем процесс  $C$  обменивается сообщениями через два порта: входной, через который поступают сообщения от процесса  $B_3$ , и выходной, который служит для передачи сообщений от процесса  $C$  к процессу  $A_1$ .



Одним из основных понятий многоуровневой организации управления процессами в компьютерных сетях является понятие уровня, которое лежит в основе моделей всех сетевых технологий.

**Уровень (layer)** – понятие, позволяющее разделить всю совокупность функций обработки и передачи данных в вычислительной сети на несколько иерархических групп. На каждом уровне реализуются определенные функции обработки и передачи данных с помощью аппаратных и/или программных средств сети. Каждый уровень обслуживает вышележащий уровень и, в свою очередь, пользуется услугами нижележащего.

### 1.3.3. Модель взаимодействия открытых систем (OSI-модель)

Международная Организация по Стандартам (МОС, International Standards Organization – ISO) предложила в качестве стандарта открытых систем семиуровневую коммуникационную модель (рис.1.19), известную как **OSI-модель** (Open Systems Interconnection) – модель Взаимодействия Открытых Систем (ОСС).



Каждый уровень OSI-модели отвечает за отдельные специфические функции в коммуникациях и реализуется техническими и программными средствами вычислительной сети.

#### 1.3.3.1. Физический уровень

**Уровень 1 – физический (physical layer)** – самый низкий уровень OSI-модели, определяющий процесс прохождения сигналов через среду передачи между сетевыми устройствами (узлами сети).

*Реализует управление каналом связи:*

- подключение и отключение канала связи;
- формирование передаваемых сигналов и т.п.

*Описывает:*

- механические, электрические и функциональные характеристики среды передачи;
- средства для установления, поддержания и разъединения физического соединения.

*Обеспечивает при необходимости:*

- кодирование данных;
- модуляцию сигнала, передаваемого по среде.

Данные физического уровня представляют собой поток битов (последовательность нулей или единиц), закодированные в виде электрических, оптических или радио сигналов.

Из-за наличия помех, действующих на электрическую линию связи, **достоверность передачи**, измеряемая как вероятность искажения одного бита, составляет  $10^{-4} - 10^{-6}$ . Это означает, что в среднем на 10000 – 1000000 бит передаваемых данных один бит оказывается искажённым.

### 1.3.3.2. Канальный уровень

**Канальный уровень** или **уровень передачи данных** (*data link layer*) является вторым уровнем OSI-модели.

*Реализует управление:*

- доступом сетевых устройств к среде передачи, когда два или более устройств могут использовать одну и ту же среду передачи;
- надежной передачей данных в канале связи, позволяющей увеличить достоверность передачи данных на 2-4 порядка.

*Описывает* методы доступа сетевых устройств к среде передачи, основанные, например, на передаче маркера или на соперничестве.

*Обеспечивает:*

- функциональные и процедурные средства для установления, поддержания и разрыва соединения;
- управление потоком для предотвращения переполнения приемного устройства, если его скорость меньше, чем скорость передающего устройства;
- надежную передачу данных через физический канал с вероятностью искажения данных  $10^{-8} - 10^{-9}$  за счёт применения методов и средства контроля передаваемых данных и повторной передачи данных при обнаружении ошибки.

Таким образом, канальный уровень обеспечивает достаточно надежную передачу данных через ненадежный физический канал.

Блок данных, передаваемый на канальном уровне, называется **кадром (frame)**.

На канальном уровне появляется свойство *адресуемости* передаваемых данных в виде *физических (машинных) адресов*, называемых также **MAC-адресами** и являющихся обычно уникальными идентификаторами сетевых устройств.

Как будет показано в разделе 3, универсальные MAC-адреса в ЛВС Ethernet и Token Ring являются 6-байтными и записываются в шестнадцатеричном виде, причём байты адреса разделены дефисом, например: **00-19-45-A2-B4-DE**.

К процедурам канального уровня относятся:

- добавление в кадры соответствующих адресов;
- контроль ошибок;
- повторная, при необходимости, передача кадров.

На канальном уровне работают ЛВС Ethernet, Token Ring и FDDI.

#### 1.3.3.3. Сетевой уровень

**Сетевой уровень** (network layer), в отличие от двух предыдущих, отвечает за передачу данных в СПД и управляет маршрутизацией сообщений – передачей через несколько каналов связи по одной или нескольким сетям, что обычно требует включения в пакет *сетевого адреса получателя*.

Блок данных, передаваемый на сетевом уровне, называется *пакетом (packet)*.

**Сетевой адрес** – это специфический идентификатор для каждой промежуточной сети между источником и приемником информации.

Сетевой уровень реализует:

- обработку ошибок;
- мультиплексирование пакетов;
- управление потоками данных.

Самые известные протоколы этого уровня:

- X.25 в сетях с коммутацией пакетов;
- IP в сетях TCP/IP;
- IPX/SPX в сетях NetWare.

Кроме того, к сетевому уровню относятся протоколы построения маршрутных таблиц для маршрутизаторов: OSPF, RIP, ES-IS, IS-IS.

#### 1.3.3.4. Транспортный уровень

**Транспортный уровень** (transport layer) наиболее интересен из высших уровней для администраторов и разработчиков сетей, так как он управляет сквозной передачей сообщений между оконечными узлами сети ("end-end"), обеспечивая надежность и экономическую эффективность передачи данных независимо от пользователя. При этом оконечные узлы возможно взаимодействуют через несколько узлов или даже через несколько транзитных сетей.

На транспортном уровне реализуется:

- 1) преобразование длинных сообщений в пакеты при их передаче в сети и обратное преобразование;
- 2) контроль последовательности прохождения пакетов;
- 3) регулирование трафика в сети;
- 4) распознавание дублированных пакетов и их уничтожение.

Способ коммуникации "end-end" облегчается еще одним способом адресации – *адресом процесса*, который соотносится с определенной прикладной программой (прикладным процессом), выполняемой на компьютере. Компьютер обычно выполняет одновременно несколько программ, в связи с чем необходимо знать какой прикладной программе (процессу) предназначено поступившее сообщение. Для этого на транспортном уровне используется специальный адрес, называемый *адресом порта*. Сетевой уровень доставляет каждый пакет на конкретный адрес компьютера, а транспортный уровень передаёт полностью собранное сообщение конкретному прикладному процессу на этом компьютере.

Транспортный уровень может предоставлять различные типы сервисов, в частности, передачу данных без установления соединения или с предварительным установлением соединения. В последнем случае перед началом передачи данных с использованием специальных управляющих пакетов устанавливается соединение с транспортным уровнем компьютера, которому предназначены передаваемые данные. После того как все данные переданы, подключение заканчивается. При передаче данных без установления соединения транспортный уровень используется для передачи одиночных пакетов, называемых *дейтаграммами*, не гарантируя их надежную доставку. Передача данных с установлением соединения применяется для надежной доставки данных.

#### **1.3.3.5. Сеансовый уровень**

**Сеансовый уровень** (session layer) обеспечивает обслуживание двух "связанных" на уровне представления данных объектов сети и управляет ведением диалога между ними путем синхронизации, заключающейся в установке служебных меток внутри длинных сообщений. Эти метки позволяют после обнаружения ошибки повторить передачу данных не с самого начала, а только с того места, где находится ближайшая предыдущая метка по отношению к месту возникновения ошибки.

Сеансовый уровень предоставляет услуги по организации и синхронизации обмена данными между процессами уровня представлений.

На сеансовом уровне реализуется:

- 1) *установление соединения с адресатом и управление сеансом*;
- 2) *координация связи прикладных программ на двух рабочих станциях*.

#### **1.3.3.6. Уровень представления**

**Уровень представления** (presentation layer) обеспечивает совокупность служебных операций, которые можно выбрать на прикладном уровне для интерпретации передаваемых и получаемых данных. Эти служебные операции включают в себя:

- *управление информационным обменом*;
- *преобразование (перекодировка) данных* во внутренний формат каждой конкретной ЭВМ и обратно;
- *шифрование и дешифрование данных* с целью защиты от несанкционированного доступа;
- *сжатие данных*, позволяющее уменьшить объём передаваемых данных, что особенно актуально при передаче мультимедийных данных, таких как аудио и видео.

Служебные операции этого уровня представляют собой основу всей семиуреневой модели и *позволяют связывать воедино терминалы и средства вычислительной техники (компьютеры) самых разных типов и производителей*.

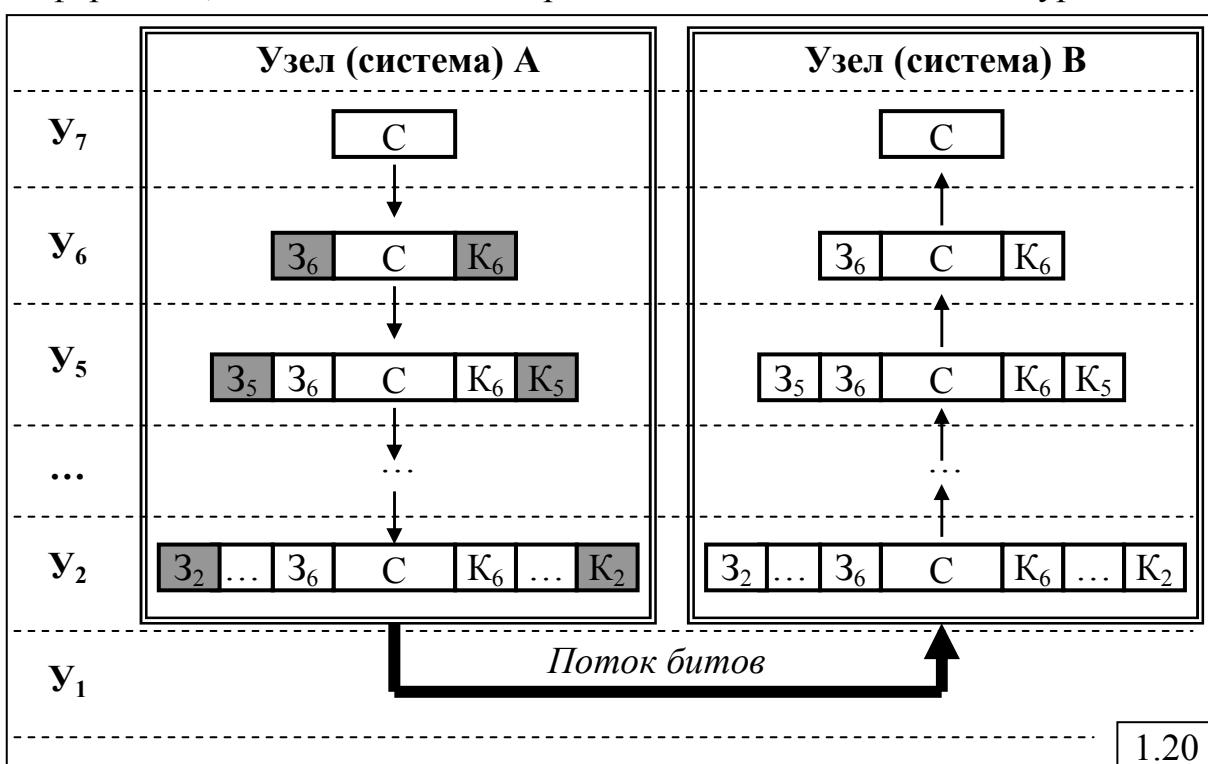
### 1.3.3.7. Прикладной уровень

**Прикладной уровень** (application layer) обеспечивает непосредственную поддержку прикладных процессов и программ конечного пользователя, а также управление взаимодействием этих программ с различными объектами сети. Другими словами, прикладной уровень обеспечивает интерфейс между прикладным ПО и системой связи. Он предоставляет прикладной программе доступ к различным сетевым службам, включая передачу файлов и электронную почту.

### 1.3.3.8. Процесс передачи сообщений в OSI-модели

Транспортный, сеансовый, представительский и прикладной уровни (уровни 4 – 7) относятся к **высшим уровням OSI-модели**. В отличие от **низших уровней** (1 – 3) они отвечают за коммуникации типа "end-end", т.е. коммуникации между источником и приемником сообщения.

В соответствии с OSI-моделью сообщения в передающем **узле А** (компьютере) проходят вниз через все уровни от верхнего  $Y_7$  до самого нижнего  $Y_1$  (рис.1.20), причем многоуровневая организация управления процессами в сети порождает необходимость модифицировать на каждом уровне передаваемые сообщения применительно к функциям, реализуемым на этом уровне. Модификация заключается в добавлении к сообщению на каждом уровне соответствующих заголовков  $Z_i$  и концевиков  $K_i$ , называемых **обрамлением сообщения**, в которых содержится информация об адресах взаимодействующих объектов, а также информация, необходимая для обработки сообщения на данном уровне.



Когда сообщение достигает низшего (физического) уровня  $Y_1$ , оно пересыпается к другому узлу **В** в виде потока битов, представляющего собой физические сигналы (электрические, оптические или радиоволны)

передающей среды. В приемном узле (компьютере) сообщение от нижнего физического уровня  $Y_1$  проходит наверх через все уровни, где от него отсекаются соответствующие заголовки и концевики. Таким образом, каждый уровень оперирует с собственным заголовком и концевиком, за счет чего обеспечивается независимость данных, относящихся к разным уровням управления передачей сообщений.

### 1.3.4. IEEE-модель локальных сетей

Институт инженеров по электронике и электротехнике (Institute of Electrical and Electronics Engineers – IEEE) предложил вариант OSI-модели, используемый при разработке и проектировании локальных сетей и получивший название **IEEE-модели**.

В IEEE-модели канальный уровень разбивается на два подуровня (рис.1.21):

- *подуровень управления доступом к среде передачи (Medium Access Control, MAC-подуровень)*, описывающий способ доступа сетевого устройства к среде передачи данных;
- *подуровень управления логическим соединением (Logical Link Control, LLC-подуровень)*, описывающий способ установления и завершения соединения, а также способ передачи данных.

**LLC-подуровень** представляет более высоким уровням возможность управлять качеством услуг и обеспечивает сервис трех типов:

- 1) сервис без установления соединения и без подтверждения доставки;
- 2) сервис без установления соединения с подтверждением доставки;
- 3) сервис с установлением соединения.

Сервис без установления соединения и подтверждения доставки не гарантирует доставку данных и обычно применяется в приложениях, использующих для контроля передачи данных и защиты от ошибок протоколы более высоких уровней.

Сервис с установлением соединения обеспечивает надежный обмен данными.

Главной функцией **MAC-уровня** является обеспечение доступа к каналу передачи данных. На этом уровне формируется физический адрес устройства, который называется **MAC-адресом**. Каждое устройство сети идентифицируется этим **уникальным** адресом, который присваивается всем сетевым устройствам.

Уровни OSI-модели	Подуровни IEEE-модели
7 - прикладной	
6 - представления	
5 - сеансовый	
4 - транспортный	
3 - сетевой	
<b>2 - канальный</b>	<b>LLC</b>
	<b>MAC</b>
1 - физический	

1.21

### 1.3.5. Понятия интерфейса и протокола

Описание сетевой технологии и алгоритма функционирования компьютерной сети связано с описанием соответствующих интерфейсов и протоколов.

**Интерфейс** – соглашение о взаимодействии (границе) между уровнями одной системы, определяющее структуру данных и способ (алгоритм) обмена данными между соседними уровнями OSI-модели.

Интерфейсы подразделяются на:

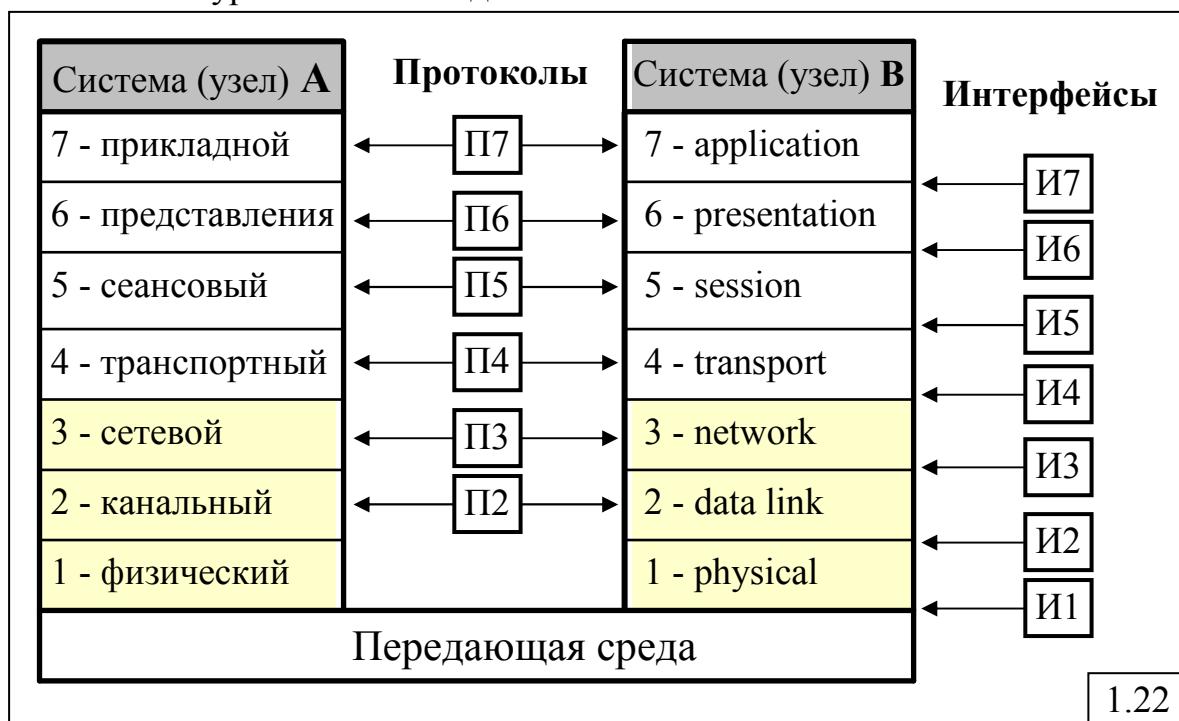
- 1) *схемные* – совокупность интерфейсных шин;
- 2) *программные* – совокупность процедур реализующих порядок взаимодействия между уровнями.

**Протокол** – совокупность правил, регламентирующих формат и процедуры взаимодействия процессов *одноименных уровней* на основе обмена сообщениями.

Описание протокола предполагает задание:

- 1) **логической характеристики протокола**, определяющей *структуру* (формат) и *содержание* (семантику) *сообщений* путём перечисления типов сообщений и их смысла;
- 2) **процедурной характеристики протокола**, представляющей собой *правила выполнения действий*, предписанных протоколом взаимодействия и задаваемых в форме: операторных схем алгоритмов, автоматных моделей, сетей Петри и др.

Рис.1.22 иллюстрирует понятия интерфейсов и протоколов и их соответствие уровням OSI-модели.



Как сказано выше, каждая сетевая технология характеризуется совокупностью протоколов и интерфейсов разных уровней OSI-модели. Совокупность протоколов всех уровней некоторой сетевой технологии

называется **стеком протоколов**. В настоящее время существует большое количество разнообразных сетевых технологий и соответствующих им стеков протоколов, наиболее известными и распространёнными среди которых являются стеки протоколов: TCP/IP, XNS, IPX, AppleTalk, DECnet, SNA. Краткое описание перечисленных стеков протоколов приводится в конце данного раздела (см. п.1.7).

### 1.3.6. Протокольные блоки данных (PDU)

Данные, передаваемые на разных уровнях в сети, формируются в виде блоков, называемых **протокольными блоками данных** (Protocol Data Unit – PDU). PDU представляет собой единицу данных, передаваемую как единое целое и имеющую обрамление в виде заголовка со служебной информацией (адрес отправителя, адрес получателя, длина блока и т.п.) и, возможно, концевика.

На разных уровнях OSI-модели используются разные PDU, имеющие специальные названия. Наибольшее распространение получили следующие названия блоков данных: *сообщение, дейтаграмма, пакет, кадр* (рис. 1.23).

<b>Уровни OSI-модели</b>		<b>PDU</b>	
7	Прикладной	<i>Сообщение</i>	Message
...	...	...	...
4	Транспортный	<i>Дейтаграмма</i>	Datagram
3	Сетевой	<i>Пакет</i>	Packet
2	Канальный	<i>Кадр</i>	Frame

1.23

**Сообщение (message)** – блок данных, рассматриваемых как единое целое при передаче между двумя пользователями (процессами) и имеющих определенное смысловое значение. Сообщения используются на 7-м уровне OSI-модели для передачи данных между прикладными процессами и могут иметь произвольную длину.

**Кадр (frame)** – блок данных 2-го (канального) уровня OSI-модели, имеющий ограниченную длину и передаваемый как единое целое в локальной сети или по выделенному каналу связи между двумя узлами.

**Пакет (packet)** – блок данных на 3-го (сетевого) уровня OSI-модели, имеющий ограниченную длину и представляющий собой единицу передачи данных в СПД.

**Дейтаграмма (datagram)** – блок данных 4-го (транспортного) уровня OSI-модели, передаваемый дейтаграммным способом без установления соединения.

Предельный размер кадра, пакета и дейтаграммы зависит от сетевой технологии и устанавливается соответствующими протоколами, определяющими формат и допустимый размер блока данных.

Кроме перечисленных названий в стеке протоколов TCP/IP блок данных протокола TCP называется **сегментом**, который получается путём вырезания из неструктурированного **потока** байтов, поступающих к протоколу TCP в рамках логического соединения от протоколов более высокого уровня.

Для блоков данных 5-го и 6-го уровней OSI-модели нет устоявшихся общепринятых названий, что в значительной степени обусловлено отсутствием этих уровней в наиболее распространённом стеке протоколов TCP/IP.

Отметим, что в ATM-сетях данные передаются в виде блоков фиксированного размера в 53 байта, которые называются **ячейками (cell)**.

### 1.3.7. Сетевая операционная система

Основной задачей сетевой операционной системы (ОС) является организация процессов обработки и передачи данных в компьютерной сети, связанная, в том числе, с разделением ресурсов сети (например, дискового пространства) и администрированием сети (определение разделяемых ресурсов, паролей и прав доступа для каждого пользователя или группы пользователей).

Для решения этих задач сетевая операционная система, в отличие от операционной системы ЭВМ, должна обладать встроенными возможностями для работы в сети за счёт **дополнительных функций**, таких как:

- поддержка функционирования сетевого оборудования – маршрутизаторов, коммутаторов, шлюзов и т.п.;
- поддержка сетевых протоколов, включая протоколы маршрутизации и протоколы авторизации;
- реализация доступа к среде передачи данных и к удалённым ресурсам сети и т.д.

Совокупность операционных систем отдельных ЭВМ, входящих в состав вычислительной сети можно рассматривать как составную часть сетевой операционной системы. При этом разные ЭВМ могут работать под управлением как одинаковых, так и разных ОС (Windows XP, Windows Vista, UNIX, NetWare, Solaris и т.д.). Последнее характерно для современных вычислительных сетей, объединяющих обычно множество компьютеров разных типов различных производителей. Все эти ОС обеспечивают управление вычислительным процессом и распределением ресурсов в каждой из конкретной ВС, выполняя следующие функции:

- управление памятью, включая распределение и защиту памяти;
- планирование и управление пользовательскими и системными процессами;
- управление файлами и внешними устройствами;
- защита данных и администрирование, включая поддержку отказоустойчивости аппаратных и программных средств;

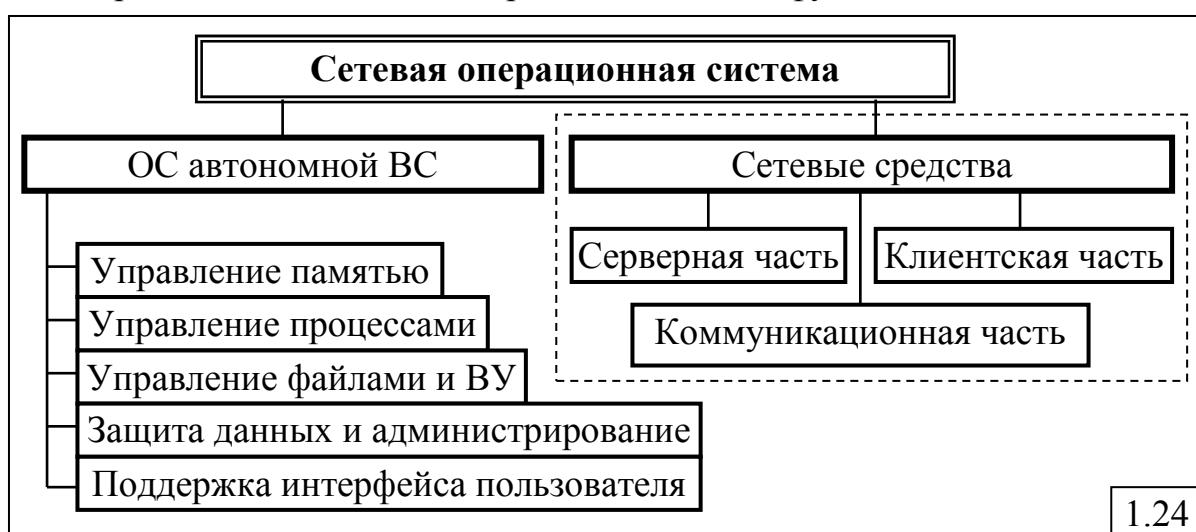
- обеспечение удобного интерфейса для прикладных программ и пользователей и т.д.

Для обеспечения функций по обмену данными между ЭВМ сети операционные системы всех ЭВМ имеют в своём составе дополнительные компоненты – **сетевые средства**, организующие взаимодействие процессов, выполняющихся в разных ЭВМ, и разделение общих ресурсов между пользователями сети. Сетевые средства можно рассматривать как совокупность трёх составляющих:

- **серверная часть ОС**, предназначенная для предоставления локальных ресурсов и услуг в общее пользование;
- **клиентская часть ОС**, обеспечивающая реализацию запросов доступа к удалённым ресурсам и услугам;
- **коммуникационная** (транспортная) часть ОС, обеспечивающая совместно со средствами телекоммуникаций передачу данных в виде сообщений между пользователями вычислительной сети.

Состав сетевой ОС показана на рис.1.24.

Существуют специальные сетевые ОС, которым приданы функции обычных систем (например Windows NT) и обычные ОС, которым приданы сетевые функции (например Windows XP). Сегодня практически все современные ОС имеют встроенные сетевые функции.



1.24

Примерами сетевых операционных систем могут служить:

- Microsoft Windows (95, NT и более поздние);
- Novell NetWare;
- различные UNIX системы, такие как Solaris, и т.д.

Реализация обмена данными между удаленными пользователями – одна из основных функций вычислительной сети. Эффективность передачи данных характеризуется совокупностью показателей (характеристик), в частности, временем и надежностью доставки сообщений, и в значительной степени зависит от структурной и функциональной организации вычислительной сети.

## **1.4. Принципы структурной организации компьютерных сетей**

Структурная организация компьютерной сети определяется:

- 1) *составом узлов* (номенклатура и количество сетевых устройств, компьютеров и терминалов) и *топологией* сети передачи данных;
- 2) *производительностью* узлов обработки и передачи данных и *пропускной способностью* каналов связи.

Одной из важнейшей составляющей структурной организации компьютерной сети является её топология, оказывающая существенное влияние как на качество передачи, так и на эффективность обработки данных.

Ниже рассматриваются типовые топологии, используемые при построении компьютерных сетей, и проводится их сравнительный анализ.

### **1.4.1. Сетевые топологии**

Многообразие типов компьютерных сетей обуславливает многообразие топологий, обеспечивающих выполнение заданных требований к качеству их функционирования. В современных компьютерных сетях наибольшее распространение получили следующие топологии (рис. 1.25):

- а) «Общая шина»;
- б) «Дерево»;
- в) «Звезда (узловая)»;
- г) «Кольцо»;
- д) «Полносвязная»;
- е) «Многосвязная (ячеистая)»;
- ж) «Смешанная».

Следует различать *физическую* и *логическую* топологию сети.

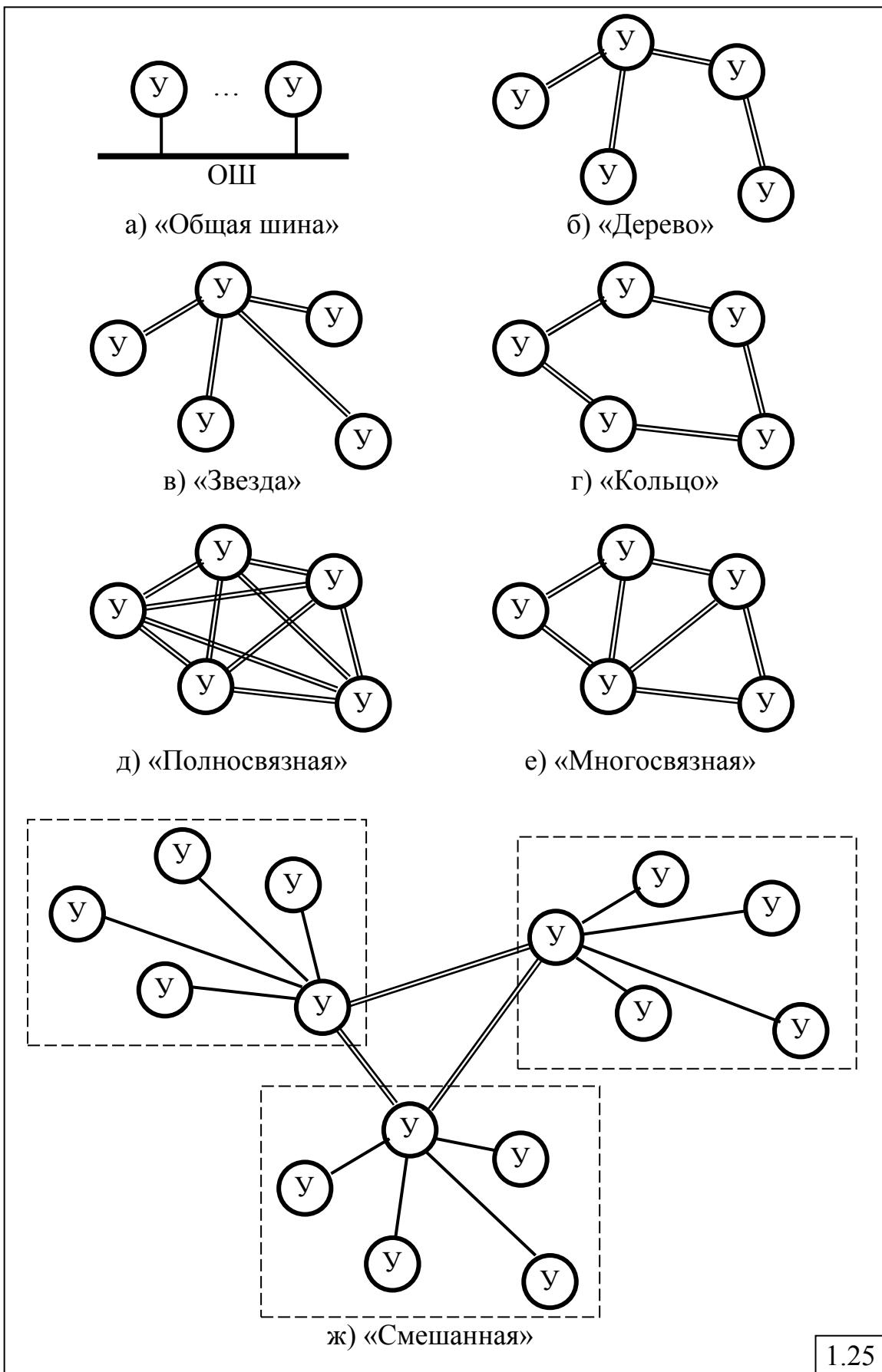
**Физическая (структурная) топология** отображает структурную взаимосвязь узлов сети.

**Логическая (функциональная) топология** определяется функциональной взаимосвязью узлов сети, то есть отображает последовательность передачи данных между узлами сети.

Физическая и логическая топологии сети, как мы увидим ниже, могут различаться.

**Топология «общая шина»** (рис. 1.25, а), представляет собой кабель, называемый *шиной* или *магистралью*, к которому подсоединенны компьютеры сети. Данные, передаваемые любым компьютером, занимают шину на всё время передачи, при этом остальные компьютеры, имеющие данные для передачи, должны ждать освобождения общей шины. Таким образом, в каждый момент времени передавать данные может только один компьютер сети, и пропускная способность общей шины некоторым образом распределяется между всеми компьютерами. Основным достоинством топологии «общая шина» является простота структурной и функциональной организации и, как следствие, дешевизна, что делает её

наиболее привлекательной для локальных сетей. Недостаток этой топологии заключается в низкой надёжности сети – выход из строя общей шины приводит к полной остановке сети.



1.25

**Топология «дерево»** (рис. 1.25,б) формируется по принципу «минимума суммарной длины связей между узлами сети» и является основой для построения иерархических сетей. В таких сетях для передачи данных существует только один путь между двумя любыми узлами, что делает процедуру маршрутизации тривиальной.

**Топология «звезда»** (рис. 1.25,в) содержит один центральный узел, к которому присоединяются все остальные узлы сети. В качестве центрального узла может выступать мощный компьютер, к которому присоединены менее мощные периферийные компьютеры. В этом случае центральный компьютер может предоставлять свои ресурсы (файлы, дисковое пространство, ресурсы процессора) периферийным компьютерам, либо выполнять функции маршрутизатора при обмене данными между компьютерами сети. Возможна и другая организация топологии «звезда», когда в качестве центрального узла используется сетевое устройство (например, концентратор или коммутатор), с помощью которого все компьютеры связаны в единую сеть и которое обеспечивает только обмен данными между компьютерами. Если в качестве центрального узла сети используется концентратор, то логическая топология сети может быть как «звезда», так и «общая шина».

**В топологии «кольцо»** каждый узел связан с двумя другими узлами так, как это показано на рис.1.25,г), при этом данные, переданные каким-либо узлом, пройдя через все другие узлы сети, могут вернуться в исходный узел. Основным достоинством этой топологии по сравнению с рассмотренными выше топологиями является возможность передачи данных по двум направлениям, то есть наличие в каждом узле альтернативного пути, по которому могут быть переданы данные при отказе основного пути. При этом стоимость сети при небольшом количестве узлов соизмерима со стоимостью сетей с топологиями «звезда» и «дерево». Однако с увеличением количества узлов в сети стоимость может оказаться значительной.

**Топология «полносвязная»** (рис. 1.25,д) формируется по принципу «каждый с каждым», то есть каждый узел сети имеет связь со всеми другими узлами. Такая топология является наиболее эффективной по всем основным показателям качества функционирования: надёжности, производительности и т.д., но из-за большой стоимости практически не используется.

**Топология «многосвязная»** или **«ячеистая»** (рис. 1.25,е) представляет собой топологию произвольного вида, которая формируется по принципу «каждый узел сети связан с не менее чем двумя другими узлами», то есть для каждого узла сети всегда должен быть хотя бы один альтернативный путь. Такая топология может быть получена путем удаления из полносвязной топологии некоторых каналов связи (например, не использующихся для передачи данных или мало загруженных), что во многих случаях существенно снижает стоимость сети.

**Топология «смешанная»** представляет собой любую комбинацию рассмотренных выше топологий и образуется обычно при объединении нескольких локальных сетей, например так, как это показано на рис.1.25,ж), где 3 сети с топологией «звезда» связаны в сеть с топологией «кольцо».

### 1.4.2. Сравнительный анализ топологий

Сравнительный анализ топологий компьютерных сетей будем проводить на основе следующих признаков:

1) *простота структурной организации*, измеряемая количеством каналов связи между узлами сети;

2) *надёжность*, определяемая наличием «узких мест», при отказе которых сеть перестаёт функционировать или же резко падает её эффективность, а также наличием альтернативных путей, благодаря которым, при отказах отдельных каналов и узлов, передача данных может осуществляться в обход отказавших элементов;

3) *производительность сети*, измеряемая количеством блоков данных (сообщений или пакетов), передаваемых в сети за единицу времени с учётом возможного снижения эффективной скорости передачи данных из-за конфликтов в сети;

4) *время доставки* сообщений (пакетов), измеряемое, например, в *хопах (hop)*, представляющих собой число промежуточных каналов или узлов на пути передачи данных;

5) *стоимость* топологии, зависящая как от состава и количества оборудования (например, каналов при заданном количестве узлов), так и от сложности реализации.

Перечисленные признаки взаимосвязаны. Естественно, что более эффективные топологии с позиций надёжности, производительности и времени доставки являются более сложными в реализации и, как следствие, более дорогими. Сравнение рассмотренных выше топологий будем проводить на качественном уровне, результаты которого представлены в виде табл.1.1. В таблице наилучшему показателю соответствует значение 1, заключённое в фигурные скобки, а наихудшему показателю – значение 5.

Таблица 1.1

<b>Показатель</b>	<b>Топология</b>						
	ОШ	Звезда	Дерево	Кольцо	Полно-связная	Много-связная	Смешанная
Простота	{1}	2	2	3	5	4	4
Стоимость	{1}	2	2	3	5	4	4
Надёжность	5	4	4	3	{1}	2	2
Производит.	5	4	4	3	{1}	2	2
Время дост.	3	2	4	5	{1}	3	3

**Простота структурной организации и стоимость.** По количеству каналов связи *наиболее простой* топологией компьютерной сети является топология «*общая шина*», которая содержит один канал связи, объединяющий все компьютеры сети. Простота такой сети обусловлена также отсутствием каких-либо специальных сетевых устройств, таких как маршрутизаторы, коммутаторы и т.п. Единственным необходимым устройством для подключения к общейшине служит сравнительно простое устройство – сетевой адаптер (сетевая карта). Еще одним фактором, обуславливающим простоту этой топологии, является простота подключения новых компьютеров к общейшине. Естественно, что простота структурной организации топологии «*общая шина*» определяет и её низкую стоимость.

К сравнительно простым и дешёвым топологиям можно отнести топологии «*дерево*» и «*звезда*», что обусловлено небольшим количеством связей (каналов)  $N_K$  между узлами сети, которое на единицу меньше количества узлов  $N_y$ :  $N_K = N_y - 1$ .

Топология «*кольцо*» по показателю «простота» занимает следующую позицию после рассмотренных топологий. Легко убедиться, что для этой топологии количество связей (каналов) между узлами сети равно количеству узлов:  $N_K = N_y$ .

Полносвязная топология является наиболее сложной, поскольку имеет максимально возможное количество связей (каналов) в сети, равное  $N_K = \frac{N_y(N_y - 1)}{2}$ . Следствием этого является высокая стоимость сети, что делает нецелесообразным применение такой топологии при построении компьютерных сетей, особенно с большим числом узлов.

При построении глобальных сетей наибольшее распространение получили топологии многосвязные (ячеистые) и смешанные, занимающие промежуточное положение между простыми и дешёвыми топологиями «*звезда*» и «*кольцо*» и полносвязной топологией.

**Надёжность.** По показателю надёжности *наилучшей*, естественно, является *полносвязная* топология, которая характеризуется отсутствием «узких мест» с точки зрения надёжности и наличием максимально возможного количества альтернативных путей для передачи данных, которые могут быть задействованы при отказах одного или даже нескольких каналов и узлов сети. При этом сеть продолжает функционировать и передавать данные, правда, с более низким качеством.

Наименее надёжными топологиями являются топологии «*общая шина*», «*звезда*» и «*дерево*», имеющие «узкие места» соответственно в виде общейшины, центрального и корневого узла сети, при отказе которых сеть перестает функционировать.

Несколько выше надежность топологии «*кольцо*» за счёт наличия альтернативного пути, обратного по отношению к основному пути

передачи данных, что позволяет при отказах канала или узла сети передавать сообщения в противоположном направлении.

Многосвязные (ячеистые) и смешанные топологии за счёт наличия, в общем случае, нескольких альтернативных путей для передачи данных, обладают более высокой надёжностью, чем топология «кольцо», приближаясь по этому показателю к полносвязной топологии.

**Производительность сети.** Под производительностью сети передачи данных будем понимать количество пакетов, передаваемых в сети за единицу времени. Очевидно, что производительность сети зависит от количества пакетов, одновременно находящихся в сети: чем больше пакетов в сети, тем выше её производительность. Производительность сети растёт до некоторого предельного значения, называемого *пропускной способностью сети передачи данных* (СПД). Значение пропускной способности СПД определяется узким местом сети – наиболее загруженным узлом или каналом связи, загрузка которого близка к единице. Ясно, что пропускная способность СПД в значительной степени определяется пропускными способностями каналов связи, измеряемыми количеством бит, передаваемых по каналу за единицу времени, и количеством каналов связи в СПД, по которым одновременно могут передаваться пакеты, причем, чем больше каналов в СПД, тем выше производительность и пропускная способность сети. Таким образом, при условии, что все каналы связи сравниваемых топологий имеют одинаковые пропускные способности, можно сделать следующий вывод: наибольшей производительностью обладает полносвязная топология, а наименьшей – «общая шина», имеющая только один канал для передачи данных всех компьютеров. Следует также иметь в виду, что в общейшине могут возникать коллизии в результате столкновения данных, одновременно передаваемых от нескольких компьютеров, что ещё больше снижает пропускную способность общей шины. Остальные топологии занимают промежуточное положение между полносвязной топологией и топологией «общая шина».

**Время доставки.** Как и ранее, положим, что все каналы связи сравниваемых топологий имеют одинаковые пропускные способности. В этом случае время доставки пакетов в сети удобно оценивать в *хопах* (hop) – количестве каналов на пути передачи пакетов между узлами сети. Очевидно, что наименьшее время доставки пакетов, равное одному хопу между любыми двумя узлами сети, обеспечивает полносвязная топология. В топологии «звезда» время доставки пакетов не более двух хопов – двух каналов связи между любыми двумя периферийными узлами, путь между которыми пролегает через центральный узел. В многосвязных и смешанных топологиях время доставки несколько больше, чем в топологии «звезда», и зависит от степени связности – количества каналов связи и, соответственно, количества альтернативных путей. Время доставки пакетов в сети с топологией «дерево» зависит от конфигурации связей и, при одном и том же количестве узлов  $N_y$ , может принимать

различные максимальные значения: 2 – в случае конфигурации, совпадающей с топологией «звезда», и  $(N_y - 1)$  – в случае линейной конфигурации, когда все узлы сети, связанные последовательно друг с другом, образуют цепочку:  $Y_1-Y_2-Y_3-\dots-Y_N$ . При достаточно большом количестве узлов наибольшее время доставки может оказаться у сети с топологией «кольцо». Поскольку в реальных сетях с кольцевой топологией пакеты обычно передаются в одном направлении, среднее время доставки, измеренное в хопах, будет равно  $N_y/2$ , где  $N_y$  - количество узлов и, соответственно, каналов связи в сети.

Несколько сложнее оценить время доставки пакетов для сети с топологией «общая шина». Действительно, поскольку канал один – шина, то время доставки равно одному хопу. Однако следует учитывать, что пропускная способность общей шины делится между всеми компьютерами сети, вследствие чего реальное время доставки, измеренное в секундах, может оказаться во много раз больше, чем в канале полносвязной сети с такой же пропускной способностью. Кроме того, возникающие в общей шине коллизии в результате столкновений пакетов от разных компьютеров и необходимость их повторной передачи ещё больше увеличивают время доставки.

Выполненный качественный анализ различных топологий позволяет сделать следующие **выводы**.

Основным требованием, предъявляемым к локальным вычислительным сетям, объединяющим обычно недорогие персональные компьютеры, является *низкая стоимость сетевого оборудования*, что достигается использованием наиболее простых и, следовательно, дешевых топологий: «общая шина», «звезда» и «кольцо». Глобальные вычислительные сети строятся обычно на основе многосвязной или смешанной топологии.

Представленные результаты сравнительного анализа различных сетевых топологий носят относительный характер, то есть показывают уровень того или иного показателя некоторой топологии относительно других топологий, и не могут служить количественной оценкой. Более того, при оценке этих показателей не учитывались значения количественных параметров структурной организации компьютерной сети, таких как пропускные способности и надёжность каналов связи, производительность узлов связи, стоимость компонент сети, эксплуатационные расходы и т.п. Учёт этих параметров в каждом конкретном случае может привести к ситуации, когда более простые топологии оказываются более производительными, а сложные топологии – более дешёвыми, чем простые топологии, например, потому, что в них используются каналы связи с небольшой пропускной способностью.

Существенное влияние на рассмотренные выше характеристики оказывает также функциональная организация компьютерной сети.

## 1.5. Принципы функциональной организации компьютерных сетей

Функциональная организация компьютерной сети складывается из функциональной организации вычислительного процесса (обработки данных) и процесса передачи данных.

Функциональная организация вычислительного процесса определяется режимами функционирования отдельных компьютеров сети и способом реализации обработки данных в компьютерной сети.

Обработка данных в компьютерных сетях может быть реализована двумя способами:

- *распределённая обработка*, при которой обработка данных распределяется между несколькими узлами (компьютерами) и выполняется параллельно;
- *централизованная обработка*, при которой данные обрабатываются в одном центральном узле (компьютере), в качестве которого обычно выступает сервер, при этом другие компьютеры рассматриваются как клиенты (удалённые терминалы), формирующие запросы к центральному узлу.

Функциональная организация процесса передачи данных в значительной степени определяется:

- *способом организации взаимодействия* между абонентами сети – *способом коммутации*;
- *методами управления трафиком* (потоками данных), реализуемыми на разных уровнях OSI-модели.

### 1.5.1. Коммутация

Передача данных в компьютерной сети предполагает организацию физического или логического соединения между взаимодействующими пользователями сети (конечными узлами).

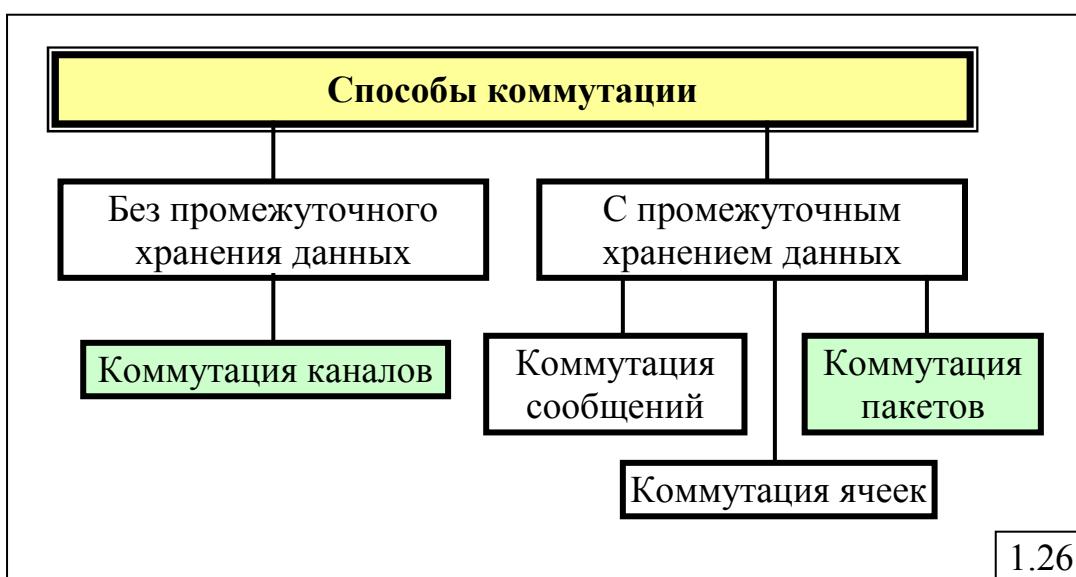
*Организация взаимодействия* между абонентами компьютерной сети называется **коммутацией**. Коммутация в сети может быть реализована разными способами (рис.1.26), которые можно разбить на две группы:

- способы коммутации без промежуточного хранения данных;
- способы коммутации с хранением данных в промежуточных узлах.

В качестве способа коммутации без промежуточного хранения данных в компьютерных сетях применяется коммутация каналов, используемая в традиционных *телефонных* сетях связи.

Для передачи данных в компьютерных сетях был разработан новый способ коммутации – коммутация сообщений, предполагающая использование в качестве узлов связи специализированных средств вычислительной техники, что позволяло реализовать в промежуточных узлах хранение передаваемых данных, обеспечивающее ряд преимуществ по сравнению с коммутацией каналов. Дальнейшее развитие способов

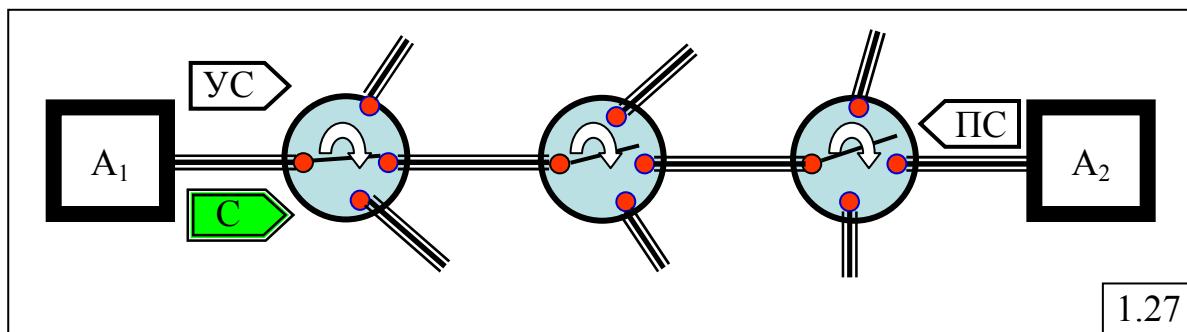
коммутаций было направлено на усовершенствование коммутации сообщений для обеспечения определенного качества передачи данных.



Рассмотрим перечисленные способы коммутации и в процессе сравнительного анализа выявим присущие им достоинства и недостатки.

#### **1.5.1.1. Коммутация каналов**

**Коммутация каналов** основана на формировании единого физического соединения (канала) между взаимодействующими абонентами для непосредственной передачи данных из конца в конец также, как это реализуется в традиционных телефонных сетях (рис.1.27).



Если абонент A<sub>1</sub> хочет передать данные абоненту A<sub>2</sub>, то перед началом передачи он предварительно должен установить соединение с абонентом A<sub>2</sub> путем посылки специального служебного сообщения «УС – установить соединение», которое «прокладывает» путь, формируя в каждом из промежуточных узлов непосредственное физическое (электрическое) соединение между входным и выходным портами узла. После того, как служебное сообщение достигнет абонента A<sub>2</sub>, последний формирует и посыпает по созданному пути (маршруту) абоненту A<sub>1</sub> новое служебное сообщение «ПС – подтвердить соединение», подтверждающее установление соединения между абонентами сети. Только после получения такого сообщения абонент A<sub>1</sub> может начать передачу сообщения С абоненту A<sub>2</sub> по установленному маршруту. Созданное физическое

соединение обычно существует в течение времени передачи данных, называемого *сеснсом* или *сессией* (*session*), по завершению которого это соединение может быть разрушено. Такой канал между двумя абонентами сети называется *временным* или *коммутируемым*, в отличие от *некоммутируемого* (*выделенного*) канала, который формируется единожды и существует постоянно или, по крайней мере, в течение длительного времени, независимо от того, передаются данные или же канал простояивает.

В простейшем случае узел сети с коммутацией каналов можно рассматривать как переключатель, обеспечивающий в каждый момент времени электрическое соединение между двумя портами (точками входа и выхода) узла. В телефонной сети такими «переключателями» являются автоматические телефонные станции (АТС).

К основным **достоинствам** коммутации каналов относятся:

- *возможность использования существующих и достаточно хорошо развитых телефонных сетей связи;*
- *отсутствие необходимости в хранении передаваемых данных в промежуточных узлах сети;*
- *высокая эффективность при передаче больших объемов данных,* поскольку в этом случае относительное значение накладных расходов на установление соединения оказывается незначительным.

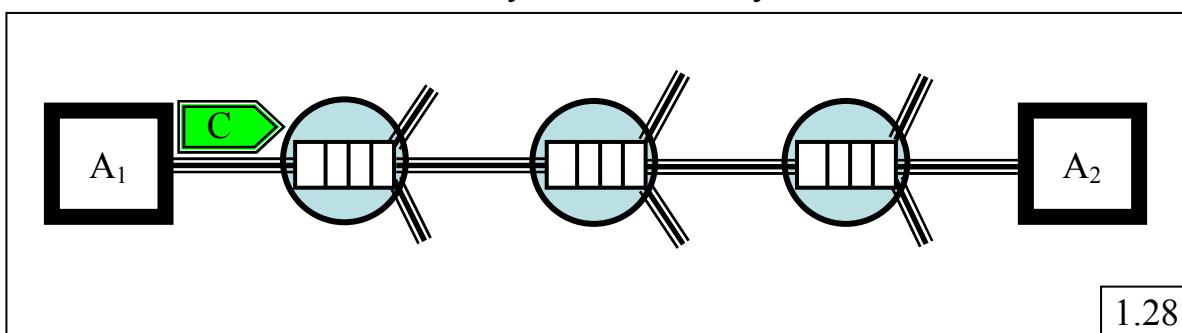
В то же время коммутация каналов обладает следующими серьёзными **недостатками**:

- каналы связи на всем пути передачи данных *должны иметь одинаковые пропускные способности* и обеспечивать одинаковую скорость передачи данных, в противном случае, если пропускная способность некоторого канала связи окажется меньше пропускной способности предыдущего канала, произойдёт потеря передаваемых данных, поскольку в промежуточных узлах отсутствует возможность буферирования (временного хранения) данных;
- *большие накладные расходы на установление соединения* на начальном этапе, что негативно сказывается при передаче небольших объёмов данных, поскольку в этом случае относительное значение накладных расходов на установление соединения оказывается существенным, что приводит к неэффективному использованию ресурсов (пропускной способности) каналов связи, что проявляется в значительном уменьшении реальной скорости передачи данных по отношению к максимально возможной скорости канала, называемой *пропускной способностью*;
- телефонные каналы связи, ориентированные на передачу голоса, имеют сравнительно низкое качество и обеспечивают передачу компьютерных данных *с невысокой скоростью*, что не позволяет их использовать в высокоскоростных магистральных сетях.

Альтернативой коммутации каналов, устраниющей присущие ей недостатки, является коммутация сообщений.

### 1.5.1.2. Коммутация сообщений

**Коммутация сообщений**, в отличие от коммутации каналов, предполагает хранение передаваемых сообщений в буферной памяти промежуточных узлов, находящихся на пути передачи, который прокладывается в каждом узле в соответствии с заданным алгоритмом маршрутизации (рис.1.28). При этом не требуется предварительно устанавливать соединение между взаимодействующими абонентами.



Если абонент А<sub>1</sub> желает передать сообщение С абоненту А<sub>2</sub>, то он, не устанавливая непосредственное соединение с А<sub>2</sub>, посыпает сообщение к узлу связи, к которому он подключен. Там сообщение хранится в буфере узла в течение некоторого времени, необходимого для анализа заголовка, определения в соответствии с заданным алгоритмом маршрутизации следующего узла и, возможно, ожидания освобождения канала связи с этим узлом, если канал занят передачей ранее обработанного сообщения. Проходя таким образом через все узлы, находящиеся на пути передачи, сообщение достигает конечного абонента А<sub>2</sub>. Отметим ещё раз, что направление передачи сообщения, то есть его маршрут в сети, определяется только после поступления сообщения в тот или иной узел сети, а не устанавливается заранее, как это происходит при коммутации каналов.

Благодаря такой организации передачи данных между взаимодействующими абонентами, коммутация сообщений обладает следующими достоинствами по сравнению с коммутацией каналов:

- не требуется предварительное установление соединения, что существенно снижает накладные расходы, но не делает их нулевыми, поскольку имеются непроизводительные затраты времени в каждом узле на обработку заголовка и реализацию алгоритма маршрутизации; однако в целом эти затраты существенно меньше по сравнению с затратами на установление соединения при коммутации каналов;
- каналы связи на всем пути передачи могут иметь *разные пропускные способности*, поскольку буферирование сообщений в узлах сети позволяет сгладить различие в пропускных способностях входного и выходного канала узла.

Недостатками коммутации сообщений являются:

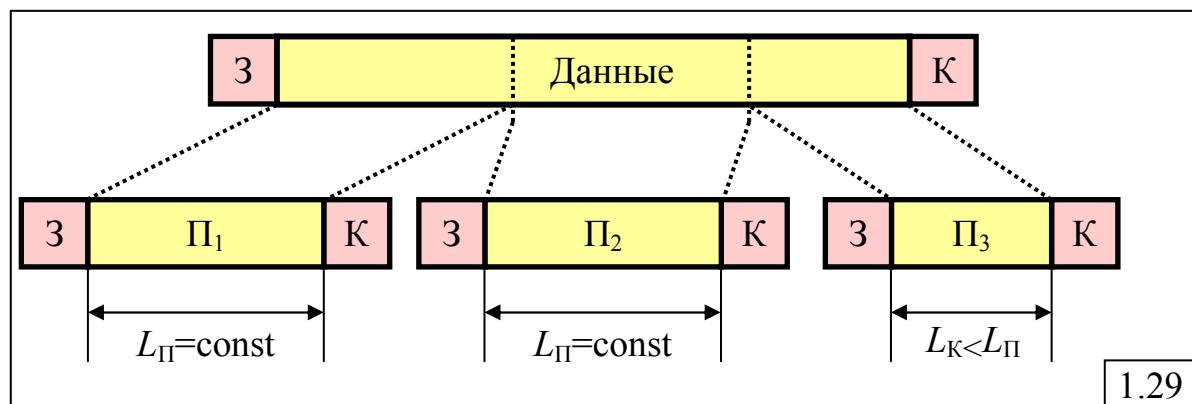
- необходимость хранения передаваемых сообщений в промежуточных узлах, что требует значительной ёмкости буферной

памяти, которая рассчитывается как произведение ёмкости одного буфера на максимально возможное количество сообщений, которые одновременно могут находиться в узле; ёмкость одного буфера должна быть рассчитана на сообщения максимальной длины, которая, например, для видео файлов может составлять несколько гигабайт, что делает ёмкость буферной памяти узла неоправданно большой; при этом коэффициент использования (загрузки) буферной памяти оказывается незначительным, поскольку большинство сообщений, занимая один буфер, будут иметь длину много меньше, чем ёмкость буфера;

- задержка в промежуточных узлах может оказаться значительной, особенно из-за большого времени ожидания освобождения выходного канала связи при большой загрузке сети, что приводит к увеличению времени доставки сообщений;
- монополизация среды передачи (канала связи) на длительный промежуток времени при передаче длинных сообщений приводит к неоправданно большим задержкам коротких сообщений в связи с ожиданием освобождения канала, длительность которого может многократно превышать время непосредственной передачи этих сообщений.

#### 1.5.1.3. Коммутация пакетов

**Коммутация пакетов** отличается от коммутации сообщений лишь тем, что каждое сообщение в сети разбивается на блоки фиксированной длины  $L_{\Pi} = \text{const}$  (кроме последнего блока:  $L_K \leq L_{\Pi}$ ), называемых **пакетами** (рис.1.29), каждый из которых имеет структуру аналогичную структуре сообщений: заголовок, текст и, возможно, концевик. При этом, заголовки всех пакетов одного и того же сообщения содержат одни и те же адреса назначения и источника. Каждый пакет сообщения передаётся в сети как независимый блок данных в соответствии с адресом назначения, указанным в заголовке.



Коммутация пакетов по сравнению с коммутацией сообщений позволяет реализовать более эффективную передачу данных за счёт следующих присущих ей достоинств:

- меньшее время доставки сообщения в сети;
- более эффективное использование буферной памяти в узлах;

- более эффективная организация надёжной передачи данных;
- среда передачи не монополизируется одним сообщением на длительное время;
- задержка пакетов в узлах меньше, чем задержка сообщений.

Рассмотрим каждое из перечисленных достоинств более подробно.

**Уменьшение времени доставки сообщений** при коммутации пакетов достигается за счёт параллельной передачи пакетов по каналам связи. Покажем это на следующем примере.

Положим, что сообщение длиной  $L$  передаётся от абонента  $A_1$  к абоненту  $A_2$  в сети с коммутацией сообщений так, как это показано на рис.1.28. В процессе передачи сообщение проходит через  $K$  каналов связи с одинаковыми пропускными способностями  $C_{KC}$  и  $(K - 1)$  промежуточных узла. Время передачи сообщения длиной  $L$  в одном канале с пропускной способностью  $C_{KC}$  будет равно:  $t = \frac{L}{C_{KC}}$ . Пренебрегая

временем распространения сигнала в канале связи и задержкой сообщения в узлах, определим время доставки сообщения от абонента  $A_1$  к абоненту  $A_2$ :

$$T_C = Kt = \frac{KL}{C_{KC}}.$$

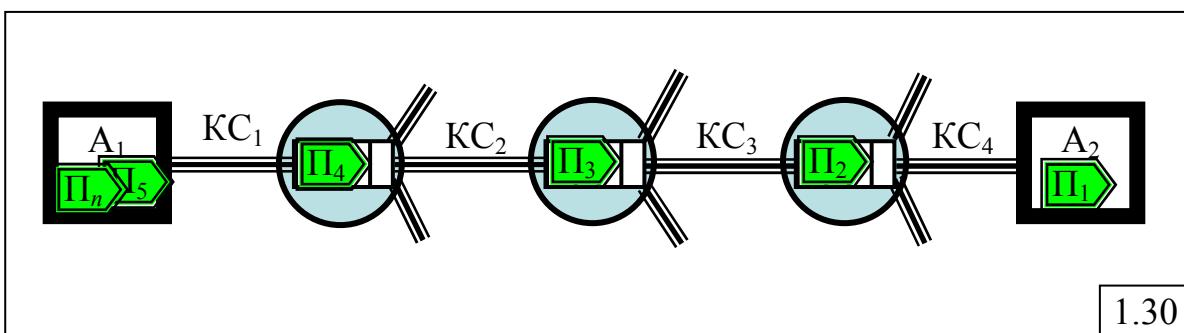
Положим теперь, что в рассматриваемой сети реализован принцип коммутации пакетов, и передаваемое от абонента  $A_1$  к абоненту  $A_2$  сообщение длиной  $L$  разбивается на  $n$  пакетов, длина каждого из которых равна  $l = \frac{L}{n}$ . Тогда время передачи пакета в канале с пропускной

способностью  $C_{KC}$  будет равно:  $t_n = \frac{l}{C_{KC}} = \frac{L}{nC_{KC}}$ . Как и ранее, пренебрегая

временем распространения сигнала в канале связи и задержкой сообщения в узлах, определим время доставки сообщения от абонента  $A_1$  к абоненту  $A_2$ . Очевидно, что первый пакет будет доставлен к абоненту  $A_2$  за время

$t_1 = Kt_n = \frac{KL}{nC_{KC}}$ . На момент доставки к абоненту  $A_2$  первого пакета  $\Pi_1$

остальные пакеты  $\Pi_2, \Pi_3, \Pi_4$  сообщения, двигаясь по тому же маршруту, окажутся в промежуточных узлах, как это показано на рис.1.30, а пакеты  $\Pi_5, \dots, \Pi_n$  будут находиться в исходном узле у абонента  $A_1$ .



Дальнейшее перемещение пакетов приведёт к тому, что пакет  $\Pi_2$  окажется у абонента  $A_2$  через время  $t_2 = t_1 + t_{\pi} = \frac{(K+1)L}{n C_{KC}}$ . Аналогично,

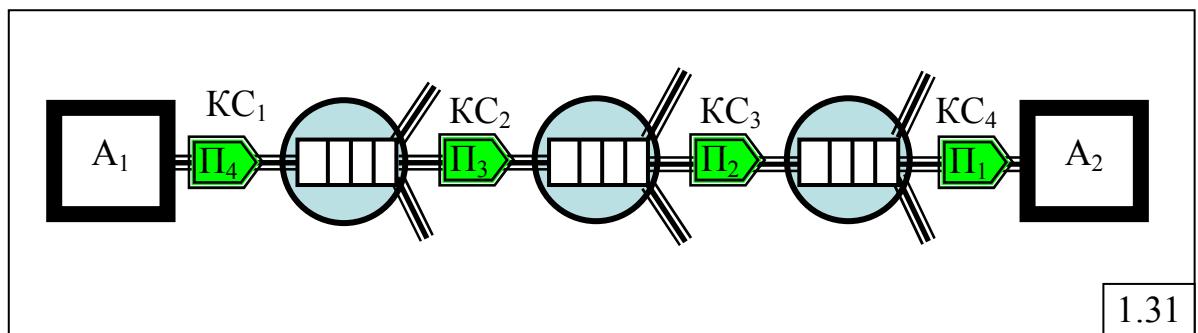
пакет  $\Pi_3$  окажется у абонента  $A_2$  через время  $t_3 = t_2 + t_{\pi} = \frac{(K+2)L}{n C_{KC}}$ , и т.д..

Последним к абоненту  $A_2$  придёт пакет  $\Pi_n$  через время  $t_n = t_{n-1} + t_{\pi} = \frac{(K+n-1)L}{n C_{KC}}$ . Таким образом, все  $n$  пакетов, а, следовательно,

всё сообщение будут доставлены к абоненту  $A_2$  за время  $T_{\pi} = t_n = \frac{(K+n-1)L}{n C_{KC}}$ .

Сравнивая времена доставки сообщения при использовании коммутации пакетов  $T_{\pi} = \frac{(K+n-1)L}{n C_{KC}}$  и коммутации сообщений  $T_C = \frac{KL}{C_{KC}}$ , можно убедиться, что при  $n > 1$ :  $T_{\pi} < T_C$ , т.е. время доставки сообщения при коммутации сообщений больше времени доставки сообщения при использовании коммутации каналов в  $k = \frac{T_C}{T_{\pi}} = \frac{Kn}{K+n-1}$  раз.

Для значений  $K = 4$  и  $n = 5$  (четыре канала связи, как на рис.1.30, и пять пакетов) получим, что время доставки сообщения при коммутации пакетов уменьшится в  $k = 2,5$  раза по сравнению с коммутацией сообщений, а при разбиении исходного сообщения на 17 пакетов – в  $k = 3,4$  раз. Легко убедиться, что при  $n \rightarrow \infty$  выигрыш  $k$  во времени доставки стремится к  $K$ :  $k \rightarrow K$ , то есть максимально возможный выигрыш при коммутации пакетов определяется количеством каналов связи, через которые проходят пакеты. Этот вывод очевиден, если учесть, что выигрыш во времени доставки обусловлен тем, что разные пакеты сообщения одновременно (параллельно) друг за другом перемещаются в последовательных каналах (рис.1.31): когда пакет  $\Pi_1$  находится в канале  $KC_4$ , пакет  $\Pi_2$  передаётся по каналу  $KC_3$ , пакет  $\Pi_3$  – по каналу  $KC_2$  и пакет  $\Pi_4$  – по каналу  $KC_1$ , что обеспечивает в процессе передачи пакетов уровень параллелизма, равный четырём. Ясно, что чем больше каналов связи на пути пакетов, тем выше уровень параллелизма и, следовательно, тем больше выигрыш.



1.31

Еще больший выигрыш может быть получен, если передача пакетов одного того же сообщения осуществляется параллельно по разным маршрутам.

Представленные выше расчёты выигрыша во времени доставки сообщений при использовании коммутации пакетов по сравнению с коммутацией сообщений естественно являются упрощёнными, поскольку не учитывают задержки пакетов в узлах сети, а также дополнительные накладные расходы на передачу обрамления (заголовков и концевиков) пакетов. Несмотря на это, они достаточно убедительно показывают наличие такого выигрыша.

**Более эффективное использование буферной памяти** при коммутации пакетов по сравнению с коммутацией сообщений обусловлено тем, что размер буфера строго фиксирован и определяется максимально допустимой (фиксированной) длиной передаваемых пакетов, которая может составлять от нескольких десятков байт до нескольких килобайт. За счёт этого достигается более высокая загрузка одного буфера, которая при передаче длинных сообщений близка к единице и, как следствие, более высокая загрузка всей буферной памяти узла.

**Более эффективная организация надежной передачи данных**, по сравнению с коммутацией сообщений, обусловлена тем, что контроль передаваемых данных осуществляется для каждого пакета и в случае обнаружения ошибки повторно передается только один пакет, а не всё сообщение.

**Среда передачи не монополизируется** одним сообщением на длительное время, поскольку длинное сообщение разбивается на пакеты ограниченной длины, которые передаются как независимые единицы данных. При этом механизм управления трафиком организуется таким образом, что после пакета одного сообщения по тому же каналу связи могут быть переданы пакеты других сообщений, а затем снова пакет первого сообщения. Это позволяет уменьшить среднее время ожидания пакетами освобождения канала связи и за счёт этого увеличить оперативность передачи данных. При этом, чем меньше предельно допустимая длина пакетов, тем выше указанный эффект.

**Задержка пакетов в узлах меньше, чем задержка сообщений**, которая складывается из следующих составляющих:

- приём (запись) поступающего блока данных (пакета или сообщения) во входной буфер узла;
- подсчёт и проверка контрольной суммы блока данных;
- передача блока данных из входного буфера в выходной буфер;
- ожидание освобождения выходного канала, занятого передачей ранее поступивших блоков данных;
- передача данных в выходной канал связи и освобождение выходного буфера узла.

Очевидно, что все эти задержки пропорциональны длине блока данных.

Несмотря на очевидные достоинства, коммутации пакетов присущи недостатки, которые состоят в следующем:

- *большие накладные расходы* на передачу и анализ заголовков всех пакетов сообщения, что снижает эффективную (реальную) пропускную способность канала связи, используемую непосредственно для передачи данных, и, следовательно, увеличивает время доставки сообщения в сети, в том числе и за счёт дополнительных затрат времени на обработку заголовков пакетов в узлах сети;
- *необходимость сборки из пакетов сообщения* в узле назначения может существенно увеличить время доставки сообщения конечному абоненту за счёт ожидания прихода всех пакетов сообщения, поскольку в случае потери хотя бы одного пакета, сообщение не сможет быть собрано в конечном узле сети; при этом возникает серьёзная проблема, связанная с определением предельно допустимого времени ожидания пакетов для сборки сообщения в конечном узле; при большом значении этого времени в конечном узле может скопиться большое число пакетов разных сообщений, что приведёт к переполнению буферной памяти узла и, как следствие, к потере передаваемых пакетов или к отказу в приёме новых пакетов, что, в свою очередь, не позволит собрать сообщения; маленькое значение предельно допустимого времени ожидания пакетов для сборки сообщения в конечном узле может создавать такую ситуацию, при которой большое количество сообщений не смогут дождаться прихода последнего пакета и, поскольку по истечении этого времени все пакеты таких сообщений будут удалены из буферной памяти, потребуется повторная передача всех пакетов этих сообщений, что приведёт к значительной загрузке оборудования (узлов и каналов) сети и, в пределе, может вызвать перегрузку сети.

#### 1.5.1.4. Коммутация ячеек

**Коммутация ячеек** – способ коммутации, который можно рассматривать как частный случай коммутации пакетов со строго фиксированной длиной передаваемых блоков данных в 53 байта, называемых **ячейками** (рис.1.32).

Первые компьютерные сети строились для передачи цифровых (компьютерных) данных с единственным требованием – обеспечить надёжную (без ошибок) доставку данных, при этом время доставки не являлось критичным. Развитие компьютерных технологий и появление необходимости передачи мультимедийных данных, таких как речь и видео, выдвинуло, наряду с надёжной доставкой, новое требование к передаче данных в компьютерных сетях: минимизация времени доставки сообщений. Для реализации этой концепции в начале девяностых годов прошлого столетия была разработана сетевая



1.32

технология, получившая название **Asynchronous Transfer Mode (ATM)** - режим асинхронной передачи, назначение которой – передача мультимедийных данных в компьютерной сети с минимальной задержкой.

Как было показано выше при рассмотрении коммутации пакетов, чем короче пакеты, тем меньше время доставки всего сообщения. Исходя из этого, в ATM-сетях в качестве единицы передачи данных был выбран блок размером в 53 байта (5 байт – заголовок и 48 байт – данные), названный ячейкой (рис.1.32). Столь странный размер ячейки появился в результате компромисса двух противодействующих групп, из которых одна группа (по одной из версий: традиционные связисты – телефонисты) настаивала на меньшем значении поля данных в 32 байта, а другая (компьютерщики) – на значении в 64 байта. Действительно, меньшее значение размера ячейки обеспечило бы меньшие задержки при доставке данных, однако не следует забывать, что при этом возрастают накладные расходы на передачу заголовков ячеек, что снижает полезную (эффективную) пропускную способность среды передачи. В ATM-сетях это снижение составляет около 10%. Если же размер поля данных будет 32 байта, то при том же заголовке в 5 байт снижение полезной пропускной способности составит 13,5%. Принимая во внимание, что в мультимедийных сетях обычно используются высокоскоростные каналы, потери пропускной способности могут оказаться значительными, что отрицательно скажется на экономической эффективности компьютерной сети.

Подводя итог сказанному, можно отметить следующие достоинства коммутации ячеек:

- маленькие задержки ячеек (не монополизируется канал связи);
- быстрая обработка заголовка ячейки в узлах, поскольку местоположение заголовка строго фиксировано;
- более эффективная, по сравнению с коммутацией пакетов, организация буферной памяти и надежной передачи данных.

Основным недостатком коммутации ячеек является:

- наличие сравнительно больших накладных расходов на передачу заголовка (почти 10%) и, как следствие, значительная потеря пропускной способности, особенно в случае высокоскоростных каналов связи.

*Коммутация пакетов и коммутация каналов* – основные способы передачи данных в компьютерных сетях, поскольку коммутация пакетов обеспечивает более эффективную передачу данных через СПД по сравнению с коммутацией сообщений (в первую очередь, значительно меньшие задержки), а коммутация каналов может быть достаточно легко реализована на основе существующей телефонной сети.

### 1.5.2. Способы передачи пакетов

Пакеты в сети могут передаваться двумя способами (рис.1.33):

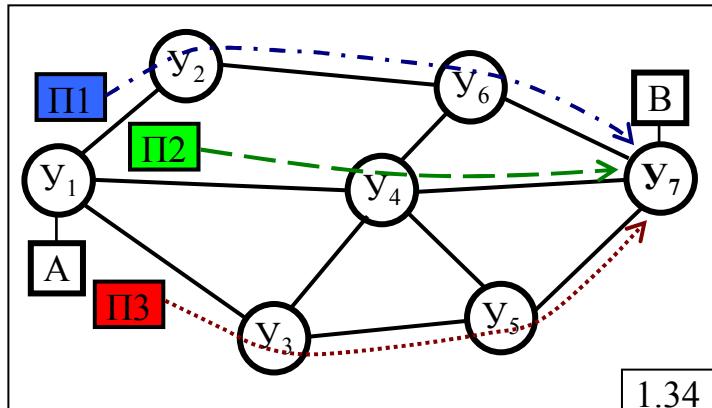
- дейтаграммным;

- путем формирования «виртуального канала».



### 1.5.2.1. Дейтаграммная передача

При дейтаграммном способе пакеты одного и того же сообщения могут передаваться между двумя взаимодействующими пользователями **A** и **B** по разным маршрутам, как это показано на рис.1.34, где пакет **П1** передаётся по маршруту  $Y_1-Y_2-Y_6-Y_7$ , пакет **П2** – по маршруту  $Y_1-Y_4-Y_7$  и пакет **П3** – по маршруту  $Y_1-Y_3-Y_5-Y_7$ . В результате такого способа передачи все пакеты приходят в конечный узел сети *в разное время и в произвольной последовательности*. Пакеты одного и того же сообщения, рассматриваемые в каждом узле сети как самостоятельные независимые единицы данных и передаваемые разными маршрутами, называются **дейтаграммами** (datagram). В узлах сети для каждой дейтаграммы всякий раз определяется наилучший путь передачи в соответствии с выбранной метрикой маршрутизации, не зависимо от того, по какому пути переданы были предыдущие дейтаграммы с такими же адресами назначения (получателя) и источника (отправителя).



Дейтаграммный способ передачи пакетов может быть реализован:

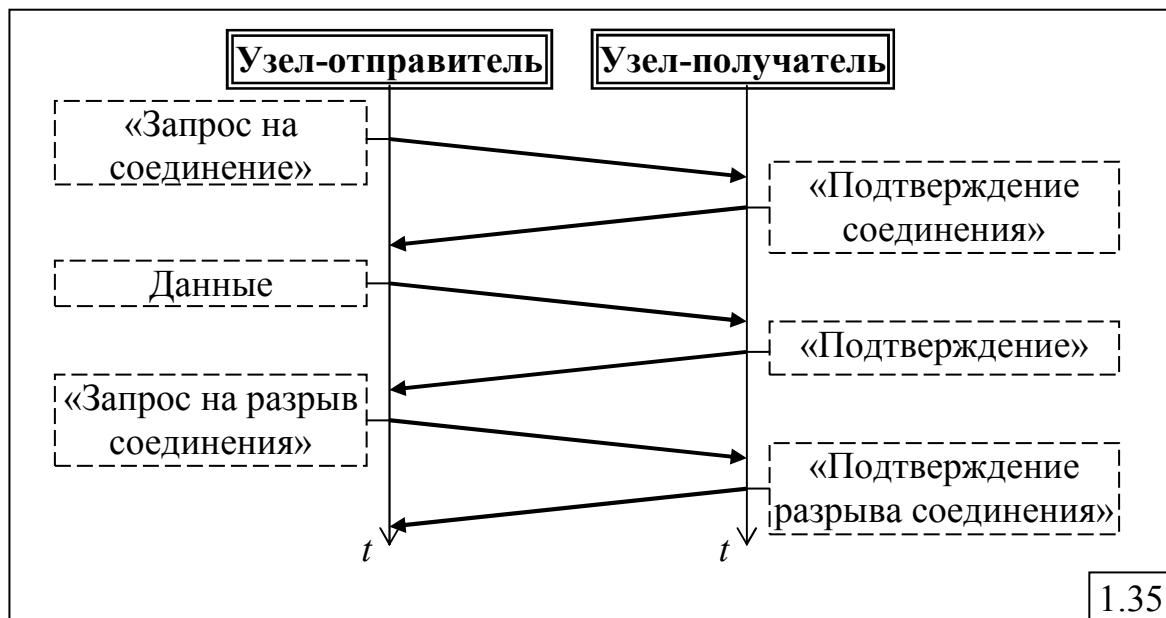
- без установления соединения между абонентами сети;
- с установлением соединения между взаимодействующими абонентами сети.

В последнем случае между взаимодействующими абонентами предварительно устанавливается соединение путём обмена служебными пакетами: «запрос на соединение» и «подтверждение соединения», означающее готовность принять передаваемые данные. В процессе установления соединения могут «оговариваться» значения параметров передачи данных, которые должны выполняться в течение сеанса связи.

После установления соединения отправитель начинает передачу, причём пакеты одного и того же сообщения могут передаваться разными маршрутами, то есть дейтаграммным способом. По завершении сеанса передачи данных выполняется процедура разрыва соединения путём обмена служебными пакетами: «запрос на разрыв соединения» и «подтверждение разрыва соединения». Описанная процедура передачи пакетов с установлением соединения иллюстрируется на диаграмме (рис.1.35).

*Достоинствами* дейтаграммного способа передачи пакетов в компьютерных сетях являются:

- *простота* организации и реализации передачи данных – каждый пакет (дейтаграмма) сообщения передаётся независимо от других пакетов;
- в узлах сети для каждого пакета выбирается *наилучший путь* (маршрут);
- передача данных может выполняться как *без установления соединения* между взаимодействующими абонентами, так и при необходимости *с установлением соединения*.



К недостаткам дейтаграммного способа передачи пакетов следует отнести:

- *необходимость сборки сообщения* в конечном узле: сообщение не может быть передано получателю, пока в конечном узле сети не соберутся все пакеты данного сообщения, поэтому в случае потери хотя бы одного пакета сообщение не сможет быть сформировано и передано получателю;
- при длительном ожидании пакетов одного и того же сообщения в конечном узле может скопиться достаточно большое количество пакетов сообщений, собранных не полностью, что требует значительных затрат на организацию в узле буферной памяти большой ёмкости;
- для предотвращения переполнения буферной памяти узла время нахождения (ожидания) пакетов одного и того же сообщения в конечном узле ограничивается, и по истечении этого времени все поступившие

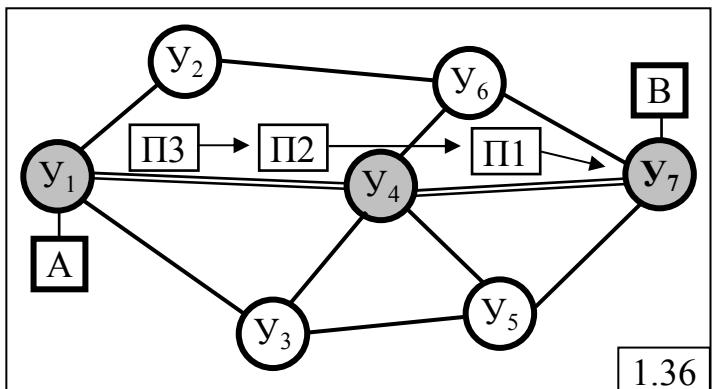
пакеты не полностью собранного сообщения уничтожаются, после чего выполняется запрос на повторную передачу данного сообщения; это приводит к *увеличению нагрузки* на сеть и, как следствие, к *снижению её производительности*, измеряемой количеством сообщений, передаваемых в сети за единицу времени.

### 1.5.2.2. Виртуальный канал

Способ передачи пакетов «виртуальный канал» заключается в формировании единого «виртуального» канала на время взаимодействия абонентов для передачи всех пакетов сообщения. Этот способ реализуется с использованием предварительного установления соединения между взаимодействующими абонентами, в процессе которого формируется наиболее рациональный единый для всех пакетов маршрут, по которому, в отличие от дейтаграммного способа, все пакеты сообщения передаются в *естественной последовательности*, как это показано на рис.1.36.

Пакеты П1, П2 и П3 сообщения передаются в естественной последовательности от пользователя А к пользователю В по предварительно созданному виртуальному каналу через узлы У<sub>1</sub>-У<sub>4</sub>-У<sub>7</sub>.

Виртуальный канал, как и реальный физический канал в случае коммутации каналов, существует только в течение сеанса связи, при этом ресурсы реальных каналов связи (пропускная способность) и узлов сети (буферная память), находящихся на маршруте, резервируются на всё время сеанса.



Не следует путать и смешивать *коммутацию каналов* и *способ передачи пакетов «виртуальный канал»*. Основное их отличие состоит в том, что «виртуальной канал» реализуется с промежуточным хранением пакетов в узлах сети, в то время как коммутация каналов реализуется без промежуточного хранения передаваемых пакетов за счёт создания реального (а не виртуального) физического канала между абонентами сети.

К достоинствам способа передачи пакетов «виртуальный канал» по сравнению с дейтаграммной передачей пакетов можно отнести:

- *меньшие задержки в узлах сети*, обусловленные резервированием ресурсов, и прежде всего пропускной способности каналов связи, в процессе установления соединения;
- *небольшое время ожидания* в конечном узле для сборки всего сообщения, поскольку пакеты передаются последовательно друг за другом по одному и тому же маршруту (виртуальному каналу), и вероятность того, что какой-либо пакет «заблудится» в результате неудачно выбранного

маршрута или его время доставки окажется слишком большим, как это может произойти при дейтаграммном способе, близка к нулю;

- более эффективное использование буферной памяти промежуточных узлов за счёт её предварительного резервирования, а также буферной памяти в конечном узле в связи с небольшим временем ожидания прихода всех пакетов сообщения.

К недостаткам способа передачи пакетов «виртуальный канал» можно отнести:

- наличие накладных расходов (издержек) на установление соединения;
- неэффективное использование ресурсов сети, поскольку они резервируются на всё время взаимодействия абонентов (сеанса) и не могут быть предоставлены другому соединению, даже если они в данный момент не используются.

### 1.5.3. Маршрутизация

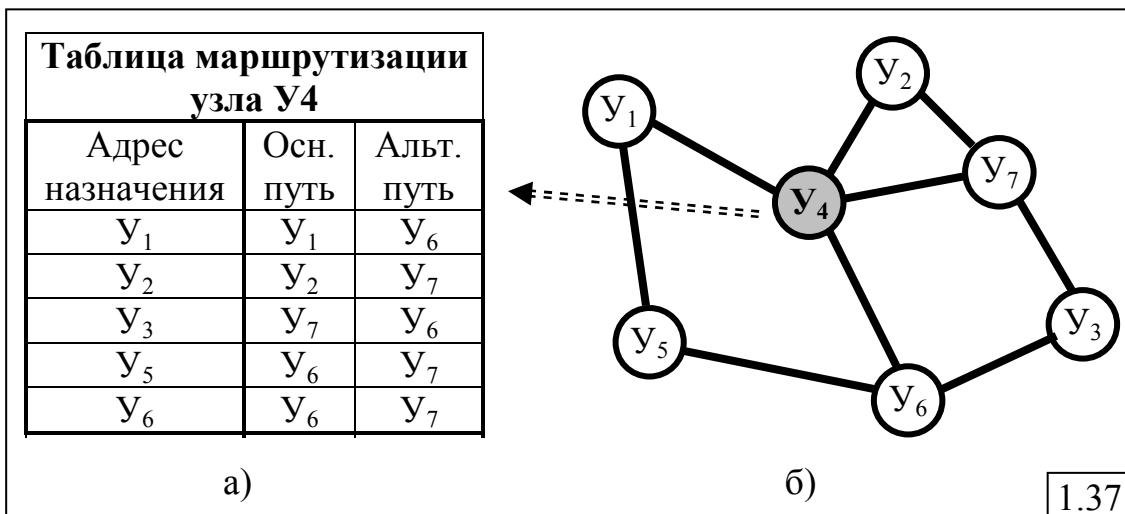
*Маршрутизация* – одна из основных функций компьютерной сети, определяющая эффективность передачи данных. Проблема маршрутизации в компьютерных сетях аналогична проблеме организации автомобильного движения по улицам города и состоит в выборе в каждом узле сети направления передачи данных (выходного канала) из множества возможных направлений в соответствии с адресом назначения и с учётом требований, предъявляемых к качеству передачи. Очевидно, что наиболее просто маршрутизация реализуется в узлах с двумя каналами: данные, поступившие по одному каналу, автоматически направляются в другой канал узла.

#### 1.5.3.1. Таблица маршрутизации

При наличии нескольких выходных каналов, по которым могут быть переданы данные, маршрутизация реализуется на основе **таблицы маршрутизации**, вид которой зависит от используемого в сети алгоритма маршрутизации. В простейшем случае каждому адресу назначения ставится в соответствие адрес следующего соседнего узла, к которому должен быть направлен пакет с указанным в заголовке адресом назначения. При наличии *альтернативных маршрутов*, например в многосвязных сетях, дополнительно могут быть указаны адреса других соседних узлов, через которые проходят альтернативные маршруты. При этом для каждого маршрута задаётся значение некоторой *метрики*, на основе которой выбирается тот или иной маршрут. В качестве метрики может использоваться расстояние до узла назначения, измеряемое, например, в хопах, пропускная способность соответствующего выходного канала связи и т.д.

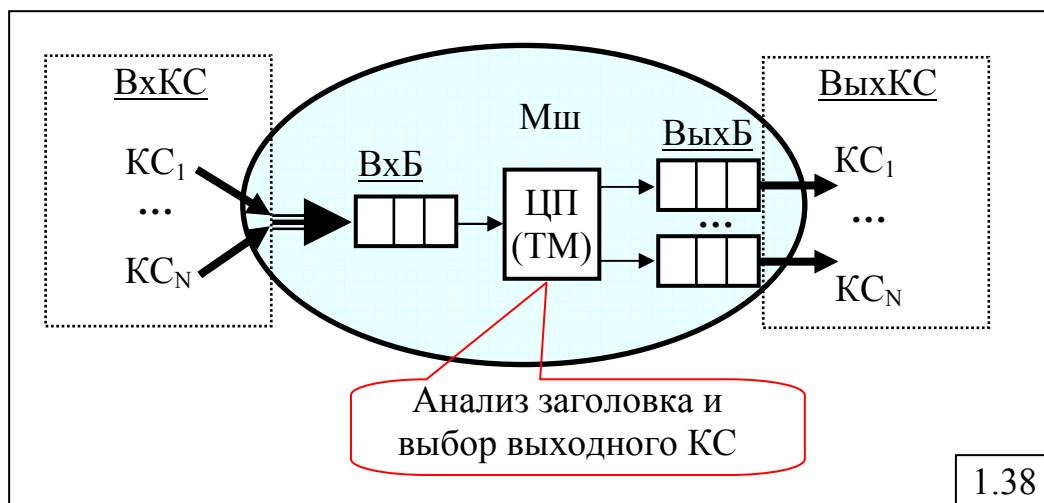
На рис. 1.37,а) показан пример простейшей *таблицы маршрутизации* узла 4 сети с топологией, представленной на рис.1.37,б). В таблице для каждого адреса назначения указывается направление передачи

данных по основному пути и альтернативному пути в случае невозможности передачи по основному пути, например в случае отказа основного пути.



### 1.5.3.2. Модель маршрутизатора

На рис.1.38 показана концептуальная модель функционирования маршрутизатора. По входным каналам связи (ВхКС) пакеты с данными поступают во входной буфер (ВхБ) маршрутизатора. Центральный процессор (ЦП) последовательно анализирует заголовки пакетов и в соответствии с таблицей маршрутизации (ТМ) определяет направление передачи пакета и соответствующий выходной канал связи (ВыхКС). Затем пакет направляется в выходной буфер (ВыхБ) этого канала, где он ожидает освобождения канала, если последний занят передачей предыдущих пакетов. Пакеты, находящиеся в выходном буфере, образуют очередь перед каналом связи. Для дифференцированного обслуживания пакетов разных типов, имеющих разные требования к качеству обслуживания, выбор очередного пакета для передачи по каналу связи может осуществляться в соответствии с некоторой, например приоритетной, дисциплиной обслуживания.

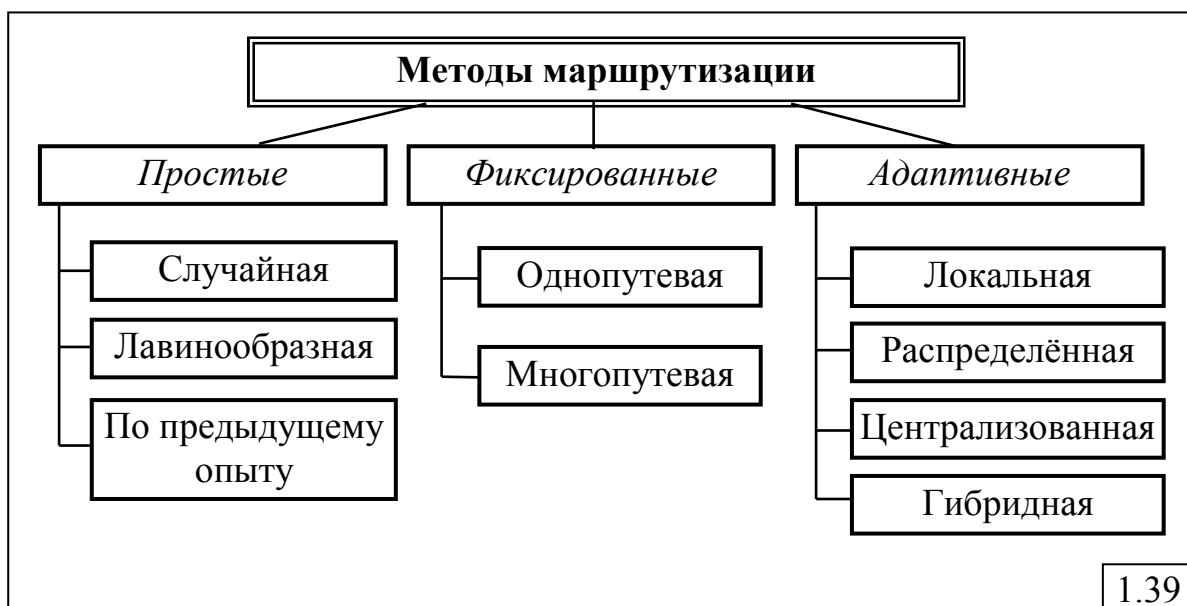


Отметим, что конкретные реализации реальных маршрутизаторов могут существенно различаться. Например, буферная память для хранения пакетов может быть разделена на входную и выходную, как это показано на рис.1.38, либо выполнена как единая память, где хранятся все пакеты.

#### **1.5.3.3. Классификация методов маршрутизации**

В компьютерных сетях теоретически могут использоваться самые разнообразные методы (алгоритмы) маршрутизации, обеспечивающие разные эффекты и зависящие от структурно-функциональных особенностей сети и требований, предъявляемых к качеству функционирования сети. На рис.1.39 представлена одна из возможных классификаций различных методов маршрутизации, которые можно разбить на 3 группы:

- простые;
- фиксированные;
- адаптивные.



#### **1.5.3.4. Простые методы маршрутизации**

К простым относятся следующие методы маршрутизации.

1. **Случайная маршрутизация**, при которой выбор направления передачи данных осуществляется случайным образом между всеми каналами узла (портами маршрутизатора) за исключением канала, по которому эти данные поступили в узел. Например, если маршрутизатор имеет 4 порта (канала) и по одному из них поступили данные, то вероятность передачи по любому из трёх других каналов будет равна  $1/3$ , при этом адрес назначения не используется для выбора выходного канала. Очевидно, что применение такого алгоритма маршрутизации оправдано только в том случае, если отсутствует информация о топологии сети и сетевых адресах, что делает невозможным построение таблицы маршрутизации. Несмотря на то, что направление передачи пакетов

осуществляется случайным образом, вероятность доставки пакета конечному адресату отлична от нуля, но меньше единицы, поскольку существует вероятность зацикливания пакета в сети.

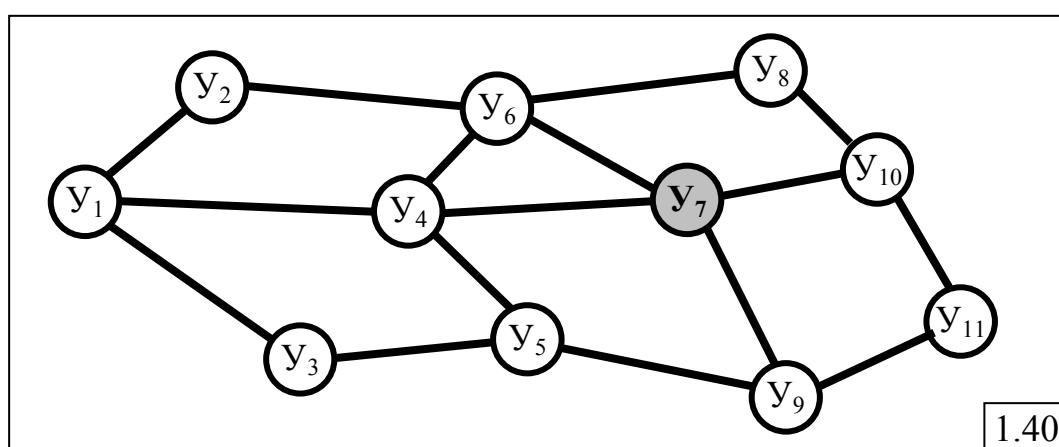
**2. Лавинообразная маршрутизация**, заключающаяся в размножении поступившего пакета и рассылке его копии по всем направлениям, кроме того, по которому поступил пакет. Такое размножение приводит к большой загрузке каналов и узлов сети и, в то же время, обеспечивает доставку пакета конечному адресату с вероятностью единица. Если в некоторый узел поступает несколько копий одного и того же пакета, то все они, кроме одного пакета, уничтожаются. Как и в предыдущем случае, применение лавинообразного алгоритма оправдано, если невозможно построить таблицу маршрутизации из-за отсутствия информации о топологии сети и сетевых адресах.

Случайная и, особенно, лавинообразная маршрутизации являются скорее экзотическими методами, которые могут использоваться в условиях неопределённости, возникших, например, в результате боевых действий, приведших к выходу из строя значительной части сетевых ресурсов и, как следствие, к отсутствию сведений о топологии сети и сетевых адресах.

**3. Маршрутизация по предыдущему опыту** является наиболее интересной среди простых алгоритмов и заключается в автоматическом построении таблицы маршрутизации.

Заголовки пакетов, передаваемых в сети с маршрутизацией от источника, кроме адреса получателя АП и адреса отправителя АО содержат специальное поле «расстояние», значение которого в узле-отправителе устанавливается равным 0. В процессе передачи пакета в сети в каждом промежуточном узле значение поля «расстояние» увеличивается на единицу. Таким образом, в каждом узле значение этого поля показывает расстояние, которое прошел пакет от узла-отправителя до этого узла и которое измеряется в количестве промежуточных узлов на пути передачи пакета.

Рассмотрим принцип реализации метода маршрутизации по предыдущему опыту на примере построения таблицы маршрутизации узла  $Y_7$  сети, показанной на рис. 1.40.



Положим, что в некоторый момент времени в узел  $Y_7$  поступает пакет от узла  $Y_1$  (адрес отправителя АО =  $Y_1$ ) по маршруту, пролегающему через узлы  $Y_3$ ,  $Y_5$ ,  $Y_9$ , в каждом из которых значение поля «расстояние» было увеличено на 1:

$$Y_1 \rightarrow Y_3 \rightarrow Y_5 \rightarrow Y_9 \rightarrow Y_7.$$

В узле  $Y_7$  анализируется адрес отправителя АО и, если такой адрес отсутствует в таблице маршрутизации, то он заносится в таблицу. Для этого же адреса одновременно указывается адрес соседнего узла  $Y_9$ , от которого поступил этот пакет, и расстояние до узла-отправителя, содержащееся в поле «расстояние» заголовка пакета и равное 3 (рис.1.41).

Таблица маршрутизации узла $Y_7$ (1)		
Адрес назначения	Адрес соседнего узла	Расстояние
$Y_1$	$Y_9$	3
...	...	...

1.41

Положим теперь, что через некоторое время в узел  $Y_7$  поступит новый пакет от узла  $Y_1$  с адресом отправителя АО= $Y_1$ , маршрут которого пролегал через узлы  $Y_2$ ,  $Y_6$ :

$$Y_1 \rightarrow Y_2 \rightarrow Y_6 \rightarrow Y_7.$$

Поскольку в таблице маршрутизации узла  $Y_7$  уже есть строка с адресом  $Y_1$ , то для этого адреса сравнивается значение расстояния от узла отправителя, содержащееся в заголовке поступившего пакета в поле «расстояние», со значением расстояния, записанного в таблице маршрутизации. Если расстояние, указанное в заголовке поступившего пакета, меньше расстояния, записанного в таблице маршрутизации, то новый маршрут считается более коротким и в таблице маршрутизации корректируется строка, соответствующая адресу назначения  $Y_1$ : адрес соседнего узла заменяется на  $Y_6$ , а расстояние до адреса назначения становится равным 2 (рис.1.42).

Таблица маршрутизации узла $Y_7$ (2)		
Адрес назначения	Адрес соседнего узла	Расстояние
$Y_1$	$Y_6$	2
...	...	...

1.42

И наконец, если через некоторое время в узел  $Y_7$  поступит пакет от узла  $Y_1$ , маршрут которого пролегал через узел  $Y_4$ :  $Y_1 \rightarrow Y_4 \rightarrow Y_7$ , то поле «расстояние» в заголовке пакета будет иметь значение, равное 1, что меньше значения в таблице маршрутизации. Тогда после корректировки таблицы маршрутизации, соответствующая строка примет вид, показанный на рис.1.43.

Таблица маршрутизации узла $Y_7$ (3)		
Адрес назначения	Адрес соседнего узла	Расстояние
$Y_1$	$Y_4$	1
...	...	...

1.43

Таким образом, анализируя всякий раз адрес отправителя и расстояние от узла-отправителя всех проходящих через узел пакетов и корректируя таблицу маршрутизации, после некоторого времени получим в таблице маршрутизации наилучший маршрут, по которому будут передаваться пакеты с соответствующим адресом назначения. В нашем примере поступающие в узел  $Y_7$  пакеты с адресом назначения с АН= $Y_1$  будут направляться в узел  $Y_4$ .

#### 1.5.3.5. Методы фиксированной маршрутизации

Вторую группу методов маршрутизации образуют методы *фиксированной маршрутизации* (см. рис.1.39), предполагающие наличие таблицы маршрутизации, которая формируется в узле администратором сети и не изменяется, по крайней мере, в течение длительного периода функционирования сети.

Фиксированная маршрутизация может быть:

- **однопутевая**, когда таблица маршрутизации содержит для каждого адреса назначения только один маршрут, и пакеты с одним и тем же адресом назначения направляются всегда к одному и тому же узлу;
- **многопутевая**, когда таблица маршрутизации содержит для каждого адреса назначения несколько маршрутов (адресов соседних узлов), по которым могут быть направлены пакеты с одним и тем же адресом назначения.

Достоинством фиксированной маршрутизации, несомненно, следует считать простоту реализации.

В то же время существенным недостатком фиксированной маршрутизации является отсутствие гибкости, что проявляется в невозможности изменения маршрутов при изменении состава и топологии сети, а также при отказах узлов и каналов связи. В связи с этим, такие

методы маршрутизации могут применяться только в небольших и не изменяющихся в течение длительного промежутка времени сетях.

#### **1.5.3.6. Методы адаптивной маршрутизации**

*Адаптивная* или *динамическая маршрутизация* (рис.1.39) предполагает оперативное изменение таблиц маршрутизации при изменении состава и топологии сети, а также при отказах узлов и каналов связи. Адаптивная маршрутизация может быть реализована как:

- локальная;
- распределённая;
- централизованная;
- гибридная.

**Локальная маршрутизация** означает, что таблица маршрутизации изменяется (корректируется) на основе локальной информации о состоянии соответствующего узла, например о загрузке выходных каналов узла или о количестве пакетов, ожидающих в очереди освобождения выходного канала. При этом, если загрузка некоторого канала оказывается значительной, то таблица маршрутизации корректируется таким образом, чтобы выровнять загрузки всех выходных каналов.

*Недостаток* локальной маршрутизации состоит в том, что выбранный на основе локальной информации о состоянии узла маршрут может оказаться плохим, если соседний узел, к которому направляются пакеты, перегружен.

При **распределённой маршрутизации** корректировка таблицы маршрутизации осуществляется на основе не только локальной информации о состоянии соответствующего узла, но и с учётом состояний соседних узлов сети. Для этого узлы могут обмениваться специальными служебными пакетами, содержащими информацию о состоянии соседних узлов.

Недостаток распределённой маршрутизации очевиден – служебные пакеты создают дополнительную нагрузку в каналах и узлах сети, что при неудачной организации может существенно снизить производительность среды передачи данных, измеряемую количество пакетов, передаваемых с сети за единицу времени.

**Централизованная маршрутизация** предполагает наличие в сети специально выделенного узла, собирающего и анализирующего информацию о состоянии всех узлов сети. Результаты анализа рассылаются в виде служебных пакетов всем узлам, которые на их основе корректируют свои таблицы маршрутизации. Несмотря на кажущуюся эффективность такой маршрутизации, результирующий эффект может оказаться незначительным и даже привести к снижению эффективности передачи данных по сравнению с распределённой маршрутизацией в связи со значительным ростом числа передаваемых служебных пакетов, существенно загружающих каналы связи и сеть передачи данных в целом.

*Гибридная маршрутизация* представляет собой любую комбинацию рассмотренных выше методов маршрутизации.

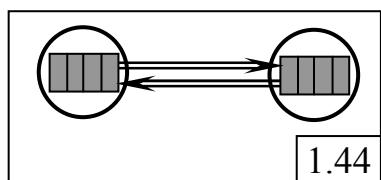
На практике в современных сетях передачи данных реализованы только некоторые из рассмотренных выше методов маршрутизации, причём конкретная реализация в маршрутизаторах разных фирм может быть различной и часто является секретом фирмы-разработчика.

#### 1.5.4. Задачи управления трафиком

Необходимость управления трафиком в сети обусловлена следующими **особенностями**, присущими сетевому трафику современных компьютерных сетей:

- *неоднородность трафика*, характеризующаяся наличием в сети нескольких типов данных, которые можно разделить на две большие группы: мультимедийные (речь, аудио и видео) и компьютерные (электронные письма, файлы и т.п.)
- наличие *различных (дифференцированных) требований* к качеству передачи данных разных типов;
- *случайный характер и нестационарность* сетевого трафика, обусловленные изменением интенсивностей потоков данных в различное время суток и непредсказуемостью характера и темпа работы пользователей в компьютерной сети;
- в свою очередь, нестационарность сетевого трафика может привести к возникновению в компьютерной сети периодов *перегрузок* и даже к блокировкам.

Блокировки в сети могут возникнуть в результате заполнения буферной памяти узлов. Простейший пример блокировок показан на рис.1.44, где буфера двух соседних узлов, желающих обменяться пакетами, заполнены до конца. Это приводит к ситуации, когда обмен пакетами невозможен, несмотря на то, что в принципе буферной памяти достаточно для хранения имеющихся пакетов. Однако, для того чтобы принять пакет от соседнего узла, необходимо иметь хотя бы один свободный буфер. Таким образом, узлы оказываются заблокированными, что может, в конечном счете, привести к остановке (блокировке) всей сети.

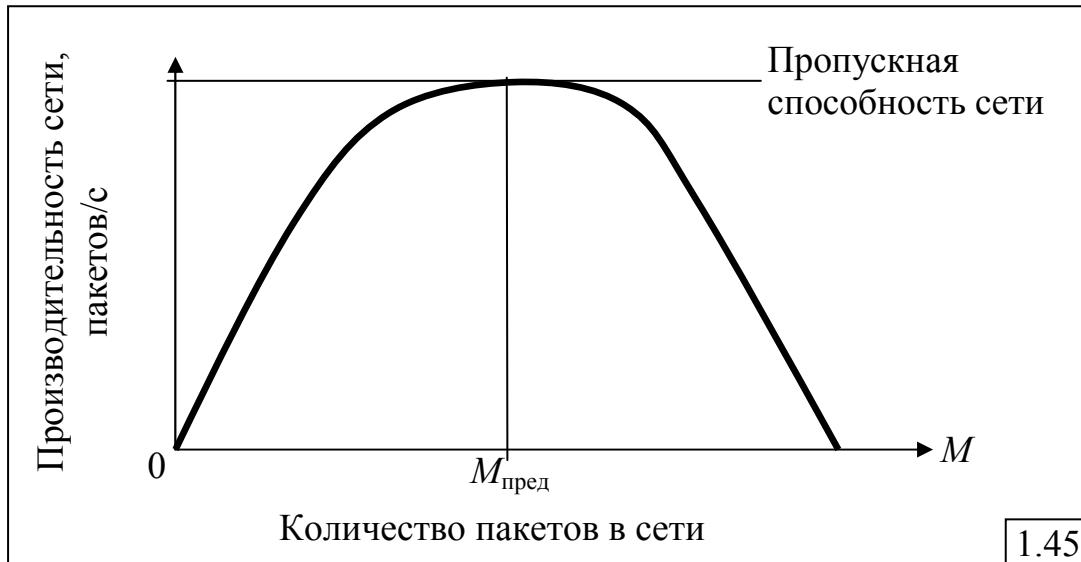


1.44

На рис.1.45 показана зависимость производительности сети передачи данных, измеряемая количеством пакетов, передаваемых в сети за единицу времени, от количества пакетов, находящихся в сети.

Вначале производительность сети передачи данных, как и следовало ожидать, растёт с увеличением количества находящихся в сети пакетов  $M$ , достигая при  $M_{\text{пред}}$  некоторого предельного значения, представляющего собой *пропускную способность сети*. При этом загрузка, по крайней мере, одного из узлов или каналов связи, называемого **узким местом**, достигает при  $M = M_{\text{пред}}$  значения 1, что приводит к *перегрузке* сети. Дальнейшее

увеличение количества пакетов в сети не приводит к росту производительности, значение которой будет определяться производительностью узкого места. Более того, дальнейшее увеличение количества пакетов в сети ведёт к снижению производительности и даже к прекращению передачи пакетов, то есть к остановке сети, что, в частности, связано с возникающими в сети блокировками.



Перечисленные выше особенности компьютерных сетей обуславливают необходимость управления неоднородным трафиком в сети для решения следующих задач:

- 1) обеспечение надежной передачи данных, предполагающей доставку данных абоненту без потерь и без искажения данных (за счет применения механизмов квитирования и тайм-аута);
- 2) обеспечение эффективной загрузки дорогостоящего сетевого оборудования (каналов и узлов) сети (за счет реализации механизма скользящего окна и перераспределения потоков данных в процессе адаптивной маршрутизации);
- 3) малые задержки при передаче по сети сообщений и, прежде всего, мультимедийных (за счет маршрутизации и приоритетов);
- 4) предотвращение перегрузок и блокировок при передаче данных (за счет приоритетов и ограничения входящего в сеть трафика).

Управление потоком данных реализуется на различных уровнях OSI-модели. Ниже рассматриваются некоторые наиболее типичные методы управления трафиком на первых трёх уровнях, а именно:

- процедура бит-стаффинга, используемая на физическом уровне;
- механизм «скользящего окна», используемый на канальном уровне;
- методы маршрутизации, используемые на сетевом уровне.

## 1.5.5. Методы управления трафиком на физическом уровне

### 1.5.5.1. Способы разделения кадров

На физическом уровне для разделения потока битов, соответствующих разным блокам данных 2-го уровня – кадрам, могут использоваться различные способы:

1) указание в заголовке кадра его длины и подсчет количества символов в процессе приема потока данных (основной недостаток – неустойчивость к помехам);

2) использование в качестве границы кадров запрещенных сигналов физического уровня;

3) использование в качестве границы кадров специальных стартовых и стоповых символов (байтов);

4) использование в качестве границы кадров специальных последовательностей битов.

### 1.5.5.2. Бит-стаффинг

При использовании в качестве границы кадров специальных последовательностей битов (например, в протоколах семейства HDLC используется специальная последовательность битов: 0111110, называемая *флагом*) возникает проблема, связанная с тем, что такая последовательность битов может встретиться внутри кадра и будет ошибочно воспринята аппаратурой передачи данных как обрамление, т.е. как начало следующего кадра. Для исключения этого используется процедура обеспечения прозрачности канала – бит-стаффинг.

*Бит-стаффинг* (*bit stuffing – вставка битов*) – техника вставки и стирания битов, используемая в высокоскоростных цифровых каналах связи с большим числом линий связи, не имеющих взаимной синхронизации, а также средство синхронизации в протоколах управления каналом связи типа HDLC.

Бит-стаффинг реализуется следующим образом. На передающем узле после пяти подряд следующих единиц внутри кадра принудительно вставляется 0, который автоматически изымается на приемном узле. Таким образом, исключается возможность появления внутри кадра последовательности битов 0111110, используемой для разделения кадров.

На рис.1.46 иллюстрируется процедура бит-стаффинга. Положим, что необходимо передать кадр, показанный на рис.1.46,а), в котором встречаются:

- шесть подряд идущих единиц (которые находятся между двумя нулевыми битами и могут быть восприняты как граница кадра);
- ровно пять единиц;
- более шести единиц.

В соответствии с рассмотренным выше принципом реализации бит-стаффинга в передающем узле после пяти любых подряд идущих единиц принудительно будут вставлены нулевые биты, как это показано на

рис.1.46,б). Отметим, что нули вставляются не зависимо от того, совпадает или не совпадает внутрикадровая битовая последовательность с флагом 01111110, используемым для разделения кадров. В результате такой процедуры по каналу связи будет передана последовательность битов, показанная на рис.1.46,в), которая анализируется в принимающем узле. Если после пяти подряд поступивших в узел единиц два следующих бита имеют значения 1 и 0, то такая комбинация рассматривается как граница кадра. Если же после пяти единиц следующий бит равен 0, то он изымается, и текст кадра принимает исходный вид рис.1.46,а).

а) 10001111101100111010110111101100001111111  
 б) 1000111110101100111010110111110011000011111011

в)

011111010001111101011001110101101111100110000111110110111110

1.46

При использовании в качестве границы кадров специальных стартовых и стоповых символов (байтов) реализуется «байт-стаффинг» – техника вставки, а точнее замены байтов, совпадающих с граничными в тексте кадра, на определённые последовательности других символов (см.протокол SLIP).

### 1.5.6. Управление трафиком на канальном уровне

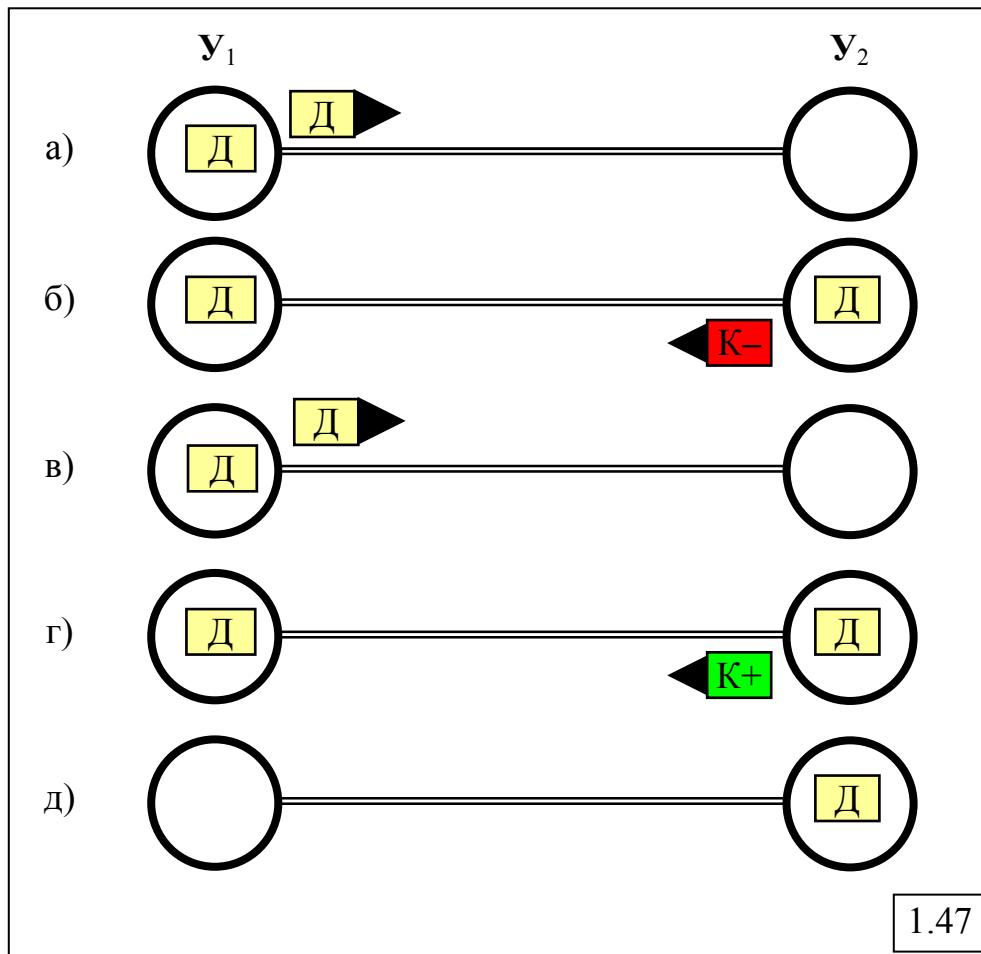
**На канальном уровне** управление потоком в канале связи между двумя узлами реализуется за счет применения:

- механизма квитирования;
- механизма тайм-аута;
- механизма скользящего окна.

#### 1.5.6.1. Квитирование

**Механизм квитирования** предназначен для обеспечения надёжной передачи данных (кадров или пакетов) и может быть реализован как на канальном, так и на более высоком уровне (например, сетевом или транспортном) OSI-модели. Реализация механизма квитирования на канальном уровне (в звене передачи данных) показана на рис.1.47 Положим, что в некоторый момент времени узел  $Y_1$  отправляет в узел  $Y_2$  кадр с данными ( $D$ ), причём копия отправленного кадра сохраняется в буферной памяти узла (рис.1.47,а). Узел  $Y_2$  после получения кадра от узла  $Y_1$  подсчитывает контрольную сумму и сравнивает её со значением, содержащимся в концевике. Если эти значения не совпадают, то узел  $Y_2$  формирует и отправляет узлу  $Y_1$  специальный служебный кадр ( $K-$ ), называемый *отрицательной квитацией*, свидетельствующей о том, что кадр был передан с ошибкой (рис.1.47,б). Узел  $Y_1$  анализирует квитацию и, если квитанция была отрицательной, повторно посыпает тот же самый

кадр Д (рис.1.47,в). Если подсчитанная в узле  $Y_2$  контрольная сумма совпадает со значением, содержащимся в концевике, то узел  $Y_2$  формирует и отправляет **положительную квитацию** (К+), свидетельствующую о том, что кадр был передан без ошибок (рис.1.47,г). Узел  $Y_1$  анализирует квитацию и, если квитация была положительной, удаляет сохранённую копию этого кадра из буферной памяти (рис.1.47,д).



### 1.5.6.2. Тайм-аут

Недостаток рассмотренного механизма квитирования состоит в том, что в случае потери кадра данных или квитанции в процессе передачи между узлами  $Y_1$  и  $Y_2$  узел-отправитель  $Y_1$  может ожидать прихода квитанции бесконечно долго. При этом становится невозможной передача других данных к узлу  $Y_2$ , что может привести в конечном счёте к прекращению передачи данных в сети. Для исключения подобной ситуации был реализован **механизм тайм-аута**, заключающийся в следующем. Узел-отправитель  $Y_1$  после завершения передачи данных (кадра) к узлу  $Y_2$  запускает таймер и ожидает поступления квитанции (положительной или отрицательной) в течение ограниченного промежутка времени  $\Delta t$ , называемого **тайм-аутом**.

Величина тайм-аута выбирается из следующего условия:  $\Delta t$  должно быть больше, чем удвоенное время передачи кадра между узлами, то есть  $\Delta t > 2\tau_k$ . Время передачи кадра между узлами  $\tau_k$  складывается из времени

распространения сигнала по каналу связи  $\tau_c$  и времени передачи кадра максимальной длины  $\tau_{\max}$ :  $\tau_k = \tau_c + \tau_{\max}$ .

Время распространения сигнала по каналу связи определяется как  $\tau_c = \frac{L}{v}$ , где  $L$  – длина канала и  $v$  – скорость распространения сигнала в среде передачи. Время передачи кадра максимальной длины зависит от длины кадра  $l_{\max}$  и пропускной способности канала  $C_{KC}$ :  $\tau_{\max} = \frac{l_{\max}}{C_{KC}}$ .

Тогда:  $\tau_k = \frac{L}{v} + \frac{l_{\max}}{C_{KC}}$  и условие для выбора величины тайм-аута примет вид:  $\Delta t > 2 \left( \frac{L}{v} + \frac{l_{\max}}{C_{KC}} \right)$ .

Если по истечении тайм-аута  $\Delta t$  узел-отправитель  $Y_1$  не получает квитанцию, то он повторно передаёт тот же кадр. Для исключения бесконечного числа передач одного и того же кадра обычно устанавливается некоторое предельное количество попыток передать кадр, после которого передача этого кадра прекращается, и данное направление передачи (маршрут) исключается из рассмотрения и в дальнейшем не используется, поскольку предполагается, что канал или узел данного маршрута находится в неисправном состоянии. Для рассматриваемого кадра выбирается новое направление передачи в соответствии с используемым методом маршрутизации.

*Недостатком* рассмотренного способа передачи данных является низкий коэффициент полезной загрузки канала, обусловленный большими накладными расходами на ожидание и передачу служебных квитанций. Коэффициент полезной загрузки канала, измеряемый как доля времени, используемого для передачи непосредственно пользовательских данных, составляет менее 30%, в чём несложно убедиться, используя следующие рассуждения.

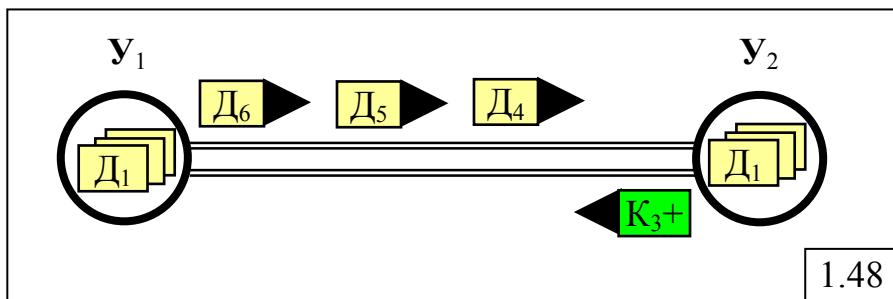
Пусть время передачи кадра данных равно  $\tau_k$ . Как показано выше, величина тайм-аута выбирается из условия:  $\Delta t > 2(\tau_c + \tau_{\max})$ , где  $\tau_c$  – время распространения сигнала в канале связи,  $\tau_{\max}$  – время передачи кадра максимальной длины. С учётом того, что  $\tau_k < \tau_{\max}$  и  $\tau_c > 0$ , положим  $\Delta t = 3\tau_k$ . Тогда коэффициент полезной загрузки канала:  $\rho_{KC} = \frac{\tau_k}{\Delta t} = \frac{\tau_k}{3\tau_k} = 0,33$ .

Следует иметь в виду, что этот результат справедлив при условии, что положительная квитанция поступила с первого раза. Если же первая передача кадра окажется неудачной, и в узел-отправитель поступит отрицательная квитанция, что потребует повторной передачи кадра, коэффициент полезной загрузки канала окажется гораздо ниже и составит:

$\rho_{KC} = \frac{\tau_k}{2\Delta t} = 0,165$ , то есть менее 20%. Это означает, что реальная скорость передачи данных по каналу с пропускной способностью 10 Мбит/с будет составлять менее 2 Мбит/с. Очевидно, что такая ситуация является экономически неприемлемой, особенно для высокоскоростных каналов.

### 1.5.6.3. Скользящее окно

Для увеличения коэффициента полезной загрузки канала используется **механизм «скользящего окна»**. Предварительно отметим, что если рассмотренные выше механизмы квитирования и тайм-аута предполагали наличие между взаимодействующими узлами полудуплексного канала, то механизм скользящего окна может быть реализован только при наличии дуплексного канала. При этом, кадры данных и квитанции могут передаваться одновременно по разным каналам (рис.1.48).



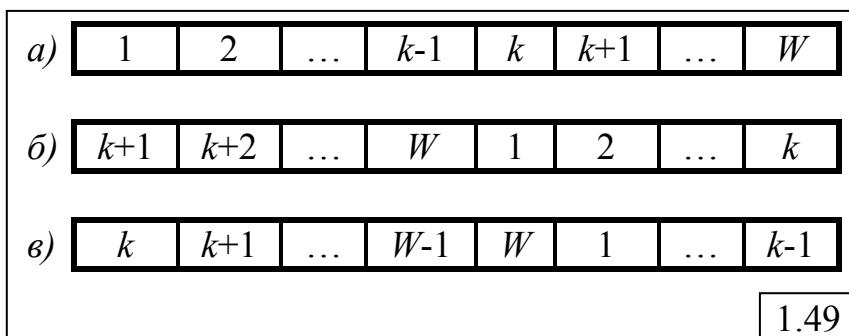
Суть механизма «скользящего окна» заключается в следующем. Узел-отправитель может послать подряд несколько кадров данных без получения на эти кадры квитанций. При этом кадры циклически нумеруются от 1 до  $W$ , где  $W$  – *размер (ширина) окна* – максимальное количество кадров, которые могут быть переданы без подтверждения. Номер кадра указывается в заголовке. Ширина окна может быть выбрана из условия максимальной загрузки прямого канала связи от узла-отправителя к узлу-получателю, которая может быть достигнута за счёт передачи ещё нескольких кадров за время ожидания квитанции на первый кадр:

$$W > \frac{T}{\tau_k} = \frac{2(\tau_c + \tau_k) + \tau_o}{\tau_k} = 2 + \frac{2\tau_c + \tau_o}{\tau_k},$$

где  $T = 2(\tau_c + \tau_k) + \tau_o$  – минимальное время ожидания квитанции;  $\tau_k$  – время передачи кадра,  $\tau_c$  – время распространения сигнала по каналу связи,  $\tau_o$  – время, затрачиваемое в узле-получателе на обработку кадра и формирование квитанции.

Как следует из представленного выражения, если пренебречь временем распространения сигнала по каналу связи и временем обработки кадра в узле-получателе  $Y_2$ , то минимальная ширина окна должна быть не менее 2.

Положим, что в начальный момент времени окно узла-отправителя  $Y_1$  выглядит так, как это показано на рис.1.49,а), что означает возможность передачи  $W$  кадров без подтверждения. Для того чтобы простой канала связи свести к минимуму, квитанция в узле-получателе может быть сформирована раньше, чем закончится передача всех  $W$  кадров, то есть узел-получатель может отправить квитанцию узлу-отправителю в любой удобный для него момент времени. Такой момент обычно связан с формированием кадра данных, посыпанного по обратному каналу от узла  $Y_2$  к узлу  $Y_1$ . При этом в заголовок этого кадра вставляется квитанция, указывающая номер последнего кадра, который был принят без ошибок (положительная квитанция) или с ошибкой (отрицательная квитанция). Если квитанция на кадр с номером  $k$  ( $1 < k < W$ ) – положительная, то окно в узле  $Y_1$  сдвигается так, как это показано на рис.1.49,б), что означает возможность передачи ещё  $W$  кадров с номерами  $k+1, \dots, W, 1, \dots, k$  без квитанции. Если квитанция на кадр с номером  $k$  ( $1 < k < W$ ) – отрицательная, то это означает, что кадры с номерами до  $(k-1)$  приняты правильно, а кадры, начиная с номера  $k$ , должны быть переданы повторно. При этом окно в узле  $Y_1$  сдвигается так, как это показано на рис.1.49,в) что означает возможность передачи ещё  $W$  кадров с номерами  $k, \dots, W, 1, \dots, k-1$  без квитанции. Таким образом, квитанция может формироваться не на все передаваемые кадры, а только на некоторые из них, причём, если положительная квитанция пришла на кадр с номером  $k$ , то считается, что этот кадр и все предыдущие кадры с номерами от 1 до  $(k-1)$  приняты без ошибок. Аналогично, отрицательная квитанция на кадр с номером  $k$  означает, что все предыдущие кадры приняты без ошибок, и повторной передаче подлежат все ранее переданные кадры, начиная с номера  $k$ .



### 1.5.7. Управление трафиком на высших уровнях OSI-модели

**На сетевом уровне** управление потоком в сети передачи данных реализуется за счет:

- применения различных методов маршрутизации;
- установления приоритетов между различными типами трафика.

**На транспортном уровне** управление потоком между конечными узлами сети реализуется за счет:

- установления приоритетов между различными типами трафика;
- ограничения поступающего от абонента трафика (например, когда скорость работы отправителя выше скорости получателя);
- ограничения доступа в сеть передачи данных.

**На сеансовом уровне** управление в коммутируемых сетях сеансом связи реализуется за счет применения различных способов установления соединения между абонентами.

## 1.6. Параметры и характеристики компьютерных сетей

Эффективность компьютерной сети может быть охарактеризована совокупностью величин, которые можно разделить на два класса (рис.1.50):

- параметры;
- характеристики.



**Параметры** компьютерной сети представляют собой величины, описывающие структурно-функциональную организацию сети и ее взаимодействие с внешней средой, в том числе, создаваемую в сети нагрузку.

**Характеристики** компьютерной сети описывают её эффективность и зависят от параметров.

Характеристики определяются в процессе эксплуатации сети путем измерений с помощью специальных измерительных средств – *сетевых мониторов* и в процессе решения задач системного анализа как функции параметров, т.е. являются *вторичными* по отношению к параметрам.

### 1.6.1. Параметры компьютерных сетей

Все параметры компьютерной сети можно разделить на три группы (см. рис.1.50):

- 1) **структурные параметры**, описывающие состав и структуру сети;

2) **функциональные параметры**, описывающие стратегию управления передачей данных в компьютерной сети и стратегию управления обработкой данных в узлах;

3) **нагрузочные параметры**, описывающие взаимодействие сети с внешней средой, то есть нагрузку, создаваемую в сети решаемыми прикладными задачами и передаваемыми в вычислительной сети данными.

В качестве *структурных* параметров компьютерных сетей используются:

- количество узлов, входящих в состав сети, и их взаимосвязь (топология сети);
- типы узлов, состав и количество оборудования (ЭВМ и сетевых устройств);
- технические данные устройств (производительность ВС и сетевых устройств – маршрутизаторов и коммутаторов, пропускные способности каналов связи и т.п.).

К *функциональным* параметрам компьютерных сетей относятся:

- способ коммутации;
- метод доступа к каналу связи;
- алгоритм выбора маршрута передачи данных в сети;
- распределение прикладных задач по узлам сети;
- режим функционирования ВС;
- последовательность выполнения прикладных задач в ВС;
- приоритеты задач и т.д.

В качестве *нагрузочных* параметров компьютерных сетей могут использоваться:

- число типов потоков данных (аудио, видео, компьютерные данные);
- интенсивности поступления сообщений (пакетов, кадров) разных типов в сеть или к отдельным ресурсам (узлам и каналам связи);
- длина передаваемых по сети блоков данных (пакетов, кадров);
- число типов прикладных задач;
- ресурсоемкость каждой задачи и т.д.

### 1.6.2. Характеристики компьютерных сетей

Характеристики компьютерных сетей – это совокупность показателей эффективности (качества) сети.

Характеристики компьютерных сетей можно разделить на две группы (см. рис.1.50):

- качественные;
- количественные.

Примерами *качественных* характеристик могут служить:

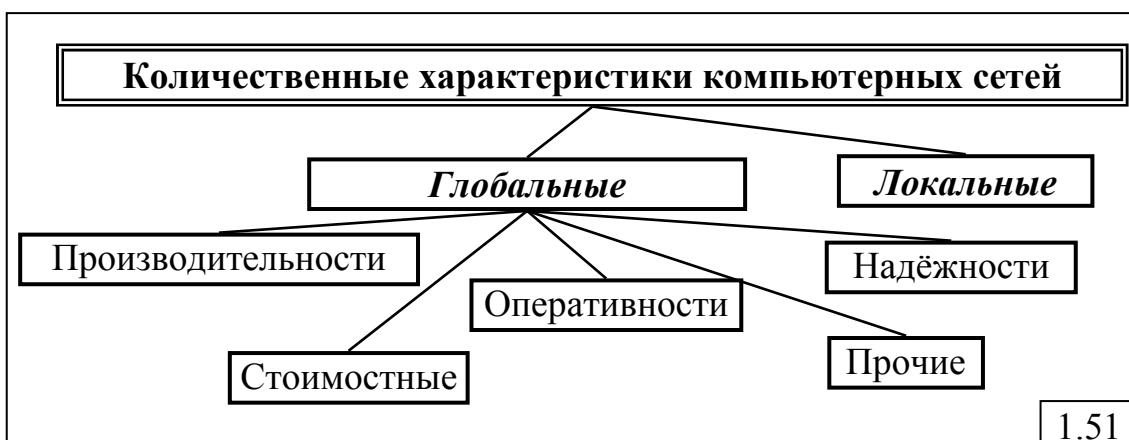
• **операционные возможности** сети, представляющие собой перечень услуг (сервисов) по передаче и обработке данных, предоставляемых пользователям сети, таких как передача данных между удаленными пользователями сети, доступ к удаленным файлам, доступ к

разнообразным вычислительным средствам, в том числе, к высокопроизводительным ВС, электронная почта, возможность передачи по сети разнообразных данных (речь, аудио, видео) и т.д.;

- **масштабируемость** – способность сети при ее наращивании (при увеличении ресурсов) линейно увеличивать свою производительность, которую можно оценить количественно через отношение прироста производительности системы к приросту ресурсов: чем ближе это отношение к единице, тем выше масштабируемость;
- **управляемость** – возможность администрирования с целью выявления и разрешения возникающих в сети проблем, а также планирования развития и модернизации сети;
- **гибкость** – сохранение качества функционирования сети при изменении её состава и конфигурации в результате выхода из строя оборудования или добавления новых устройств.

*Количественные* характеристики компьютерных сетей можно разделить на две группы (рис.1.51):

- **глобальные**, определяющие наиболее важные свойства сети как целостного объекта;
- **локальные**, определяющие свойства отдельных устройств или частей сети и позволяющие получить более детальное представление об эффективности сети.



К *глобальным* характеристикам относятся:

- характеристики производительности;
- характеристики оперативности;
- характеристики надежности;
- стоимостные характеристики;
- прочие характеристики (энергопотребления, массогабаритные и т.п.).

#### **1.6.2.1. Характеристики производительности**

**Производительность компьютерной сети** – мера мощности сети, определяющая количество работы, выполняемой сетью в единицу времени.

Понятие производительности охватывает широкую номенклатуру показателей эффективности компьютерной сети, определяющих качество

функционирования как сети в целом, так и отдельных ее подсистем и элементов – технических и программных средств.

Производительность сети зависит, в первую очередь, от производительности отдельных ее элементов, называемой *скоростью работы* или *быстродействием* устройств, например, скорость передачи данных по каналам связи, измеряемая объёмом данных, передаваемых за единицу времени, быстродействие ЭВМ или, точнее, процессора, измеряемое числом команд, выполняемых в единицу времени, и т.п.

Для оценки производительности компьютерной сети в целом используется следующая совокупность показателей:

- **производительность СТК** (сети передачи данных), измеряемая числом сообщений (пакетов, кадров, бит) передаваемых по сети за единицу времени;

- **производительность СВТ** (средств обработки данных), представляющая собой суммарную производительность всех средств ВТ (ЭВМ и систем), входящих в состав сети.

*Производительность СТК (коммуникационная мощность)* может быть задана следующими показателями:

- *максимальная* или *пределная производительность*, называемая **пропускной способностью сети передачи данных** и измеряемая количеством пакетов (кадров), передаваемых в сети за единицу времени;

- *реальная* или *фактическая производительность* сети передачи данных, которая может быть задана как среднее значение на некотором интервале времени или как мгновенное значение в конкретный момент времени.

*Производительность СВТ (вычислительная мощность)* в целом складывается из производительностей ВС, выполняющих обработку данных в сети.

Наиболее важным показателем производительности ВС, как совокупности технических и программных средств, является **системная производительность**  $\lambda_0$ , измеряемая числом задач, выполняемых системой за единицу времени:

$$\lambda_0 = \lim_{T \rightarrow \infty} \frac{m(T)}{T},$$

где  $m(T)$  - число задач, выполненных за время  $T$ .

Очевидно, что системная производительность зависит от режима функционирования, реализуемого управляющими программами операционной системы, и класса решаемых задач, т.е. вычислительной нагрузки.

#### **1.6.2.2. Характеристики оперативности**

Характеристики оперативности описывают задержки, возникающие при передаче и обработке данных в сети.

Для оценки оперативности сети в целом используются следующие показатели:

- время доставки пакетов (сообщений);
- время отклика (ответа).

**Время доставки (время задержки)** пакетов характеризует эффективность организации передачи данных в вычислительной сети и представляет собой интервал времени, измеряемый от момента поступления пакета или сообщения в сеть до момента получения пакета адресатом.

В общем случае, время задержки – величина случайная, что обусловлено случайным характером процессов поступления и передачи данных в сети. В компьютерных сетях обычно время доставки задаётся средним значением  $T$ , на которое может налагаться ограничение  $T < T^*$  в зависимости от типа передаваемых данных.

При передаче мультимедийных данных кроме среднего значения времени доставки пакетов важной характеристикой является **вариация** или **джиттер задержки**, представляющая собой среднеквадратическое отклонение времени задержки разных пакетов.

**Время отклика (ответа)** – интервал времени от момента поступления запроса (сообщения, транзакции) в сеть до момента завершения его обслуживания, связанного с выполнением некоторой прикладной или обслуживающей программы, с обращением к базе данных и т.п. Время ответа представляет собой *время пребывания запроса в сети* и характеризует эффективность как телекоммуникационных, так и вычислительных средств компьютерной сети.

Время отклика, как и время задержки, – величина случайная и может задаваться средним значением  $U$  или в виде вероятности  $P(t_u < U^*)$  непревышения некоторого заданного значения  $U^*$ .

В сетях реального времени вместо термина "время ответа" часто используют термин "время реакции".

#### **1.6.2.3. Характеристики надежности**

**Надежность** - способность компьютерной сети сохранять свои наиболее существенные свойства на заданном уровне и выполнять возложенные на нее функции в течение фиксированного промежутка времени при определенных условиях эксплуатации.

При рассмотрении вопросов надежности следует различать отказы и сбои.

**Отказ** – частичная или полная утрата работоспособности сети, приводящая к невыполнению или неправильному выполнению возложенных на нее функций. Для восстановления работоспособности системы при отказе требуется проведение ремонта.

**Сбой** – кратковременная утрата работоспособности сети, характеризуемая возникновением ошибки при передаче и обработке данных. Для восстановления работоспособности сети при сбое требуется проведение повторных действий по передаче (обработке) данных или части данных или перезагрузки отдельных узлов или всей сети. Сбои не

приводят к выходу сети из строя, однако могут существенно снизить эффективность функционирования, что проявляется в ухудшении характеристик функционирования сети (увеличивается время доставки сообщений и снижается производительность сети).

В качестве характеристик надежности обычно используются следующие показатели:

- **вероятность безотказной работы** сети  $P(t)$  – вероятность того, что в течение времени  $t$  не произойдет отказа;
- **интенсивность отказов**  $\lambda_o$  – среднее число отказов за единицу времени;
- **время наработки на отказ** – промежуток времени между двумя смежными отказами – величина случайная, а ее среднее значение  $T_o$  называется *средней наработкой на отказ*  $T_o = 1/\lambda_o$ ;
- **время восстановления** – интервал времени от момента наступления отказа до момента восстановления работоспособности системы – величина случайная и обычно задается средним значением  $T_b$ , называемым *средним временем восстановления*;
- **коэффициент готовности**  $K_r$  – доля времени, в течение которого сеть работоспособна:  $K_r = T_o/(T_o+T_b)$ .

Величина  $K_r$  может трактоваться как вероятность того, что в любой момент времени сеть работоспособна. Аналогично, значение  $(1-K_r)$  определяет вероятность того, что сеть находится в состоянии восстановления (неработоспособна).

#### **1.6.2.4. Стоимостные характеристики**

В качестве стоимостных (экономических) характеристик компьютерной сети могут использоваться следующие показатели:

- полная стоимость владения (*Total cost of ownership*, ТСО) – затраты, рассчитываемые на всех этапах жизненного цикла сети и включающие стоимость технических, информационных и программных средств (прямые затраты) и затраты на эксплуатацию сети (косвенные затраты);
- стоимость (цена) передачи данных и обработки данных в сети, определяемая объемом и стоимостью используемых ресурсов сети соответственно при передаче и обработке данных.

#### **1.6.2.5. Локальные характеристики ВС**

В качестве локальных характеристик компьютерных сетей могут использоваться *в зависимости от целей исследования* самые разнообразные показатели эффективности.

Локальные характеристики описывают эффективность функционирования:

- узлов и каналов связи;
- отдельных сегментов сети;
- узлов обработки данных: ВС и ее подсистем.

Локальные характеристики могут быть разбиты на две группы:

- временные;
- безразмерные.

К временными характеристикам относятся:

- время доставки (задержки) пакетов при передаче между соседними узлами сети;
- время ожидания передачи данных в узлах сети или освобождения ресурсов ВС (сервера);
- время пребывания данных в различных узлах, устройствах или подсистемах.

К безразмерным характеристикам относятся:

- число пакетов, находящихся в буферной памяти узлов (маршрутизаторов, коммутаторов);
- коэффициенты загрузок узлов, каналов связи и устройств ВС и т.д.

**Коэффициент загрузки** или просто **загрузка**  $\rho$  устройства – это доля времени, в течение которого устройство работает:  $\rho = \lim_{T \rightarrow \infty} \frac{t}{T}$ , где  $t$  – время, в течение которого устройство работало;  $T$  – время наблюдения. Загрузка  $\rho$  характеризует степень использования устройства и часто называется *коэффициентом использования устройства*. Поскольку  $0 \leq \rho \leq 1$ , то загрузка может трактоваться как вероятность того, что в любой момент времени устройство работает. Величина  $\eta = 1 - \rho$  называется **коэффициентом простоя** устройства и характеризует долю времени, в течение которого устройство не работает (простаивает).

## 1.7. Сетевые протоколы

В современном мире существует большое количество различных сетевых технологий, каждая из которых реализуется множеством протоколов.

Множество протоколов разных уровней одной сетевой технологии называется **стеком протоколов**.

В настоящее время существует большое количество сетевых технологий с соответствующими стеками протоколов, в том числе: TCP/IP, XNS, IPX, AppleTalk, DECnet, SNA и др. Рассмотрим кратко некоторые из них и попытаемся установить их соответствие разработанной OSI-модели.

### 1.7.1. TCP/IP

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol) разработан по заказу Министерства обороны США с целью обеспечения быстрого увеличения числа компьютеров с разными операционными системами в сети за счет стандартизации.

Содержит 4 уровня.

**Уровень 1 – сетевой интерфейс** – реализует функции физического и канального уровня в OSI-модели:

- управляет обменом данными между устройством и сетью;
- маршрутизирует данные между устройствами одной сети.

**Уровень 2 – межсетевой** – соответствует сетевому уровню в OSI-модели:

- управляет обменом данными между устройствами, находящимися в разных сетях (обеспечивает дейтаграммный сервис в терминах IEEE-модели);
- отвечает за функции сетевой адресации.

**Уровень 3 – транспортный** – соответствует транспортному уровню в OSI-модели: обеспечивает связь "end-to-end" между источником и приемником данных.

**Уровень 4 – прикладной** – соответствует высшим уровням (5-7) в OSI-модели и обеспечивает функции, необходимые пользовательским (прикладным) программам, например, удаленное подключение к машине, передача файлов и т.д.

### 1.7.2. XNS

Стек протоколов XNS (Xerox Network Services Internet Transport Protocol) разработан компанией Xerox для передачи данных по сетям Ethernet.

Содержит 5 уровней.

**Уровень 1 – среда передачи** – реализует функции физического и канального уровня в OSI-модели:

- управляет обменом данными между устройством и сетью;
- маршрутизирует данные между устройствами одной сети.

**Уровень 2 – межсетевой** – соответствует сетевому уровню в OSI-модели:

- управляет обменом данными между устройствами, находящимися в разных сетях (обеспечивает дейтаграммный сервис в терминах IEEE-модели);
- описывает способ прохождения данных через сеть.

**Уровень 3 – транспортный** – соответствует транспортному уровню в OSI-модели:

- обеспечивает связь "end-to-end" между источником и приемником данных.

**Уровень 4 – контролльный** – соответствует сессионному и представительному уровню в OSI-модели:

- управляет представлением данных;
- управляет контролем над ресурсами устройств.

**Уровень 5 – прикладной** – соответствует высшим уровням в OSI-модели:

- обеспечивает функции обработки данных для прикладных задач.

### 1.7.3. IPX

Протокол IPX (Internet Packet Exchange) описан компанией Novell как "сервис", который позволяет приложениям посыпать и получать сообщения через сеть. Поддерживает большое многообразие топологий ЛВС и физических средств передачи данных.

Содержит, как и протокол XNS, 5 уровней и во многом повторяет XNS.

Отличие заключается только в том, что IPX имеет несколько добавочных функций, например, возможность передачи служебных сообщений.

Протокол IPX обеспечивает:

- высокую производительность файлового сервера в ЛВС;
- простоту администрирования в малых и средних сетях;
- может работать в больших сетях и сетях с неоднозначными маршрутами, в том числе с несколькими соединениями сервера для распределения нагрузки.

Протокол IPX не гарантирует доставки сообщения, т.е. IPX-пакет может быть потерян. Для обеспечения гарантированной доставки разработан протокол SPX (Sequenced Packet Exchange - последовательный обмен пакетами), обеспечивающий подтверждение успешного прохождения сообщения по сети. В большинстве случаев IPX и SPX реализуются как единый протокол (одной программой) IPX/SPX.

### 1.7.4. AppleTalk

Протокол AppleTalk (компании Apple Computer) предназначен для связи между компьютерами Macintosh и наиболее близок к OSI-модели - содержит 6 уровней, причем высший (представительный) уровень объединяет в себе функции прикладного и представительного уровней OSI-модели.

### 1.7.5. DECnet

Стек протоколов DECnet (Digital Equipment Corporation net) содержит 7 уровней (рис.1.52).

Уровень	Наименование
7	Прикладной (пользовательский)
6	Сетевые приложения
5	Контроль сессии
4	Коммуникации "конец связи"
3	Маршрутизационный
2	Канальный
1	Физический канал

1.52

Несмотря на разницу в терминологии, уровни DECnet очень похожи на уровни OSI-модели.

DECnet реализует концепцию сетевой архитектуры DNA (Digital Network Architecture), разработанную фирмой DEC, согласно которой разнородные вычислительные системы (ЭВМ разных классов), функционирующие под управлением различных операционных систем, могут быть объединены в территориально-распределенные информационно-вычислительные сети.

### 1.7.6. SNA

Протокол SNA (System Network Architecture) компании IBM предназначен для удаленной связи с большими компьютерами и содержит 7 уровней (рис.1.53).

Уровень	Наименование
7	Сервис транзакций
6	Представительный сервис
5	Контроль потока данных
4	Контроль передачи
3	Контроль маршрута
2	Контроль канала
1	Физический контроль

1.53

SNA основана на концепции главной (хост)-машины и обеспечивает доступ удаленных терминалов к мейнфреймам IBM.

Основной отличительной чертой SNA является наличие возможности доступа каждого терминала к любой прикладной программе главной ЭВМ. Системная сетевая архитектура реализована на базе виртуального телекоммуникационного метода доступа (Virtual Telecommunication Access Method - VTAM) в главной ЭВМ. VTAM управляет всеми линиями связи и терминалами, причем каждый терминал имеет доступ ко всем прикладным программам.

### 1.7.7. Сопоставление коммуникационных моделей и протоколов

Ниже в табл.1.2 представлены рассмотренные стеки протоколов и показано их соответствие рекомендованной Международной организацией по стандартизации OSI-модели.

Таблица 1.2

	<b>OSI</b>	<b>TCP/IP</b>	<b>XNS(IPX)</b>	<b>AppleTalk</b>	<b>DECnet</b>	<b>SNA</b>
7	Прикладной	Прикладной	Прикладной	Представления	Прикладной (пользовательский)	Сервис транзакций
6	Представления		Контрольный		Сетевые приложения	Представительный сервис
5	Сеансовый (сессионный)			Сессионный	Контроль сессии	Контроль потока данных
4	Транспортный	Транспортный	Транспортный	Транспортный	Коммуникации "конец-связи"	Контроль передачи
3	Сетевой	Межсетевой	Межсетевой	Сетевой	Маршрутизационный	Контроль маршрута
2	Канальный (передачи данных)	Сетевой интерфейс	Канальный интерфейс	Канальный	Канальный	Контроль канала
1	Физический			Физический	Физический канал	Физический контроль

## **Раздел 2. СРЕДСТВА ТЕЛЕКОММУНИКАЦИЙ**

## **2.1. Основные понятия техники связи**

## **2.1.1. Телекоммуникация**

**电信** Телекоммуникация (греч. *tele* – вдаль, далеко и лат. *communicatio* – общение) – передача данных на большие расстояния. **远距离传输数据**

**Средства телекоммуникации** – совокупность технических, программных и организационных средств для передачи данных на большие расстояния.

**Телекоммуникационная сеть** – множество средств телекоммуникации, связанных между собой и образующих сеть определённой топологии (конфигурации). Телекоммуникационными сетями являются (рис.2.1):

- телефонные сети для передачи телефонных данных (голоса);
  - радиосети для передачи аудиоданных;
  - телевизионные сети для передачи видеоданных;
  - цифровые (компьютерные) сети или сети передачи данных (СПД) для передачи цифровых (компьютерных) данных.



Данные в цифровых телекоммуникационных сетях формируются в виде *сообщений*, имеющих определенную структуру и рассматриваемых как единое целое.

Данные (сообщения) могут быть:

- непрерывными;
  - дискретными.

Непрерывные данные могут быть представлены в виде непрерывной функции времени, например, речь, звук, видео. Дискретные данные состоят из знаков (символов).

Передача данных в телекоммуникационной сети осуществляется с помощью их физического представления – *сигналов*.

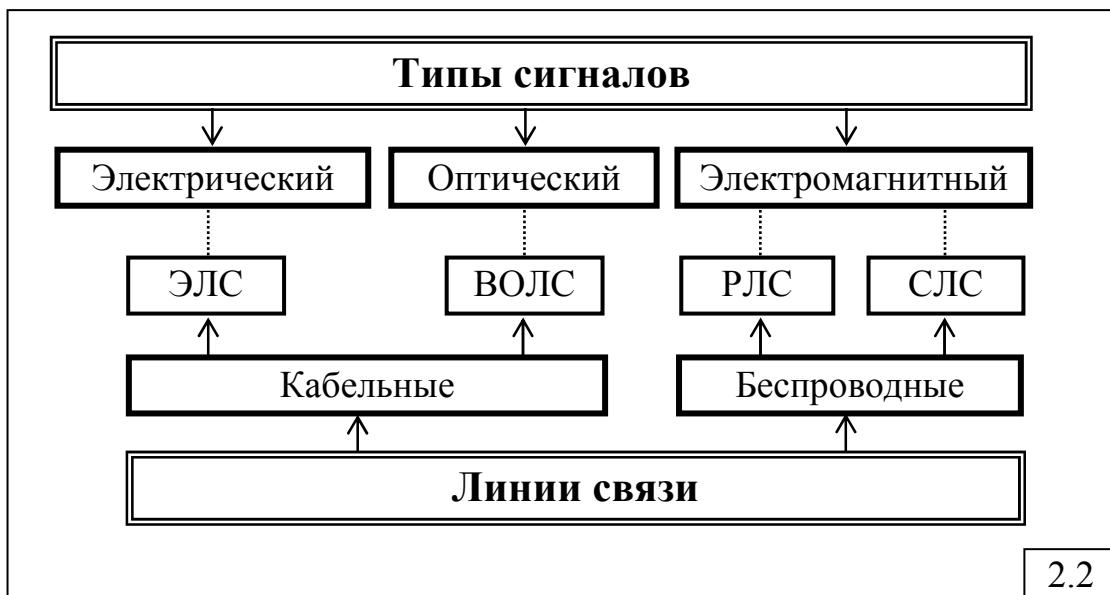
В компьютерных сетях для передачи данных используются следующие типы сигналов (рис.2.2):

- электрический (электрический ток);
  - оптический (свет);
  - электромагнитный (электромагнитное поле излучения – радиоволны).

Для передачи электрических и оптических сигналов применяются кабельные линии связи соответственно (рис.2.2):

- электрические (ЭЛС);
- волоконно-оптические (ВОЛС).

Передача электромагнитных сигналов осуществляется через радиолинии (РЛС) и спутниковые линии связи (СЛС).



Сигналы, как и данные, могут быть:

- *непрерывными*;
- *дискретными*.

При этом, непрерывные и дискретные *данные* могут передаваться в телекоммуникационной сети либо в виде непрерывных, либо в виде дискретных *сигналов*.

Процесс преобразования (способ представления) данных в вид, требуемый для передачи по линии связи и позволяющий, в некоторых случаях, обнаруживать и исправлять ошибки, возникающие из-за помех при их передаче, называется **кодированием**. Примером кодирования является представление данных в виде двоичных символов. В зависимости от параметров среды передачи и требований к качеству передачи данных могут использоваться различные методы кодирования.

**Линия связи** – физическая среда, по которой передаются информационные сигналы, формируемые специальными техническими средствами, относящимися к линейному оборудованию (передатчики, приемники, усилители и т.п.). Линию связи часто рассматривают как совокупность физических цепей и технических средств, имеющих общие линейные сооружения, устройства их обслуживания и одну и ту же среду распространения. Сигнал, передаваемый в линии связи, называется **линейным** (от слова линия).

Линии связи можно разбить на 2 класса (см. рис.2.2):

- кабельные (электрические и волоконно-оптические линии связи);
- беспроводные (радиолинии).

На основе линий связи строятся каналы связи.

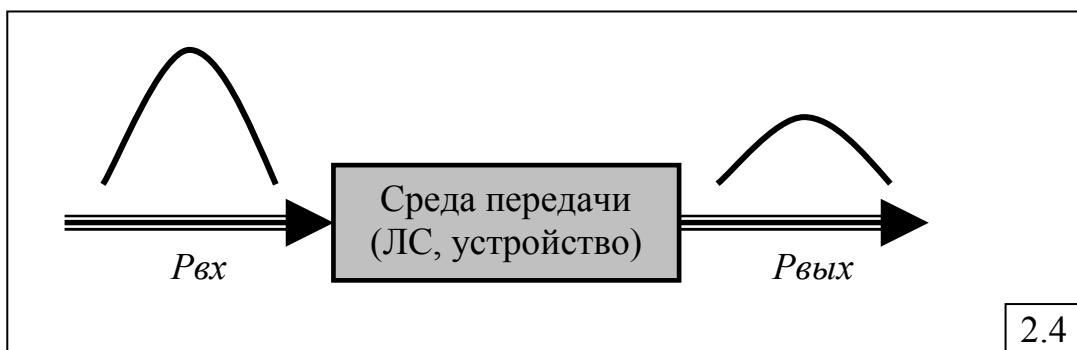
**Канал связи** представляет собой совокупность одной или нескольких линий связи и канaloобразующего оборудования, обеспечивающих передачу данных между взаимодействующими абонентами в виде физических сигналов, соответствующих типу линии связи.

Канал связи может состоять из нескольких последовательных линий связи, образуя составной канал, например, как это показано на рис.2.3: между абонентами A1 и A2 сформирован канал связи, включающий телефонные (ТфЛС) и волоконно-оптическую (ВОЛС) линии связи. В то же время, в одной линии связи, как будет показано ниже, может быть сформировано несколько каналов связи, обеспечивающих одновременную передачу данных между несколькими парами абонентов.



## 2.1.2. Сигналы

При передаче сигнала через некоторую среду передачи (линия связи, некоторое устройство) происходит изменение сигнала (усиление или ослабление), обусловленное техническими и физическими свойствами среды передачи (рис.2.4.).



Усиление и ослабление (отношение энергий или мощностей) некоторой физической величины – *сигнала* (напряжения, тока, мощности, энергии поля и т.д.) в электротехнике, радиотехнике, электросвязи и акустике измеряют в **децибелах** (дБ) – логарифмических единицах усиления (ослабления):

$$d[\text{дБ}] = 10 \lg \frac{P_{вых}}{P_{вх}},$$

где  $P_{вх}$  и  $P_{вых}$  – значения мощности (энергии) соответственно входного и выходного сигналов.

Отношение  $K = P_{вых} / P_{вх}$  называется **коэффициентом передачи**.

Величина  $d$ , выраженная в децибелах, называется **коэффициентом усиления**, если  $d > 0$ , и **коэффициентом затухания**, если  $d < 0$ . На практике обычно знак минус перед коэффициентом затухания опускают и определяют часто коэффициент затухания как положительную величину.

Соответствие между значением коэффициента затухания (усиления), вычисленного в децибелах, и значением коэффициента передачи иллюстрируется следующей таблицей:

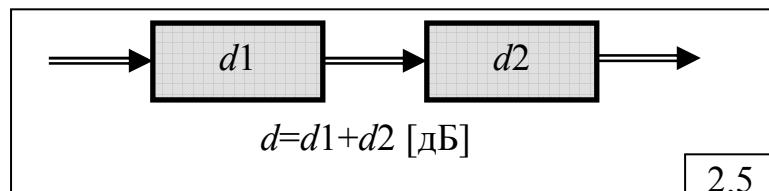
$d, \text{дБ}$	1	2	3	5	10	13	16	17	20	25	30
K	1,26	1,59	2,0	3,16	10	19,95	39,8	50,1	100	316,2	1000

В децибелах также может быть выражено отношение двух напряжений  $U$  или токов  $I$ :

$$d[\text{дБ}] = 20 \lg \left( \frac{U_{\text{вых}}}{U_{\text{вх}}} \right) \quad \text{или} \quad d[\text{дБ}] = 20 \lg \left( \frac{I_{\text{вых}}}{I_{\text{вх}}} \right).$$

Например, ослабление  $d=10$  дБ/км означает, что ослабление напряжения или тока на расстоянии в 1 км согласно уравнению  $10 = 20 \lg K$  будет равно  $K = \sqrt{10} \approx 3,3$  раза.

Удобство вычисления ослабления (усиления) в децибелах состоит в том, что при каскадном включении нескольких участков линии или технических устройств значения  $d$  складываются (рис.2.5).



Например, в случае  $d=10$  дБ/км ослабление на расстоянии в 2 км будет равно 20 дБ.

Сигналы, как и данные, могут быть:

- **непрерывными (аналоговыми)** – в виде непрерывной функции времени (изменение тока, напряжения, электромагнитного поля излучения);
- **дискретными (цифровыми)** – в виде импульсов тока, напряжения, света.

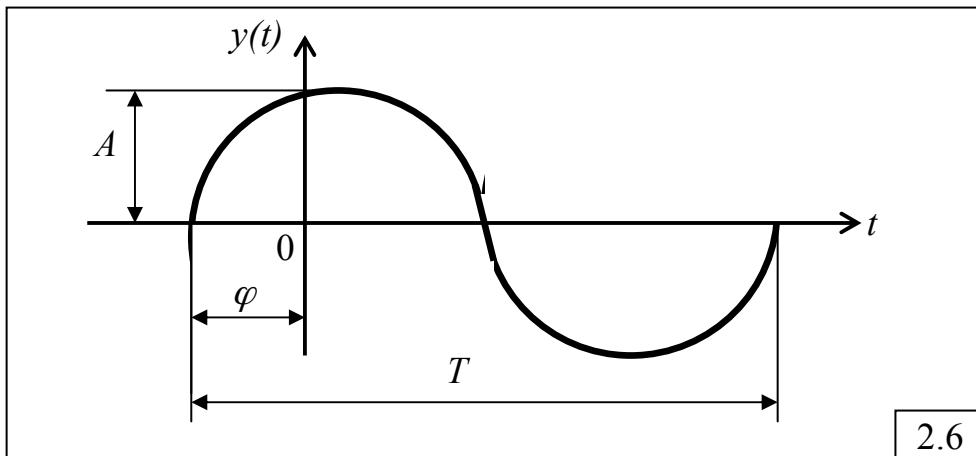
Сигналы, используемые для передачи данных, должны быть **информационными**, то есть нести информацию о передаваемом сообщении. Очевидно, что постоянный ток, не изменяющий своего значения и направления передачи, не может служить переносчиком информации. Сигнал должен иметь некоторые изменяющиеся параметры, которые на приёмном конце позволят идентифицировать передаваемые данные. В качестве такого информационного сигнала часто используют так называемый гармонический сигнал.

### 2.1.3. Спектр

В простейшем случае *непрерывный сигнал* может быть представлен в виде гармонического колебания (рис.2.6), описываемого синусоидой:

$$y(t) = A \sin(\omega t + \varphi) = A \cos(\omega t + \varphi'),$$

где  $A$  – амплитуда;  $\omega$  – круговая частота:  $\omega = 2\pi f$  (здесь  $f$  – линейная частота:  $f = 1/T$  – величина, обратная периоду  $T$ );  $\varphi, \varphi'$  – начальная фаза, причем:  $\varphi' = \varphi - \frac{\pi}{2}$ .



Синусоидальный сигнал несет в себе информацию в виде трех параметров: *амплитуды, частоты и фазы*, причем с точки зрения обеспечения высокой скорости передачи данных основной является частота сигнала – чем выше частота, тем больше скорость передачи данных. Среда передачи должна обеспечивать качественный перенос сигнала с минимально возможными искажениями его параметров.

Функция времени  $y(t)$ , описывающая некоторый непрерывный сигнал, в общем случае, может быть произвольной и иметь временные изменения любой скорости – от самых медленных и вплоть до бесконечно быстрых скачкообразных изменений. Тогда широкий класс периодических функций  $y(t)$  может быть представлен рядом Фурье:

$$y(t) = \sum_{i=0}^{\infty} A_i \cos(\omega_i t + \varphi_i) = \frac{A_0}{2} + \sum_{i=1}^{\infty} A_i \cos(\omega_i t + \varphi_i),$$

где  $A_i$  – амплитуда;  $\varphi_i$  – начальная фаза;  $\omega_i$  – круговая частота  $i$ -й синусоиды, причем эти синусоиды пронумерованы таким образом, что:  $\omega_0 < \omega_1 < \dots < \omega_{\infty}$ ,  $\omega_0 = 2\pi f_0 = 0$  ( $T_0 = 1/f_0 = \infty$ ) и  $\omega_{\infty} = 2\pi f_{\infty} = \infty$  ( $T_{\infty} = 1/f_{\infty} = 0$ ).

Таких сигналов, обладающих бесконечным спектром, которые содержат синусоиды (гармоники) с частотами в интервале от  $f_0 = 0$  до  $f_{\infty} = \infty$ , в природе практически нет. Преобладающая часть энергии реальных сигналов сосредоточена в ограниченной полосе частот. Такие сигналы и отображающие их функции называются **сигналами**

**(функциями) с ограниченным спектром** и могут быть представлены в виде конечной суммы синусоидальных сигналов:

$$y(t) = \sum_{i=1}^n A_i \cos(\omega_i t + \varphi_i).$$

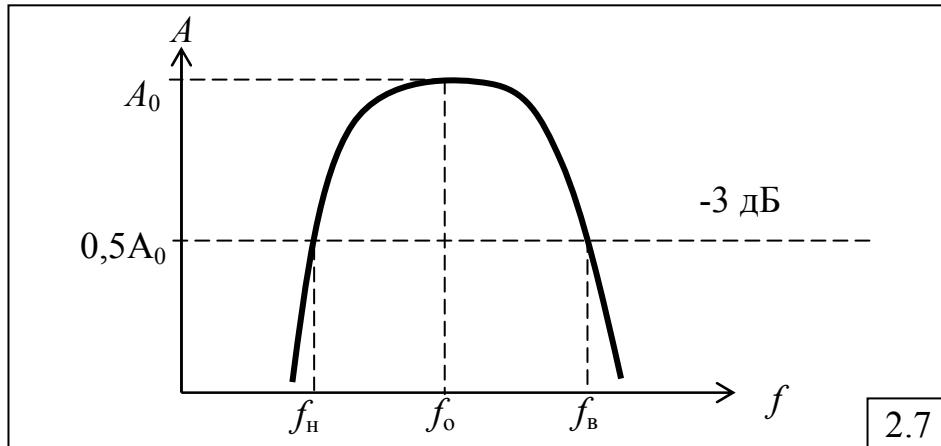
Пусть, как и ранее,  $\omega_1 < \omega_2 < \dots < \omega_n$ , причём  $\omega_1 = 2\pi f_1 > 0$  и  $\omega_n = 2\pi f_n < \infty$ . Тогда:  $S = (f_n - f_1)$  представляет собой **спектр сигнала**  $y(t)$ , где  $f_n$  – верхняя граница частот (верхняя частота);  $f_1$  – нижняя граница частот (нижняя частота).

Для того чтобы передать такой сигнал *без искажений*, канал связи должен иметь *полосу пропускания* шириной не менее  $S$ .

#### 2.1.4. Полоса пропускания

**Полосой пропускания (частот)** канала (линии) связи называется диапазон частот, в пределах которого амплитудно-частотная характеристика (АЧХ) канала достаточно равномерна для того, чтобы обеспечить передачу сигнала без существенного искажения.

*Полоса пропускания*  $F$  для канала (линии) связи определяется как область частот в окрестности  $f_0$ , в которой амплитуда сигнала (напряжение или ток) уменьшается не более чем в  $\sqrt{2} = 1,41$  раз (в 2 раза для мощности) по сравнению с максимальным значением  $A_0$ , что примерно соответствует значению -3 дБ (рис.2.7):  $F = f_v - f_n$ .



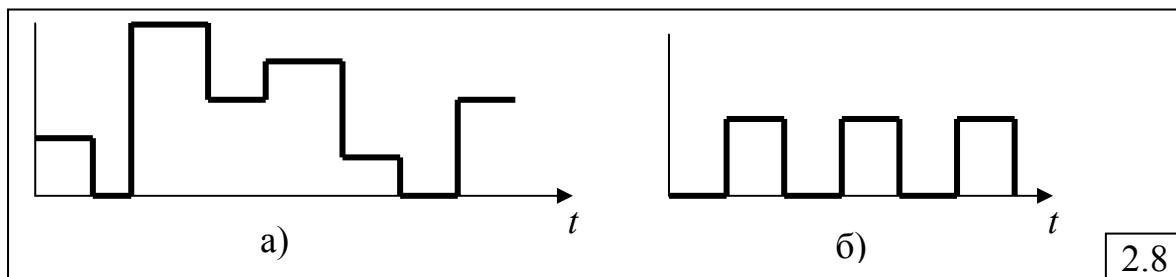
*Дискретные сигналы* (рис.2.8,а) характеризуются бесконечным спектром частот и могут быть представлены в виде бесконечной суммы синусоидальных сигналов:

$$y(t) = \sum_{i=0}^{\infty} A_i \cos(\omega_i t + \varphi_i).$$

Бесконечную ширину имеет также спектр двоичного сигнала, представляющего собой последовательность чередующихся посылок "0" и "1" (рис.2.8,б).

При проектировании системы передачи данных, в частности, при расчете ее пропускной способности, важно знать *максимальную ширину*

спектра частот передаваемого сигнала, независимо от его структуры (непрерывный, дискретный).



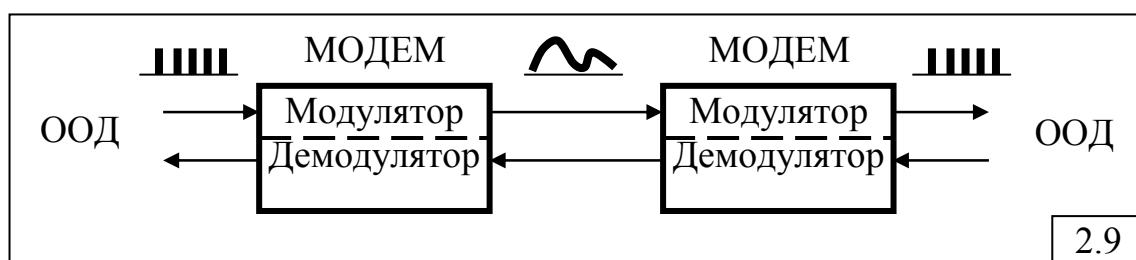
Для качественной передачи сигнала по каналу связи с возможностью его восстановления (распознавания) в точке приёма необходимо, чтобы выполнялись следующие условия:

- полоса пропускания (частот)  $F = f_e - f_n$  канала связи должна быть не менее чем спектр частот сигнала  $S = f_n - f_1$ :  $F \geq S$ ;
- ослабление (затухание) сигнала не превышало некоторой пороговой величины, необходимой для его корректного восстановления (распознавания) в точке приема сигнала (**искажение амплитуды сигнала**);
- дрожание фазы (джисттер) не превышало пороговой величины, необходимой для его корректного восстановления (распознавания) в точке приема сигнала (**искажение фазы сигнала**).

### 2.1.5. Модуляция

При использовании низкочастотных кабельных каналов связи (например телеграфных), полоса частот которых начинается примерно от нуля, дискретные сигналы можно передавать в их естественном виде – без модуляции (в первичной полосе частот) – с небольшой скоростью 50 – 200 бит/с.

В высокоскоростных каналах связи с резко ограниченной полосой пропускания передача сигналов осуществляется посредством модуляции и демодуляции с помощью специальных устройств, называемых **модемами** (**модулятор-демодулятор**). На рис.2.9 показано применение модемов для преобразования дискретного сигнала, поступающего от оконечного оборудования данных (ООД), в непрерывный сигнал, передаваемый по линии связи (**модуляция**), и обратное преобразование непрерывного сигнала в дискретный на приёмном конце (**демодуляция**).



**Модуляция** (modulation) – перенос сигнала в заданную полосу частот путем изменения параметра (амплитуды, частоты, фазы; величины или направления постоянного тока) переносчика сигнала, называемого *несущей*, в соответствии с функцией, отображающей передаваемые данные. Другими словами *модуляция* – это изменение характеристик *несущей* в соответствии с информативным сигналом.

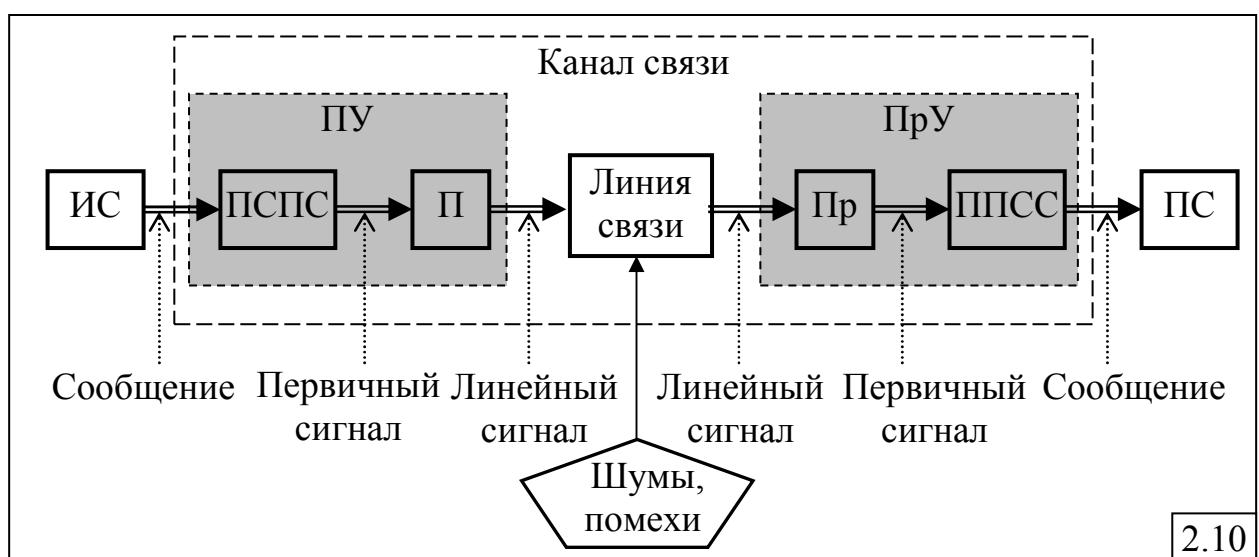
**Несущая** (carrier) – аналоговый высокочастотный сигнал, подвергаемый модуляции в соответствии с некоторым информативным сигналом. Несущая, как правило, имеет *меньшие показатели затухания и искажения*, чем немодулированный информативный сигнал.

## 2.2. Система связи

**Система связи** – совокупность среды передачи (канала связи), оконечного оборудования (терминальное устройство) источника и получателя данных (сообщения), характеризующаяся определенными способами преобразования передаваемого сообщения в сигнал и восстановления сообщения по принятому сигналу.

Система связи в общем случае включает в себя (рис.2.10):

- источник сообщения (ИС);
- передающее устройство (ПУ), включающее в себя:
  - преобразователь сообщения в первичный сигнал (ПСПС), реализующий кодирование;
  - передатчик (П), преобразующий первичный сигнал в линейный сигнал для передачи по линии связи (модуляция);
- приемное устройство (ПрУ), включающее в себя:
  - приемник (Пр), преобразующий линейный сигнал, поступающий из линии связи, в первичный сигнал (демодуляция);
  - преобразователь первичного сигнала в сообщение (ППСС), реализующий декодирование;
- получатель сообщения (ПС).



На линию связи воздействуют внутренние шумы и внешние помехи, искажающие передаваемые сигналы. Способность системы противостоять вредному воздействию помех называется **помехоустойчивостью**.

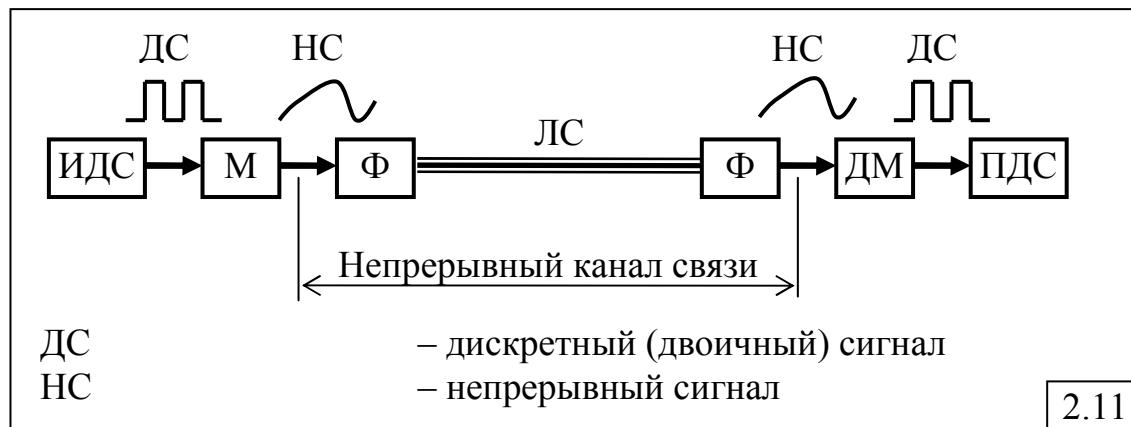
Линия связи может содержать усилители и регенераторы. **Усилитель**, обычно используемый в аналоговых системах связи, просто усиливает сигнал вместе с помехами и передаёт дальше. **Регенератор** («переприёмник»), используемый в цифровых системах связи, восстанавливает сигнал без помех и заново формирует линейный сигнал.

Конкретная структура системы связи зависит от вида передаваемых данных. Для передачи дискретных данных, представленных в двоичном виде, используются *двоичные системы связи* как с непрерывными (аналоговыми), так и с дискретными (цифровыми) каналами связи.

### 2.2.1. Системы связи на основе непрерывного канала

Каноническая схема системы связи на основе *непрерывного (аналогового) канала связи* для передачи двоичных сигналов, представленная на рис.2.11, содержит:

- источник двоичных сигналов (ИДС);
- модулятор (М);
- фильтры (Ф);
- демодулятор (ДМ);
- приёмник двоичных сигналов (ПДС).



**Фильтры** выполняют функции корректирующих устройств, обеспечивая требуемые динамические или частотные свойства передаваемого сигнала:

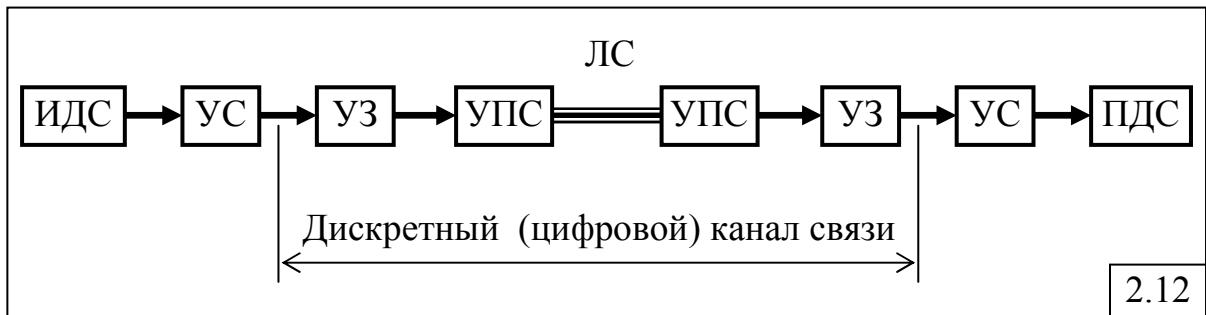
- при передаче – преобразование сигнала, передаваемого в ЛС, таким образом, чтобы он обладал определенными свойствами;
- при приеме – выделение полезного сигнала на фоне помех.

Примером непрерывно канала связи может служить телефонный канал, называемый *каналом тональной частоты* (ТЧ), с полосой пропускания 3100 Гц. Строгое ограничение полосы пропускания канала ТЧ связано с использованием аппаратуры уплотнения и коммутации каналов в телефонных сетях и реализуется с помощью фильтров, отсекающих частоты менее  $f_h=300$  Гц и более  $f_b=3400$  Гц.

## 2.2.2. Системы связи на основе дискретного канала

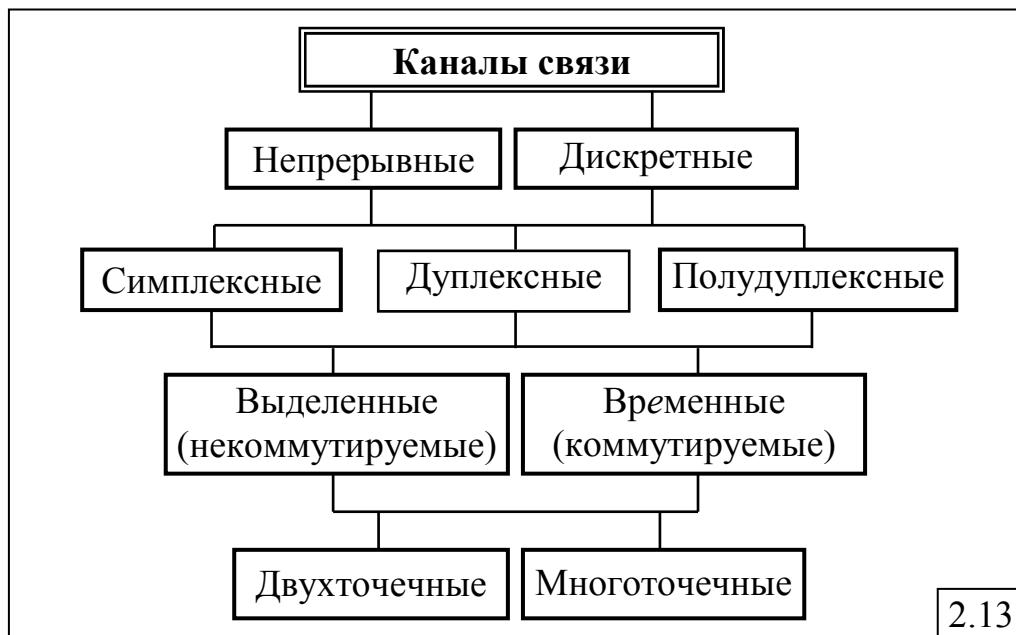
Каноническая схема системы связи на основе *дискретного (цифрового) канала связи*, представленная на рис.2.12, содержит:

- устройство сопряжения с каналом связи (УС);
- устройство защиты от ошибок (УЗО);
- устройство преобразования сигналов (УПС).



## 2.2.3. Классификация каналов связи

Классификация каналов связи представлена на рис.2.13.



В зависимости от типа передаваемых данных каналы связи делятся на **непрерывные**, предназначенные для передачи непрерывных (аналоговых) сигналов, и **дискретные**, предназначенные для передачи дискретных (цифровых) сигналов.

В зависимости от направления передачи данных различают каналы связи:

- **симплексные**, в которых данные передаются только в *одном направлении*;
- **дуплексные**, представляющие собой два симплексных канала, в которых данные могут передаваться в *один и тот же момент времени* в двух направлениях – прямом и обратном;

- **полудуплексные**, в которых данные могут передаваться *поочерёдно* в прямом и обратном направлении.

Каналы связи могут быть всегда доступны для передачи данных за счёт постоянно существующего соединения между абонентами. Такие каналы называются **выделенными** или **некоммутуемыми**. Альтернативой им являются **коммутуемые** или **временные** каналы связи, передача данных по которым возможна только после установления соединения между абонентами, причём канал существует только в течение времени передачи данных (сессии связи).

**Двухточечный** канал связи строится по принципу «точка-точка», то есть связывает только двух абонентов. **Многоточечный** канал связи строится по принципу «точка-многоточка» и обеспечивает передачу данных от одного абонента к нескольким абонентам, например так, как это происходит при конференцсвязи.

#### 2.2.4. Характеристики каналов связи

В качестве основных *характеристик каналов связи* используются следующие величины.

1. **Скорость модуляции** [бод] – число интервалов модуляции передаваемого сигнала в секунду (число переключений, сделанных за секунду); величина, обратная единичному интервалу:  $B = 1/T$ .

2. **Пропускная способность канала связи** [бит/с или bps – bits per second] – предельная скорость передачи данных – количество данных, которое может быть передано по каналу связи за единицу времени.

Предельная пропускная способность **непрерывного (аналогового) КС** зависит от *полосы пропускания*  $F = f_{\text{в}} - f_{\text{н}}$  и *SNR* (*Signal-to-Noise Ratio*) – отношения мощности сигнала  $P_c$  к мощности шума (помех)  $P_{\text{ш}}$  и может быть рассчитана по формуле Шеннона:

$$C = F \log_2 \left( 1 + \frac{P_c}{P_{\text{ш}}} \right).$$

Как следует из формулы Шеннона, пропускная способность канала связи может быть повышена за счёт увеличения полосы пропускания  $F$  или увеличения отношения сигнал/шум, причём более эффективным является первый способ, поскольку логарифмическая зависимость пропускной способности  $C$  от отношения  $P_c/P_{\text{ш}}$  делает второй способ менее эффективным и более трудоёмким.

При передаче данных по телефонному каналу с полосой пропускания  $F=3,1$  кГц ( $f_{\text{н}}=0,3$  кГц;  $f_{\text{в}}=3,4$  кГц) с использованием *модемов* основной способ повышения пропускной способности состоит в увеличении отношения сигнал/шум. С учётом того, что максимальное значение SNR в аналоговом телефонном канале составляет примерно 3000, получим предельную пропускную способность  $C$  около 34 кбит/с, что согласуется со стандартным значением 33600 бит/с. Более высокие скорости передачи могут быть обеспечены только при условии передачи данных по

цифровым телефонным линиям связи, причём на пути передачи должны находиться только цифровые телефонные станции.

Пропускная способность **дискретного КС**, построенного на основе непрерывного канала, *без учета шума на линии* может быть вычислена по формуле Найквиста:

$$C = \frac{1}{T} \log_2 n_c = 2F \log_2 n_c = B \log_2 n_c,$$

где  $T = \frac{1}{2F}$  – длительность единичного интервала;  $n_c$  – число значащих позиций в коде (количество различимых состояний информационного параметра).

Реальная **скорость передачи** по каналу связи, измеряемая как количество данных, передаваемое за единицу времени (бит/с), обычно меньше пропускной способности и зависит от параметров каналообразующей аппаратуры и способа организации передачи данных.

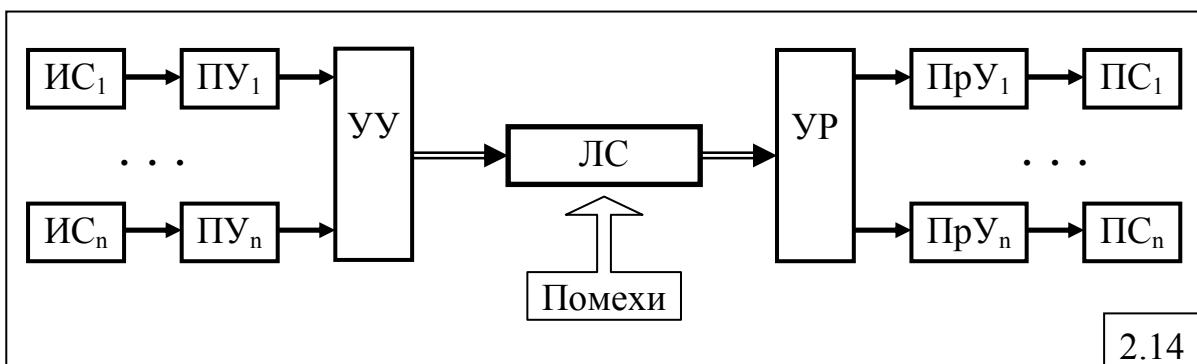
**3. Достоверность передачи данных** – вероятность искажения бита из-за воздействия помех и наличия шумов в канале связи (обычно для КС без дополнительных средств защиты составляет от  $10^{-4}$  до  $10^{-6}$ ); иногда используется единица измерения BER (Bit Error Rate) – *интенсивность битовых ошибок*.

### 2.2.5. Многоканальные системы связи

Системы связи, в которых по одной линии связи осуществляется одновременная независимая передача сигналов между несколькими парами абонентов, называются **многоканальными**.

Использование общей линии для осуществления многоканальной связи называется **уплотнением** линии, а соответствующие технические средства – *аппаратурой уплотнения*.

Схема многоканальной системы связи приведена на рис.2.14 где основными устройствами являются: устройство уплотнения (УУ), объединяющее в единый поток поступающие от передающих устройств (ПУ) сообщения, формируемые источниками сообщений (ИС), и устройство разделения (УР), выделяющее из единого потока данных сообщения, поступающие в приемные устройства (ПрУ) и предназначенные соответствующим получателям сообщений (ПС).



2.14

Традиционные методы уплотнения (мультиплексирования, разделения) каналов:

1) **частотный** – предоставление каждой паре взаимодействующих абонентов в разных частотных диапазонах определенной полосы пропускания, достаточной для передачи данных;

2) **временной** – поочередное подключение в разных временных интервалах взаимодействующих абонентов к общей линии связи.

Таким образом, в одной ЛС может быть организовано несколько КС. В этом случае ЛС можно рассматривать как совокупность технических средств для передачи сигналов, а КС – как долю ресурсов ЛС с соответствующей каналообразующей аппаратурой (аппаратурой уплотнения), предоставляемых одной паре взаимодействующих абонентов для передачи данных.

## 2.2.6. Методы мультиплексирования

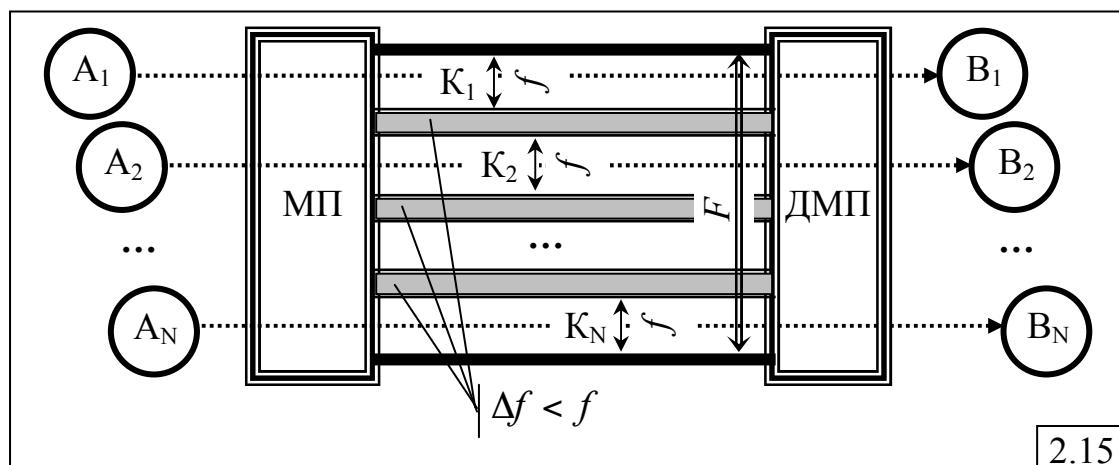
**Мультиплексирование** - технология разделения среды передачи данных между несколькими парами пользователей. В результате мультиплексирования в одном физическом канале создается группа логических каналов.

В компьютерных сетях используются следующие методы мультиплексирования:

- частотное мультиплексирование;
- временное мультиплексирование;
- волновое мультиплексирование.

### 2.2.6.1. Частотное мультиплексирование

**Частотное мультиплексирование** (Frequency Division Multiplexing – FDM) состоит в формировании в пределах полосы пропускания  $F$  физического канала (линии связи) нескольких логических каналов  $K_1, K_2, \dots, K_N$ , связывающих соответственно пользователей  $A_1-B_1, A_2-B_2, \dots, A_N-B_N$ . Каждый такой логический канал занимает полосу  $f << F$  (рис.2.15).



2.15

Для исключения влияния друг на друга сигналов, передаваемых по соседним логическим каналам, между ними формируется частотный промежуток  $\Delta f < f$ , служащий границей между каналами.

Примерами частотного мультиплексирования могут служить радиовещание и сотовая связь.

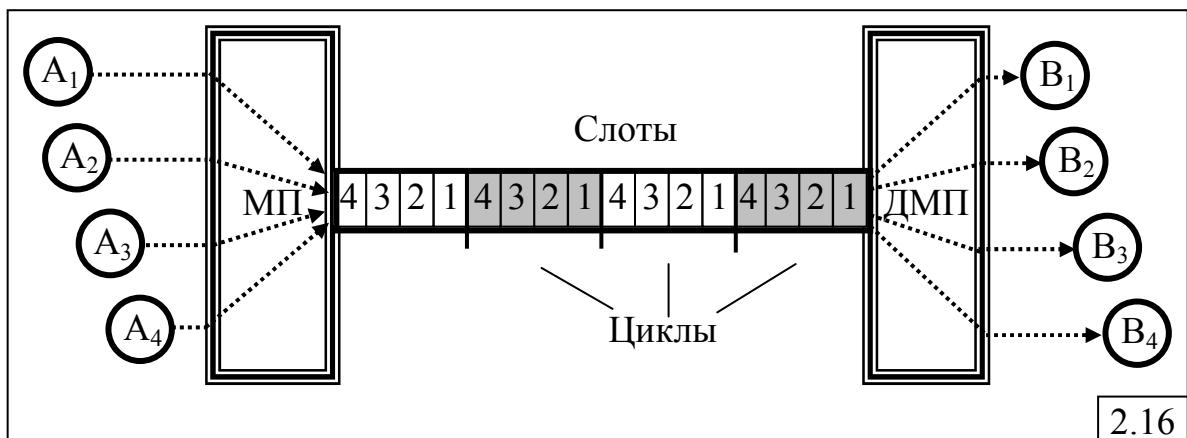
#### 2.2.6.2. Временное мультиплексирование

**Временное мультиплексирование** (Time Division Multiplexing – TDM) заключается в поочерёдном предоставлении взаимодействующим пользователям на небольшой промежуток времени, называемый **временным слотом**, всей пропускной способности канала.

В качестве такого временного слота может служить интервал времени, необходимый для передачи одного байта, кадра или пакета.

Временное мультиплексирование появилось и разрабатывалось для цифровых сетей связи.

На рис.2.16 иллюстрируется временное мультиплексирование, обеспечивающее параллельную передачу данных между четырьмя парами пользователей:  $A_1-B_1$ ,  $A_2-B_2$ ,  $A_3-B_3$ ,  $A_4-B_4$ . Для передачи одного байта каждой паре пользователей в строго определённой последовательности предоставляется временной слот: слот 1 для передачи байта от  $A_1$  к  $B_1$ , слот 2 – от  $A_2$  к  $B_2$ , слот 3 – от  $A_3$  к  $B_3$ , слот 4 – от  $A_4$  к  $B_4$ . Четыре таких слота, содержащие по одному байту для каждой пары пользователей, образуют **цикл**. Циклы последовательно повторяются до тех пор, пока не закончится передача данных. Если в цикле отсутствуют данные для передачи от пользователя  $A_i$ , то соответствующий слот  $i$  остаётся пустым и не может быть занят другим пользователем. Это необходимо для того, чтобы на приёмной стороне демультиплексор (ДМП) мог корректно разделять поступающий поток байтов по номеру слота и направлять каждый байт именно тому пользователю, которому он предназначен. Рассмотренный метод временного мультиплексирования называется **статическим** или **синхронным**, поскольку каждый байт от пользователей  $A_1$ ,  $A_2$ ,  $A_3$ ,  $A_4$  занимает строго определённый слот в каждом цикле.



Очевидно, что недостатком синхронного мультиплексирования является снижение реальной пропускной способности канала связи в тех

случаях, когда в пределах цикла не все временные слоты заняты, причём чем больше слотов не занято, тем ниже реальная пропускная способность канала.

Альтернативой синхронному временному мультиплексированию служит **статистическое** или **асинхронное** мультиплексирование, отличающееся тем, что слоты не привязаны строго к конкретной паре пользователей. Это означает, что при отсутствии данных для передачи у какого-то пользователя, очередной слот не остаётся пустым, а предоставляется другому пользователю. Таким образом, за счёт сокращения простоев реальная пропускная способность канала связи оказывается выше, чем при синхронном мультиплексировании.

Для того чтобы на приёмной стороне ДМП мог направить поступившие в очередном слоте данные именно тому пользователю, которому они предназначены, необходимо, чтобы эти данные имели некоторый идентификатор (например, адрес), определяющий конкретного пользователя-получателя. Это означает, что такой метод временного мультиплексирования, используемый например в АТМ-сетях, предполагает в качестве содержимого слота не байт, а некоторый блок данных, называемый в АТМ-сетях **ячейкой** и содержащий идентификаторы отправителя и получателя.

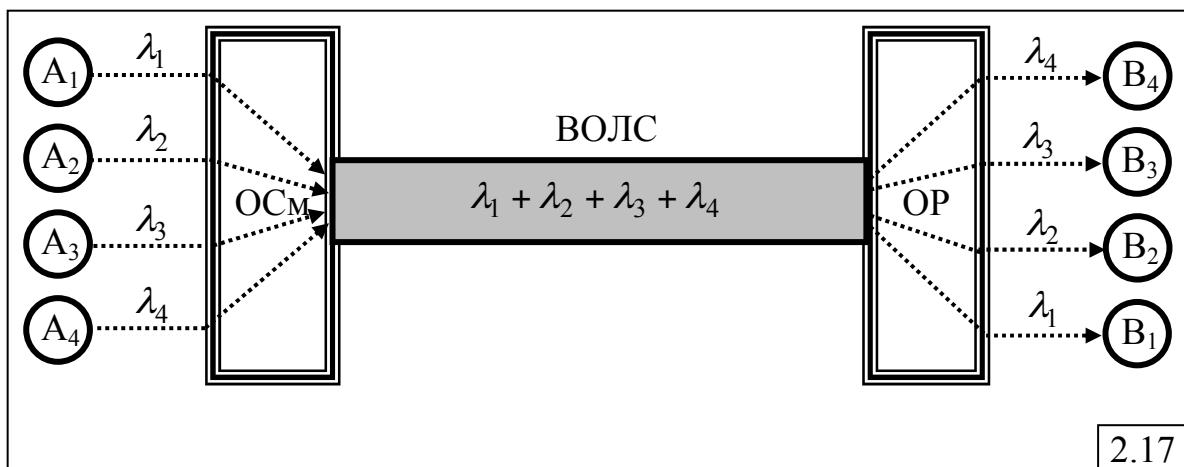
#### **2.2.6.3. Волновое мультиплексирование**

**Волновое мультиплексирование** (Wavelength Division Multiplexing – WDM), называемое также **спектральным уплотнением**, используется в волоконно-оптических линиях связи. По своей сути, волновое мультиплексирование представляет собой частотное уплотнение на очень высоких частотах (сотни ТГц).

На рис.2.17 показана передача данных по волоконно-оптической линии связи (ВОЛС) от четырёх пользователей  $A_1, A_2, A_3, A_4$  к пользователям  $B_1, B_2, B_3, B_4$  соответственно. Для одновременной передачи по одной и той же линии связи используются разные длины волн:  $\lambda_1, \lambda_2, \lambda_3, \lambda_4$  или, что то же самое, разные частоты светового диапазона. На передающей стороне оптические лучи объединяются с помощью оптического сумматора (ОСм) в единый световой поток  $\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4$ . На приёмной стороне оптический разделитель (ОР) выделяет оптические сигналы по известной длине волны и направляет их соответствующим пользователям.

Технология WDM появилась в начале 90-х годов прошлого века. Первые реализации позволяли передавать одновременно данные по 8 спектральным каналам со скоростью 2,5 Гбит/с по каждому каналу. Затем появились реализации, содержащие 16, 32, 40 и более спектральных каналов со скоростями 10 Гбит/с по каждому каналу. Увеличение числа логических каналов привело к появлению оптических магистралей нового поколения, построенных по технологии **уплотнённого волнового**

**мультиплексирования** – DWDM (Dense WDM), отличающегося от WDM значительно меньшим расстоянием между длинами волн.



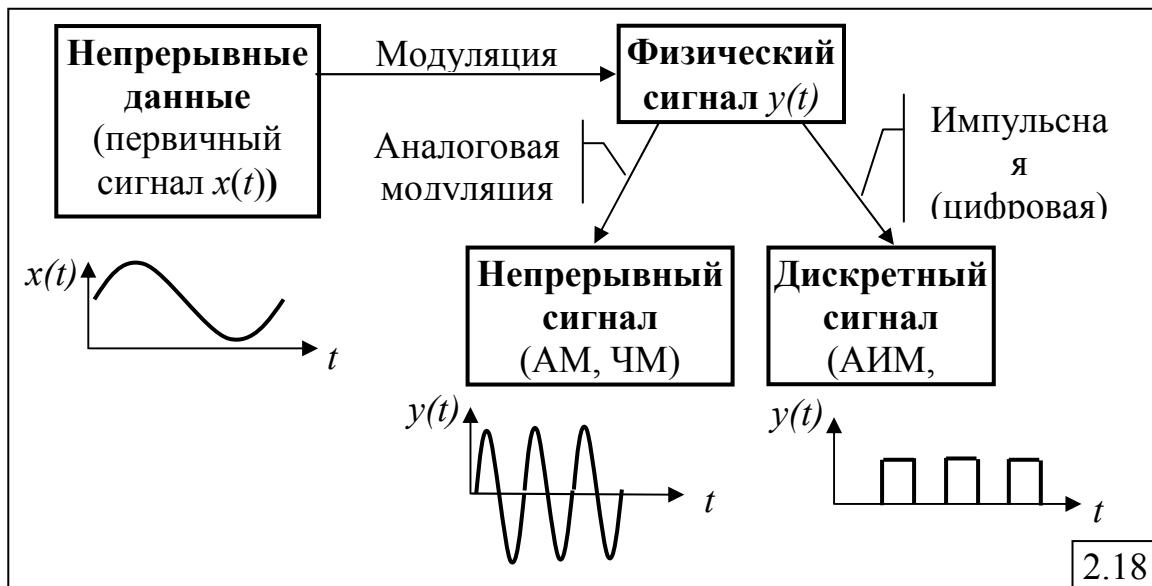
### 2.3. Методы модуляции и кодирования данных

Передача данных осуществляется в виде физических сигналов различной природы (электрические, оптические, радиоволны) в зависимости от среды передачи. Для обеспечения качественной передачи используются различные способы преобразования данных, представляемых в виде непрерывных или дискретных *первичных* сигналов, в *линейные* физические сигналы (непрерывные или дискретные), передаваемые по линии связи.

Процесс преобразования *непрерывных сигналов* и их представление в виде физических сигналов для качественной передачи по каналам связи называется **модуляцией**.

Модуляция может осуществляться (рис.2.18):

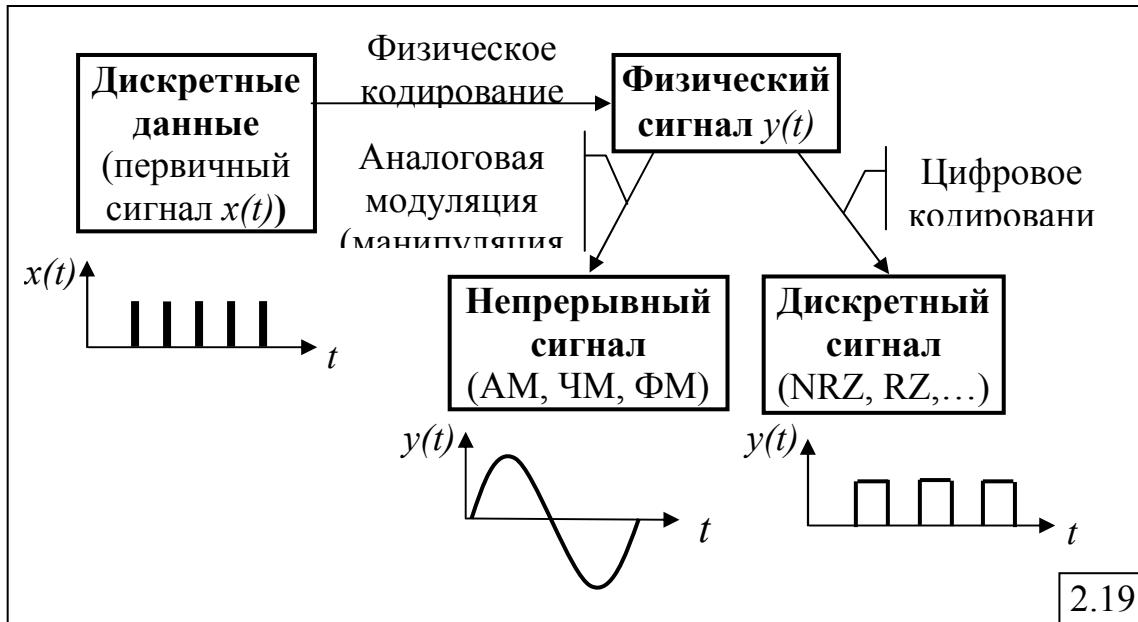
- на основе *непрерывного* (аналогового) высокочастотного синусоидального сигнала, называемого *несущей* (**аналоговая модуляция**);
- на основе *дискретного* (цифрового) сигнала в виде импульсов (**импульсная** или **цифровая** модуляция).



Процесс преобразования дискретных данных, представляемых дискретными *первичными* сигналами, в физические *линейные* сигналы (непрерывные или дискретные), передаваемые по каналу (линии) связи, называется **физическими кодированием**.

Основные типы физического кодирования (рис.2.19):

- на основе *непрерывного* (аналогового) синусоидального несущего сигнала (**манипуляция**);
- на основе последовательности прямоугольных импульсов (**цифровое кодирование**).



2.19

### 2.3.1. Методы модуляции непрерывных данных

#### 2.3.1.1. Аналоговая модуляция

**Аналоговая модуляция** – преобразование непрерывного низкочастотного сигнала  $x(t)$  (рис.2.20,а) в непрерывный высокочастотный сигнал  $y(t)$ , называемый *несущей* и обладающей более высокими характеристиками в отношении дальности передачи и затухания. Аналоговая модуляция может быть реализована двумя способами:

1) **амплитудная модуляция**, при которой амплитуда высокочастотного сигнала  $y(t)$  изменяется в соответствии с исходной функцией  $x(t)$  так, как это показано на рис.2.20,б: огибающая амплитуды несущей повторяет форму исходной функции  $x(t)$ ;

2) **частотная модуляция** (рис.2.20,в), при которой в соответствии с исходной функцией  $x(t)$  изменяется частота несущей – чем больше значение  $x(t)$ , тем больше частота несущей  $y(t)$ .

Аналоговая модуляция используется в радиовещании при работе множества радиостанций в одной общей среде передачи (радиоэфире): **амплитудная модуляция** для работы радиостанций в АМ-диапазоне

(Amplitude Modulation) и частотная модуляция для работы радиостанций в FM-диапазоне (Frequency Modulation).

### 2.3.1.2. Импульсная модуляция

Использование цифровых каналов связи для передачи телефонных данных (речевого сигнала) в начале 60-х годов прошлого века потребовало разработки методов преобразования непрерывных сигналов в дискретные, таких как:

- 1) амплитудно-импульсная модуляция;
- 2) импульсно-кодовая модуляция.

#### Амплитудно-импульсная модуляция

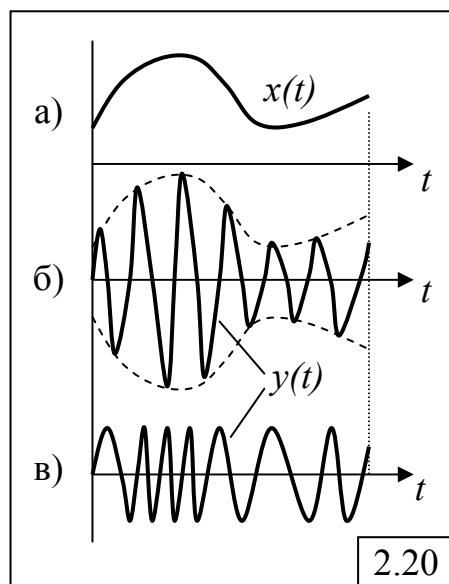
**(АИМ)** (Pulse Amplitude Modulation – PAM) заключается в преобразовании непрерывного сигнала в совокупность дискретных сигналов (*импульсов*) с определенной *амплитудой*. Для этого исходная непрерывная функция  $x(t)$  подвергается дискретизации (квантуется) по времени так, как это показано на рис.2.21,а. Частота дискретизации по времени определяется в соответствии с *теоремой Котельникова*, которая гласит, что для восстановления без потерь непрерывного сигнала, представленного в дискретном виде, частота дискретизации  $F_d$  должна удовлетворять условию:  $F_d > 2f_b$ , где  $f_b$  – верхняя частота передаваемого сигнала  $x(t)$ . В полученные таким образом дискретные моменты времени передаются импульсы  $y(t)$ , амплитуда которых *пропорциональна* значениям функции  $x(t)$  в эти же моменты времени (рис.2.21,б).

Существенным недостатком АИМ при передаче оцифрованных данных по каналу связи является сложность корректного восстановления функции  $x(t)$  на приёмном конце, что обусловлено непропорциональным изменением (затуханием) амплитуд разных импульсов  $y(t)$  в процессе передачи по каналу связи. В связи с этим, более широкое распространение получил другой метод передачи непрерывных данных в дискретном виде – импульсно-кодовая модуляция.

**Импульсно-кодовая модуляция (ИКМ)** (Pulse Code Modulation – PCM) – метод модуляции, при котором аналоговый сигнал кодируется сериями импульсов, представляющими собой *цифровые коды* амплитуд в точках отсчета аналогового сигнала.

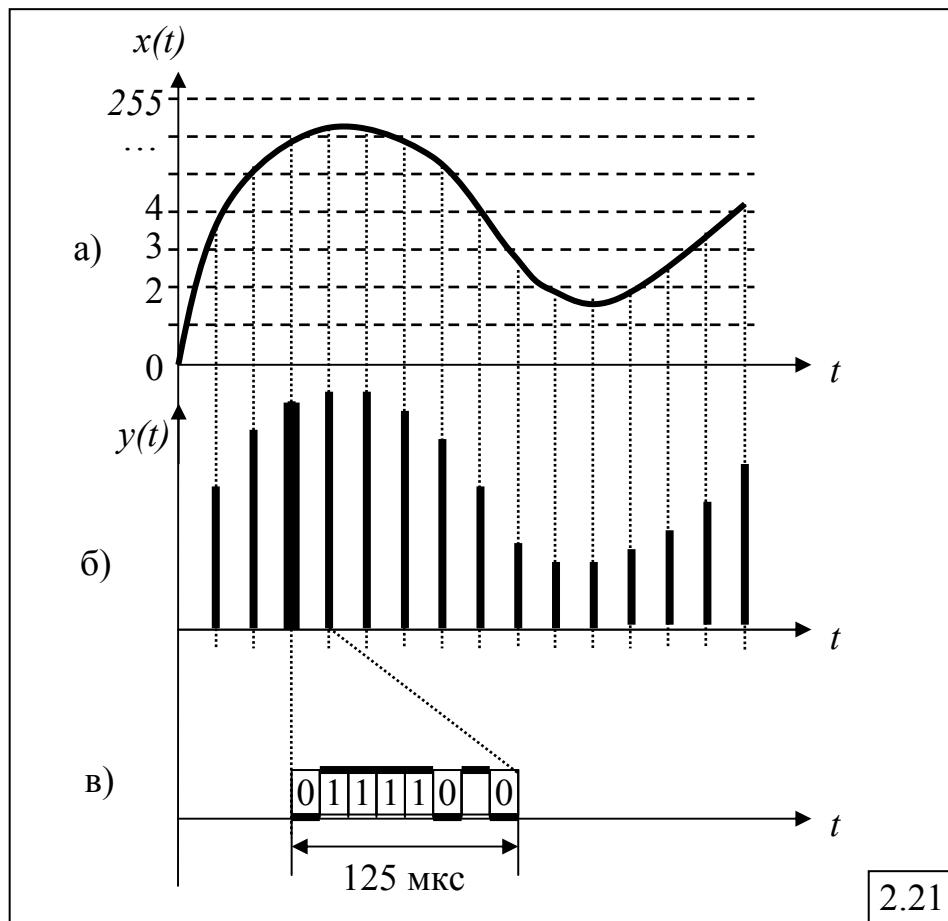
Для этого исходный сигнал подвергается дискретизации (квантуется) по двум координатам:

- по оси абсцисс – дискретизация по времени;
  - по оси ординат – дискретизация по уровню.
- Дискретизация по времени, как и в случае АИМ, выполняется в соответствии с теоремой Котельникова. Поскольку ИКМ первоначально разрабатывалась для передачи телефонных данных (голоса) по



2.20

телефонным каналам, имеющим резко ограниченную полосу пропускания в интервале от 300 Гц до 3400 Гц, то в соответствии с теоремой Котельникова частота дискретизации должна быть больше, чем 6800 Гц. Стандартом была рекомендована частота дискретизации 8000 Гц. Таким образом, амплитуда аналогового сигнала измеряется 8000 раз в секунду, то есть каждые 125 мкс.



Кроме того, было установлено, что для качественного восстановления аналогового сигнала (голоса) достаточно иметь 256 уровней дискретизации (рис.2.21,а), что позволяет передавать в каждый момент времени значение амплитуды (номер уровня) сигнала с помощью 8-разрядного цифрового кода (8 битов), как это показано на рис.2.21,в.

Таким образом, *результатирующий дискретный поток данных передается со скоростью*  $8000 \text{ [раз в секунду]} * 8 \text{ [бит]} = 64\,000 \text{ бит/с}$ , то есть *для передачи оцифрованного голоса требуется канал связи с пропускной способностью 64 кбит/с.*

Для уменьшения требуемой для передачи оцифрованного голоса пропускной способности канала связи применяется модифицированный метод ИКМ, стандартизованный комитетом ITU-T (стандарт G.726) – **адаптивная дифференциальная импульсно-кодовая модуляция** (АДИКМ, Adaptive Differential Pulse Code Modulation – ADPCM).

Термин «дифференциальная (разностная)» означает, что по каналу связи передаётся не значение амплитуды, а *разность* между текущим

значением непрерывного сигнала в точке квантования и предыдущим. Поскольку скорость изменения исходного аналогового сигнала меньше частоты квантования, то вероятность большого различия между соседними амплитудами чрезвычайно мала, и для кодирования этой разности достаточно 4-х бит, позволяющих закодировать эту разность в интервале от 0 до 15. Тогда при условии, что частота квантования по времени составляет 8000 раз в секунду, получим скорость передачи  $8000 \times 4 = 32$  кбит/с, что вдвое меньше стандартной скорости ИКМ.

Более сложным вариантом дифференциальной импульсно-кодовой модуляции является *кодирование с предсказанием*, при котором кодируется и передаётся разница между реальным и предсказанным на основе нескольких предыдущих отсчётов значением сигнала. Это позволяет ещё больше уменьшить количество битов для кодирования одного замера сигнала и, следовательно, уменьшить требование к пропускной способности канала связи. Стандарт G.726 допускает использование 5-и, 3-х и 2-х битов для кодирования одного замера сигнала, что позволяет получить скорости передачи (**битрейты**) 40, 24 и 16 кбит/с.

Адаптивность модуляции заключается в динамической подстройке шага квантования разницы по предыдущим значениям.

### 2.3.2. Методы модуляции дискретных данных

Процесс представления дискретных (цифровых) данных в виде непрерывного высокочастотного синусоидального сигнала (несущей) по своей сути является аналоговой модуляцией дискретных данных. Однако, для того чтобы его отличать от аналоговой модуляции непрерывных данных, такое преобразование часто называют **манипуляцией**.

Манипуляция применяется для передачи дискретных данных (сигналов) в виде непрерывных сигналов по каналам с узкой полосой частот, например по телефонным каналам, имеющим ограниченную полосу пропускания в 3100 Гц, и реализуется с помощью модемов.

Компьютерные данные – двоичные «1» и «0» – обычно изображаются в виде потенциалов соответственно высокого и низкого уровней (рис.2.22,*a*). Такой метод представления двоичных данных является наиболее естественным и простым и называется **потенциальным кодированием**.

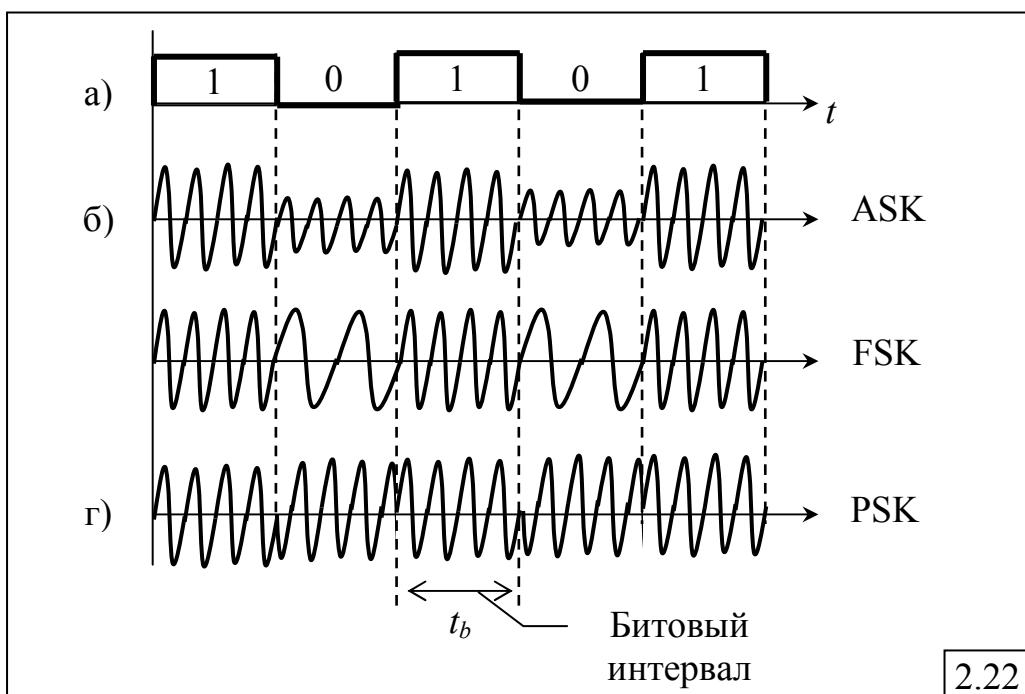
Время, затрачиваемое на передачу одного бита («1» или «0»), называется **битовым интервалом**. Длительность  $t_b$  битового интервала связана с пропускной способностью канала связи  $C$  (скоростью передачи) зависимостью:  $t_b = 1/C$ .

При потенциальном кодировании *скорость модуляции B* численно совпадает с *пропускной способностью канала*:  $B$  [бод] =  $C$  [бит/с].

Например, для канала связи с пропускной способностью =10 Мбит/с длительность битового интервала = 100 нс, а скорость модуляции =10 Мбод.

Для передачи двоичных данных могут использоваться следующие методы манипуляции:

- **амплитудная манипуляция** (Amplitude Shift Keying, ASK): для представления «1» и «0» используются разные уровни амплитуды высокочастотной несущей (рис.2.22,б); из-за низкой помехоустойчивости этот метод обычно применяется в сочетании с другими методами, например с фазовой манипуляцией;
- **частотная манипуляция** (Frequency Shift Keying, FSK): значения «0» и «1» передаются синусоидами с различной частотой (рис.2.22,в); этот метод прост в реализации и обычно применяется в низкоскоростных модемах;
- **фазовая манипуляция** (Phase Shift Keying, PSK): значениям «0» и «1» соответствуют синусоиды одинаковой частоты и с одинаковой амплитудой, но с различной фазой, например 0 и 180 градусов (рис.2.22,г).



На практике обычно используются комбинированные методы модуляции, обеспечивающие более высокие скорости передачи и лучшую помехозащищённость. Например, метод *квадратурной амплитудной модуляции* (*Quadrature Amplitude Modulation, QAM*) основан на сочетании фазовой модуляции с 8 значениями величин сдвига фазы и амплитудной модуляции с 4 уровнями амплитуды. Распознавание ошибок при передаче осуществляется за счёт избыточности кодирования, заключающейся в использовании не всех 32-х возможных комбинаций сигнала.

### 2.3.3. Цифровое кодирование

При цифровом кодировании дискретных данных применяются потенциальные и импульсные коды. В потенциальных кодах для представления двоичных единиц и нулей используется разные значения

потенциала сигнала, а в импульсных кодах – импульсы разной полярности или же перепады потенциала в разном направлении.

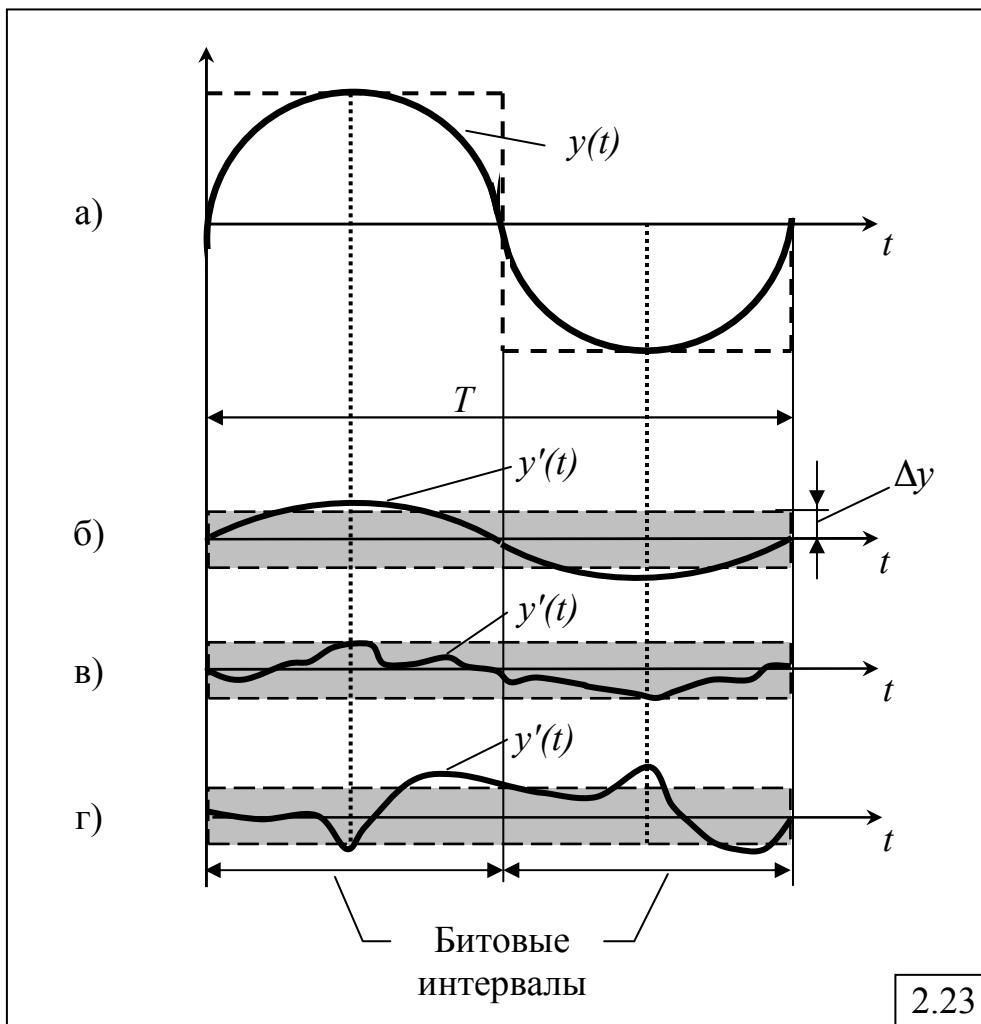
### **2.3.3.1. Особенности передачи цифровых сигналов**

Для того чтобы разобраться в проблемах, возникающих при передаче цифровых данных на большие расстояния, рассмотрим, каким изменениям подвержен сигнал в процессе передачи по каналу связи.

В простейшем случае двоичные данные могут быть представлены в виде синусоидального сигнала, в котором положительная часть синусоиды соответствует двоичной «1», а отрицательная – «0» (рис.2.23,а). Частота такого сигнала определяется величиной битового интервала  $t_b$ :  $f_0 = \frac{1}{2t_b}$ , связанного с пропускной способностью канала  $C$  зависимостью  $t_b = 1/C$ , откуда:  $f_0 = C/2$ .

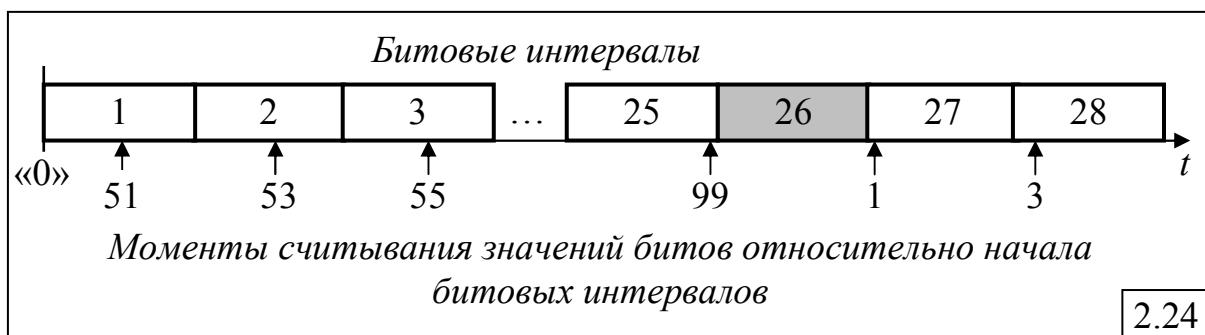
Передача сигнала на большие расстояния связана со следующими особенностями.

Как известно, сигнал в процессе передачи по каналу связи затухает, его мощность в точке приёма оказывается значительно меньше мощности исходного информативного сигнала (рис.2.23,б). В любом реальном канале связи имеются внутренние шумы, обусловленные техническими характеристиками среды передачи (линии связи) и каналаобразующей аппаратуры. Эти шумы приводят к появлению некоторого фонового сигнала, налагающегося на информативный сигнал. Для того чтобы шум в канале связи не воспринимался на приёмной стороне как информативный сигнал, в приёмнике обычно устанавливается некоторое предельное значение уровня сигнала  $\Delta u$ , которое рассматривается как уровень естественного шума и не воспринимается как информативный сигнал. Если мощность информативного сигнала в точке приёма меньше  $\Delta u$ , то он будет не различим и, следовательно, потерян. Очевидно, что на приёмной стороне наибольшую мощность синусоидальный сигнал сохраняет в центре битового интервала. Следовательно, для того чтобы с уверенностью распознать его значение, желательно снимать отсчёт в центре битового интервала. Для этого в передающем и принимающем узле необходимо иметь высокоточные часы (таймеры), с помощью которых определяются: в передатчике – моменты формирования сигналов, в приёмнике – моменты снятия значения информативного сигнала в центре битового интервала. Очевидно, что для качественного распознавания сигналов на приёмной стороне, необходимо, чтобы часы передатчика и приёмника работали синхронно. Однако известно, что все часы имеют некоторую погрешность, которая с течением времени приводит к различию в показаниях двух разных часов, находящихся в узле-передатчике и узле-приёмнике, причём это различие со временем растёт. Всё это может привести к тому, что на приёмной стороне некоторые биты могут быть не считаны (пропущены), либо значения некоторых битов будут считаны дважды.



Покажем это на следующих примерах.

**Пример 1.** Пусть длительность битового интервала  $t_b = 100$  нс, что соответствует пропускной способности канала связи  $C = 10$  Мбит/с. Положим, что часы приёмника за один битовый интервал *отстают* от часов передатчика на 2 нс. Это означает, что в каждом следующем битовом интервале значение очередного бита будет считано на 2 нс позже по отношению к моменту считывания значения предыдущего интервала, как это показано на рис.2.24.



Здесь предполагается, что в начальный момент времени «0» часы передатчика и приёмника синхронизированы, поэтому считывание значения первого битового интервала произойдёт на 51-й наносекунде,

поскольку за первые 50 нс часы приёмника отстанут только на 1 нс. Моменты считывания значений битов отмечены стрелками, а их значения указаны относительно начала очередного битового интервала. Как видно из рисунка, при отсутствии синхронизации часов передатчика и приёмника не будет считано значение 26-го битового интервала.

**Пример 2.** Положим теперь, что при той же длительности битового интервала в 100 нс часы приёмника за один битовый интервал *опережают* часы передатчика на 2 нс. Это означает, что в каждом следующем битовом интервале значение очередного бита будет считано на 2 нс раньше по отношению к моменту считывания значения предыдущего интервала, как это показано на рис.2.25. После синхронизации часов передатчика и приёмника считывание значения первого битового интервала произойдёт на 49-й наносекунде. Как видно из рисунка, при отсутствии синхронизации приёмник дважды считает значение 25-го битового интервала.



Для того чтобы не возникали такие ситуации, необходимо поддерживать синхронизацию часов передатчика и приёмника. В компьютерах при обмене цифровыми данными между устройствами эта проблема решается путём использования дополнительного специального канала, по которому передаются тактовые импульсы, определяющие моменты времени, в которые должна сниматься информация. Однако такое решение не приемлемо при передаче информации на большие расстояния ввиду высокой стоимости дополнительного «тактового» канала, а также неодинаковой скорости распространения информативного сигнала и тактовых импульсов из-за неоднородности среды передачи. Последнее может привести к тому, что тактовый импульс придет позже или раньше соответствующего сигнала, в результате чего бит данных будет пропущен или считан повторно. Для решения проблемы синхронизации в компьютерных сетях применяются специальные методы кодирования, позволяющие выполнять синхронизацию часов приёмника и передатчика автоматически. Такие коды называются *самосинхронизирующими*.

Заметим, что рассмотренная ситуация в действительности оказывается более сложной, поскольку шумы влияют не только на устанавливаемый уровень чувствительности приёмника, но и искажают форму информативного сигнала. Кроме того, канал связи подвержен влиянию различного рода помех, также искажающих сигнал. Поэтому

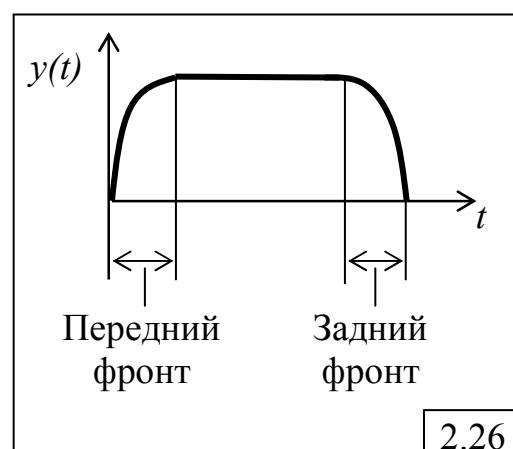
реальный сигнал в точке приёма оказывается мало похожим на исходный синусоидальный сигнал (рис.2.23,в). Это может привести к тому, что даже при абсолютно точной синхронизации передатчика и приёмника значение сигнала либо пропадёт, если его уровень окажется меньше  $\Delta u$  (рис.2.23,в), либо будет считано неверное значение (рис. 2.23,г).

Для того чтобы не возникало таких ситуаций, желательно приблизить форму передаваемого информативного сигнала к исходному прямоугольному виду.

При потенциальном кодировании исходный прямоугольный сигнал, отображающий двоичные «1» и «0», является идеальным теоретическим сигналом, обладающим бесконечным спектром, который получается непосредственно из формул Фурье для периодической функции. Если дискретные данные, содержащие последовательность чередующихся «1» и «0», передаются с битовой скоростью  $C$  бит/с, то спектр состоит из постоянной составляющей нулевой частоты и бесконечного ряда гармоник с частотами  $f_0$ ,  $f_1 = 3f_0$ ,  $f_2 = 5f_0$ , ...,  $f_i = (2i+1)f_0$ , ..., где  $f_0 = C/2$  – частота основной гармоники;  $i = 0, 1, 2, \dots$ . Амплитуды этих гармоник убывают с коэффициентами  $1/3, 1/5, \dots, 1/(2i+1)$ , ... от амплитуды  $A_0$  основной гармоники. Таким образом, спектр потенциального кода требует для качественной передачи большую полосу пропускания – в пределе равную бесконечности.

Действительно, в начале и в конце такого сигнала скорость изменения его значения (верхняя частота) равна бесконечности, а между ними скорость изменения сигнала (нижняя частота) равна нулю. Реальные сигналы обладают ограниченным спектром, обусловленным наличием переднего и заднего фронта потенциального сигнала (рис.2.26), скорость изменения которых конечна и определяется быстродействием элементной базы передатчика, формирующего потенциальный сигнал.

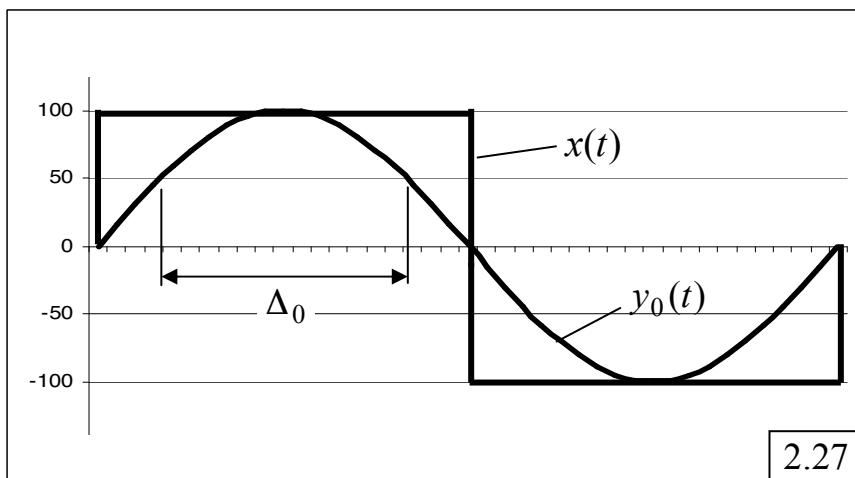
Однако передача такого сигнала с конечным спектром оказывается проблематичной из-за наличия в спектре нулевой составляющей. Дело в том, что линии связи с большой полосой пропускания имеют нижнюю границу частот, значительно отличающуюся от нуля. Следовательно, такой сигнал будет передаваться с большими искажениями, что затруднит его восстановление на приёмном конце. Для того чтобы сузить спектр потенциального сигнала, необходимо увеличить нижнюю границу спектра. Это может быть достигнуто, например, наложением высокочастотной составляющей на постоянную составляющую сигнала, заключённую между передним и задним фронтами потенциального сигнала.



2.26

Для того чтобы представить, как это можно реализовать, рассмотрим, как изменяется синусоидальный сигнал при добавлении высокочастотных гармоник, приближающих форму передаваемого сигнала к прямоугольной. На рис.2.27-2.30 показаны 4 вида сигналов, которые могут использоваться для передачи потенциального кода, различающиеся количеством гармоник.

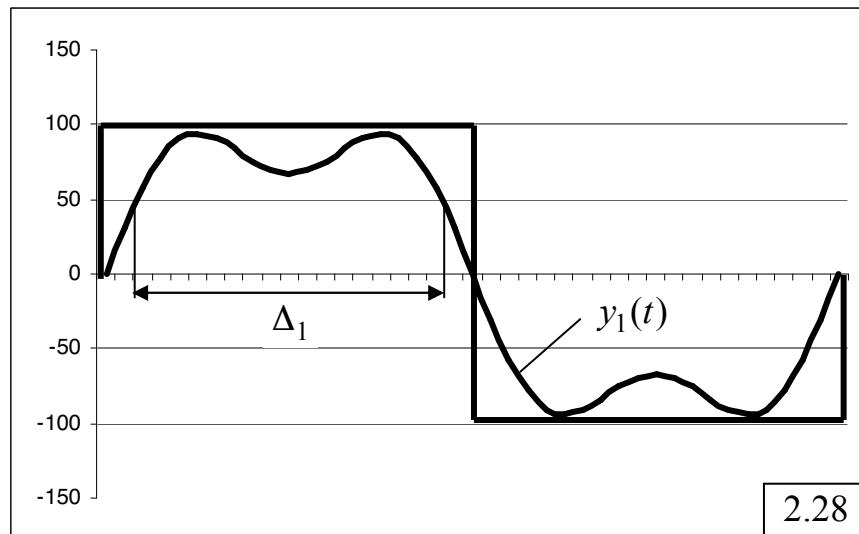
На рис.2.27 показан сигнал, содержащий одну гармонику, которая называется **основной гармоникой**.



Основная гармоника  $y_0(t)$  имеет частоту  $f_0 = \frac{1}{2t_b}$ , где  $t_b$  — длительность битового интервала, и амплитуду  $A_0 = 100$ , равную уровню потенциала исходного потенциального кода  $x(t)$ :  $y_0(t) = A_0 \sin(2\pi f_0 t)$ . Здесь же показан интервал  $\Delta_0$ , в котором значения сигнала  $y_0(t) \geq 50$ . Интервал  $\Delta_0$  можно рассматривать как область битового интервала, в пределах которого с высокой вероятностью гарантируется правильное распознавание значения передаваемого бита.

На рис.2.28 показан сигнал, содержащий две гармоники:  $y_1(t) = A_0 \sin(2\pi f_0 t) + A_1 \sin(2\pi f_1 t)$ , где  $A_1 = \frac{A_0}{3}$  и  $f_1 = 3f_0$ . Кроме основной гармоники сигнал  $y_1(t)$  содержит ещё одну синусоиду, частота которой в 3 раза больше, а амплитуда — в 3 раза меньше, чем у основной гармоники.

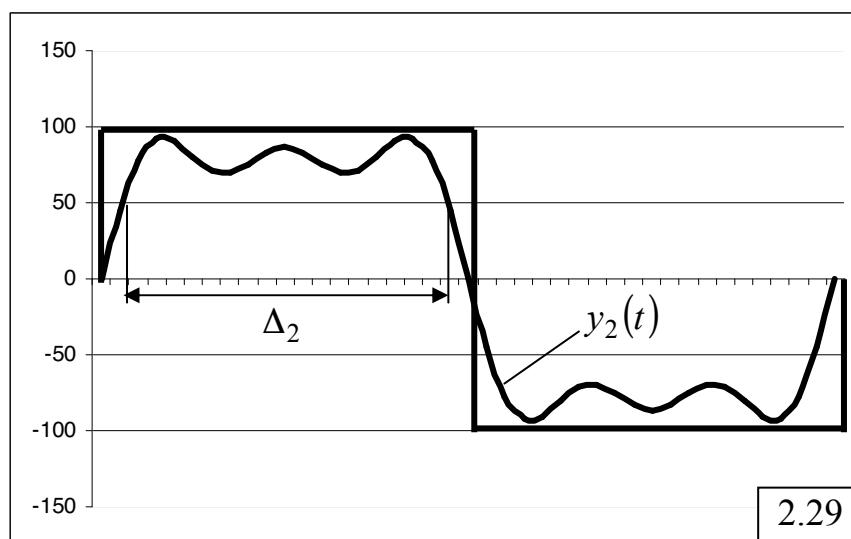
Отметим, что интервал  $\Delta_1$ , в котором значения сигнала  $y_1(t) \geq 50$ , больше, чем  $\Delta_0$ . Благодаря этому увеличивается вероятность правильного распознавания значения переданного бита на приёмном конце и уменьшается требование к точности синхронизации часов передатчика и приёмника. Заметим, что это достигается за счёт трёхкратного увеличения спектра сигнала и, как следствие, увеличения требуемой полосы пропускания канала связи.



2.28

На рис.2.29 показан сигнал, содержащий три гармоники:  $y_2(t) = A_0 \sin(2\pi f_0) + A_1 \sin(2\pi f_1) + A_2 \sin(2\pi f_2)$ , где  $A_2 = \frac{A_0}{5}$  и  $f_2 = 5f_0$ .

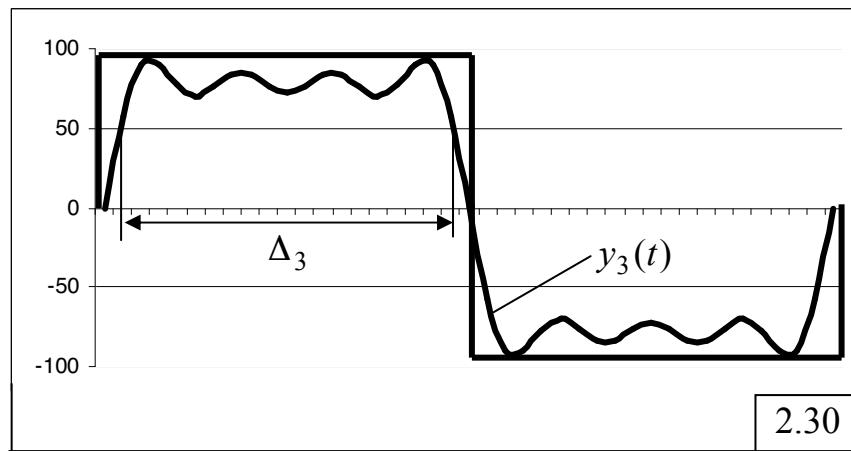
Таким образом, сигнал  $y_2(t)$  содержит ещё одну синусоиду, частота которой в 5 раз больше, а амплитуда – в 5 раз меньше, чем у основной гармоники, а интервал  $\Delta_2$ , в котором значения сигнала  $y_2(t) \geq 50$ , больше, чем интервал  $\Delta_1$ .



2.29

И, наконец, на рис.2.30 показан сигнал, содержащий 4 гармоники:  $y_3(t) = A_0 \sin(2\pi f_0) + A_1 \sin(2\pi f_1) + A_2 \sin(2\pi f_2) + A_3 \sin(2\pi f_3)$ , где  $A_3 = \frac{A_0}{7}$  и  $f_3 = 7f_0$ .

Частота четвёртой гармоники в 7 раз больше, а амплитуда – в 7 раз меньше, чем у основной гармоники. Интервал  $\Delta_3$ , в котором значения сигнала  $y_3(t) \geq 50$ , больше интервала  $\Delta_2$ .



2.30

Следует помнить, что спектр сигнала меняется в зависимости от передаваемых данных. Например, передача длинной последовательности нулей или единиц сдвигает спектр сигнала потенциального кода в сторону низких частот и приводит к появлению в сигнале так называемой **постоянной составляющей**. В предельном случае, когда передаваемые данные состоят только из единиц (или только из нулей), частота передаваемого сигнала будет равна нулю. При передаче чередующихся единиц и нулей постоянная составляющая отсутствует. Поэтому спектр результирующего сигнала потенциального кода при передаче произвольных данных занимает полосу от некоторой величины, близкой к 0 Гц, до, в пределе, бесконечности. Однако на практике верхний предел спектра обычно ограничивается значениями  $3f_0$ ,  $5f_0$  или  $7f_0$ . Гармониками с частотами выше  $7f_0$  можно пренебречь из-за их малого вклада в результирующий сигнал – амплитуда этих гармоник составляет 11% и менее от амплитуды основной гармоники.

Требование отсутствия постоянной составляющей, то есть наличия постоянного тока между передатчиком и приемником, связано также с применением трансформаторных схем гальванической развязки, которые не пропускают постоянный ток. Необходимость гальванической развязки в электрических линиях связи обусловлена требованием защиты компьютеров сети от непредвиденных ситуаций. В частности, короткое замыкание в одном из компьютеров сети не должно приводить к выходу из строя всех остальных компьютеров, объединённых единой электрической средой передачи данных.

Рассмотренные особенности передачи цифровых сигналов позволяют сделать следующий вывод.

При цифровой передаче данных для восстановления исходного сигнала требуется меньше гармоник, чем при аналоговой передаче. Технология передачи и приема цифровых сигналов позволяет восстановить исходный сигнал по основной гармонике (несущей), однако для уменьшения числа ошибок необходимо присутствие хотя бы первой гармоники, что, правда, втрое увеличивает спектр передаваемого сигнала и, следовательно, требуемой полосы пропускания канала связи.

### 2.3.3.2. Требования к методам цифрового кодирования

Методы цифрового кодирования оказывают существенное влияние на качество передачи дискретных данных (надёжность и достоверность доставки сообщений, возможность обнаружения и исправления ошибок, стоимость реализации) и в значительной мере определяют требуемую пропускную способность среды передачи.

В связи с этим, к методам цифрового кодирования предъявляются следующие **требования** (рис.2.31):

- минимизация спектра результирующего сигнала при одной и той же битовой скорости;
- поддержка синхронизации между передатчиком и приёмником сигналов за счёт наличия свойства самосинхронизации;
- отсутствие постоянной составляющей;
- возможность обнаружения ошибок и их исправления;
- низкая стоимость реализации метода кодирования.



**Минимизация спектра результирующего сигнала** позволяет при одной и той же полосе пропускания канала связи передавать больший объем данных за единицу времени, например, за счёт частотного мультиплексирования и организации нескольких логических каналов в одной и той же линии связи, что обеспечивает более высокую скорость передачи данных.

Кроме того, часто к спектру сигнала предъявляется требование отсутствия постоянной составляющей, то есть наличия постоянного тока между передатчиком и приемником, поскольку применение различных трансформаторных схем *гальванической развязки* в электрических линиях связи препятствует прохождению постоянного тока.

Спектр результирующего сигнала зависит от:

- метода кодирования (модуляции);
- скорости модуляции, определяющей скорость передачи данных;
- состава передаваемых данных.

**Поддержка синхронизации** между передатчиком и приёмником сигналов для определения момента считывания в приёмнике значения очередного битового интервала может быть реализована за счёт применения *самосинхронизирующихся методов кодирования*. Указанием

для синхронизации приемника с передатчиком в этих методах может служить любой резкий перепад сигнала – так называемый **фронт**.

**Отсутствие постоянной составляющей** необходимо для поддержки синхронизации приёмника с передатчиком, а также для того, чтобы нижняя частота кодированного сигнала как можно больше отличалась от нуля, что, соответственно, уменьшает спектр сигнала и не препятствует прохождению постоянного тока при наличии трансформаторных схем гальванической развязки в электрических линиях связи.

**Возможность обнаружения ошибок** и их исправления – желательное, но не обязательное требование, предъявляемое к методам кодирования. Обнаружение ошибки на физическом уровне экономит время, так как приёмник отбрасывает ошибочный кадр, не ожидая полного его приёма в буфер.

**Низкая стоимость реализации** метода кодирования связана с количеством уровней сигнала – чем больше уровней сигнала, тем выше стоимость реализации. Это обусловлено необходимостью применения более мощного и, следовательно, более дорогого приёмно-передающего оборудования.

Требования, предъявляемые к методам кодирования, являются взаимно противоречивыми, поэтому каждый из рассматриваемых ниже методов цифрового кодирования по сравнению с другими обладает своими достоинствами и недостатками.

#### **2.3.3.3. Потенциальный код без возврата к нулю (NRZ)**

На рис.2.32,а показан метод потенциального кодирования, называемый также кодированием *без возврата к нулю* – NRZ (Non Return to Zero). В этом методе высокий потенциал соответствует значению бита «1», а низкий – значению «0».

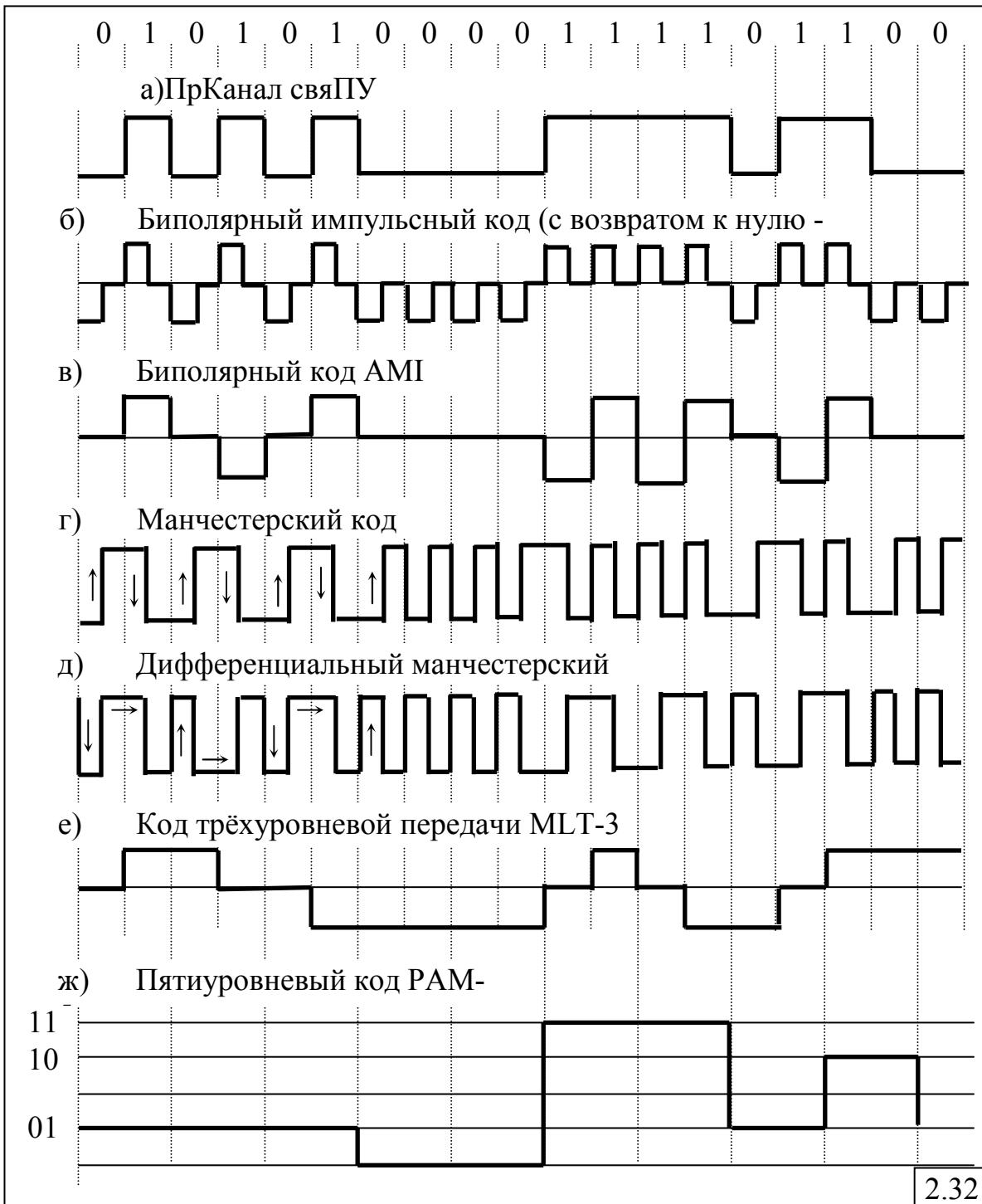
##### **Достоинства:**

- низкая частота основной гармоники:  $f_0 = \frac{1}{2C}$  Гц (С – битовая скорость передачи данных), которая меньше, чем у других методов кодирования;
- наличие только двух уровней потенциала и, как следствие, простота и низкая стоимость.

##### **Недостатки:**

- не обладает свойством самосинхронизации: при передаче длинной последовательности единиц или нулей сигнал не изменяется и возможна рассинхронизация часов приёмника и передатчика;
- наличие низкочастотной составляющей не позволяет использовать этот вид кодирования в каналах связи, не обеспечивающих прямого гальванического соединения между приемником и источником.

По этим причинам в компьютерных сетях код NRZ в чистом виде не используется. Тем не менее, используются его модификации, в которых устраняют постоянную составляющую и отсутствие самосинхронизации.



#### 2.3.3.4. Биполярный импульсный код (RZ)

Кроме потенциальных кодов в компьютерных сетях используются импульсные коды, в которых данные представлены полным импульсом или же его частью – фронтом. Наиболее простым является *биполярный импульсный код*, называемый также кодированием с *возвратом к нулю* (Return to Zero, RZ), в котором единица представлена импульсом одной полярности, а ноль – импульсом другой полярности (рис.2.32,б). Каждый импульс длится половину такта (битового интервала). В середине каждого битового интервала происходит возврат к нулевому потенциалу.

**Достоинство:**

- обладает свойством самосинхронизации – возврат в середине каждого битового интервала к нулевому потенциалу служит признаком (стробом) для синхронизации часов приёмника.

**Недостатки:**

- наличие трех уровней сигнала, что требует увеличения мощности передатчика для обеспечения достоверности приема и, как следствие, большая стоимость реализации;
- спектр сигнала шире, чем у потенциальных кодов; так, при передаче всех нулей или единиц частота основной гармоники кода будет равна  $C$  Гц, что в два раза выше основной гармоники кода NRZ.

Из-за слишком широкого спектра биполярный импульсный код используется редко.

**2.3.3.5. Биполярное кодирование с альтернативной инверсией (AMI)**

Одной из модификаций метода RZ является метод *биполярного кодирования с альтернативной инверсией* (Bipolar Alternate Mark Inversion, AMI), в котором используются три уровня потенциала – положительный, нулевой и отрицательный (рис.2.32,в). Двоичный «0» кодируется нулевым потенциалом, а двоичная «1» – либо положительным потенциалом, либо отрицательным, при этом потенциал следующей единицы противоположен потенциальному предыдущей.

**Достоинства:**

- ликвидируется проблема постоянной составляющей и отсутствия самосинхронизации при передаче *длинных последовательностей единиц*, поскольку сигнал в этом случае представляет собой последовательность разнополярных импульсов с тем же спектром, что и у кода NRZ, передающего чередующиеся нули и единицы, то есть с частотой основной гармоникой Гц;
- в целом, использование кода AMI приводит к более узкому спектру сигнала, чем для кода NRZ, а значит и к более высокой пропускной способности канала связи, в частности, при передаче чередующихся единиц и нулей частота основной гармоники Гц;
- предоставляет возможность распознавать ошибочные сигналы при нарушении чередования полярности сигналов; сигнал с некорректной полярностью называется *запрещенным сигналом*.

**Недостатки:**

- наличие трёх уровней сигнала, что требует увеличения мощности передатчика;
- наличие постоянной составляющей в сигнале в случае длинных последовательностей нулей.

### **2.3.3.6. Потенциальный код с инверсией при единице (NRZI)**

Потенциальный код с инверсией при единице (Non Return to Zero with ones Inverted, NRZI) похож на AMI, но имеет только два уровня сигнала. При передаче нуля он передает потенциал, который был установлен в предыдущем такте, а при передаче единицы потенциал меняется на противоположный.

### **2.3.3.7. Манчестерский код**

В локальных сетях (ЛВС Ethernet и Token Ring) до недавнего времени применялся манчестерский код (рис.2.32,г), в котором для кодирования двоичных единиц и нулей используется переход сигнала в середине каждого битового интервала:

- «1» кодируется переходом от высокого уровня сигнала к низкому;
- «0» – обратным переходом от низкого уровня сигнала к высокому.

Если данные содержат подряд несколько единиц или нулей, то в начале каждого битового интервала происходит дополнительный служебный переход сигнала.

#### **Достоинства:**

- обладает свойством самосинхронизации, так как значение потенциала всякий раз изменяется в середине битового интервала, что может служить сигналом для синхронизации приёмника с передатчиком;
- имеет только *два уровня* потенциала;
- спектр манчестерского кода *меньше*, чем у биполярного импульсного, в среднем в 1,5 раза: основная гармоника при передаче последовательности единиц или нулей имеет частоту  $f_0 = \frac{1}{C}$  Гц, а при передаче чередующихся единиц и нулей она равна  $f_0 = \frac{1}{2C}$  Гц, как и у кода NRZ;
- нет постоянной составляющей.

#### **Недостатки:**

- спектр сигнала шире, чем у кода NRZ и кода AMI.

### **2.3.3.8. Дифференциальный манчестерский код**

Дифференциальный или разностный манчестерский код используется в сетях Token Ring (стандарт 802.5) и FDDI и представляет собой разновидность манчестерского кода с двумя уровнями потенциала:

- «0» кодируется изменением потенциала в начале битового интервала;
- «1» – сохранением предыдущего уровня потенциала.

В середине каждого битового интервала обязательно присутствует переход с одного уровня потенциала на другой (рис.2.32,д).

### **2.3.3.9. Код трехуровневой передачи MLT-3**

Код трехуровневой передачи MLT-3 (Multi Level Transmission-3) имеет много общего с кодом AMI. Единице соответствует последовательный переход на границе битового интервала с одного уровня сигнала на другой. При передаче нулей сигнал не меняется (рис. 2.32,е).

Максимальная частота сигнала достигается при передаче длинной последовательности единиц. В этом случае изменение уровня сигнала происходит последовательно с одного уровня на другой с учетом предыдущего перехода.

MLT-3 используется в сетях FDDI на основе медных проводов, известных как CDDI, и Fast Ethernet стандарта 100Base-TX совместно с избыточным методом логического кодирования 4B/5B.

#### **Недостатки:**

- отсутствие свойства самосинхронизации;
- наличие трех уровней сигнала;
- наличие постоянной составляющей в сигнале в случае длинной последовательности нулей.

### **2.3.3.10. Пятиуровневый код РАМ-5**

В пятиуровневом коде РАМ-5 используется 5 уровней амплитуды сигнала и двухбитовое кодирование (рис.2.32,ж), означающее наличие четырёх уровней, соответствующих двум битам передаваемых данных: 00, 01, 10, 11, то есть в одном битовом интервале передаются сразу два бита. Пятый уровень добавлен для создания избыточности кода, используемого для исправления ошибок.

#### **Достоинства:**

- при одной той же скорости модуляции (длительности битового интервала) по каналу связи можно передавать данные в два раза быстрее по сравнению с AMI или NRZI, так как в одном битовом интервале передаются сразу два бита.

#### **Недостатки:**

- длинные последовательности одинаковых пар бит приводят к появлению в сигнале постоянной составляющей;
- наличие 4-х уровней требует большей мощности передатчика, чтобы уровни четко различались приемником на фоне помех.

Код РАМ-5 используется в сетях 1000Base-T (Gigabit Ethernet).

## **2.3.4. Логическое кодирование**

**Логическое кодирование** предназначено для улучшения потенциальных кодов типа AMI, NRZI или MLT-3 и направлено на ликвидацию длинных последовательностей единиц или нулей, приводящих к постоянному потенциальному.

Для улучшения потенциальных кодов используются два способа:

- избыточное кодирование;
- скремблирование.

Оба способа относятся к логическому, а не физическому кодированию, так как они не определяют форму сигналов.

#### **2.3.4.1. Избыточное кодирование**

При **избыточном кодировании** исходный двоичный код рассматривается как совокупность символов, представляющих собой последовательность нескольких битов, каждый из которых заменяется новым символом, содержащим большее количество бит, чем исходный.

Примерами методов избыточного кодирования являются 4B/5B (используется в ЛВС Fast Ethernet стандартов 100Base-TX и 100Base-FX и в сети FDDI), 5B/6B (100VG-AnyLAN), 8B/10B (10GBase-X), 64B/66B (10GBase-R и 10GBase-W). Буква «В» в названии кода означает, что элементарный сигнал имеет 2 состояния (от английского binary – двоичный), а цифры указывают, какое количество бит содержится в одном символе исходного и результирующего кода соответственно. В частности, метод 4B/5B означает, что каждые 4 бита в исходном коде заменяются 5-ю битами в результирующем коде, то есть четырёхбитные символы исходного кода заменяются символами, содержащими по 5 бит. Для этого используется специальная **таблица перекодировки** (табл.2.1), устанавливающая соответствие между исходными четырёхбитовыми символами и результирующими пятибитовыми символами.

*Таблица 2.1.*

<i>Исходные символы</i>	<i>Результирующие символы</i>	<i>Исходные символы</i>	<i>Результирующие символы</i>
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

Количество результирующих символов больше количества исходных символов. Так, в коде 4B/5B результирующих символов может быть  $2^5=32$ , в то время как исходных символов только  $2^4=16$ . Поэтому среди результирующих символов можно отобрать 16 таких, любое сочетание которых не содержит длинных последовательностей нулей или единиц (в худшем случае 3 нуля или 8 единиц). Остальные 16 символов рассматриваются как *запрещенные*, появление которых означает ошибку в передаваемых данных.

Избыточность кода 4B/5B составляет 25% ( $1/4 = 0,25$ ), поскольку на 4 информационных бита приходится 1 «лишний» избыточный бит. Это означает, что реальная пропускная способность канала будет на 25% меньше номинальной. Для обеспечения заданной пропускной способности канала передатчик должен работать с повышенной тактовой частотой. В частности, для передачи кодов 4B/5B со скоростью 100 Мбит/с передатчик должен работать с тактовой частотой 125 МГц. При этом спектр сигнала увеличивается по сравнению со случаем, когда передается не избыточный код. Тем не менее, спектр избыточного кода меньше спектра манчестерского кода, что оправдывает использование логического кодирования.

#### **Достоинства:**

- код становится самосинхронизирующимся, так как прерываются длинные последовательности нулей и единиц;
- исчезает постоянная составляющая, а значит, сужается спектр сигнала;
- появляется возможность обнаружения ошибок за счёт запрещённых символов;
- простая реализация в виде таблицы перекодировки.

#### **Недостатки:**

- уменьшается полезная пропускная способность канала связи, так как часть пропускной способности тратится на передачу избыточных бит;
- дополнительные временные затраты в узлах сети на реализацию логического кодирования.

В сети Fast Ethernet стандарта 100Base-T4 используется метод логического кодирования 8B/6T с тремя состояниями результирующего сигнала, в котором для кодирования 8 бит (B) исходного сообщения используется код из 6 троичных (T) символов, имеющих 3 состояния. Количество избыточных, то есть запрещённых кодов:  $3^6 - 2^8 = 729 - 256 = 473$ .

#### **2.3.4.2. Скремблирование**

Скремблирование состоит в преобразовании исходного двоичного кода по заданному алгоритму, позволяющему исключить длинные последовательности нулей или единиц. Технические или программные средства, реализующие заданный алгоритм, называются *скремблерами* (scramble – свалка, беспорядочная сборка). На приёмной стороне *дескремблер* восстанавливает исходный двоичный код.

В качестве алгоритма преобразования может служить соотношение:

$$B_i = A_i \oplus B_{i-3} \oplus B_{i-5} \quad (i = 1, 2, \dots),$$

где  $A_i$ ,  $B_i$  – значения  $i$ -го разряда соответственно исходного и результирующего кода;  $B_{i-3}$  и  $B_{i-5}$  – значения соответственно  $(i-3)$ -го и  $(i-5)$ -го разряда результирующего кода;  $\oplus$  – операция исключающего ИЛИ (сложение по модулю 2).

Например, для исходной последовательности  $A=110110000001$  скремблер даст следующий результирующий код:

$$\begin{aligned}B_1 &= A_1 = 1; \\B_2 &= A_2 = 1; \\B_3 &= A_3 = 0; \\B_4 &= A_4 \oplus B_1 = 1 \oplus 1 = 0; \\B_5 &= A_5 \oplus B_2 = 1 \oplus 1 = 0; \\B_6 &= A_6 \oplus B_3 \oplus B_1 = 0 \oplus 0 \oplus 1 = 1; \\B_7 &= A_7 \oplus B_4 \oplus B_2 = 0 \oplus 0 \oplus 1 = 1; \\B_8 &= A_8 \oplus B_5 \oplus B_3 = 0 \oplus 0 \oplus 0 = 0; \\B_9 &= A_9 \oplus B_6 \oplus B_4 = 0 \oplus 1 \oplus 0 = 1; \\B_{10} &= A_{10} \oplus B_7 \oplus B_5 = 0 \oplus 1 \oplus 0 = 1; \\B_{11} &= A_{11} \oplus B_8 \oplus B_6 = 0 \oplus 0 \oplus 1 = 1; \\B_{12} &= A_{12} \oplus B_9 \oplus B_7 = 1 \oplus 1 \oplus 1 = 1.\end{aligned}$$

Таким образом, на выходе скремблера появится последовательность  $B=110001101111$ , в которой нет последовательности из шести нулей, присутствовавшей в исходном коде.

Дескремблер восстанавливает исходную последовательность на основании обратного соотношения:

$$C_i = B_i \oplus B_{i-3} \oplus B_{i-5} \quad (i = 1, 2, \dots).$$

Легко убедиться, что  $C_i = A_i$ .

Различные алгоритмы скремблирования отличаются количеством слагаемых, дающих цифру результирующего кода и величиной сдвига между слагаемыми. Так, в сетях ISDN при передаче данных от сети к абоненту используется преобразование со сдвигами в 5 и 23 позиции, а при передаче данных от абонента в сеть – со сдвигами 18 и 23 позиции.

#### **Достоинство:**

- не уменьшается полезная пропускная способность канала связи, поскольку отсутствуют избыточные биты.

#### **Недостатки:**

- дополнительные затраты в узлах сети на реализацию алгоритма скремблирования-дескремблирования;
- не всегда удается исключить длинные последовательности нулей и единиц.

## **2.4. Кабельные линии связи**

При организации компьютерных сетей широко используются кабельные линии связи.

**Кабельная линия связи** (КЛС) – линия связи, состоящая из кабеля, кабельной арматуры и кабельных сооружений (туннели, колодцы, распределительные шкафы, кабельные столбы).

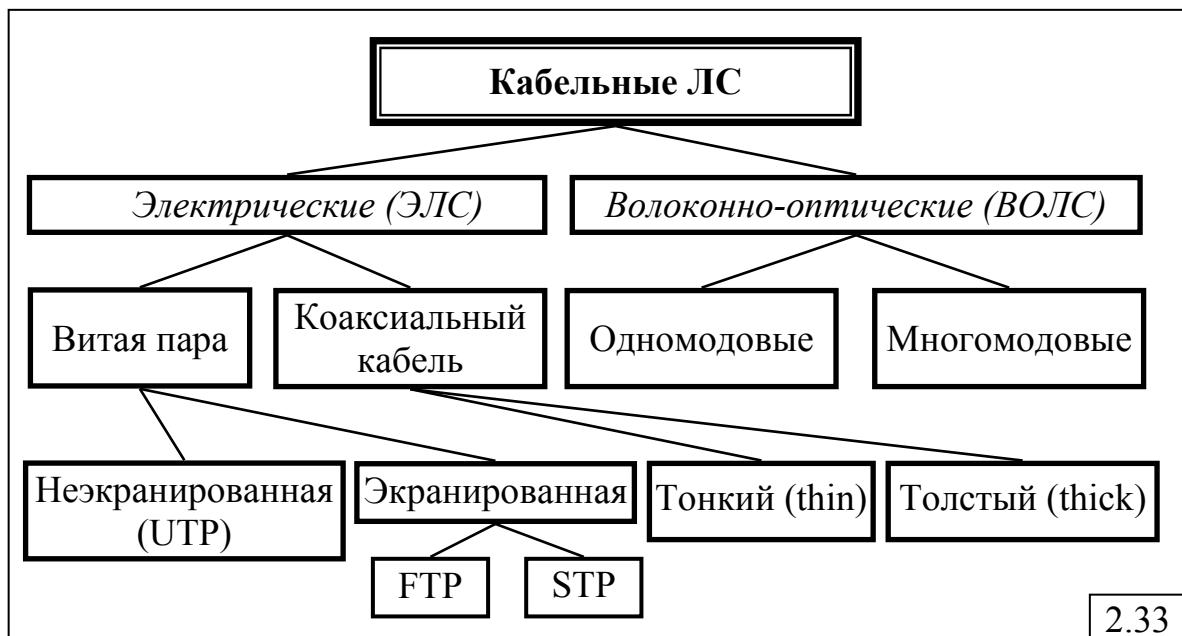
**Кабель** (от голл. kabel – канат, трос) – совокупность гибких изолированных проводов, заключенных в защитную (обычно герметичную) оболочку.

**Электрический (медный) кабель** – кабель из электрических (médных) проводников (токопроводящих жил), применяемый для передачи на расстояние электрической энергии (*силовой кабель*) или электрических сигналов (*кабель связи*).

**Волоконно-оптический кабель** – кабель из оптических волокон для передачи светового потока.

**Кабель связи** предназначен для передачи информации электрическими или оптическими (световыми) сигналами.

Таким образом, кабельные линии связи делятся на две большие группы: электрические (ЭЛС) и волоконно-оптические (ВОЛС). Типы кабельных линий связи, используемых в компьютерных сетях, представлены на рис.2.33.



#### 2.4.1. Электрические кабельные линии связи

В сетях передачи данных применяются следующие типы электрических кабелей (рис.2.33):

- 1) витая пара:
  - неэкранированная;
  - экранированная;
- 2) коаксиальный кабель:
  - толстый (thick);
  - тонкий (thin).

##### 2.4.1.1. Основные электромагнитные характеристики электрических кабелей связи

Основные электромагнитные характеристики электрических кабелей связи представлены на рис.2.34.

1. **Затухание (коэффициент затухания)** – уменьшение мощности сигнала (потеря амплитуды) при передаче между двумя точками:

- является одной из основных характеристик, учитываемых при проектировании ЭЛС и определении максимальной длины кабеля между узлами;
- зависит от частоты передаваемого сигнала;
- измеряется в [дБ/м].



2. **Импеданс** (волновое сопротивление) – полное (активное и реактивное) сопротивление электрической цепи:

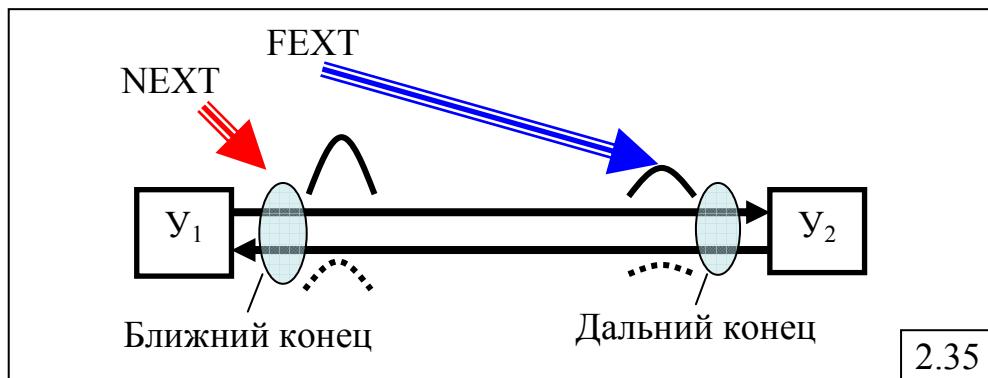
- измеряется в Омах и является относительно постоянной величиной для кабельных систем (в высокоскоростных сетях зависит от частоты);
- резкие изменения импеданса по длине кабеля могут вызвать процессы внутреннего отражения, приводящие к возникновению стоячих волн, при этом станция, подключенная вблизи узла стоячей волны, не будет получать адресованные ей данные.

3. **Перекрестные наводки** между витыми парами **на ближнем конце** (NEXT – Near End Crosstalk) и **на дальнем конце** (FEXT – Far End Crosstalk) – результат интерференции электромагнитных сигналов (рис.2.35):

- значения NEXT и FEXT зависят от частоты передаваемого сигнала;
- чем **больше абсолютное значение** NEXT (FEXT), тем лучше, так как наводки в соседних проводниках будут меньше;
- измеряется в дБ при определённой частоте.

Из рис.2.35 видно, что на ближнем конце проводника (по отношению к передающему узлу) высокий уровень сигнала, передаваемого от узла  $Y_1$  к узлу  $Y_2$ , наводит паразитный сигнал (показан пунктиром), искажающий информационный (полезный) сигнал во втором проводнике, по которому передаются данные от  $Y_2$  к  $Y_1$ . Из рисунка также видно, что на дальнем конце паразитный сигнал во втором проводнике значительно меньше, поскольку в результате затухания меньше уровень информационного сигнала, передаваемого в первом проводнике от  $Y_1$  к  $Y_2$ . С учётом того, что уровень информационного сигнала во втором проводнике на «дальнем конце» имеет максимальное значение, можно сделать вывод, что наведённый паразитный сигнал незначительно искажит информационный сигнал. Отсюда следует, что NEXT является более важной

характеристикой, чем FEXT, так как его значение в большей мере сказывается на качестве передачи сигналов.



**4. Активное сопротивление** – сопротивление электрической цепи постоянному току:

- не зависит от частоты и возрастает с увеличением длины кабеля;
- измеряется в Омах на 100 м.

**5. Ёмкость** – свойство металлических проводников накапливать электрическую энергию:

- является нежелательной величиной и должна быть минимальной;
- высокое значение ёмкости в кабеле приводит к искажению сигнала и ограничивает полосу пропускания линии.

#### 2.4.1.2. Витая пара

**Витая пара** (*Twisted Pair – TP*) – изолированные проводники, попарно свитые между собой минимально необходимое число раз на определенном отрезке длины (рис.2.36,а), что требуется для уменьшения перекрестных наводок между проводниками, и заключённые в изолирующую оболочку.

Витая пара – самый распространенный вид кабеля в телефонии. Скручивание применяется с целью *уменьшения излучения и повышения помехозащищенности* кабеля.

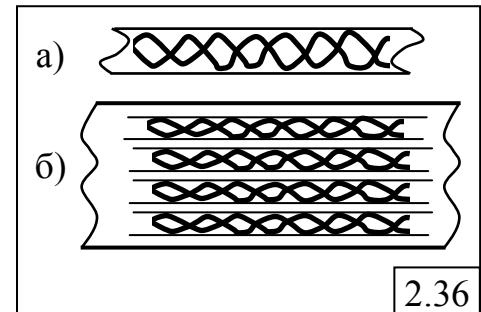
Несколько витых пар (обычно 4 или 8), заключённые в общую пластиковую оболочку, образуют **кабель** (рис.2.36,б).

Существует несколько категорий **незащищенной витой пары** (*Unshielded Twisted Pair – UTP*), причём чем выше категория кабеля, тем больше его полоса пропускания.

Кабели 1-й и 2-й категорий используются для передачи речи и данных на низких скоростях и не включены в стандарты для передачи данных в компьютерных сетях.

Стандарт EIA/TIA-568, разработанный American National Standards Institute (ANSI, США) определяет спецификации для 3-й, 4-й и 5-й категорий UTP и нормирует следующие характеристики:

- коэффициент затухания,



- волновое сопротивление,
- емкость,
- переходное затухание на ближнем конце и др.

Например, для кабеля 5-й категории определены следующие характеристики:

- затухание – не более 23,6 дБ на 100 м (0,236 дБ/м) при частоте 100 МГц;
- волновое сопротивление – не более 100 Ом $\pm$ 15%;
- NEXT – не менее 27 дБ при частоте 100 МГц;
- активное сопротивление – не более 9,4 Ом на 100 м;
- емкость не более 5,6 нФ на 100 м.

**Экранированная витая пара** – кабель, содержащий одну или несколько пар скрученных медных проводов, заключенных в изолирующую оболочку. Снаружи кабель покрыт экранирующей оплеткой и еще одной изолирующей оболочкой, за счёт чего меньше излучает и лучше защищён от электромагнитных помех, чем неэкранированная витая пара. Применяется в сетях Token Ring.

Экранированная витая пара подразделяется на две разновидности:

- с экранированием каждой пары и общим экраном (Shielded Twisted Pair – STP);
- с одним общим экраном (Foiled Twisted Pair – FTP).

Для высокоскоростных сетей разработаны еще две категории медного кабеля:

- категория 6 – обеспечивает работу на частоте 250 МГц и может быть реализована как экранированный, так и неэкранированный кабель;
- категория 7 – обеспечивает работу на частоте до 600 МГц и использует экранирование каждой пары кабеля и общий экран.

В табл.2.2 приведены значения полосы пропускания для разных категорий современных медных кабелей.

Наиболее широко в настоящее время в локальных сетях применяется электрический кабель категории 5.

Таблица 2.2

Категория кабеля	Полоса пропускания, МГц
3	16
4	20
5	100
6	250
7	600

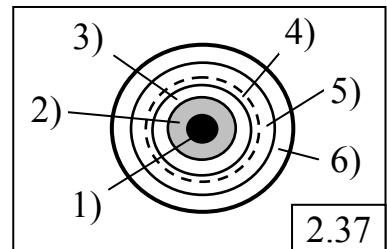
#### 2.4.1.3. Коаксиальный кабель

**Коаксиальный кабель** (от лат. *co* – совместно и *axis* – ось) – кабель, в котором проводники представляют собой 2 соосных металлических цилиндра, разделенных диэлектриком. Коаксиальный кабель используется для передачи высокочастотных сигналов (до нескольких ГГц) и характеризуется высокой помехозащищенностью и малым затуханием

сигналов. Это обусловлено отсутствием внешнего электромагнитного поля – вся энергия распространяется только внутри кабеля.

Коаксиальный кабель содержит (рис.2.37):

- 1) внутренний проводник диаметром от 0,4 мм до 2,5 мм;
- 2) диэлектрик, в качестве которого обычно применяется обычный полиэтилен или физически вспененный полиэтилен с низкой плотностью, позволяющий уменьшить коэффициент затухания;
- 3) внешний проводник, в качестве которого обычно используется фольга;
- 4) медную оплетку с покрытием из олова;
- 5) защитную пленку;
- 6) внешнюю оболочку.



В ранних сетях Ethernet применялись два типа коаксиального кабеля:

- **толстый (thick)** диаметром около 1 см, для которого, в отличие от тонкого, характерны следующие особенности:
  - более надежная защита от внешних помех;
  - прочнее;
  - требует применения специального отвода (прокалывающего разъема и отводящего кабеля) для подключения компьютера или другого устройства;
- **тонкий (thin)** диаметром около 0,5 см, для которого, в отличие от толстого, характерны следующие особенности:
  - передает данные на более короткие расстояния;
  - дешевле;
  - использует более простые соединители.

Основные недостатки коаксиальных кабелей:

- сложность прокладки, а также добавления и отключения станций;
- высокая удельная стоимость.

## 2.4.2. Волоконно-оптические линии связи (ВОЛС)

Волоконно-оптические линии связи (ВОЛС) используются для высокоскоростной передачи данных, представляемых в виде *оптических сигналов*, по оптическим диэлектрическим *световодам*, являющимся самой перспективной физической средой для передачи данных.

*Оптический сигнал* представляет собой модулированный световой поток, генерируемый *светодиодами* или *диодными лазерами*.

Основными компонентами ВОЛС являются:

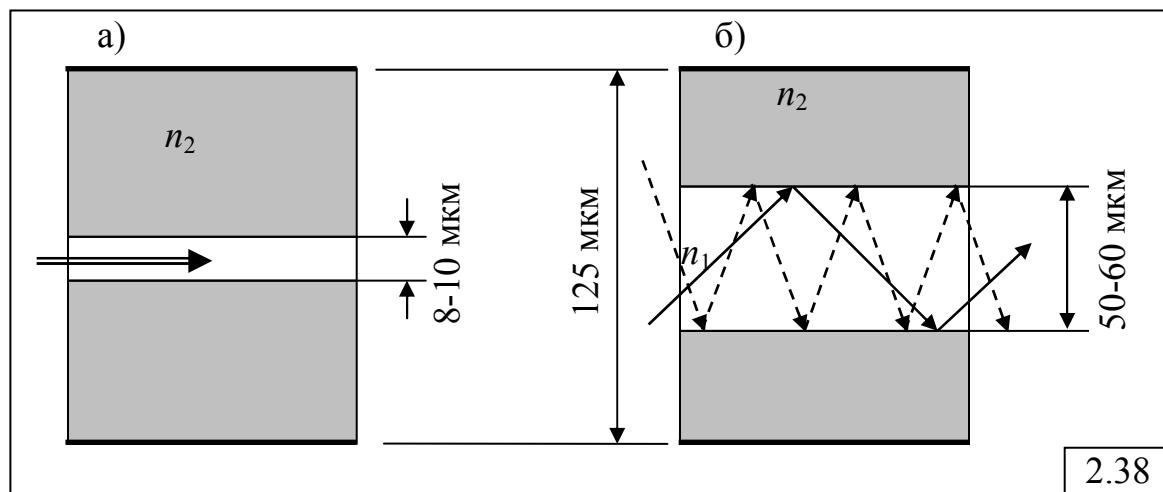
- 1) оптическое волокно;
- 2) волоконно-оптический кабель;
- 3) оптические компоненты и устройства;
- 4) электронные компоненты систем оптической связи.

### 2.4.2.1. Оптическое волокно

**Оптическое волокно** – главный компонент ВОЛС – состоит из **сердцевины (световодной жилы)** и **оболочки** с разными показателями преломления  $n_1$  и  $n_2$  (рис.2.38).

Оптические волокна в зависимости от способа распространения в них излучения делятся на:

- **одномодовые** (рис.2.38,а), в которых световодная жила имеет диаметр 8–10 мкм, в которых может распространяться только один луч (одна мода);
- **многомодовые** (рис.2.38,б), в которых световодная жила имеет диаметр 50–60 мкм, что делает возможным распространение в них большого числа лучей (много мод).



2.38

Важнейшими параметрами оптического волокна являются:

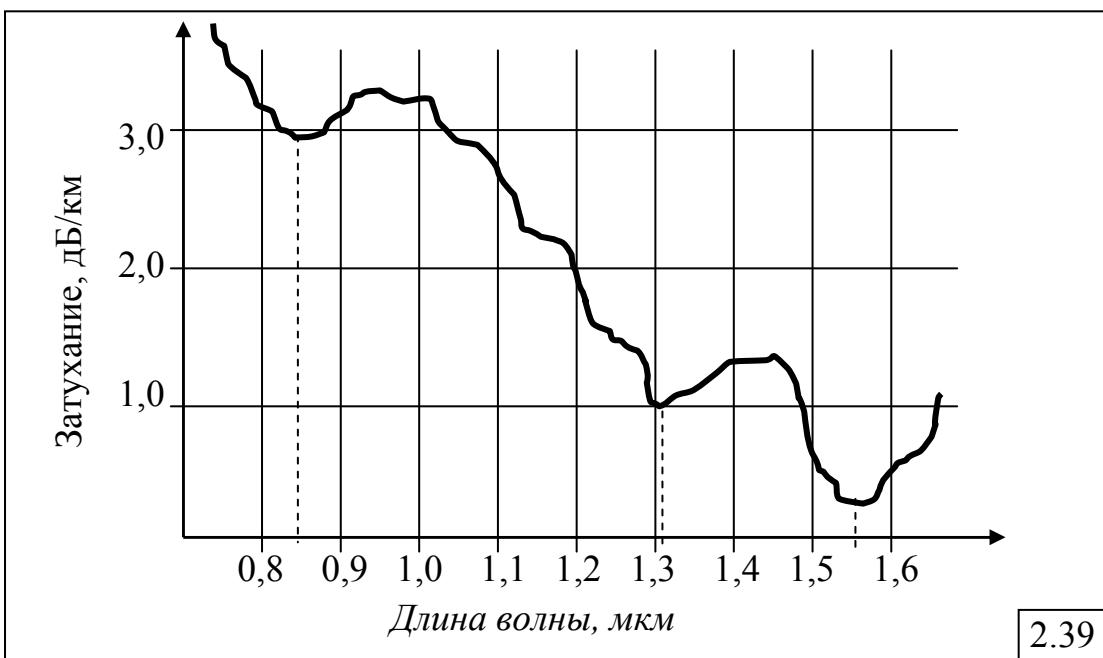
- затухание;
- дисперсия.

**Затухание** определяется потерями на поглощение и рассеяние излучения в оптическом волокне и измеряется в децибелах на километр (дБ/км). Потери на поглощение зависят от чистоты материала, а потери на рассеяние – от неоднородностей его показателя преломления.

Затухание зависит и от длины волны излучения, вводимого в волокно. Передача сигналов по оптическому волокну осуществляется в трех диапазонах: 0,85 мкм, 1,3 мкм и 1,55 мкм, так как именно в этих диапазонах кварц имеет повышенную прозрачность (рис.2.39).

Оптическое волокно характеризуется малым затуханием светового сигнала, составляющим 0,1–0,2 дБ/км при длине волны 1,55 мкм, что позволяет строить ЛС длиной до нескольких десятков километров без регенерации сигналов.

Ведутся разработки еще более "прозрачных", так называемых, **фтороцирконатных волокон** с затуханием порядка 0,02 дБ/км при длине волны 2,5 мкм, на основе которых могут быть созданы ЛС, обеспечивающие гигабитные скорости передачи и с регенерационными участками через каждые 4-5 тысяч километров.



2.39

В последние годы наряду с когерентными системами связи развивается альтернативное направление – **солитоновые** системы.

**Солитон** – уединенная волна, которая не затухает и не поглощается средой, а сохраняет свои размеры и форму сколь угодно долго.

**Солитон** – это световой импульс с необычными свойствами: он сохраняет свою форму и теоретически может распространяться по "идеальному" световоду бесконечно далеко. Длительность импульса составляет примерно 10 пс.

Солитоновые системы, в которых отдельный бит информации кодируется наличием или отсутствием солитона, имеют пропускную способность не менее 5 Гбит/с при расстоянии 10 000 км.

**Дисперсия** – рассеяние во времени спектральных и модовых составляющих оптического сигнала.

Поскольку при передаче информации светодиод или лазер излучает некоторый спектр длин волн, дисперсия приводит к уширению импульсов при распространении по волокну и тем самым порождает искажения сигналов (рис.2.40). При оценке дисперсии пользуются термином "**полоса пропускания**" – величина, обратная величине уширения импульса  $\Delta t$  при прохождении им по оптическому волокну расстояния в 1 км:  $\Pi = \frac{1}{\Delta t}$ .

Измеряется полоса пропускания в мегагерцах на километр (МГц\*км).

Из определения полосы пропускания следует, что дисперсия налагает ограничения на дальность передачи и верхнее значение частоты передаваемых сигналов. Если полоса пропускания оптического волокна составляет 1000 МГц\*км (что соответствует величине уширения импульса в 1 нс/км), то пропускная способность линии связи длиной в 1 км будет не более 1 Гбит/с, а при длине линии связи в 10 км – не более 100 Мбит/с.

Значения дисперсии и затухания различны для разных типов волокон.

**Достоинства** одномодовых волокон:

- лучшие характеристики по затуханию и полосе пропускания, так как в них распространяется только один луч;
- максимальное затухание составляет 0,5 дБ/км при длине волны 1,31 мкм и 1,55 мкм;
- при использовании лазерных передатчиков расстояние между узлами может составлять до 40 км.

**Недостатки** одномодовых волокон:

- одномодовые источники излучения дороже многомодовых;
- в одномодовое волокно труднее ввести световой луч из-за малого диаметра световодной жилы;
- по этой же причине трудно минимизировать потери сигнала при спаечивании одномодовых волокон;
- дороже монтаж оптических разъемов на концах одномодовых кабелей.

**Достоинства** многомодовых волокон:

- более удобны при монтаже, так как в них больше размер световодной жилы;
- проще снабдить оптическими разъемами с малыми потерями (до 0,3 дБ).
- имеют меньшую стоимость.

**Недостатки** многомодовых волокон:

- большое затухание, составляющее при длине волны 0,85 мкм – 3-4 дБ/км;
- обеспечивает передачу данных без применения промежуточных повторителей на расстояние не более 2-х км;
- недостаточная полоса пропускания многомодовых волокон для магистральных линий связи, которая составляет порядка 1000 МГц\*км (но вполне приемлемая для локальных сетей).

Результаты сравнительного анализа одномодовых и многомодовых волокон представлены в табл.2.3, где **полужирным шрифтом** выделены лучшие показатели.

Таблица 2.3

Показатель	Одномодовое волокно	Многомодовое волокно
Затухание	<b>0,5 дБ/км</b>	1,5 – 3 дБ/км
Полоса пропускания	<b>более 500 МГц*км</b>	до 500 МГц*км
Расстояние	<b>+ (до 50 км)</b>	(до 2 км)
Стоимость	высокая	<b>низкая</b>
Ввод светового луча	сложнее	<b>легче</b>
Потери при сращивании	выше	<b>ниже</b>

#### 2.4.2.2. Волоконно-оптический кабель

**Волоконно-оптический кабель (ВОК)** – среда передачи данных, состоящая из оптических волокон (стеклянных или пластиковых), заключенных в защитную герметичную оболочку.

Информация в ВОК переносится модулированным световым потоком, генерируемым светодиодами или диодными лазерами.

**Достоинства ВОК** по сравнению с электрическими кабелями:

- высокая пропускная способность;
- отсутствие электромагнитного излучения, что исключает утечку информации;
- помехоустойчивость;
- большое расстояние передачи (не менее 2 км без повторителей);
- малый вес;
- высокое электрическое сопротивление, обеспечивающее гальваническую развязку соединяемых устройств;
- умеренная стоимость, незначительно превышающая стоимость медного кабеля.

**Недостатки ВОК:**

- трудоемкость монтажа, требующая специального оборудования;
- высокая стоимость сетевых устройств.

#### 2.4.2.3. Оптические компоненты

Оптические компоненты включают в себя:

- оптические соединители;
- системы спектрального уплотнения;
- оптические шнуры;
- оптические разветвители;
- распределительные панели;
- кроссовые шкафы;
- соединительные муфты;
- аттенюаторы и т.д.

**Оптические соединители (коннекторы)** предназначены для соединения ВОК с приёмно-передающей аппаратурой через специальные розетки.

*Системы спектрального (волнового) уплотнения WDM* (фильтры WDM) реализуют мультиплексирование и демультиплексирование оптических сигналов.

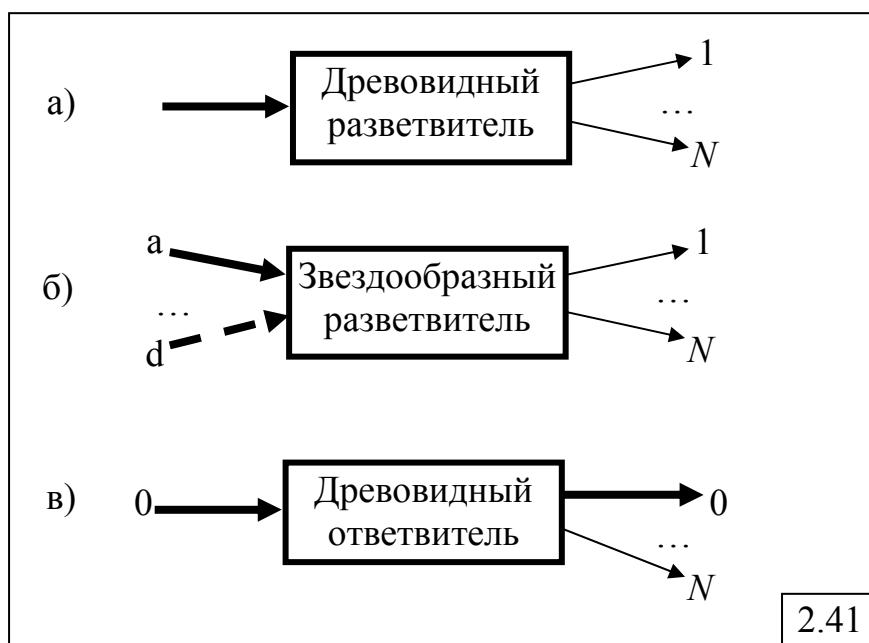
*Оптический шнур* – это оптический миникабель, оба конца которого снабжены соединителями.

*Оптический разветвитель* – многополюсное устройство, в котором подаваемый на вход оптический сигнал разветвляется по нескольким выходным направлениям.

Типы оптических разветвителей:

- древовидный (рис. 2.41, а) – разветвляет один входной оптический сигнал по нескольким выходам (в равной степени по мощности) или наоборот объединяет несколько сигналов в один выходной;
- звездообразный (рис. 2.41, б) – разветвляет поступающий по одному из входов оптический сигнал по нескольким выходам (в равной степени по мощности);
- ответвитель (рис. 2.41, в), где большая часть мощности остается в магистральном канале.

*Аттенюаторы* используются для уменьшения мощности входного оптического сигнала.



#### 2.4.2.4. Особенности ВОЛС

*Физические свойства ВОЛС:*

• *высокая частота несущей* ( $f_n = 10^{14}$  Гц), обуславливающая широкополосность оптических сигналов, то есть возможность передачи данных со скоростью порядка  $10^{12}$  бит/с = 1 Тбит/с;

• *высокая пропускная способность* за счет передачи данных в одном оптическом волокне сразу на нескольких длинах волн;

• *малое затухание светового сигнала*, что позволяет строить протяженные ЛС до сотен километров без регенерации сигналов.

**Достоинства ВОЛС:**

- *невысокая стоимость* материала – кварца (основу которого составляет двуокись кремния), из которого изготавливается волокно, по сравнению с медью;
- оптические волокна *компактны и легки* (их диаметр около 100 мкм), а, следовательно, перспективны для использования в авиации, приборостроении и т.д.;
- обеспечивается *гальваническая развязка сегментов*, так как стеклянные волокна не проводят электричество;
- *безопасны в электрическом отношении*, так как не содержат металла, и, следовательно, могут монтироваться на мачтах существующих линий электропередач;
- *устойчивы к электромагнитным помехам*;
- *данные*, передаваемые по ВОЛС, *защищены от несанкционированного доступа*, так как ВОЛС чрезвычайно трудно подслушать неразрушающим способом, а всякие воздействия на ВОЛС могут быть зарегистрированы с помощью мониторинга (непрерывного контроля) целостности линии;
- возможно применение разных вариантов *скрытой передачи информации*, например путем:
  - модулирования сигналов по фазе и их перемешивания со смещенным на некоторое время сигналом из того же информационного потока;
  - распределения передаваемой информации по множеству сигналов;
  - передачи нескольких шумовых сигналов;
- *долговечность*, означающая сохранение свойств волокна в определенных пределах в течение 25 и более лет;
- обеспечивают *сверхвысокие скорости передачи данных* – десятки и более Гбит/с.

**Недостатки ВОЛС:**

- необходимы специальные технические средства, а именно:
  - высоконадежные адаптеры, преобразующие электрические сигналы в световые и обратно;
  - оптические коннекторы (соединители) с малыми оптическими потерями и большим ресурсом на включение-выключение;
- для монтажа оптических волокон необходимо прецизионное, а, следовательно, дорогое технологическое оборудование;
- высокие затраты по сравнению с медным кабелем на восстановление оптического кабеля при его повреждении (обрыве).

**2.4.2.5. Применение ВОЛС в ЛВС**

Наряду с глобальными сетями оптическое волокно широко используется и при создании ЛВС – Ethernet, FDDI, Token Ring.

**Основные преимущества применения ВОЛС в ЛВС:**

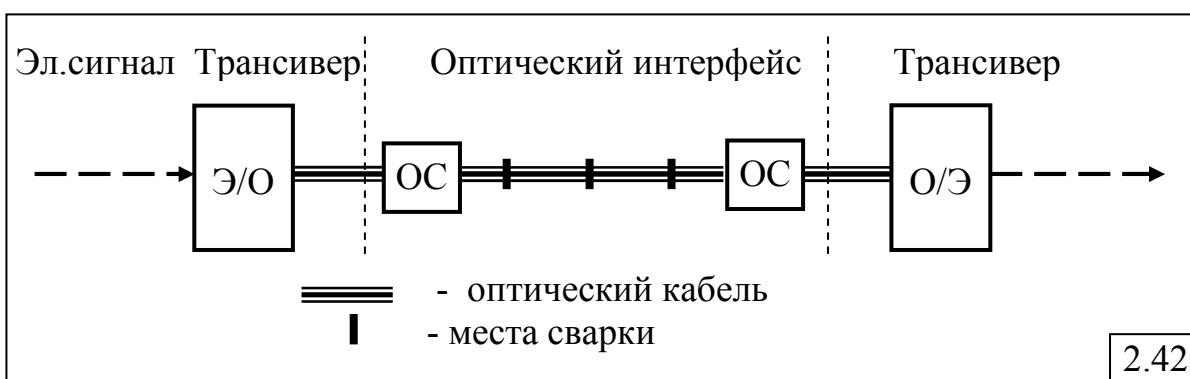
- не требуются повторители на протяженных сегментах ЛВС;
- вероятность искажения информации – не более  $10^{-10}$  благодаря низкому уровню шумов в оптических линиях связи;
- возможность наращивания вычислительной мощности сети без замены кабельных коммуникаций.

**Недостатки** использования ВОЛС в ЛВС:

- несмотря на возможно невысокую стоимость кабеля, стоимость работы по его прокладке может быть значительной.

В состав схемы ВОЛС (рис.2.42) входят:

- сетевой адаптер, устанавливаемый в рабочую станцию или сервер;
- приемопередатчик (трансивер), преобразующий электрический сигнал в оптический (Э/О) и обратно (О/Э);
- оптический соединитель (ОС);
- оптический кабель.



#### 2.4.2.6. Способы сращивания оптических волокон

Для сращивания оптических волокон используются следующие средства.

1. **Специальные сварочные аппараты**, обеспечивающие:

- возможность сваривать любые типы волокон в ручном и автоматическом режимах;
- предварительное тестирование волокна;
- оценку качества поверхности волокон перед сваркой;
- установку оптимальных параметров работы;
- измерение потерь в точке их соединения.

При сварке одно- и многомодовых волокон потери составляют всего 0,01 дБ, что является превосходным результатом.

*Достоинства:*

- высокое качество сварки;
- большая скорость проведения работ, что немаловажно при ликвидации аварий на магистральных линиях связи.

*Недостаток:* высокая стоимость сварочных аппаратов;

2. **Механические "спlices"** (splice), представляющие собой пластиковые устройства размером со спичечный коробок (40x7x4 мм) и состоящие из крышки и корпуса со специальным желобом, в который с двух сторон вставляются соединяемые волокна, закрепляемые крышкой-

замком. Особая конструкция спайса обеспечивает надежное центрирование, герметичное и качественное соединение волокон с потерями на стыке порядка 0,1 дБ.

Достоинства:

- простота и дешевизна способа соединения;
- малое время на соединение двух волокон (около 30 с после соответствующей подготовки волокон);
- удобство при работе в труднодоступном месте, так как монтаж ведется без применения клея и специального оборудования.

**3. Прецизионные втулки**, в которых в месте стыка волокон находится гель на основе силикона высокой прозрачности с показателем преломления, близким к показателю преломления оптического волокна, что обеспечивает оптический контакт между торцами сращиваемых волокон и одновременно герметизирует место стыка.

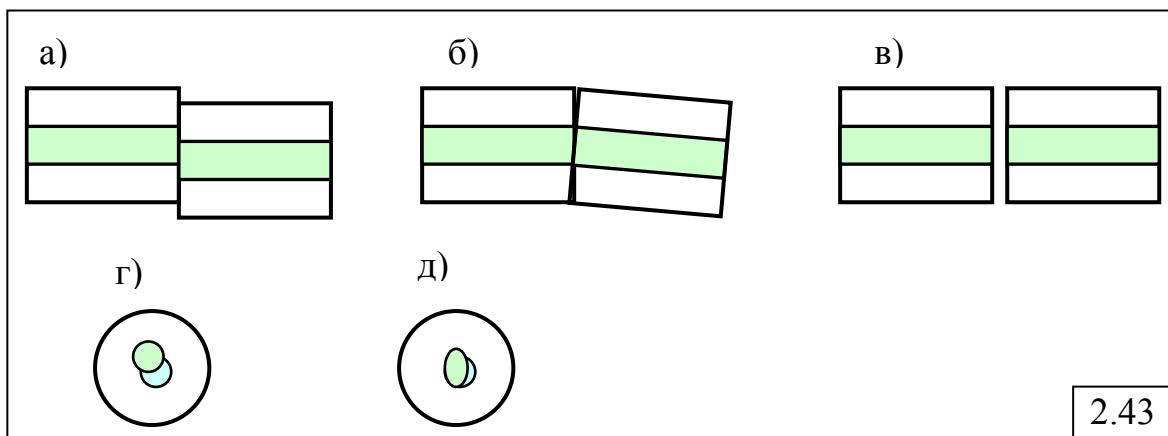
В местах сращивания оптических волокон возникают *потери энергии*, обусловленные:

1) внешними факторами:

- линейное смещение оптических волокон (рис.2.43,а);
- угловое смещение оптических волокон (рис. 2.43,б);
- воздушный зазор между сращиваемыми волокнами (рис. 2.43,в);

2) внутренними факторами:

- эксцентриситет сердцевины (рис. 2.43,г);
- эллиптичность сердцевины (рис. 2.43,д).



#### 2.4.2.7. Перспективы ВОЛС

Работы по увеличению пропускной способности оптических сетей ведутся в двух направлениях:

- увеличивается скорость передачи данных на одной длине волны: в коммерческих системах достигнут уровень 40 Гбит/с, а в тестовых – 320 Гбит/с;
- увеличивается число длин волн, передаваемых по одному волокну: 80 длин волн в коммерческих системах и до 1000 в тестовых.

Теоретическая пропускная способность одного волокна составляет около 300 Тбит/с, что превышает объем всего Интернет-трафика. С учетом

того, что в выпускаемых сегодня кабелях может находиться до 864 волокон, можно говорить о неограниченной полосе пропускания оптических сетей связи.

Кроме того, появляются новые полностью оптические сетевые устройства, обрабатывающие трафик без преобразования оптических сигналов в электрические и обратно.

### **2.4.3. Кабельные системы**

*Кабельная система* представляет собой совокупность:

- кабелей разных типов (незащищенный витая пара, коаксиальный кабель, волоконно-оптический кабель);
- соединительных розеток;
- кроссовых кабелей;
- распределительных панелей.

*Основными причинами сбоев и отказов* в работе локальной вычислительной сети являются:

- отказ кабельной системы – около 50% (в крупных сетях – до 70%);
- сбои программного обеспечения – около 20%;
- сбои серверов и рабочих станций – около 15%;
- сбои сетевых плат – около 5%;
- прочие – около 10%.

Для диагностики и сертификации кабельных систем используется специальное оборудование, а именно:

- **сетевые анализаторы** – дорогостоящие измерительные приборы для диагностики и сертификации кабелей и кабельных систем в лабораторных условиях специально обученным персоналом;
- **приборы для сертификации кабельных систем** – более простые и компактные (размером с видеокассету) приборы, чем сетевые анализаторы, выполняющие те же функции, но обеспечивающие меньшую точность;
- **кабельные сканеры** – приборы для определения длины кабеля, электромагнитных характеристик (NEXT, затухание, импеданс), схемы разводки кабеля, уровня электрических шумов;
- **тестеры (мультиметры)** – наиболее простые и недорогие приборы, позволяющие определить только факт обрыва кабеля.

### **2.4.4. Структурированные кабельные системы**

К современным кабельным системам, используемым, в первую очередь, в компьютерных сетях, предъявляются следующие **требования**:

- *интеграция систем связи*, реализующих передачу различных видов данных (компьютерных, речи, видео), с системами контроля и управления;
- *открытость архитектуры* кабельной системы, обеспечивающей монтаж, последующее обслуживание и развитие комплексных,

стыкующихся со всем сертифицированным оборудованием систем проводки для различных сооружений;

- обеспечение эффективного функционирования и развития компьютерных сетей;
- обеспечение высокой скорости передачи данных – 100 и более Мбит/с.

Для достижения указанных требований была разработана и стандартизована технология построения кабельных систем, получившая название «**СКС - структурированная кабельная система**».

**Структурированная кабельная система (СКС)** представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы, основными среди которых являются:

- вертикальная проводка между этажами здания;
- горизонтальная проводка на этажах;
- кроссовые (коммутационные) панели (кросс-панели);
- модульные розетки на рабочих местах.

К основным **особенностям** СКС можно отнести следующее:

- для передачи компьютерных данных, голоса и видеоинформации используется единая кабельная система;
- большие капиталовложения (по сравнению с традиционным подходом) оправдываются за счет длительной эксплуатации сети;
- обладают модульностью и возможностью внесения изменений и наращивания кабельной сети;
- допускают одновременное использование нескольких различных сетевых протоколов;
- не зависят от изменений сетевых технологий и смены поставщика оборудования;
- используют стандартные компоненты и материалы и позволяют комбинировать в одной сети кабели разных видов.

К **достоинствам** структурированного подхода относятся:

- максимальная гибкость в размещении соответствующего коммуникационного оборудования;
- возможность внедрения новых приложений и технологий;
- гарантированное соответствие всех ее компонентов международным стандартам;
- возможность подключения различных видов оборудования с помощью универсальных розеток на рабочих местах.

**Недостатки** структурированного подхода:

- больший срок построения, чем при традиционном подходе;
- дополнительные капитальные затраты на избыточное оборудование (кабели, розетки, кросс-панели), которые, впрочем, быстро окупаются в процессе эксплуатации.

Основным стандартом, описывающим СКС, является стандарт ANSI/TIA/EIA-568-А, разработанный и утвержденный комитетами American

National Standards Institute (ANSI), Telecommunications Industry Association (TIA) и Electronics Industry Association (EIA).

## **2.5. Беспроводные системы связи**

*Недостатки, присущие кабельным линиям связи (включая оптоволоконные):*

- высокая стоимость арендуемых выделенных каналов;
- подверженность механическим воздействиям в процессе эксплуатации (обрывы и замыкания) и, в связи с высокой трудоемкостью их устранения, выход системы из строя на длительный срок;
- невозможность организации мобильной (подвижной) связи.

### **2.5.1. Общие принципы организации беспроводной связи**

Для построения беспроводных сетей передачи данных необходимо иметь специальные технические и программные средства. Кроме того, необходимо иметь *лицензию* Государственной инспекции электросвязи на право использования определенных частот или арендовать у других организаций уже выделенные им частоты.

Беспроводная связь основана на использовании в качестве информационных сигналов **радиоволн** или, точнее, **электромагнитного поля излучения (ЭПИ)**. Источниками и приемниками ЭПИ являются разного вида *антенны*.

#### **2.5.1.1. Виды беспроводной связи**

На рис.2.44 представлена классификация традиционных видов беспроводной связи, которая включает в себя:

- наземную радиосвязь в диапазоне частот от 30 МГц до нескольких десятков ГГц;
- радиорелайную связь (РРС) в диапазоне частот от 1 до 300 ГГц;
- спутниковую связь в диапазоне частот от 1 до 100 ГГц;
- лазерную (на ИК-лучах) в диапазоне частот от 300 до 400 ТГц.



Эти же виды беспроводной связи находят всё более широкое применение и в компьютерных сетях.

#### **2.5.1.2. Характеристики ЭПИ**

Основными характеристиками ЭПИ (радиоволн) являются:

- длина волны:  $\lambda = \frac{c}{f}$ , где  $c$  – скорость света;  $f$  – частота колебаний радиоволн;
- мощность излучения  $P$  (энергия за секунду), измеряемая в ваттах;
- напряженность поля излучения, измеряемая в вольтах на метр.

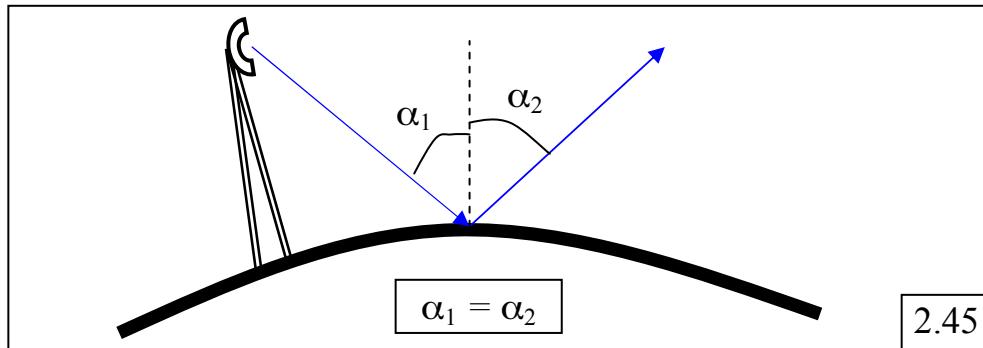
### 2.5.1.3. Условия распространения ЭПИ разных частот

На передачу ЭПИ в точке приема оказывают влияние 3 фундаментальных физических процесса:

- 7) отражение электромагнитного поля (от Земли, зданий и т.п.);
- 8) преломление его лучей в ионизированных слоях атмосферы;
- 9) явление дифракции.

**Отражение** электромагнитного поля от Земли (рис.2.45) приводит:

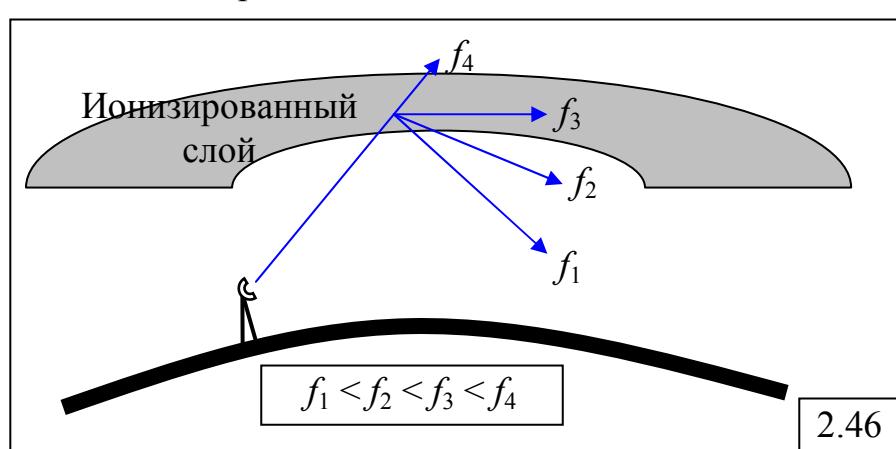
- к ослаблению поля (чем больше частота, тем больше ослабление);
- к изменению его фазы.



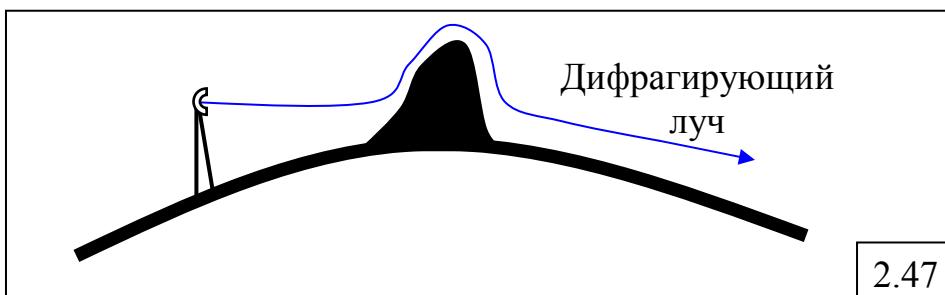
**Ионизированный слой** в атмосфере создается в основном ультрафиолетовым излучением солнца и меняет свои свойства в течение суток и в разные времена года.

В ионосфере происходит (рис.2.46):

- преломление лучей, при этом чем короче волна, то есть чем больше частота, тем меньше преломление при прочих равных условиях, поэтому для связи с космическими объектами используются высокочастотные радиоволны;
- поглощение энергии.



**Дифракция** (рис.2.47) – явление огибания препятствий, приводящее к ослаблению поля: чем больше расстояние и чем больше частота, тем слабее явление дифракции и больше ослабление поля в точке приема.



При выборе длины волны (частоты передачи) для беспроводной передачи необходимо принимать во внимание условия распространения радиоволн, зависящие от:

- трех выше рассмотренных факторов (поглощение, отражение, дифракция);
- интенсивности помех;
- скорости передачи и др.

#### 2.5.1.4. Диапазоны радиоволн

В радиовещательных приёмниках радиоволны условно разделены на следующие диапазоны:

- *длинные* (2000 – 600 м или 150 – 500 кГц);
- *средние* (600 – 200 м или 500 – 1500 кГц);
- *короткие* (100 – 10 м или 3 – 30 МГц);
- *ультракороткие* (менее 10 м или более 30 МГц).

Более научно обоснованным и узаконенным Госстандартом является деление волн на:

- *километровые* (частота < 300 кГц);
- *гектометровые* (300 – 3000 кГц);
- *декаметровые* (3 – 30 МГц);
- *метровые* (30 – 300 МГц);
- *дециметровые* (300 – 3000 МГц);
- *сантиметровые* (3 – 30 ГГц);
- *миллиметровые и субмиллиметровые* (> 30 ГГц).

#### 2.5.1.5. Свойства радиоволн разных диапазонов

Использование радиоволн разных диапазонов в тех или иных областях определяется их свойствами, которые кратко рассматриваются ниже.

##### Километровые волны:

- *Диапазон длин волн (частот):* более 1 000 м (менее 300 кГц).
- *Недостаток:* плохая излучательная способность антенн (низкий К.П.Д. антенны).

- Используются для создания систем устойчивого радиовещания и связи на большие расстояния, для связи под водой, куда не проникают волны более высоких частот.

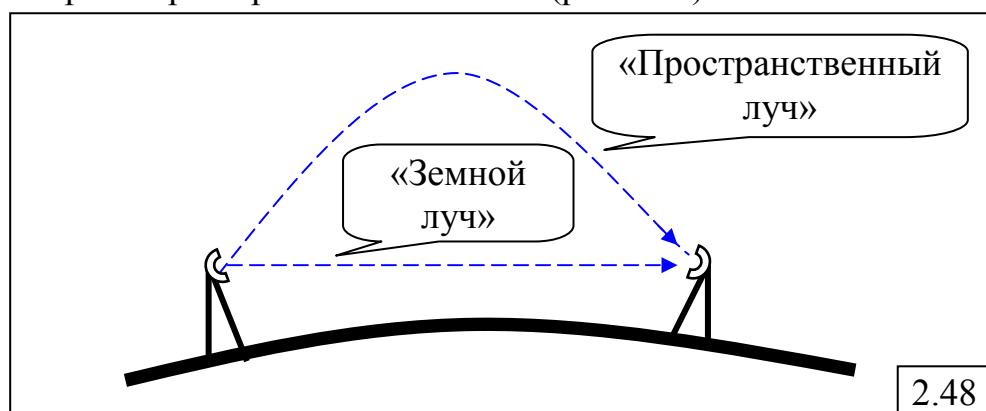
### Гектометровые волны:

- Диапазон длин волн (частот): 1000 – 100 м (300 – 3000 кГц).
- Имеет место эффект замирания поля (фединг) из-за:
  - изменения плотности ионосферы;
  - взаимодействия "пространственных" и "земного" лучей, пришедших в одну точку (рис.2.48).
- Используется для радиовещания и связи на флоте и в авиации.

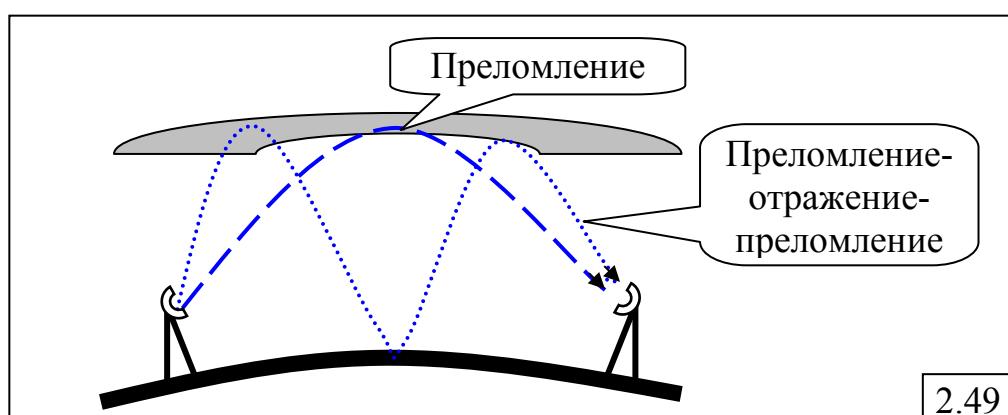
На волне  $\lambda = 600$  м передавался международный сигнал бедствия "SOS".

### Декаметровые волны:

- Диапазон длин волн (частот): 100 – 10 м (3 – 30 МГц).
- Явление дифракции несущественно из-за резкого возрастания потерь энергии при отражении от Земли (рис.2.49).



- Поле в точке приема создается в основном за счет преломления волн в ионизированном слое атмосферы (пунктирная линия на рис.2.49).
- Имеет место замирание поля и пропадание связи из-за преломления волн в ионосфере и взаимодействия лучей (рис.2.48 и рис.2.49).
- На создание поля влияют солнечные вспышки, рассеяние волн на мелких неоднородностях ионосферы, "расщепление" (разделение) лучей из-за наличия магнитного поля Земли.
- Применяются при создании протяженных (магистральных) линий радиосвязи и для любительской связи.



### **Метровые волны:**

- Диапазон длин волн (*частот*): 10 – 1 м (30 – 300 МГц).
- Практически отсутствует явление дифракции.
- Имеет место явление *рефракции волн в атмосфере*, когда волны распространяются не по прямым линиям, а по дугам.
  - На волнах короче 4 м начинает существенно сказываться явление *рассеяния радиоволн* на малых неоднородностях атмосферы и ионосферы, в результате чего поле оказывается очень слабым, но по-прежнему устойчивым.
  - При повышении мощностей передатчиков до нескольких киловатт можно осуществлять радиосвязь на расстояния до нескольких тысяч километров.

### **Дециметровые волны:**

- Диапазон длин волн (*частот*): 1 – 0,1 м (300 – 3000 МГц).
- Ионосфера для дециметровых волн полностью прозрачна – поле ею не преломляется, поэтому возможна связь с космическими объектами.
- Энергия поля значительно уменьшается из-за поглощения в каплях дождя, тумана, в молекулах кислорода и других газов.

### **Сантиметровые волны:**

- Диапазон длин волн (*частот*): 0,1 – 0,01 м (3 – 30 ГГц).
- Распространяются практически только в пределах прямой видимости.
  - Используются специальные остронаправленные антенны: параболические, рупорные и др.
  - Для волн короче 1,5 см начинают проявляться *процессы молекулярного поглощения* электромагнитного поля.

### **Миллиметровые и субмиллиметровые волны:**

- Диапазоны длин волн (*частот*): 0,01 – 0,001 м (30 – 300 ГГц) – миллиметровые волны и менее 0,001 м (более 300 ГГц) – волны субмиллиметровые.
  - Ослабление поля из-за поглощения в тумане и дожде возрастает до 30-100 дБ/км.
  - В настоящее время диапазон волн, используемых в беспроводной связи, простирается до:
    - инфракрасных: 100–0,75 мкм (3–400 ТГц);
    - видимых, генерируемых лазерами: 0,75–0,4 мкм (400–750 ТГц).
  - Поглощение в тумане и дожде инфракрасных и видимых волн может достигать сотен дБ/км, что означает их практическую неприменимость в открытом пространстве – их использование целесообразно в закрытых системах: волноводах и световодах.

**Метровые и дециметровые** волны используются в телевидении, радиовещании, для местной связи и навигации на аэродромах, для связи с подвижными объектами в городах.

На **сантиметровых** волнах работают: радиорелейные линии, радиолокационные системы, системы связи с космическими объектами.

При построении компьютерных сетей используются высокочастотные радиоволны, начиная с дециметрового диапазона частот: сантиметровые и миллиметровые.

### 2.5.2. Наземная радиосвязь

К техническим средствам наземной радиосвязи относятся:

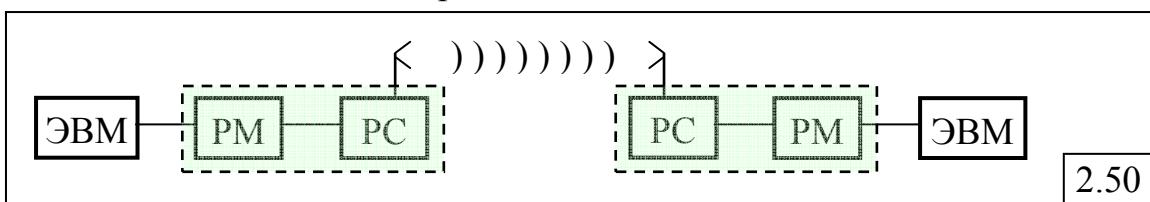
- радиостанции КВ- и УКВ-диапазонов;
- терминальные сетевые контроллеры – *радиомодемы*.

**Радиомодем** (PM) предназначен для управления обмена данными по радиоканалу и включается между ЭВМ и радиостанцией (PC) (рис.2.50).

PM обычно предоставляет следующие возможности:

- выбор скорости передачи;
- установка адреса получателя;
- регулировка чувствительности, предотвращающая прием фонового сигнала в отсутствие информативного.

Для предотвращения приема фонового сигнала в отсутствие информативного в радиомодеме встраивается регулятор чувствительности, который задает пороговое значение входного сигнала, при котором радиомодем включается на прием.



**Чувствительность** – пороговое значение входного сигнала, при котором PM включается на прием.

Конструктивно PM и PC обычно выполняются в виде одного устройства.

**Достоинства** использования наземной радиосвязи:

- сравнительно невысокая стоимость передачи данных, поскольку, несмотря на значительные начальные вложения по сравнению с телефонной связью, арендная плата за один радиоканал значительно ниже арендной платы за выделенный телефонный канал;
- возможность работы на одном радиоканале нескольких абонентов;
- возможность организации мобильной связи.

Типичным примером беспроводной наземной радиосвязи может служить беспроводная телефония, получившая название сотовой связи, обеспечивающая передачу не только речи, но и других типов данных, включая мультимедийные, а также выход в Интернет и другие телекоммуникационные сети.

В последнее десятилетие всё более широкое распространение получают беспроводные локальные вычислительные сети, реализуемые в рамках наземной радиосвязи. Отличительными особенностями таких сетей (по сравнению с «традиционной» наземной радиосвязью) являются:

- используемые диапазоны частот 1 и более ГГц;

- сравнительно небольшой территориальный охват (до нескольких сотен метров);
- специальные методы кодирования передаваемых данных.

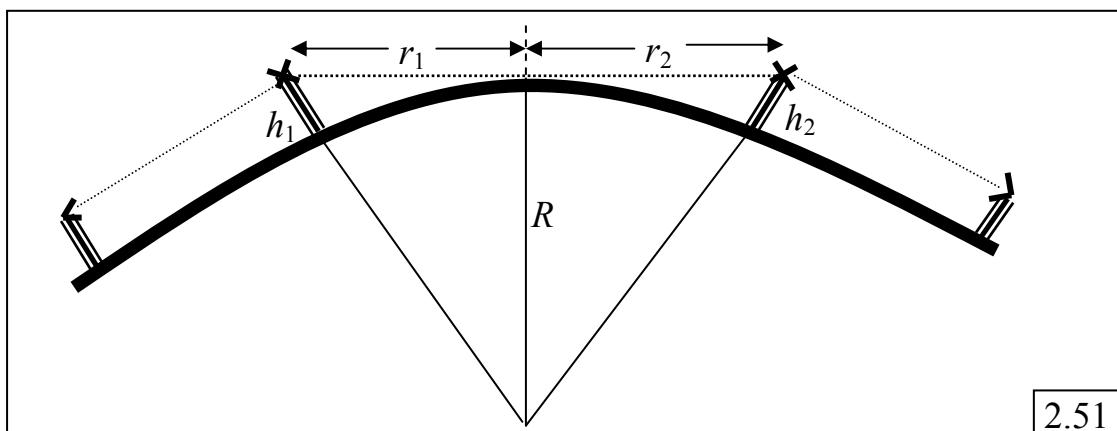
### 2.5.3. Радиорелейные линии связи

Радиорелейные линии связи (РРЛС) представляют собой цепочку приемно-передающих станций, антенны которых отстоят друг от друга на расстоянии прямой видимости. РРЛС использует **принцип ретрансляции**, когда каждая станция, входящая в РРЛС, принимает, усиливает и излучает сигнал в направлении соседней станции (рис.2.51).

Полагая, что Земля – шар, расстояние  $r$  между двумя находящимися на прямой видимости антеннами в случае гладкой поверхности Земли (равнина без леса или водная поверхность) определяется из условия (см. рис.2.51):

$$r = r_1 + r_2 = \sqrt{(R + h_1)^2 - R^2} + \sqrt{(R + h_2)^2 - R^2} = \sqrt{2Rh_1 + h_1^2} + \sqrt{2Rh_2 + h_2^2}$$

,  
где  $h_1, h_2$  – высота установки соответственно передающей и приемной антенн соседних станций;  $R$  – радиус земного шара.



Учитывая, что  $h_1^2 \approx h_2^2 \approx 0$  по сравнению с  $2Rh_1$  и  $2Rh_2$ , получим:

$$r \approx \sqrt{2Rh_1} + \sqrt{2Rh_2} = \sqrt{2R}(\sqrt{h_1} + \sqrt{h_2})$$

Принимая, что  $R \approx 6400$  км = 6 400 000 м, получим:

$$r \approx \sqrt{13\,000\,000} (\sqrt{h_1} + \sqrt{h_2}) [\text{м}] = 3,6 \cdot 1000 (\sqrt{h_1} + \sqrt{h_2}) [\text{м}] = 3,6 (\sqrt{h_1} + \sqrt{h_2}) [\text{км}].$$

Таким образом, в случае абсолютно гладкой земной поверхности расстояние (в километрах), обеспечивающее прямую видимость между антennами, может быть рассчитано по формуле:

$$r \approx 3,6 (\sqrt{h_1} + \sqrt{h_2}) [\text{км}],$$

где  $h_1, h_2$  – высоты установки соответственно передающей и приемной антенн соседних станций (в метрах).

При  $h_1 = h_2 = 100$  м получим:  $r \approx 72$  км.

Для передачи сигналов по РРЛС применяются остронаправленные антенны с большим коэффициентом усиления 30-40 дБ ( $10^3 - 10^4$  раз по мощности), что позволяет применять передатчики небольшой мощности (не более 10-20 Вт).

Для работы РРЛС выделяются частоты в области от 1 до 30 ГГц.

Достоинства этих диапазонов:

- 1) высокая пропускная способность;
- 2) высокая помехоустойчивость и надежность.

Для увеличения пропускной способности РРЛС на каждой станции обычно устанавливается несколько комплектов приемно-передающей аппаратуры, подключаемых к одной общей антенне и использующих разные несущие (рабочие) частоты. Цепочка станций с одним комплектом однотипной высокочастотной приемно-передающей аппаратуры, установленной на каждой станции (без модуляторов и демодуляторов), образуют так называемый **высокочастотный (ВЧ) ствол** РРЛС или **радиоствол**.

**Цифровые радиорелейные линии связи** (ЦРРЛС) предназначены для передачи высокоскоростных потоков цифровых данных, которые характеризуются широким спектром частот и требуют широких полос пропускания приемно-передающей аппаратуры. ЦРРЛС работают на частотах более 10 ГГц и в миллиметровом диапазоне волн с частотой от 30 ГГц до 300 ГГц. ЦРРЛС используются в многоканальных цифровых сетях связи и характеризуются высокой скоростью передачи данных.

## 2.5.4. Спутниковые системы связи

### 2.5.4.1. Общие сведения

В общем случае, под **спутниковой связью** понимают связь между земными станциями (ЗС) через космические станции (КС), представляющие собой пассивные искусственные спутники Земли (ИСЗ), реализующие функции ретранслятора.

Организационно-техническая совокупность ЗС связи различного базирования, КС (спутники-ретрансляторы) и автоматизированной системы управления образуют **спутниковую систему связи (ССС)**.

Спутники могут обеспечивать прямые каналы между двумя точками в сетях связи, разделяя пропускную способность канала посредством частотного или временного уплотнения. Однако более эффективным является способ организации, при котором каждому пользователю для передачи данных предоставляется вся полоса пропускания. При этом на одной частоте  $f_1$  формируется канал от земных станций к принимающей спутниковой станции, а на другой частоте  $f_2 \neq f_1$  – широковещательный канал к земным станциям от спутника, который ретранслирует пакеты, используя также всю полосу пропускания. Эти пакеты принимаются всеми земными станциями, находящимися в радиусе действия антенны спутника. Анализируя адрес, содержащийся в заголовке пакета, земная станция

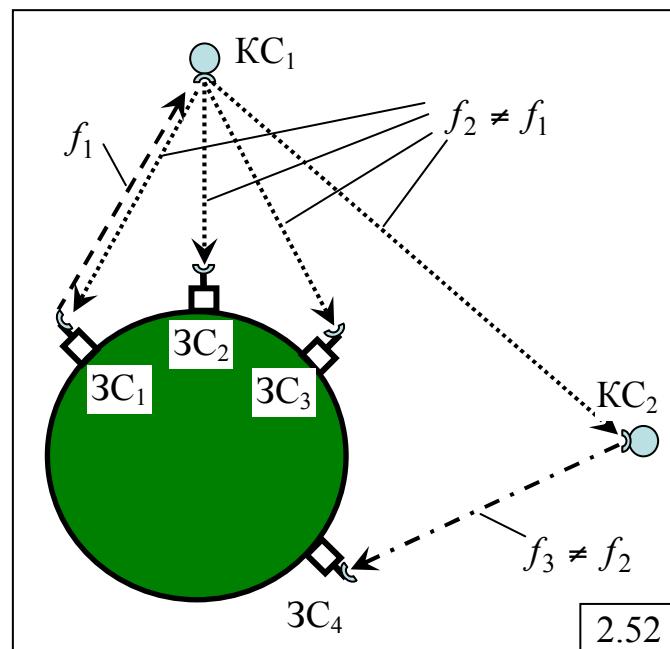
принимает те пакеты, которые предназначены непосредственно ей, и игнорирует остальные.

На рис.2.52 показан принцип реализации спутниковой связи. Земная станция  $3C_1$  передаёт пакет космической станции  $KC_1$  на частоте  $f_1$ , которая ретранслирует полученные данные на частоте  $f_2 \neq f_1$ . Все станции ( $3C_1, 3C_2, 3C_3$ ), находящиеся в зоне видимости  $KC_1$ , включая станцию отправитель  $3C_1$ , получают передаваемый пакет, то есть передача от  $KC_1$  к земным станциям реализуется по схеме «точка-многоточка». Земная станция, адрес которой указан в передаваемом пакете как адрес назначения, заносит этот пакет в буфер. Остальные ЗС игнорируют этот пакет.

Для передачи данных станции  $3C_4$ , находящейся вне зоны видимости  $KC_1$ , может использоваться ещё один спутник  $KC_2$ , который на частоте  $f_3 \neq f_2$  ретранслирует пакет, поступивший от  $KC_1$ .

Описанный принцип работы имеет много общего с наземными радиосистемами. Самое большое *различие* между спутниковыми и наземными радиосистемами состоит во времени распространения передаваемых сигналов. При нахождении геостационарного спутника на высоте около 36 000 км общее время распространения сигнала (к спутнику и обратно) составляет от 240 мс до 270 мс в зависимости от того, находится ли спутник в зените или вблизи горизонта, а с учетом мультиплексирования, коммутации и задержек обработки сигнала общая задержка может составлять до 400 мс. Благодаря высокой скорости передачи пакетов земная станция может успеть передать большое число пакетов, прежде чем первый из пакетов возвратится на Землю. Поэтому в спутниковых системах неприемлемы методы предотвращения столкновений пакетов с помощью контроля несущей, которые используются в наземных радиосистемах.

В спутниковой системе не нужен механизм подтверждения правильности принятых данных с помощью квитанций, поскольку все земные станции принимают пакеты от КС (в том числе и станция-источник  $3C_1$  на рис.2.52). Если станция-источник принимает свой пакет в том же виде, в каком он был передан космической станции, то это с высокой степенью вероятности свидетельствует о том, что пакет правильно принят станцией назначения. В то же время, правильный прием пакета станцией-



источником показывает, что столкновения пакетов в канале коллективного доступа не произошло. Конечно, ошибка может возникнуть в самой станции назначения. В этом случае она может запросить повторную передачу пакета.

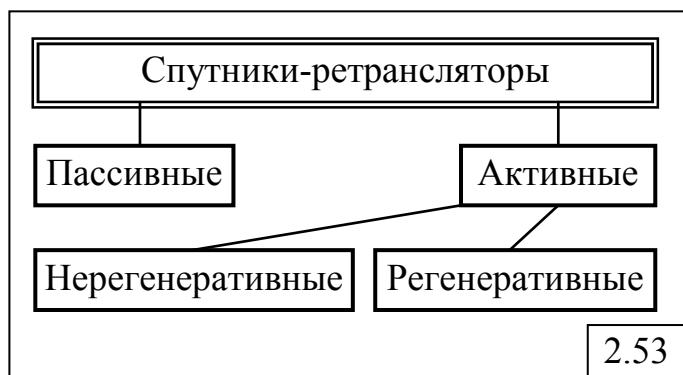
Спутники-ретрансляторы могут быть пассивными и активными (рис.2.53). Все современные спутники-ретрансляторы являются **активными**, которые в отличие от **пассивных**, представляющих собой простой отражатель радиосигнала, оборудованы аппаратурой для *приема, обработки, усиления и ретрансляции* сигнала.

Активные спутники могут быть нерегенеративными и регенеративными (рис.2.53).

**Нерегенеративный** спутник, приняв сигнал от одной земной станции, переносит его на другую частоту, усиливает и передает другой земной станции.

**Регенеративный** спутник производит демодуляцию принятого сигнала и заново модулирует его. Благодаря этому исправление ошибок производится дважды: на спутнике и на принимающей земной станции. Недостаток этого метода – сложность и, следовательно, более высокая стоимость, а также увеличенная задержка сигнала.

Один и тот же спутник связи может использоваться несколькими системами связи, имеющими свои комплексы ЗС.



Основные достоинства ССС:

- высокая пропускная способность;
- возможность перекрытия больших расстояний;
- возможность обеспечения связью труднодоступных районов;
- независимость стоимости и качества спутниковых каналов от их протяженности.

#### 2.5.4.2. Классификация спутниковых систем по типу орбиты

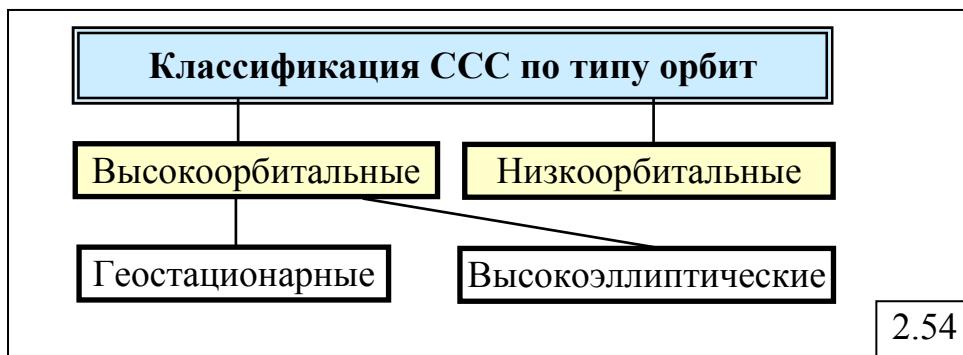
**Орбита** – траектория движения спутника связи.

ССС могут быть классифицированы в зависимости от типа орбит (рис.2.54).

**Высокоорбитальные ССС** используют *высокие* орбиты (диаметром десятки тысяч км), к которым относятся:

- геостационарная орбита;
- высокоэллиптическая орбита;
- **Низкоорбитальные ССС** используют низкие круговые орбиты, имеющие сравнительно небольшой диаметр (от нескольких сотен до

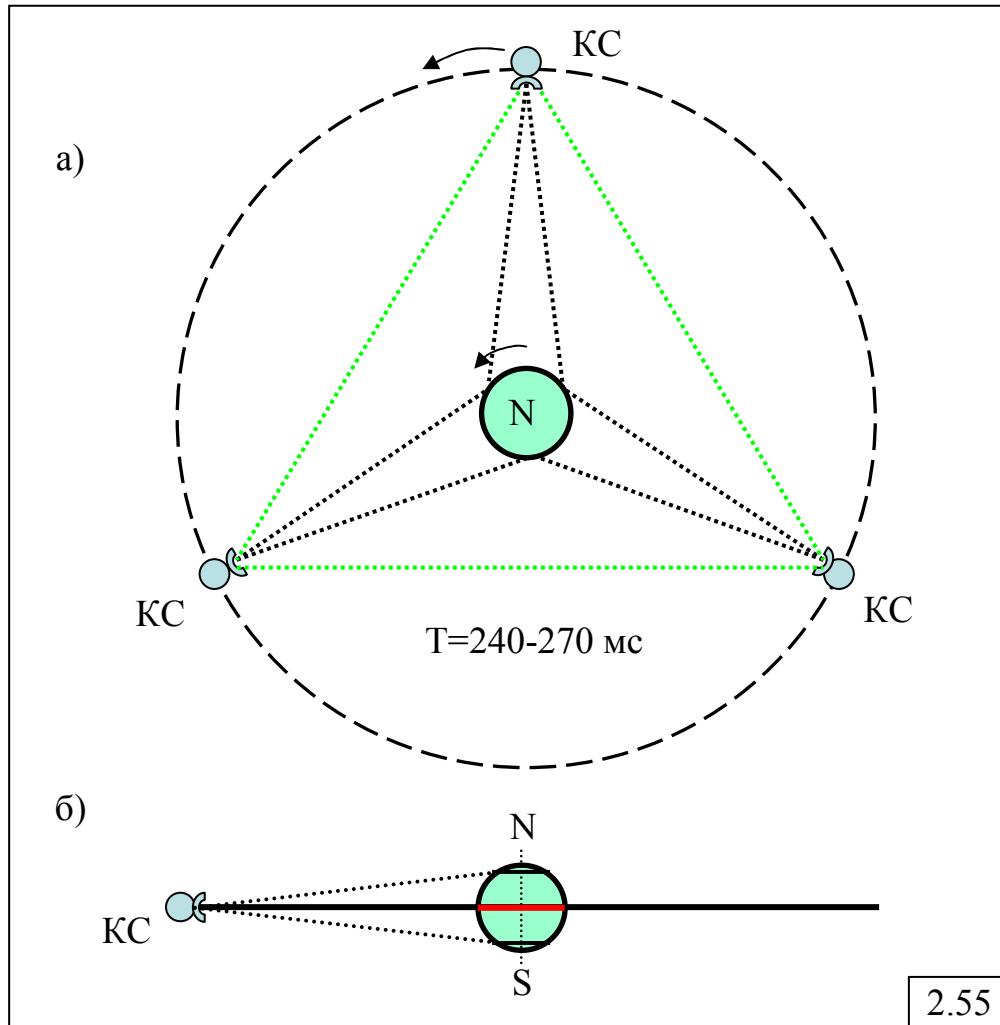
нескольких тысяч км), наклоненные под некоторым углом относительно экватора.



#### 2.5.4.3. Геостационарная орбита

**Геостационарная орбита** или орбита геостационарного спутника – это круговая (эксцентриситет эллипса  $e = 0$ ) экваториальная (наклонение – угол между плоскостью орбиты и плоскостью экватора –  $\alpha = 0$ ) синхронная орбита с периодом обращения 24 ч, с движением ИСЗ в восточном направлении (рис.2.55).

Геостационарный спутник оказывается "зависшим", неподвижным относительно земной поверхности. Он располагается над экватором на высоте 35 875 км с неизменной долготой подспутниковой точки.



**Достоинства геостационарных орбит:**

- 1) связь осуществляется непрерывно, круглосуточно, без переходов с одного ИСЗ на другой и без необходимости отслеживания антеннами положения спутника;
- 2) ослабление сигнала на трассе между ЗС и спутником является стабильным вследствие неизменности расстояния от ИСЗ до ЗС;
- 3) отсутствует или, по крайней мере, весьма мал сдвиг частоты сигнала со спутника связи, вызываемый его движением (эффект Доплера);
- 4) зона видимости геостационарного спутника – около трети земной поверхности, что обуславливает теоретическую достаточность трех ИСЗ для создания глобальной системы связи (см. рис.2.55,а).

Благодаря указанным преимуществам геостационарную орбиту используют очень широко.

Геостационарные спутники Земли стали использоваться для передачи информации на несколько лет раньше, чем возникли первые сети с коммутацией пакетов. Коммерческие спутники связи начали работать с 1965 г. Геостационарную орбиту используют спутниковые системы связи: ГОРИЗОНТ, ЭКРАН-М (Россия), INTELSAT; EUTELSAT и другие.

**Недостатки геостационарных орбит:**

- 1) в высоких широтах (больше 75 градусов) геостационарный спутник практически не виден (см. рис.2.55,б);
- 2) углы места наведения антенны на спутник дополнительно уменьшаются с удалением по долготе точки приема от долготы ИСЗ.

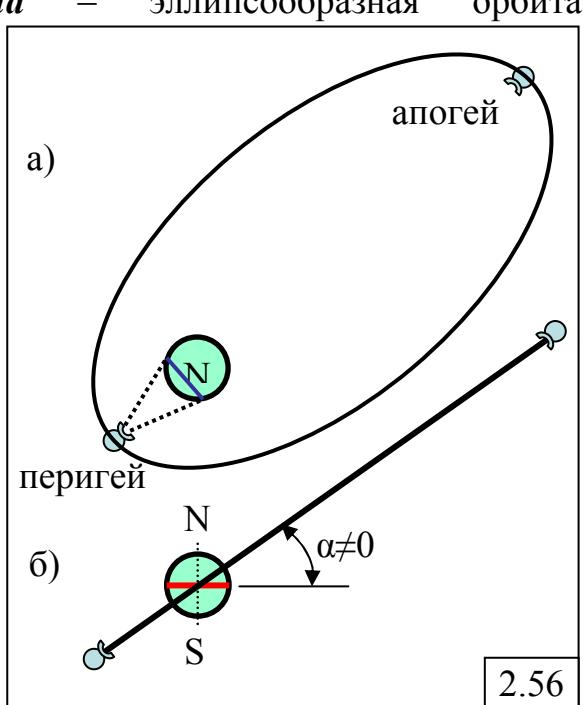
Все это приводит к необходимости использовать другие типы орбит для обеспечения спутниковой связью соответствующих районов Земного шара.

**2.5.4.4. Высокоэллиптическая орбита**

**Высокоэллиптическая орбита** (эксцентриситет эллипса не равен 0) с ненулевым наклонением (угол между плоскостью орбиты и плоскостью экватора отличен от 0) с периодом обращения 12 ч. Земля расположена в плоскости орбиты близко к одному из концов эллипса (рис.2.56).

**Апогей** – наиболее удалённая точка орбиты; **перигей** – наименее удалённая точка орбиты.

Высокоэллиптическая орбита используется с апреля 1965 года системами связи и вещания нашей страны при эксплуатации спутников связи типа "Молния". Обслуживание всей территории России возможно в



течение примерно 8 часов, поэтому трех-четырех ИСЗ, сменяющих друг друга, достаточно для организации круглосуточной радиосвязи.

Основное **достоинство** высокоэллиптической орбиты – организация связи для территорий, находящихся в высоких широтах.

#### **2.5.4.5. Низкоорбитальные ССС**

Для обеспечения связью потребителей с небольшим трафиком используются две концепции построения низкоорбитальных ССС:

- 1) использование малых низкоорбитальных спутников связи;
- 2) технология малоапertureных спутниковых терминалов (VSAT-технология).

**Системы малых низкоорбитальных спутников связи** представляют собой многоспутниковую (от десятка до нескольких сотен спутников) низкоорбитальную группу малых космических аппаратов, размещённых на круговых орбитах высотой от 600 до 2000 км и наклонением от 30 до 85 градусов. При этом для любой точки обслуживаемой области земной поверхности в зоне ее радиовидимости будет находиться хотя бы один космический аппарат.

*Достоинства* системы малых низкоорбитальных спутников связи:

- 1) сравнительно небольшие расстояния от ЗС до спутников-ретрансляторов приводят к:
  - значительному энергетическому выигрышу по сравнению с системами связи через высокоорбитальные спутники связи;
  - возможности применения земных станций с малой мощностью передатчика;
  - упрощению конструкции ретранслятора;
  - снижению массогабаритных показателей космического аппарата;
- 2) стоимость системы связи примерно на порядок ниже, чем связь через геостационарные ИСЗ.

Примеры систем малых низкоорбитальных спутников связи: IRIDIUM, GLOBALSTAR, TELEDESIC.

**Технология малоапertureных спутниковых терминалов** (VSAT – Very Small Aperture Terminal) заключается в разработке и использовании земных станций с очень малыми размерами антенн (диаметром 0,9–2,4 м) и усилителем высокой частоты небольшой мощности (1–5 Вт), находящимися непосредственно у абонента. Это позволяет существенно уменьшить габариты и стоимость таких станций и делает их доступными мелким и средним фирмам и компаниям.

С момента своего появления сети спутниковой связи наряду с проводными, радиорелейными, тропосферными и т.д. рассматривались в качестве так называемых **первичных сетей связи**, т.е. систем образования типовых каналов связи и групповых трактов передачи сигналов.

На базе типовых каналов первичных сетей организуются **вторичные сети связи** – телефонные, телеграфные, передачи данных, факсимильной

связи и др. Это обусловило определенную самостоятельность в разработке средств спутниковой связи и ориентирование при создании вторичных сетей на возможности и особенности спутниковых каналов связи.

### 2.5.5. Беспроводные сети на ИК-лучах

**Назначение:** для быстрого развертывания сетей и ноутбуков.

**Особенности построения и функционирования сетей на ИК-лучах:**

1) нет необходимости тянуть кабели, когда нет таких возможностей, например, в полевых условиях;

2) небольшой радиус действия: 5–10 м – в пределах одного помещения, что обеспечивает конфиденциальность;

3) излучаемая мощность невысока, а воздействие ИК-излучения на организм, в отличие от СВЧ, изучено предельно хорошо;

4) устойчивость к радиопомехам;

5) не требуется лицензирование частот.

**Технические характеристики:**

1) дальность работы приемо-передатчика (П):

- внутри помещения: 10 м – 20 м;

- между зданиями или внутри длинных коридоров: до 500 м;

2) рабочие длины волн: 800 – 900 нм (частоты 300 – 400 ТГц);

3) скорость передачи данных: до 10 Мбит/с;

4) концентратор (К) с охватом  $360^{\circ}$  (рис.2.57) обеспечивает одновременную работу с 255 станциями.

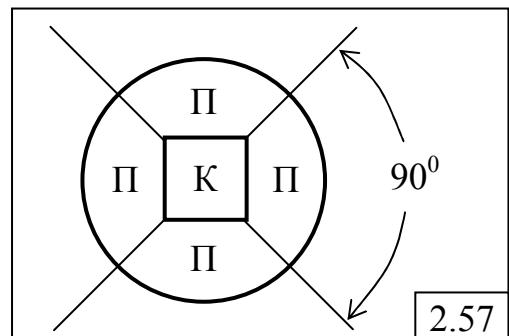
**Недостатки** сетей на ИК-лучах:

1) ПП требуют ручной ориентации друг на друга;

2) нет технических средств для мобильных пользователей;

3) малые расстояния;

4) зависимость от погодных условий (дождь, туман, снег).



Беспроводные сети на ИК-лучах не получили широкого распространения и в последние годы практически полностью вытеснены беспроводными сетями, использующими радиодиапазон.

## 2.6. Телекоммуникационные сети

### 2.6.1. Классификация телекоммуникационных сетей

В зависимости от вида передаваемых данных телекоммуникационные сети делятся на:

- аналоговые сети;
- цифровые сети.

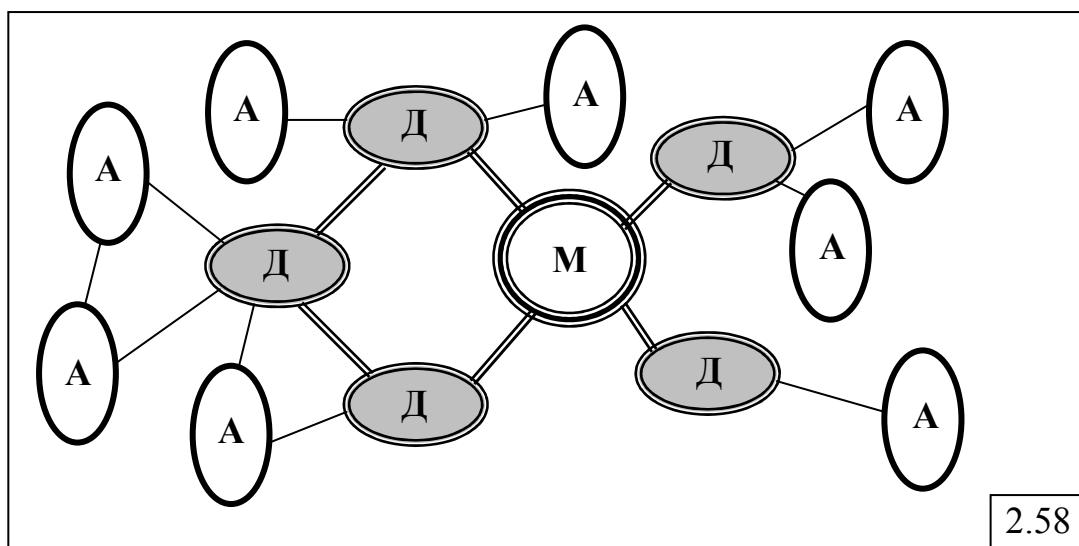
К современным телекоммуникационным сетям предъявляются два основных *требования*:

- интеграция – возможность передачи в сети данных разных типов (неоднородного трафика), предъявляющих разные требования к качеству передачи;

- высокие скорости передачи за счет использования широкополосных каналов связи (построения широкополосных сетей передачи данных).

В зависимости от назначения в структуре современных телекоммуникационных сетей выделяют несколько уровней иерархии (рис.2.58):

- абонентские сети (A)**, представляющие собой домашние, офисные и корпоративные сети на основе LAN или WAN;
- сети доступа (Д)**, объединяющие потоки от нескольких абонентских сетей в единый поток, направляемый в магистральную сеть;
- магистральная сеть (М)**, представляющая собой высокоскоростную широкополосную сеть на основе первичных транспортных сетей (волоконно-оптических, спутниковых и т.д.).



**Сети доступа** могут быть построены на основе:

- коммутуемых каналов* – традиционные аналоговые телефонные сети (ТФОП) и цифровые сети ISDN;
- выделенных каналов* – от аналоговых каналов ТЧ с полосой пропускания 3,1 кГц до цифровых каналов SDH с пропускной способностью десятки Гбит/с;
- коммутации пакетов* – технологии X25, Frame Relay, ATM, а также TCP/IP (Internet).

**Магистральные сети** строятся обычно на основе выделенных цифровых каналов с пропускными способностями до десятков Гбит/с.

Сети доступа и магистральные сети образуют транспортную (опорную) систему, назначение которой быстрая и надежная доставка данных.

Транспортные системы на основе выделенных каналов можно разбить на 2 класса: *цифровые (цикловые)* и *аналоговые (нециклические)*.

Аналоговые транспортные системы реализуются в основном на основе существующих телефонных каналов

Цифровые транспортные системы могут быть реализованы на основе следующих технологий:

- плезиохронные (PDH);
- синхронные (SDH);
- асинхронные (ATM).

## 2.6.2. Передача данных на основе телефонных сетей

Телефонная сеть объединяет телефонные станции разных уровней – сельские, городские, междугородние и т.д.

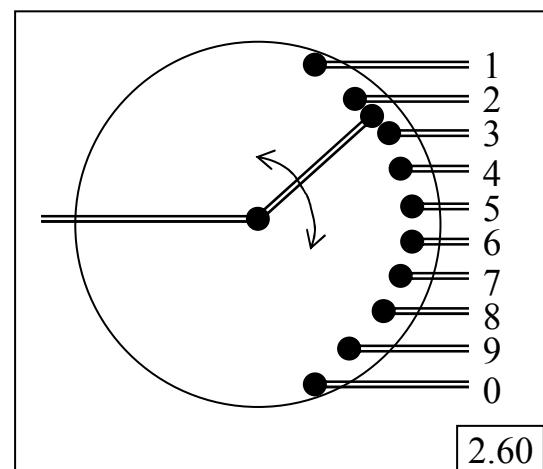
**АТС** – автоматическая телефонная станция, основной функцией которой является коммутация потока речевых (телефонных) данных. В общем случае, АТС можно рассматривать как пространственный коммутатор.

В процессе эволюции АТС прошли путь от *электромеханических станций* до современных станций *с программным управлением* (рис.2.59).



**Электромеханические АТС** представлены двумя типами станций.

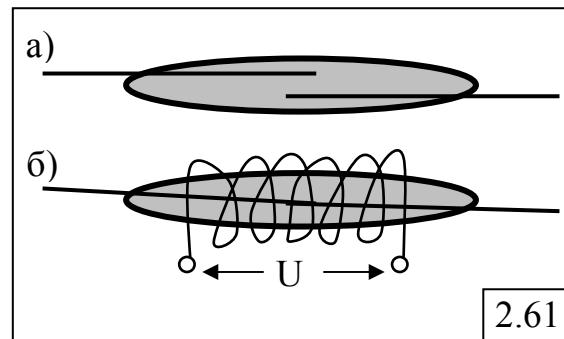
1. **Декадно-шаговые АТС**, в которых в качестве коммутационного элемента используется декадно-шаговый искатель – электромеханическое устройство, представляющее собой набор из 10 контактов, которые замыкаются бегунком в зависимости от поданного числа электрических импульсов, формируя электрическую цепь (рис.2.60). При подаче одного импульса бегунок замыкает контакт 1, двух – контакт 2, ..., десяти импульсов – контакт 0. Наличие подвижных электромеханических контактов обуславливает появление значительных помех, что существенно осложняет передачу цифровых данных и не позволяет достичь сколь-нибудь приемлемой скорости передачи.



**2. Координатные АТС**, в которых в качестве коммутационных устройств используются многократные координатные соединители (МКС), представляющие собой приборы релейного действия, имеющие по сравнению с декадно-шаговыми искателями более простое устройство, что позволяет уменьшить эксплуатационное обслуживание коммутационного оборудования и обеспечить более высокое качество коммутации разговорного тракта.

**АТС с программным управлением** также представлены двумя типами станций.

**1. Квазиэлектронные АТС**, в которых коммутационное устройство реализовано на основе герконов, а управление коммутационным устройством – средствами микропроцессорной техники. **Герконы** (сокращение от «герметичный контакт») представляют собой пару ферромагнитных контактов, запаянных в герметичную стеклянную колбу (рис.2.61,а), которые вместе с электромагнитной катушкой образуют герконовое реле. При прохождении тока через электромагнитную катушку контакты замыкаются, формируя электрическую цепь для передачи данных (рис.2.61,б).



2.61

**2. Цифровые (электронные) АТС**, в которых коммутация и управление полностью цифровые. Аналоговый сигнал оцифровывается в абонентском комплекте и передаётся внутри АТС и между АТС в цифровом виде, что гарантирует отсутствие затухания и уменьшает влияние помех на передаваемые данные. Это обеспечивает качественную передачу данных с максимальной возможной скоростью.

Упрощённо структуру электронной АТС можно представить в виде четырёх основных блоков (рис.2.62).

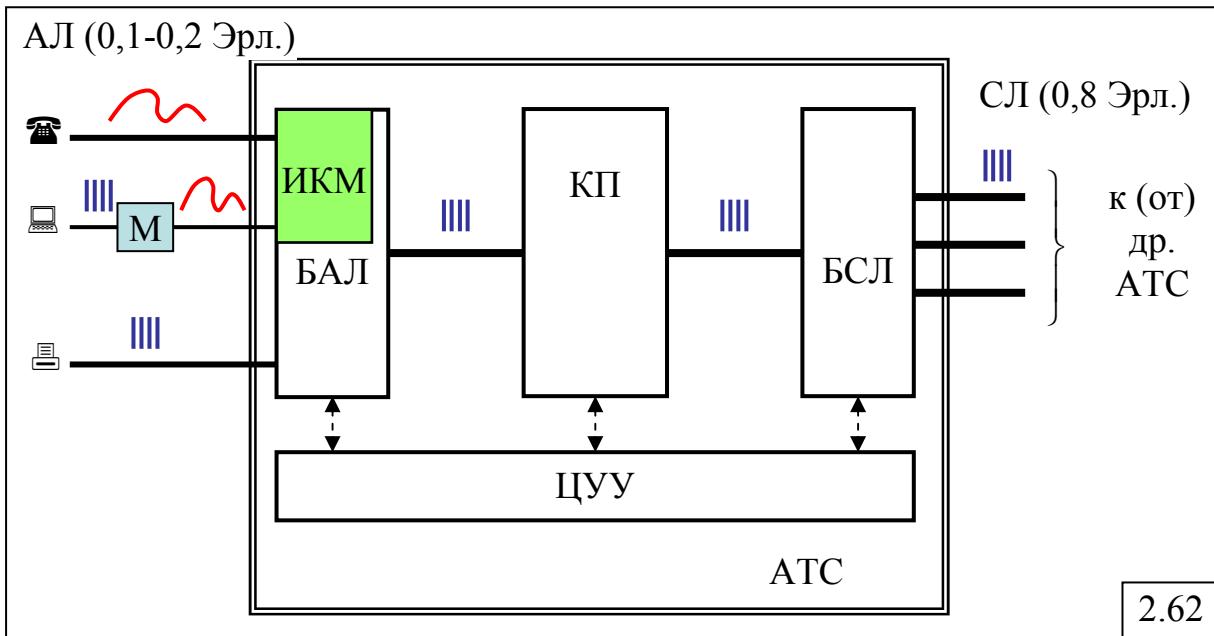
1. БАЛ – блок абонентских линий (АЛ), реализующий функции обслуживания абонентов, в качестве которых могут выступать:

- обычные аналоговые телефоны, передающие к АТС данные в виде непрерывных сигналов по аналоговым АЛ;
- компьютеры, дискретные сигналы от которых преобразуются с помощью модемов в непрерывные, передаваемые по аналоговым АЛ;
- цифровое оборудование (компьютеры, принтеры и т.п.), дискретные сигналы от которых передаются к АТС по цифровым АЛ.

Аналоговые сигналы, поступающие от абонентов с использованием ИКМ преобразуются в АТС в цифровой вид.

Уровень нагрузки в телефонии принято измерять в Эрлангах (Эрл.). Единица измерения нагрузки получила название в честь основоположника методов расчёта телефонной нагрузки.

Нагрузка на одну АЛ принимается равной 0,1-0,2 Эрл.



2. БСЛ – блок соединительных линий (СЛ), обеспечивающих связь с другими АТС. При связи с другой цифровой АТС сигналы по СЛ передаются в цифровом виде. Если же соседняя АТС является аналоговой, то цифровые сигналы преобразуются в аналоговый вид.

При расчёте необходимого количества СЛ нагрузка на одну СЛ принимается равно 0,8 Эрл.

3. КП – коммутационное поле может быть реализовано либо в виде некоторого электронного коммутатора, либо в виде «речевого запоминающего устройства» (РЗУ). В последнем случае речь, представленная в цифровом виде сначала записывается в РЗУ, а затем передаётся в соответствующую АЛ к абоненту-получателю или в СЛ к другой АТС.

4. ЦУУ – цифровое управляющее устройство предназначено для управления оборудованием АТС (БАЛ, БСЛ, КП), потоками данных в станции и всей АТС в целом.

Современные цифровые АТС строятся в соответствии с принципом коммутации пакетов и реализуют передачу данных на основе протокола IP. Таким образом, современная АТС представляет собой фактически большой специализированный компьютер, реализующий функции коммутатора, который может входить в состав цифровой сети передачи данных. При этом через АТС могут передаваться не только речевые (телефонные) данные, но и компьютерные данные, а также аудио и видео.

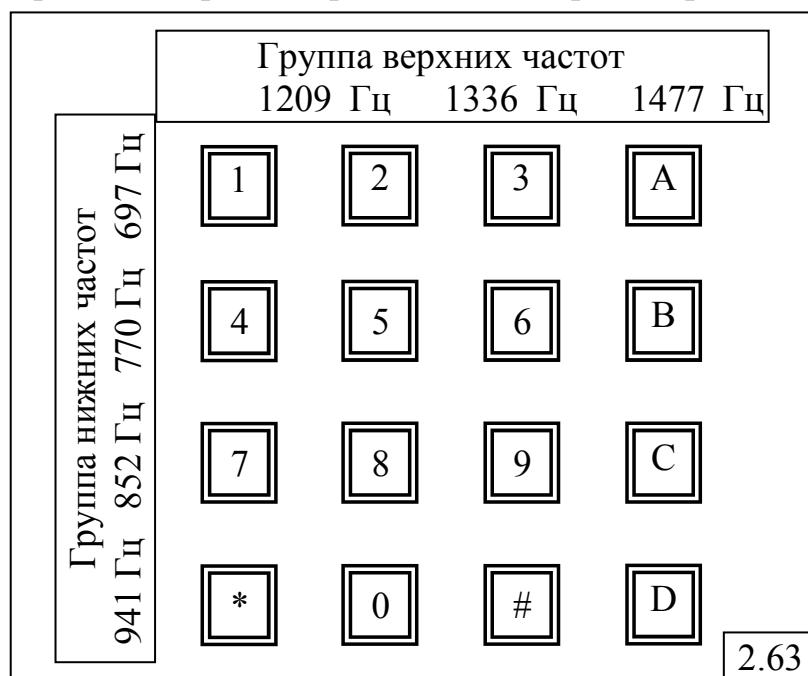
В зависимости от времени существования телефонные каналы могут быть двух типов:

- *коммутируемые* или *временные*, создаваемые только на время передачи данных;

- *выделенные* или *постоянные*, создаваемые на длительный промежуток времени и существующие не зависимо от того, передаются данные или нет.

В случае коммутируемых телефонных каналов подключение абонентов к АТС или сети может выполняться путём набора номера одним из двух способов:

- **импульсный (декадный)** способ, при котором набор цифры номера приводит к формированию импульсов с частотой 10 Гц: длительность импульса 50 мс и длительность паузы 50 мс, причём количество импульсов равно значению цифры (цифре «0» соответствует 10 импульсов);
- **тоновый (частотный)** способ, при котором набор абонентом номера приводит к формированию сигналов с частотой 10 Гц, причём каждой цифре соответствует сигнал определённой частоты; для повышения надёжности распознавания для каждого сигнала (для каждой цифры) используются 2 частоты – из нижней и верхней группы частот, значения которых подобраны определенным образом (рис.2.63).



Благодаря широкому распространению телефонных сетей связи, они находят массовое применение в качестве средств доступа к ресурсам цифровых сетей и для выхода в Интернет. При этом передача компьютерных данных может выполняться:

- по аналоговым АЛ;
- по цифровым АЛ.

Передача цифровых данных по аналоговым АЛ реализуется на частотах разговорного канала с применением модемов, причем максимальная скорость передачи – 56 кбит/с достигается только в том случае, если на пути передачи данных все АТС – цифровые.

Цифровая АЛ может обеспечить гораздо большие скорости передачи и с меньшей стоимостью, чем при связи в полосе тональных частот.

*К преимуществам цифровых АЛ перед аналоговыми относятся:*

- легкость мультиплексирования нескольких разговорных каналов по принципу временного уплотнения;
- простота кодирования;
- новые возможности абонентской сигнализации.

*Недостатками цифровой передачи являются:*

- искажения при преобразовании речевых сигналов в цифровой вид;
- более жесткие требования к полосе пропускания;
- проблемы с эхом из-за увеличения задержек.

### **2.6.3. Модемная связь**

#### **2.6.3.1. Принципы организации модемной связи**

Методы передачи данных по телефонным каналам с использованием модемов задаются в виде **рекомендаций (стандартов)** серии V.

Модемы должны обеспечивать защиту передаваемых данных от ошибок, возникающих в каналах связи и в аппаратуре передачи данных, путем контроля и коррекции ошибок.

**Коррекция ошибок** (error correction) – отделение полезного сигнала от шумов и исправление возникающих в процессе связи ошибок.

Для контроля и коррекции ошибок при передаче данных используются **протоколы контроля ошибок**, в частности, протокол сетевого обмена MNP (Microcom Network Protocol), который стал частью **стандарта коррекции ошибок V.42**.

Модемы при передаче данных используют алгоритмы сжатия данных, что повышает скорость обмена и уменьшает время передачи.

**Сжатие данных** (data compression) – кодирование информации с целью уменьшения её объёма.

При передаче данных по телефонному каналу используются средства для *автоматической упаковки-распаковки данных*.

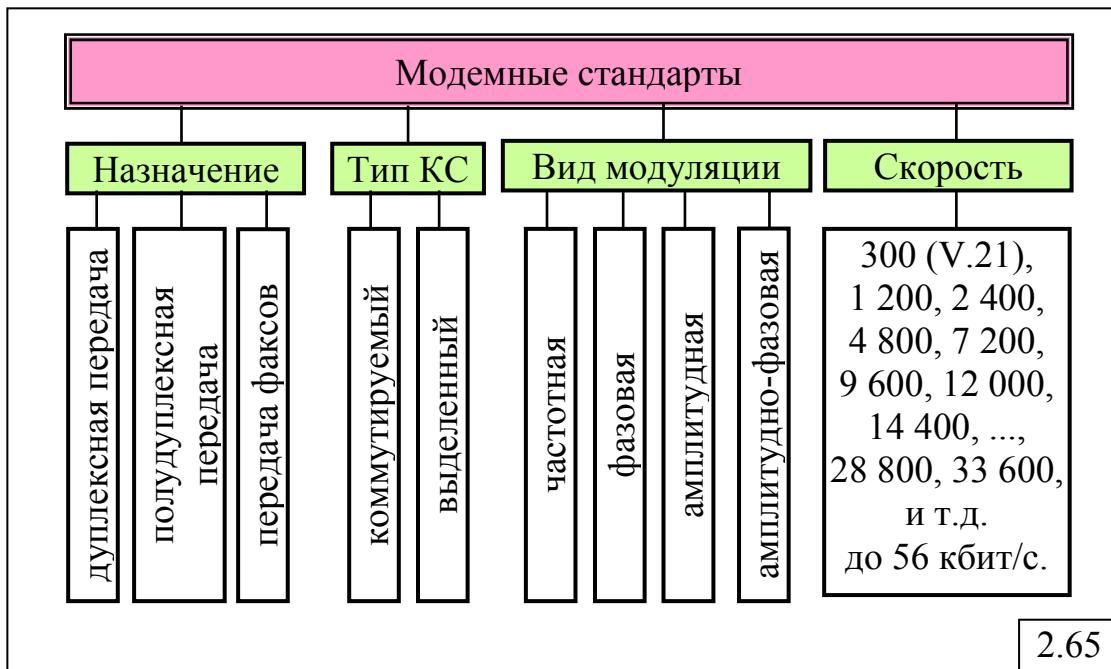
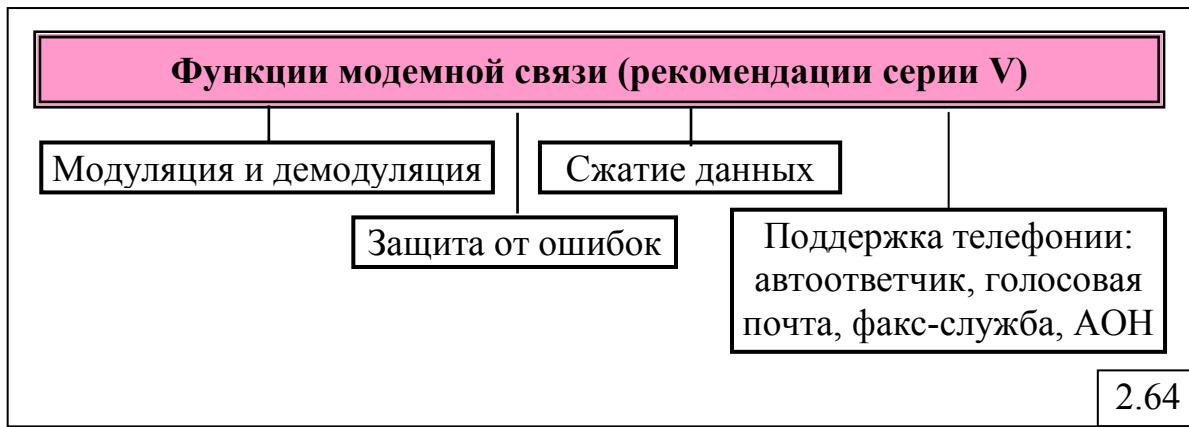
Стандарт **TAPI** (Telephony Application Programming Interface) – описывает взаимодействие ПК с телефонной линией и позволяет интегрировать в приложения для ПК обращения к услугам телефонной связи: от простого набора номера до блокировки звонков, переадресации вызовов и конференцсвязи.

На рис.2.64 перечислены основные функции модемной связи, сформулированные в рекомендациях серии V.

#### **2.6.3.2. Модемные стандарты**

Модемные стандарты серии V по передаче данных по телефонным линиям определяют (рис.2.65):

- 1) назначение;
- 2) тип канала связи;
- 3) вид модуляции;
- 4) скорость передачи.



### 2.6.3.3. Классификация модемов

На рис.2.66 представлена классификация модемов по:

- функциональному назначению;
- конструктивному исполнению;
- способу передачи данных;
- способу реализации протоколов.

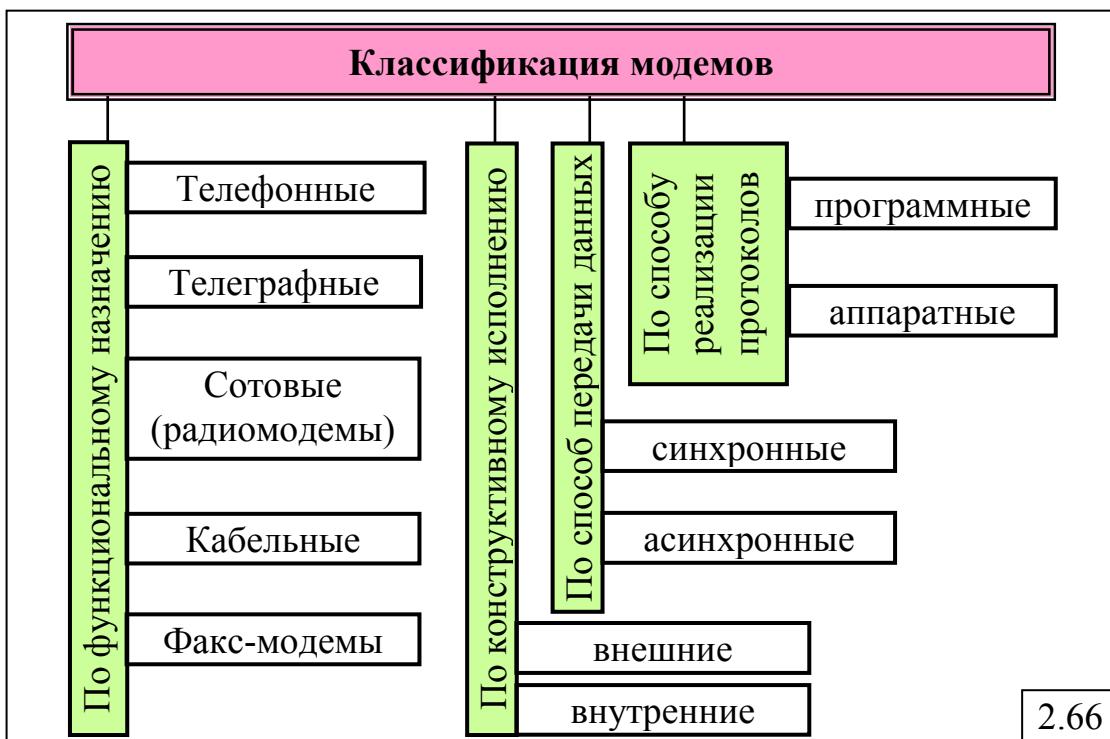
1. По **функциональному назначению** модемы делятся на:

- телефонные;
- телеграфные;
- сотовые (радиомодемы);
- факс-модемы;

д) *кабельные*, предназначенные для передачи данных по кабельным линиям связи, в частности по сети кабельного телевидения со скоростью до 10 Мбит/с

2. По **конструктивному исполнению** модемы могут быть:

- внешние, подключаемые кабелем к разъему RS-232 персонального компьютера;
- внутренние – в виде платы, устанавливаемой внутри компьютера.



3. По способу передачи данных (принципу работы в линии) модели делятся на:

а) *синхронные*, использующие синхронный способ передачи данных, при котором каждый бит посыпается через фиксированный интервал времени с использованием синхронизации приемного и передающего устройства; синхронизация обеспечивается путем передачи управляющей информации и использования в обоих устройствах тактовых генераторов; синхронный режим целесообразно применять при организации связи по типу "точка-точка" через выделенные каналы связи;

б) *асинхронные*, использующие асинхронный способ передачи данных, при котором каждый символ (реже слово или небольшой блок) посыпается отдельно и между данными могут быть произвольные промежутки времени; для распознавания поступающих данных каждый переданный элемент содержит стартовый и стоповый биты; этот способ известен также как старт-стоповая передача; модем работает в асинхронном режиме при использовании коммутируемых каналов связи;

4. По способу реализации протоколов коррекции ошибок и сжатия данных модемы бывают:

- с аппаратной реализацией;
- с программной реализацией.

#### **2.6.4. Цифровые сети с интегральным обслуживанием (ISDN-технология)**

Модемная передача компьютерных данных по абонентским линиям телефонных сетей позволяет в идеальных условиях (на пути передачи имеются только цифровые АТС и все каналы связи высокого качества) достичь предельной скорости в 56 кбит/с, что явно не достаточно для

передачи мультимедийных данных, в частности видео, со сколь-нибудь приемлемым качеством. Для обеспечения более высоких скоростей передачи данных по АЛ была разработана технология, получившая название ISDN.

**Цифровые сети с интегральным обслуживанием – ЦСИО (Integrated Services Digital Networks – ISDN)** – цифровая сеть, построенная на базе телефонной сети связи, в которой могут передаваться сообщения разных видов – данные, а также оцифрованные видеоизображения и речь.

Обычная телефонная связь ориентирована на передачу голоса и позволяет модемам обмениваться данными со скоростью не выше 56 кбит/с. ISDN разработана специально для того, чтобы обойти ограничение по скорости передачи данных, но сохранить совместимость с существующими телефонными сетями.

Сеть ISDN совместима "сверху вниз" с телефонными сетями: можно позвонить с обычного телефона на номер ISDN и в обратном направлении в режиме "голосовая связь", а передача данных со скоростью 64 кбит/с и выше возможна только между двумя терминалами ISDN.

Существенная особенность ISDN – это **многоканальность**, т.е. возможность передавать данные и речь одновременно. Поскольку в интерфейсе ISDN предусмотрен служебный канал, режим передачи может быть изменен без разрыва соединения.

ISDN по сравнению с обычной модемной связью обеспечивает:

- более высокую скорость передачи данных;
- более высокую надежность;
- принципиально иное качество взаимодействия между абонентами.

**Преимущества** сетей ISDN:

1) *сокращение времени установления соединений* за счет использования выделенного канала сигнализации и передачи по нему сигналов управления и взаимодействия (занятие линии, набор номера, ответ, разъединение и т.д.) в цифровом виде;

2) *универсальность использования линий* – возможность осуществлять по одним и тем же линиям как телефонные переговоры, так и передачу данных;

3) *сопряжение служб* – возможность организации телетекста, телекса или телефакса с соответствующим устройством в любой точке земного шара.

ISDN одновременно предоставляет различные виды связи:

- телефонную;
- модемную;
- по выделенному каналу связи.

ISDN целесообразно применять в тех случаях, когда необходимо *периодически* (но не постоянно) передавать *средние и большие объемы данных на любые расстояния с высокой скоростью и надежностью*.

Реализация ISDN осуществляется в соответствии с рекомендациями ITU-T серии I.

**Абонентское оборудование и интерфейсы ISDN** показаны на рис.2.67, где:

TE1 – терминальное оборудование ISDN;

TE2 – несовместимое с ISDN терминальное оборудование;

ТА – терминальный адаптер;

NT1 – сетевое окончание уровня 1 (подача питания к абонентской установке, обеспечение ТО линии и контроля рабочих характеристик, синхронизация, мультиплексирование на 1-м (физическом) уровне, разрешение конфликтов доступа); представляет собой обычно настенную коробку;

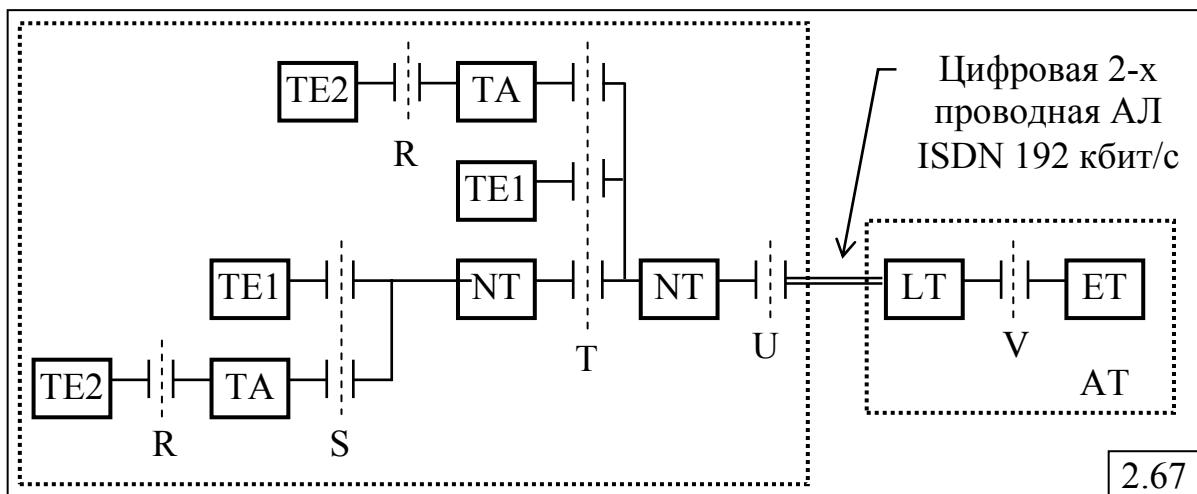
NT2 – сетевое окончание уровня 2 (функции 2-го и 3-го уровней: мультиплексирование, коммутация и концентрация, а также функции ТО и некоторые функции 1-го уровня); в качестве функционального блока NT2 могут выступать УАТС, локальная сеть или терминальный адаптер;

(функции NT1 и NT2 могут объединяться в едином физическом оборудовании, обозначаемом просто NT);

LT – линейное окончание;

ET – станционное окончание.

R, S, T, U, V – интерфейсы ISDN, в частности R-интерфейс связывает несовместимое с ISDN оборудование TE2 с ТА.



В отличие от традиционных телефонных сетей управляющая информация передаётся по специальным каналам, не загружая каналы передачи данных.

В ISDN различают два типа канала:

- **канал B** – для передачи голоса и данных с пропускной способностью 64 кбит/с;

- **канал D** – служебный (сигнальный) канал передачи управляющей информации. Один канал типа D обслуживает 2 или 30 В-каналов и обеспечивает возможность быстрой генерации и сброса вызовов, а также передачу информации о поступающих вызовах, в том числе о номере обращающегося к сети абонента.

Стандарты определяют **3 интерфейса доступа к ISDN** (типа ISDN):

- 1) базовый – BRI;

- 2) первичный – PRI;
- 3) широкополосный – B-ISDN.

**Интерфейс BRI** (Basic Rate Interface) – стандартный (базовый) интерфейс, обозначаемый как (2B+D). Это означает, что для передачи данных используется 2 канала B со скоростью передачи 64 кбит/с по каждому каналу и 1 служебный (сигнальный) канал D со скоростью передачи 16 кбит/с. Таким образом, пропускная способность интерфейса BRI равна:  $2 \cdot 64 \text{ кбит/с} + 1 \cdot 16 \text{ кбит/с} = 144 \text{ кбит/с}$ .

BRI предназначен для подключения телефонной аппаратуры (телефонов, факсов, автоответчиков и т.п.) и компьютеров к ISDN.

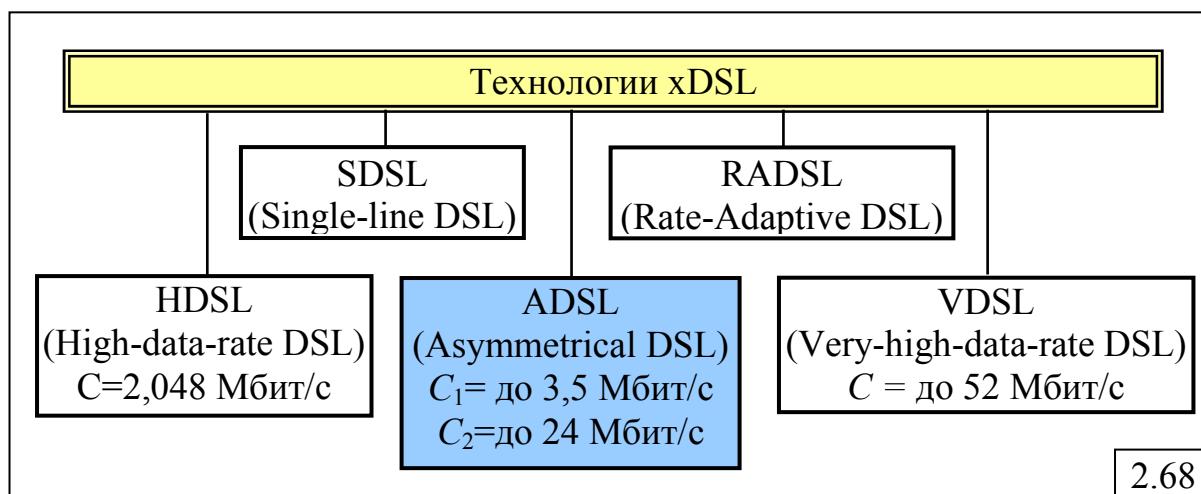
**Интерфейс PRI** (Primary Rate Interface) объединяет несколько BRI и соединяется с узлом. В зависимости от конкретных местных стандартов он включает в себя 23 B-канала (США и Япония) или 30 B-каналов (Европа), поддерживая интегральные скорости передачи данных 1,544 Мбит/с и 2,048 Мбит/с соответственно.

**B-ISDN** (Broadband ISDN) обеспечивает высокие скорости передачи (155 Мбит/с и 622 Мбит/с), что позволяет реализовать передачу видеоданных.

## 2.6.5. Технологии xDSL

**xDSL (Digital Subscriber Line)** – технологии передачи цифровых данных по телефонным каналам связи, обеспечивающие гораздо более высокие скорости передачи по обычным медным проводам, чем традиционная модемная связь и ISDN. Высокие скорости достигаются за счет использования ряда технических решений, в частности эффективных линейных кодов и адаптивных методов коррекции искажений на линии.

xDSL объединяет различные технологии (рис.2.68), которым в абривиатуре xDSL соответствуют разные значения символа «x». Эти технологии различаются в основном по используемому способу модуляции и скорости передачи данных.



**HDSL (High-data-rate DSL)** – высокоскоростная цифровая абонентская линия, обеспечивающая симметричную дуплексную передачу

данных по двум телефонным парам со скоростями до 2,048 Мбит/с в каждом направлении на расстояние до 4,5 км.

**SDSL (Symmetrical DSL)** – однопарная версия HDSL, обеспечивающая симметричную дуплексную передачу цифрового потока со скоростью 2048 кбит/с по одной паре телефонного кабеля.

**ADSL (Asymmetrical DSL)** – асимметричная цифровая абонентская линия, позволяющая по одной паре телефонного кабеля передавать данные от пользователя в сеть на скоростях от 16 кбит/с до 3,5 Мбит/с и в обратном направлении из сети к пользователю со скоростями до 24 Мбит/с на максимальное расстояние до 5,5 км.

**RADSL (Rate-Adaptive ADSL)** – ADSL с адаптируемой скоростью, учитывающей характеристики конкретной линии (длина, соотношение сигнал-шум и т.п.), за счет чего достигается максимальная пропускная способность в реальных условиях.

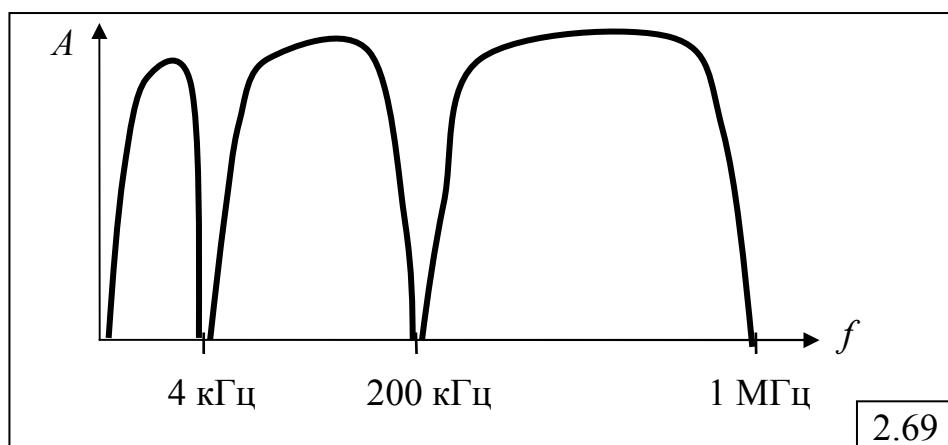
**VDSL (Very-high-data-rate DSL)** – сверхвысокоскоростная цифровая абонентская линия, имеющая по сравнению с ADSL значительно более высокие скорости передачи данных: до 56 Мбит/с в направлении от сети к пользователю и до 11 Мбит/с от пользователя к сети при работе в асимметричном режиме и при работе в симметричном режиме – примерно 26 Мбит/с в каждом направлении при максимальном расстоянии до 1,3 км.

Наиболее распространённой технологией является ADSL, основные принципы организации которой рассматриваются ниже.

Увеличение скорости передачи данных в ADSL обусловлено предоставлением пользователю большей полосы пропускания абонентской линии, чем при традиционной телефонной связи: 1 МГц вместо 3100 Гц. Это достигается за счёт исключения на пути передачи данных фильтров, ограничивающих полосу телефонного канала в интервале от 300 Гц до 3400 Гц.

В пределах полосы в 1 МГц формируется 3 частотных диапазона для передачи трёх потоков данных (рис.2.69):

- телефонных (голосовых) в диапазоне частот от 300 Гц до 4 кГц;
- компьютерных от пользователя в сеть в диапазоне частот от 4 кГц до 200 кГц;
- от сети к пользователю в диапазоне частот от 200 кГц до 1 МГц.



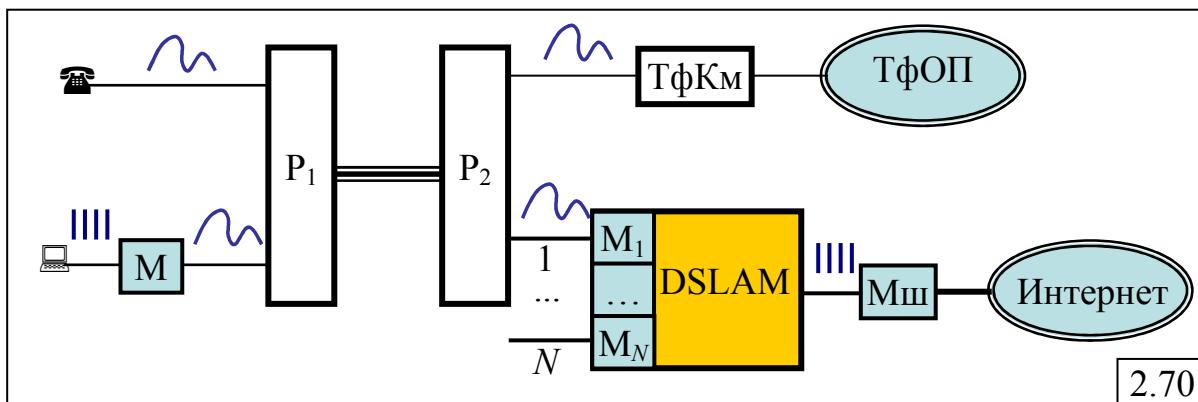
Таким образом, для передачи цифровых данных формируются два **асимметричных** частотных каналов:

- высокоскоростной (до 24 Мбит/с) нисходящий канал передачи данных из сети в компьютер пользователя;
- низкоскоростной (от 16 кбит/с до 3,5 Мбит/с) восходящий канал передачи данных из компьютера в сеть.

Третий канал предназначен для передачи телефонных разговоров.

Асимметричность каналов для передачи компьютерных данных обусловлена тем, что традиционно объём передаваемых данных от пользователя в сеть гораздо меньше объёма данных, передаваемых в обратном направлении. Отметим, что при необходимости можно изменять границы частотных диапазонов для перераспределения скоростей передачи данных в исходящем и восходящем каналах.

На рис.2.70 представлена схема организации ADSL.



2.70

Оборудование пользователя (телефон и компьютер на схеме) подключается к точке доступа – *распределителю* P<sub>1</sub>, выделяющему определённую полосу частот для передачи голосовых сигналов от аналогового телефона и данных от компьютера. Компьютер подключается к распределителю через ADSL-модем (M), осуществляющему модуляцию, то есть преобразование сигнала из цифрового вида в аналоговый. На другом конце к распределителю P<sub>2</sub>, отделяющему потоки компьютерных данных от голосовых сигналов, подключены *телефонный коммутатор* (ТфКм), обеспечивающий доступ в телефонную сеть общего пользования (ТфОП), и *мультиплексор доступа к цифровой абонентской линии* (DSLAM – DSL Access Multiplexer), который преобразует сигнал из аналогового вида в цифровой вид (демодуляция) и направляет его к маршрутизатору, обеспечивающему доступ в Интернет. Количество N ADSL-модемов M<sub>1</sub>,...,M<sub>N</sub>, входящих в состав DSLAM, определяет количество пользователей, которые могут быть подключены к DSLAM.

Высокие скорости передачи данных и сравнительно невысокая стоимость абонентской платы для пользователей делают технологии xDSL наиболее перспективными для организации доступа в Интернет, полностью вытесняющими традиционную модемную связь и ISDN.

## 2.6.6. Мобильная телефонная связь

Мобильная телефонная связь относится к средствам беспроводной связи и может быть двух типов:

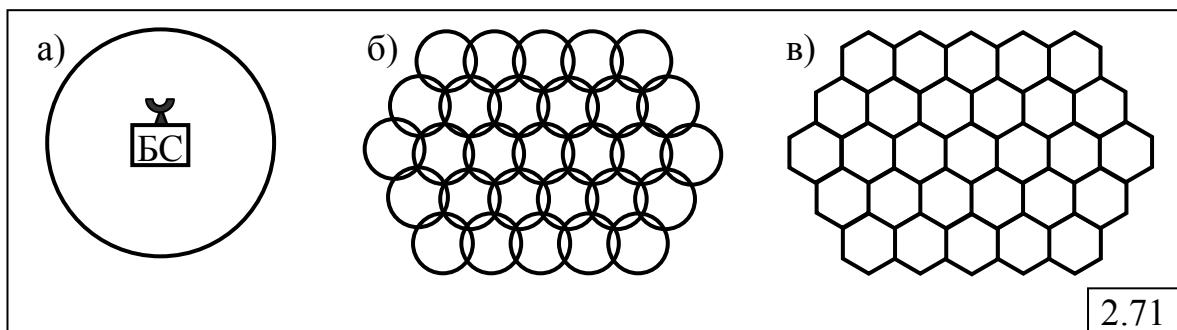
- домашние *радиотелефоны*;
- мобильные *сотовые телефоны*.

**Радиотелефоны** обеспечивают ограниченную мобильность в пределах одного или нескольких рядом расположенных помещений и состоят из базовой станции и одной или нескольких переносных трубок.

Значительно большую, практически неограниченную, мобильность обеспечивает **мобильная сотовая связь**, которая в настоящее время позволяет передавать, кроме голоса, цифровые данные и даже видео.

### 2.6.6.1. Принципы организации сотовой связи

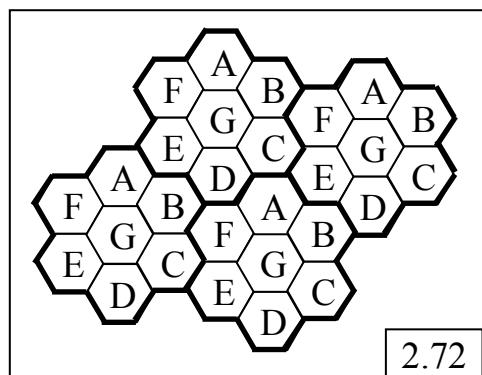
Основной принцип сотовой связи заключается в разделении всей зоны охвата телефонной связью на ячейки, называемые сотами. В центре каждой соты находится базовая станция (БС), поддерживающая связь с мобильными абонентами (сотовыми телефонами), находящимися в зоне её охвата. Базовые станции обычно располагают на крышах зданий и специальных вышках. На идеальной (ровной и без застройки) поверхности зона покрытия одной БС представляет собой круг (рис.2.71,а), диаметр которого не превышает 10-20 км. Соты частично перекрываются и вместе образуют сеть (рис.2.71,б), которая для простоты обычно изображается в виде множества шестиугольных сот (рис.2.71,в).



2.71

Каждая сотовая связь работает на своих частотах, не пересекающихся с соседними (рис.2.72). Все соты одного размера и объединены в группы по 7 сот. Каждая из букв (A, B, C, D, E, F, G) соответствует определённому диапазону частот, используемому в пределах одной соты. Соты с одинаковыми диапазонами частот разделены сотами, работающими на других частотах. Небольшие размеры сот обеспечивают ряд преимуществ по сравнению с традиционной наземной беспроводной связью, а именно:

- большое количество пользователей, которые одновременно могут работать в сети в разных частотных диапазонах (в



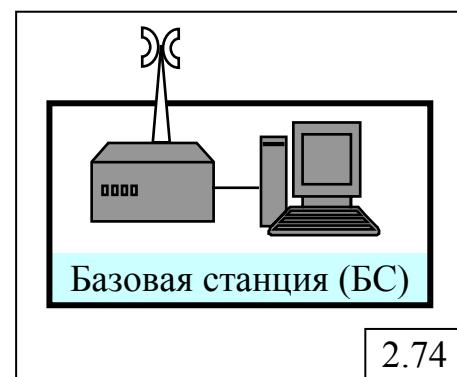
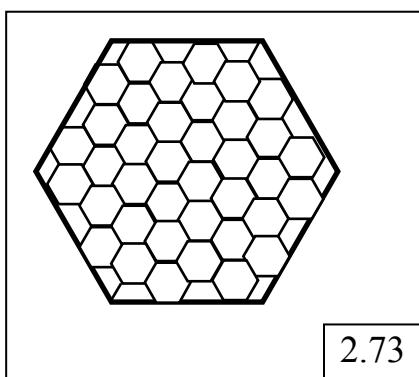
2.72

разных сотах);

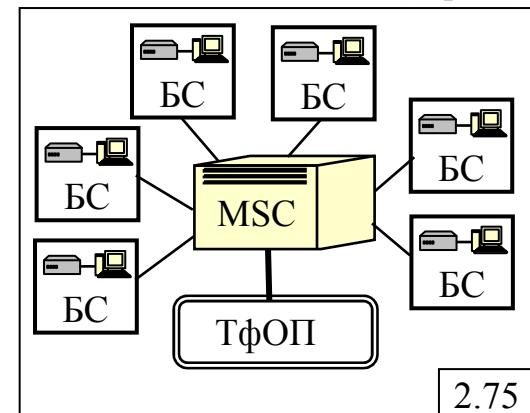
- небольшая мощность приемно-передающего оборудования, обусловленная небольшим размером сот (выходная мощность телефонных трубок составляет десятые доли ватт);
- меньшая стоимость устройств сотовой связи как маломощных устройств.

Если в какой-то соте количество пользователей оказывается слишком большим, то она может быть разбита на соты меньшего размера, называемые микросотами, как это показано на рис.2.73.

Базовая станция, в общем случае, содержит приёмопередатчик (ПП), поддерживающий связь с мобильными телефонами, и компьютер, реализующий протоколы беспроводной мобильной связи (рис.2.74).

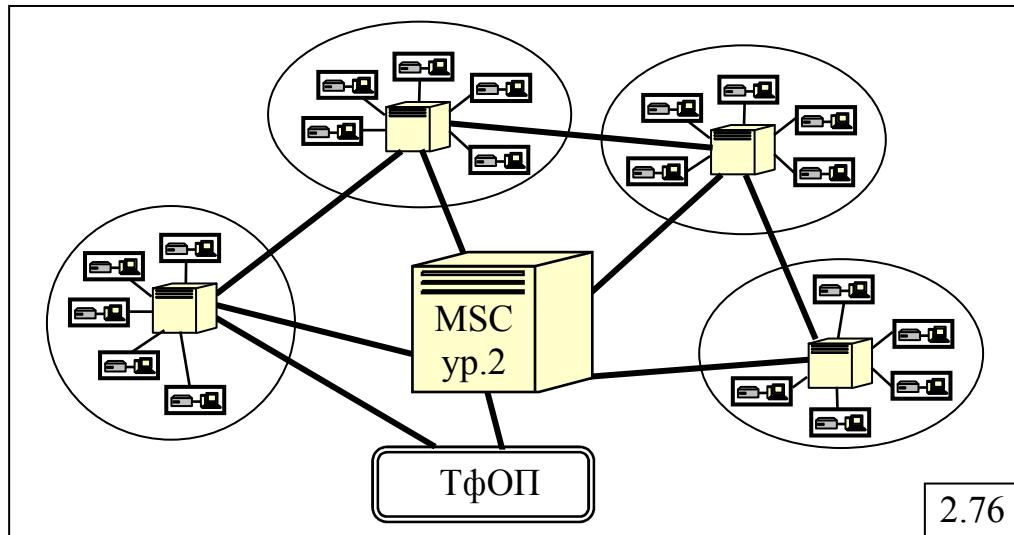


В небольших сетях все базовые станции соединены с коммутатором MSC (Mobile Switching Center – мобильный коммутационный центр) и имеют выход в телефонную сеть общего пользования (ТфОП), обеспечивающий связь мобильных телефонов со стационарными (рис.2.75). В больших сетях коммутаторы 1-го уровня (MSC) соединяются с коммутатором 2-го уровня (рис.2.76) и т.д., при этом все MSC имеют выход в ТфОП напрямую, либо через коммутатор более высокого уровня (см.рис.2.76). Связанные таким образом базовые станции и коммутаторы образуют *сеть сотовой связи*, административно подчиняющиеся одному оператору, предоставляющему услуги мобильной связи.



Базовые станции совместно с коммутационным оборудованием реализуют функции по определению текущего местоположения подвижных пользователей и обеспечивают непрерывность связи при перемещении пользователей из зоны действия одной БС в зону действия другой БС. При включении сотовый телефон ищет сигнал базовой станции и посыпает станции свой уникальный идентификационный код. Телефон и БС поддерживают постоянный радиоконтакт, периодически обмениваясь служебными данными. При выходе телефона из зоны действия БС (или

ослаблении радиосигнала) устанавливается связь с другой БС. Для этого базовая станция, фиксирующая ослабление сигнала, опрашивает все окружающие БС с целью выявить станцию, которая принимает наиболее мощный сигнал от мобильного телефона. Затем БС передаёт управление данным телефоном базовой станции той соты, в которую переместился мобильный телефон. После этого, телефону посыпается информация о переходе в новую соту и предлагается переключиться на новую частоту, которая используется в этой соте. Этот процесс называется *передачей* и длится доли секунды.



Сотовые сети разных операторов соединяются друг с другом, а также со стационарной ТфОП, что позволяет абонентам разных операторов связываться друг с другом, а также делать звонки с мобильных телефонов на стационарные и, наоборот, со стационарных на мобильные телефоны. Используя возможности роуминга, абонент, находясь вне зоны покрытия своей сети, может совершать и принимать звонки через сеть другого оператора.

#### **2.6.6.2. Поколения мобильной сотовой связи**

Различают 4 поколения мобильной сотовой связи, обозначаемые как 1G, 2G, 3G, 4G. В то же время, между 2G и 3G, 3G и 4G выделяют промежуточные поколения, получившие обозначения 2.5G и 3.5G соответственно.

Эти поколения можно разбить на две группы (рис.2.77):

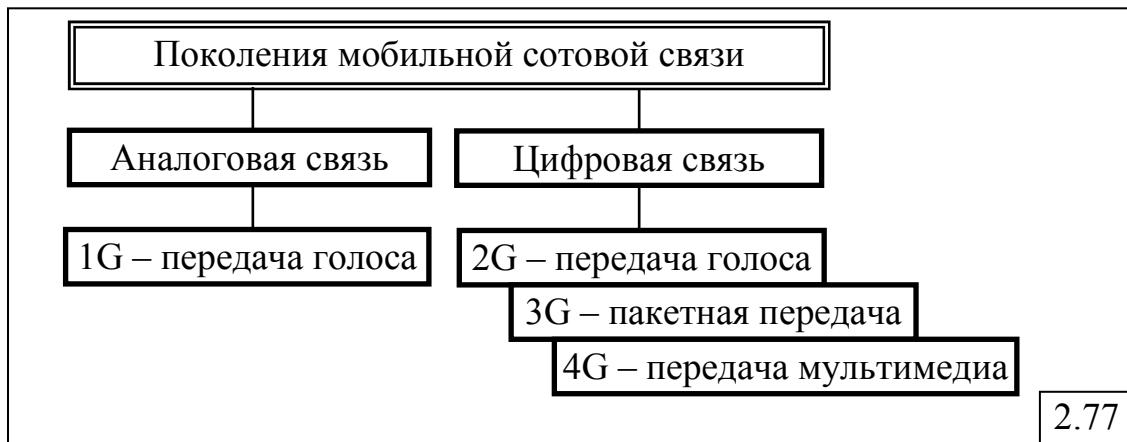
- аналоговая связь (1G);
- цифровая связь (все остальные, начиная с 2G, отличающиеся прежде всего предоставляемыми возможностями по передаче цифровых данных, а также скоростями передачи).

Рассмотрим кратко каждое из поколений.

#### **2.6.6.3. Поколение 1G**

Первые сети мобильной сотовой связи поколения 1G появились в начале 80-х годов прошлого века и представляли собой аналоговые

беспроводные сети, основной и, фактически, единственной функцией которых была передача речи со скоростями, не превышавшими 9,6 кбит/с.



Наиболее известными стандартами сотовой связи первого поколения являются AMPS и NMT.

Стандарт **AMPS (Advanced Mobile Phone System)**, разработанный в США, использует частотное уплотнение, формируя 832 дуплексных канала, каждый из которых состоит из двух симплексных каналов шириной по 30 кГц, в диапазоне частот от 824 до 894 МГц. Радиус действия одной базовой станции от 10 до 20 км.

Стандарт **NMT** (**Nordic Mobile Telephone system**), разработанный пятью скандинавскими странами (Данией, Финляндией, Исландией, Норвегией и Швецией), предписывает работу в диапазоне частот 453-458 МГц (NMT-450), используя до 180 каналов связи по 25 кГц каждый. Радиус действия базовой станции в зависимости от нагрузки достигает 5-25 км. Модернизированная версия NMT-900, работающая на частоте 900 МГц, позволила уменьшить размеры телефонных аппаратов, а также добавить несколько новых сервисов.

В начале 90-х годов на смену аналоговой сотовой связи пришла цифровая связь, которая в настоящее время полностью её вытеснила.

Основной недостаток аналоговой беспроводной связи – отсутствие защиты от несанкционированного перехвата разговора.

#### **2.6.6.4. Поколение 2G**

Второе и последующие поколения мобильной сотовой связи относятся к цифровым сетям связи и, в отличие от первого поколения, предоставляют пользователям, кроме передачи речи, множество дополнительных видов услуг (сервисов).

Стандартами сотовой связи второго поколения являются D-AMPS, GSM, CDMA, в основе которых лежит метод мультиплексирования TDMA.

**TDMA** (Time Division Multiple Access) – множественный доступ с разделением по времени – метод мультиплексирования в беспроводной связи, при котором несколько пользователей для передачи данных используют разные временные интервалы (слоты) в одном частотном диапазоне.

диапазоне, при этом каждому пользователю предоставляется полный доступ к выделенной полосе частот в течение короткого периода времени.

Стандарт **D-AMPS (Digital-AMPS)** был разработан так, чтобы мобильные телефоны первого и второго поколений могли работать одновременно в одной и той же соте. Коммутатор может определять и динамически изменять тип канала (цифровой, аналоговый).

Наибольшее распространение среди перечисленных стандартов получили GSM (заменивший NMT) и CDMA.

**GSM (Global System for Mobile Communications)** – глобальная система мобильной связи, использующая частотное уплотнение. Каждая пара (для передачи в прямом и обратном направлении) частотных каналов разбивается с помощью временного уплотнения (TDMA) на кадровые интервалы, используемые несколькими абонентами. Каналы GSM имеют полосу пропускания в 200 кГц, что значительно шире каналов AMPS с полосой пропускания 30 кГц. Это обусловливает более высокие скорости передачи данных.

GSM, как и D-AMPS, использует частотное и временное уплотнение для разделения спектра на каналы и разделения каналов на временные интервалы соответственно.

GSM обеспечивает поддержку следующих услуг:

- передача данных (синхронный и асинхронный обмен данными, в том числе пакетная передача данных — GPRS);
  - передача речевой информации;
  - передача коротких сообщений (SMS);
  - передача факсимильных сообщений.
  - определение вызывающего номера;
  - переадресация вызовов на другой номер;
  - ожидание и удержание вызова;
  - конференцсвязь (одновременная голосовая связь между тремя и более пользователями);
  - голосовая почта
- и многие другие.

К основным достоинствам стандарта GSM следует отнести:

- меньшие по сравнению с аналоговыми стандартами размеры и вес телефонных аппаратов при большем времени работы без подзарядки аккумулятора;
- хорошее качество связи;
- возможность большого числа одновременных соединений;
- низкий уровень индустриальных помех в выделенных частотных диапазонах;
- защита от прослушивания и нелегального использования за счёт применения алгоритмов шифрования с разделяемым ключом.

Недостатками стандарта GSM являются:

- искажение речи при цифровой обработке и передаче;

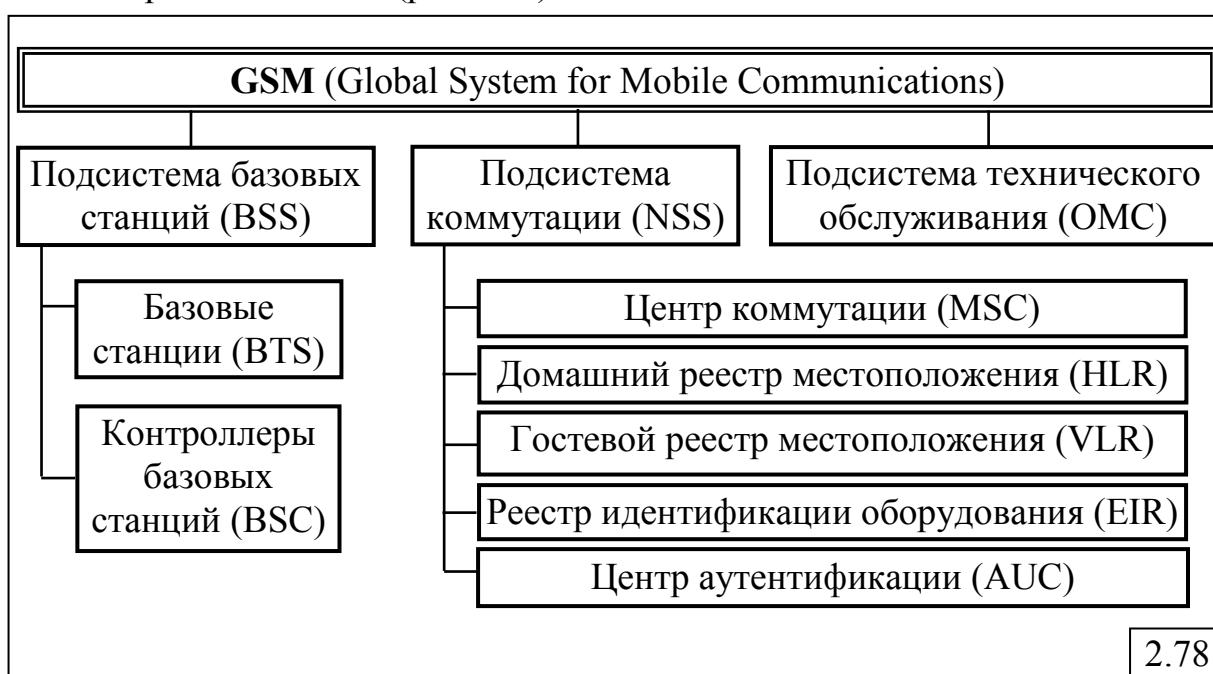
- большее, чем в NMT-450, количество передатчиков, используемых для покрытия определённой площади.

В стандарте GSM определены 4 диапазона частот для передачи данных: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц, наиболее популярными среди которых являются 900 МГц (стандарт GSM-900) и 1800 МГц (GSM-1800). Соты могут иметь диаметр от 400 м до 50 км.

Основные отличия GSM-1800 от GSM-900:

- максимальная излучаемая мощность мобильных телефонов стандарта GSM-1800 (около 1 Вт) вдвое меньше, чем у GSM-900, что увеличивает время непрерывной работы без подзарядки аккумулятора и снижает уровень радиоизлучения;
- большая ёмкость сети;
- возможность совместного использования телефонных аппаратов стандартов GSM-900 и GSM-1800 в одной и той же сети;
- зона охвата для каждой базовой станции значительно меньше и, как следствие, необходимо большее число базовых станций.

В состав системы GSM, кроме мобильных сотовых телефонов, называемых в стандарте *мобильными станциями* (MS – Mobile Station), входят три подсистемы (рис.2.78).



**1. Подсистема базовых станций (BSS – Base Station Subsystem)** состоит из собственно базовых станций и контроллеров базовых станций.

*Базовая станция (BTS – Base Transceiver Station)* обеспечивает приём/передачу сигнала между мобильной станцией и контроллером базовых станций.

*Контроллер базовых станций (BSC – Base Station Controller)* контролирует соединения между базовой станцией и подсистемой коммутации, а также управляет очерёдностью соединений, скоростью передачи, распределением радиоканалов, сбором статистики и переходом MS в другую соту.

## 2. Подсистема сетевой коммутации (NSS – Network Switching Subsystem) построена из следующих компонентов.

- центр коммутации;
- домашний реестр местоположения;
- гостевой реестр местоположения;
- реестр идентификации оборудования;
- центр аутентификации.

*Центр коммутации (MSC – Mobile Switching Centre)* реализует следующие функции:

- устанавливает соединения внутри сети GSM;
- обеспечивает интерфейс с ТфОП и другими сетями;
- выполняет маршрутизацию и управление вызовами;
- управляет передачей обслуживания при перемещении мобильной станции из одной соты в другую;
- постоянно отслеживает положение мобильной станции, используя данные из домашнего (HLR) и гостевого (VLR) реестров местоположения, что необходимо для быстрого нахождения и установления соединения с мобильной станцией в случае её вызова;
- собирает статистические данные;
- по завершению вызова передаёт данные в центр расчётов для формирования счета за предоставленные услуги.

*Домашний реестр местоположения (HLR – Home Location Registry)* содержит базу данных абонентов, приписанных к нему, с информацией о предоставляемых абоненту услугах и о состоянии каждого абонента, а также **международный идентификатор мобильного абонента** (IMSI – International Mobile Subscriber Identity), который используется для аутентификации абонента. Каждый абонент приписан к одному домашнему реестру. К домашнему реестру имеют доступ все центры коммутации и гостевые реестры данной GSM-сети, а в случае межсетевого роуминга и центры коммутации других сетей.

*Гостевой реестр местоположения (VLR – Visitor Location Registry)* содержит базу данных о перемещающихся абонентах, которые находятся в данный момент в этой зоне, в том числе об абонентах других систем GSM, называемых **роумерами**. Если абонент переместился в другую зону, данные о нём удаляются из гостевого реестра. Такая схема позволяет сократить количество запросов к домашнему реестру и, следовательно, время обработки вызова.

*Реестр идентификации оборудования (EIR – Equipment Identification Registry)* содержит базу данных, необходимую для установления подлинности мобильной станции по **международному идентификатору мобильного устройства IMEI** (International Mobile Equipment Identity) в виде трёх списков:

- **белый** – мобильная станция допущена к использованию;
- **серый** – имеются проблемы с идентификацией мобильной станции;

- чёрный - мобильная станция запрещена к использованию.

*Центр аутентификации (AUC – Authentication Centre)* осуществляет аутентификацию абонента по SIM-карте (Subscriber Identity Module). Для этого он посыпает на мобильный телефон случайное число, которое шифруется параллельно в центре аутентификации и в мобильном телефоне с использованием специального алгоритма. Результаты шифрования возвращаются в центр коммутации, где они сравниваются. Если результаты шифрования совпадают, аутентификация считается успешной, и пользователь получает доступ к сети.

**3. Центр технического обслуживания (ОМС – Operations and Maintenance Centre)** обеспечивает:

- управление всей сетью;
  - контроль качества функционирования;
  - обработку аварийных сигналов;
  - проверку состояния сети
- и ряд других функций.

В сетях **CDMA (Code Division Multiple Access)** используется совершенно иной принцип передачи данных, подробно рассмотренный ниже. В отличие от GSM скорость передачи данных в CDMA может достигать 1,23 Мбит/с. Кроме того, существенным отличием является использование распределённого спектра, что усложняет обнаружение и идентификацию передаваемого сигнала и, соответственно, обеспечивает надёжную защиту от случайного подслушивания.

#### **2.6.6.5. Поколение 2.5G**

В процессе разработки принципов и стандартов третьего поколения мобильной сотовой связи появилось промежуточное поколение 2.5G, отличающееся от второго поколения большей ёмкостью сети и пакетной передачей данных. Поколение 2.5G реализовано в виде стандартов GPRS, EDGE и 1xRTT, наиболее распространённым среди которых является GPRS.

**GPRS (General Packet Radio Service)** – технология пакетной радиосвязи общего пользования, ориентированная на реализацию «мобильного Интернета».

GPRS использует базовые станции GSM для передачи данных в виде пакетов, что делает его внедрение достаточно простым и позволяет обеспечить доступ в Интернет. Пакеты передаются через свободные в данный момент каналы. Возможность использования сразу нескольких каналов обеспечивает достаточно высокие скорости передачи данных (до 171,2 кбит/с). Передача данных разделяется по направлениям: «вниз» (downlink, DL) – от сети к абоненту, и «вверх» (uplink, UL) – от абонента к сети. Один и тот же канал поочерёдно могут использовать несколько абонентов, при этом ресурсы канала предоставляются только на время

передачи пакета, что приводит к появлению очереди на передачу пакетов и, как следствие, к увеличению задержки пакетов.

Принцип работы GPRS аналогичен Интернету: данные разбиваются на пакеты и отправляются получателю (возможно разными маршрутами), где происходит их сборка. При установлении сессии каждому устройству присваивается уникальный адрес. Пакеты могут иметь формат IP или X.25, при этом в качестве протоколов транспортного и прикладного уровней могут использоваться любые протоколы Интернета: TCP, UDP, HTTP и др. Мобильный телефон в GPRS рассматривается как клиент внешней сети, которому присваивается постоянный или динамический IP-адрес.

#### **2.6.6.6. Поколение 3G**

Первые реализации третьего поколения сотовой связи появились в 2002 году. Существует три основных стандарта 3G:

- UMTS;
- CDMA2000;
- WCDMA (Wide CDMA).

Все они ориентированы на пакетную передачу данных и, соответственно, на работу с цифровыми компьютерными сетями, включая Интернет. Скорость передачи данных может достигать 2,4 Мбит/с что позволяет передавать качественный звук, а также реализовать «видеозвонок».

При необходимости сеть 3G может быть наложена на уже ранее развёрнутую сеть GSM или другую сеть второго поколения.

**UMTS** (Universal Mobile Telecommunications System – универсальная мобильная телекоммуникационная система) – технология сотовой связи третьего поколения, разработанная Европейским Институтом Стандартов Телекоммуникаций (ETSI) для внедрения в Европе. UMTS поддерживает скорость передачи до 21 Мбит/с и позволяет пользователям проводить сеансы видеоконференций, загрузку музыкального и видео контента.

UMTS обычно реализуется на основе технологий радиоинтерфейса, например W-CDMA. При переходе от GSM к UMTS сохраняется значительная часть прежней инфраструктуры. Основным отличием UMTS от GSM является возможность осуществлять стыки с сетями ISDN, Internet, GSM или другими сетями UMTS.

Для передачи данных от мобильного станции к базовой станции и обратно используют разные диапазоны частот: 1885 МГц – 2025 МГц и 110 МГц – 2200 МГц соответственно, причём оба канала имеют ширину 5 МГц (для сравнения CDMA2000 – 1,25 МГц).

К недостаткам UMTS-технологии следует отнести:

- относительно высокий вес мобильных терминалов наряду с низкой ёмкостью аккумуляторных батарей;

- сложность реализации перехода абонента из зоны действия одной базовой станции в зону действия другой без потери разговора (хэндовера) между сетями UMTS и GSM;

- небольшой радиус соты: 1-1,5 км.

В перспективе планируется эволюция UMTS в сеть четвёртого поколения 4G, позволяющие базовым станциям передавать и принимать данные на скоростях 100 Мбит/с и 50 Мбит/с соответственно.

**CDMA2000** представляет собой развитие технологии CDMA и обеспечивает скорость передачи данных до 153 кбит/с, что позволяет предоставлять услуги голосовой связи, передачу коротких сообщений, работу с электронной почтой, интернетом, базами данных, передачу данных и неподвижных изображений.

Основными достоинствами CDMA2000 являются:

- широкая зона обслуживания;
- высокое качество речи;
- гибкость и дешевизна внедрения новых услуг;
- высокая помехозащищённость;
- устойчивость канала связи от перехвата и прослушивания;
- низкая излучаемая мощность радиопередатчиков абонентских устройств - менее 250 мВт (для сравнения: в GSM-900 этот показатель составляет 2 Вт, а GSM-1800 – 1 Вт).

**WCDMA** (Wideband Code Division Multiple Access) – технология широкополосного множественного доступа с кодовым разделением каналов в диапазоне частот 1900 – 2100 МГц. Термин WCDMA также используется для стандарта сотовой сети, который разрабатывался как надстройка над GSM. WCDMA ориентирована на предоставление мультимедийных услуг, доступа в Интернет и видеоконференции со скоростями передачи данных:

- до 2 Мбит/с на коротких расстояниях;
- 384 кбит/с на больших расстояниях с полной мобильностью.

Такие скорости обеспечиваются за счёт широкой полосы частот канала в 5 МГц, что больше, чем в стандарте CDMA2000, использующем один или несколько каналов с полосой 1,25 МГц для каждого соединения.

#### **2.6.6.7. Поколение 3.5G**

Поколение 3.5G, как промежуточное поколение, характеризуется более высокими скоростями передачи данных по сравнению с 3-м поколением.

Начиная с 2006 года на сетях UMTS повсеместно распространяется технология HSDPA.

**HSDPA** (High Speed Downlink Packet Access – высокоскоростная пакетная передача данных от базовой станции к мобильной станции) – стандарт поколения 3.5G, представляющий собой модернизированный 3G

со средней скоростью передачи данных 3 Мбит/с и максимальной – 14 Мбит/с.

#### **2.6.6.8. Поколение 4G**

Четвёртое поколение мобильных коммуникаций представляет собой эволюционное развитие 3G. Инфраструктура стандарта 4G базируется на IP-протоколе, что позволяет обеспечивать простой и быстрый доступ к Интернету. Высокие скорости передачи данных (100-200 Мбит/с) должны обеспечить передачу не только качественного звука, но и видео. Планируется дальнейшее увеличение скорости передачи данных до 2,5 Гбит/с. Такие высокие скорости объясняются тем, что в четвёртом поколении используется только пакетная передача данных, включая голосовой трафик, передаваемый через протокол IP (мобильная VoIP-телефония). Помимо этого, сети 4G должны обеспечивать глобальный роуминг, связь корпоративных сетей, мобильное телевидение высокой чёткости.

В качестве стандарта 4G активно продвигается технология широкополосной беспроводной связи для быстрого доступа в Интернет с мобильных компьютеров WiMAX, описанная стандартом IEEE802.16.

**WiMAX** (Worldwide Interoperability for Microwave Access) – телекоммуникационная технология, предоставляющая высокоскоростной беспроводной доступ к сети на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов).

Скорости работы WiMAX-сетей будут достигать 75 Мбит/с и выше, что обеспечит не только доступ в Интернет, но и качественную передачу аудио- и видеинформации, а также позволит использовать эту технологию в качестве «магистральных каналов».

Разработаны два стандарта технологии WiMAX – IEEE 802.16 d и IEEE 802.16 e, определяющие:

- рабочие диапазоны частот;
- ширину полосы пропускания;
- мощность излучения;
- методы передачи и доступа;
- способы кодирования и модуляции сигнала;
- принципы повторного использования радиочастот
- и другие показатели.

**Стандарт IEEE 802.16 d**, известный как *фиксированный* WiMAX и утверждённый в 2004 году, позволяет обслуживать только «статичных» абонентов, которые могут находиться как в зоне прямой видимости, так и вне зоны прямой видимости.

**Стандарт IEEE 802.16 e**, известный как *мобильный* WiMAX и утверждённый в 2005 году, ориентирован на работу с пользователями, передвигающимися со скоростью до 120 км/ч, и поддерживает ряд специфических функций, таких как хэндовер, режим ожидания (idle mode)

и роуминг, что позволяет использовать его в сетях сотовой связи. Возможна работа при отсутствии прямой видимости. Естественно, что мобильный WiMAX может применяться и для обслуживания фиксированных пользователей. Частотные диапазоны для сетей Mobile WiMAX расположены в интервале 2,3 - 3,8 ГГц.

Сети WiMAX состоят из следующих основных частей: базовых и абонентских станций, а также оборудования, связывающего базовые станции между собой, с поставщиком сервисов и с Интернетом. Для соединения базовой станции с абонентской используется диапазон частот от 1,5 ГГц до 11 ГГц. В идеальных условиях скорость обмена данными может достигать 70 Мбит/с, при этом не требуется наличия прямой видимости между базовой станцией и приёмником.

Конкурирующей по отношению к WiMAX является технология LTE.

LTE (Long Term Evolution) – технология мобильной передачи данных, предназначенная для повышения эффективности, снижения издержек, расширения оказываемых услуг путём интегрирования с существующими протоколами. Скорость передачи данных в соответствии со стандартом может достигать: 173 Мбит/с «вниз» (download) и 58 Мбит/с «вверх» (upload). Радиус действия базовой станции LTE зависит от мощности и используемых частот и составляет около 5 км, а при высоко расположенной антенне может достигать 100 км.

Важной проблемой в сетях 4-го поколения является поддержка высокой скорости передачи данных при перемещении мобильных станций с высокими скоростями, учитывая, что скорость передачи данных падает с увеличением скорости перемещения и с удалением от базовой станции. Кроме того, необходимо обеспечить передачу управления мобильной станцией при её переходе с высокой скоростью (например, при движении в автомобиле или в поезде) из одной соты в другую без прерывания передачи данных и потери качества передаваемой информации.

Предполагается, что 4G станет единым стандартом, который заменит GSM, CDMA, UMTS и другие стандарты.

### **2.6.7. Цифровые выделенные линии**

Цифровые выделенные линии строятся на основе коммутационной аппаратуры, работающей на принципе разделения канала во времени – Time Division Multiplexing (TDM).

Основными технологиями передачи данных по цифровым выделенным линиям являются:

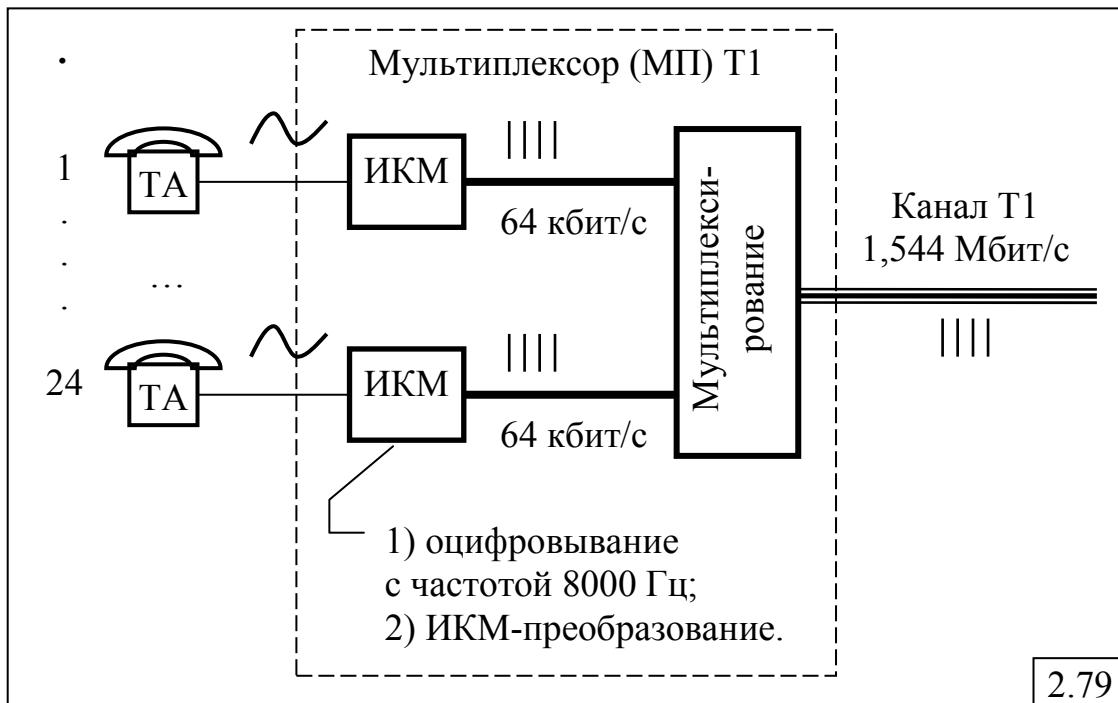
- плезиохронная (почти синхронная) цифровая иерархия (ПЦИ);
- синхронная цифровая иерархия (СЦИ).

#### **2.6.7.1. Плезиохронная цифровая иерархия**

Плезиохронная цифровая иерархия (Plesiochronous Digital Hierarchy, PDH) была разработана фирмой AT&T в конце 60-х годов для связи крупных АТС между собой по высокоскоростным соединительным линиям

и реализована в виде цифровой аппаратуры мультиплексирования и коммутации, которая получила название Т1 и позволяла в цифровом виде мультиплексировать, передавать и коммутировать данные 24-х абонентов.

Схема формирования канала Т1 показана на рис.2.79. Поскольку абоненты пользовались обычными аналоговыми телефонными аппаратами, функции оцифровывания и кодирования голоса на основе ИКМ-преобразования возлагались на мультиплексор (МП). Таким образом, мультиплексор Т1, объединяя 24 речевых каналов со скоростями 64 кбит/с, обеспечивал формирование канала с пропускной способностью 1,544 Мбит/с, который получил название «канал Т1».



2.79

Каналы Т1 представляют собой дуплексные цифровые каналы для передачи цифровых сигналов. Первоначально каналы Т1 выполняли роль магистральных каналов телефонной сети, обеспечивающих повышенную пропускную способность. По мере совершенствования цифровой технологии и снижения стоимости каналы Т1 стали использоваться в качестве выделенных или арендуемых каналов.

Для подключения узла компьютерной сети к каналу Т1 используется специальное оборудование:

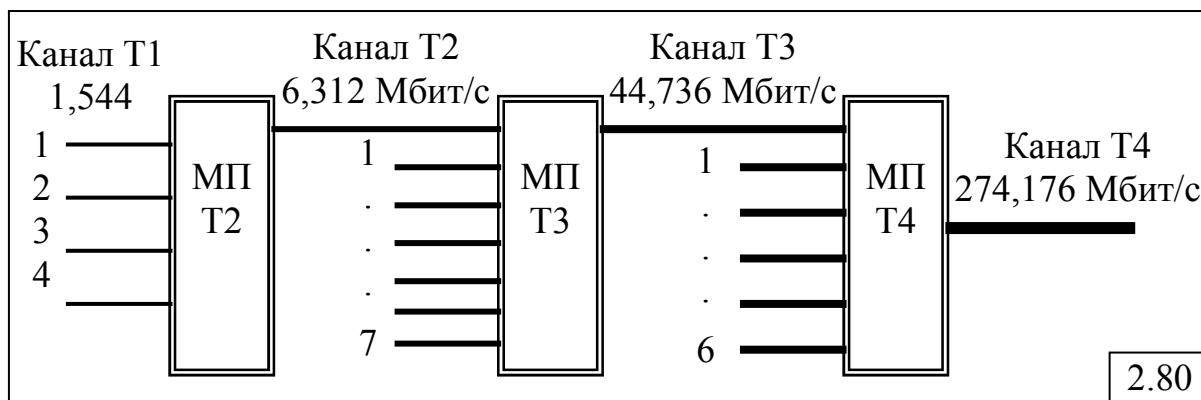
- **CSU (Channel Service Unit)** – устройство обслуживания канала;
- **DSU (Data Service Unit)** – устройство обслуживания данных.

CSU реализует фактический интерфейс между каналом Т1 и узлом, поддерживает качество канала, отслеживает соединения и выполняет в канале Т1 роль физической оконечной точки. DSU преобразует сигналы, выполняет синхронизацию, формирует кадры каналов Т1/E1, усиливает сигнал и осуществляет выравнивание загрузки канала. DSU подключается к CSU и обычно обозначается как одно устройство – DSU/CSU, которое подключается к мостам и маршрутизаторам.

В дальнейшем была разработана аппаратура мультиплексирования цифровых потоков более высокого уровня, которая получила обозначения T2, T3 и T4 и позволила сформировать иерархию скоростей передачи данных по каналам, обозначаемым аналогичным образом:

- канал T2 с пропускной способностью 6,312 Мбит/с получен путём мультиплексирования 4-х каналов T1;
- канал T3 с пропускной способностью 44,736 Мбит/с получен путём мультиплексирования 7-и каналов T2;
- канал T4 с пропускной способностью 274,176 Мбит/с получен путём мультиплексирования 6-и каналов T3.

**Схема формирования каналов T2-T4** представлена на рис.2.80.



В Европе применяется отличающийся от американского международный стандарт, использующий следующие обозначения каналов:

- канал E1 с пропускной способностью 2,048 Мбит/с, полученной в результате мультиплексирования 30 речевых каналов;
- канал E2 с пропускной способностью 8,488 Мбит/с, полученной в результате мультиплексирования 4-х каналов E1;
- канал E3 с пропускной способностью 34,368 Мбит/с, полученной в результате мультиплексирования 4-х каналов E2;
- канал E4 с пропускной способностью 139,264 Мбит/с, полученной в результате мультиплексирования 4-х каналов E3.

Скорости (пропускные способности) каналов Ti и Ei обозначаются в виде **DS-n** (Digital Signal):

- DS-0: 1 речевой канал с пропускной способностью 64 кбит/с;
- DS-1: канал T1/E1 (1,544 Мбит/с / 2,048 Мбит/с);
- DS-2: канал T2/E2 (6,312 Мбит/с / 8,488 Мбит/с);
- DS-3: канал T3/E3 (44,736 Мбит/с / 34,368 Мбит/с);
- DS-4: канал T4/E4 (274,176 Мбит/с / 139,264 Мбит/с).

На практике в основном используются каналы T1/E1 и T3/E3.

На рис.2.81 показаны форматы кадров T1 (DS-1) и T2 (DS-2).

Кадр T1 (рис.2.84,а) объединяет 24 речевых каналов, в каждом из которых передаётся 1 байт, и бит синхронизации S. Длина кадра составляет:  $24 \times 8 + 1 = 193$  бит. Кадры передаются 8000 раз в секунду. Тогда скорость передачи данных:  $193 \text{ бит} \times 8000 = 1,544 \text{ Мбит/с}$ .

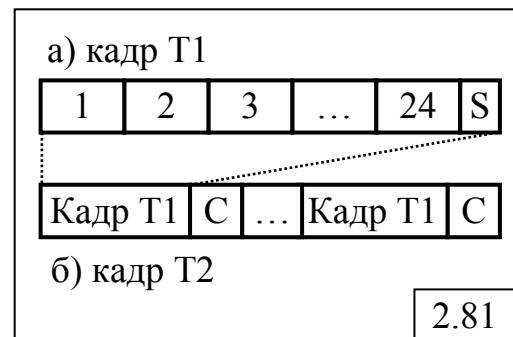
Кадр T2 (рис.2.84,б) объединяет 4 кадра T1, которые разделены служебным полем C, обеспечивающим в том числе синхронизацию.

Аналогично, кадр T3 объединяет 7 кадров T2, а кадр T4 – 6 кадров T3.

Физический уровень PDH поддерживает:

- витую пару;
- коаксиальный кабель;
- волоконно-оптический кабель.

Последние два типа кабеля используются для каналов T3/E3.



### **Недостатки PDH:**

- сложность мультиплексирования и демультиплексирования;
- отсутствие развитых встроенных процедур контроля и управления сетью, а также процедур поддержки отказоустойчивости;
- невысокие по современным меркам скорости передачи данных: 139 Мбит/с для E4, в то время как ВОК позволяет реализовать десятки Гбит/с и более.

#### **2.6.7.2. Синхронная цифровая иерархия**

Синхронная цифровая иерархия (Synchronous Digital Hierarchy, SDH) первоначально появилась в США под названием **SONET** – Synchronous Optical NETs (стандарт принят в 1984 году). Европейский стандарт SDH описан в спецификациях G.707 - G.709. SDH и SONET полностью совместимы.

Цель разработки SDH – создание универсальной технологии для передачи трафика цифровых каналов T1/E1 и T3/E3 и обеспечение иерархии скоростей до нескольких Гбит/с на основе ВОК.

#### **Обозначение уровней иерархии:**

- в **SDH**: STM-n (Synchronous Transport Module);
- в **SONET**:
  - STS-n (Synchronous Transport Signal) – при передаче электрическим сигналом;
  - OC-n (Optical Carrier) – при передаче данных световым лучом по ВОК.

Форматы кадров STS и OC – идентичны.

Иерархия скоростей технологий SDH и SONET представлена в табл.2.4.

Структура сети SDH показана на рис.2.82.

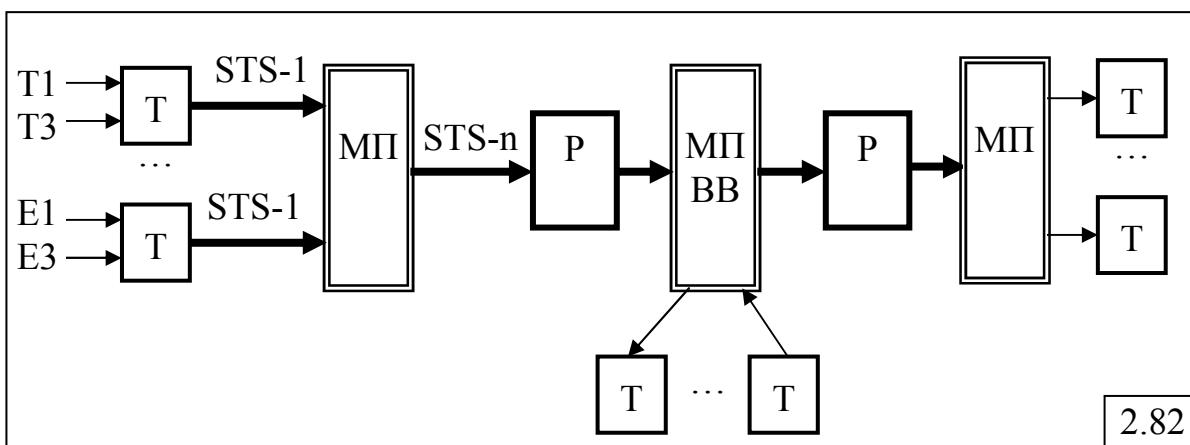
В состав SDH входят следующие устройства:

- *терминальные устройства (T)* – сервисные адаптеры (Service Adapter, SA);
- *мультиплексоры (МП)*;

- мультиплексоры ввода-вывода (МПВВ); принимают и передают транзитом поток STS-n, вставляя или удаляя без полного демультиплексирования пользовательские данные;
- регенераторы (Р);
- цифровые кросс-коннекторы для коммутации высокоскоростных потоков данных.

Таблица 2.4

SDH	SONET		Скорость
	STS	OC	
-	STS-1	OC-1	51,840 Мбит/с
STM-1	STS-3	OC-3	155,520 Мбит/с
STM-3	STS-9	OC-9	466,560 Мбит/с
STM-4	STS-12	OC-12	622,080 Мбит/с
STM-6	STS-18	OC-18	933,120 Мбит/с
STM-8	STS-24	OC-24	1,244 Гбит/с
STM-12	STS-36	OC-36	1,866 Гбит/с
STM-16	STS-48	OS-48	2,488 Гбит/с
STM-64	STS-192	OS-64	9,953 Гбит/с
STM-256	STS-768	OS-256	39,81 Гбит/с



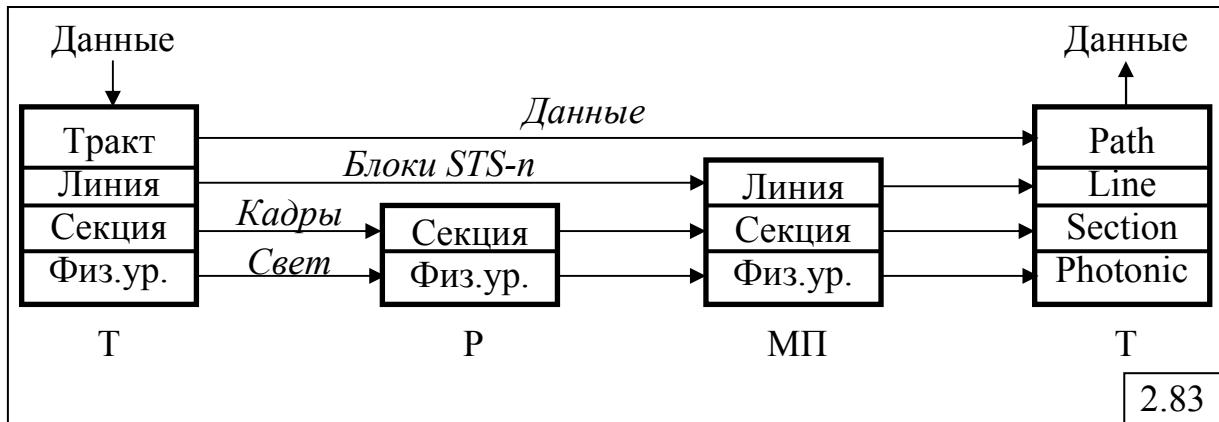
Стек протоколов SDH содержит 4 уровня (рис.2.83).

1. **Физический уровень** (Photonic). Кодирование методом NRZ (модуляция света).

2. **Уровень секции** (Section). Секция – непрерывный отрезок ВОК между двумя устройствами. Проводит тестирование секции и поддерживает операции административного контроля.

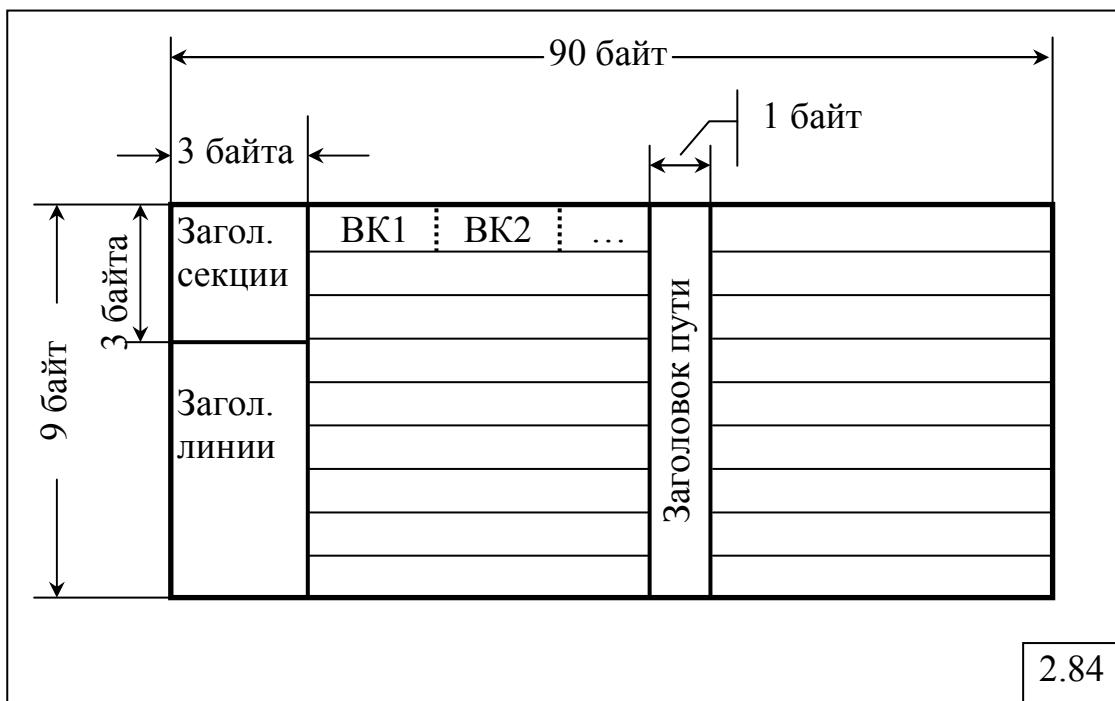
3. **Уровень линии** (Line). Отвечает за передачу данных между МП. Протокол этого уровня выполняет операции мультиплексирования и демультиплексирования, а также вставки и удаления пользовательских данных.

4. **Уровень тракта** (Path). Отвечает за доставку данных между конечными пользователями. Тракт – составное виртуальное соединение между пользователями. Протокол принимает и преобразовывает данные из Ti/Ei в STS-n.



На рис.2.84 представлен формат кадра STS-1 в виде матрицы размером 9 на 90 байт, содержащей:

- заголовок секции – для контроля и реконфигурации секции;
- заголовок линии – для реконфигурации, контроля и управления линией;
- заголовок пути – указывает местоположение виртуальных контейнеров в кадре.



**Виртуальный контейнер** (ВК) – это подкадры, которые переносят потоки данных с более низкими скоростями, чем STS-1 (51,84 Мбит/с), т.е. которые вкладываются в кадр STS-1, как это показано на рис.2.87. В качестве таких виртуальных контейнеров могут выступать, например, ATM-ячейки, кадры T1/E1 и т.д.

С учётом того, что кадр STS-1 размером  $90 \times 9 = 810$  байт передаётся 8000 раз в секунду, получим:  $810[\text{байт}] \times 8[\text{бит}] \times 8000[\text{с}^{-1}] = 51,840$  Мбит/с.

Таким образом, SDH – это основанная на волоконно-оптических каналах интегрированная сеть связи, позволяющая передавать все виды трафика и обеспечивающая:

- использование синхронной передачи с побайтовым чередованием при мультиплексировании;
- использование стандартного периода повторения кадров в 125 мкс;
- включение в иерархию большого числа уровней;
- использование технологии компоновки (инкапсуляции) протоколов в виде виртуальных контейнеров, их упаковки и транспортировки, позволяющие загружать и переносить в них кадры PDH.

## Раздел 3. ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

**Локальная вычислительная сеть** (ЛВС, локальная сеть / Local Area Network, LAN) – компьютерная сеть, обеспечивающая передачу данных на небольшие расстояния (от нескольких десятков метров до нескольких километров) со скоростью, как правило, не менее 1 Мбит/с.

Примеры ЛВС: Ethernet, Token Ring, FDDI.

### 3.1. Принципы организации ЛВС

#### 3.1.1. Характерные особенности ЛВС

1. *Территориальный охват* – от нескольких десятков метров до нескольких километров.
2. Соединяет обычно *персональные компьютеры* и другое электронное офисное *оборудование*, позволяя пользователям обмениваться информацией и совместно эффективно использовать общие ресурсы, например, принтеры, модемы и устройства для хранения данных.
3. *Интерфейс – последовательный*.
4. *Отсутствует АПД*, так как сигналы передаются в "естественной" цифровой форме.
5. В качестве устройства сопряжения ЭВМ со средой передачи используется достаточно простое устройство – *сетевой адаптер*.
6. *Простые типовые топологии*: "общая шина", "кольцо", "звезда".
7. *Отсутствует маршрутизация* (3-й уровень модели OSI).
8. *Высокая скорость передачи* данных, как правило, более 1 Мбит/с.
9. *Сравнительно небольшие затраты* на построение сети.

Перечисленные особенности обусловливают основные **достоинства** ЛВС, заключающиеся в *простоте сетевого оборудования и организации кабельной системы* и, как следствие, в *простоте эксплуатации* сети.

#### 3.1.2. Состав ЛВС

В общем случае ЛВС включает в себя:

- *множество ЭВМ*, обычно персональных компьютеров (ПК), называемых *рабочими станциями*;
- *сетевые адAPTERы*, представляющие собой электронную плату для сопряжения ПК со средствами коммуникации;
- *среду передачи (магистраль)*, представляющую собой совокупность средств коммуникаций (коммуникационная сеть, сеть связи), объединяющая все ПК в единую вычислительную сеть кабельной системой или радиосвязью.

**Сетевые адAPTERы (СА)** (платы, карты) предназначены для сопряжения ПК со средствами коммуникации с учетом принятых в данной сети правилами обмена информацией.

Перечень функций, возлагаемых на СА, зависит от конкретной сети и, в общем случае, может быть разбит на две группы:

- 1) *магистральные (канальные) функции*, обеспечивающие сопряжение адаптера с ПК и сетевой магистралью;
- 2) *сетевые функции*, обеспечивающие передачу данных в сети и реализующие принятый в сети протокол обмена.

К магистральным функциям СА относятся:

- 1) электрическое буферирование сигналов магистрали;
- 2) распознавание (дешифрация) собственного адреса на магистрали;
- 3) обработка стробов обмена на магистрали и выработка внутренних управляющих сигналов.

К сетевым функциям СА относятся:

- 1) *гальваническая развязка* ПК и средств коммуникации (отсутствует в случае оптоволоконной и беспроводной связи);
- 2) *преобразование уровней сигналов* при передаче и приёме данных;
- 3) *кодирование сигналов* при передаче и *декодирование* при приёме (отсутствует при использовании кода NRZ);
- 4) *распознавание своего кадра* при приёме;
- 5) *преобразование кода*: параллельного в последовательный при передаче и последовательного в параллельный при приёме;
- 6) *буферирование* передаваемых и принимаемых данных в буферной памяти СА;
- 7) *проведение арбитража обмена* по сети (контроль состояния сети, разрешение конфликтов и т.д.);
- 8) *подсчет контрольной суммы кадра* при передаче и приёме.

Первые четыре функции всегда реализуются аппаратно, остальные могут быть реализованы программно, что естественно снижает скорость обмена.

**Алгоритм функционирования СА** при передаче кадров содержит следующих этапы (при приёме – обратная последовательность).

1. *Передача данных*. Данные передаются из ОЗУ ПК в буферную память СА (из буферной памяти СА в ОЗУ ПК при приёме) через программируемый канал ввода/вывода, канал прямого доступа к памяти или разделяемую память.

2. *Буферизация*. Необходима для хранения данных во время обработки в СА и обеспечения согласования между собой скоростей передачи и обработки информации различными компонентами ЛВС.

3. *Формирование кадра (сообщения)*:

- сообщение разделяется на кадры при передаче (кадры объединяются в сообщение при приёме);
- к кадру добавляются (удаляются при приёме) заголовок и концевик.

4. *Доступ к кабелю*. Проверяется возможность передачи кадра в линию связи: для Ethernet проверяется незанятость линии связи, для Token Ring – наличие маркера. При приёме кадра этот этап отсутствует.

5. *Преобразование данных* из параллельной формы в последовательную при передаче и из последовательной формы в параллельную при приёме.

6. *Кодирование/декодирование данных*. Формируются электрические сигналы, используемые для представления данных.

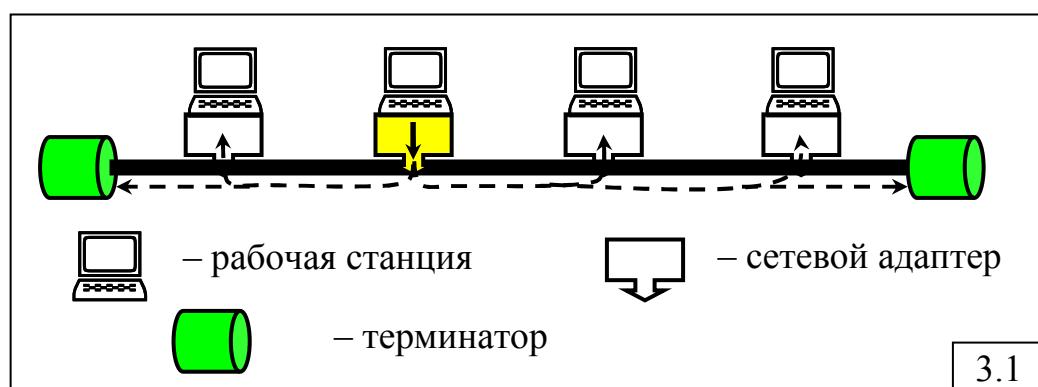
7. *Передача/прием импульсов*. Закодированные электрические импульсы передаются в линию связи (при приеме принимаются из линии связи и направляются на декодирование).

Кроме этих этапов при приеме СА вместе с программным обеспечением ПК *распознают и обрабатывают ошибки*, возникающие из-за электрических помех, конфликтов в сетях со случайным доступом или из-за плохой работы оборудования.

### 3.1.3. Топологии ЛВС

В ЛВС наиболее широкое распространение получили следующие топологии.

1. **"Шина"** (**bus**) – представляет собой кабель, именуемый **магистралью** или **сегментом**, к которому подключены все компьютеры сети (рис.3.1).



Кадр, передаваемый от любого компьютера, распространяется по шине в обе стороны и поступает в буферы сетевых адаптеров всех компьютеров сети, как это пунктиром показано на рис.3.1. Но только тот компьютер, которому адресуется данный кадр, сохраняет его в буфере для дальнейшей обработки. Следует иметь в виду, что в каждый момент времени *передачу может вести только один компьютер*.

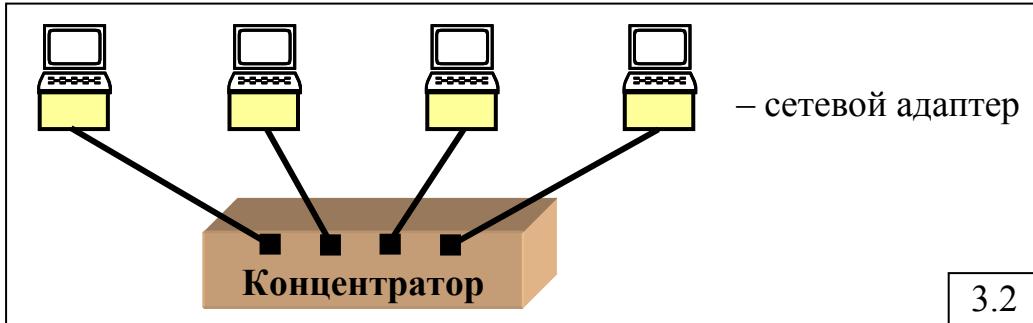
На производительность сети (скорость передачи данных) влияют следующие факторы:

- количество компьютеров в сети и их технические параметры;
- интенсивность (частота) передачи данных;
- типы работающих сетевых приложений;
- тип сетевого кабеля;
- расстояние между компьютерами в сети.

Для предотвращения отражения электрических сигналов на каждом конце кабеля устанавливают **терминаторы**, поглощающие отраженные сигналы.

При нарушении целостности сети (обрыв или отсоединение кабеля), а также при отсутствии терминаторов, сеть "падает" и прекращает функционировать.

2. **"Звезда"** (star), в которой все компьютеры подключаются к центральному компоненту – концентратору (рис.3.2).

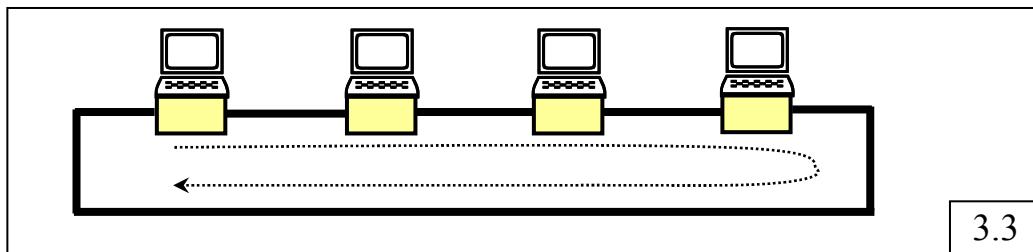


Передаваемый кадр может быть доступен всем компьютерам сети, как в топологии «шина», или же, в случае интеллектуального концентратора, работающего на 2-м уровне OSI-модели, направляться конкретному компьютеру в соответствии с адресом назначения.

Основными недостатками такой топологии являются:

- значительный расход кабеля для территориально больших сетей;
- низкая надежность (узкое место – концентратор).

3. **"Кольцо"** (ring). Сигналы передаются по кольцу *в одном направлении* и проходят через каждый компьютер (рис.3.3). В отличие от пассивной топологии "шина", каждый компьютер выступает в роли повторителя, записывая кадр в буфер сетевого адаптера и затем передавая их следующему компьютеру.



В зависимости от способа передачи сигналов различают:

- 1) *пассивные топологии*, в которых компьютеры только "слушают" передаваемые по сети данные, но не перемещают их от отправителя к получателю, поэтому выход из строя одного из компьютеров не оказывается на работе остальных;
- 2) *активные топологии*, в которых компьютеры регенерируют сигналы и передают их по сети.

### 3.1.4. Архитектуры ЛВС

Типы архитектур ЛВС:

- одноранговые сети;
- сети типа "клиент-сервер";

- комбинированные сети, в которых могут функционировать оба типа операционных систем (одноранговая и серверная).

#### **3.1.4.1. Одноранговые (равноранговые) сети**

*Одноранговые сети (peer-to-peer)* – сети с равноправными компьютерами, которые могут использовать ресурсы друг друга. Некоторые одноранговые сети позволяют использовать компьютеры как в качестве рабочей станции в составе сети, так и в качестве выделенного и невыделенного сервера.

Архитектура одноранговой сети оправдана, если:

- количество пользователей не превышает 10;
- пользователи расположены компактно;
- вопросы защиты данных не критичны;
- имеется необходимость повысить производительность и эффективность офисной деятельности путем совместного использования файлов и периферийного оборудования.

*Достоинства:*

- умеренная стоимость;
- простота построения и эксплуатации (нет необходимости в сетевом администрировании).

*Недостатки:*

- небольшой размер сети, объединяющей обычно не более 10 пользователей (компьютеров), образующих рабочую группу;
- трудно обеспечить должную защиту информации при большом размере сети.

Примерами одноранговых сетевых операционных систем являются LANtastic (фирмы Artisoft), NetWare Lite (Novell). Поддержка одноранговых сетей встроена также в операционные системы Windows (Windows NT Workstation, Windows 95 и др.) фирмы Microsoft.

#### **3.1.4.2. Сети типа "клиент-сервер"**

Сети типа "клиент-сервер" содержат:

- **серверы** – мощные компьютеры, владеющие разделяемыми между пользователями сети ресурсами и управляющие доступом к ним клиентов;
- **клиенты** – менее мощные компьютеры сети, владеющие неразделяемыми ресурсами и имеющие доступ к ресурсам серверов.

Архитектура сети типа "клиент-сервер" оправдана, если:

- в сети планируется работа с единым сетевым ресурсом, например, одновременная работа нескольких пользователей с общей базой данных, расположенной на сервере;
- целесообразно сосредоточить все разделяемые сетевые ресурсы (например, сетевой принтер) в одном месте и не требуется общение рабочих станций между собой.

*Достоинства:*

- высокая производительность за счет разделения ресурсов сети;

- возможность организации эффективной защиты данных;
- эффективная организация резервного копирования данных;
- способность поддерживать работу в сети сотен и тысяч пользователей;
- хорошие возможности для расширения.

*Недостатки:*

- требуют постоянного квалифицированного обслуживания – администрирования.

### **3.1.4.3. Серверы ЛВС**

**Сервер ЛВС** – выделенный компьютер, который предоставляет другим компьютерам сети доступ к общим сетевым ресурсам. Программа, реагирующая на соответствующие запросы и выполняющая их, называется **службой** или **сервисом**.

Серверы делятся на:

- файл-серверы;
- прикладные серверы.

**Файл-сервер** предоставляет доступ к общему дисковому пространству, в котором хранятся общедоступные файлы, и, в основном, определяет возможности ЛВС.

**Прикладные серверы** представляют собой средства расширения возможностей ЛВС и включают в себя: сервер баз данных, сервер печати, сервер резервирования, факс-сервер и т.д.

### **3.1.5. Многосегментная организация ЛВС**

Основной недостаток ЛВС – наличие ограничения на общую протяженность кабельной сети, составляющую несколько сотен метров. Так для стандарта Ethernet длина сегмента (расстояние от одной крайней станции до другой) составляет не более 500 метров – для электрического кабеля.

Максимальное расстояние между двумя наиболее удаленными друг от друга (крайними) станциями называется **диаметром сети**.

Простейший путь увеличения диаметра сети и количества компьютеров – **многосегментная организация ЛВС** с использованием:

- нескольких сетевых адаптеров в файл-сервере;
- повторителей;
- концентраторов.

#### **3.1.5.1. Использование нескольких сетевых адаптеров**

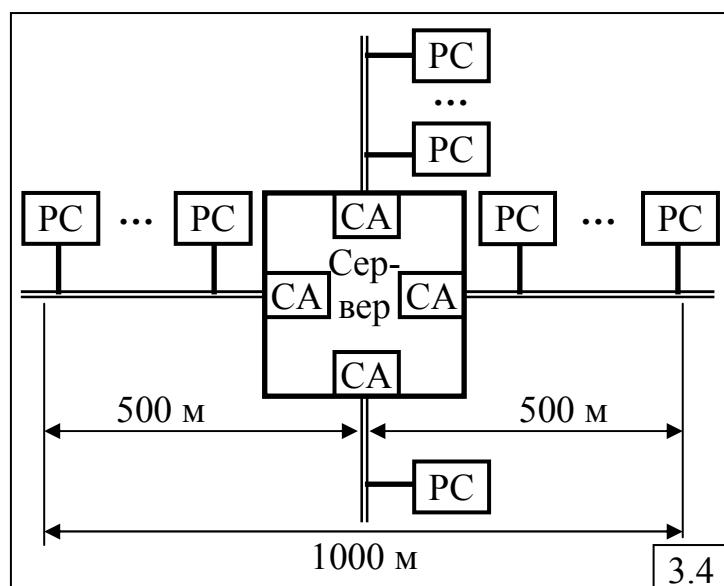
Одно из первых и наиболее простых решений, направленных на увеличение размера локальной сети, – использование нескольких сетевых адаптеров (рис.3.4), что позволяло увеличить диаметр сети почти вдвое по сравнению с односегментной ЛВС. Например, в сети Ethernet могло быть до 5 сегментов, каждый из которых имел отдельную кабельную систему.

*Достоинство:*

- простота реализации и невысокая стоимость.

*Недостатки:*

- необходимость использования по дополнительному сетевому адаптеру (СА) на каждый сегмент;
- большая нагрузка на сервер и, как следствие, невозможность построения больших (с большим числом рабочих станций) сетей.



### 3.1.5.2. Повторители

**Повторитель (repeater)** – простейшее сетевое устройство для построения многосегментных ЛВС, усиливающий сигнал, полученный с одного сегмента, и передающий его в другой сегмент (рис.3.5). Повторитель принимает сигналы из одного сегмента кабеля и побитно синхронно повторяет их в другом сегменте, улучшая форму и мощность импульсов, а также синхронизируя импульсы.

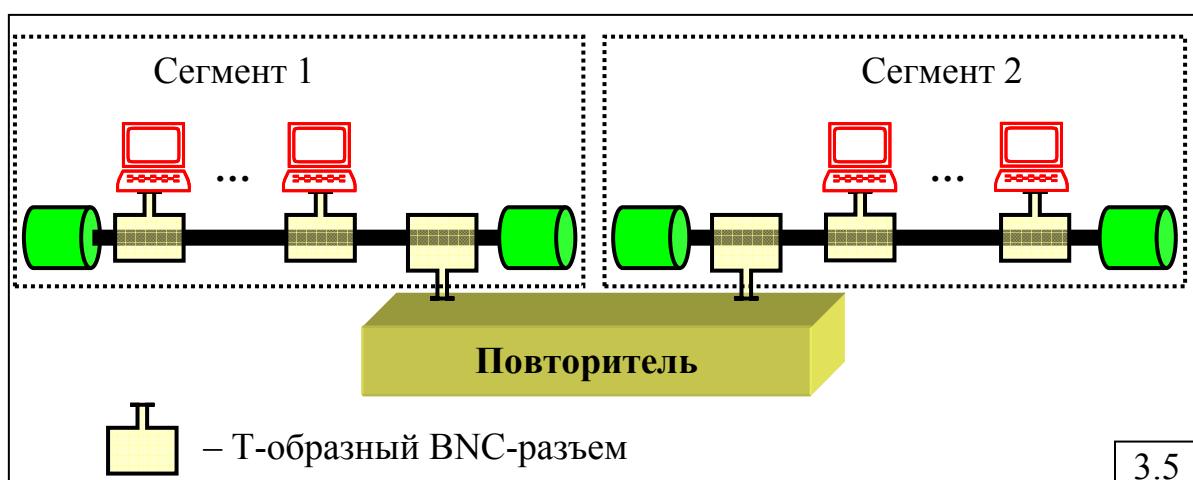
Повторитель объединяет *абсолютно идентичные* сети и работает на самом нижнем – *физическом уровне* OSI-модели.

*Достоинства:*

- простота организации многосегментных ЛВС;
- дешевизна.

*Недостатки:*

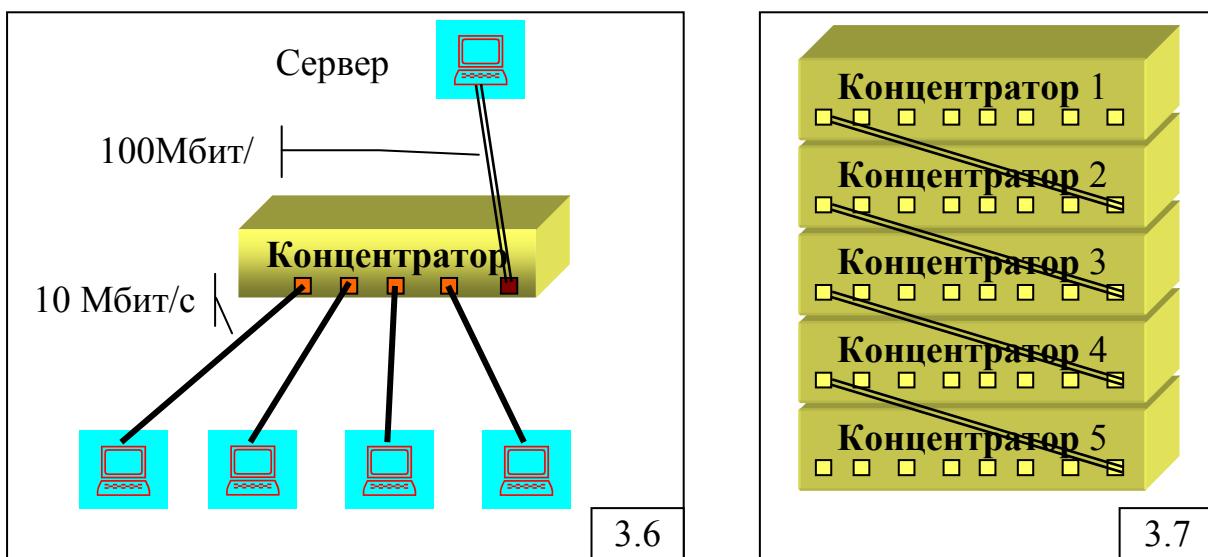
- значительное повышение загрузки в обоих сегментах, т.к. даже "местные" сообщения одного сегмента передаются в другую сеть;
- снижение производительности (скорости передачи данных) СПД.



### 3.1.5.3. Концентраторы

**Концентратор (hub / хаб)** – сетевое устройство, используемое в сетях на *витой паре*, в котором концентрируются идущие от рабочих станций отрезки кабеля (рис.3.6). Через концентратор компьютер подсоединяется к единой среде обмена данными между станциями ЛВС – серверу или магистральному каналу. Простейший концентратор представляет собой *многопортовый повторитель* и используется в качестве центрального узла ЛВС с топологией «звезда».

Концентратор может иметь от 8 до 32 портов для подключения компьютеров. Дальнейшее увеличение количества портов достигается путем объединения концентраторов в единый **стек концентраторов**, как это показано на рис.3.7.



Кроме портов для подсоединения рабочих станций с помощью витой пары концентраторы могут иметь разъем для подсоединения к высокоскоростному магистральному каналу на коаксиальном кабеле или волоконно-оптическом кабеле.

### 3.1.6. Методы управления доступом в ЛВС

На эффективность функционирования ЛВС существенное влияние оказывает **метод управления доступом** (Access Control Method), определяющий порядок предоставления сетевым узлам доступа к среде передачи данных с целью обеспечения каждому пользователю приемлемого уровня обслуживания. Методы доступа к среде передачи реализуются *на канальном уровне* OSI-модели.

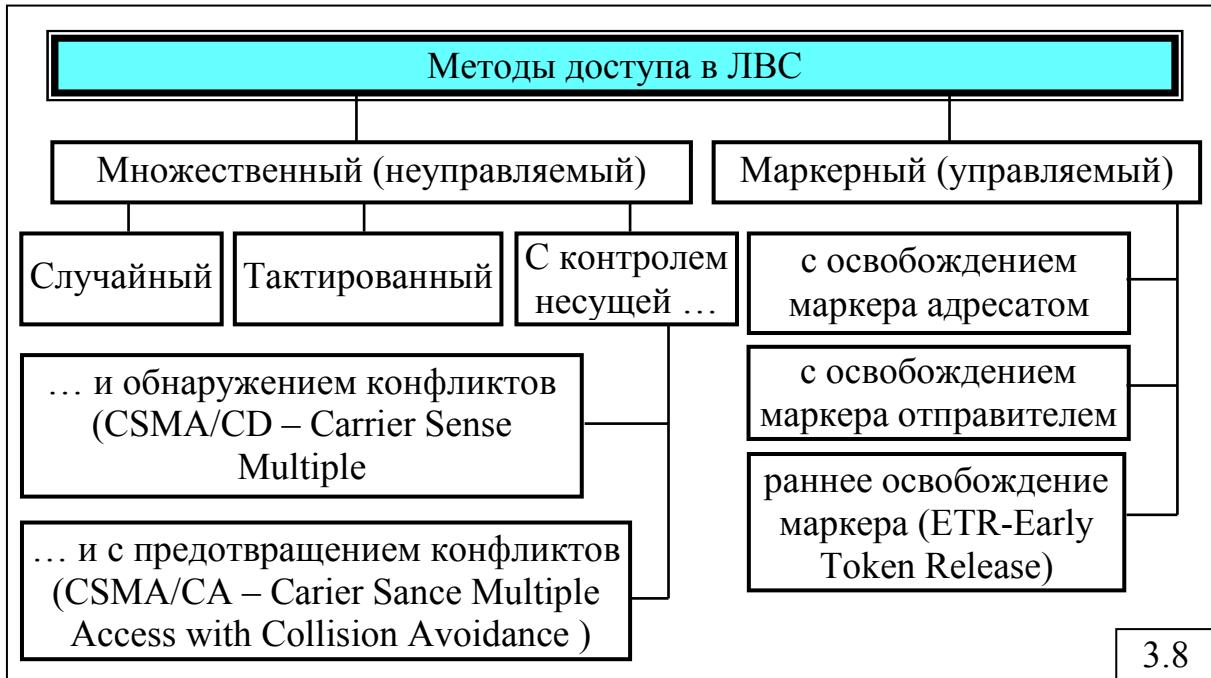
**Классификация методов доступа** представлена на рис.3.8.

**Множественный доступ** – метод доступа множества сетевых узлов к общей среде передачи (например, общейшине), основанный на соперничестве станций за доступ к среде передачи. Каждая станция может пытаться передавать данные в любой момент времени.

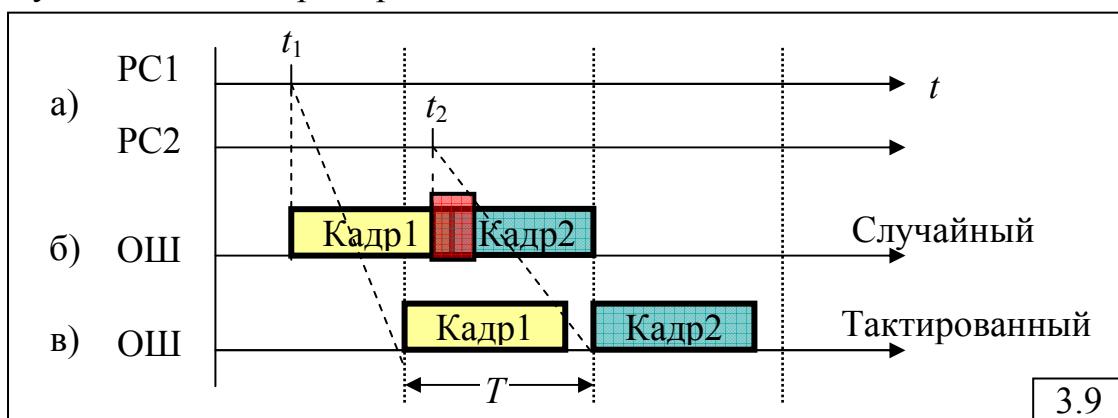
К методам множественного доступа относятся:

- случайный доступ;

- тактированный доступ;
- доступ с контролем несущей и обнаружением конфликтов;
- доступ с контролем несущей и предотвращением конфликтов.



Наиболее простым и естественным методом доступа к общей среде передачи является **случайный доступ**, означающий, что каждая станция сети начинает передачу кадра в момент его появления (формирования), не зависимо от того, занята общая среда передачи или свободна. Если две и более станций осуществляют передачу в одно и то же время, то их кадры взаимно искажаются, и возникает **коллизия**. На рис.3.9,а) показан случай, когда две рабочие станции PC1 и PC2 начинают передачу кадров «Кадр1» и «Кадр2» в случайные моменты времени  $t_1$  и  $t_2$  соответственно. В момент  $t_2$  возникает коллизия (рис.3.9,б), искажающая оба кадра. Можно показать, что коэффициент использования канала связи при случайному методе доступа составляет примерно 16%.



Уменьшение коллизий и увеличение коэффициента использования канала связи может быть достигнуто за счёт использования **тактированного доступа**, который заключается в следующем. Весь

временной интервал разбивается на такты длиной  $T$ , где значение  $T$  должно быть больше времени передачи кадра максимальной длины. Каждая рабочая станция может начать передачу кадра только в начале очередного такта. В этом случае «Кадр2» будет передан в другом такте по отношению к «Кадру1» (рис.3.9,в), и коллизия не возникнет. Однако следует отметить, что остается достаточно высокой вероятность возникновения коллизий в тех случаях, когда моменты формирования кадров в разных станциях оказываются в пределах одного такта. В связи с этим, коэффициент использования канала связи, хотя и увеличивается, но незначительно, и составляет примерно 32%.

**Множественный доступ с контролем несущей и обнаружением конфликтов (Carrier Sense Multiple Access with Collision Detection – CSMA/CD)** – метод доступа к среде передачи, при котором станция, имеющая данные для передачи, прослушивает канал, чтобы определить, не передаёт ли данные в это время другая станция. Отсутствие сигнала несущей означает, что канал свободен и станция может начать передачу. Однако не исключено, что в течение времени распространения сигнала по среде передачи другие станции почти одновременно также начнут передачу своих данных.

Во время передачи станция продолжает прослушивать канал, чтобы удостовериться в отсутствии коллизии. Если коллизия не зафиксирована, данные считаются успешно переданными.

При обнаружении коллизии станция повторяет передачу через некоторое случайное время. Повторные передачи повторяются до тех пор, пока данные не будут успешно переданы.

**Множественный доступ с контролем несущей и предотвращением конфликтов (Carrier Sense Multiple Access with Collision Avoidance – CSMA/CA)** – метод доступа к среде передачи, при котором передача данных предваряется посылкой сигнала блокировки (jam) с целью захвата передающей среды в монопольное пользование. Этот метод доступа рекомендован комитетом IEEE 802.11 для беспроводных ЛВС.

**Маркерный доступ** предполагает наличие в сети кадра специального формата, называемого **маркером**, который непрерывно циркулирует в сети и управляет процессом доступа рабочих станций к среде передачи данных. В каждый момент времени данные может передавать только та станция, которая владеет маркером. Рабочая станция, владеющая маркером, присоединяет свой кадр данных к маркеру и отправляет адресату. При этом возможны различные варианты освобождения и передачи маркера другой станции:

1) **освобождение маркера адресатом:** адресат отсоединяет маркер от данных и может использовать его для отправки своего кадра, если таковой есть, или передать маркер другой станции;

2) **освобождение маркера отправителем:** маркер с присоединенным кадром данных делает полный оборот и *отсоединяется*

отправителем (в версии Token Ring для скорости 4 Мбит/с), если оно вернулось без ошибок; в противном случае, этот же кадр с маркером направляется повторно в среду передачи данных;

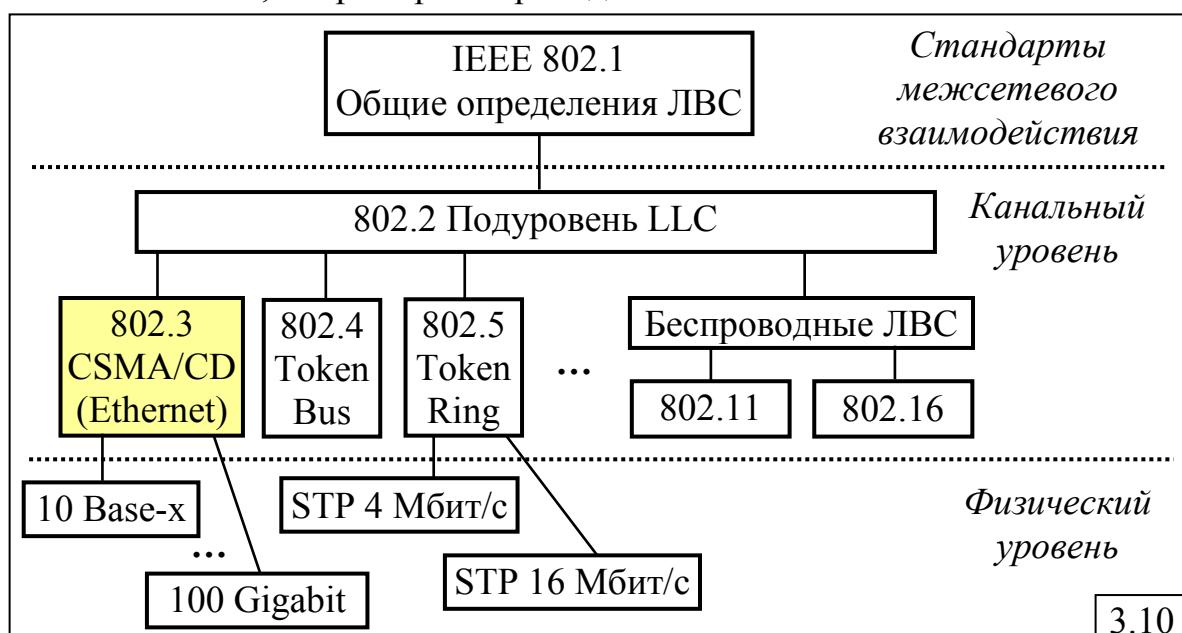
3) метод **раннего освобождения маркера ETR** (Early Token Release), когда рабочая станция освобождает маркер сразу после передачи своих данных и передаёт его другой станции, не ожидая возвращения отправленного кадра данных (в версии Token Ring для скорости 16 Мбит/с и в сети FDDI).

Маркерный доступ используется в сетях:

- с шинной топологией в ЛВС ARCnet: рекомендация IEEE 802.4 (Token Bus – маркерная шина);
- с кольцевой топологией в ЛВС Token Ring и FDDI: рекомендация IEEE 802.5 (Token Ring – маркерное кольцо).

### 3.1.7. Стандарты локальных сетей

Основным разработчиком стандартов локальных сетей является комитет 802, организованный в 1980 году в IEEE. В рамках этого комитета были образованы подкомитеты 802.1, 802.2, ..., в которых разрабатываются стандарты разных уровней IEEE-модели и различных технологий построения ЛВС. На рис.3.10 перечислены некоторые из этих стандартов, представляющие собой рекомендации по разработке ЛВС, обеспечивающие выполнение основных требований к организации сетей, таких как открытость, гибкость и совместимость. Стандарты ЛВС обрастают дополнениями, которые находят отражение в обозначениях 802.x в виде букв, например 802.1р (стандарт, описывающий приоритезацию трафика на канальном уровне), а также пополняются новыми стандартами, отражающими появление новых технологий локальных сетей, например беспроводных сетей 802.11 и 802.16.



Ниже рассматриваются принципы организации наиболее популярной ЛВС Ethernet, использующей метод доступа CSMA/CD (IEEE 802.3), и

ЛВС Token Ring, использующей метод доступа «маркерное кольцо» (IEEE 802.5), а также беспроводных технологий передачи данных, известных как WiFi (IEEE 802.11) и WiMAX (IEEE 802.16).

Метод доступа Token Bus – «маркерная шина», описанный в стандарте IEEE 802.4, был реализован в локальной сети ArcNET, не получившей широкого распространения.

## **3.2. ЛВС Ethernet**

### **3.2.1. Общие сведения**

**Ethernet** – технология ЛВС, разработанная совместно фирмами DEC, Intel и Xerox (DIX) и опубликованная в 1980 году в виде стандарта Ethernet II для сети с пропускной способностью 10 Мбит/с, построенной на основе коаксиального кабеля.

На основе стандарта Ethernet II был разработан стандарт IEEE 802.3, который имеет следующие отличия:

- канальный уровень разбит на два подуровня: MAC и LLC;
- внесены некоторые изменения в формат кадра при тех же минимальных и максимальных размерах кадров.

В зависимости от физической среды передачи данных IEEE 802.3 предусматривает различные варианты реализации ЛВС на физическом уровне:

- 10Base-5 – толстый коаксиальный кабель;
- 10Base-2 – тонкий коаксиальный кабель;
- 10Base-T – витая пара;
- 10Base-F – оптоволокно.

В 1995 году был принят стандарт Fast Ethernet с пропускной способностью среды передачи 100 Мбит/с, который представлен в виде дополнительного раздела 802.3u к стандарту IEEE 802.3.

В 1998 году принят стандарт Gigabit Ethernet, описанный в разделе 802.3z для ЛВС с пропускной способностью 1 Гбит/с.

В 2002 году утверждена спецификация IEEE 802.3ae для ЛВС с пропускной способностью 10 Гбит/с (10 Gigabit Ethernet), предусматривающая использование волоконно-оптических кабелей.

В июне 2010 года принят стандарт IEEE P802.3ba для ЛВС с пропускными способностями 40 Гбит/с и 100 Гбит/с: 40 Gigabit Ethernet (40GbE) и 100 Gigabit Ethernet (100GbE).

Перечисленные варианты ЛВС Ethernet и годы появления соответствующих стандартов сведены в табл.3.1.

В стандарте IEEE 802.3 определен *метод доступа*, используемый в сетях Ethernet (в том числе Fast Ethernet и Gigabit Ethernet) – CSMA/CD – множественный доступ с контролем несущей и проверкой столкновений.

Компьютеры в ЛВС Ethernet подключаются к разделяемой среде в соответствии с топологией «общая шина» (рис. 3.1), которая обеспечивает обмен данными между двумя любыми компьютерами сети. Управление

доступом к общей среде передачи реализуется средствами сетевого адаптера. Каждый сетевой адаптер, имеет уникальный адрес.

Таблица 3.1

Вариант ЛВС Ethernet	Пропускная способность	Стандарт	Год
Ethernet DIX	10 Мбит/с	Ethernet II	1980
Ethernet	10 Мбит/с	IEEE 802.3	1982
Fast Ethernet	100 Мбит/с	IEEE 802.3u	1995
Gigabit Ethernet	1 Гбит/с	IEEE 802.3z	1998
10 Gigabit Ethernet	10 Гбит/с	IEEE 802.3ae	2002
40 Gigabit Ethernet	40 Гбит/с	IEEE P802.3ba	2010
100 Gigabit Ethernet	100 Гбит/с	IEEE P802.3ba	2010

Кадры, передаваемые станциями, проходят через сетевые адаптеры всех станций сети, но только та из них, кому адресован данный кадр, принимает и записывает его в буфер адаптера для дальнейшего формирования сообщения и передачи его в память рабочей станции. Таким образом, в каждый момент времени в сети может передаваться только один кадр. Если передачу кадров начинают одновременно две и более станции, возникает коллизия, в результате которой все кадры искажаются и требуется повторная передача кадров.

Часть сети Ethernet, все узлы которой распознают коллизию, независимо от того, в какой части этой сети коллизия возникла, называется **доменом коллизий** (collision domain).

Стандарт IEEE 802.3 определяет ограничения, налагаемые на размер ЛВС Ethernet:

- максимальное число станций в сети – 1024;
- максимальная протяженность сети – 3-4 км;
- максимальная длина сегмента сети (*расстояние между крайними станциями*), зависящая от типа передающей среды:
  - 500 метров – для толстого коаксиального кабеля;
  - 185 метров – для тонкого коаксиального кабеля;
  - 100 метров – для витой пары;
  - 2000 метров – для оптоволоконного кабеля.

Основными топологиями ЛВС Ethernet являются:

- "общая шина", в которой в качестве среды передачи данных используется коаксиальный кабель;
- "звезда", в которой центральным узлом является концентратор, а в качестве среды передачи данных используется витая пара или оптоволоконный кабель.

### 3.2.2. Физический уровень ЛВС Ethernet

Кабельная система сети Ethernet является коммуникационной средой, по которой перемещаются кадры данных. Стандарт физического

уровня содержит описание (спецификации) кабелей различных типов, пригодных для реализации сетей с методом доступа CSMA/CD. Обозначение спецификаций физического уровня в соответствии со стандартом 802.3:

**<СП>Base-<ТК>**,

где **<СП>** – скорость передачи в Мбит/с – может принимать значения 10, 100, 1000, а в случае гигабитных скоростей – 1G, 10G, 4G, ...; **Base** – метод передачи, означающий *основополосную* передачу (**Baseband**); **<ТК>** – тип кабеля:

- 2 – тонкий коаксиальный;
- 5 – толстый коаксиальный;
- Т – витая пара (Twisted pair);
- F – волоконно-оптический (Fiber); ....

#### ***Основополосная (прямая, немодулированная) передача (baseband)***

– метод передачи данных, при котором цифровой сигнал направляется непосредственно в среду передачи без модуляции несущей, при этом вся полоса пропускания используется для передачи только одного цифрового сигнала. Этот метод удобен для передачи данных по каналам с широкой полосой пропускания на небольшие расстояния и характеризуется простотой и дешевизной реализации, в связи с чем широко используется в ЛВС.

***Широкополосная передача (broadband)*** – метод передачи данных, основанный на частотном FDM, временном TDM или волновом WDM уплотнении и создании нескольких частотных или временных каналов, по которым независимо друг от друга могут передаваться несколько потоков данных.

Для всех вариантов физического уровня технологии Ethernet, обеспечивающих пропускную способность 10 Мбит/с, используется *манчестерское кодирование*.

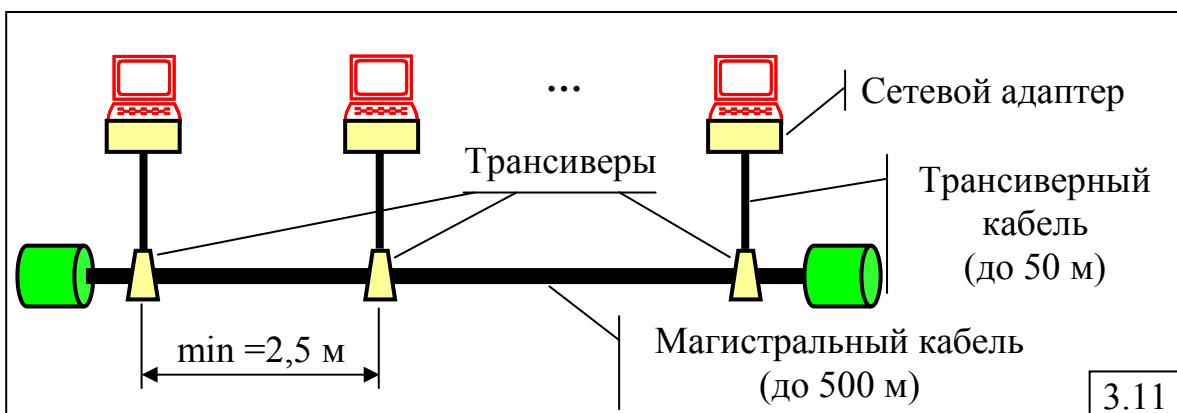
##### **3.2.2.1. Спецификация 10Base-5**

10Base-5 – стандарт физического уровня, являющийся частью стандарта IEEE 802.3 и описывающий работу сети Ethernet на толстом коаксиальном кабеле (thick Ethernet), используемом в качестве основной магистрали.

На рис.3.11 показан *сегмент* ЛВС Ethernet на толстом коаксиальном кабеле. Рабочие станции подключаются к магистральному кабелю с помощью трансиверного кабеля, состоящего из 4-х витых пар длиной до 50 м, и приемопередатчика (трансивера), расположенного непосредственно на коаксиальном кабеле. Трансивер представляет собой электрическое устройство, осуществляющее физическую передачу и приём данных.

Расстояние между соседними трансиверами должно быть кратно 2,5 м для исключения влияния стоячих волн в кабеле на качество передачи сигнала. На концах магистрального кабеля располагаются терминаторы, поглощающие распространяющийся в кабеле информационный сигнал и

препятствующие возникновению отражённого сигнала, искажающего полезный сигнал.

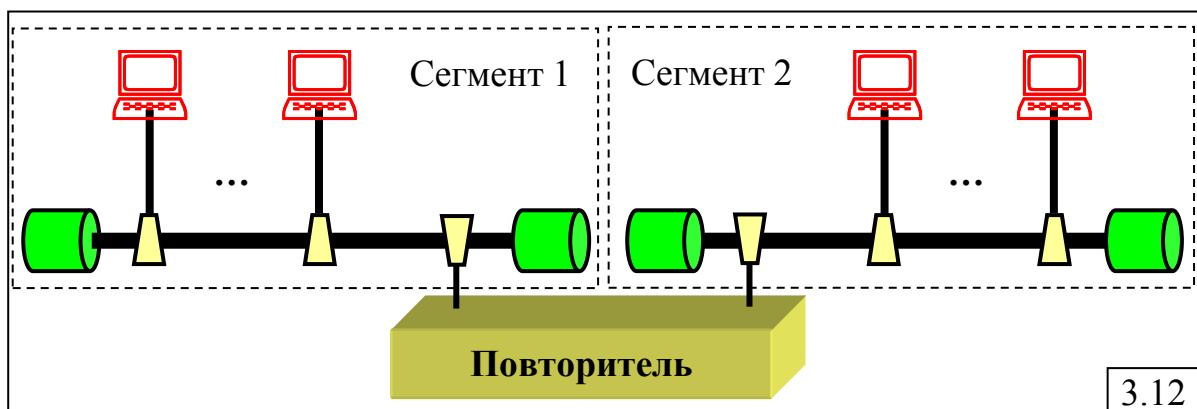


Несмотря на громоздкость и трудности при разводке, такая кабельная система позволяет строить достаточно протяженные сети.

Таким образом, основные ограничения для одного сегмента ЛВС Ethernet в соответствии со спецификацией 10Base-5 имеют вид:

- максимальная длина сегмента (расстояние между крайними узлами) – 500 м;
- минимальное расстояние между трансиверами – 2,5 м;
- максимальное число узлов (трансиверов) на сегменте – 100;
- максимальная длина трансиверного кабеля – 50 м.

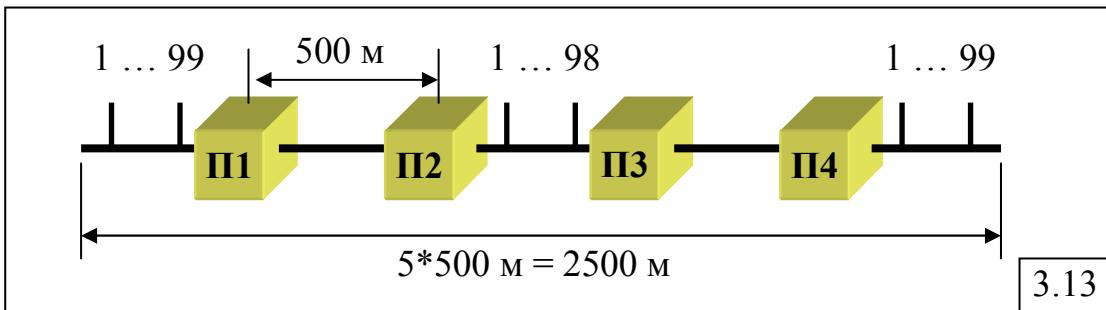
Стандарт 10Base-5 допускает построение многосегментных сетей с использованием повторителей. На рис.3.12 показана двухсегментная сеть. Максимальное количество сегментов в сети, допускаемое стандартом, равно 5. Это ограничение обусловлено тем, что повторители только усиливают сигналы, не восстанавливая их форму, что при большом количестве сегментов в сети может привести к появлению значительного процента ошибок.



При построении многосегментной сети необходимо учитывать следующие ограничения (рис.3.13):

- сеть может состоять из 5 сегментов, соединенных через повторители;
- в трёх сегментах можно подключать к кабелю до 100 узлов; два других сегмента используются только для увеличения общей протяженности сети;

- повторитель рассматривается как специальный узел, подключенный к сети, поэтому в центральном сегменте с двумя повторителями допускается иметь только 98 станций.



*Правило построения многосегментной сети с такими ограничениями получило название «5-4-3», означающее 5 сегментов соединяются с помощью 4-х повторителей, причём нагруженными являются только 3 сегмента.*

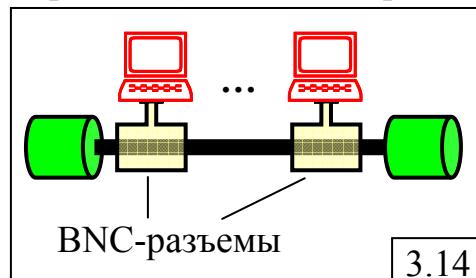
Таким образом, одна сеть Ethernet 10Base-5:

- может содержать не более 296 узлов (рабочих станций);
- иметь диаметр (максимальную длину кабеля) – не более 2,5 км.

### 3.2.2.2. Спецификация 10Base-2

10Base-2 – стандарт физического уровня, утвержденный комитетом IEEE 802.3, описывающий работу сети Ethernet на тонком коаксиальном кабеле (*thin Ethernet* – тонкий Ethernet, иначе ещё называемый *Cheapernet* – дешевый Ethernet).

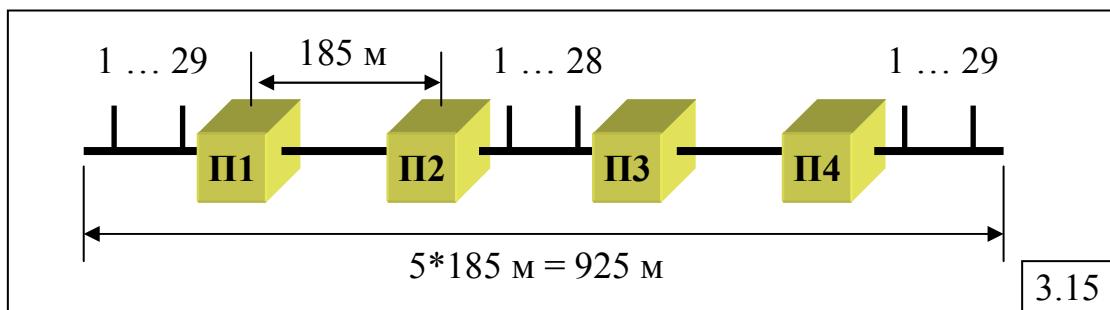
Согласно этой спецификации *недопустимо использование отводов к рабочим станциям*. Станции подключаются непосредственно к основной магистрали через Т-образные BNC-разъемы (рис.3.14). Таким образом, тонкий коаксиальный кабель проходит через сетевые адаптеры всех станций. В остальном, принципы и правила построения одно- и многосегментных ЛВС на тонком и толстом коаксиальном кабеле аналогичны. Отличие – только в ограничениях на размер сети и количество станций.



Основные ограничения для ЛВС Ethernet в соответствии со спецификацией 10Base-2 имеют вид:

- максимальная длина сегмента (расстояние между крайними узлами) – 185 м;
- максимальное число узлов на сегменте – 30;
- минимальное расстояние между узлами – 1 м;
- многосегментная сеть строится по правилу «5-4-3»: максимально 5 сегментов, 4 повторителя, причём нагруженными являются 3 сегмента;
- в каждом из трёх (средний и два крайних) сегментов можно подключать к кабелю до 30 узлов (рис.3.15);

- два других сегмента используются только для увеличения общей протяженности сети, к ним нельзя подсоединять станции;
- повторитель рассматривается как специальный узел, подключенный к сети, поэтому в сети с двумя повторителями допускается иметь только 28 станций.



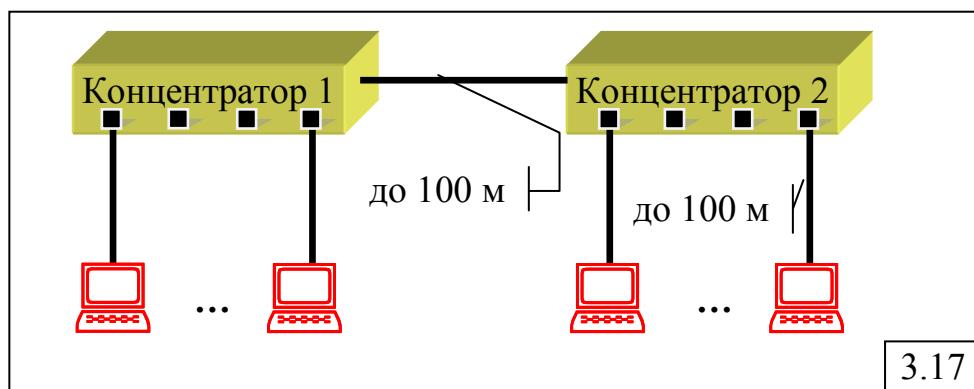
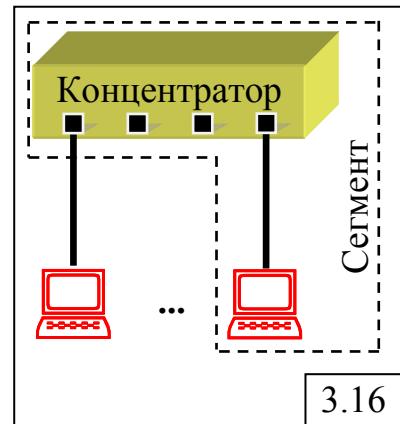
Таким образом, одна сеть Ethernet 10Base-2:

- может содержать не более 86 узлов;
- иметь диаметр (максимальную длину кабеля) – не более 925 м.

### 3.2.2.3. Спецификация 10Base-T

Спецификация 10Base-T, добавленная к стандарту 802.3 в конце 1991 года, описывает сеть Ethernet с топологией типа "звезда" и кабельной системой на основе *неэкранированной витой пары*. Согласно спецификации 10Base-T сегментом сети является кабель, соединяющий рабочую станцию и концентратор. Это означает, что к каждому сегменту может быть подключено лишь два устройства: станция и концентратор (рис.3.16), а количество сегментов равно количеству подключённых к концентратору станций.

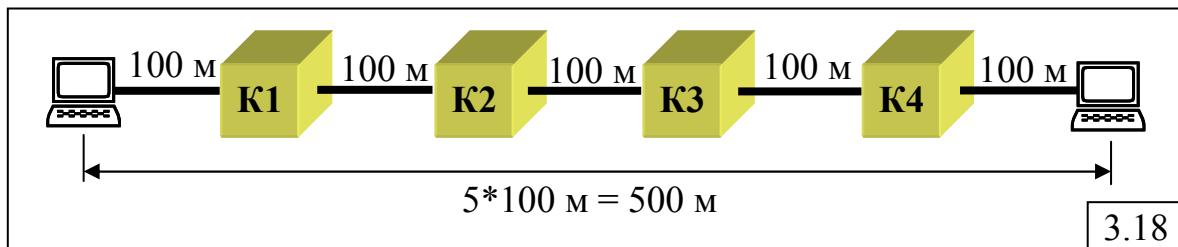
Однако ниже при рассмотрении многосегментных сетей для устранения неоднозначности под сегментом сети Ethernet 10Base-T будем понимать концентратор со всеми подключёнными к нему станциями, то есть сеть, показанную на рис.3.16, будем условно считать односегментной сетью. Многосегментная сеть будет представлять собой объединение нескольких концентраторов с подключёнными к ним станциями (рис.3.17).



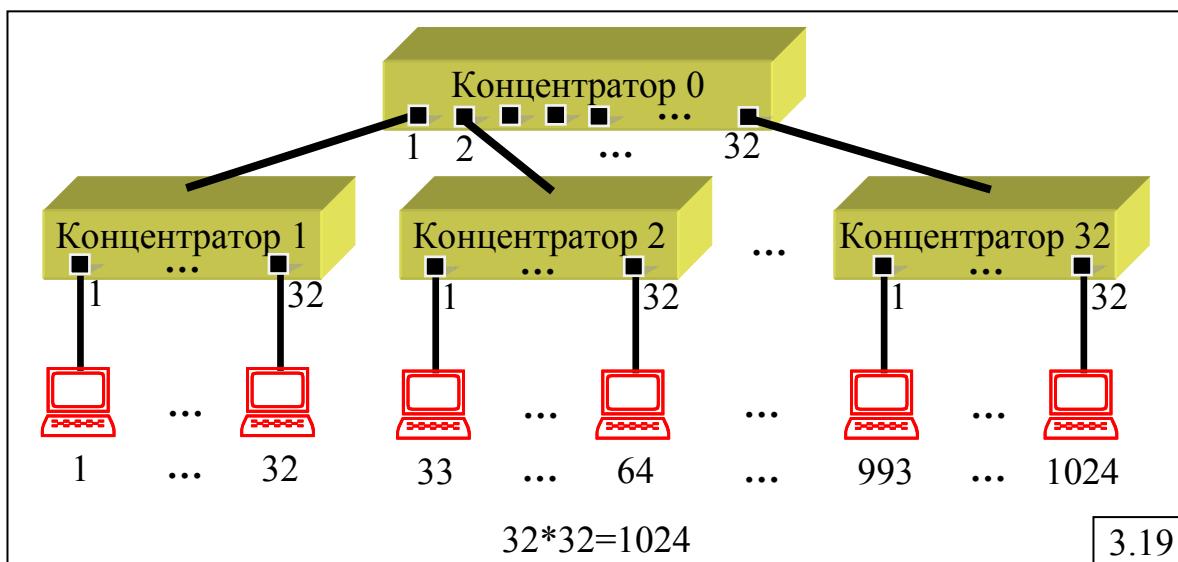
В отличие от рассмотренных выше спецификаций 10Base-5 и 10Base-2, при построении многосегментной сети Ethernet 10Base-T вместо правила «5-4-3» используется правило «4-х хабов», которое гласит, что между любыми двумя станциями в сети должно быть не более 4-х концентраторов (хабов).

Основные ограничения для ЛВС Ethernet в соответствии со спецификацией 10Base-T имеют вид:

- максимальная длина кабеля (между концентратором и рабочей станцией или между двумя концентраторами) – 100 м (рис.3.17);
- число концентраторов между любыми станциями – не более 4;
- максимальный диаметр сети – 500 м (рис.3.18);
- максимальное количество станций в сети – 1024.



Отметим, что максимальное количество станций в ЛВС Ethernet, равное 1024, может быть достигнуто только для спецификации 10Base-T за счёт применения 32-х портовых концентраторов (рис.3.19). В то же время для сетей, построенных на коаксиальном кабеле (10Base-5 и 10Base-2), это значение не достижимо.



Благодаря меньшей стоимости кабельной системы и возможности построения сетей с максимально допустимым количеством станций, сети 10Base-T получили доминирующее положение на рынке и практически полностью вытеснили сети, построенные на коаксиальном кабеле.

#### **3.2.2.4. Спецификация 10Base-F**

10Base-F – совокупность стандартов физического уровня, описывающих работу сети Ethernet на волоконно-оптическом кабеле с

пропускной способностью 10 Мбит/с. В качестве среды передачи данных в оптоволоконной сети Ethernet используется многомодовый волоконно-оптический кабель (ВОК).

Структурная организация сети аналогична стандарту 10Base-T: сетевые адаптеры рабочих станций соединяются с многопортовым повторителем (концентратором) с помощью ВОК и образуют физическую топологию «звезда».

10Base-F включают в себя следующие стандарты.

**1. Стандарт FOIRL (Fiber Optic Inter-Repeater Link):**

- длина оптоволоконного кабеля между повторителями – до 1 км;
- максимальное число повторителей – 4;
- максимальный диаметр сети – 2500 м.

**2. Стандарт 10Base-FL (Fiber Link)** – улучшенный вариант стандарта FOIRL, заключающийся в увеличении мощности передатчиков, за счёт чего максимальное расстояние между узлом и повторителем может достигать 2000 м, при этом:

- максимальное число повторителей – 4;
- максимальный диаметр сети – 2500 м.

**3. Стандарт 10Base-FB (Fiber Backbone)** предназначен только для объединения повторителей в магистраль, при этом:

- между узлами сети можно установить до 5 повторителей стандарта 10Base-FB;
- максимальная длина одного сегмента – 2000 м;
- максимальный диаметр сети – 2740 м.

В отличие от ранее рассмотренных сетей, повторители, используемые в ЛВС Ethernet 10Base-FB, при отсутствии кадров для передачи обмениваются специальными последовательностями сигналов, что позволяет постоянно поддерживать синхронизацию в сети. Поэтому ЛВС, построенную по стандарту 10Base-FB, называют «синхронный Ethernet». Благодаря меньшим задержкам при передаче данных из одного сегмента в другой, количество повторителей увеличено до 5.

В табл.3.2 сведены основные параметры стандартов оптических сетей Ethernet 10Base-F.

Таблица 3.2

Стандарт	FOIRL	10Base-FL	10Base-FB
<b>Отличительная особенность</b>		Мощные передатчики	Для соединения повторителей
<b>Расстояние между узлами</b>	1000 м	2000 м	2000 м
<b>Число повторителей</b>	4	4	5
<b>Диаметр сети</b>	2500 м	2500 м	2740 м

### 3.2.3. Канальный уровень ЛВС Ethernet

Стандарт ЛВС Ethernet канального уровня IEEE 802.3 описывает формат используемых в сети кадров и метод доступа к среде передачи данных CSMA/CD.

В процессе эволюции сетей Ethernet появились 4 типа кадров:

- Ethernet II или Ethernet DIX, предложенный фирмами DEC, Intel и Xerox (DIX);
- Raw 802.3 или 802.3/Novell, появившийся в результате усилий компании Novell по созданию своего стека протоколов в сетях Ethernet;
- 802.3/LLC или 802.3/802.2, появившийся как результат разделения функций канального уровня на подуровни MAC и LLC;
- Ethernet SNAP, появление которого было вызвано необходимостью приведения предыдущих форматов к общему стандарту.

#### 3.2.3.1. Кадр Ethernet II (Ethernet DIX)

Стандарт Ethernet II был разработан фирмами DEC, Intel и Xerox (DIX) и с небольшими изменениями принят в 1982 году.

Формат кадра Ethernet II представлен на рис.3.20.



**П – преамбула** (8 байт):

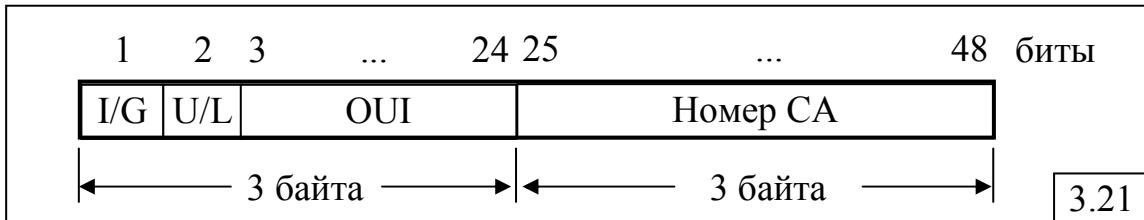
- используется для синхронизации станций сети;
- содержит код 10101010 в первых семи байтах и код 10101011 в последнем байте.

**AH – адрес назначения** (6 байт):

- длина поля составляет 6 байт, но может быть 2 байта, если адрес установлен администратором ЛВС только для внутреннего пользования;
- старший (самый первый) бит в поле адреса (рис.3.21) указывает тип адреса (I/G – Individual/Group):

- 0 – адрес назначения является **индивидуальным**, т.е. кадр предназначен конкретной рабочей станции; в остальных разрядах поля адреса назначения указывается уникальный физический адрес (MAC-адрес) конкретной рабочей станции;
- 1 – адрес назначения является **групповым**, т.е. кадр предназначен группе рабочих станций (тогда в последующих разрядах указывается адрес конкретной группы рабочих станций), или **широковещательным**, если все остальные разряды равны 1, то есть кадр адресован всем рабочим станциям в ЛВС;

- второй бит в поле адреса указывает *способ назначения адреса* (U/L – Universal/Local):
  - **0** – адрес является **универсальным** физическим адресом в ЛВС, т.е. адрес сетевого адаптера назначен *централизованно* комитетом IEEE, который распределяет между производителями сетевых адаптеров так называемые организационно уникальные идентификаторы (Organizationally Unique Identifier, OUI), размещаемые в первых трех байтах адреса, а в следующих трех байтах помещается номер сетевого адаптера, присваиваемый производителем (рис.3.21);
  - **1** – адрес **локальный**, т.е. назначен администратором ЛВС и используется только в пределах этой сети.



#### **АИ – адрес источника** (6 байт):

- длина поля составляет 6 байт, но, как и адрес назначения, может иметь длину 2 байта;
  - старший бит первого байта (поля I/G) всегда равен 0;
  - не может содержать широковещательный адрес:  
FF-FF-FF-FF-FF-FF.

#### **Тип – тип протокола** (2 байта):

- идентифицирует тип протокола более высокого уровня, используемого для его передачи или приема, и позволяющего множеству протоколов высокого уровня разделять ЛВС без вникания в содержимое кадров друг друга;
  - примеры значений поля «тип», идентифицирующих различные протоколы:

➤ IP (Internet Protocol)	$0800_{16}$
➤ ARP (Adress Resolution Protocol)	$0806_{16}$
➤ Reverse ARP	$8035_{16}$
➤ Apple Talk	$809B_{16}$
➤ NetWare IPX/SPX	$8137_{16}$

(здесь индекс  $_{16}$  – означает шестнадцатеричное число).

#### **Данные – поле данных** (46-1500 байт):

- может иметь длину от 46 до 1500 байт.

#### **КС – контрольная сумма:**

- содержит *остаток избыточной циклической суммы* (Cyclic Redundancy Checksum – CRC), вычисленной с помощью полиномов типа CRC-32 для всех полей кадра: АН+АИ+Тип+Данные (без преамбулы).

Таким образом, *минимальная длина* кадра Ethernet (без преамбулы) **64** байта, а *максимальная – 1518* байтов.

### 3.2.3.2. Кадр Raw 802.3 (IEEE 802.3/Novell)

В основу стандарта IEEE 802.3 был положен кадр Raw 802.3, предложенный фирмой Novell и называемый также кадром 802.3/Novell, формат которого показан на рис.3.22.



Основные отличия этого кадра от кадра Ethernet II заключаются в следующем:

- 1) из восьмибайтового поля преамбулы **П**, которое стало длиной 7 байт, выделено однобайтовое поле **НО** – «Начальный ограничитель кадра», которое содержит код 10101011, указывающий на начало кадра;
- 2) вместо поля «Тип протокола» появилось двухбайтовое поле **Д** – «Длина», которое определяет длину поля данных в кадре; отсутствие поля «Тип протокола» обусловлено тем, что кадр 802.3/Novell соответствует только протоколу IPX/SPX и лишь этот протокол может работать с ним;
- 3) поле данных может содержать от 0 до 1500 байт, но если длина поля меньше 46 байт, то используется дополнительное поле **Н** – «Набивка», с помощью которого кадр дополняется до минимально допустимого значения в 46 байт, если поле данных меньше 46 байт.

Таким образом, длина кадра находится в диапазоне от 64 до 1518 байт, не считая преамбулы и признака начала кадра. Важной особенностью стандарта IEEE 802.3 является возможность передачи прикладным процессом данных длиной менее 46 байтов, благодаря тому, что кадр автоматически дополняется до нужного размера пустыми символами в поле «Набивка». В стандарте Ethernet II такие ситуации рассматриваются как ошибочные.

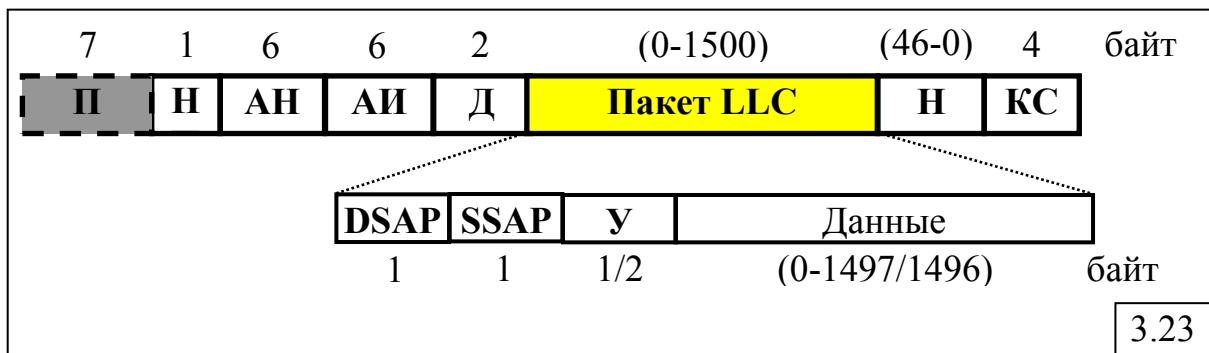
### 3.2.3.3. Кадр 802.3/LLC (кадр 802.3/802.2)

Кадр 802.3/LLC (802.3/802.2) содержит те же поля, что и Raw 802.3 (рис.3.23). Отличие состоит лишь в том, что в поле данных вставляется пакет подуровня управления логическим соединением LLC (без граничных флагов), содержащий в качестве заголовка три однобайтовых поля:

- **DSAP** (Destination Service Access Point) – точка доступа к услугам получателя (1 байт) определяет тип протокола верхнего (сетевого) уровня получателя кадра;
- **SSAP** (Source Service Access Point) – точка доступа к услугам источника (1 байт) определяет тип протокола верхнего (сетевого) уровня источника кадра;
- **У** – управление (1 или 2 байта) – содержит информацию для управления одним из трех сервисов, предоставляемых подуровнем LLC; например, значение  $03_{16}$  соответствует ненумерованному формату в

стандарте Ethernet 802.2, указывающему, что подуровень LLC обеспечивает обслуживание без установления логического соединения.

Поля DSAP, SSAP и У образуют заголовок пакета LLC.



Так как поле «Управление» пакета LLC имеет длину 1 (в режиме LLC1) или 2 байта (в режиме LLC2), то максимальный размер поля данных уменьшается до 1497 или 1496 байт соответственно.

#### 3.2.3.4. Кадр Ethernet SNAP

Кадр Ethernet SNAP (SNAP – SubNetwork Access Protocol), протокол доступа к подсетям) предназначен для устранения разнообразия в форматах кадров и в кодировках типов протоколов, сообщения которых вложены в поле данных кадров Ethernet.

Структура кадра SNAP является развитием структуры кадра 802.3/LLC за счет введения дополнительного заголовка протокола *SNAP*, который находится за заголовком пакета LLC и включает в себя 2 поля:

- **идентификатор организации** (3 байта) содержит идентификатор той организации, которая контролирует коды протоколов, указываемые в поле «тип» (коды протоколов для ЛВС контролирует IEEE, который имеет идентификатор организации, равный 000000; если в будущем потребуются другие коды протоколов, то достаточно указать другой идентификатор организации, назначающей эти коды, не меняя старые значения кодов);
- **тип** (2 байта) – состоит из 2-х байт и соответствует полю «Тип» кадра Ethernet II, то есть в нем используются те же значения кодов протоколов более высокого *сетевого уровня*.

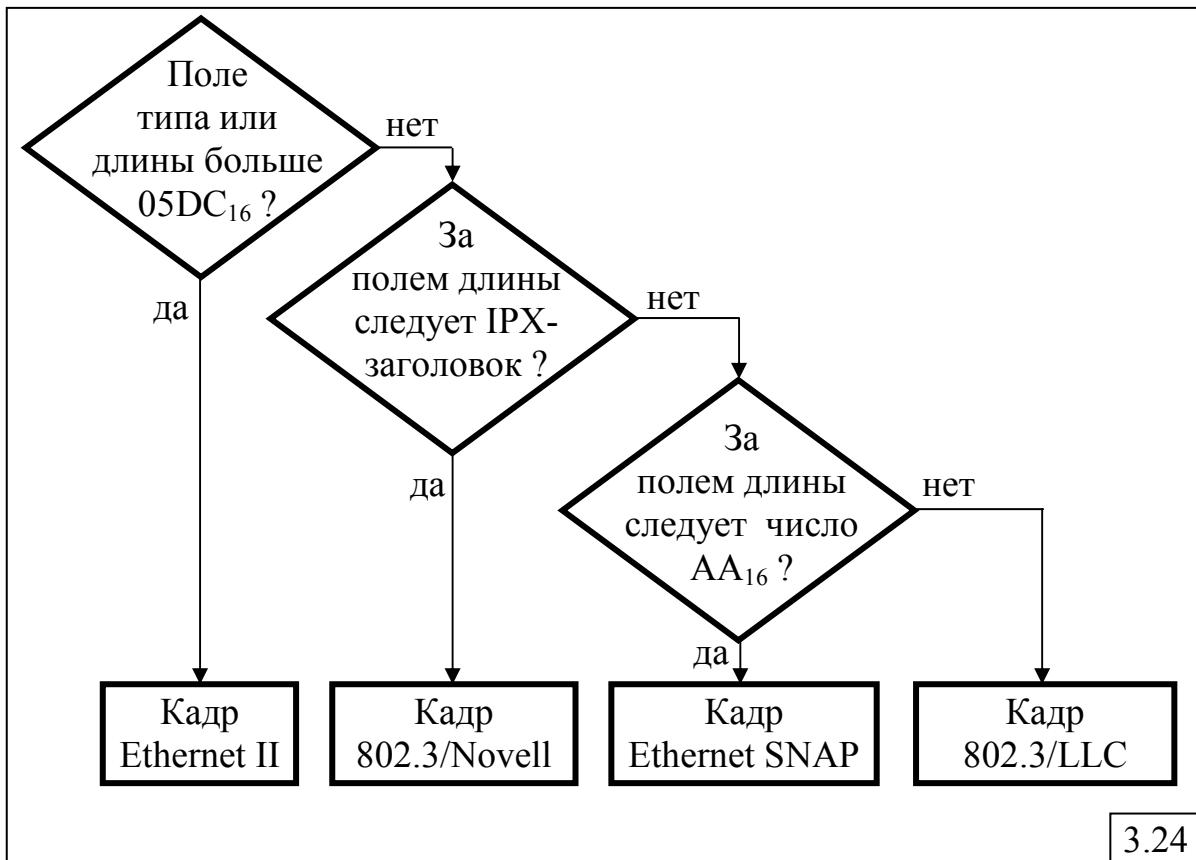
При этом 3 поля заголовка пакета LLC в кадре Ethernet SNAP имеют вполне конкретные значения:

- **DSAP** (1 байт) всегда содержит AA<sub>16</sub> и указывает на то, что кадр имеет формат типа Ethernet SNAP;
- **SSAP** (1 байт) всегда содержит AA<sub>16</sub> и указывает на то, что кадр имеет формат типа Ethernet SNAP;
- **управление** (1 байт) содержит число 03<sub>16</sub>.

#### 3.2.3.5. Алгоритм определения типа кадра

Практически все сетевые адAPTERЫ Ethernet могут работать со всеми четырьмя типами кадров, автоматически распознавая их.

На рис.3.24 приведена схема алгоритма определения типа кадра в ЛВС Ethernet. Поскольку для кодирования типа протокола в двухбайтовом поле «Тип/Длина» указываются значения, превышающие значение максимальной длины поля данных, равное 1500 или в шестнадцатеричной системе счисления  $05DC_{16}$ , кадры Ethernet II легко отличить от других типов кадров по значению этого поля. Затем проверяется наличие или отсутствие полей LLC, которые могут отсутствовать только в том случае, если за полем длины следует заголовок пакета IPX, а именно 2-байтовое поле заполненное единицами. Затем проверяются значения полей DSAP и SSAP: если они равны  $AA_{16}$ , то это кадр Ethernet SNAP, в противном случае – кадр 802.3/LLC.



3.24

### 3.2.3.6. Протокол CSMA/CD

При описании протокола CSMA/CD временные интервалы удобно измерять не в абсолютных единицах времени (мкс или мс), а в количестве так называемых «битовых интервалов».

**Битовый интервал** – это интервал, соответствующий передаче одного бита, то есть это время между появлением двух последовательных бит. Обозначим через  $bt$  – битовый интервал, тогда длительность битового интервала будет определяться следующим образом:  $\tau_{bt} = 1/C$ , где  $C$  – пропускная способность среды передачи (скорость передачи данных). При пропускной способности  $C=10$  Мбит/с длительность битового интервала  $\tau_{bt} = 100$  нс и  $\tau_{bt} = 10$  нс при  $C=100$  Мбит/с.

Поскольку протокол CSMA/CD применяется в ЛВС Ethernet с пропускными способностями среды передачи данных 10 Мбит/с, 100 Мбит/с и 1 Гбит/с, использование понятия битового интервала позволяет обобщить описание протокола CSMA/CD для всех этих сетей.

**При передаче данных** согласно протоколу CSMA/CD станции выполняют следующие этапы.

1. *Прослушивание* до начала передачи.

Станция может передавать кадр, если разделяемая среда (канал связи) свободна. Для этого станции непрерывно следят, не появился ли в канале сигнал "наличие несущей", который распознается по уровню напряжения и свидетельствует о занятости канала.

2. *Задержка передачи*, если канал занят. При этом кадр, ожидающий освобождения канала, находится в буфере сетевого адаптера.

3. *Начало передачи* кадра, если канал свободен. Признаком незанятости канала является отсутствие в нём несущей частоты.

Если канал свободен или только что освободился (сигнал "отсутствие несущей"), станция может начать передачу, выдержав технологическую паузу, называемую **межкадровым интервалом**, длиной в 96 битовых интервалов, что для ЛВС с пропускной способностью 10 Мбит/с составляет 9,6 мкс.

**Необходимость межкадрового интервала** обусловлена следующими обстоятельствами. Во-первых, поскольку все станции отслеживают передачу всех кадров в сети, то после завершения передачи все *сетевые адаптеры должны быть приведены в исходное состояние* для приёма очередного кадра, для чего требуется определённое время. Во-вторых, использование межкадрового интервала *предотвращает монопольный захват среды* одной станцией.

По завершении межкадрового интервала станции могут начать передачу своего кадра. Из-за задержек распространения сигнала по кабелю не все станции строго одновременно фиксируют факт окончания передачи кадра.

4. *Передача кадра и прослушивание коллизий*. Кадр передается по кабельной системе в обоих направлениях. Если в это же время ещё одна станция начнёт передачу кадра, в канале возникнет **коллизия**. Кадры, вовлеченные в коллизию, превратятся во **фрагменты** (произойдет наложение кадров). Поэтому во время передачи станции прослушивают канал с целью обнаружения коллизий. Возникновение коллизии распознается по наличию сигнала в канале, уровень которого не меньше уровня сигнала, производимого при одновременной передаче двумя или несколькими трансиверами.

Если коллизия возникла, но другие станции еще не обнаружили ее, они могут попытаться начать передачу. Кадры этих станций тогда будут вовлечены в новую коллизию. Для исключения такой ситуации вовлеченные в коллизию станции начинают передавать **сигнал затора** с

тем, чтобы все остальные станции сегмента удостоверились в том, что линия занята.

**Сигнал затора** – специальная последовательность из 32 бит, называемая *jam-последовательностью*.

Станции, вовлеченные в коллизию, увеличивают на 1 свои **счетчики числа попыток передачи**.

Станция считает, что она *управляет сегментом* кабеля, если ею уже передано более 64 байт. Коллизия, возникающая с кадром длиной более 64 байт, называется **поздней коллизией**, что обычно свидетельствует о некорректном монтаже кабельной системы, например, о том, что какой-то сегмент может быть длиннее, чем это определено спецификацией для данного типа кабельной системы.

### 5. Ожидание перед повторной передачей.

Для выбора момента повторной передачи станция действует согласно так называемому **алгоритму отступления**, обеспечивающему различные времена готовности к повторной передаче. Повторная передача откладывается на случайное время кратное 512 битовым интервалам, что для ЛВС с пропускной способностью 10 Мбит/с составляет 51,2 мкс:

$$t = 51,2 * N.$$

Здесь  $N$  – случайная величина, принимающая целочисленное значение из интервала  $(0; 2^n)$  в соответствии с равномерным законом распределения, где  $n$  – количество коллизий (повторных передач), причем  $n = 1, 2, \dots, 10$ .

При  $n = 1$  случайная величина  $N$  может принять с вероятностью 1/3 одно из трёх значений: 0, 1, 2, а при  $n = 2$  – с вероятностью 1/5 одно из пяти значений: 0, 1, 2, 3, 4.

После десятой коллизии  $n$  не меняется и остается равным 10. Таким образом, максимальное время, на которое откладывается передача кадра, равно  $\tau_{\max} = 51,2 \text{ мкс} * 2^{10} \cong 52,4 \text{ мс}$ .

### 6. Повторная передача или прекращение работы.

Станция может попытаться передать кадр до 16 раз, прежде чем прекратит свои попытки. В этом случае кадр остается не переданным.

**При приёме данных** станция, находящаяся в сети, должна выполнять следующие действия.

1. *Просмотр поступающих кадров* данных и обнаружение фрагментов.

В ЛВС Ethernet все станции просматривают все кадры, проходящие по каналу связи. При этом для каждого кадра проверяется, имеет ли он допустимую длину (не менее 64 байт), то есть не является ли он фрагментом, порожденным коллизией.

### 2. Проверка адреса получателя.

Если кадр данных не является фрагментом, принимающая станция проверяет адрес получателя кадра, чтобы определить, следует ли обрабатывать кадр.

Если кадр адресован данной станции, является широковещательным или имеет соответствующий групповой адрес, станция проверяет целостность кадра.

### 3. Проверка целостности кадра данных.

Для того, чтобы избежать обработки искаженных при передаче по каналу или некорректно сформированных на передающей станции кадров, принимающая станция должна проверить:

- *длину кадра*: если кадр длиннее 1518 байт, он считается переполненным; переполненные кадры могут появляться в результате неисправностей сетевого драйвера;
- *контрольную последовательность кадра* с помощью циклического избыточного кода;
- если контрольная последовательность некорректна, проверяется *выравненность кадра*: все кадры должны содержать целое число байт (например, не 122,5 байт).

Если контрольная последовательность кадра некорректна, но кадр содержит целое число байт (корректно выровнен), считается, что имеет место ошибка контрольной последовательности.

Таким образом, проверка кадра принимающей станцией заключается в определении:

- является ли кадр фрагментом;
- не слишком ли велика его длина;
- ошибочна ли его контрольная последовательность;
- корректно ли он выровнен.

Если какая-либо проверка завершилась неудачей, кадр уничтожается и его содержимое не передается для обработки протоколу сетевого уровня.

### 4. Обработка кадра.

Кадр, успешно прошедший все проверки, считается корректным, правильно сформированным и имеющим допустимую длину. Такой кадр освобождается от заголовка и концевика, а его содержимое передаётся для дальнейшей обработки протоколу сетевого уровня.

Если станция корректно подключена к сети, обладает исправными картами и трансиверами, то она должна принимать и передавать корректно сформированные кадры данных. Для проверки работоспособности сети используются анализаторы протоколов, которые обеспечивают проверку качества связи со станциями и с файл-сервером. Для этого используются специальные диагностические кадры в виде широковещательного сообщения, называемого кадром "пинг-понг", на который должны ответить станции сети.

## 3.2.4. Многосегментные ЛВС Ethernet

ЛВС Ethernet может объединять сегменты, построенные на основе разных типов кабелей: толстого или тонкого коаксиального кабеля, витой пары, волоконно-оптического кабеля. При этом количество сегментов в сети может превышать указанное ранее в соответствии с правилом «5-4-3»

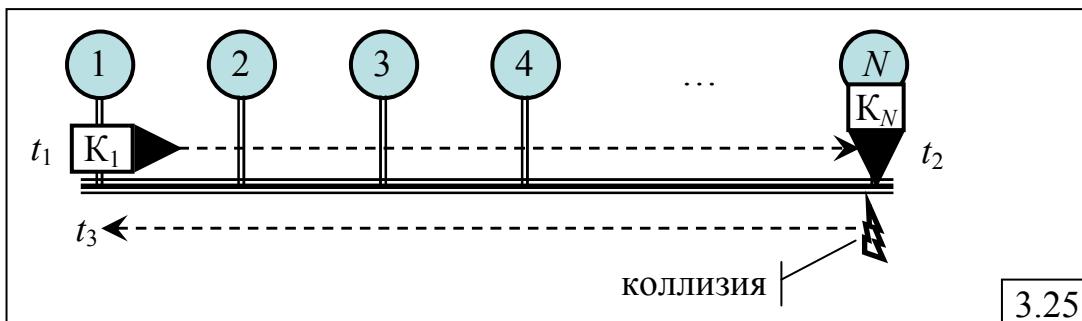
значение 5. Чтобы сеть Ethernet, состоящая из сегментов различной физической природы, работала корректно, необходимо выполнение четырех основных условий:

- количество станций в сети не более 1024;
- максимальная длина каждого сегмента не более величины, определенной в соответствующем стандарте физического уровня (500 м и 185 м – соответственно для толстого и тонкого коаксиального кабеля; 100 м – для неэкранированной витой пары; 2000 м – для оптоволоконного кабеля);
- время двойного оборота сигнала (Path Delay Value, PDV) между двумя самыми удаленными друг от друга станциями сети не более 575 битовых интервала;
- сокращение межкадрового интервала (Path Variability Value, PVV) при прохождении последовательности кадров через все повторители должно быть не больше, чем 49 битовых интервала. Так как при отправке кадров конечные узлы обеспечивают начальное межкадровое расстояние в 96 битовых интервалов, то после прохождения повторителей оно должно быть не меньше, чем  $96 - 49 = 47$  битовых интервалов.

Соблюдение этих требований обеспечивает корректность работы сети даже в тех случаях, когда нарушаются правила конфигурирования, определяющие максимальное количество повторителей и общую длину сети в 2500 м.

#### 3.2.4.1. Условие корректности ЛВС

Для корректной работы сети Ethernet необходимо, чтобы станции всегда могли обнаружить коллизию, если она возникла в процессе передачи кадра. Если станция прекратит прослушивание среды передачи раньше, чем коллизия может произойти, передаваемый кадр будет потерян. Поэтому передающая станция должна обнаружить коллизию, которую вызвал переданный ею кадр, еще до того, как она закончит передачу этого кадра. Поскольку до начала передачи все станции сети прослушивают канал, то коллизия в худшем случае может возникнуть при передаче кадров между наиболее удаленными друг от друга станциями сети. Такая ситуация показана на рис.3.25.



В момент времени  $t_1$  узел 1 начинает передачу кадра  $K_1$ . Положим, что в момент  $t_2$ , когда кадр  $K_1$  почти достигает наиболее удалённого узла  $N$ , последний начинает передачу кадра  $K_N$ . В результате столкновения

кадров  $K_1$  и  $K_N$  возникает коллизия, которая распространяется по каналу и в момент  $t_3$  достигает узла 1. Таким образом, сигнал проходит дважды между наиболее удаленными друг от друга узлами сети в течение времени  $T_{PDV} = t_3 - t_1$ , которое называется *временем двойного оборота* (*Path Delay Value, PDV*). Для распознавания такой коллизии узлом 1 необходимо, чтобы минимальное время  $T_{\min}$  передачи кадра этим узлом было больше *времени двойного оборота*  $T_{PDV}$ :  $T_{\min} > T_{PDV}$ .

Минимальное время  $T_{\min}$  передачи кадра связано с минимальной длиной кадра  $l_{\min}$  и пропускной способностью канала связи  $C$  соотношением:  $T_{\min} = \frac{l_{\min}}{C}$ .

Время двойного оборота  $T_{PDV}$  зависит от максимального расстояния между наиболее удаленными станциями ЛВС (длины кабельной системы)  $L$  и скорости распространения сигнала в кабеле  $v$ :  $T_{PDV} = \frac{2L}{v}$ , где скорость распространения сигнала зависит от типа передающей среды и определяется как  $v = \frac{c}{2 \div 3}$  ( $c$  – скорость света).

Тогда *условие корректности ЛВС*, обусловленное необходимостью обнаружения всех возникающих в сети коллизий, примет вид:

$$\frac{l_{\min}}{C} > \frac{2L}{v}.$$

Последнее выражение может использоваться для определения максимального расстояния между наиболее удаленными станциями или для определения минимального размера кадра при заданном расстоянии:

$$L < \frac{vl_{\min}}{2C}; \quad l_{\min} > \frac{2LC}{v}.$$

**Пример.** Рассмотрим сети Fast Ethernet и Gigabit Ethernet.

Пусть:  $v = 10^8 \text{ м/с}$ ;  $l_{\min} = 64 \text{ байт} = 512 \text{ бит}$ ,

Пропускные способности сетей Fast Ethernet (*FE*) и Gigabit Ethernet (*GE*) соответственно равны:  $C_{FE} = 10^8 \text{ бит/с}$  и  $C_{GE} = 10^9 \text{ бит/с}$ .

Тогда:

$$L_{FE} < \frac{10^8 * 512}{2 * 10^8} = 256 \text{ м} \quad \text{и} \quad L_{GE} < \frac{10^8 * 512}{2 * 10^9} = 25,6 \text{ м}.$$

Таким образом, диаметр сети Fast Ethernet не должен превышать 256 метров, а диаметр сети Gigabit Ethernet – 25 метров.

Очевидно, что столь маленький размер сети Gigabit Ethernet не мог удовлетворить ни разработчиков, ни пользователей сети.

Для увеличения диаметра сети Gigabit Ethernet хотя бы до 200 м необходимо увеличить минимальную длину кадра до значения:

$$l_{\min} > \frac{2LC}{v} = \frac{2 * 200 * 10^9}{10^8} = 4000 \text{бит} = 500 \text{байт.}$$

В ЛВС GigabitEthernet, как будет показано ниже, минимальная длина кадра увеличена до значения 512 байт, что позволило увеличить диаметр сети до 200 м.

### 3.2.4.2. Расчёт времени двойного оборота (PDV)

Для упрощения расчета PDV обычно используются справочные данные IEEE, содержащие значения задержек распространения сигналов в повторителях, приемопередатчиках и различных физических средах. В табл.3.3 приведены данные, необходимые для расчета значения PDV для всех физических стандартов сетей Ethernet.

**Левый сегмент** – это передающий сегмент. Затем сигнал проходит через **промежуточные сегменты** и доходит до наиболее удаленного **правого** (принимающего) сегмента. Именно здесь в худшем случае происходит столкновение кадров и возникает коллизия.

С каждым сегментом связана постоянная задержка, названная **базой**, которая зависит только от типа сегмента и от положения сегмента на пути сигнала (левый, промежуточный или правый). Кроме того, с каждым сегментом связана задержка распространения сигнала вдоль кабеля сегмента, которая зависит от длины сегмента и вычисляется путем умножения времени задержки сигнала на одном метре кабеля (в битовых интервалах) на длину кабеля в метрах.

Таблица 3.3

Тип сегмента	База левого сегмента, bt	База промежуточного сегмента, bt	База правого сегмента, bt	Задержка среды на 1 м, bt	Максим. длина сегмента, м
10Base-5	11,8	46,5	169,5	0,0866	500
10Base-2	11,8	46,5	169,5	0,1026	185
10Base-T	15,3	42,0	165,0	0,113	100
10Base-FB	-	24,0	-	0,1	2000
10Base-FL	12,3	33,5	156,5	0,1	2000
FOIRL	7,8	29,0	152,0	0,1	1000

Расчёт PDV выполняется для двух наиболее удаленных (по времени распространения сигнала) станций сети и заключается в вычислении задержек, вносимых каждым отрезком кабеля, и суммировании этих задержек с базами левого, промежуточных и правого сегментов. Общее значение PDV (сумма значений всех сегментов) не должно превышать 575 битовых интервалов. Это значение получено, исходя из минимальной длины кадра в 10-мегабитном Ethernet в 64 байта плюс преамбула 8 байт, всего 72 байта или 576 бит. Следовательно, время двойного оборота должно быть меньше 57,5 мкс.

Так как левый и правый сегменты имеют различные величины базовой задержки, необходимо выполнить расчеты дважды, поменяв при втором расчёте местами левый и правый сегменты сети.

На основе представленных в табл.3.3 значений задержки (в битовых интервалах) распространения сигнала по кабелю в расчете на 1 метр можно оценить скорость распространения сигнала по кабелю и соответствующие значения коэффициентов замедления (уменьшения скорости передачи сигнала по сравнению со скоростью света):

- для толстого коаксиального кабеля:

$$v_5 = \frac{1000}{8,66} 10^6 [\text{м}/\text{с}] \approx 115,5 * 10^6 [\text{м}/\text{с}] = 115500 [\text{км}/\text{с}]; \quad k_5 = \frac{300000}{115500} \approx 2,6;$$

- для тонкого коаксиального кабеля:

$$v_2 = \frac{1000}{10,26} 10^6 [\text{м}/\text{с}] \approx 97,5 * 10^6 [\text{м}/\text{с}] = 97500 [\text{км}/\text{с}]; \quad k_2 = \frac{300000}{97500} \approx 3,1;$$

- для витой пары:

$$v_T = \frac{1000}{11,3} 10^6 [\text{м}/\text{с}] \approx 88500 [\text{км}/\text{с}]; \quad k_T = \frac{300000}{88500} \approx 3,4;$$

- для оптического кабеля:

$$v_F = \frac{1000}{10} 10^6 [\text{м}/\text{с}] = 100000 [\text{км}/\text{с}]; \quad k_F = \frac{300000}{100000} = 3.$$

### 3.2.4.3. Расчёт уменьшения межкадрового интервала (PVV)

Для того чтобы определить корректность построения многосегментной сети, необходимо рассчитать уменьшение межкадрового интервала повторителями при передаче кадров в сети, то есть величину PVV.

Для расчета PVV используются рекомендованные институтом IEEE предельные значения (в битовых интервалах), определяющие уменьшение межкадрового интервала при прохождении повторителей различных физических сред. Эти значения для передающих и промежуточных сегментов приведены в табл.3.4.

Сумма этих величин дает значение PVV, которое должно быть меньше предельного значения в 49 битовых интервала.

Таблица 3.4

Тип сегмента	Передающий сегмент, bt	Промежуточный сегмент, bt
10Base-5 или 10Base-2	16	11
10Base-FB	-	2
10Base-FL	10,5	8
10Base-T	10,5	8

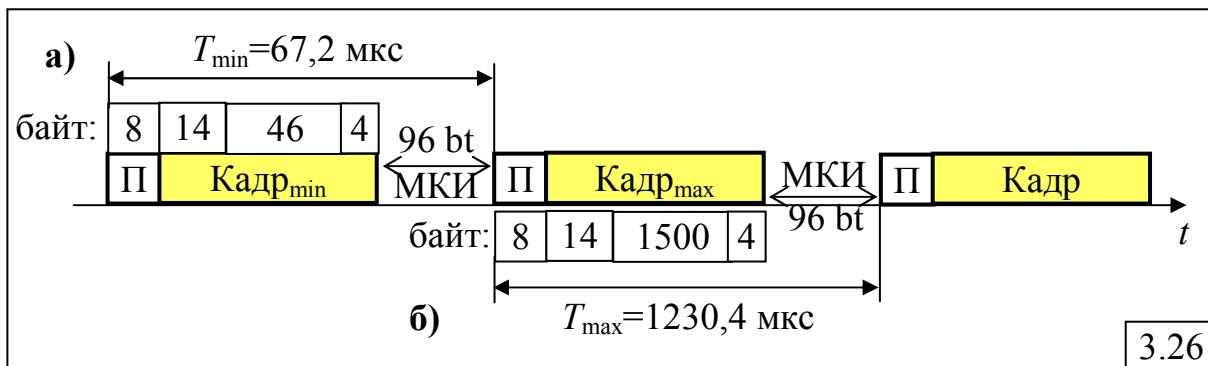
### 3.2.5. Расчет показателей производительности ЛВС Ethernet

В качестве показателей производительности среды передачи данных в ЛВС Ethernet используются следующие величины:

- **пропускная способность канала связи**  $C$  [бит/с], определяемая как предельная скорость передачи данных;
- **полезная (эффективная) пропускная способность канала связи**  $C_n$  [бит/с], определяемая как предельная скорость передачи данных пользователя без учета передаваемых служебных символов в заголовках и концевиках и без учета возможных простоев канала и коллизий;
- **реальная (фактическая) скорость передачи данных**  $C_p$  [бит/с], определяемая с учетом возможных простоев канала и коллизий;
- **пропускная способность среды передачи**  $\Lambda$  [кадров/с], измеряемая количеством кадров, передаваемых за единицу времени.

Выполним расчёт перечисленных характеристик применительно к ЛВС Ethernet с пропускной способностью  $C=10$  Мбит/с.

Определим **пропускную способность**  $\Lambda$  [кадров/с] **среды передачи** для кадров минимальной (рис.3.26,а) и максимальной (рис.3.26,б) длины.



**Кадр минимальной длины с преамбулой:**

$$L_{min} = 8 \text{ байт (преамбула)} + 64 \text{ байта (кадр)} = 72 \text{ байта * 8 бит} = 576 \text{ бит};$$

$$T_{min} = 576 \text{ бит * } 0,1 \text{ мкс} = 57,6 \text{ мкс} + 9,6 \text{ мкс (межкадр.интервал)} = 67,2 \text{ мкс};$$

$$\Lambda_{max} = 1 / T_{min} \approx 14880 \text{ кадров / с.}$$

**Кадр максимальной длины с преамбулой:**

$$L_{max} = 8 \text{ байт (преамб.)} + 1518 \text{ байт (кадр)} = 1526 \text{ байт * 8 бит} = 12208 \text{ бит};$$

$$T_{max} = 12208 \text{ бит * } 0,1 \text{ мкс} = 1220,8 \text{ мкс} + 9,6 \text{ мкс (межкадр.инт.)} = 1230,4 \text{ мкс};$$

$$\Lambda_{min} = 1 / T_{max} \approx 813 \text{ кадров / с.}$$

Таким образом, в 10-мегабитной сети Ethernet без учёта возможных коллизий **максимально** может быть передано за одну секунду от **813 кадров** (максимальной длины) до **14 880 кадров** (минимальной длины).

Отсюда легко определить полезную (эффективную) пропускную способность и коэффициент использования канала связи при передаче кадров минимальной и максимальной длины:

$$C_{\min} = 14880 * 46 * 8 = 5,48 \text{ Мбит/с}; \quad k_{\min} = \frac{C_{\min}}{C} = 0,548;$$

$$C_{\max} = 813 * 1500 * 8 = 9,76 \text{ Мбит/с}; \quad k_{\max} = \frac{C_{\max}}{C} = 0,976.$$

Полученные значения показателей производительности и коэффициента использования канала связи не учитывают *простоты сети* и возникающие при передаче данных *коллизии*, значительно снижающие реальную пропускную способность ЛВС Ethernet.

### 3.2.6. Достоинства и недостатки ЛВС Ethernet

В качестве достоинств ЛВС Ethernet следует отметить:

- *простоту установки и эксплуатации*;
- *невысокую стоимость реализации*, обусловленную простотой и невысокой стоимостью сетевых адаптеров и концентраторов;
- возможность использования *различных типов кабеля* и схем прокладки кабельной системы.

К недостаткам сети Ethernet можно отнести:

- *снижение реальной скорости* передачи данных в сильно загруженной сети, вплоть до ее полной остановки;
- *трудности поиска неисправностей*: при обрыве кабеля отказывает весь сегмент ЛВС и локализовать неисправный узел или участок сети достаточно сложно.

## 3.3. Высокоскоростные технологии Ethernet

Первыми высокоскоростными технологиями для передачи данных по сети Ethernet со скоростью 100 Мбит/с были две конкурирующие технологии – Fast Ethernet и 100VG-AnyLAN.

### 3.3.1. Fast Ethernet

**Fast Ethernet (Быстрый Ethernet)** – высокоскоростная технология, предложенная фирмой 3Com для реализации сети Ethernet со скоростью передачи данных 100 Мбит/с, сохранившая в максимальной степени особенности 10-мегабитного Ethernet (Ethernet-10) и реализованная в виде стандарта 802.3u.

Основной целью при разработке технологии Fast Ethernet было обеспечение преемственности по отношению к 10-мегабитному Ethernet за счёт сохранения формата кадров и метода доступа CSMA/CD, что позволяет использовать прежнее программное обеспечение и средства управления сетями Ethernet. Одним из требований было также использование кабельной системы на основе витой пары категории 3, получившей на момент появления Fast Ethernet широкое распространение в сетях Ethernet-10. В связи с этим все отличия Fast Ethernet от Ethernet-10 сосредоточены на физическом уровне.

В Fast Ethernet предусмотрены 3 варианта *кабельных систем*:

- многомодовый ВОК (используется 2 волокна);

- витая пара категории 5 (используется 2 пары);
- витая пара категории 3 (используется 4 пары).

*Структура* сети – иерархическая древовидная, построенная на концентраторах (как 10Base-T и 10Base-F), поскольку не предусматривалось использование коаксиального кабеля.

Диаметр сети Fast Ethernet, как показано в п.3.2.5, составляет немногим более 200 метров, что объясняется уменьшением времени передачи кадра минимальной длины в 10 раз в результате увеличения пропускной способности канала в 10 раз по сравнению с Ethernet-10. Тем не менее, возможно построение крупных сетей на основе технологии Fast Ethernet, благодаря появлению в начале 90-х годов прошлого века коммутаторов. При использовании коммутаторов протокол Fast Ethernet может работать в полнодуплексном режиме, в котором нет ограничений на общую длину сети, а остаются только ограничения на длину физических сегментов, соединяющих соседние устройства (адаптер – коммутатор или коммутатор – коммутатор).

Стандарт IEEE 802.3u определяет 3 спецификации физического уровня Fast Ethernet, несовместимых друг с другом:

- 100Base-TX – для передачи данных используются две неэкранированные пары UTP категории 5 или STP Type 1;
- 100Base-T4 – для передачи данных используются четыре неэкранированных пары UTP категорий 3, 4 или 5;
- 100Base-FX – для передачи данных используются два волокна многомодового ВОК.

### **3.3.1.1. Спецификации 100Base-TX и 100Base-FX.**

Технологии 100Base-TX и 100Base-FX, несмотря на использование разных кабельных систем, имеют много общего с точки зрения построения и функционирования, в том числе, одинаковый метод логического кодирования – 4B/5B при различных методах физического кодирования – **MLT-3** в 100Base-TX и **NRZI** в 100Base-FX.

Кроме того, в технологии 100Base-TX имеется функция автопереговоров, обеспечивающая автоматическое определение скорости передачи (10 или 100 Мбит/с) между двумя связанными устройствами (СА, концентратор, коммутатор) путем посылки при подключении пачки специальных импульсов FLP – Fast Link Pulse burst – со стороны устройства, которое может работать на скорости 100 Мбит/с. Если встречное устройство не откликается на эти импульсы, это означает, что оно может работать только на скорости 10 Мбит/с, и первое устройство устанавливает режим передачи данных 10 Мбит/с.

### **3.3.1.2. Спецификация 100Base-T4.**

К моменту появления Fast Ethernet большинство ЛВС Ethernet в качестве кабельной системы использовали неэкранированную витую пару категории 3. Желание сохранить кабельную систему 10-мегабитных ЛВС

Ethernet обусловило применение специального метода логического кодирования – 8B/6T, обеспечившего более узкий спектр сигнала, что при скорости 33 Мбит/с позволило уложиться в полосу 16 МГц витой пары категории 3.

При кодировании 8B/6T 8 бит заменяются 6-ю троичными цифрами. Длительность одной троичной цифры – 40 нс. Следовательно, один байт передается за 240 нс ( $6 \times 40$  нс), что соответствует скорости передачи в 33,3 Мбит/с. Для передачи данных используется 3 пары UTP категории 3 ( $3 \times 33,3$  Мбит/с = 100 Мбит/с), и еще одна пара используется для прослушивания несущей с целью обнаружения коллизий.

Скорость изменения сигнала на каждой паре составляет:  $1/(40 \text{ нс}) = 25 \text{ Мбод}$ , что позволяет использовать витую пару категории 3.

### 3.3.1.3. Правила построения многосегментных ЛВС Fast Ethernet

1. Повторители Fast Ethernet делятся на два класса:

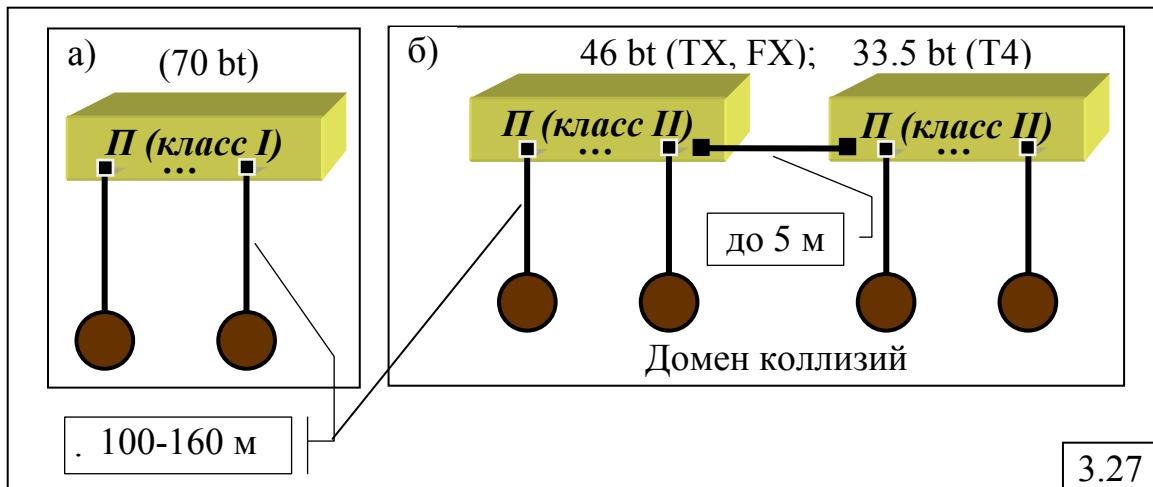
- **класс I** – поддерживает все виды логического кодирования (4B/5B, 8B/6T) и может иметь порты всех трех типов физического уровня: 100Base-TX, 100Base-T4 и 100Base-FX;

- **класс II** – поддерживает только один вид логического кодирования (4B/5B или 8B/6T) и имеет либо все порты 100Base-T4, либо порты 100Base-TX и 100Base-FX, так как последние используют один логический код 4B/5B.

2. Максимальное число повторителей ( $\Pi$ ) в одном домене коллизий:

- только 1 повторитель *класса I* из-за большой задержки распространения сигнала – 70 bt, обусловленной необходимостью транслировать различные системы сигнализации (рис.3.27,а);

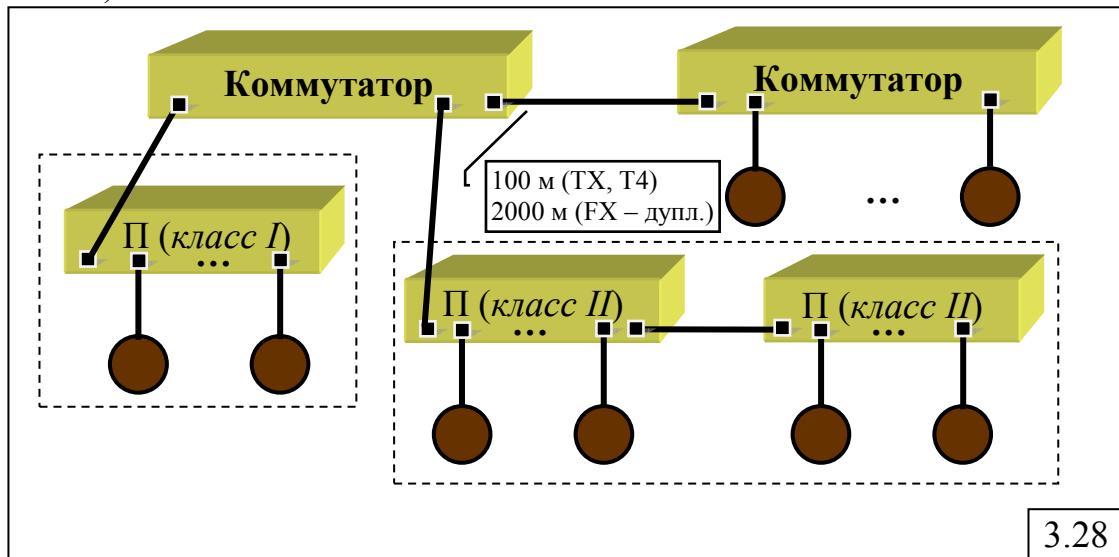
- 2 повторителя *класса II*, вносящих меньшую задержку при передаче сигналов: 46 bt для портов 100Base-TX и 100Base-FX и 33,5 bt для портов 100Base-T4 (рис.3.27,б).



3. Максимальное расстояние от повторителя до рабочей станции зависит от типа кабельной системы и составляет 100-160 м.

4. Максимальное расстояние между повторителями класса II – 5 м.

5. Несколько доменов коллизий могут объединяться с помощью коммутаторов и маршрутизаторов, образуя сети произвольных размеров (рис.3.28)



### 3.3.2. 100VG-AnyLAN

100VG-AnyLAN – технология, разработанная фирмами IBM и Hewlett-Packard на основе технологии 100Base-VG (Voice Grade) для передачи данных со скоростью 100 Мбит/с с использованием протоколов (кадров) ЛВС Ethernet или Token Ring (AnyLAN).

Предшествующая технология 100Base-VG разрабатывалась для передачи данных в сети Ethernet со скоростью 100 Мбит/с по неэкранированной витой паре (UTP) категории 3, широко используемой для передачи речи и называемой по этой причине кабелем VG (Voice Grade). В 100VG-AnyLAN, как и в 100Base-VG, вместо CSMA/CD реализован метод доступа с приоритетами (Demand Priority) и новая схема кодирования данных Quartet Coding (квартетное кодирование), благодаря которому данные передаются со скоростью 25 Мбит/с по 4-м парам UTP одновременно, что в сумме дает 100 Мбит/с.

Метод Demand Priority заключается в следующем. Станция, имеющая кадр для передачи, посыпает низкочастотный сигнал концентратору, запрашивая низкий приоритет для обычных данных и высокий для данных, чувствительных к временным задержкам (например, речь и видео). Если сеть свободна, концентратор разрешает передачу кадра. После анализа адреса получателя в принятом кадре концентратор отправляет кадр станции назначения. Это означает, что в отличие от концентратора Ethernet, концентратор 100VG-AnyLAN работает на 2-м уровне OSI-модели. Если же сеть занята, концентратор ставит полученный запрос в очередь, которая обрабатывается в порядке поступления запросов с учетом приоритетов: запросы с более высоким приоритетом выполняются первыми.

*Метод доступа к среде передачи данных – детерминированный.*

*Максимальное число станций в сети – 1024.*

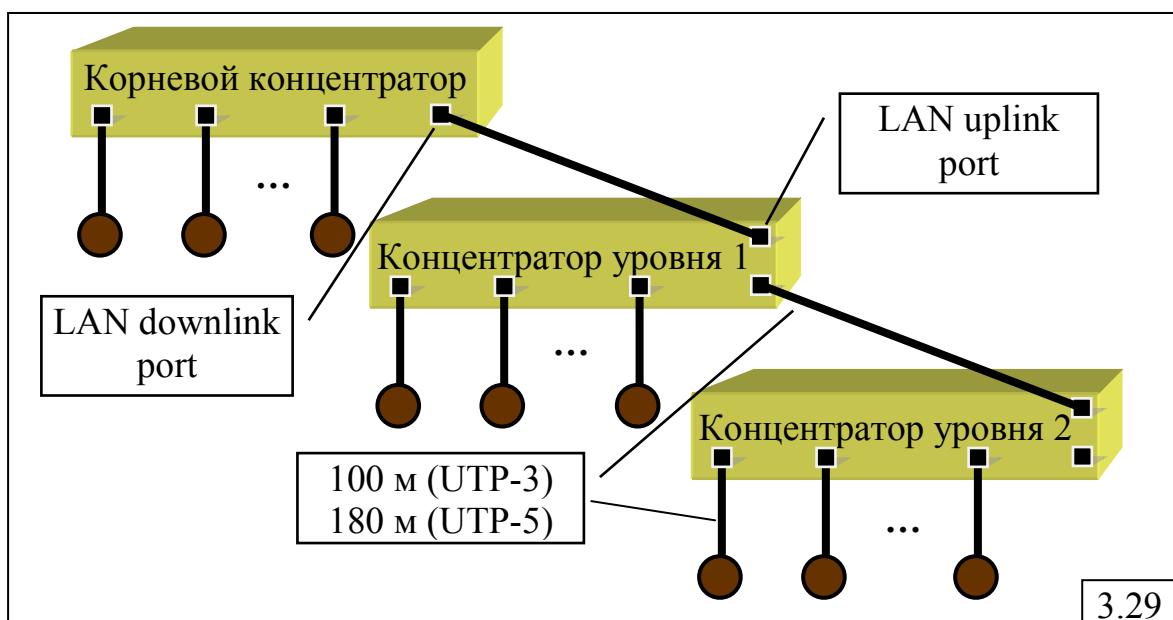
Максимальная протяженность сети – 3 км.

Максимальное расстояние между станциями:

- 100 м – для витой пары (UTP категории 3);
- 180 м – для витой пары (UTP категории 5).

Топология сети 100VG-AnyLAN очень похожа на топологию сетей 10Base-T и Token Ring, а именно логическая общая шина и маркерное кольцо соответственно, в то же время физическая топология обязательно "звезда", при этом *петли и ветвления* не допускаются.

Связующим элементом сети 100VG-AnyLAN является коммутирующий **концентратор**, причём допускается *три уровня каскадирования* (рис.3.29).



Концентратор сети 100VG-AnyLAN имеет два вида портов:

- LAN downlink port (порт связи "вниз") – предназначен для подключения конечных узлов и концентраторов нижнего уровня;
- LAN uplink port (порт связи "вверх") – предназначен для подключения концентратора верхнего уровня.

Кроме концентраторов в сети 100VG-AnyLAN могут использоваться:

- коммутаторы;
- маршрутизаторы;
- сетевые адаптеры.

Стандарт IEEE 802.12 поддерживает 3 типа кадров:

- IEEE 802.3 – Ethernet;
- IEEE 802.5 – Token Ring;
- IEEE 802.12 – кадры тестирования соединений в 100VG-AnyLAN.

В одном сегменте сети может поддерживаться только один тип кадров передачи данных – либо Ethernet, либо Token Ring.

Одной из составляющих стандарта IEEE 802.12 является **протокол приоритетных запросов** (Demand Priority Protocol – DPP).

DPP назначает порядок обработки запросов и установления соединений между конечными узлами. Если конечный узел готов

отправить кадр, он передает концентратору запрос обычного или высокого приоритета. Если узлу или концентратору нечего передать, он отправляет сигналы режима ожидания (Idle – незанят). Корневой концентратор опрашивает все свои узлы, в том числе концентраторы нижнего уровня, принимая от них сигналы Idle. Если узел не активен (компьютер выключен), он, естественно, не генерирует такие сигналы. Концентратор циклически опрашивает порты, начиная с порта с меньшим номером, выясняя их готовность к передаче. Если одновременно к передаче готовы несколько узлов, то концентратор анализирует их запросы с учетом:

- приоритета запроса;
- физического номера порта, к которому подключен передающий узел.

Высокий приоритет назначается:

- приложениям, критичным ко времени реакции;
- порту концентратора.

При каскадном соединении концентраторов доступ к среде передачи данных реализуется протоколом DPP следующим образом:

1) запрос от узла, подключённого к концентратору нижнего уровня, транслируется на концентратор более высокого уровня;

2) при опросе порта *LAN downlink port* инициируется опрос всех портов концентратора нижнего уровня, и только после этого возобновляется опрос портов концентратора более высокого уровня.

**Основные достоинства** технологии 100VG-AnyLAN:

- возможность использования существующей кабельной системы сети 10Base-T;
- *отсутствие потерь производительности из-за конфликтов* в среде передачи данных;
- возможность построения протяженных (до 4 км) сетей без использования коммутаторов.

### **3.3.3. Gigabit Ethernet**

Высокоскоростная технология Gigabit Ethernet обеспечивает пропускную способность системы телекоммуникации в 1 Гбит/с и описана в рекомендациях 802.3z и 802.3ab (на UTP 5-й категории).

*Особенности* технологии Gigabit Ethernet:

- сохранены все виды кадров, используемых в предыдущих технологиях Ethernet;
- предусмотрено использование двух версий протокола доступа к среде передачи данных:
  - полудуплексная версия протокола с методом доступа CDMA/CD;
  - полнодуплексная – с коммутаторами;
- предусмотрено использование следующих типов кабеля:
  - ВОК;
  - витая пара категории 5;

➤ коаксиальный кабель.

По сравнению с технологиями Ethernet-10 и Fast Ethernet изменения имеются как на физическом уровне, так и на уровне MAC.

Для обеспечения диаметра сети до 200 м реализованы следующие решения.

1. Увеличен минимальный размер кадра с 64 до 512 байт, что составляет 4096 битовых интервалов (bt). Кадр дополняется до 512 байт полем **расширения** (extension) размером от 448 до 0 байт, заполненным запрещенными символами кода 8B/10B (рис.3.30).

П	АН	АИ	Тип	Данные	КС	Поле расширения
8	6	6	2	46-1500	4	448-0 байт

от 512 до 1518 байт

3.30

2. Для уменьшения накладных расходов конечным узлам разрешено передавать несколько кадров подряд, без освобождения среды передачи для других станций. Такой режим передачи называется «**Burst Mode**». При этом станция может передать подряд несколько кадров с общей длиной 8192 байта = 65536 бит.

В стандарте 802.3z определены следующие типы физической среды:

- одномодовый ВОК;
- многомодовый ВОК 62,5/125;
- многомодовый ВОК 50/125;
- двойной коаксиал с волновым сопротивлением 75 Ом;
- многомодовый кабель.

Спецификации кабельных систем технологии Gigabit Ethernet представлены в табл.3.5.

Таблица 3.5

IEEE 802.3z	1000Base-SX	1000Base-LX
Физическая среда	Одно (о/м)- и многомодовый (м/м) ВОК	
Длина волны	850 нм	1300 нм
Длина сегмента	до 500 м (м/м ВОК)	5000 м (о/м ВОК)
	100 м (дупл.)	550 м (м/м ВОК)

Gigabit Ethernet может быть реализована на витой паре категории 5 (рекомендация IEEE 802.3ab) с использованием 4-х пар проводников, по которым одновременно передаются данные со скоростью 1000 Мбит/с. Следовательно, каждая пара должна обеспечить скорость 250 Мбит/с. Используемый метод кодирования – PAM-5 (5 уровней потенциала).

Максимальная частота спектра несущей при передаче двухбитовых символов кода РАМ-5 составляет 62,5 МГц. С учетом передачи первой гармоники протоколу 1000Base-T требуется полоса частот до 125 МГц.

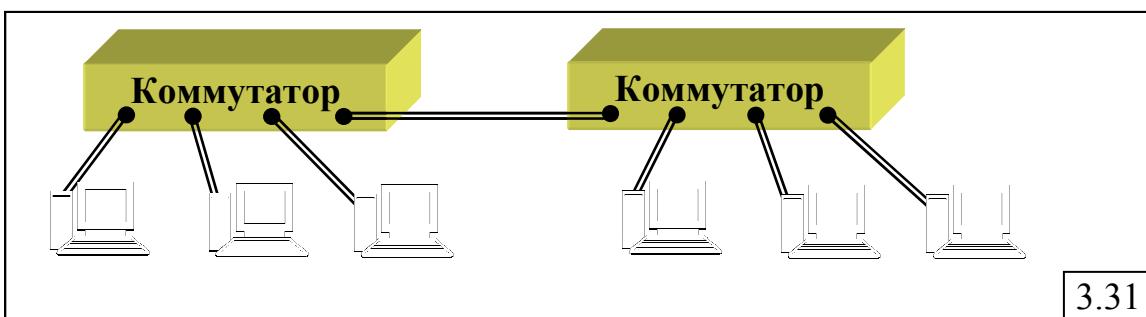
### 3.3.4. 10Gigabit Ethernet

Ряд фирм производителей, включая Cisco System, Foundry Networks и Nortel, разработали оборудование для сетей Ethernet с пропускной способностью 10 Гбит/с. В 2002 году утверждена спецификация IEEE 802.3ae (10GEthernet), предусматривающая использование волоконно-оптических кабелей. В 2006 году принят стандарт 10GBase-T (IEEE 802.3an-2006), использующий для передачи данных на расстояние до 100 метров экранированную витую пару категории 6 или ба.

Технология 10GEthernet предназначена для передачи данных на значительные расстояния, что позволяет операторам связи предлагать своим клиентам новые услуги по объединению локальных сетей. Технология 10GEthernet увеличивает протяженность сетей Ethernet до нескольких десятков километров (в зависимости от длины волны оптического сигнала и типа используемого кабеля).

Основные особенности ЛВС 10GEthernet:

- 1) реализован только дуплексный режим на основе коммутаторов (рис.3.31);
- 2) специфицированы три группы стандартов физического уровня: 10GBase-X (спецификация 10GBase-LX4), 10GBase-R, 10GBase-W;
- 3) передающая среда – волоконно-оптический кабель.



Спецификации кабельных систем технологии Gigabit Ethernet представлены в табл.3.6.

В группе 10GBase-X предусмотрена только одна спецификация: 10GBase-LX4, где L – означает, что используется второй диапазон прозрачности – 1310 нм.

В группах 10GBase-R и 10GBase-W реализованы 3 по спецификации в зависимости от длины волны:

- 1) 10GBase-RS и 10GBase-WS;
- 2) 10GBase-RL и 10GBase-WL;
- 3) 10GBase-RE и 10GBase-WE,

где S – означает, что используется первый диапазон прозрачности (850 нм); L – второй диапазон прозрачности (1310 нм); E –третий диапазон прозрачности (1550 нм).

Таблица 3.6

<b>10 GEthernet</b>	<b>10GBase-LX4</b>	<b>10GBase-Rx 10GBase-Wx</b>
<i>Метод кодирования</i>	8B/10B	64B/66B
<i>Длина волны</i>	1310 нм	850 нм (x=S)
		1310 нм (x=L)
		1550 нм (x=E)
<i>&lt;Количество волн&gt;*&lt;Проп.способн.&gt;</i>	$4*2,5 \text{ Гбит/с} = 10 \text{ Гбит/с}$	$1*10 \text{ Гбит/с}$
<i>Расстояние между передатчиком и приемником</i>	до 300 м (м/м ВОК)	40 км (для 10GBase-RE и 10GBase-WE)
	10 км (о/м ВОК)	

Максимальное расстояние между передатчиком и приемником для окна прозрачности Е может достигать 40 км, что позволяет строить территориально протяженные транспортные сети.

### 3.3.5. 40Gigabit Ethernet и 100Gigabit Ethernet

В июне 2010 года IEEE принял новый стандарт IEEE 802.3ba в виде дополнения к стандарту IEEE 802.3 Ethernet, в котором предусмотрены две скорости передачи данных по сети Ethernet – 40 Гбит/с и 100 Гбит/с.

Основная цель разработки этого стандарта состояла в том, чтобы распространить протокол 802.3 на сверхвысокие скорости передачи данных, и при этом обеспечить максимальную совместимость интерфейсов со стандартом 802.3 с целью сохранения предыдущих инвестиций в сетевую инфраструктуру. Необходимость появления этого стандарта обусловлена всё возрастающим числом приложений и большими объемами передаваемых данных. Высокие требования к пропускной способности среды передачи данных значительно превышают существующие возможности Ethernet.

Стандарт 40/100 Gigabit Ethernet поддерживает дуплексный режим и ориентирован на различные типы (среды) физического уровня (PHY).

Основными целями разработки стандарта 40/100 Gigabit Ethernet были следующие:

- сохранение формата кадра 802.3, используемого на MAC-уровне;
- сохранение минимального и максимального размера кадра стандартов 802.3;
- обеспечение достоверности передачи данных на MAC-уровне – вероятность битовой ошибки (BER) не должна превышать  $10^{-12}$ ;
- обеспечение поддержки открытой транспортной сети (OTN – The Open Transport Network) – высоконадежной среды для передачи разнородного трафика;

- обеспечение спецификаций физического уровня (PHY) для передачи по одномодовому оптическому волокну (SMF), многомодовому оптическому волокну (MMF), медным кабелям и объединительной плате (backplane).

Основными пользователями сетей IEEE 802.3ba могут стать производители систем и компонентов для серверов, сетей хранения данных, серверных ферм, высокопроизводительных вычислений, центров обработки данных, телекоммуникационных компаний, а также системных операторов. Использование всё более мощных серверных архитектур, центров обработки данных, сетей провайдеров и конечных пользователей делает, во многих случаях, среду передачи данных узким местом. Сети IEEE 802.3ba позволяют устранить узкие места, обеспечивая надежную, масштабируемую архитектуру среды передачи данных для удовлетворения требований к пропускной способности.

Дальнейшие перспективы развития высокоскоростных технологий передачи данных связывают с разработкой сетей Ethernet со скоростью передачи 1 Тбит/с (**Terabit Ethernet**). Предполагается, что технология будет разработана к 2015 году, для чего придется решить немало проблем. Технологией, которая может обеспечить передачу всё возрастающего трафика, возможно, станет технология DWDM. Для этого, как отмечает один из создателей Ethernet Боб Меткалф, «необходимо преодолеть множество ограничений, включая 1550-нанометровые лазеры и модуляцию с частотой 15 ГГц. Для будущей сети нужны новые схемы модуляции, а также новое оптоволокно, новые лазеры, в общем, все новое. Неясно также, какая сетевая архитектура потребуется для ее поддержки. Возможно, оптические сети будущего должны будут использовать волокно с вакуумной сердцевиной или углеродные волокна вместо кремниевых. Операторы должны будут внедрять больше полностью оптических устройств и оптику в свободном пространстве (безволоконную)».

### **3.4. ЛВС *Token Ring***

#### **3.4.1. Общие сведения**

**Token Ring** (*маркерное кольцо*) – сетевая технология, в которой станции могут передавать данные только тогда, когда они владеют *маркером*, непрерывно циркулирующим по кольцу.

Технология Token Ring, предложенная фирмой IBM в 1985 году, описана в стандарте IEEE 802.5. Назначением Token Ring было объединение в сеть всех типов ЭВМ, выпускаемых фирмой – от ПК до больших ЭВМ.

Основные *технические характеристики* Token Ring:

- максимальное число станций в одном кольце – 256;
- максимальное расстояние между станциями зависит от типа передающей среды и составляет:

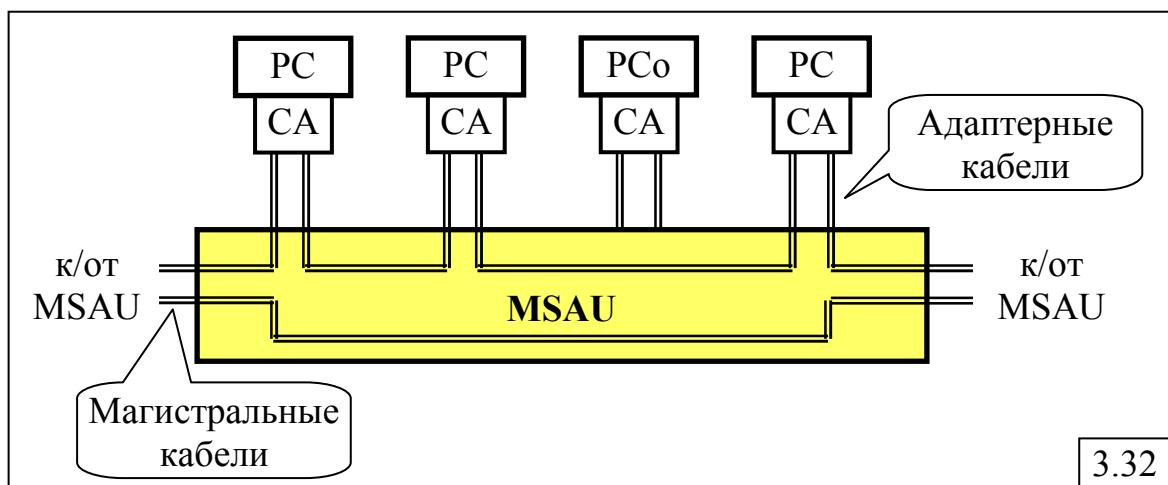
- 100 метров – для витой пары (UTP категории 4);
- 150 метров – для витой пары (IBM тип 1);
- 3000 метров – для оптоволоконного многомодового кабеля;
- до 8 колец могут быть соединены мостами.

Максимальная протяженность сети зависит от конфигурации.

Существуют два варианта технологии Token Ring, обеспечивающие скорость передачи данных 4 и 16 Мбит/с соответственно. Современные адаптеры Token Ring, поддерживают оба варианта.

### 3.4.2. Структурная организация Token Ring

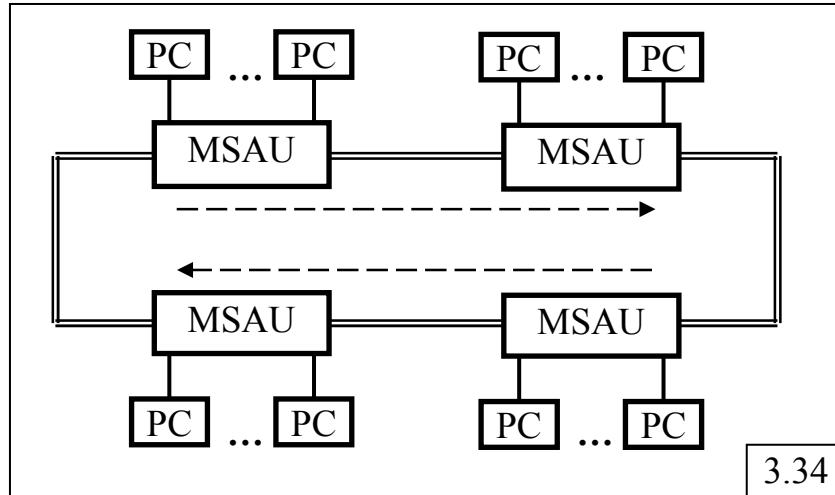
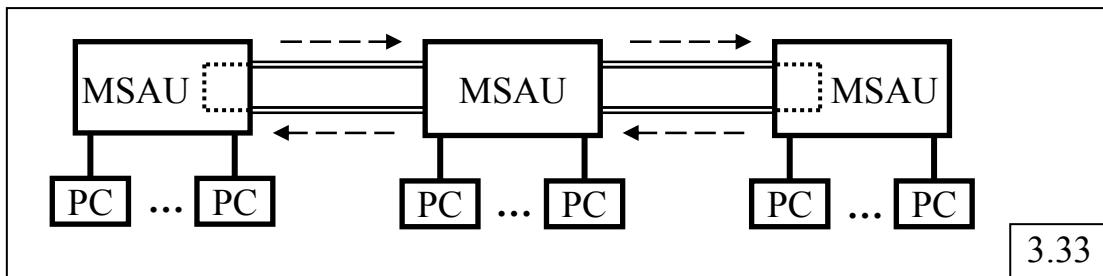
Физическая топология Token Ring "звезда" (рис.3.32) реализуется за счёт подключения всех компьютеров (рабочих станций, PC) через сетевые адаптеры (CA) к устройству множественного доступа (MSAU – Multistation Access Unit), которое осуществляет передачу кадров от узла к узлу и представляет собой концентратор Token Ring. MSAU имеет 8 портов для подключения компьютеров с помощью *адаптерных кабелей* и два крайних разъема для подключения к другим концентраторам. При включении компьютера, подсоединеного к MSAU, происходит автоматическое подключение к *магистральному* кабелю. В случае отказа или отключения станции MSAU организует обход порта этой станции, как это показано на рис.3.32 для станции PC<sub>o</sub>, при этом связность кольца сохраняется.



Логическая топология во всех способах – "кольцо". Пакет передается от узла к узлу по кольцу до тех пор, пока он не вернется в узел, где он был порожден.

Несколько MSAU могут конструктивно объединяться в группу (клuster, cluster), внутри которого абоненты соединены в кольцо, что позволяет увеличить количество абонентов, подключенных к одному центру.

Каждый адаптер соединяется с MSAU с помощью двух разнонаправленных линий связи. Такими же двумя разнонаправленными линиями связи, входящими в магистральный кабель, могут быть связаны MSAU в кольцо (рис.3.33), в отличие от однонаправленного магистрального кабеля, как это показано на рис.3.34.



В качестве среды передачи в сети Token Ring сначала использовалась витая пара (UTP, STP), затем появились варианты аппаратуры для коаксиального кабеля и оптоволоконного кабеля в стандарте FDDI.

### 3.4.3. Функциональная организация Token Ring

Каждый узел ЛВС принимает кадр от соседнего узла, восстанавливает уровни сигналов и передает кадр следующему узлу.

Передаваемый кадр может содержать данные (*кадр данных*) или являться маркером. **Маркер** – специальный служебный кадр, предоставляющий узлу, который им владеет, право на передачу данных.

Когда узлу необходимо передать кадр, его адаптер дожидается поступления маркера, а затем преобразует его в кадр, содержащий данные, сформированные по протоколу соответствующего уровня, и передает его в сеть. Кадр передается по сети от узла к узлу, пока не достигнет адресата, который установит в нем определенные биты для подтверждения того, что кадр получен адресатом, и ретранслирует его далее в сеть. Пакет продолжает движение по сети до возвращения в узел-отправитель, в котором проверяется правильность передачи. Если кадр был передан адресату без ошибок, узел может сформировать и передать очередной кадр данных (если таковой есть) или передать маркер следующему узлу. Количество кадров данных, которое может быть передано одним узлом, определяется *временем удержания маркера*, которое обычно составляет 10 мс. По истечении этого времени узел должен отдать маркер другому узлу. Маркер, как и кадр данных, перемещается по кольцу от узла к узлу. Если в узле, получившем маркер, нет данных (кадра) для передачи, то он

отправляет маркер к следующему узлу. Если в узле, получившем маркер, имеется кадр для передачи, то сравнивается уровень приоритета этого кадра (узла) со значением, так называемого *зарезервированного приоритета*, находящимся в поле маркера в виде *битов резервирования*. Если уровень приоритета кадра равен или больше значения зарезервированного приоритета, то узел захватывает маркер, присоединяет к нему кадр, формируя кадр данных, и передаёт его в сеть. В противном случае, если уровень приоритета кадра меньше значения зарезервированного приоритета, маркер направляется по кольцу к следующему узлу.

В процессе передачи маркера и кадра данных по кольцу каждый узел, принимая их, проверяет кадр на наличие ошибок и при их обнаружении устанавливает соответствующий *признак ошибки*, в соответствии с которым все остальные узлы игнорируют передаваемый кадр и просто ретранслируют его узлу-отправителю. Кроме того, каждый узел, имеющий данные для передачи, может в поле резервирования приоритета кадра или маркера установить уровень приоритета ожидающего кадра данных, если этот приоритет больше, чем значение, находящееся в этом поле и записанное предшествующими узлами. В конечном результате, кадр данных, вернувшийся после полного оборота по кольцу в узел-отправитель, будет иметь в поле резервирования приоритета значение, соответствующее максимальному уровню приоритета среди всех кадров, готовых к передаче.

Таким образом, в ЛВС Token Ring реализуется *приоритетное управление трафиком*, причём столкновения кадров невозможны, поскольку в каждый момент времени в сети передаётся только один кадр.

При передаче небольших кадров, например запросов на чтение файла, возникают дополнительные непроизводительные задержки на время, необходимое для полного оборота кадра по сети через множество станций и в течение которого сеть недоступна для передачи других кадров. Узел после передачи кадра мог бы отправить в ЛВС некоторое количество символов до возвращения в него отправленного кадра: от 50 до 100 символов в ЛВС со скоростью 4 Мбит/с и до 400 символов в ЛВС со скоростью 16 Мбит/с.

Для увеличения производительности сети в Token Ring со скоростью 16 Мбит/с используется так называемый *режим ранней передачи маркера* (Early Token Release – ETR), при котором узел передает маркер следующему узлу сразу после передачи своего кадра. Такая возможность обусловлена тем, что сеть Token Ring состоит из набора независимых межкомпьютерных связей, а не представляет собой единый кабель, проходящий через все компьютеры. С точки зрения передачи сигналов кадр от узла идет только до ближайшего соседа.

При инициализации ЛВС Token Ring одна из рабочих станций назначается в качестве *активного монитора*, на который возлагаются дополнительные контрольные функции в кольце:

- временной контроль в логическом кольце с целью выявления ситуаций, связанных с потерей маркера;
- формирование нового маркера после обнаружения потери маркера;
- формирование диагностических кадров при определенных обстоятельствах.

При выходе активного монитора из строя, назначается новый активный монитор из множества других РС. В качестве монитора автоматически может быть назначена станция, имеющая, например, наибольший MAC-адрес.

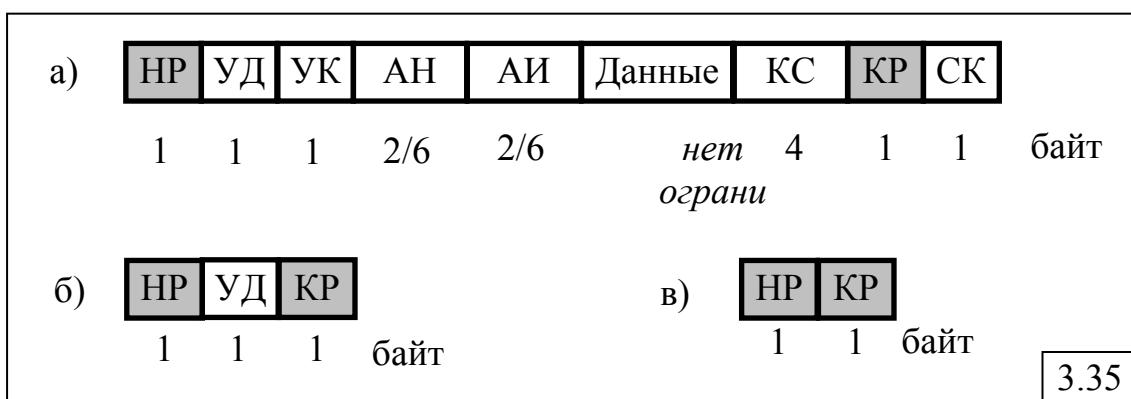
#### 3.4.4. Форматы кадров

В сети Token Ring используются 3 типа кадров:

- кадр данных (рис.3.35,а);
- маркер (рис.3.35,б);
- последовательность завершения (рис.3.35,в).

**Кадр данных** – основной тип кадра, содержащий следующие поля (рис.3.35,а):

- НР – начальный разделитель (1 байт);
- УД – управление доступом (1 байт);
- УК – управление кадром (1 байт);
- АН – адрес назначения (2 или 6 байт);
- АИ – адрес источника (2 или 6 байт);
- Данные – поле данных;
- КС – контрольная сумма (4 байта);
- КР – концевой разделитель (1 байт);
- СК – статус (состояние) кадра (1 байт).



**Маркер** – служебный кадр, содержащий 3 однобайтовых поля (рис.3.35,б):

- НР – начальный разделитель;
- УД – управление доступом;
- КР – концевой разделитель.

**Последовательность завершения** – служебный кадр, который при необходимости используется для прекращения процесса передачи в любой момент времени, содержащий 2 однобайтовых поля:

- НР – начальный разделитель;

- КР – концевой разделитель.

#### 3.4.4.1. Начальный и концевой разделители

**Начальный разделитель** (Start Delimiter – SD) и **концевой разделитель** (End Delimiter – ED) – уникальные битовые последовательности, указывающие соответственно на начало и конец кадра и имеющие вид:

НР: 

J	K	0	J	K	0	0	0
---	---	---	---	---	---	---	---

КР: 

J	K	1	J	K	1	ПК	ОО
---	---	---	---	---	---	----	----

Здесь **J** и **K** – соответственно 1 и 0 в дифференциальном манчестерском коде; **0** и **1** – обычные нулевые и единичные значения; **ПК** – бит промежуточного кадра; **ОО** – бит обнаруженной ошибки.

**Бит промежуточного кадра** (Intermediate Frame) принимает значения:

- **1**, если данный кадр является промежуточным кадром многокадровой передачи;
- **0**, если кадр является последним или единственным.

**Бит обнаруженной ошибки** (Error-detected) устанавливается в **0** в момент создания кадра в узле-источнике и может быть изменен на значение **1** любым узлом, обнаружившим ошибку при прохождении кадра по сети. После этого кадр ретранслируется без контроля ошибок в последующих узлах до достижения узла-источника, который в этом случае предпримет повторную попытку передачи кадра.

Поля **НР** и **КР** входят в состав всех трёх кадров сети Token Ring.

#### 3.4.4.2. Управление доступом

Поле **УД - Управление доступом** (Access Control) длиной 8 бит имеет следующую структуру:

P	P	P	T	M	R	R	R
---	---	---	---	---	---	---	---

Здесь **PPP** – биты приоритета; **T** – бит маркера: 1 для маркера и 0 для кадра данных; **M** – бит монитора: 1, если кадр передан активным монитором и 0 – в противном случае; **RRR** – биты резервирования.

В сети Token Ring, в отличие от сети Ethernet, предусмотрена возможность *приоритетной передачи* кадров за счёт присваивания сетевым адаптером приоритета маркеру и кадрам данных. Это реализуется путем записи в поле PPP уровня приоритета от 0 до 7 (7 – наивысший приоритет). Узел, получивший маркер, имеет право передать кадр только в том случае, если приоритет кадра не ниже приоритета маркера. В противном случае маркер передаётся следующему узлу.

Совместно с битами приоритета **PPP** используются биты резервирования **RRR**. Узлы сети в процессе передачи кадра по кольцу могут зарезервировать дальнейшее использование сети, поместив значение

приоритета кадра, ожидающего передачи, в биты резервирования **RRR**, если этот приоритет выше текущего значения поля резервирования. После этого, когда передающий узел, получив вернувшийся кадр данных, формирует новый маркер, он устанавливает его приоритет **PPP** равным значению поля резервирования **RRR** вернувшегося кадра. Таким образом, маркер будет передан узлу, установившему в поле резервирования наивысший приоритет.

Использование бита монитора **M** позволяет выявить ситуацию, когда кадр или маркер обошёл ЛВС по кольцу и не нашёл адресата.

Признаком этого является получение активным монитором кадра с битом монитора **M=1**.

#### **3.4.4.3. Управление кадром**

Кадр данных сети Token Ring может содержать в поле данных:

- информацию для управления логическим кольцом (данные уровня MAC), которой обмениваются адаптеры для выполнения функций контроля и управления работой логического кольца; такие кадры называются *кадрами управления доступом к среде* или **MAC-кадрами**;
- пользовательские данные (данные уровня LLC – **LLC-кадры**).

Поле **УК – управление кадром** (Frame Control – FC) – определяет тип кадра (MAC или LLC) и контрольный код MAC-кадра:

<b>FF</b>	<b>00</b>	<b>CCCC</b>
-----------	-----------	-------------

Здесь: **FF** – тип кадра: 00 – для MAC-кадра; 01 – для LLC-кадра (значения 10 и 11 зарезервированы и не используются); **00** – резервные разряды; **CCCC** – код *MAC-кадра*, определяющий к какому типу (определенным стандартом IEEE 802.5) управляющих кадров уровня MAC он принадлежит.

Существует 25 типов MAC-кадров, которые можно разделить на следующие группы:

- кадры инициализации станции (5 типов);
- кадры управления средой (5 типов);
- кадры сообщений об ошибках (3 типа);
- кадры управления станциями (12 типов).

Примеры MAC-кадров:

**0000** – **тест дублирования адреса** – передается рабочей станцией, впервые присоединяемой к логическому кольцу, чтобы убедиться, что ее адрес является уникальным;

**0010** – **очистка кольца** – передается в случае обнаружения серьезных проблем в ЛВС, таких как обрыв в кабеле или начало передачи узлом до получения им маркера; для локализации проблемы диагностическим программам достаточно определить узел, который передает это сообщение;

**0011 – требование маркера** – если запасной монитор обнаруживает, что активный монитор перестал функционировать, он приступает к передаче кадров с требованием маркера; запасные мониторы в этом случае начинают процесс взаимодействия друг с другом, чтобы назначить новый активный монитор;

**0100 – аварийная сигнализация (чистка)** – передается после инициализации логического кольца, и после установки нового активного монитора;

**0101 – наличие (присутствие) активного монитора** – передается активным монитором достаточно часто для уведомления других РС о том, что активный монитор функционирует;

**0110 – наличие запасного (резервного) монитора** – передается запасными мониторами.

#### **3.4.4.4. Адреса**

В сети Token Ring могут использоваться адреса длиной 2 или 6 байт. Формат адресов сети Token Ring совпадает с форматом адресов сети Ethernet.

Первый бит (I/G – Individual/Group) *адреса назначения (АН)* является признаком индивидуального или группового адреса. Первый бит *адреса источника (АИ)* всегда равен 0.

Второй бит определяет тип адреса: универсальный или локальный (U/L – Universal/Local). Остальные биты определяют физический адрес узла.

#### **3.4.4.5. Данные**

**Данные – поле данных** может содержать пользовательские данные, полученные или предназначенные для протоколов сетевого уровня, таких как IPX, IP, или содержать один из типов кадров уровня MAC. Специального ограничения на длину поля данных нет, хотя практически оно возникает из-за ограничений на допустимое время задержания маркера (10 мс) одной станцией. За это время сеть со скоростью передачи 4 Мбит/с может передать:

$$4 \text{ Мбит/с} * 0,01 \text{ с} = 0,04 \text{ Мбит} = 40\,000 \text{ бит} = 5 \text{ кбайт.}$$

Аналогично, сеть со скоростью передачи 16 Мбит/с может передать:

$$16 \text{ Мбит/с} * 0,01 \text{ с} = 0,16 \text{ Мбит} = 160\,000 \text{ бит} = 20 \text{ кбайт.}$$

С учётом задержек при передаче данных и накладных расходов на заголовок и концевик кадра, принято считать, что максимальная длина поля данных не должна превышать **4 кбайт** и **18 кбайт** для ЛВС Token Ring с пропускной способностью 4 Мбит/с и 16 Мбит/с соответственно.

#### **3.4.4.6. Контрольная сумма**

Поле *контрольной суммы (КС)* содержит *остаток избыточной циклической суммы* (CRC – Cyclic Redundancy Checksum), вычисленной с помощью полиномов типа CRC-32 для всех полей кадра, начиная с поля управления кадром (УК) и заканчивая полем данных. Остальные поля

содержат данные, изменяемые при распространении кадра по кольцу, например, бит монитора или биты резервирования в поле УД.

#### **3.4.4.7. Статус кадра**

Однобайтовое поле СК – *статус (состояние) кадра* (Frame Status – FS) – имеет следующий вид:

AC	RR	AC	RR
----	----	----	----

Здесь: R - резервный бит (4 бита); A – бит (*признак*) *распознавания адреса*; C – бит (*признак*) *копирования пакета*.

Так как контрольная сумма не охватывает поле СК, то каждое однобитное поле A и C в байте задублировано для гарантии достоверности передаваемых данных.

Узел-источник в процессе формирования кадра для передачи устанавливает в 0 биты A и C. Узел-приёмник, адрес которого совпал с адресом назначения, указанным в заголовке передаваемого кадра, после получения кадра устанавливает бит A в 1.

Если после копирования кадра в буфер узла-приёмника не обнаружено ошибок в кадре, то бит C также устанавливается в 1.

Таким образом, признаком успешной передачи кадра является возвращение кадра к источнику с битами: A=1 и C=1.

A=0 означает, что станции-адресата больше нет в сети или станция вышла из строя (выключена).

A=1 и C=0 означает, что произошла ошибка на пути кадра от источника к адресату (при этом также будет установлен в 1 бит обнаружения ошибки в концевом разделителе).

A=1, C=1 и бит обнаруженной ошибки OO=1 означает, что ошибка произошла на обратном пути кадра от адресата к источнику, после того как кадр был успешно принят узлом-адресатом.

#### **3.4.5. Достоинства и недостатки ЛВС Token Ring**

**Достоинства Token Ring:**

- *отсутствие конфликтов* в среде передачи данных;
- обеспечивается *гарантированное время доступа* всем пользователям сети;
- сеть Token Ring хорошо функционирует *при большой загрузке*, вплоть до загрузки в 100%, в отличие от Ethernet, в которой уже при загрузке 30% и более существенно возрастает время доступа, что крайне нежелательно для сетей реального времени;
- больший допустимый размер передаваемых данных в одном кадре (до 18 кбайт), по сравнению с Ethernet, обеспечивает более *эффективное функционирование сети при передаче больших объемов данных*;

- реальная скорость передачи данных в сети Token Ring с пропускной способностью 4 Мбит/с может оказаться выше, чем в 10-мегабитной сети Ethernet.

#### **Недостатки Token Ring:**

- более высокая стоимость сети Token Ring по сравнению с Ethernet, так как:

- дороже адAPTERы из-за более сложного протокола Token Ring;
- дополнительные затраты на приобретение MSAU;
- меньшие размеры сети Token Ring по сравнению с Ethernet;
- пропускные способности сетей Token Ring в настоящее время значительно меньше пропускных способностей, достигнутых в ЛВС Ethernet (десятка Гбит/с и выше).

### **3.5. ЛВС FDDI**

**FDDI (Fiber Distributed Data Interface – оптоволоконный интерфейс распределения данных)** – одна из первых высокоскоростных технологий ЛВС с пропускной способностью 100 Мбит/с, реализованная на волоконно-оптическом кабеле.

#### **3.5.1. Общие сведения**

Стандарт FDDI, разработанный Американским национальным институтом стандартов (ANSI – American National Standards Institute), реализован с максимальным соответствием стандарту IEEE 802.5 – Token Ring. Небольшие отличия от этого стандарта определяются необходимостью обеспечения большей скорости передачи данных на большие расстояния.

FDDI-технология предусматривает использование оптического волокна в качестве среды передачи, что обеспечивает:

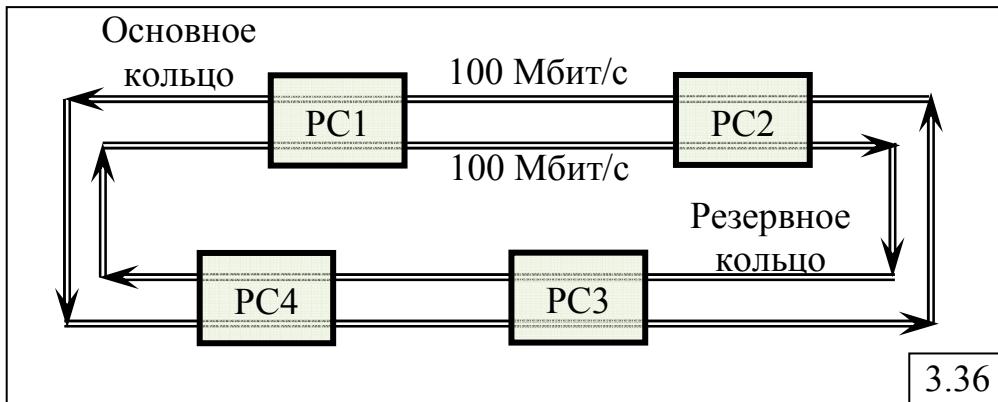
- высокую надежность;
- гибкость реконфигурации;
- высокую скорость передачи данных – 100 Мбит/с;
- большие расстояния между станциями (для многомодового волокна – 2 км; для одномодового при использовании лазерных диодов – до 40 км; длина сети – до 100 км).

#### **3.5.2. Структурная организация сети FDDI**

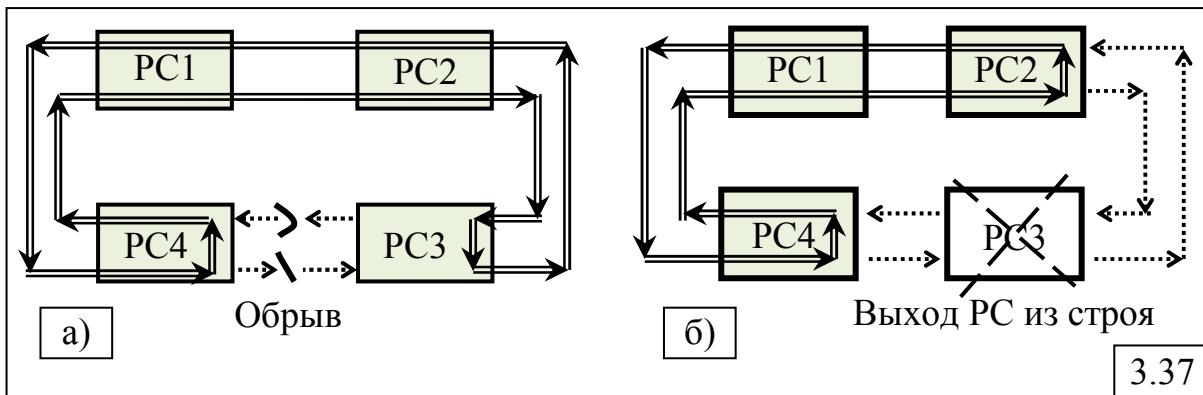
Топология сети FDDI – *двойное кольцо* (рис.3.36), причем применяются два разнонаправленных оптоволоконных кабеля, что позволяет использовать полнодуплексную передачу данных с удвоенной эффективной скоростью в 200 Мбит/с, при этом каждый из двух каналов работает со скоростью 100 Мбит/с.

Кольца сети FDDI образованы соединениями "точка-точка" между рабочими станциями (PC).

Станции, непосредственно включенные в кольцо, называются *станциями с двойным подключением* – DAS (Dual Attach Station).



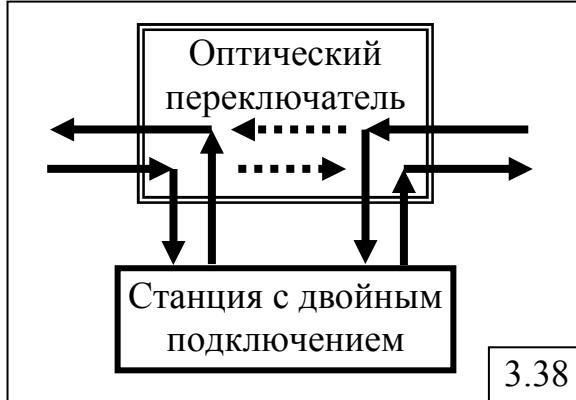
В нормальном режиме работы для передачи данных используется основное кольцо. Второе кольцо – резервное, обеспечивает передачу данных в противоположном направлении и автоматически активизируется в случае повреждения кабельной системы (рис.3.37,а) или возникновения неисправности на одной из станций (рис.3.37,б).



Можно дополнительно повысить надежность кольца FDDI, если использовать **оптический обходной переключатель** – OBS (Optical Bypass Switch) (рис.3.38).

В этом случае при выходе станции из строя она исключается из кольца, но целостность кольца при этом сохраняется, и резервное кольцо не задействуется. OBS вносит существенные потери излучения, что ограничивает число последовательно соединенных переключателей.

Соединение "точка-точка"



между станциями в кольце не только упрощает стандартизацию, но также позволяет одновременно применять на разных участках кольца одномодовые и многомодовые волокна. Это означает, что отдельная DAS-станция в кольце FDDI может связываться с дальним соседом (более 2 км) по одномодовому волокну и иметь лазерные диоды в передающей системе физического уровня, а с ближним соседом (менее 2 км) – по многомодовому волокну и использовать недорогие светоизлучательные диоды.

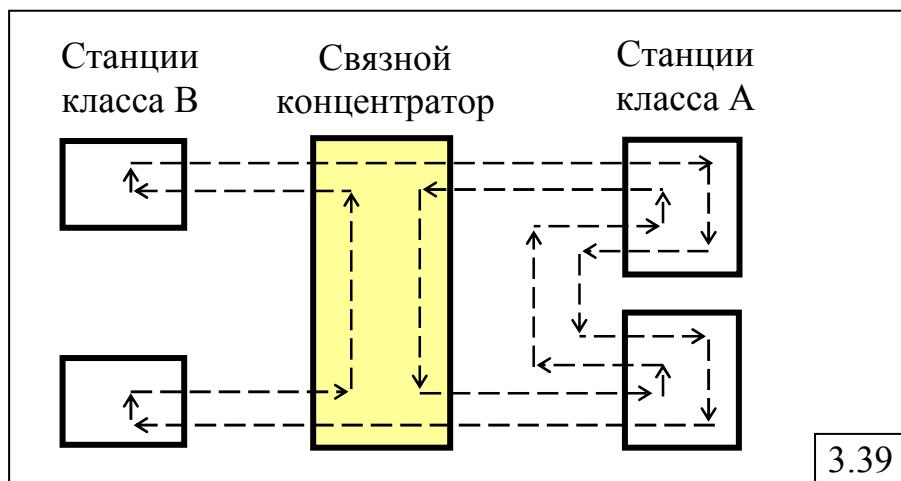
Стандарт FDDI для достижения высокой гибкости сети предусматривает применение сетевых адаптеров двух типов:

- **адаптеры класса А**, подключающиеся к внутреннему и внешнему кольцам сети, что позволяет реализовать возможность обмена со скоростью 200 Мбит/с или же возможность резервирования кабеля сети (при повреждении основного кабеля используется резервный кабель); эти адаптеры используются в самых критичных частях сети;
- **адаптеры класса В**, подключающиеся только к внешнему кольцу сети; эти адаптеры более простые и дешевые и не имеют возможностей адаптеров класса А.

Кроме собственно абонентов (компьютеров, терминалов и т.д.) в сети FDDI могут использоваться **связные концентраторы**, которые обеспечивают:

- *контроль* за работой сети, диагностику неисправностей и упрощение реконфигурации за счет объединения в одном месте всех точек подключения;
- *преобразование* электрических сигналов в оптические и наоборот при применении кабелей разных типов (оптоволоконных и электрических).

Пример конфигурации сети FDDI с использованием связных концентраторов представлен на рис.3.39.



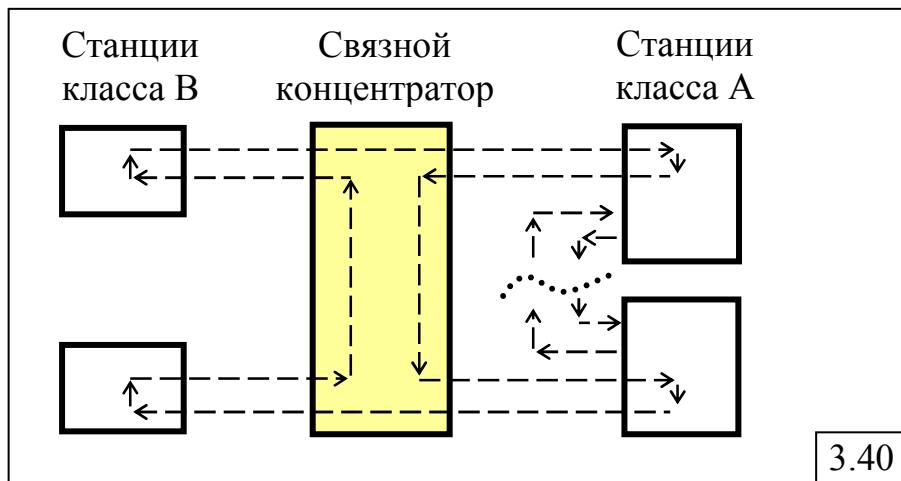
В случае повреждения кабеля поврежденный участок кабеля исключается из кольца, но целостность сети при этом не нарушается вследствие перехода на одно кольцо вместо двух, т.е. адаптеры класса А начинают работать как адаптеры класса В (рис.3.40).

Для **кодирования** передаваемых данных в FDDI применяется код 4B/5B, специально разработанный для этого стандарта. Использование символов, представляющих 4 бита (полубайт или **ниббл**), позволяет аппаратным средствам FDDI оперировать с полубайтами или байтами, а не с битами, тем самым способствуя увеличению скорости обмена.

### 3.5.3. Функциональная организация FDDI

За основу стандарта FDDI был взят метод маркерного доступа, описанный в протоколе IEEE 802.5 Token Ring. Основные отличия метода

доступа FDDI от метода, специфицированного протоколом IEEE 802.5, заключаются в следующем.

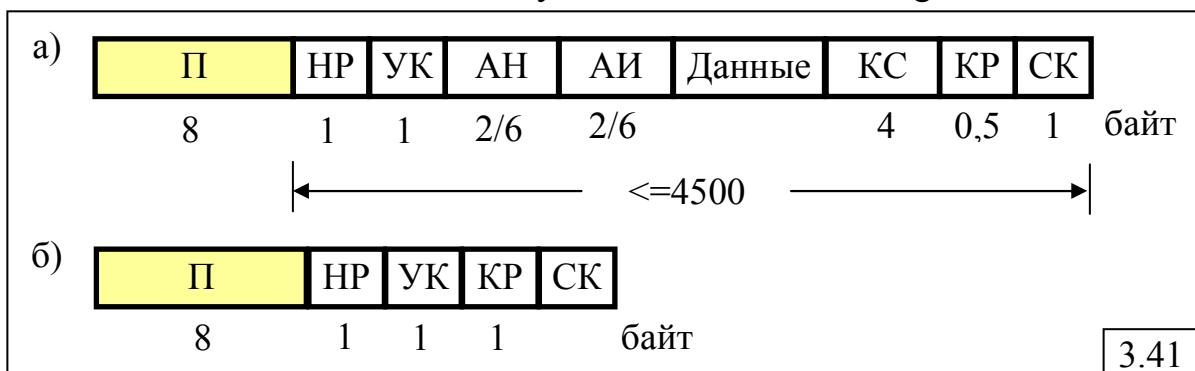


1. В FDDI применяется **множественная передача маркера**, при котором новый маркер передается другой станции сразу же после окончания передачи кадра, не ожидая его возвращения.

2. FDDI не предусматривает возможности установки приоритетов пакетов и резервирования, которые используются в IEEE 802.5 для выделения ресурсов сети. Вместо этого каждая РС классифицируется как **асинхронная**, для которой время доступа к сети не критично, и **синхронная**, для которой время доступа к сети жестко ограничено, т.е. существуют очень жесткие требования к интервалам времени между передачами. FDDI использует сложный алгоритм для предоставления доступа к сети этим двум классам устройств.

### 3.5.4. Форматы кадров

Форматы кадра данных (рис.3.41,а) и маркера (рис.3.41,б) сети FDDI несколько отличаются от используемых в сети Token Ring.



Кадр данных FDDI так же, как и кадр IEEE 802.5, может нести информацию по управлению логическим кольцом (данные уровня MAC) или содержать пользовательские данные (данные уровня LLC).

Поля в кадре FDDI имеют следующие значения.

**П – преамбула** – служит для начальной синхронизации приема. Несмотря на то, что изначально длина этого поля равна 64 бит (16

символьных полубайтов), узлы могут динамически изменять ее в соответствии со своими требованиями к синхронизации.

**НР – начальный разделитель** (Start Delimiter – SD) – уникальное двухсимвольное (однобайтовое) поле, указывающее на начало кадра (маркера).

**УК – управление кадром** (Frame Control – FC) – определяет тип кадра (MAC или LLC) и контрольный код MAC:

<b>C</b>	<b>L</b>	<b>FF</b>	<b>TTTT</b>
----------	----------	-----------	-------------

Здесь: **C** – бит, который определяет, будет ли кадр использоваться для синхронного или асинхронного обмена; **L** – индикатор длины адреса, которая может быть 16 или 48 бит (в отличие от Ethernet и Token Ring в сети FDDI допускается использование адресов разной длины); **FF** – формат кадра определяет, принадлежит ли кадр подуровню MAC (т.е. предназначен для целей управления кольцом) или подуровню LLC (т.е. предназначен для передачи данных); если кадр является кадром подуровня MAC, то биты **TTTT** определяют тип кадра, содержащего данные по управлению в поле данных.

**AH – адрес назначения** длиной 16 или 48 бит.

**AI – адрес источника** длиной 16 или 48 бит.

**Данные** – **поле данных** может содержать пользовательские данные или данные типа MAC, предназначенные для управления кольцом; длина поля данных является переменной, но ограничена суммарной длиной кадра, не превосходящей 4500 байт.

**КС – контрольная сумма** типа CRC-32.

**КР – концевой разделитель** (End Delimiter – ED) – уникальная последовательность 0 и 1, указывающая конец кадра (маркера); имеет длину: полбайта (1 символ) для кадра данных и 1 байт (2 символа) для маркера.

**СК – статус кадра** (Frame Status – FS) – поле произвольной длины, содержащее биты: "Обнаружена ошибка", "Адрес опознан" и "Данные скопированы".

### 3.5.5. Технические характеристики FDDI

Максимальное число станций в кольце – 500.

Максимальная протяженность сети – 100 км.

Среда передачи оптоволоконный кабель.

Максимальное расстояние между станциями зависит от типа передающей среды (линии связи) и составляет:

- 2 км – для оптоволоконного многомодового кабеля.
- 40 км – для оптоволоконного одномодового кабеля;
- 100 м – для витой пары (UTP категории 5);
- 100 м – для экранированной витой пары (IBM тип 1).

Метод доступа – маркерный.

Скорость передачи данных – 100 Мбит/с (200 Мбит/с для дуплексного режима передачи).

Ограничение на общую длину сети обусловлено ограничением времени полного прохождения сигнала по кольцу для обеспечения предельно допустимого времени доступа. Максимальное расстояние между абонентами определяется затуханием сигнала в кабеле.

### 3.5.6. Достоинства и недостатки FDDI

#### Достоинства:

- высокая помехозащищенность;
- секретность передачи информации;
- прекрасная гальваническая развязка абонентов;
- высокая скорость передачи данных на большие расстояния без ретрансляции, что позволяет строить протяженные сети, например городские, сохраняя при этом все преимущества локальных сетей, в частности низкий уровень ошибок;
- возможность объединения большого количества пользователей;
- гарантированное время доступа к сети;
- отсутствие конфликтов в среде передачи при любом уровне нагрузки.

#### Недостатки:

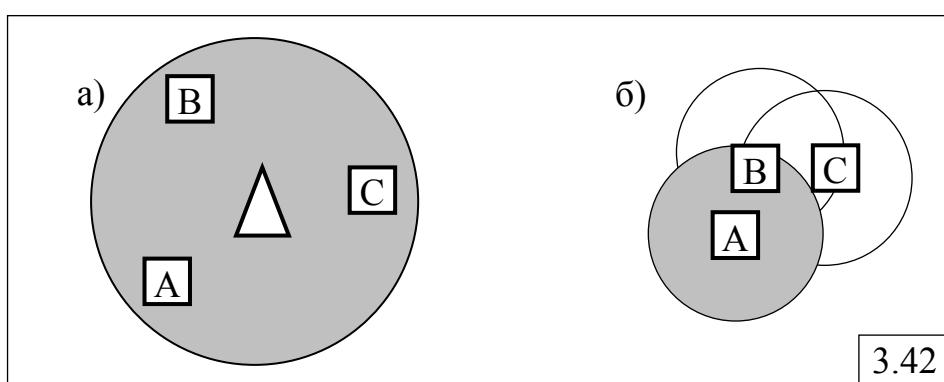
- высокая стоимость по сравнению с другими технологиями ЛВС;
- сложная в эксплуатации из-за наличия оптоволоконного кабеля.

## 3.6. Беспроводные ЛВС

### 3.6.1. Общие принципы построения беспроводных ЛВС

Способы организации БЛВС (рис.3.42):

- 1) с базовой станцией (рис.3.42,а), когда обмен данными между рабочими (мобильными) станциями (A, B, C) осуществляется через базовую станцию;
- 2) без базовой станции (рис.3.42,б), когда обмен данными между станциями (A, B, C) осуществляется напрямую.



*Преимущества беспроводных ЛВС (БЛВС) по сравнению с проводными:*

- простота и дешевизна построения и реорганизации сети;

- мобильность пользователей.

*Недостатки беспроводных ЛВС:*

- низкая помехоустойчивость;
- неопределенность зоны покрытия;
- проблема «скрытого терминала».

Проблема «скрытого терминала» состоит в следующем. Положим, что станция А (рис.3.42,б), передаёт данные станции В. Станция С не «слышит» станцию А (она является «скрытым терминалом» для станции С) и, полагая, что среда передачи свободна, начинает передачу данных, предназначенных для станции В. Очевидно, что возникающая при этом коллизия приведёт к искажению передаваемых данных как от станции А, так и от станции С.

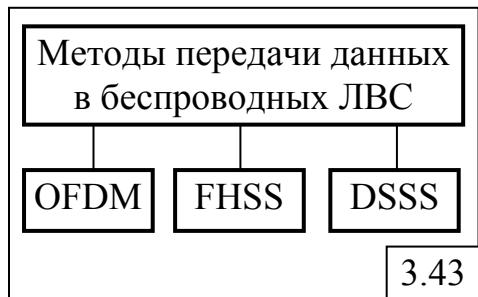
В БЛВС вместо метода доступа с прослушиванием несущей и распознаванием коллизий (CSMA/CD) используются методы *предотвращения коллизий* (CSMA/CA). В сетях с базовой станцией обычно применяются *методы опроса*, когда базовая станция опрашивает все станции, находящиеся в зоне её действия, и, при наличии у нескольких станций данных для передачи, предоставляет право на передачу одной из них в соответствии с принятой в этой сети стратегией.

Для повышения помехоустойчивости кода для сигналов малой мощности в беспроводных сетях разработана специальная **технология расширенного спектра**, ориентированная на широкую полосу пропускания, позволяющую применять модуляцию с несколькими несущими. В рамках этой технологии используются различные методы передачи данных.

### 3.6.2. Методы передачи данных

Основными методами передачи данных в беспроводных ЛВС, основанными на технологии расширения спектра, являются (рис.3.43):

- ортогональное частотное мультиплексирование (OFDM);
- расширение спектра скачкообразным изменением частоты (FHSS);
- прямое последовательное расширение спектра (DSSS).



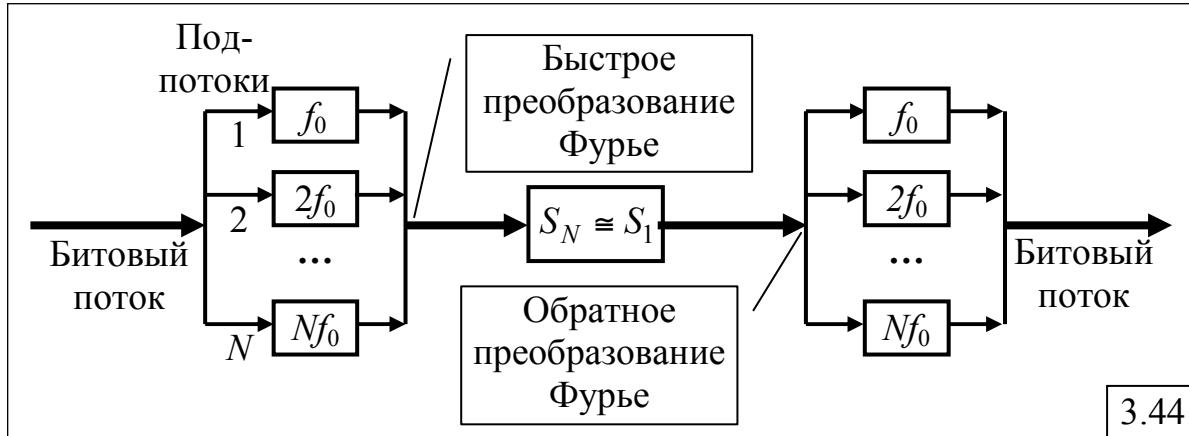
#### 3.6.2.1. Ортогональное частотное мультиплексирование

**Ортогональное частотное мультиплексирование** (OFDM – Orthogonal Frequency Division Multiplexing) используется для передачи данных со скоростью до 54 Мбит/с в диапазоне 5 ГГц.

На рис.3.44 показана схема реализации OFDM.

Битовый поток данных делится на  $N$  подпотоков, каждый из которых модулируется с помощью методов частотной (FSK) или фазовой (PSK) манипуляции с использованием несущей, которая обычно кратна основной

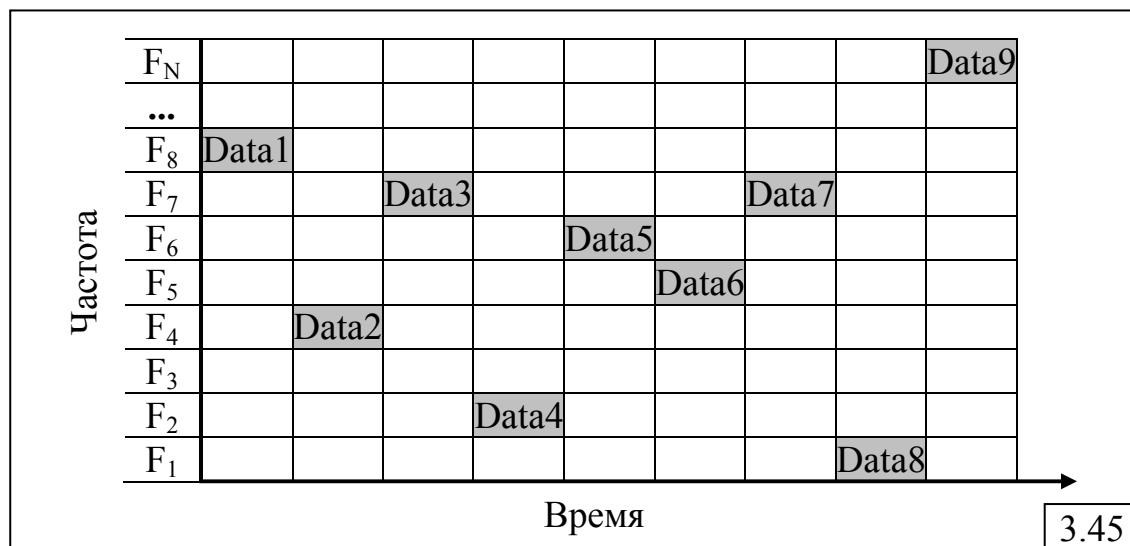
частоте  $f_0$ . На основе быстрого преобразования Фурье все несущие сворачиваются в общий сигнал, спектр которого примерно равен спектру сигнала, кодируемого одной несущей. После передачи такого сигнала на приёмной стороне с использованием преобразования Фурье выделяются несущие подпотоки, из которых формируется исходный битовый поток.



Разделение исходного высокоскоростного потока на несколько низкоскоростных потоков позволяет уменьшить интерференцию передаваемых сигналов за счёт увеличения битового интервала.

### 3.6.2.2. Расширение спектра скачкообразным изменением частоты

Метод *расширения спектра скачкообразной перестройкой частоты* (FHSS – Frequency Hopping Spread Spectrum) основан на постоянной смене несущей в пределах широкого диапазона частот (рис.3.45).



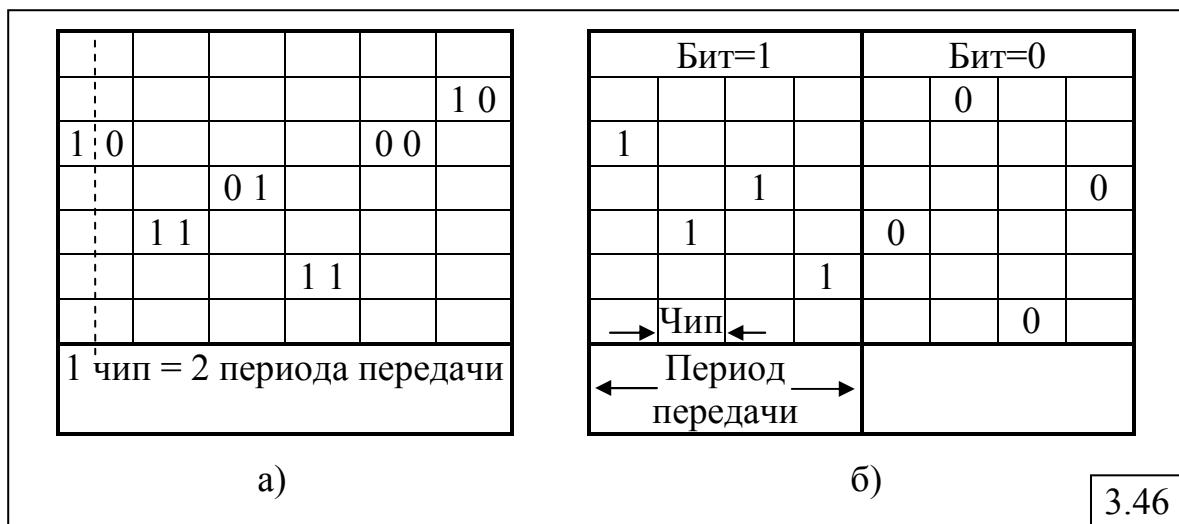
Частота несущей  $F_1, \dots, F_N$  случайным образом меняется через определенный период времени, называемый *периодом отсечки (чип)*, в соответствии с выбранным алгоритмом выработки псевдослучайной последовательности. На каждой частоте применяется модуляция (FSK или PSK). Передача на одной частоте ведётся в течение фиксированного интервала времени, в течение которого передаётся некоторая порция

данных (Data). В начале каждого периода передачи для синхронизации приемника с передатчиком используются синхробиты, которые снижают полезную скорость передачи.

В зависимости от скорости изменения несущей различают 2 режима расширения спектра:

- медленное расширение спектра (рис.3.46,а) – за один период отсечки передается несколько бит;
- быстрое расширение спектра (рис.3.46,б) – один бит передается за несколько периодов отсечки, то есть повторяется несколько раз.

В первом случае *период передачи данных* меньше *периода передачи чипа*, во втором – больше.



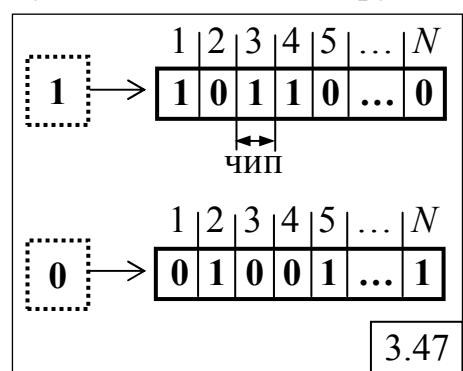
Метод быстрого расширения спектра обеспечивает более надёжную передачу данных при наличии помех за счёт многократного повторения значения одного и того же бита на разных частотах, но более сложен в реализации, чем метод медленного расширения спектра.

### 3.6.2.3. Прямое последовательное расширение спектра

Метод прямого последовательного расширения спектра (DSSS – Direct Sequence Spread Spectrum) состоит в следующем.

Каждый «единичный» бит в передаваемых данных заменяется двоичной последовательностью из  $N$  бит, которая называется **расширяющей последовательностью**, а «нулевой» бит кодируется инверсным значением расширяющей последовательности (рис.3.47). В этом случае тактовая скорость передачи увеличивается в  $N$  раз, следовательно, спектр сигнала также расширяется в  $N$  раз.

Зная выделенный для беспроводной передачи (линии связи) частотный диапазон, можно соответствующим образом выбрать скорость передачи данных и значение  $N$ , чтобы спектр сигнала заполнил весь диапазон.



Основная цель кодирования DSSS как и FHSS – повышение помехоустойчивости.

**Чиповая скорость** – скорость передачи результирующего кода.

**Коэффициент расширения** – количество битов  $N$  в расширяющей последовательности. Обычно  $N$  находится в интервале от 10 до 100. Чем больше  $N$ , тем больше спектр передаваемого сигнала.

Например, последовательность Баркера (Barker) с коэффициентом расширения  $N=11$  имеет вид: 10110111000, основное достоинство которого заключается в том, что при сдвиге на один бит влево или вправо количество совпадений битов меньше половины:

1) сдвиг влево (5 совпадений)

0110111000x

10110111000

2) сдвиг вправо (5 совпадений)

x1011011100

10110111000

DSSS в меньшей степени защищен от помех, чем метод быстрого расширения спектра.

#### 3.6.2.4. Множественный доступ с кодовым разделением

Методы расширения спектра широко используются в сотовых сетях, в частности, при реализации метода доступа CDMA (Code Division Multiple Access) – **множественный доступ с кодовым разделением**. CDMA может использоваться совместно с FHSS, но в беспроводных сетях чаще с DSSS.

Каждый узел сети использует собственную расширяющую последовательность, которая выбирается так, чтобы принимающий узел мог выделить данные из суммарного сигнала.

Рассмотрим принцип реализации CDMA на примере.

Пусть в сети работают 4 узла: **A, B, C, D**, каждый из которых использует свою расширяющую последовательность:

**A:0000**

**B:0101**

**C:0011**

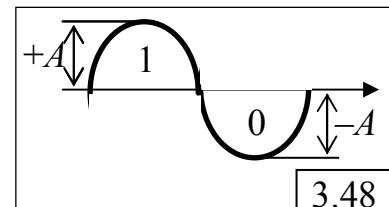
**D:0110**

Для представления 1 и 0 используются аддитивные инверсные сигналы, показанные на рис.3.48 и обозначенные соответственно как  $(+A)$  и  $(-A)$ . Очевидно, что:

$$(+A) + (-A) = 0.$$

Для упрощения выкладок обозначим:  
 $(+A) = 1$  и  $(-A) = -1$ .

Тогда расширяющие последовательности для узлов **A, B, C** и **D** примут вид:



Узел	«единичный» бит				«нулевой» бит			
<b>A</b>	-1	-1	-1	-1	+1	+1	+1	+1
<b>B</b>	-1	+1	-1	+1	+1	-1	+1	-1
<b>C</b>	-1	-1	+1	+1	+1	+1	-1	-1
<b>D</b>	-1	+1	+1	-1	+1	-1	-1	+1

Положим теперь, что передачу ведут все 4 узла: **A**, **B**, **C**, **D** и в некоторый момент времени они передают соответственно биты 1, 0, 1, 0 в виде соответствующих расширяющих последовательностей (РП):

Узел	бит	РП				
		-1	-1	-1	-1	
<b>A</b>	1	-1	-1	-1	-1	
<b>B</b>	0	+1	-1	+1	-1	
<b>C</b>	1	-1	-1	+1	+1	
<b>D</b>	0	+1	-1	-1	+1	
<b>X</b>	<b>S</b>	<b>0</b>	<b>-4</b>	<b>0</b>	<b>0</b>	

Для простоты допустим, что все узлы синхронизированы.

Положим, что некоторый узел **X** хочет принять данные от узла **A**. В рассматриваемый момент времени он принимает сигнал **S** в виде вектора  $(0 \ -4 \ 0 \ 0)$ . Для определения значения принятого от узла **A** бита узел **X** должен использовать демодулятор CDMA с расширяющей последовательностью узла **A**.

Алгоритм работы демодулятора:

1) умножение принятого сигнала **S** на вектор расширяющей последовательности узла **A**:

$$S \times A = (0 \ -4 \ 0 \ 0) \times (-1 \ -1 \ -1 \ -1) = 0 + 4 + 0 + 0 = +4;$$

2) результат делится на количество узлов (станций) в сети; если результат положительный, то исходный бит равен 1, если результат отрицательный, то исходный бит равен 0; для узла **A**:

$+4/4=+1$ , следовательно, значение бита от узла **A** равно 1.

Аналогично, при приеме данных от узла **B**:

$$S \times B = (0 \ -4 \ 0 \ 0) \times (-1 \ +1 \ -1 \ +1) = 0 - 4 + 0 + 0 = -4/4 = -1,$$

следовательно, значение бита от узла **B** равно 0.

При приеме данных от узла **C**:

$$S \times C = (0 \ -4 \ 0 \ 0) \times (-1 \ -1 \ +1 \ +1) = 0 + 4 + 0 + 0 = +4/4 = +1,$$

следовательно, значение бита от узла **C** равно 1.

При приеме данных от узла **D**:

$$S \times D = (0 \ -4 \ 0 \ 0) \times (-1 \ +1 \ +1 \ -1) = 0 - 4 + 0 + 0 = -4/4 = -1,$$

следовательно, значение бита от станции **D** равно 0.

Достоинство CDMA заключается в повышенной защищенности и скрытности передачи данных: не зная расширяющей последовательности, невозможно получить сигнал, а иногда и обнаружить его присутствие.

### 3.6.3. Технология WiFi

Технология беспроводных ЛВС (WLAN) определяется стеком протоколов IEEE 802.11, который описывает физический уровень и канальный уровень с двумя подуровнями: MAC и LLC.

На физическом уровне определены несколько вариантов спецификаций, которые различаются:

- используемым диапазоном частот;
- методом кодирования;
- скоростью передачи данных.

Варианты построения беспроводных ЛВС стандарта 802.11, получившего название WiFi, представлены в табл. 3.7. Ниже дана их краткая характеристика.

Таблица 3.7

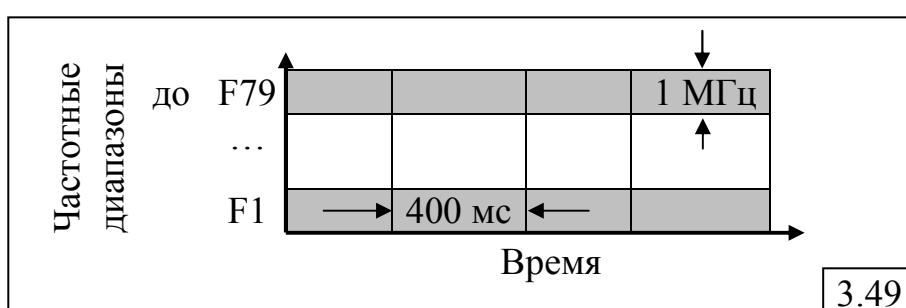
Вариант	Стандарт	Диапазон частот	Метод кодирования	Скорость передачи	Год
1	IEEE 802.11	ИК 850 нм		1 Мбит/с; 2 Мбит/с	1997
2	IEEE 802.11	2,4 ГГц	FHSS	1 Мбит/с; 2 Мбит/с	1997
3	IEEE 802.11	2,4 ГГц	DSSS	1 Мбит/с; 2 Мбит/с	1997
4	IEEE 802.11a	5 ГГц	OFDM	до 54 Мбит/с	1999
5	IEEE 802.11b	2,4 ГГц	DSSS	до 11 Мбит/с	1999
6	IEEE 802.11g	2,4 ГГц	OFDM	до 54 Мбит/с	2003

#### IEEE 802.11 (вариант 1):

- среда передачи – ИК-излучение;
- передача в зоне прямой видимости;
- используются 3 варианта распространения излучения:
  - ненаправленная антенна;
  - отражение от потолка;
  - фокусное направленное излучение («точка-точка»).

#### IEEE 802.11 (вариант 2):

- среда передачи – микроволновый диапазон 2,4 ГГц;
- метод кодирования – FHSS: до 79 частотных диапазонов шириной 1 МГц, длительность каждого из которых составляет 400 мс (рис.3.49);
  - при 2-х состояниях сигнала обеспечивается пропускная способность среды передачи в 1 Мбит/с, при 4-х – 2 Мбит/с.



**IEEE 802.11 (вариант 3):**

- среда передачи – микроволновый диапазон 2,4 ГГц;
- метод кодирования – DSSS с 11-битным кодом в качестве расширяющей последовательности: 10110111000.

**IEEE 802.11a:**

- 1) диапазон частот – 5 ГГц;
- 2) скорости передачи: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с;
- 3) метод кодирования – OFDM.

Недостатки:

- слишком дорогое оборудование;
- в некоторых странах частоты этого диапазона подлежат лицензированию.

**IEEE 802.11b:**

- 1) диапазон частот – 2,4 ГГц;
- 2) скорость передачи: до 11 Мбит/с;
- 3) метод кодирования – модернизированный DSSS.

**IEEE 802.11g:**

- 1) диапазон частот – 2,4 ГГц;
- 2) максимальная скорость передачи: до 54 Мбит/с;
- 3) метод кодирования – OFDM.

В сентябре 2009 года был утверждён стандарт IEEE 802.11n. Его применение позволит повысить скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с.

Радиус действия беспроводных сетей IEEE 802.11 – до 100 метров.

### **3.6.4. Технология WiMax**

Технология беспроводного широкополосного доступа с высокой пропускной способностью WiMax представлена группой стандартов IEEE 802.16 и первоначально была предназначена для построения протяжённых (до 50 км) беспроводных сетей, относящихся к классу региональных или городских сетей.

Стандарт IEEE 802.16 или IEEE 802.16-2001 (декабрь 2001 года), являющийся первым стандартом «точка-многоточка», был ориентирован на работу в спектре от 10 до 66 ГГц и, как следствие, требовал нахождения передатчика и приёмника в области прямой видимости, что является существенным недостатком, особенно в условиях города. Согласно описанным спецификациям, сеть 802.16 могла обслуживать до 60 клиентов со скоростью канала T-1 (1,554 Мбит/с).

Позднее появились стандарты IEEE 802.16a, IEEE 802.16-2004 и IEEE 802.16e (мобильный WiMax), в которых было снято требование прямой видимости между передатчиком и приёмником.

Основные параметры перечисленных стандартов технологии WiMax сведены в табл.3.8.

Таблица 3.8

Параметр	<i>IEEE 802.16</i>	<i>IEEE 802.16a</i>	<i>IEEE 802.16-2004</i>	<i>IEEE 802.16e</i>
<b>Принят, год</b>	2001	2003	2004	2005
<b>Диапазон частот, ГГц</b>	10 - 66	менее 11	менее 11	2 - 6
<b>Модуляция</b>	QPSK, 16 QAM, 64 QAM	OFDM 256	OFDM 256	OFDM 256
<b>Скорость, Мбит/с</b>	32 - 134	1 - 75	1 - 75	до 30
<b>Мобильность</b>	Нет	Нет	Нет	Да
<b>Ширина канала, МГц</b>	20, 25 и 28	От 1,25 до 20 с 16 логическими каналами	От 1,25 до 20 с 16 логическими каналами	Более 5
<b>Радиус ячейки, км</b>	1 - 5	5 – 8, максимум 50	5 – 8, максимум 50	1 - 5

Рассмотрим основные **отличия технологий WiMax от WiFi**.

1. *Малая мобильность.* Первоначально стандарт разрабатывался для стационарной беспроводной связи на большие расстояния и предусматривал мобильность пользователей в пределах здания. Лишь в 2005 году был разработан стандарт IEEE 802.16e, ориентированный на мобильных пользователей. В настоящее время ведётся разработка новых спецификаций 802.16f и 802.16h для сетей доступа с поддержкой работы мобильных (подвижных) клиентов при скорости их движения до 300 км/ч.

2. *Использование более качественных радиоприемников и передатчиков* обуславливает более высокие затраты на построение сети.

3. *Большие расстояния* для передачи данных требуют решения ряда специфических проблем: формирование сигналов разной мощности, использование нескольких схем модуляции, проблемы защиты информации.

4. *Большое число пользователей* в одной ячейке.

5. *Более высокая пропускная способность*, предоставляемая пользователю.

6. Высокое качество обслуживания мультимедийного трафика.

Первоначально считалось, что IEEE **802.11** – мобильный аналог *Ethernet*, **802.16** – беспроводной стационарный аналог кабельного телевидения. Однако появление и развитие технологии WiMax (IEEE 802.16e) для поддержки мобильных пользователей делает это утверждение спорным.

### 3.6.5. Беспроводные персональные сети

**Персональные сети** (Personal Area Networks – PAN) предназначены для взаимодействия устройств, принадлежащих одному владельцу и расположенных территориально на небольшом расстоянии (около 10 м).

Особенности PAN:

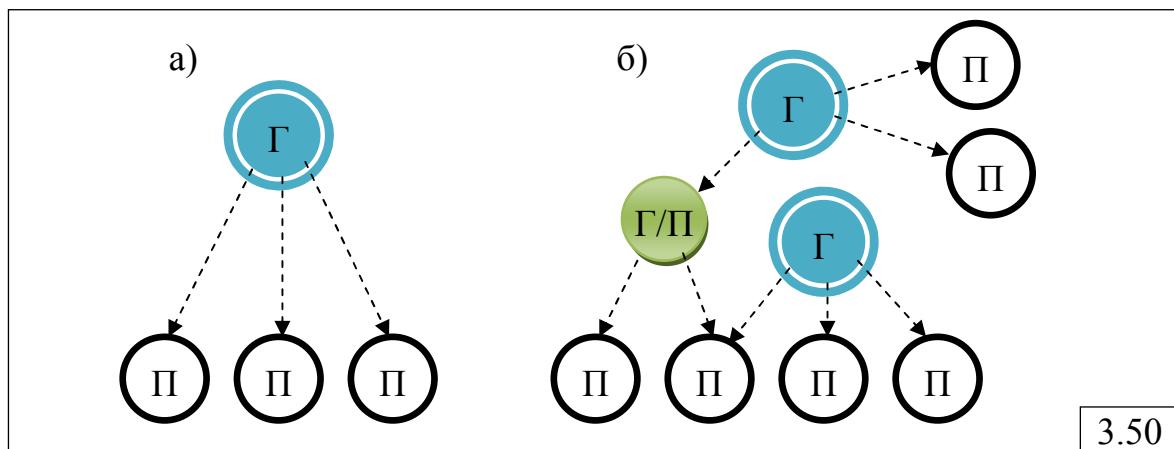
- простота, малые размеры и низкая стоимость объединяемых устройств и, как следствие этого, низкая стоимость реализации сети;
- небольшой диаметр сети;
- высокие требования к безопасности;
- беспроводная реализация;
- небольшая мощность излучаемых сигналов (не более 100 мВт).

#### 3.6.5.1. Технология Bluetooth

Технология Bluetooth, описанная в стандарте IEEE 802.15.1 обеспечивает взаимодействие различных устройств в разделяемой среде диапазона 2,4 МГц со скоростью передачи до 1 Мбит/с.

В основе Bluetooth лежит концепция *пикосети*, которая характеризуется следующими особенностями:

- небольшая область покрытия от 10 м до 100 м;
- количество устройств в сети – до 255;
- количество активных (одновременно взаимодействующих) устройств – до 8;
- одно устройство *главное* ( $\Gamma$ ), в качестве которого обычно используется персональный компьютер, остальные *подчиненные* ( $\Pi$ ) (см. рис.3.50,а);
- несколько пикосетей могут образовывать рассредоточенную сеть, в которой одно устройство, называемое мостом, одновременно принадлежит нескольким сетям и может быть главным устройством одной пикосети и подчинённым устройством другой пикосети (рис.3.50,б);
- метод доступа – CDMA с использованием техники FHSS;
- надёжность передачи данных реализуется с помощью механизма квитирования;
- кадры имеют длину до 343 байт;
- для передачи голоса используются кадры длиной 30 байт.



### 3.6.5.2. Технология ZigBee

ZigBee – технология, описанная в стандарте IEEE 802.15.4 и предназначенная для построения беспроводных персональных сетей (WPAN) с использованием небольших маломощных радиопередатчиков. Спецификация ZigBee нацелена на приложения, которым требуется большее время автономной работы от батарей и большая безопасность, при небольших скоростях передачи данных.

Основная особенность технологии ZigBee заключается в том, что она при относительно *невысоком энергопотреблении* поддерживает не только простые топологии беспроводной связи («точка-точка» и «звезда»), но и сложные беспроводные сети с многосвязной (ячеистой) топологией с ретрансляцией и маршрутизацией сообщений. Области применения технологии ZigBee – это построение беспроводных сенсорных сетей, автоматизация жилых и строящихся помещений, создание индивидуального диагностического медицинского оборудования, системы промышленного мониторинга и управления, а также применение в бытовой электронике и персональных компьютерах.

Технология ZigBee разработана с целью быть *проще и дешевле*, чем другие беспроводные персональные сети, такие как Bluetooth.

Устройство ZigBee может активироваться (переходить от спящего режима к активному) за 15 миллисекунд или меньше, что существенно меньше по сравнению с Bluetooth, для которого задержка при переходе от спящего режима к активному достигает 3-х секунд. Так как устройства ZigBee большую часть времени находятся в спящем режиме, уровень потребления энергии может быть очень низким, благодаря чему достигается продолжительная работа батарей.

Типовые области применения технологии ZigBee:

- домашняя автоматизация – температурный контроль, охрана и безопасность, датчики воды и мониторинг энергии, датчики задымления и пожара и т.д.;
- мобильные службы – мобильные оплата, мониторинг и контроль, охрана и контроль доступа в помещения, охрана здоровья, телепомощь;
- промышленное и коммерческое применение — контроль производственных процессов и промышленного оборудования, управление энергией, контроль доступа.

Существуют три типа устройств ZigBee.

- **Координатор ZigBee (ZC)** – наиболее ответственное устройство, формирующее пути дерева сети и связывающееся с другими сетями. В каждой сети есть один координатор ZigBee, который запускает сеть и может хранить информацию о сети.
- **Маршрутозадающий ZigBee (ZR)** – может выступать в качестве промежуточного устройства, передавая данные между остальными устройствами.

- **Конечное устройство** ZigBee (ZED) – может обмениваться информацией с материнским узлом (координатором или маршрутизатором), но не может передавать данные от других устройств. Такое поведение позволяет узлу большую часть времени пребывать в спящем состоянии, что позволяет экономить энергоресурс батареи. Конечное устройство имеет небольшую память, что делает его дешёвым в производстве.

Устройства ZigBee должны быть совместимы со стандартом IEEE 802.15.4 беспроводных персональных сетей, который описывает нижние слои протокола (физический слой PHY и управление доступом MAC). Стандарт IEEE 802.15.4 (ZigBee) предусматривает использование метода широкополосной модуляции с прямым расширением спектра и работу в трех диапазонах:

- 1 канал в диапазоне 868,0-868,6 МГц;
- 10 каналов в диапазоне 902-928 МГц (шаг центральных частот 2 МГц, самая нижняя из них – 906 МГц);
- 16 каналов в диапазоне 2400-2483,5 МГц (шаг центральных частот 5 МГц, самая нижняя из них – 2405 МГц).

Соответственно скорость передачи данных составляет 20 кбит/с, 40 кбит/с и 250 кбит/с для каждого канала, расстояние передачи – от 10 до 75 метров.

Базовый режим доступа к каналу в сетях ZigBee – CSMA/CA – множественный доступ с контролем несущей и предотвращением коллизий. Однако возможны ситуации, исключающие применение CSMA. Например, при передаче пакетов подтверждения приема данных (если потеря пакета критична)

Стандарт ZigBee призван заполнить вакуум в спектре низкоскоростных и дешевых беспроводных сетевых технологий, поскольку делает возможным построение сетей с низким потреблением энергии и гибкими функциями поддержки беспроводного взаимодействия.

### **3.6.6. Беспроводные сенсорные сети**

Беспроводная сенсорная сеть (WSN – Wireless Sensor Network) представляет собой распределённую самоорганизующуюся устойчивую к отказу отдельных элементов сеть, состоящую из множества необслуживаемых и не требующих специальной установки **датчиков (сенсоров)** и **исполнительных устройств**, объединенных посредством радиоканала. Область покрытия сенсорной сети может составлять *от нескольких метров до нескольких километров* за счет ретрансляции сообщений от одного элемента к другому.

Беспроводные сенсорные сети находят всё более широкое применение в производстве, на транспорте, в системах обеспечения жизнедеятельности, в охранных системах и т.п. Использование недорогих беспроводных сенсорных устройств контроля параметров делает возможным применение сенсорных сетей для контроля:

- различных параметров (температура, давление, влажность и т. п.);
- доступа в режиме реального времени к удаленным объектам мониторинга;
- отказов исполнительных механизмов;
- экологических параметров окружающей среды.

Беспроводные сенсорные сети состоят из *миниатюрных вычислительных устройств – мотов*, снабженных сенсорами (датчиками температуры, давления, освещенности, уровня вибрации, местоположения и т. п.) и *приемопередатчиками сигналов*, работающими в заданном радиодиапазоне. Сенсорная сеть позволяет подключать до 65000 устройств.

Каждый узел сенсорной сети может содержать различные датчики для контроля внешней среды, микрокомпьютер и приемопередатчик. Это позволяет устройству проводить измерения, самостоятельно проводить начальную обработку данных и поддерживать связь с внешней информационной системой.

«Классическая» архитектура сенсорной сети основана на типовом узле, который может быть представлен тремя устройствами.

**1. Сетевой координатор (FFD — Fully Function Device):**

- осуществляет глобальную координацию, организацию и установку параметров сети;
- наиболее сложное устройство, требующее память большой ёмкости и источник питания.

**2. Устройство с полным набором функций (FFD — Fully Function Device):**

- поддерживает стандарт 802.15.4 (ZigBee);
- дополнительная память и энергопотребление позволяют выполнять роль координатора сети;
- поддерживает все топологии («точка-точка», «звезда», «дерево», «ячеистая сеть»);
- общается с другими устройствами сети.

**3. Устройство с ограниченным набором функций (RFD — Reduced Function Device):**

- поддерживает ограниченный набор функций стандарта 802.15.4;
- поддерживает топологии «точка-точка», «звезда»;
- не выполняет функции координатора;
- обращается к координатору сети и маршрутизатору.

### **3.6.7. Сравнение беспроводных технологий**

Технологии WiMAX и WiFi имеют много общего – терминыозвучны, название стандартов, на которых основаны эти технологии, похожи (стандарты разработаны IEEE, оба начинаются с «802.»), а также обе технологии используют беспроводное соединение и могут использоваться для подключения к Интернету. Но, несмотря на это, эти технологии направлены на решение совершенно разных задач.

В табл. 3.9 для сравнения сведены рассмотренные выше беспроводные технологии передачи данных.

Таблица 3.9

Техноло- гия	Стандарт	Область примен.	Пропускная способность	Радиус действия	Диапазон частот
<i>WiFi</i>	802.11a	WLAN	до 54 Мбит/с	до 100 м	5,0 ГГц
<i>WiFi</i>	802.11b	WLAN	до 11 Мбит/с	до 100 м	2,4 ГГц
<i>WiFi</i>	802.11g	WLAN	до 108 Мбит/с	до 100 м	2,4 ГГц
<i>WiFi</i>	802.11n	WLAN	до 300 Мбит/с, в перспективе до 600 Мбит/с	до 100 м	2,4 - 2,5; 5,0 ГГц
<i>WiMax</i>	802.16d	WMAN	до 75 Мбит/с	6-10 км	1,5-11 ГГц
<i>WiMax</i>	802.16e	Mobile WMAN	до 40 Мбит/с	1-5 км	2.3-13.6 ГГц
<i>Bluetooth v.1.1</i>	802.15.1	WPAN	до 1 Мбит/с	до 10 м	2,4 ГГц
<i>Bluetooth v.1.1</i>	802.15.3	WPAN	от 11 Мбит/с до 55 Мбит/с	до 100 м	2,4 ГГц
<i>ZigBee</i>	802.15.4	WPAN	от 20 кбит/с до 250 кбит/с	1-100 м	2,4 ГГц (16 каналов); 915МГц (10); 868 МГц (1)
<i>Инфра- красный порт</i>	IrDa	WPAN	до 16 Мбит/с	до 50 см; од- носторонняя связь до 10 м	

## Раздел 4. ГЛОБАЛЬНЫЕ СЕТИ

Совокупность различных сетей (подсетей, ЛВС), расположенных на значительных расстояниях друг от друга и объединенных в единую сеть с помощью телекоммуникационных средств, представляет собой **территориально-распределенную сеть**, которую можно рассматривать как совокупность различных сред передачи, коммуникационных протоколов и систем управления сетями. Примерами территориально-распределенных сетей являются корпоративные сети организаций, объединяющие офисные сети, расположенные в разных городах, регионах и даже на разных континентах, городские, региональные, государственные сети и т.п.

Современные средства телекоммуникаций объединяют множество взаимосвязанных территориально-распределённых и локальных вычислительных сетей (представляющие собой подсети) различных организаций практически всего земного шара в единую сеть – **глобальную вычислительную сеть Internet**.

Поскольку территориально-распределённые и глобальные сети используют одинаковые принципы, технологии и оборудование, то их принято называть единым термином – **глобальные сети** или *Wide Area Network (WAN)*.

Для корректной работы глобальных сетей необходимо все сетевые стандарты связать так, чтобы они могли сосуществовать друг с другом, включая сети не на ЛВС-стандартах, такие как сети X.25 или IBM SNA.

### 4.1. Принципы организации глобальных сетей

#### 4.1.1. Характерные особенности глобальных сетей

В отличие от ЛВС характерными особенностями глобальных сетей являются следующие.

1. *Неограниченный* территориальный охват.
2. Сеть объединяет ЭВМ самых *разных классов* (от персональных до суперЭВМ), локальные и территориальные сети *разных технологий*.
3. Для объединения различных сетей и передачи данных на большие расстояния используется специальное оборудование, а именно: *аппаратура передачи данных* (модемы, приемопередатчики и т.п.) и *активное сетевое оборудование* (маршрутизаторы, коммутаторы, шлюзы).
4. Топология глобальных сетей, в общем случае, *произвольная*.
5. Одной из важнейших задач, решаемой при построении глобальной сети, является организация эффективной *маршрутизации* передаваемых данных.
6. Глобальная сеть может содержать *каналы связи разных типов*: кабельные оптические и электрические, в том числе телефонные, беспроводные радио и спутниковые каналы, имеющие различные пропускные способности (от нескольких кбит/с до сотен Гбит/с).

### 4.1.2. Достоинства глобальных сетей

1. Предоставление пользователям сети неограниченного доступа к любым вычислительным и информационным ресурсам, а также множества специфических услуг, таких как электронная почта, голосовая связь, конференцсвязь, телевидение по запросу, доступ к разнообразным информационным ресурсам и т.д.

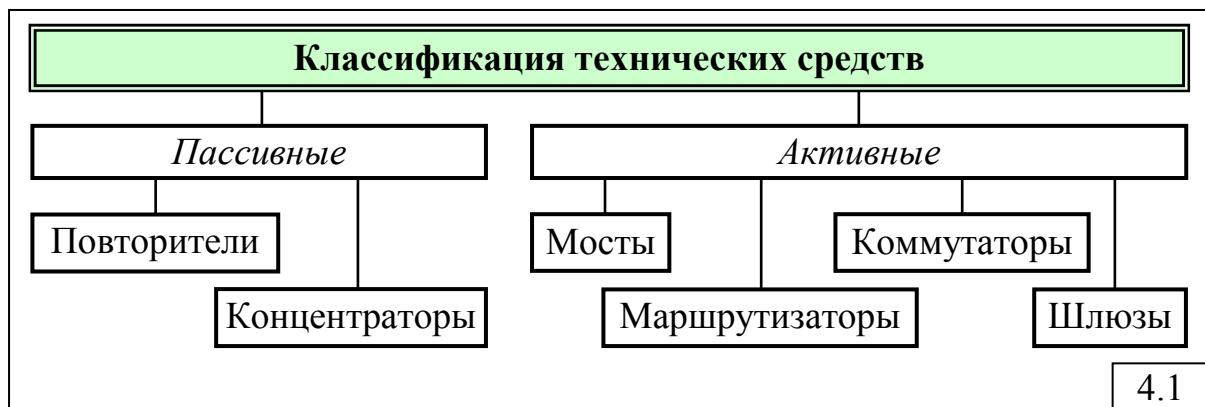
2. Возможность доступа к ресурсам сети практически из любой точки Земного шара.

3. Возможность передачи по сети любых видов данных, в том числе таких специфических как аудио и видео.

### 4.2. Технические средства объединения сетей

Классификация технических средств объединения сетей, представленная на рис.4.1, включает в себя:

- *пассивные* технические средства, используемые для объединения отдельных сегментов и расширения ЛВС, к которым относятся:
  - повторители (repeater);
  - концентраторы (hub);
- *активные* технические средства, используемые для построения территориально-распределённых и глобальных сетей путём объединения как ЛВС, так и сетей других не ЛВС-технологий:
  - мосты (bridge);
  - маршрутизаторы (router);
  - коммутаторы (switch);
  - шлюзы (gateway).

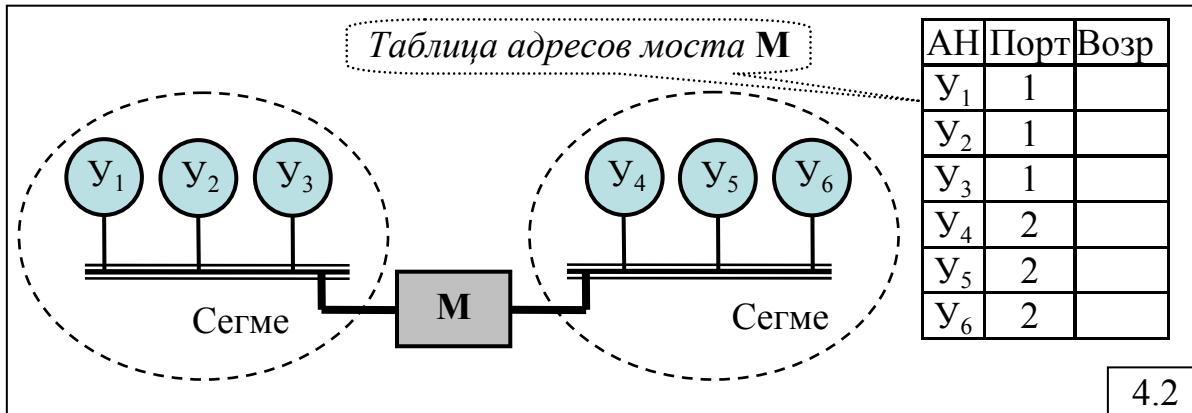


Активные технические средства, в отличие от пассивных, основной функцией которых является усиление передаваемого сигнала, управляют трафиком на основе адресов назначения передаваемых данных, то есть работают на 2-м и более высоких уровнях OSI-модели. Пассивные технические средства работают, в основном, на 1-м физическом уровне.

#### 4.2.1. Мосты

**Мост** – простейшее сетевое устройство, объединяющее локальные или удаленные сегменты и регулирующее прохождение кадров между ними. Подсоединенные к мосту сегменты образуют логически единую

сеть, в которой любая станция может использовать сетевые ресурсы, как своего сегмента, так и всех доступных через мост сегментов (рис.4.2).



Мост работает на *подуровне MAC* второго канального уровня и прозрачен для протоколов более высоких уровней, то есть принимает решение о передаче кадра из одного сегмента в другой на основании физического адреса (MAC-адреса) станции назначения. Для этого мост формирует **таблицу адресов** (ТА), которая содержит (рис.4.2):

- список MAC-адресов (адресов назначения, AH) станций, подключенных к мосту;
- направление (**порт**), к которому станция подключена;
- "взраст" с момента последнего обновления этой записи.

Так как кадры, предназначенные для станции того же сегмента, не передаются через мост, трафик локализуется в пределах сегментов, что снижает нагрузку на сеть и повышает информационную безопасность. В отличие от повторителя, который действует на физическом уровне и всего лишь повторяет и восстанавливает сигналы, мост *анализирует целостность кадров и фильтрует кадры*, в том числе испорченные.

Мосты не нагружают работой остальные сетевые устройства – они находятся в одной большой сети с единым сетевым адресом и разными MAC-адресами.

Для получения информации о местоположении станций мосты изучают адреса станций, читая адреса всех проходящих через них кадров. При получении кадра мост сравнивает адрес назначения с адресами в ТА и, если такого адреса нет, то мост передает кадр по всем направлениям (кроме отправителя кадра). Такой процесс передачи называется "затоплением" (flooding). Если мост находит в ТА адрес назначения, то он сравнивает номер порта из ТА с номером порта, по которому пришёл кадр. Их совпадение означает, что адреса отправителя и получателя расположены в одном сегменте сети, следовательно, кадр не надо транслировать, и мост его игнорирует. Если же адреса отправителя и получателя расположены в разных сегментах, мост отправляет кадр в нужный сегмент сети.

*Достиныами мостов являются:*

- относительная простота и дешевизна объединения ЛВС;

- "местные" (локальные) кадры остаются в данном сегменте и не загружают дополнительно другие сегменты;
- присутствие мостов прозрачно для пользователей;
- мосты автоматически адаптируются к изменениям конфигурации сети;
- мосты могут объединять сети, работающие с разными протоколами сетевого уровня;
- ЛВС, объединенные мостами, образуют логически единую сеть, т.е. все сегменты имеют один и тот же сетевой адрес; поэтому перемещение компьютера из одного сегмента в другой не требует изменения его сетевого адреса;
- мосты, благодаря простой архитектуре, являются недорогими устройствами.

*Недостатки* состоят в следующем:

- дополнительная задержка кадров в мостах;
- не могут использовать альтернативные пути; из возможных путей всегда выбирается один, остальные – блокируются;
- могут способствовать значительным всплескам трафика в сети, например, при передаче кадра, адрес которого еще не содержится в таблице моста; такие кадры передаются во все сегменты;
- не могут предотвращать "широковещательные штормы";
- не имеют средств для изоляции ошибочно функционирующих сегментов.

Существуют мосты четырех основных типов (рис.4.3):

- прозрачные (transparent);
- транслирующие (translating);
- инкапсулирующие (encapsulating);
- с маршрутизацией от источника (source routing).



#### 4.2.1.1. Прозрачные мосты

**Прозрачные мосты** (transparent bridges) предназначены для объединения сетей с *идентичными протоколами* на канальном и физическом уровнях, например, Ethernet-Ethernet, Token Ring-Token Ring.

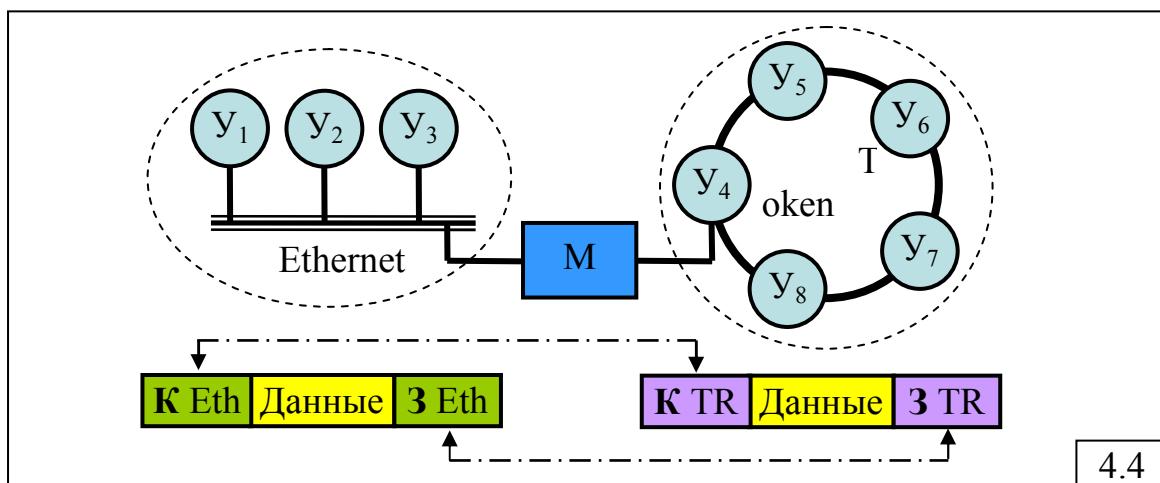
Прозрачный мост является самообучающимся устройством: в процессе работы для каждого подключенного сегмента автоматически строит таблицу адресов с адресами станций, находящихся в сегменте.

### Алгоритм функционирования моста:

- 1) прием поступающего кадра в буфер моста;
- 2) анализ адреса отправителя (АО) и его поиск в таблице адресов (ТА);
- 3) если АО отсутствует в ТА, то этот адрес и номер порта, по которому поступил кадр, заносятся в ТА;
- 4) анализ адреса получателя (АП) и его поиск в ТА;
- 5) если АП найден в ТА, и он принадлежит тому же сегменту, что и АО (т.е. номер выходного порта совпадает с номером входного порта), кадр удаляется из буфера;
- 6) если АП найден в ТА, и он принадлежит другому сегменту (на соответствующий порт);
- 7) если АП отсутствует в ТА, то кадр передается во все сегменты, кроме того сегмента, из которого он поступил.

#### 4.2.1.2. Транслирующие мосты

**Транслирующие мосты** (translating bridges) предназначены для объединения сетей с *разными протоколами* на канальном и физическом уровнях, например, Ethernet и Token Ring (рис.4.4).

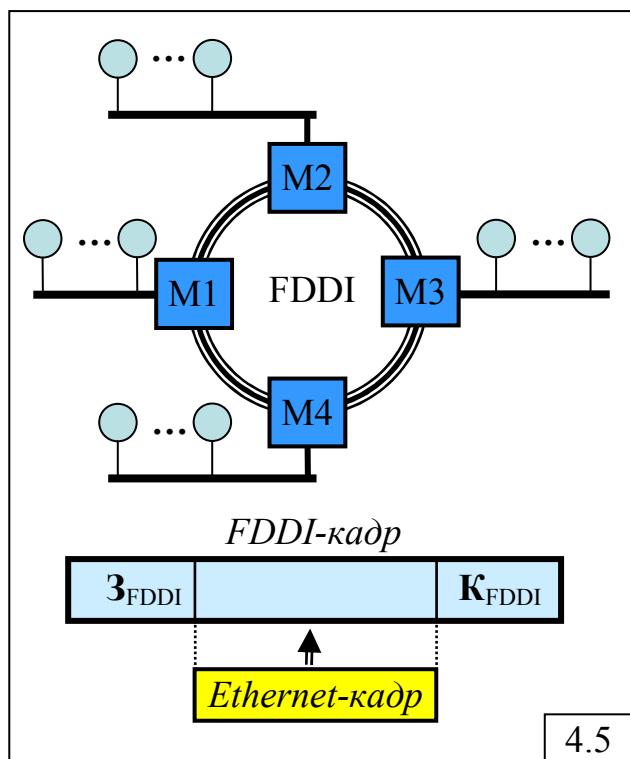


Транслирующие мосты объединяют сети путем манипулирования "конвертами": при передаче кадра из сети Ethernet в сеть TokenRing осуществляется замена заголовка (**З Eth**) и концевика (**K Eth**) Ethernet-кадра на заголовок (**З TR**) и концевик (**К TR**) TokenRing-кадра и наоборот. Поскольку в разных сетях используются кадры разной длины, а транслирующий мост не может разбивать кадры на части, то каждое сетевое устройство должно быть сконфигурировано для передачи кадров одинаковой длины.

#### 4.2.1.3. Инкапсулирующие мосты

**Инкапсулирующие мосты** предназначены для объединения сетей с одинаковыми протоколами канального и физического уровня через высокоскоростную магистральную сеть с другими протоколами, например 10-мегабитные сети Ethernet, объединяемые сетью FDDI (рис.4.5).

В отличие от транслирующих мостов, которые преобразуют "конверты" одного типа в другой, инкапсулирующие мосты вкладывают полученные кадры вместе с заголовком и концевиком в другой "конверт" (см. рис.4.5), который используется в магистральной сети (отсюда термин "инкапсуляция") и передает его по этой магистрали другим мостам для доставки к узлу назначения. Конечный мост извлекает Ethernet-кадр из FDDI-кадра и передаёт его в сегмент, в котором находится адресат. Длина поля данных FDDI-кадра достаточна для размещения Ethernet-кадра максимальной длины.



#### 4.2.1.4. Мосты с маршрутизацией от источника

**Мосты с маршрутизацией от источника** (source routing bridges) функционируют на основе информации, формируемой станцией, посылающей кадр, и хранимой в конверте кадра. В этом случае мостам не требуется иметь базу данных с адресами.

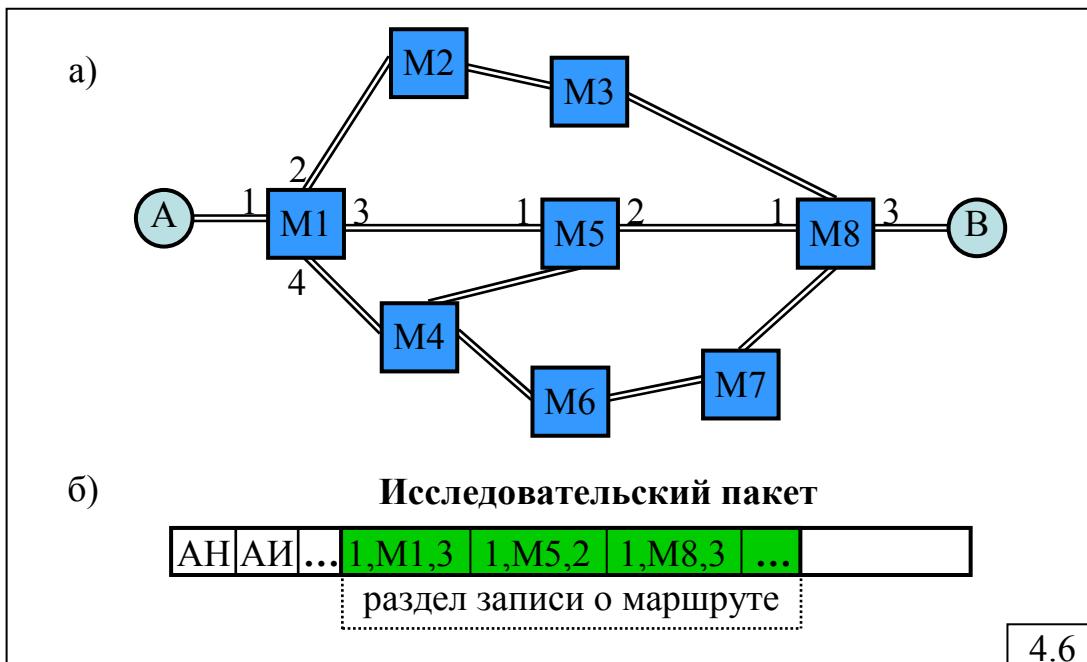
Каждое сетевое устройство определяет путь к адресату через процесс, называемый "*обнаружение маршрута*" (route discovery).

Упрощенно принцип обнаружения маршрута можно проиллюстрировать на следующем примере (рис.4.6).

Устройство-источник инициализирует обнаружение маршрута, посыпая специальный кадр (рис.4.6,б), называемый "*исследовательским*" (explorer). Исследовательские кадры используют специальный конверт, распознаваемый мостами с маршрутизацией от источника. При получении такого кадра каждый мост в специально отведенное в кадре место – *поле записи о маршруте* (routing information field), заносит следующие данные: номер входного порта, с которого был получен кадр, идентификатор моста ( $M_i$ ) и номер выходного порта, например: 1,M1,3 (см. рис.4.6,б). Далее мост передает этот кадр по всем направлениям, исключая то, по которому кадр был получен.

В итоге, станция назначения получает несколько исследовательских кадров, число которых определяется числом возможных маршрутов. Станция назначения выбирает один из маршрутов (самый быстрый, самый короткий или другой) и посылает ответ станции-источнику. В ответе содержится информация о маршруте, по которому должны посыпаться все кадры. Станция- отправитель запоминает маршрут и использует его всегда

для отправки кадров в станцию назначения. Эти кадры при отправке вкладываются в специальные конверты, понятные для мостов с маршрутизацией от источника. Мосты, получая эти конверты, находят соответствующую запись в списке маршрутов и передают кадр по нужному направлению.

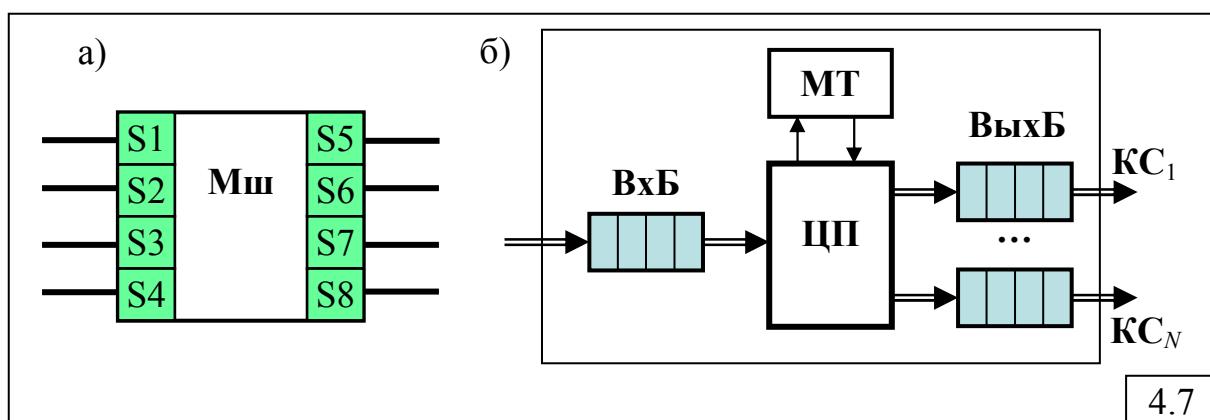


Маршрутизация от источника используется мостами в сетях Token Ring для передачи кадров между разными кольцами.

#### 4.2.2. Маршрутизаторы

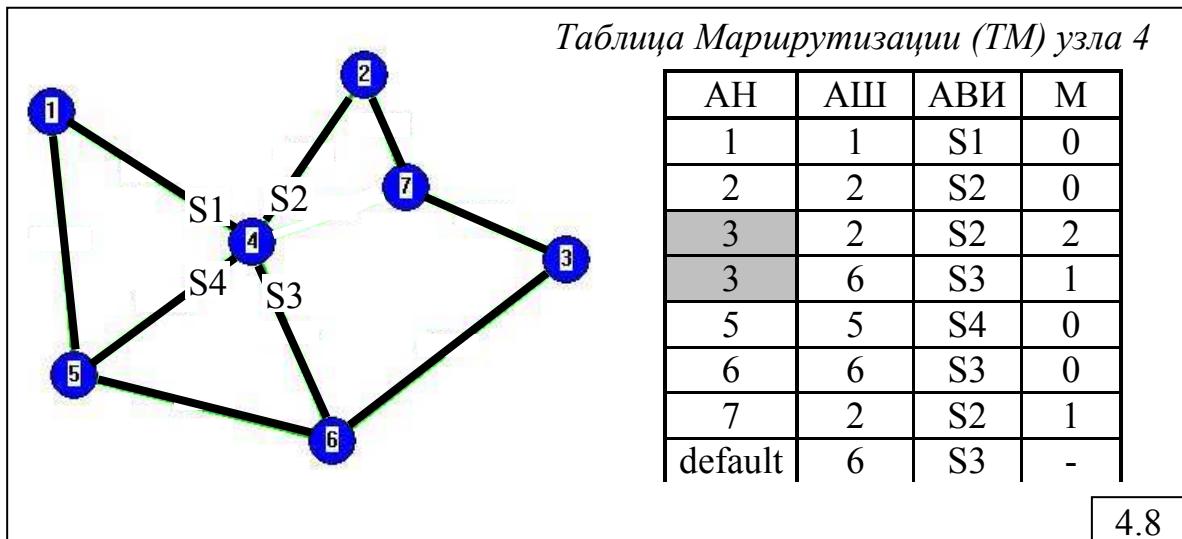
**Маршрутизаторы**, как и мосты, позволяют эффективно объединять сети и увеличивать их размеры, но, в отличие от последних, работают на *сетевом уровне* OSI-модели, то есть оперируют *сетевыми адресами*, и предоставляют более интеллектуальный сервис, заключающийся в определении наиболее подходящего пути и способа передачи пакетов.

В отличие от моста, работа которого прозрачна для сетевых устройств, работа маршрутизатора должна быть явно запрошена устройством. Для этого каждый порт (интерфейс) маршрутизатора имеет свой сетевой адрес: S<sub>1</sub>, S<sub>2</sub>, ... (рис.4.7.,а). На рис.4.7.,б показана каноническая структура маршрутизатора.



Поступающие пакеты заносятся во входной буфер **ВхБ**. Центральный процессор **ПМ** маршрутизатора последовательно анализирует заголовки пакетов и в соответствии с выбранной стратегией маршрутизации и заданной таблицей маршрутизации **ТМ** определяет выходной канал связи **КС**, в выходной буфер (**ВыхБ**) которого должен быть направлен пакет.

На рис.4.8 показан пример упрощённой маршрутной таблицы (МТ) узла (маршрутизатора) 4, находящегося в семиузловой сети.



В первом столбце указаны доступные (известные) этому маршрутизатору **сетевые адреса** назначения (АН). Для каждого АН во втором столбце указывается **адрес шлюза** (АШ) – следующего маршрутизатора, к которому должны направляться пакеты, а в третьем – сетевой адрес выходного **интерфейса** (АВИ) данного маршрутизатора: S1, S2, S3, S4. При наличии альтернативных путей для одного и того же АН может быть назначено несколько возможных путей передачи пакета. Так, например, пакеты с АН=3 могут быть направлены к маршрутизатору 2 или 6 через выходные интерфейсы S2 и S3 соответственно, что отображено в таблице в виде двух строк с одним адресом назначения. В этом случае выбор маршрута осуществляется на основе **метрики** (М), указанной в 4-м столбце.

Метрика может формироваться с учётом следующих факторов:

- расстояние между источником и приемником пакета, которое обычно измеряется "счетчиками хопов" (hop – количество маршрутизаторов, пройденных пакетом от источника до приемника);
- пропускная способность канала связи;
- время доставки разными путями;
- загрузка канала связи и т.д.

В нашем примере в качестве метрики используется расстояние до адреса назначения, измеряемое в хопах.

В больших сетях для *уменьшения размера таблицы маршрутизации* и, соответственно, времени поиска маршрута, используется ограниченный набор адресов назначения, указанных в таблице явно. Для всех других

адресов используется маршрут по умолчанию, которому в таблице соответствует строка (default), указывающая соседний маршрутизатор, используемый по умолчанию.

Весь спектр маршрутизаторов можно разбить на 3 группы (рис.4.9):

- 1) недорогие **периферийные маршрутизаторы** для соединения небольших удаленных филиалов с сетью центрального офиса;
- 2) **маршрутизаторы удаленного доступа** для сетей среднего размера;
- 3) мощные **магистральные маршрутизаторы** для базовых сетей крупных организаций.



#### **4.2.2.1. Периферийные маршрутизаторы**

**Периферийные маршрутизаторы** (Boundary Router) предназначены для объединения удаленных локальных сетей с центральной сетью и, как правило, имеют ограниченные возможности: один порт для соединения с локальной сетью и один – для соединения с центральным маршрутизатором.

Все сложные функции по маршрутизации возлагаются на центральный маршрутизатор, в связи с чем периферийный маршрутизатор не требует квалифицированного обслуживания на месте и характеризуется низкой стоимостью. Основная его функция состоит в принятии решения – пересыпать поступивший через порт локальной сети пакет по единственному каналу распределенной сети или нет. Тем самым исключается необходимость построения маршрутной таблицы.

#### **4.2.2.2. Маршрутизаторы удаленного доступа**

**Маршрутизаторы удаленного доступа** обычно имеют фиксированную (немодульную) конструкцию с небольшим числом портов, например: один LAN-порт – для сопряжения с локальной сетью, от одного до нескольких WAN-портов – для связи с маршрутизатором сети центрального офиса и один резервный порт для коммутируемого соединения.

Маршрутизаторы удаленного доступа, в общем случае, обеспечивают:

- *предоставление канала связи по требованию* (dial-on-demand) – автоматическое установление коммутируемого соединения только во время передачи данных;
- *сжатие данных*, позволяющее примерно вдвое повысить пропускную способность канала связи;

- автоматическое переключение трафика на коммутируемые линии (полностью или частично) в случае выхода из строя выделенных линий, а также при пиковых нагрузках.

#### **4.2.2.3. Магистральные маршрутизаторы**

**Магистральные маршрутизаторы**, в зависимости от архитектуры, делятся на маршрутизаторы:

- с централизованной архитектурой;
- с распределённой архитектурой.

Характерные особенности магистральных маршрутизаторов **с распределенной архитектурой**:

1) модульная конструкция:

- каждый модуль маршрутизатора снабжен собственным процессором, обрабатывающим локальный трафик, проходящий через порты этого модуля;
- центральный процессор задействуется только для маршрутизации пакетов между разными модулями;

2) наличие до нескольких десятков портов для сопряжения с локальными и территориальными сетями разных типов: Ethernet, Token Ring, FDDI, X.25, Frame Relay, ATM и т.д.;

3) поддержка средств обеспечения отказоустойчивости, необходимых для стратегически важных приложений:

- замена модулей в "горячем" режиме (без выключения питания);
- использование избыточных источников питания;
- автоматическая динамическая реконфигурация в случае отказов;
- распределенное управление.

В маршрутизаторах **с централизованной архитектурой** вся вычислительная мощность сосредоточена в одном модуле.

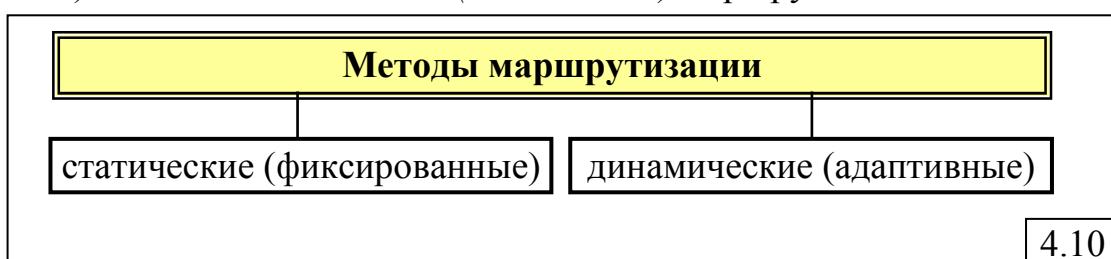
Основное *преимущество* магистральных маршрутизаторов с распределенной архитектурой по сравнению с централизованной – более высокие показатели производительности и отказоустойчивости.

Наиболее известными фирмами-поставщиками маршрутизаторов являются Cisco, 3Com, Hewlett-Packard.

#### **4.2.2.4. Методы маршрутизации**

Все методы маршрутизации, применяемые в маршрутизаторах, можно разбить на две группы (рис.4.10):

- методы *статической (фиксированной)* маршрутизации;
- методы *динамической (адаптивной)* маршрутизации.



**Статическая маршрутизация** означает, что пакеты передаются по определенному пути, установленному администратором и не изменяемому в течение длительного времени.

Статическая маршрутизация применяется в небольших мало изменяющихся сетях, благодаря таким *достоинствам как*:

- низкие требования к маршрутизатору;
- повышенная безопасность сети.

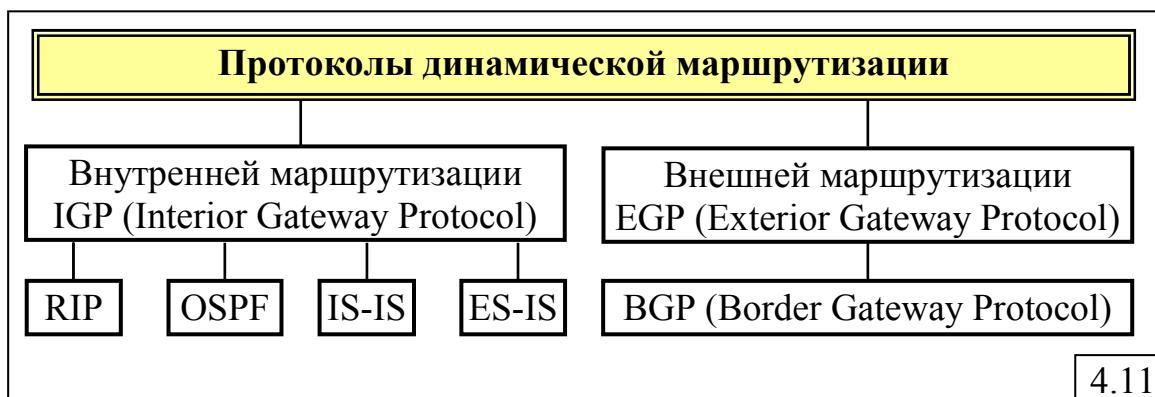
В то же время статической маршрутизации присущи следующие *недостатки*, существенно ограничивающие её применение:

- высокая трудоемкость эксплуатации (сетевые администраторы должны задавать и модифицировать маршруты вручную);
- медленная адаптация к изменениям топологии сети.

**Динамическая маршрутизация** – распределенная маршрутизация, позволяющая автоматически изменять маршрут следования пакетов при отказах или перегрузках каналов связи.

Для автоматического построения и модификации маршрутных таблиц используются протоколы (рис.4.11):

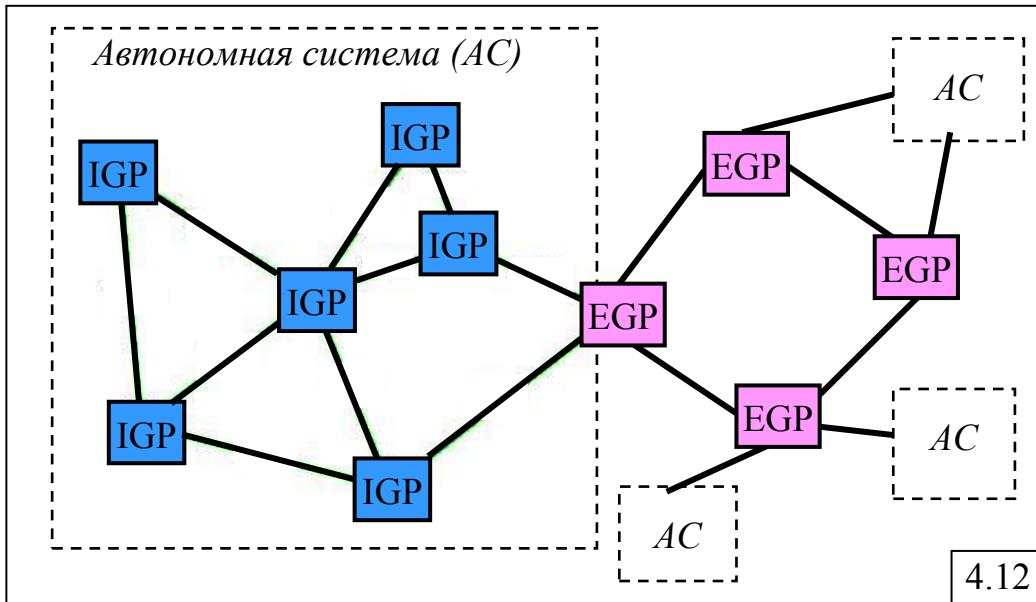
- *внутренней маршрутизации* – IGP (Interior Gateway Protocol), например RIP, OSPF, IS-IS, ES-IS;
- *внешней маршрутизации* – EGP (Exterior Gateway Protocol), например протокол BGP (Border Gateway Protocol), используемый в сети Internet.



4.11

С использованием **протоколов внутренней маршрутизации** маршрутные таблицы строятся в пределах так называемой *автономной системы* (autonomous system), представляющей собой совокупность сетей с единым административным подчинением (рис.4.12).

Для обмена маршрутной информацией между автономными системами чаще всего применяется **протокол внешней маршрутизации** EGP, разработанный для сети Internet. Этот протокол назван так потому, что внешний маршрутизатор, как правило, размещается на периферии автономной системы. Его задача заключается в сборе информации о доступности всех сетей данной автономной системы и последующей передаче этой информации внешним маршрутизаторам других автономных систем.



С учетом опыта применения протокола EGP был разработан протокол BGP, основанный на использовании надежного транспортного протокола TCP, который по сравнению с EGP:

- обеспечивает более быструю стабилизацию оптимальных маршрутов;
- меньше загружает сеть служебной информацией, в частности, за счет передачи при изменении сети информации, относящейся только к этому изменению.

#### **4.2.2.5. Протоколы маршрутизации**

Протоколы маршрутизации управляют динамическим обменом информацией о маршрутах между всеми маршрутизаторами сети, реализуются программно в маршрутизаторе, создавая таблицы маршрутизации, отображающие организацию всей сети.

Протоколы внутренней маршрутизации, как правило, основаны на алгоритмах обмена:

- таблицами "вектор-длина" – DVA (Distance Vector Algorithm) – протоколы типа «distance vector»;
- информацией о состоянии каналов – LSA (Link-State Algorithm) – протоколы типа «link state».



**DVA** - алгоритм обмена информацией о доступных сетях и расстояниях до них путём *периодической* рассылки маршрутизаторами широковещательных пакетов. К протоколам типа DVA относится один из самых первых протоколов RIP (Routing Information Protocol), который первоначально широко применялся в сети Интернет. Эти протоколы характеризуются тем, что периодически (даже если в сети не происходит изменений) посылают широковещательные пакеты с таблицами маршрутизации, которые, проходя через маршрутизаторы, обновляют таблицы маршрутизации.

В каждой строке маршрутной таблицы указываются:

- сетевой адрес некоторой сети;
- адрес маршрутизатора, через который следует передавать пакеты, направляемые в данную сеть;
- расстояние до сети.

При инициализации маршрутизатора в таблицу маршрутизации записываются:

- адреса соседних сетей;
- адреса соседних маршрутизаторов, с которыми данный маршрутизатор связан непосредственно;
- расстояние до соседних маршрутизаторов принимается равным 0 или 1 в зависимости от реализации.

Каждые 30 секунд маршрутизатор передает широковещательный пакет, содержащий пары (V, D), где V – адрес доступной сети, называемый **вектором**, а D – расстояние до этой сети, называемое **длиной вектора**.

В метрике RIP длина вектора измеряется *числом транзитных маршрутизаторов* (в хопах) между данным маршрутизатором и соответствующей сетью. На основании полученных таблиц "вектор-длина" маршрутизатор вносит дополнения и изменения в свою маршрутную таблицу, определяя пути минимальной длины во все доступные сети.

Поскольку каналы связи могут иметь разные пропускные способности, в некоторых реализациях RIP длина вектора умножается на весовой коэффициент, зависящий от скорости передачи данных по КС.

Основное достоинство RIP и других протоколов типа DVA – *простота реализации*.

*Недостатки RIP:*

- 1) *медленная стабилизация* оптимальных маршрутов;
- 2) *большая загрузка сети* передаваемыми таблицами "вектор-длина", обусловленная двумя основными факторами:

- периодичностью передачи широковещательных пакетов, содержащих таблицы "вектор-длина" – пакеты передаются даже в том случае, если в сети не было никаких изменений;
- большим объёмом этих таблиц, который пропорционален числу подсетей, входящих в сеть.

Протоколы типа distance vector целесообразно применять в небольших и относительно устойчивых сетях. В больших сетях периодически посылаемые широковещательные пакеты приводят к перегрузке сети и уменьшению пропускной способности.

**LSA** – алгоритмы обмена информацией о состоянии каналов, называемые также *алгоритмами предпочтения кратчайшего пути SPF* (Shortest Path First), основаны на динамическом построении маршрутизаторами карты топологии сети за счет сбора информации обо всех объединяющих их каналах связи. Для этого маршрутизатор периодически тестирует состояние каналов с соседними маршрутизаторами, помечая каждый канал как "активный" или "неактивный". На практике для уменьшения слишком частой смены этих двух состояний применяется следующее правило: «канал считается "активным" до тех пор, пока значительный процент тестов не даст отрицательного результата, и "неактивным" – пока значительный процент тестов не даст положительного результата».

При изменении состояния своих каналов маршрутизатор немедленно распространяет соответствующую информацию по сети всем остальным маршрутизаторам, которые, получив сообщения, обновляют свои карты сети и заново вычисляют кратчайшие пути во все точки назначения.

*Достоинства алгоритмов LSA:*

- 1) гарантированная и более быстрая стабилизация оптимальных маршрутов, чем в алгоритмах DVA;
- 2) простота отладки и меньший объем передаваемой информации, не зависящий от общего числа подсетей в сети.

Протоколы типа LSA используются в больших или быстро растущих сетях. К ним относятся такие протоколы, как Open Shortest Path First (OSPF) и Intermediate System to Intermediate System (IS-IS).

Самой распространенной реализацией алгоритма LSA является протокол OSPF – открытый стандарт, разработанный для применения в маршрутизаторах сети Интернет и широко используемый в настоящее время в других сетях (NetWare, SNA, XNS, DECNet).

Обладая всеми преимуществами алгоритмов LSA, протокол OSPF обеспечивает следующие дополнительные возможности.

1. *Маршрутизация* пакетов в соответствии с *заказанным типом обслуживания*. Сетевой администратор может присваивать межсетевым каналам различные значения "стоимости", основываясь на их пропускной способности, задержках или эксплуатационных расходах. Маршрутизатор выбирает путь следования пакета в результате анализа не только адреса получателя, но и поля "тип обслуживания" в заголовке.

2. *Равномерное распределение нагрузки* между альтернативными путями одинаковой стоимости (в отличие от протокола RIP, вычисляющего только один путь в каждую точку назначения).

3. *Маршрутизация* пакетов в соответствии с классом обслуживания. Сетевой администратор может создать несколько очередей с различными приоритетами. Пакет помещается в очередь на отправку по результатам анализа типа протокола. Для пакетов, чувствительных к временным задержкам, выделяется очередь с более высоким приоритетом.

4. *Аутентификация маршрутов.* Отсутствие этой возможности, например в протоколе RIP, может привести к перехвату пакетов злоумышленником, который будет передавать таблицы "вектор-длина" с указанной малой длиной путей от своего ПК во все подсети.

5. *Создание виртуального канала между маршрутизаторами,* соединенными не напрямую, а через некоторую транзитную сеть.

В модели OSI на основе алгоритма LSA определены протоколы маршрутизации сетевого уровня:

- "оконечная система – транзитная система", ES-IS (End System-to-Intermediate System);
- "транзитная система – транзитная система", IS-IS (Intermediate System-to-Intermediate System).

Протоколы типа LSA, в отличие от DVA, посылают информацию о маршрутах только для отображения изменений в своих сетевых соединениях.

Другое отличие заключается в возможности выбора канала передачи из нескольких возможных с учетом одного из параметров маршрутизации, задаваемого пользователем:

- задержки или скорости передачи данных;
- пропускной способности или производительности;
- надежности.

*Достоинства* маршрутизаторов по сравнению с мостами:

- высокая безопасность данных;
- высокая надежность сетей за счет альтернативных путей;
- эффективное распределение нагрузки по каналам связи за счет выбора наилучших маршрутов для передачи данных;
- большая гибкость за счёт выбора маршрута в соответствии с метрикой, учитывающей его стоимость, пропускную способность каналов связи и т.д.;
- гарантированная защита от "широковещательного шторма";
- возможность объединения сетей с разной длиной пакетов.

*Недостатки* маршрутизаторов:

- вносят сравнительно большую задержку в передачу пакетов;
- более сложны в установке и конфигурировании, чем мосты;
- при перемещении компьютера из одной подсети в другую требуется изменить его сетевой адрес;
- более дорогие, чем мосты, так как требуются более мощные процессоры, больший объем оперативной памяти, более дорогое

программное обеспечение, стоимость которого зависит от числа поддерживаемых протоколов.

В табл.4.1 сведены характерные особенности мостов и маршрутизаторов.

Таблица 4.1

### Характерные особенности мостов и маршрутизаторов

Признак	Мосты	Маршрутизаторы
1. Адресация	Работают с MAC-адресами	Работают с сетевыми адресами
2. Данные	Используют только адреса отправителя и получателя	Используют много разных источников для выбора маршрута
3. Конверт	Не имеют доступа к данным в конверте	Могут разбивать пакеты на более короткие
4. Пересылка	Пакеты только отфильтровываются	Пересылают пакеты на конкретный адрес
5. Приоритеты	Не учитывают	Учитывают, обеспечивая разные типы сервиса
6. Время задержки	Небольшое, однако при перегрузках возможны потери кадров	Большая задержка, но имеют более высокую производительность
7. Надежность	Нет гарантии доставки кадров	Гарантируют доставку пакетов
8. Отказоустойчивость	Перестают работать при неисправных сетях	Более устойчивы к отказам сети (за счет многих путей)
9. Безопасность	Могут ограничить доступ к устройствам	Обеспечивают более высокую степень защиты

Сети с протоколами, не обладающими сетевым уровнем и, соответственно, не имеющие сетевого адреса, не могут использовать маршрутизаторы и объединяются с помощью мостов или коммутаторов. Однако существуют маршрутизаторы, которые одновременно могут выполнять функции моста и называются *мостами/маршрутизаторами* (bridge/router или иногда brouter).

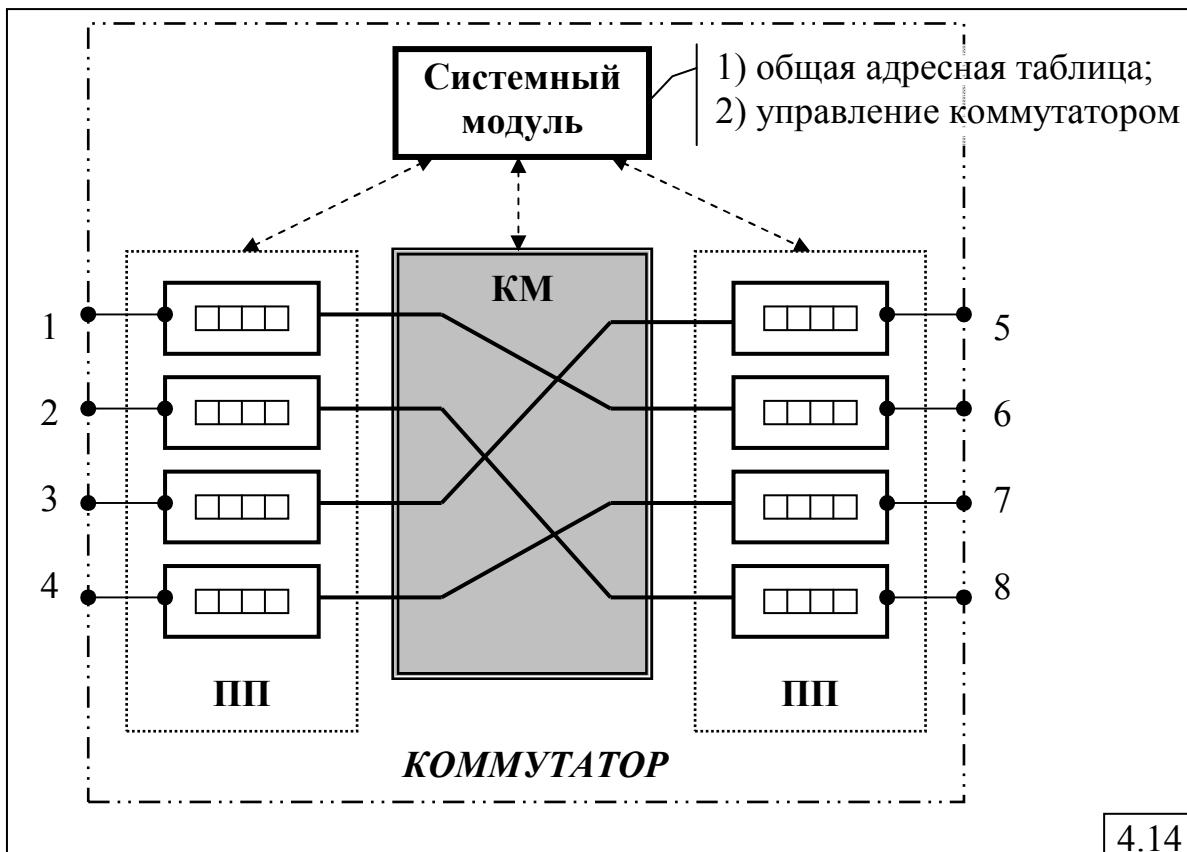
#### 4.2.3. Коммутаторы

Технология коммутации сегментов для ЛВС Ethernet появилась в 1990 году. Коммутатор по функциональным возможностям занимает промежуточное положение между мостом и маршрутизатором и при объединении сегментов локальных сетей работает на 2-м канальном уровне, то есть коммутирует данные на основе анализа MAC-адресов.

Производительность коммутаторов значительно выше, чем мостов, и достигает нескольких миллионов кадров в секунду.

#### 4.2.3.1. Каноническая структура коммутатора

Каноническая структура коммутатора представлена на рис.4.14.



Здесь: КМ – коммутационная матрица; ПП – процессоры портов с буферной памятью для хранения кадров.

В отличие от моста в коммутаторе каждый порт имеет свой процессор, в то время как все порты моста управляются одним процессором. В коммутаторе устанавливается один путь для всех кадров одного и того же сообщения, имеющих один адрес назначения и образующих так называемую «пачку», в то время как в маршрутизаторе для каждого пакета определяется свой наилучший путь. Передача кадров из входных буферов разных портов в выходные буфера коммутатора может происходить параллельно и независимо друг от друга. Эти особенности коммутатора обусловливают меньшие задержки при передаче данных по сравнению с маршрутизаторами.

Коммутационная матрица передаёт кадры из входных буферов в выходные на основе *таблицы коммутации*. Общее управление коммутатором и коммутационной матрицей реализуется *системным модулем*, который кроме того поддерживает общую адресную таблицу.

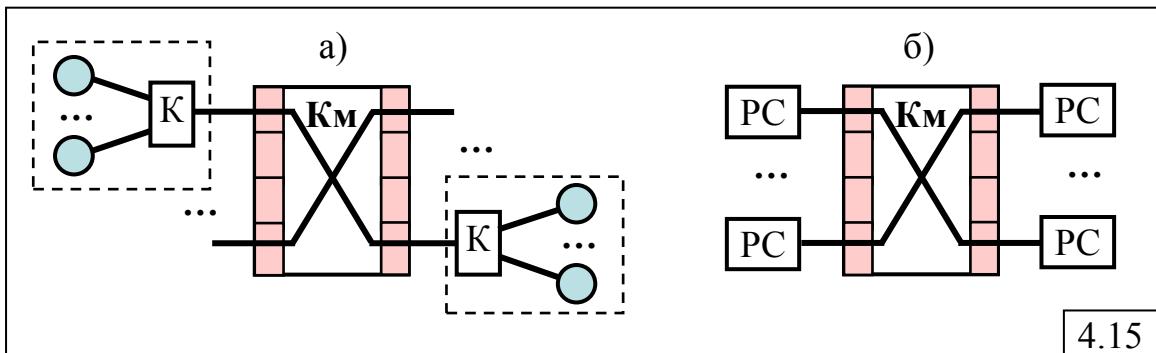
Коммутаторы могут реализовать один из двух способов коммутации:

- *с полной буферизацией кадра*, когда анализ заголовка поступающего кадра начинается только после того, как кадр будет полностью принят во входной буфер;

- «на лету» (*on-the-fly*), когда анализ заголовка поступающего кадра начинается сразу же после того, как во входной буфер принят заголовок кадра, не ожидая завершения приёма целиком всего кадра, что позволяет ещё больше сократить задержку кадра в коммутаторе.

Коммутаторы локальных сетей могут работать в одном из двух режимов:

- **полудуплексный**, когда к порту коммутатора подключается сегмент сети на коаксиальном кабеле или концентратор с подключенными к нему рабочими станциями (рис.4.15,а);
- **дуплексный**, когда к каждому порту коммутатора подключается только одна рабочая станция (рис.4.15,б).



Подключение к портам коммутатора *по одной рабочей станции* (а не сегментов) называется **микросегментацией**.

Переход на дуплексный режим требует изменения логики работы MAC-узлов и драйверов сетевых адаптеров (не фиксировать коллизии в ЛВС Ethernet, не ждать маркера в Token Ring и FDDI).

Соединения «коммутатор-коммутатор» могут поддерживать дуплексный режим.

При работе коммутатора может возникнуть ситуация, когда на один и тот же выходной порт коммутатора кадры поступают от нескольких входных портов с суммарной интенсивностью, превышающей предельное значение для данной технологии ЛВС, например для ЛВС Ethernet с пропускной способностью 10 Мбит/с – 14 880 кадров в секунду. Это приводит к перегрузкам и потерям кадров за счет переполнения выходного буфера соответствующего порта.

Для устранения подобных ситуаций необходим **механизм управления потоками кадров**.

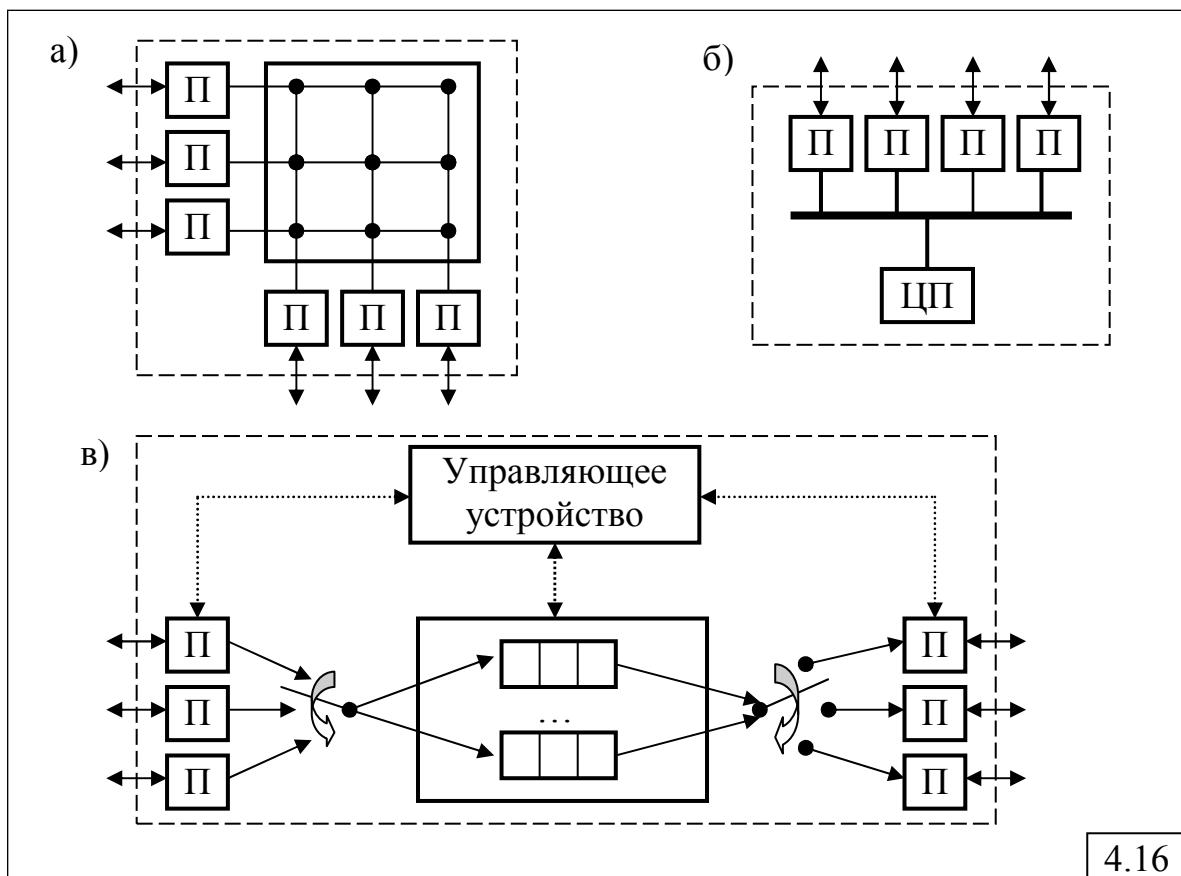
Для ЛВС Ethernet и Fast Ethernet в 1997 году принят стандарт IEEE 802.3x на управление потоком в *дуплексном режиме*, предусматривающий две команды – «Приостановить передачу» и «Возобновить передачу», которые направляются соседнему узлу. Для высокоскоростных сетей (Gigabit Ethernet и др.) с целью не допустить блокировок всех коммутаторов в сети разрабатываются более тонкие механизмы, которые указывают, *на какую величину* нужно уменьшить поток кадров, а не приостанавливать его до нуля.

При полудуплексном режиме коммутатор воздействует на конечный узел с помощью *механизмов доступа к среде*, а именно:

- **метод обратного давления**, заключающийся в создании искусственных коллизий в сегменте с помощью ѡам-последовательности;
- **метод агрессивного поведения**, когда порт коммутатора уменьшает межкадровый интервал или паузу после коллизии, что обеспечивает коммутатору преимущественный доступ к среде передачи.

#### 4.2.3.2. Техническая реализация коммутаторов

На рис.4.16 представлены типовые варианты технической реализации коммутаторов, которые во многом повторяют варианты реализации многопроцессорных вычислительных комплексов.



**Вариант 1.** На основе коммутационной матрицы (рис.4.16,а).

*Достоинства:*

- максимальная производительность;
- высокая надежность.

*Недостатки:*

- сложность и высокая стоимость;
- ограниченное число портов, поскольку с их увеличением существенно возрастает стоимость.

**Вариант 2.** На основе общей шины (рис.4.16,б).

*Достоинства:*

- простота;
- дешевизна.

*Недостатки:*

- низкая производительность;
- низкая надежность.

**Вариант 3.** На основе разделяемой многовходовой памяти (рис.4.16,в). Этот вариант занимает промежуточное положение между вариантами на основе коммутационной матрицы и на основе общей шины.

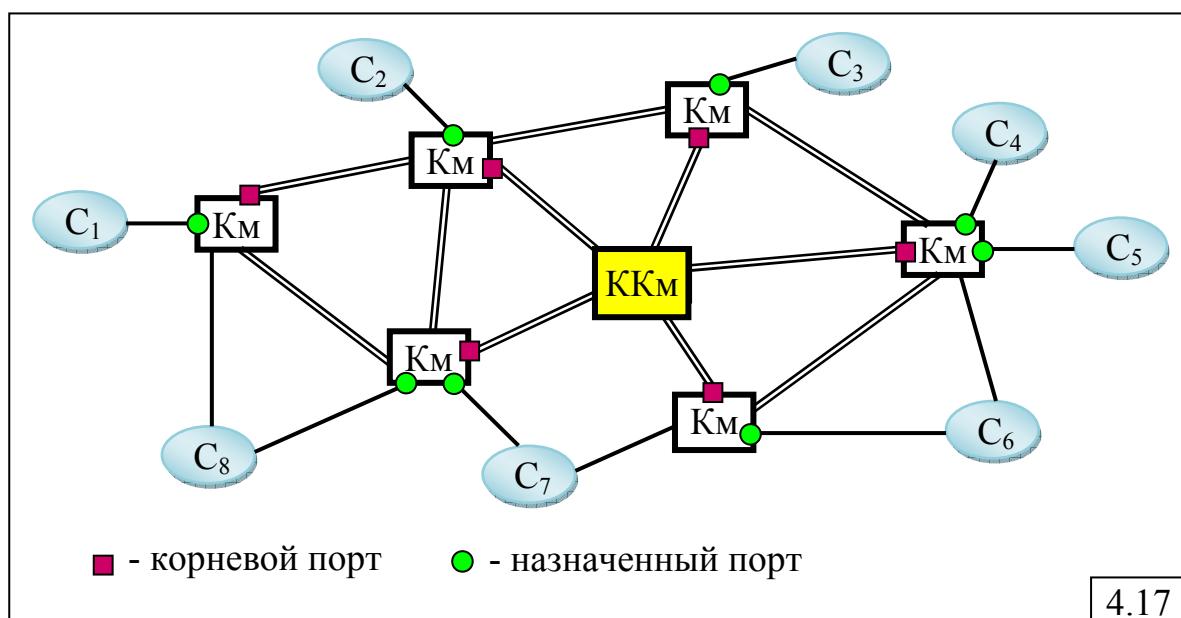
#### 4.2.3.3. Дополнительные функции коммутаторов

Коммутаторы по сравнению с мостами являются более интеллектуальными сетевыми устройствами и обладают рядом дополнительных функций.

1. Поддержка «алгоритма покрывающего дерева» («Spanning Tree»), который позволяет автоматически определять древовидную конфигурацию связей в сети для исключения петель и циклов в маршрутах (замкнутых маршрутов).

Алгоритм «Spanning Tree» реализуется в 3 этапа (рис.4.17):

- определяется автоматически (коммутатор с меньшим MAC-адресом блока управления) или назначается администратором **корневой коммутатор (ККм)**, от которого строится дерево;
- для каждого коммутатора (Км) определяется **корневой порт**, через который лежит кратчайший путь к корневому коммутатору;
- для каждого сегмента ( $C_i$ ) сети выбирается **назначенный порт** – порт, который обеспечивает кратчайшее расстояние от данного сегмента до корневого коммутатора.



2. Трансляция протоколов канального уровня.

Коммутаторы транслируют протоколы по тем же алгоритмам, что и транслирующие мосты (в соответствии со спецификациями IEEE 802.1H и RFC 1042).

3. Фильтрация кадров в соответствии с заданными условиями (например, ограничивают доступ к некоторым службам сети).

4. Приоритизация трафика независимо от технологии сети, например путём:

- приписывания приоритета портам коммутатора;
- назначения приоритета кадрам в соответствии со стандартом IEEE 802.1p, который предусматривает общий дополнительный заголовок для кадров Ethernet, состоящий из двух байт (перед полем данных кадра), где 3 бита задают приоритет кадра.

Свойства коммутаторов, позволяющие локализовать и контролировать потоки данных, а также управлять ими с помощью пользовательских фильтров, позволяют использовать коммутаторы для построения виртуальных ЛВС (ВЛВС, VLAN – Virtual LAN).

#### 4.2.4. Шлюзы

**Шлюз** – программно-аппаратный комплекс, соединяющий разнородные сети или сетевые устройства и позволяющий решать проблемы, связанные с различием протоколов и систем адресации.

Шлюзы переводят различные сетевые протоколы и позволяют различным сетевым устройствам не просто соединяться, а работать как единая сеть. В качестве примеров можно назвать пакетные адAPTERЫ (PAD), конверторы протоколов и устройства, соединяющие сети Ethernet и X.25. В сети Internet шлюзом часто называется межсетевой маршрутизатор.

Шлюзы обеспечивают еще более интеллектуальный и более медленный сервис, чем мосты и маршрутизаторы и могут работать на высших уровнях OSI-модели.

### 4.3. Сети с установлением соединений

Как указывалось в разделе 1, коммутация пакетов в компьютерных сетях может быть реализована двумя способами:

- на основе *дейтаграммной* передачи пакетов *без установления соединения* между взаимодействующими абонентами сети;
- на основе *виртуального канала с установлением соединения*.

Передача пакетов на основе *виртуальных каналов* широко применяется при построении глобальных вычислительных сетей с коммутацией пакетов и обеспечивает наибольшую эффективность для долговременных устойчивых потоков данных. Передача пакетов на основе виртуальных каналов реализована в сетях X.25, Frame Relay и ATM.

#### 4.3.1. Принцип передачи пакетов на основе виртуальных каналов

Существуют два типа виртуальных каналов:

- **коммутируемый виртуальный канал** (Switched Virtual Circuit, SVC), который создаётся по запросу абонента до начала передачи данных и только на время сеанса;
- **постоянный виртуальный канал** (Permanent Virtual Circuit, PVC), который создается вручную администратором сети (возможно, с

привлечением централизованных средств управления сетью) и не изменяется в течение достаточно длительного (в пределе неограниченного) времени.

При создании **коммутируемого виртуального канала** маршрутизация пакетов в узлах сети выполняется с использованием маршрутных таблиц *только один раз* на этапе установления соединения. При этом каждому виртуальному каналу присваивается *идентификатор (номер) виртуального канала* (Virtual Channel Identifier, VCI), на основе которого в дальнейшем происходит передача пакетов между узлами сети. Значение VCI имеет не глобальный характер, а локальный – действует только в пределах данного узла, причём VCI в разных узлах одного и того же виртуального канала в общем случае различны. В процессе создания виртуального канала для каждого порта узла формируются *таблицы коммутации*, предписывающие, на какой порт нужно передать пришедший пакет с определенным значением VCI. После создания виртуального канала узлы продвигают пакеты на основании значений VCI небольшой разрядности (не более 24 бит), а не адресов длиной десятки и даже сотни бит. Кроме того таблицы коммутации портов обычно содержат меньше записей, чем таблицы маршрутизации, так как хранят сведения только о действующих в данный момент соединениях, проходящих через данный порт коммутатора.

Такая организация передачи данных позволяет уменьшить задержку пакетов в сети за счет следующих факторов:

1) *решение о продвижении пакета принимается быстрее* из-за меньшего размера таблицы коммутации;

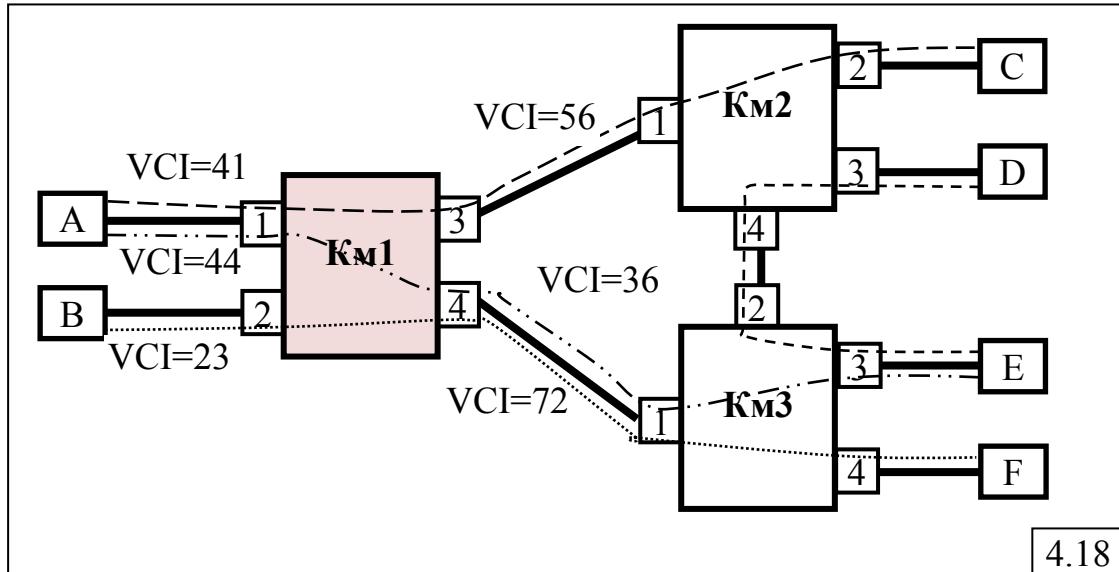
2) *возрастает эффективная (полезная) скорость передачи данных* за счет уменьшения доли служебной информации в заголовке пакета, так как идентификатор виртуального канала в заголовке пакета обычно занимает не более 24 бит, в то время как адреса конечных узлов в территориально-распределенных и глобальных сетях обычно имеют достаточно большую длину и занимают 6 и более байт.

Использование **постоянных виртуальных каналов** (PVC) более эффективно, чем коммутируемых, поскольку отсутствует этап установления соединения, и продвижение кадров выполняется на основе заранее сформированных таблиц коммутации. *Постоянный виртуальный канал* подобен *выделенному каналу* – обмен пакетами может происходить в любой момент времени. В то же время PVC отличается от выделенного канала тем, что пользователь делит пропускную способность сети с другими пользователями. С одной стороны, это обуславливает основной недостаток PVC по сравнению с выделенным каналом – отсутствие гарантий относительно реально предоставляемой пропускной способности, а с другой стороны – делает использование PVC дешевле, чем аренда выделенной линии.

Режим продвижения пакетов на основе таблицы коммутации называется **коммутацией**, а узлы сети – **коммутаторами**, которые

обычно работают не на третьем (сетевом), а на втором (канальном) уровне OSI-модели.

Принцип передачи пакетов на основе виртуальных каналов рассмотрим на примере фрагмента сети, представленного на рис.4.18. Узлы (компьютеры пользователей) А, В, С, D, E, F связаны в сеть с помощью 3-х четырёхпортовых коммутаторов Км1, Км2 и Км3.



Для установления соединения между конечными узлами узел-источник посыпает специальный пакет – запрос на установление соединения (Call Request), который содержит адрес узла назначения и номер виртуального соединения VCI. Этот номер имеет локальное значение для каждого порта (узла и коммутатора) и выбирается из множества свободных в данный момент номеров. Через один порт можно установить достаточно большое количество виртуальных соединений.

Пусть конечный узел А, устанавливающий виртуальное соединение с узлом В, сформировал пакет Call Request на установление соединения, в котором указаны адрес назначения АН=В и номер виртуального соединения VCI=41. Пакет Call Request направляется в порт 1 коммутатора Km1 сети, где по адресу назначения с использованием таблицы маршрутизации (рис.4.19,а) определяется номера порта Km1, на который нужно переслать пакет.

В соответствии с таблицей маршрутизации пакет Call Request с порта 1 направляется в порт 3. Одновременно коммутатор заменяет в пакете номер виртуального соединения VCI=41 на новое значение, которое выбирается из множества свободных номеров для выходного порта 3. В нашем примере это значение VCI=56. Наличие разных номеров VCI для разных портов коммутатора (на входе и выходе) позволяет реализовать дуплексный режим передачи данных.

Кроме таблицы маршрутизации для каждого порта формируется таблица коммутации. В таблице коммутации входного порта 1 коммутатор отмечает, что в дальнейшем пакеты, прибывшие на этот порт с номером VCI=41 должны передаваться на порт 3, причем номер виртуального

канала должен быть изменен на 56 (рис.4.19,б). Одновременно делается запись в таблице коммутации порта 3: пакеты, поступившие с VCI=56 нужно передавать на порт 1, меняя номер виртуального канала на VCI=41. Таким образом, при получении пакетов в обратном направлении узел-источник А получает пакеты с тем же номером VCI, с которым он отправлял их к узлу В.

<p><b>а)</b></p> <p><b>Таблица маршрутизации</b></p> <table border="1"> <thead> <tr> <th>AH</th> <th>Порт</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>1</td> </tr> <tr> <td>B</td> <td>2</td> </tr> <tr> <td>C</td> <td>3</td> </tr> <tr> <td>D</td> <td>3</td> </tr> <tr> <td>E</td> <td>4</td> </tr> <tr> <td>F</td> <td>4</td> </tr> </tbody> </table>	AH	Порт	A	1	B	2	C	3	D	3	E	4	F	4	<p><b>б)</b></p> <p><b>Таблицы коммутации портов</b></p> <table border="1"> <thead> <tr> <th colspan="3"><i>Порт 1</i></th> </tr> <tr> <th><b>Вх.</b></th> <th><b>Вых.</b></th> <th></th> </tr> </thead> <tbody> <tr> <td>VCI</td> <td>Порт</td> <td>VCI</td> </tr> <tr> <td>41</td> <td>3</td> <td>56</td> </tr> <tr> <td>44</td> <td>4</td> <td>36</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="3"><i>Порт 2</i></th> </tr> <tr> <th><b>Вх.</b></th> <th><b>Вых.</b></th> <th></th> </tr> </thead> <tbody> <tr> <td>VCI</td> <td>Порт</td> <td>VCI</td> </tr> <tr> <td>23</td> <td>4</td> <td>72</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="3"><i>Порт 3</i></th> </tr> <tr> <th><b>Вх.</b></th> <th><b>Вых.</b></th> <th></th> </tr> </thead> <tbody> <tr> <td>VCI</td> <td>Порт</td> <td>VCI</td> </tr> <tr> <td>56</td> <td>1</td> <td>41</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="3"><i>Порт 4</i></th> </tr> <tr> <th><b>Вх.</b></th> <th><b>Вых.</b></th> <th></th> </tr> </thead> <tbody> <tr> <td>VCI</td> <td>Порт</td> <td>VCI</td> </tr> <tr> <td>36</td> <td>1</td> <td>44</td> </tr> <tr> <td>72</td> <td>2</td> <td>23</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>	<i>Порт 1</i>			<b>Вх.</b>	<b>Вых.</b>		VCI	Порт	VCI	41	3	56	44	4	36	<i>Порт 2</i>			<b>Вх.</b>	<b>Вых.</b>		VCI	Порт	VCI	23	4	72				<i>Порт 3</i>			<b>Вх.</b>	<b>Вых.</b>		VCI	Порт	VCI	56	1	41				<i>Порт 4</i>			<b>Вх.</b>	<b>Вых.</b>		VCI	Порт	VCI	36	1	44	72	2	23			
AH	Порт																																																																													
A	1																																																																													
B	2																																																																													
C	3																																																																													
D	3																																																																													
E	4																																																																													
F	4																																																																													
<i>Порт 1</i>																																																																														
<b>Вх.</b>	<b>Вых.</b>																																																																													
VCI	Порт	VCI																																																																												
41	3	56																																																																												
44	4	36																																																																												
<i>Порт 2</i>																																																																														
<b>Вх.</b>	<b>Вых.</b>																																																																													
VCI	Порт	VCI																																																																												
23	4	72																																																																												
<i>Порт 3</i>																																																																														
<b>Вх.</b>	<b>Вых.</b>																																																																													
VCI	Порт	VCI																																																																												
56	1	41																																																																												
<i>Порт 4</i>																																																																														
<b>Вх.</b>	<b>Вых.</b>																																																																													
VCI	Порт	VCI																																																																												
36	1	44																																																																												
72	2	23																																																																												
4.19																																																																														

Аналогичные действия по запросу Call Request выполняются в коммутаторе Км2, где также в процессе маршрутизации формируются таблицы коммутации. После того, как пакет Call Request благополучно достигнет узла-назначения В, последний сформирует служебный пакет подтверждения, который будет передан узлу А по сформированному виртуальному каналу. Получение пакета подтверждения инициирует в узле А передачу пакетов с данными, которые будут передаваться в сети по сформированному виртуальному пути, причём значения VCI будут изменяться при передаче пакета от входного порта коммутаторов к выходному в соответствии с таблицами коммутаций по номерам виртуального соединения.

Пакеты данных уже не содержат длинные адреса конечных узлов, а имеют в заголовке только номер виртуального канала, на основании которого и производится коммутация всех пакетов, кроме пакета запроса на установление соединения. Созданный виртуальный канал не изменяется в течение всего времени существования соединения.

Таким образом, передача данных на основе виртуального канала реализуется в два этапа:

- этап маршрутизации всего одного пакета – запроса на установку виртуального соединения в соответствии с адресом назначения, в процессе которого формируются таблицы коммутации;
- этап коммутации пакетов на основании номера виртуального канала с использованием таблиц коммутации.

Использование виртуальных каналов оказывается эффективным при передаче через сеть долговременных потоков данных, но неэффективным для кратковременных потоков, так как на установление соединения уходит достаточно много времени.

### 4.3.2. Сети X.25

#### 4.3.2.1. Назначение и структура сетей X.25

Стандарт X.25 «Интерфейс между оконечным оборудованием данных и аппаратурой передачи данных для терминалов, работающих в пакетном режиме в сетях передачи данных общего пользования», принятый в 1976 году и дополненный в 1984 году, наилучшим образом подходит для передачи трафика низкой интенсивности, характерного для терминалов, и в меньшей степени соответствует более высоким требованиям трафика локальных сетей.

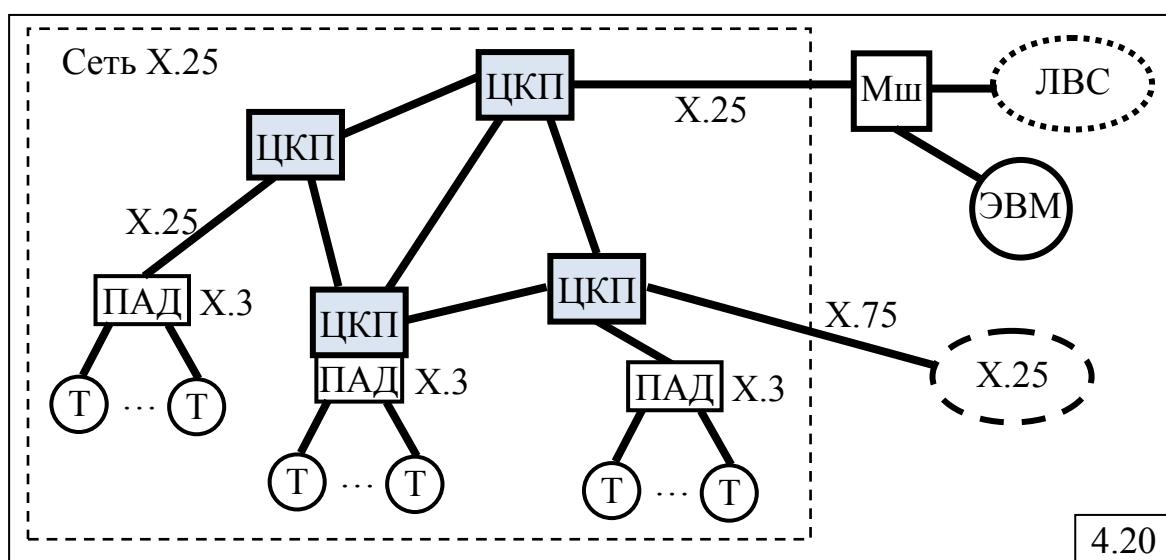
Сети, доступ к которым производится в соответствии с рекомендациями X.25, называют *сетями X.25* или *сетями пакетной коммутации*. Как видно из названия, стандарт не описывает внутреннее устройство сети X.25, а только определяет пользовательский интерфейс с сетью.

Сети X.25 долгое время были единственными доступными сетями, которые хорошо работают на ненадежных линиях благодаря протоколам с установлением соединения и коррекцией ошибок на двух уровнях – канальном и сетевом.

Взаимодействие двух сетей X.25 определяет стандарт X.75.

Сети X.25 характеризуются следующими особенностями.

Сеть X.25 состоит из коммутаторов, называемых *центрами коммутации пакетов (ЦКП)*, расположенных в различных географических точках и соединенных выделенными каналами (рис.4.20), которые могут быть как цифровыми, так и аналоговыми.



Для выполнения операций сборки нескольких низкоскоростных потоков байт от алфавитно-цифровых терминалов в пакеты, передаваемые

по сети и направляемые компьютерам для обработки, и обратной разборки пакетов, в сети используются специальные устройства – *PAD (Packet Assembler Disassembler – Сборщик-разборщик пакетов)*, которые в русскоязычных источниках называются ПАД (Пакетный Адаптер Данных). ПАД могут быть встроенным или удалёнными.

Стандартом определён *трехуровневый стек протоколов с использованием на канальном и сетевом уровнях протоколов с установлением соединения, управляющих потоками данных и исправляющих ошибки*.

Сетевой уровень рассчитан на работу только с *одним протоколом канального уровня* и не может подобно протоколу IP объединять разнородные сети.

Функциями ПАД в соответствии со стандартом X.3 являются:

- сборка символов, полученных от асинхронных терминалов T, в пакеты;
- разборка пакетов и вывод данных на асинхронные терминалы;
- управление процедурами установления соединения и разъединения по сети X.25;
- передача символов по требованию асинхронного терминала и др.

Терминалы не имеют конечных адресов сети X.25. Адрес присваивается порту ПАД, который подключен к коммутатору пакетов X.25 с помощью выделенного канала.

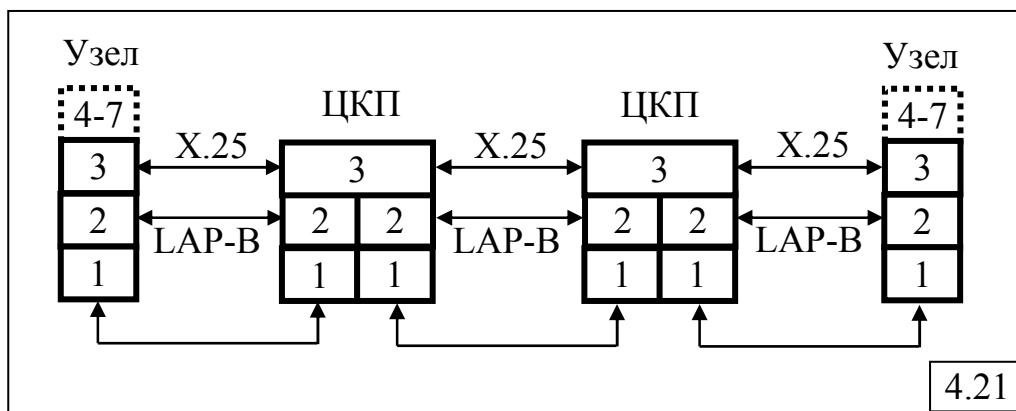
Компьютеры и локальные сети подключаются к сети X.25 непосредственно через адаптер X.25 или маршрутизатор (рис.4.20) с поддержкой протоколов X.25.

#### 4.3.2.2. Стек протоколов сети X.25

Стандарты сетей X.25 описывают 3 уровня протоколов:

- физический;
- канальный;
- сетевой.

На рис.4.21 показана модель взаимодействия конечных узлов (ЭВМ, маршрутизаторы, ПАД) и центров коммутации пакетов (ЦКП).



На физическом уровне определён протокол X.21 – универсальный интерфейс между оконечным оборудованием (DTE) и аппаратурой

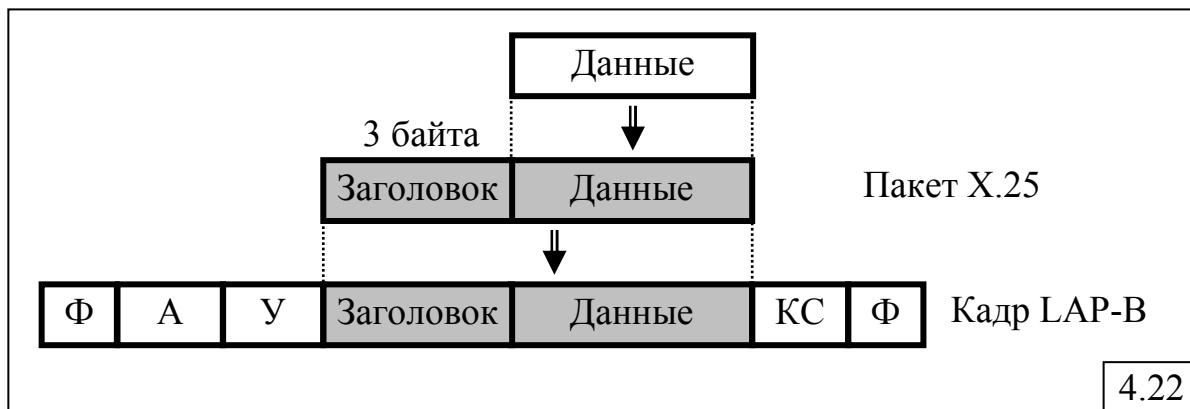
передачи данных (DCE) для синхронного режима работы в сетях общего пользования, а также протокол X.21bis для модемов, удовлетворяющих рекомендациям серии V.

На канальном уровне используется протокол LAP-B, являющийся подмножеством протокола HDLC. Этот протокол обеспечивает сбалансированный режим работы, что означает равноправие узлов, участвующих в соединении. По протоколу LAP-B устанавливается соединение между конечными узлами (компьютером, маршрутизатором или сборщиками-разборщиками пакетов) и коммутатором сети, а также между непосредственно связанными коммутаторами.

*Сетевой уровень X.25/3* (в стандарте назван *пакетным уровнем*) реализуется с использованием различных типов пакетов и выполняет функции *маршрутизации пакетов, установления и разрыва виртуального канала* между конечными абонентами сети и управления потоком пакетов.

На рис.4.22 показана последовательность формирования кадра канального уровня LAP-B, передаваемого между узлами и ЦКП.

В конечных узлах данные более высоких уровней (4-7) упаковываются на сетевом (пакетном) уровне в пакет X.25, который затем передаётся на 2-й канальный уровень, где пакет вкладывается в поле данных кадра LAP-B. Кадр LAP-B включает в себя двухбайтовый заголовок, содержащий адрес (A) и поле «Управление (У)», и концевик (2 или 4 байта), содержащий контрольную сумму (КС). В качестве обрамления кадра используется 8-битовая последовательность 01111110, называемая флагом (Ф). Назначение и содержание указанных полей рассматривается в п.4.4.10.2, посвящённом описанию протокола HDLC.



#### 4.3.2.3. Установление виртуального соединения

Для установления виртуального соединения узел-отправитель посылает узлу-получателю пакет Call Request (рис.4.23) протокола X.25.

Поля, расположенные в первых трех байтах заголовка пакета, используются во всех типах кадров протокола X.25.

Признак **Q** определяет *тип информации* в поле данных пакета: Q=1 – управляющая информация, Q=0 – данные.

Признак **D** предназначен для *подтверждения приёма* пакета узлом назначения.

Двухбитовое поле **Modulo** задаёт модуль нумерации пакетов: 10 – модуль 128, а 01 – модуль 8.

Поле **LGN** (Logical Group Number) содержит значение *номера логической группы*, объединяющей виртуальные каналы с одним общим функциональным признаком, например:

- постоянный виртуальный канал;
- коммутируемый дуплексный виртуальный канал и т.д.

Поле **LCN** (Logical Channel Number) содержит *номер виртуального канала*, назначаемый узлом-источником (для коммутируемых виртуальных каналов) или администратором сети (для постоянных виртуальных каналов). Максимальное количество виртуальных каналов, проходящих через один порт, равно  $2^8=256$ .

Поле **Тип** (Type), длиной 8 бит, указывает *тип пакета*: управляющий пакет или пакет данных. Для управляющих пакетов в этом же поле указывается подтип пакета, а для пакетов данных – номера положительных и отрицательных квитанций.

Следующие два поля определяют *длину адресов назначения и источника (DA и SA)*, которые располагаются в следующих двух полях. Адрес **DA** используется для маршрутизации пакета Call Request, а **SA** – для передачи узлом назначения подтверждения об установлении соединения путём посылки пакета Call Accepted – «Запрос принят», в котором эти адреса меняются местами. Адреса могут иметь произвольный формат.

Поля **Facilities length** (Длина поля услуг) и **Facilities** (Услуги) нужны для согласования дополнительных услуг, которые предоставляет сеть абоненту. Например, пользователь с помощью услуги «Согласование параметров управления потоком» может использовать нестандартные значения параметров протокола, таких как размер окна, максимальный размер поля данных пакета и т. п.

Поле **User Data** (Поле данных) может иметь различные максимальные значения длины: от 64 до 4096 байт. Предпочтительной является длина 128 байт.

Пакет Call Request маршрутизируется в узлах сети на основании таблицы маршрутизации, прокладывая при этом виртуальный канал. Начальное значение номера виртуального канала задает пользователь в этом пакете в поле LCN. После установления виртуального канала конечные узлы обмениваются пакетами данных (Data), в которых первые

1	2	3	4	5	6	7	8
Q	D	Modulo	LGN				
LCN							
Type							
Lengh DA		Lengh DA					
Destination address (DA)							
...							
Source address (SA)							
...							
Facilities length (FL)							
Facilities							
...							
User Data							
...							

4.23

три байта такие же, как в пакете Call Request, а адресные поля и поля услуг отсутствуют.

Коммутаторы (ЦКП) сетей X.25 проще и дешевле маршрутизаторов, поскольку не поддерживают процедур обмена маршрутной информацией и, как следствие, процедур поиска оптимальных маршрутов, а также не выполняют преобразований форматов кадров канальных протоколов. С другой стороны, по сравнению с коммутаторами локальных сетей, которые просто передают поступивший кадр на выходной порт, коммутаторы X.25 выполняют ряд дополнительных функций, а именно:

- принимают кадр LAP-B и проверяют контрольную сумму;
- при обнаружении ошибки или утере кадра организуют повторную передачу;
- формируют ответ-подтверждение с конкретным номером;
- определяют по номеру виртуального канала выходной порт, извлекают из кадра пакет X.25, а затем формируют новый кадр для дальнейшего продвижения пакета.

Наличие этих функций обуславливает сравнительно невысокую производительность коммутаторов X.25, которая составляет несколько тысяч пакетов в секунду.

Протоколы сетей X.25 были разработаны для низкоскоростных каналов связи с высоким уровнем помех и не гарантируют требуемой пропускной способности, но могут устанавливать приоритет трафика отдельных виртуальных каналов, который указывается в запросе на установление соединения в поле услуг.

### 4.3.3. Сети Frame Relay

#### 4.3.3.1. Особенности технологии Frame Relay

Frame Relay – сети, которые по сравнению с сетями X.25 гораздо лучше подходят для передачи пульсирующего трафика локальных сетей в тех случаях, когда каналы связи приближаются по качеству к каналам локальных сетей, например при использовании волоконно-оптических кабелей.

Рассмотрим кратко основные особенности технологии Frame Relay.

1. *Низкая протокольная избыточности и дейтаграммный режим работы* сетей Frame Relay обеспечивает высокую пропускную способность (до 2 Мбит/с) и небольшие задержки кадров. В то же время технология Frame Relay не обеспечивает надежную передачу кадров, возлагая эти функции на протоколы верхних уровней.

2. *Гарантированная поддержка основных показателей качества обслуживания* – средней скорости передачи данных по виртуальному каналу при допустимых пульсациях трафика – основная особенность, отличающая технологию Frame Relay от X.25.

3. Стандарты Frame Relay определяют два типа виртуальных каналов – постоянные (PVC) и коммутируемые (SVC).

4. Технология Frame Relay использует для передачи данных технику виртуальных соединений, аналогичную той, которая применяется в сетях X.25. Однако пользовательские данные (при установленном виртуальном соединении) в сетях Frame Relay передаются по протоколам только *физического и канального уровней*, в то время как в сетях X.25 после установления соединения данные передаются протоколом 3-го уровня.

5. По сравнению с технологией X.25 в сетях Frame Relay меньше *накладные расходы* при передаче данных, так как они вкладываются в кадры канального уровня, а не в пакеты сетевого уровня, как в сетях X.25.

6. Протокол канального уровня LAP-F в сетях Frame Relay, относящийся к семейству протоколов HDLC, имеет *два режима работы – основной (core) и управляющий (control)*. В основном режиме кадры передаются без преобразования и контроля, как и в коммутаторах локальных сетей. За счет этого сети Frame Relay обладают весьма высокой производительностью, так как кадры в коммутаторах не подвергаются преобразованию, а сеть не передает квитанции подтверждения между коммутаторами на каждый пользовательский кадр, как это происходит в сети X.25. Пульсирующий трафик передается в сети Frame Relay достаточно быстро и без больших задержек.

7. Технология Frame Relay, ориентированная на использование каналов связи высокого качества, не предусматривает выполнение функций по *обнаружению и коррекции искажённых кадров*. Эти функции возлагаются на конечные узлы, которые должны обнаруживать и корректировать ошибки с использованием протоколов транспортного или более высоких уровней. В этом отношении технология Frame Relay близка к технологиям локальных сетей, таким как Ethernet, Token Ring и FDDI, которые тоже только *отбрасывают искаженные кадры*, но сами не занимаются их повторной передачей.

Способность технологии Frame Relay *гарантировать некоторые параметры качества обслуживания* (QoS) является ключевой. Именно поэтому данная технология получила широкое распространение.

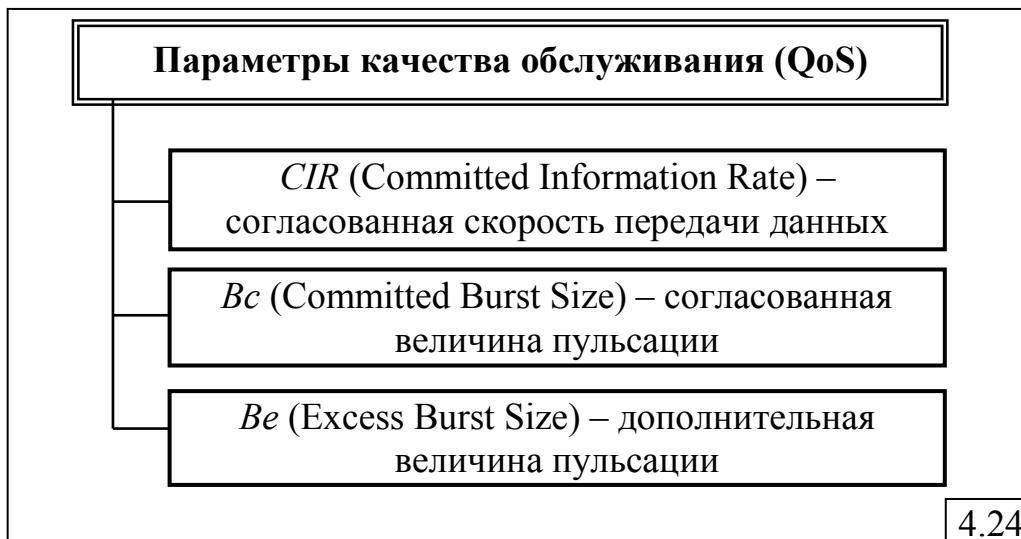
#### **4.3.3.2. Поддержка качества обслуживания**

Технология Frame Relay гарантированно обеспечивает выполнение основных параметров качества транспортного обслуживания, необходимых при объединении локальных сетей. Для этого при установлении соединения используется **процедура заказа качества обслуживания**, отсутствующая в сетях X.25 и заключающаяся в следующем.

Для каждого виртуального соединения определяются значения параметров, влияющих на качество обслуживания (рис.4.24):

- *CIR* (Committed Information Rate) – *согласованная информационная скорость*, с которой сеть будет передавать данные пользователя;

- $Bc$  (Committed Burst Size) – *согласованный объем пульсации*, то есть максимальное количество байтов, которое сеть будет передавать от этого пользователя за интервал времени  $T$ ;
- $Be$  (Excess Burst Size) – *дополнительный объем пульсации*, то есть максимальное количество байтов, которое сеть будет пытаться передать сверх установленного значения  $Bc$  за интервал времени  $T$ .



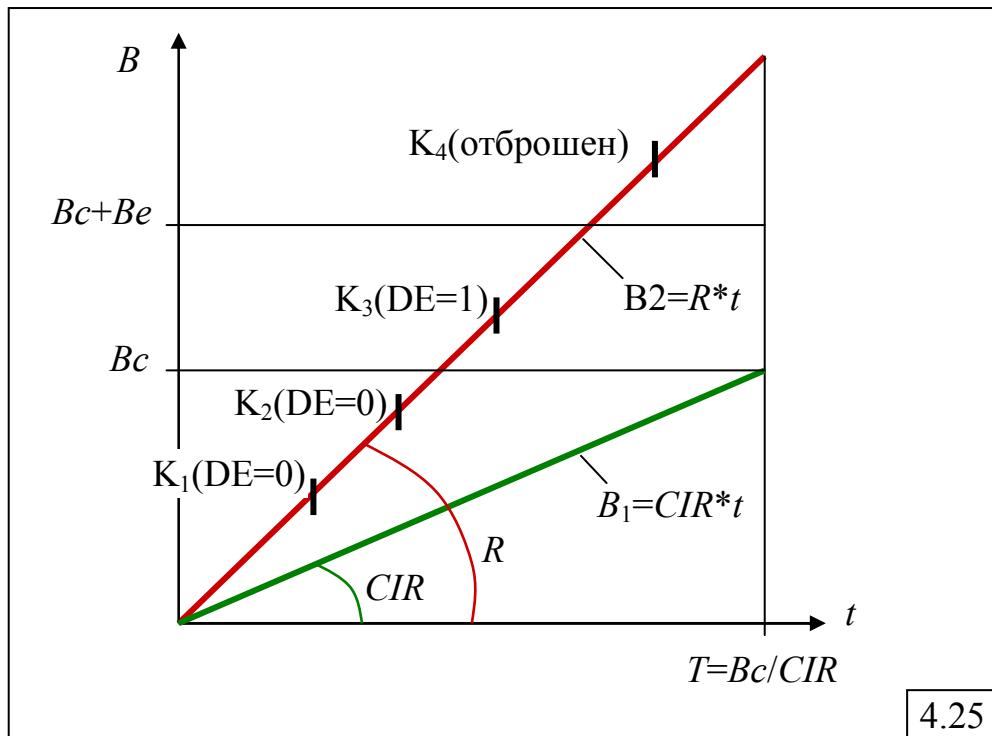
Гарантий по задержкам передачи кадров технология Frame Relay не дает, оставляя эту услугу сетям ATM.

Основным параметром, по которому абонент и сеть заключают соглашение при установлении виртуального соединения, является *согласованная скорость передачи данных*. Для постоянных виртуальных каналов это соглашение является частью контракта на пользование услугами сети. При установлении коммутируемого виртуального канала соглашение о качестве обслуживания заключается автоматически с помощью протокола Q.931/933 – требуемые параметры  $CIR$ ,  $Bc$  и  $Be$  передаются в пакете запроса на установление соединения.

Так как скорость передачи данных можно измерить только на каком-то интервале времени, то в качестве такого контрольного интервала, на котором проверяются условия соглашения, выбирается время  $T$ , значение которого определяется следующим образом:  $T = Bc / CIR$  (рис.4.25).

Пользователь в соответствии с соглашением должен передавать в сеть данные со средней скоростью, равной  $CIR$  (прямая  $B_1 = CIR * t$  на рис.4.25). Если же он нарушает соглашение и передаёт данные со средней скоростью  $R$  (прямая  $B_2 = R * t$  на рис.4.25), то сеть не гарантирует доставку кадра. При этом, до тех пор, пока объём переданных данных не превышает  $Bc$  кадры имеют специальный признак DE (Discard Eligibility), равный 0 (кадры  $K_1$  и  $K_2$ ). Если же объём переданных данных превысил  $Bc$ , то все последующие кадры помечаются признаком DE, равным 1 (кадр  $K_3$ ). Кадры, отмеченные таким признаком, подлежат удалению, однако они удаляются из сети только в том случае, если коммутаторы будут

перегружены. Если же перегрузок нет, то кадры с признаком DE=1 доставляются адресату.



Такое поведение сети соответствует случаю, когда общий объём данных, переданных пользователем в сеть за период  $T$ , не превышает ( $B_c + Be$ ). Если же этот порог превышен, то кадр не помечается признаком DE, а немедленно удаляется из сети (кадр  $K_4$ ).

Для контроля соглашения о параметрах качества обслуживания все коммутаторы сети Frame Relay выполняют так называемый алгоритм «дырявого ведра» (Leaky Bucket). Алгоритм использует *счетчик* поступивших от пользователя байт. Каждые  $T$  секунд значение счетчика уменьшается на величину  $B_c$  или же сбрасывается в 0, если значение счетчика меньше, чем  $B_c$ . Все кадры, данные которых не увеличили значение счетчика выше порога  $B_c$ , пропускаются в сеть со значением признака DE=0. Кадры, которые увеличили значение счетчика выше  $B_c$ , но меньше ( $B_c + Be$ ), также передаются в сеть, но с признаком DE=1. И наконец, кадры, которые увеличили значение счетчика выше ( $B_c + Be$ ), отбрасываются коммутатором.

Пользователь может включить в соглашение не все параметры качества обслуживания, а только некоторые. Например, использование параметров  $CIR$  и  $B_c$  обеспечивает более качественное обслуживание, так как кадры никогда не отбрасываются коммутатором сразу. Коммутатор только помечает признаком DE=1 кадры, которые превышают порог  $B_c$  за время  $T$ . Если в сети не возникают перегрузки, то кадры такого канала всегда дойдут до конечного узла, даже если пользователь нарушает соглашение с сетью.

Механизм заказа средней пропускной способности и максимальной пульсации является основным механизмом управления потоками кадров в

сетях Frame Relay. Соглашения должны заключаться таким образом, чтобы сумма средних скоростей виртуальных каналов не превосходила возможностей портов коммутаторов. При заказе постоянных каналов за это отвечает администратор, а при установлении коммутируемых виртуальных каналов – программное обеспечение коммутаторов. При правильно взятых на себя обязательствах сеть борется с перегрузками путем удаления кадров с признаком DE=1 и кадров, превысивших порог ( $Bc+Be$ ).

Кроме этого, в технологии Frame Relay определен ещё и дополнительный (необязательный) механизм управления кадрами. Это механизм оповещения конечных пользователей о перегрузках в коммутаторах сети.

При создании коммутируемого виртуального канала параметры качества обслуживания передаются в сеть с помощью протокола Q.931. Этот протокол устанавливает виртуальное соединение с помощью нескольких служебных пакетов.

#### **4.3.3.3. Использование сетей *Frame Relay***

Услуги Frame Relay и X.25 обычно предоставляются одними и теми же операторами, а производители выпускают коммутаторы, которые могут работать как по протоколам X.25, так и по протоколам Frame Relay.

Технология Frame Relay в территориальных сетях с коммутацией пакетов можно рассматривать как аналог технологии Ethernet в локальных сетях. Обе технологии:

- предоставляют быстрые базовые транспортные услуги, доставляя кадры без гарантий в узел назначения дейтаграммным способом;
- если кадры теряются, то не предпринимаются никакие усилия для их восстановления.

Отсюда вывод – полезная пропускная способность при работе через сети Frame Relay зависит от качества каналов и методов восстановления пакетов на уровнях стека протоколов, расположенного над протоколом Frame Relay. Если каналы качественные, то кадры будут теряться и искажаться редко, так что скорость восстановления пакетов протоколами транспортного уровня будет вполне приемлема. Если же кадры искажаются и теряются часто, то полезная пропускная способность в сети Frame Relay может упасть в десятки раз, как это происходит в сетях Ethernet при плохом состоянии кабельной системы. Поэтому сети Frame Relay следует применять при наличии на магистральных каналах волоконно-оптических кабелей высокого качества. Каналы доступа могут быть и на витой паре, при условии обеспечения приемлемого уровня искажения данных.

Отсутствие гарантий на задержку передачи кадров в сетях Frame Relay и сравнительно небольшая скорость передачи данных в 2 Мбит/с ограничивают их применение для передачи голоса и практически делают невозможным передачу видео.

Для передачи голоса в сетях Frame Relay используется приоритизация трафика, заключающаяся в присвоении кадрам, переносящим замеры голоса, *приоритетов*. Магистральные коммутаторы Frame Relay такие кадры обрабатывают в первую очередь.

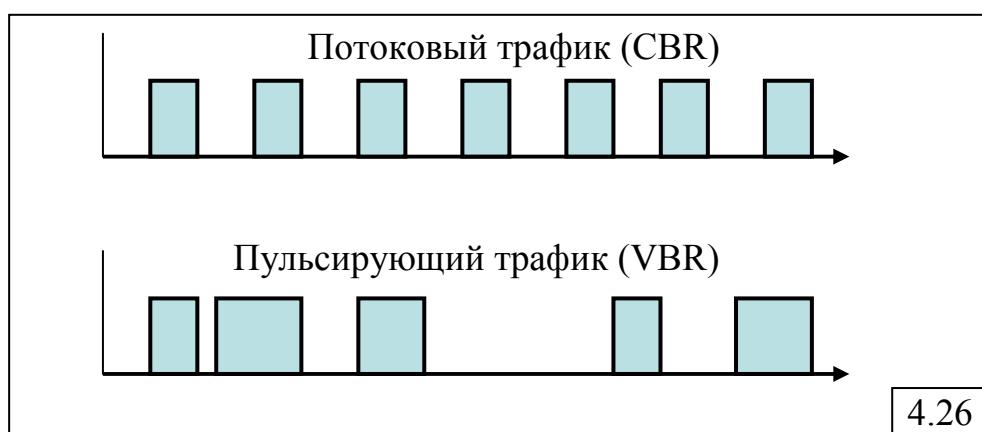
#### 4.3.4. Технология ATM

**ATM** (Asynchronous Transfer Mode) - технология *асинхронного режима передачи*, использующая маленькие пакеты фиксированного размера, называемые *ячейками* (cells), предназначенная для передачи в сети *различных видов трафика* – голос, видео и данные, обеспечивая при этом достаточную пропускную способность для каждого из них и гарантируя своевременную доставку восприимчивых к задержкам данных. Технология ATM может использоваться как для построения высокоскоростных локальных сетей, так и магистралей, объединяющих традиционные локальные сети.

ATM разрабатывалась как альтернатива *синхронной передаче* STM (Synchronous Transfer Mode), в основе которой лежит технология TDM. Главный недостаток технологии TDM заключается в невозможности перераспределять пропускную способность объединенного канала между подканалами (временными слотами), которые предоставляются пользователям для передачи данных. Если временной слот не используется пользователем и подканал свободен, его ресурсы не могут быть переданы другому пользователю, что приводит к потере пропускной способности канала и, как следствие, к снижению реальной скорости передачи данных. В технологии ATM ячейки не привязаны к временным слотам, а их идентификация на приёмной стороне осуществляется не по номеру слота, а по идентификатору виртуального соединения.

Трафик современных компьютерных сетей можно разбить на два больших класса:

- потоковый (stream), представляющий собой равномерный поток данных (рис.4.26,а) с постоянной битовой скоростью (CBR – Constant Bit Rate);
- пульсирующий (burst), представляющий собой неравномерный непредсказуемый поток данных (рис.4.26,б) с переменной битовой скоростью (VBR – Variable Bit Rate).



Потоковый трафик характерен для аудио и видео данных, для которых основной характеристикой качества обслуживания является задержка передачи данных. Пульсирующий трафик формируется приложениями, связанными, например, с передачей файлов и при работе пользователей в режиме «запрос-ответ». Пульсирующий трафик обычно нечувствителен к задержкам, но чувствителен к потерям и искажениям передаваемых пакетов.

Технология ATM разрабатывалась как технология, способная обслуживать все виды трафика в соответствии с их требованиями за счёт использования:

- техники виртуальных каналов;
- предварительного заказа параметров качества обслуживания;
- приоритезации трафика.

Стандарты определяют ATM как *интерфейс и протокол*, которые разработаны для коммутации трафика через общую *высокоскоростную* среду с постоянной или переменной битовой скоростью.

#### **4.3.4.1. Общие принципы технологии ATM**

Подход, реализованный в технологии ATM, состоит в передаче любого вида трафика – компьютерного или мультимедийного – пакетами фиксированной длины в 53 байта, называемыми ячейками (cell). Поле данных ячейки занимает 48 байт, а заголовок – 5 байт.

Размер ячеек выбирался исходя из двух противоречивых условий:

- с одной стороны, размер ячейки должен быть достаточно мал, чтобы сократить время задержки в узлах сети;
- с другой стороны, размер ячейки должен быть достаточно велик, чтобы минимизировать потери пропускной способности, обусловленные накладными расходами на передачу заголовка ячейки.

Преимущества ячеек перед кадрами локальных сетей подробно рассмотрены в п.1.5.1.4.

Для уменьшения доли служебной информации в ячейке в технологии ATM применен стандартный для территориально-распределенных вычислительных сетей прием – передача ячеек в соответствии с *техникой виртуальных каналов* с длиной номера виртуального соединения в 24 бит, что вполне достаточно для обслуживания большого количества виртуальных соединений каждым портом коммутатора сети ATM.

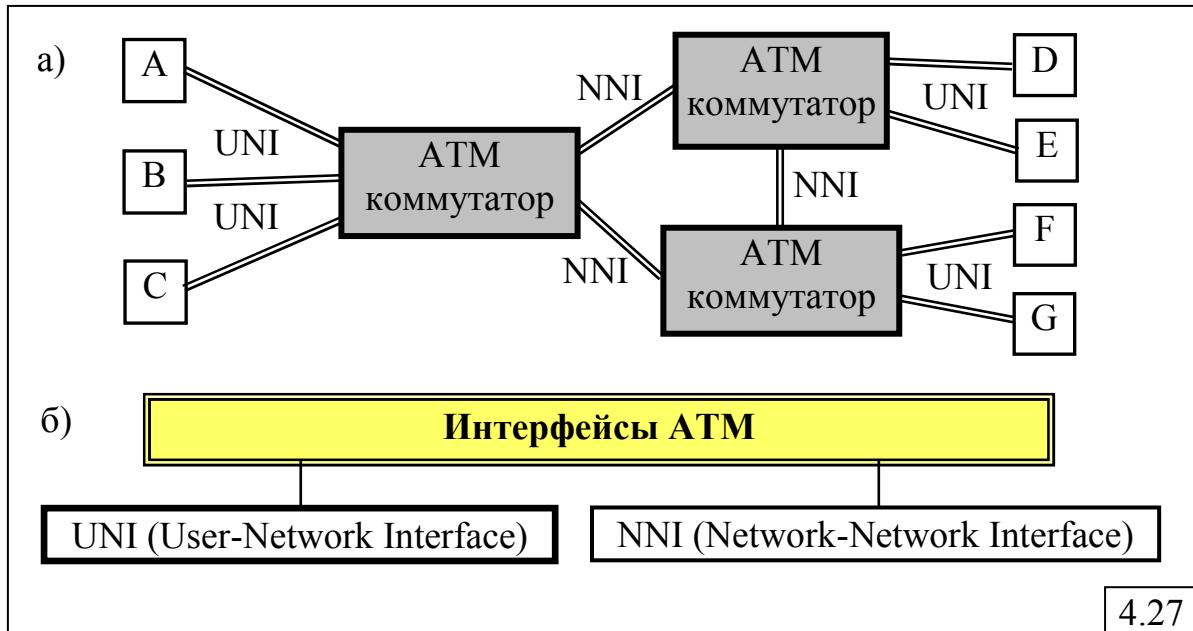
Сеть ATM имеет классическую структуру территориальной сети (рис.4.27,а) – конечные станции А, В, ..., Г соединяются индивидуальными каналами с коммутаторами, которые в свою очередь могут соединяться с другими коммутаторами. Соответственно в стандарте определены 2 типа интерфейса (рис.4.27,б):

- пользователь – сеть (User-Network Interface, UNI);
- сеть – сеть (Network-Network Interface, NNI).

Спецификация UNI определяет:

- структуру пакета,

- адресацию станций,
- обмен управляющей информацией,
- уровни протокола ATM,
- способы установления виртуального канала,
- способы управления трафиком.



Коммутация пакетов происходит на основе *идентификатора виртуального канала* (Virtual Channel Identifier, VCI), который назначается соединению при его установлении и уничтожается при разрыве соединения.

Виртуальные каналы могут быть *постоянными* (PVC) и *коммутируемыми* (SVC). Для ускорения коммутации в больших сетях используется понятие *виртуального пути* (Virtual Path), который объединяет виртуальные каналы, имеющие в сети ATM общий маршрут между исходным и конечным узлами или общую часть маршрута между двумя коммутаторами сети. *Идентификатор виртуального пути* (Virtual Path Identifier, VPI) является старшей частью локального адреса и представляет собой общий префикс для некоторого количества различных виртуальных каналов. Таким образом, адресация в технологии ATM реализована на двух уровнях:

- на уровне адресов конечных узлов (на этапе установления виртуального канала);
- на уровне номеров виртуальных каналов (при передаче данных по сформированному виртуальному каналу).

Стандарт ATM не вводит свои спецификации на реализацию физического уровня и основывается на технологии SDH/SONET, принимая её иерархию скоростей. Организация ATM Forum определила для ATM не все иерархии скоростей SDH, а только скорости OC-3 (155 Мбит/с) с использованием волоконно-оптического кабеля или неэкранированной

витой пары категории 5 и ОС-12 (622 Мбит/с) с использованием только волоконно-оптического кабеля.

Имеются и другие физические интерфейсы сетей ATM, отличные от SDH/SONET:

- интерфейсы Т1/E1 и Т3/E3, используемые в глобальных сетях;
- интерфейсы локальных сетей со скоростью 100 Мбит/с (FDDI) и 25 Мбит/с.

Для решения задачи совмещения разнородного трафика в одной сети в технологии ATM реализован принцип *заказа пропускной способности и качества обслуживания*, как в технологии Frame Relay.

#### **4.3.4.2. Стек протоколов ATM**

Стек протоколов ATM показан на рис.4.28, а распределение протоколов по конечным узлам и коммутаторам ATM – на рис.4.29.

Верхние уровни		
Уровни адаптации ATM (AAL1-5)	Подуровень конвергенции	Общая часть подуровня конвергенции
		Специфическая для сервиса часть
	Подуровень сегментации и реассемблирования	
Уровень ATM	(маршрутизация, мультиплексирование, управление потоком, обработка приоритетов)	
Физический уровень	Подуровень согласования передачи	
	Подуровень, зависящий от физической среды	

4.28

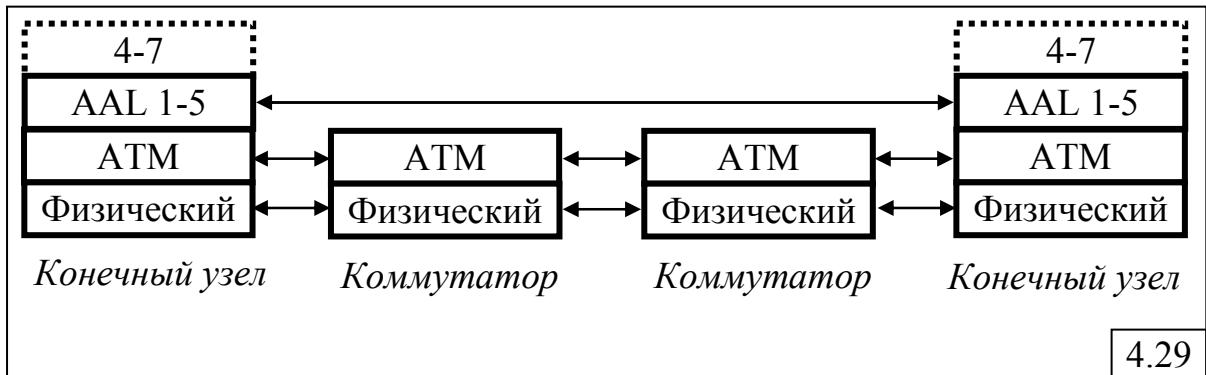
Стек протоколов ATM соответствует нижним уровням семиуровневой модели ISO/OSI и включает:

- уровень адаптации ATM,
- собственно уровень ATM;
- физический уровень.

Прямого соответствия между уровнями протоколов технологии ATM и уровнями модели OSI нет.

**Уровень адаптации (ATM Adaptation Layer, AAL)** представляет собой набор протоколов, которые преобразуют блоки данных протоколов верхних уровней сети ATM в ячейки ATM нужного формата. Функции этих уровней достаточно условно соответствуют функциям транспортного уровня модели OSI, например функциям протоколов TCP или UDP. Протоколы AAL при передаче пользовательского трафика работают только

в конечных узлах сети (см. рис.4.29), как и транспортные протоколы большинства технологий.



**Уровень ATM** занимает в стеке протоколов ATM примерно то же место, что протокол IP в стеке TCP/IP или протокол LAP-F в стеке протоколов технологии Frame Relay. Протокол ATM занимается передачей ячеек через коммутаторы при установленном и настроенном виртуальном соединении, то есть на основании готовых таблиц коммутации портов. Протокол ATM выполняет коммутацию по номеру виртуального соединения, который в технологии ATM разбит на две части – *идентификатор виртуального пути* (*Virtual Path Identifier, VPI*) и *идентификатор виртуального канала* (*Virtual Channel Identifier, VCI*). Кроме этой основной задачи протокол ATM выполняет ряд функций по контролю за соблюдением трафик-контракта со стороны пользователя сети, маркировке ячеек-нарушителей, отбрасыванию ячеек-нарушителей при перегрузке сети, а также управлению потоком ячеек для повышения производительности сети.

#### 4.3.4.3. Формат ATM-ячейки

Протокол ATM работает с ячейками следующего формата, представленного на рис.4.30.

Поле **Управление потоком** (*Generic Flow Control*) используется только в UNI при взаимодействии конечного узла и первого коммутатора сети для управления трафиком и предотвращения перегрузки. Для NNI это поле не определено, а его биты используются для расширения поля идентификатора виртуального пути (VPI).

Поля **Идентификатор виртуального пути** (*VirtualPath Identifier, VPI*) и **Идентификатор виртуального канала** (*Virtual Channel Identifier, VCI*) занимают соответственно 8 и 16 бит. Эти поля задают **номер виртуального соединения**, разделенный на старшую (VPI) и младшую (VCI) части.

Поле **Тип полезной нагрузки** (*Payload Type Identifier, PTI*) состоит из 3-х бит и задает тип полезной нагрузки, переносимой ячейкой – пользовательские данные или управляющая информация (например, для установления виртуального соединения). Кроме того, один бит этого поля используется для указания перегрузки в сети.

Заголовок ячейки (5 байт)	Биты								Байты			
	8	7	6	5	4	3	2	1				
Управление потоком (GFC)	<b>Идентификатор виртуального пути (VPI)</b>								1			
<b>Идентификатор виртуального пути (VPI)</b>	<i>Идентификатор виртуального канала (VCI)</i>								2			
<i>Идентификатор виртуального канала (VCI)</i>									3			
<i>Идентификатор виртуального канала (VCI)</i>	Тип полезной нагрузки (PTI)			<b>ППЯ</b>								
Управление ошибками в заголовке (HEC)									4			
Данные пакета									5			
									6			
									...			
									53			
									4.30			

В однобитовом поле **ППЯ** – *Приоритет Потери Ячейки (Cell Loss Priority, CLP)* коммутаторы ATM отмечают ячейки, которые нарушают соглашения о параметрах качества обслуживания, чтобы удалить их при перегрузках сети: ячейки с  $CLP=0$  являются высокоприоритетными, а ячейки с  $CLP=1$  – низкоприоритетными и могут быть удалены при перегрузках.

Поле **Управление ошибками в заголовке (Header Error Control, HEC)** содержит контрольную сумму, вычисленную для заголовка ячейки.

#### 4.3.4.4. Принцип работы коммутаторов ATM

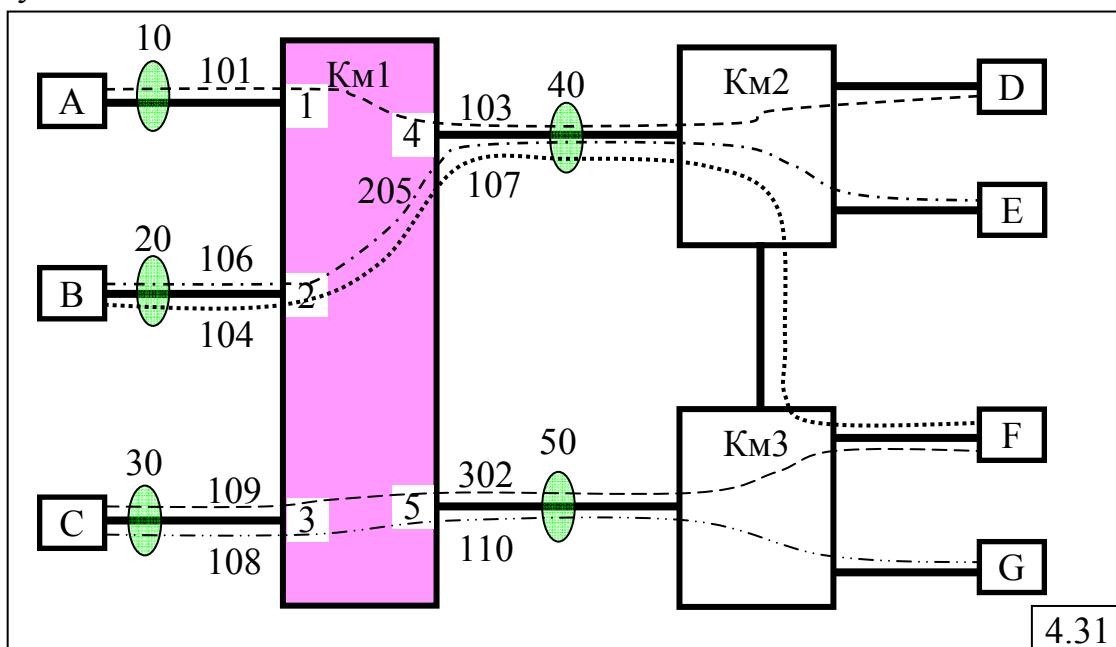
Проиллюстрируем принцип работы коммутаторов ATM на примере ATM-сети, представленной на рис.4.27,а). Для простоты положим, что узлы А, В, ... представляют собой оконечные коммутаторы, к которым подключены соответствующие пользователи (абоненты) сети. Это означает, что между узлами А, В, ... и коммутаторами Км1, Км2 и Км3 данные передаются в виде ячеек.

Положим, что в процессе установления соединения, сформированы виртуальные соединения, показанные на рис.4.31 и построена таблица коммутации для коммутатора Км1, представленная на рис.4.32.

Как видно из таблицы, сформировано 5 виртуальных соединений (каналов) между абонентами сети: А – D, В – E, В – F, С – F и С – G.

Рассмотрим процесс прохождения через Км1 ячейки от абонента А, в заголовке которой в момент её поступления в порт 1 коммутатора в качестве идентификаторов виртуального пути и виртуального канала будут находиться значения VPI=10 и VCI=101 (рис.4.31). В соответствии с

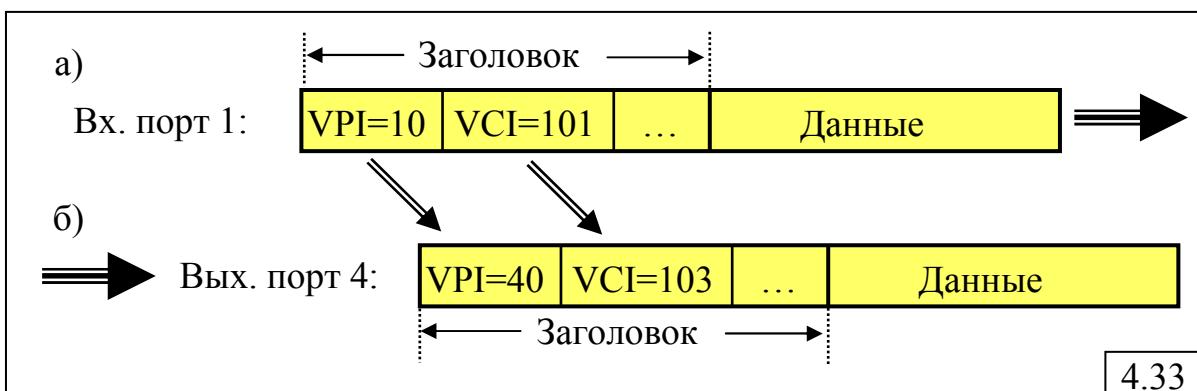
записью в первой строке таблицы коммутации, поступившая на 1-й порт ячейка с VPI=10 и VCI=101 должна быть направлена в 4-й порт коммутатора, причём в заголовке ячейки идентификаторы виртуального пути и виртуального канала должны быть заменены на значения VPI=40 и VCI=103 (рис.4.33). Аналогично, ячейка, поступившая на 2-й порт с VPI=20 и VCI=104 будет направлена в 4-й порт коммутатора, причём в заголовке идентификаторы виртуального пути и виртуального канала будут заменены на значения VPI=40 и VCI=107.



**Таблица коммутации коммутатора Км1**

<i>Вход</i>			<i>Выход</i>		
Порт	VPI	VCI	Порт	VPI	VCI
1	10	101	4	40	103
4	40	205	2	20	106
2	20	104	4	40	107
3	30	108	5	50	110
3	50	302	3	30	109

4.32



#### 4.3.4.5. Обеспечение качества обслуживания

Качество обслуживания (QoS) в ATM-сетях задаётся следующими параметрами трафика виртуального соединения:

- пиковая скорость передачи ячеек (Peak Cell Rate, PCR);
- средняя скорость передачи ячеек (Sustained Cell Rate, SCR);
- минимальная скорость передачи ячеек (Minimum Cell Rate, MCR);
- максимальная величина пульсаций (Maximum Burst Size, MBS);
- доля потерянных ячеек (Cell Loss Ratio, CLR);
- задержка ячеек (Cell Transfer Delay, CTD);
- вариация задержек ячеек (Cell Delay Variation, CDV).

В зависимости от требований, предъявляемых к качеству передачи данных, в ATM-сетях различают 5 классов трафика, отличающихся:

- скоростью передачи;
- чувствительностью к задержкам;
- способом установления соединения;
- совокупностью параметров QoS, характерных для данного класса.

В табл.4.2 представлена классификация классов трафика в соответствии с указанными признаками и приведены примеры трафика каждого класса. Здесь же представлен тип протокола (AAL1-AAL5) уровня адаптации ATM (AAL), который обеспечивает реализацию заданных требований.

Таблица 4.2

Класс	A	B	C	D	X
Скорость	Постоянная		Переменная		
К задержке	Чувствительны		Не чувствительны		
Соединение		С установлением		Без установления	
Примеры трафика	Голос, ТВ	Компрессирован. голос, ТВ	Компьютерные данные	Трафик компьютерных сетей	
Параметры QoS	PCR, CTD, CDV	PCR, SCR, MBS, CTD, CDV	PCR, SCR, MBS	Не определены	Определяются пользователем
AAL	AAL1	AAL2	AAL5	AAL3/4	

В представленной классификации предусмотрен дополнительный класс трафика, отличающийся от классов A, B, C и D, параметры которого могут быть определены пользователем.

#### **4.3.4.6. Использование технологии ATM**

Основной соперник технологии ATM в локальных сетях – гигабитные технологии Ethernet. Там, где необходима высокоскоростная магистраль и не требуется поддержка QoS разных типов трафика, целесообразно использовать технологию Gigabit Ethernet. Технология ATM может оказаться предпочтительней там, где важно обеспечить заданное качество обслуживания (видеоконференции, трансляция телевизионных передач и т. п.).

В территориально-распределенных сетях ATM применяется там, где сеть Frame Relay не справляется с большими объемами трафика, и там, где нужно обеспечить низкий уровень задержек, необходимый для передачи информации реального времени.

### **4.4. Глобальная сеть Internet**

Глобальная сеть Internet реализована на основе стека сетевых протоколов TCP/IP, обеспечивающих передачу данных между разнородными локальными и территориальными сетями, а также коммуникационными системами и устройствами.

#### **4.4.1. Краткая история создания и организационные структуры Internet**

Появлению сети Internet и стека протоколов TCP/IP предшествовала в середине 1960-х годов разработка под эгидой агентства DARPA (Defence Advanced Research Projects Agency – Управление перспективных исследований Министерства обороны США) сети, получившей название ARPANET (Advanced Research Projects Agency NETwork). Разработка сети была поручена Стэнфордскому исследовательскому институту и трём американским университетам: Калифорнийскому в Лос-Анжелесе и Университетам штата Юта и штата Калифорния в Санта-Барбаре. Экспериментальная сеть из четырёх узлов была запущена в конце 1969 года, а к концу 1972 года в сети насчитывалось более 30 узлов.

В 1974 году были разработаны модели и протоколы TCP/IP для управления обменом данными в интерсетях, а 1 января 1983 года сеть ARPANET полностью перешла на протокол TCP/IP.

В конце 1970-х годов Национальный научный фонд США (National Science Foundation, NSF) начал разработку межуниверситетской сети, получившей название NSFNet, которая имела гораздо большую пропускную способность, чем ARPANET. В середине 1980-х годов произошло объединение сетей NSFNet и ARPANET, за которым закрепилось название INTRNET (Интернет).

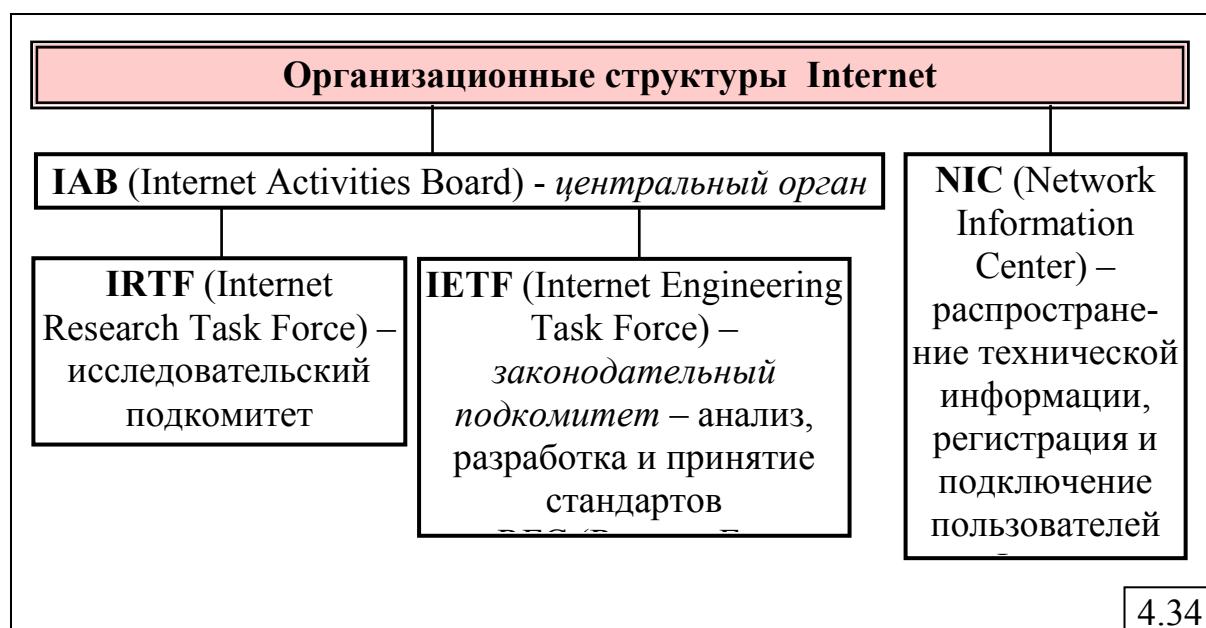
В 1984 году была разработана система доменных имён (Domain Name System, DNS), а в 1989 году появилась концепция Всемирной паутины (World Wide Web, WWW) и были разработаны протокол передачи гипертекста HTTP (HyperText Transfer Protocol) и язык разметки гипертекста HTML (HyperText Markup Language).

Благодаря отсутствию единого руководства и открытости технических стандартов Интернет объединил большинство существующих сетей и к началу 21 века стал популярным средством для обмена данными.

В настоящее время подключиться к Интернету можно через спутники связи, радио-каналы, кабельное телевидение, телефон, сотовую связь, специальные оптико-волоконные линии или электропровода.

Координация разработок и поддержка Интернета осуществляется следующими **организационными структурами** (рис.4.34):

- Internet Activities Board (IAB) – центральный орган, включающий два подкомитета:
  - исследовательский – IRTF (Internet Research Task Force);
  - законодательный – IETF (Internet Engineering Task Force), выполняющий функцию анализа, разработки и принятия стандартов сети Internet, получивших название RFC (Request For Comments);
- Network Information Center (NIC) – орган, ответственный за распространение технической информации, работу по регистрации и подключению пользователей к Internet и за решение ряда административных задач, таких как распределение адресов в сети.



#### 4.4.2. Стек протоколов TCP/IP

Под **стеком (семейством) протоколов TCP/IP** в широком смысле обычно понимают весь набор реализаций стандартов RFC.

Соответствие уровней TCP/IP уровням OSI-модели и используемые на каждом уровне основные протоколы стека TCP/IP представлены в табл.4.3.

Модель стека протоколов TCP/IP содержит 4 уровня.

На первом уровне (**Network interface – сетевой интерфейс**) находится аппаратно зависимое программное обеспечение, реализующее передачу данных в той или иной среде. Среда передачи данных может

быть реализована различными способами: от простого двухточечного звена до сложной многоузловой коммуникационной структуры сети X.25 или Frame Relay. Стек протоколов TCP/IP поддерживает все стандартные протоколы физического и канального уровней различных сетевых технологий: Ethernet, Token Ring, FDDI, PPP и другие.

Таблица 4.3

Уровни OSI-модели	Уровни TCP/IP	Протокол	Блок данных
5-7	<b>4. Application (прикладной)</b>	FTP, TFTP, BGP, HTTP, DHCP, SNMP, DNS, SIP, SMTP, POP3, IMAP, Telnet, PPTP	Сообщение
4	<b>3. Transport (транспортный)</b>	TCP, UDP, RTP	Сегмент, Дейтаграмма
3	<b>2. Internet (межсетевой)</b>	IPv4, IPv6, ICMP, IGMP, ARP, RARP, RIP, OSPF	Пакет
1-2	<b>1. Network interface (сетевой интерфейс)</b>	SLIP, HDLC, PPP Ethernet, 802.11 Wi-Fi, 802.16 WiMax, Token ring, FDDI, X.25, Frame relay, ATM	Кадр

На втором уровне (**Internet** – межсетевой) реализуется задача маршрутизации с использованием протокола IP. Вторая важная задача протокола IP – скрытие аппаратно-программных особенностей среды передачи данных и предоставление вышеперечисленным уровням единого унифицированного и аппаратно независимого интерфейса для доставки данных, что обеспечивает многоплатформенное применение приложений, работающих под TCP/IP.

На третьем уровне (**Transport** – транспортный) решаются задачи надежной доставки пакетов и сохранение их порядка и целостности.

На четвёртом уровне (**Application** – прикладной) находятся прикладные задачи, запрашивающие сервис у транспортного уровня.

Основными особенностями стека протоколов TCP/IP являются:

- независимость от среды передачи данных;
- негарантированная доставка пакетов.

Информационные объекты (данные) передаваемые на разных уровнях в сети Интернет получили следующие наименования:

- **сообщение (message)** – блок данных, которым оперирует прикладной уровень, передаваемый от приложения к транспортному уровню с соответствующими этому приложению размером и семантикой;
- **сегмент (segment)** – блок данных, которым оперирует протокол TCP на транспортном уровне;
- **дейтаграмма (datagram)** – блок данных, которым оперирует протокол UDP на транспортном уровне;

- **пакет (packet)** – блок данных, называемый также IP-дейтаграммой, которым оперирует протокол IP на межсетевом уровне;
- **кадр (frame)** – аппаратно зависимые блоки данных, полученные в результате упаковки IP-дейтаграмм в формат, приемлемый для данной физической среды передачи данных и передаваемый на нижнем уровне TCP/IP-модели, называемом «сетевым интерфейсом».

Рассмотрим кратко перечисленные в табл.4.3 протоколы стека TCP/IP, некоторые из которых (IP, UDP, TCP, HDLC, PPP) более подробно рассматриваются в последующих параграфах.

#### 4.4.2.1. Протоколы прикладного уровня

**FTP** (File Transfer Protocol – протокол передачи файлов), предназначенный для передачи файлов в сети и доступа к удалённым хостам, реализует следующие функции:

- подключение к серверам FTP;
- просмотр содержимого каталогов;
- загрузка файлов с сервера или на сервер.

FTP функционирует поверх транспортного протокола TCP и использует порт 20/TCP для передачи данных и порт 21/TCP для передачи команд. В протоколе FTP предусмотрены возможности аутентификации и передачи файла с прерванного места, если передача файла была прервана по какой-то причине.

**TFTP** (Trivial File Transfer Protocol – простой протокол передачи файлов) предназначен главным образом для первоначальной загрузки бездисковых рабочих станций. TFTP использует транспортный протокол UDP и порт 69/UDP. В отличие от FTP, протокол TFTP не содержит возможностей аутентификации, хотя возможна фильтрация по IP-адресу.

**BGP** (Border Gateway Protocol – протокол граничного шлюза) – основной протокол динамической маршрутизации в Интернете, предназначенный для обмена информацией о маршрутах между автономными системами. Функционирует поверх протокола транспортного уровня TCP и использует порт 179/TCP.

**HTTP** (HyperText Transfer Protocol – протокол передачи гипертекста) предназначен для передачи данных (изначально – в виде гипертекстовых документов) на основе клиент-серверной технологии. HTTP в настоящее время используется во Всемирной паутине для получения информации с веб-сайтов.

**DHCP** (Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) предназначен для автоматического распределения между компьютерами IP-адресов и конфигурационных параметров, необходимых для работы в сети TCP/IP. Протокол реализуется в так называемом DHCP-сервере по клиент-серверной технологии путём выдачи IP-адреса и конфигурационных параметров в ответ на поступивший запрос от компьютера. Протокол DHCP использует транспортный протокол UDP и порты 67/UDP и 68/UDP.

**SNMP** (Simple Network Management Protocol – протокол простого управления сетями) предназначен для управления и контроля за сетевыми устройствами и приложениями в сети передачи данных путём обмена управляющей информацией. Протокол SNMP встроен во все сетевые ОС и использует транспортный протокол UDP и порты 161/UDP и 162/UDP.

**DNS** (Domain Name System – система доменных имён) представляет собой компьютерную распределённую иерархическую систему для получения информации о доменах, чаще всего для получения IP-адреса по символьному имени хоста (компьютера или устройства). Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по одноимённому протоколу. Протокол DNS встроен во все сетевые ОС и использует транспортные протоколы TCP и UDP и, соответственно, порты 53/TCP и 53/UDP.

**SIP** (Session Initiation Protocol) – протокол установления сеанса, предназначенный для установления и завершения пользовательского интернет-сеанса, включающего обмен мультимедийным содержимым (видео- и аудиоконференции, онлайн-игры).

**SMTP** (Simple Mail Transfer Protocol) – простой протокол передачи почты, предназначенный для передачи электронной почты в сетях TCP/IP.

**POP3** (Post Office Protocol Version 3) – протокол почтового отделения, версия 3, обычно используемый почтовым клиентом в паре с протоколом SMTP для получения сообщений электронной почты с сервера. Протокол POP3 использует транспортный протокол TCP и порт 110/TCP. Альтернативным протоколом для сбора сообщений с почтового сервера является протокол IMAP.

**IMAP** (Internet Message Access Protocol) – протокол доступа к электронной почте Интернета, как и POP3, служит для работы со входящими письмами, однако обеспечивает ряд дополнительных функций, предоставляя пользователю доступ к хранилищу электронных писем на сервере так, как будто эти письма находятся на его компьютере. POP3 использует транспортный протокол TCP и порт 143/TCP. Для отправки писем используется протокол SMTP.

**TELNET** (TELeType NETwork) – виртуальный текстовый терминал, предназначенный для реализации текстового интерфейса в сети с использованием транспортного протокола TCP (стандартный порт 23/TCP).

**PPTP** (Point-to-point tunneling protocol) – туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в незащищённой сети. PPTP инкапсулирует кадры PPP в IP-пакеты для передачи через Интернет и может использоваться для организации туннеля между локальными сетями. PPTP использует TCP-соединение для обслуживания туннеля.

#### 4.4.2.2. Протоколы транспортного уровня

**TCP** (Transmission Control Protocol) – протокол управления передачей данных с установлением соединения, реализующий обмен данными между двумя узлами на основе некоторого соглашения об управлении потоком данных.

**UDP** (User Datagram Protocol) – дейтаграммный протокол передачи данных в виде независимых единиц – дейтаграмм (datagram).

**RTP** (Real-time Transport Protocol) предназначен для передачи трафика реального времени. Заголовок RTP-пакета содержит данные, необходимые для восстановления голоса или видеоизображения в приёмном узле, о типе кодирования информации (JPEG, MPEG и т. п.) а также временную метку и номер пакета. Эти параметры позволяют при минимальных задержках определить порядок и момент декодирования каждого пакета, а также интерполировать потерянные пакеты. В качестве нижележащего протокола транспортного уровня, как правило, используется протокол UDP.

#### 4.4.2.3. Протоколы межсетевого уровня

**IP** (Internet Protocol) - основной протокол стека TCP/IP, реализующий передачу пакетов по IP-сети от узла к узлу. Протокол IP:

а) не гарантирует:

- доставку пакетов,
- целостность пакетов,
- сохранение порядка потока пакетов;

б) не различает логические объекты (процессы), порождающие поток данных.

Эти задачи решают протоколы *транспортного уровня* TCP и UDP, реализующие различные режимы доставки данных. В отличие от IP протоколы транспортного уровня различают приложения и передают данные от приложения к приложению.

В настоящее время на смену протоколу IP версии 4 (IPv4) приходит протокол версии 6 (IPv6).

**ICMP** (Internet Control Message Protocol) – межсетевой протокол управляющих сообщений, используемый в основном для передачи сообщений об ошибках и исключительных ситуациях, возникших при передаче данных, а также выполняющий некоторые сервисные функции.

ICMP-сообщения генерируются при нахождении ошибок в заголовке IP пакета, при отсутствии маршрута к адресату, а также используются маршрутизаторами для обновления записей в таблице маршрутизации отправителя и для управления скоростью отправки сообщений отправителем. ICMP-сообщения инкапсулируются в IP пакеты.

ICMP является неотъемлемой частью IP, но при этом не делает протокол IP средством надёжной доставки сообщений. Для этих целей существует протокол TCP.

**IGMP** (Internet Group Management Protocol) – протокол управления группами Интернета, предназначенный для управления групповой (multicast) передачей данных в IP-сетях версии 4 (IPv4). IGMP используется маршрутизаторами и IP-узлами для организации групп сетевых устройств, а также для поддержки потокового видео и онлайн-игр, обеспечивая эффективное использование сетевых ресурсов.

**ARP** (Address Resolution Protocol – Протокол разрешения адресов) предназначен для определения физического адреса устройства (MAC-адреса) по его IP-адресу.

**RARP** (Reverse Address Resolution Protocol – Протокол обратного определения адреса) предназначен для определения IP-адреса устройства по его физическому адресу (MAC-адресу).

**RIP** (Routing Information Protocol) – протокол маршрутизации типа DVA, реализующий алгоритм обмена информацией о доступных сетях и расстояниях до них путём *периодической* рассылки широковещательных пакетов.

**OSPF** (Open Shortest Path First) – протокол маршрутизации типа LSA, реализующий алгоритм обмена информацией о состоянии каналов, путём периодического тестирования состояния каналов с соседними маршрутизаторами. Протокол OSPF разработанный для применения в сети Интернет и используется в других больших сетях (NetWare, SNA, XNS, DECNet).

#### **4.4.2.4. Протоколы канального уровня («сетевой интерфейс»)**

**SLIP** (Serial Line IP) – первый стандарт канального уровня для выделенных линий, разработанный специально для стека протоколов TCP/IP, который благодаря простоте может использоваться как для коммутируемых, так и для выделенных каналов. SLIP поддерживается только протоколом сетевого уровня IP.

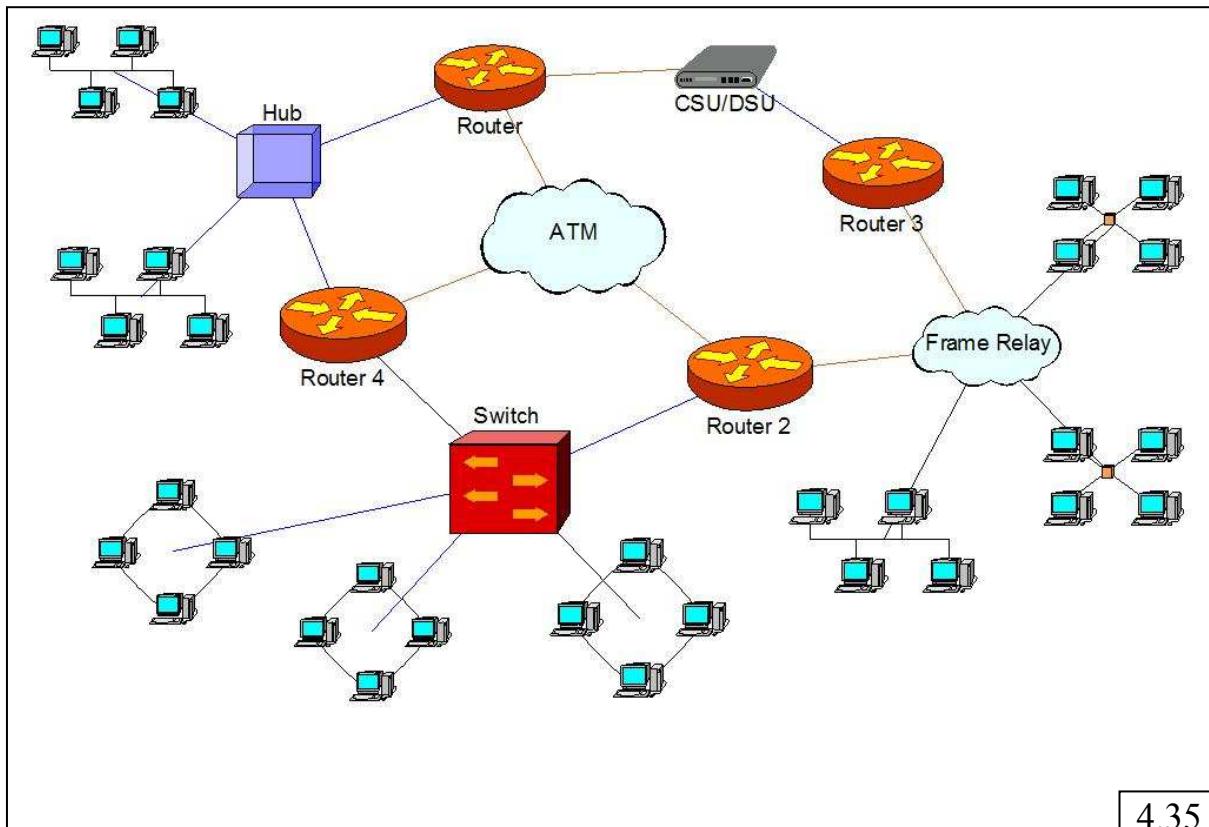
**HDLC** (High-level Data Link Control Procedure) – высокоуровневый протокол управления каналом – стандарт ISO для выделенных линий, представляющий собой семейство протоколов LAP (Link Access Protocol). HDLC относится к бит-ориентированным протоколам.

**PPP** (Point-to-Point Protocol) – протокол двухточечного соединения, пришедший на смену протоколу SLIP и построенный на основе формата кадров протоколов семейства HDLC с дополнением собственных полей. PPP является стандартным протоколом Интернета и так же, как протокол HDLC, представляет собой семейство протоколов.

### **4.4.3. Архитектурная концепция Internet**

Структура сети Internet может быть представлена как множество компьютеров, называемых *хостами*, подключенных к некоторой единой интерсети, представляющей собой совокупность физических сетей, называемых *подсетями*, соединенных маршрутизаторами (рис.4.35). В

качестве подсетей могут выступать локальные сети, работающие под управлением некоторых аппаратно зависимых протоколов (Ethernet, Token Ring), или коммуникационные системы произвольной физической природы (модемные коммутируемые или выделенные линии, сети X.25, Frame Relay, FDDI, ATM и др.). При этом все функции протокола IP выполняют хосты и маршрутизаторы, называемые узлами сети.



Основным протоколом стека TCP/IP является протокол IP, который обеспечивает:

- *негарантированную доставку* пакетов, т.к. передаваемые по сети пакеты могут быть утеряны, дублированы, задержаны, доставлены с нарушением порядка;
- *дейтаграммную доставку без установления соединения*, то есть каждый пакет представляет собой обрабатываемый независимо от других блок данных, причем последовательно исходящие от отправителя пакеты могут распространяться по различным путям в сети, менять порядок и даже теряться;
- *максимально возможную доставку* пакетов в том смысле, что потеря пакета происходит лишь в той ситуации, когда протокол не находит никаких физических средств для его доставки.

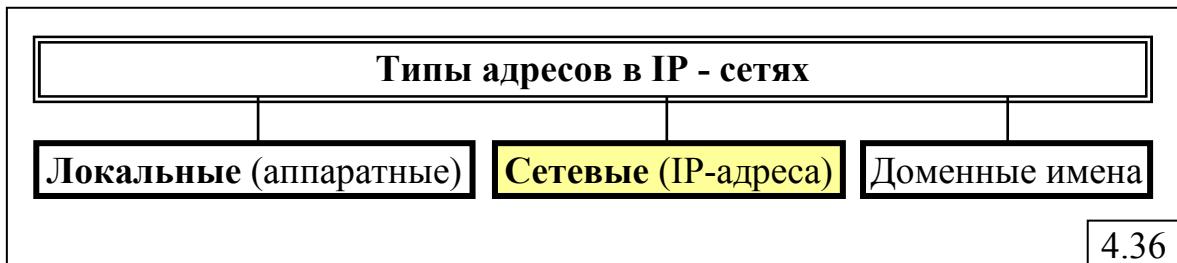
#### 4.4.4. Адресация в IP-сетях

В стеке протоколов TCP/IP используются три типа адресов (рис.4.36):

- **физические (локальные) адреса**, используемые для адресации узлов в пределах подсети, например: MAC-адреса, если подсеть

использует технологии Ethernet, Token Ring, FDDI, или IPX-адреса, если подсеть на основе технологии IPX/SPX;

- **сетевые (IP-адреса)**, используемые для идентификации узлов в пределах всей составной сети (подсети);
- **доменные имена** – символьные идентификаторы узлов, которыми оперируют пользователи.

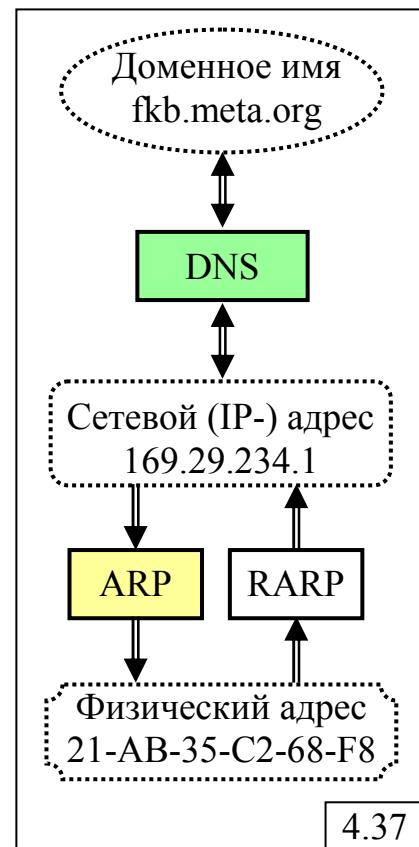


#### 4.4.4.1. Сетевые IP-адреса

Наличие трёх уровней адресации в IP-сетях требует применения процедур преобразования адресов разных уровней для установления соответствия между ними. Эти процедуры реализуются соответствующими протоколами, преобразующими адреса одного типа в другой.

Наиболее удобными для пользователей являются доменные имена, называемые также *доменными адресами*. Маршрутизация передаваемых данных в сети выполняется на основе сетевых адресов. В то же время, все устройства в компьютерной сети однозначно идентифицируются уникальными адресами канального уровня, в частности MAC-адресами в локальных сетях Ethernet и Token Ring.

Преобразование адресов в IP-сетях осуществляется в соответствии со схемой, представленной на рис.4.37. Ниже подробно рассматриваются протоколы преобразования доменных адресов в сетевые и обратно с использованием протокола DNS и преобразование сетевых адресов в физические и обратно, реализуемое протоколами ARP и RARP соответственно.

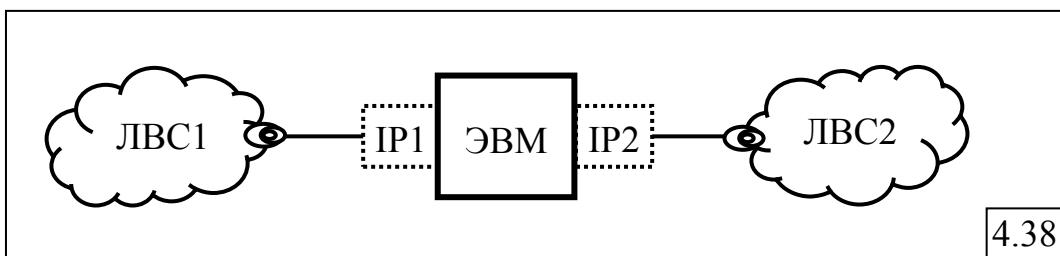


#### 4.4.4.2. Сетевые IP-адреса

**IP-адрес** – идентификатор *сетевого соединения (сетевого интерфейса)*. Это означает, что один и тот же компьютер, соединенный с двумя сетями (рис.4.38), имеет два IP-адреса: сеть 1 идентифицирует его по адресу IP1, а сеть 2 – по адресу IP2.

IP-адреса представляют собой 32-битовые идентификаторы, ориентированные на решение основной задачи протокола IP-

маршрутизации. Для удобства представления IP-адресов используется цифровое их написание в виде десятичного представления 4 байт, разделенных точками, например: **192.171.153.60**.



Первоначально в Интернете была принята так называемая классовая адресация. Все IP-адреса разделены на 5 классов (от А до Е), представленных на рис.4.39, но практическое применение находят в основном три первых класса: А, В и С. Класс D предназначен для задания группового адреса, а класс Е – не используется (зарезервирован для последующего использования).

Разряды	1	2	3	4	5	...	9	...	17	...	25	...	32		
<b>Класс А</b>	0	Номер сети										Номер узла (хоста)			
<b>Класс В</b>	1	0	Номер сети										Номер узла		
<b>Класс С</b>	1	1	0	Номер сети									Номер узла		
<b>Класс D</b>	1	1	1	0	Групповой адрес										
<b>Класс Е</b>	1	1	1	1	0	Зарезервирован для последующего использования									

4.39

IP-адрес состоит из двух полей: поле «Номер сети», представляющий собой адрес физической сети (подсети), и поле «Номер узла», выделяющий в этой подсети конкретное устройство (хост).

Признаком принадлежности адреса к определённому классу служат первые биты адреса: если первый бит равен 0, то адрес принадлежит классу А, если первый бит равен 1, а второй – 0, то адрес принадлежит классу В и т.д.

Принадлежность адреса к тому или иному классу определяет размер сети (табл.4.4):

- класс А соответствует большой сети с максимальным числом узлов ( $2^{24} - 2 = 16\ 777\ 214$ );
- класс В соответствует средней сети с числом узлов до 65534;
- класс С соответствует малой сети с числом узлов до ( $2^8 - 2 = 254$ ).

Отметим, что максимальное количество узлов в сети определяется количеством двоичных разрядов  $n$ , отводимых под номер узла:  $N_{\max} = 2^n - 2$ , то есть исключаются два номера:

- нулевой (все разряды равны 0); адрес с нулевым значением номера узла означает адрес сети;

- единичный (все разряды равны 1); адрес с единичными значениями номера узла является широковещательным и означает передачу пакета всем узлам сети.

Таблица 4.4

Показатель	Класс А	Класс В	Класс С
Размер сети	большая	средняя	малая
Номер (адрес) сети	наименьший	1.0.0.0	128.0.0.0
	наибольший	126.0.0.0	191.255.0.0
Число узлов в сети (max)	16 777 214	65 534	254
Длина поля в битах	номер сети	7	14
	номер узла	24	16
			8

IP-адрес построен таким образом, чтобы поля «Номер сети» и «Номер узла» можно было бы выделить быстро, что особенно сказывается на эффективности маршрутизации (малые временные затраты на выделение адреса «Номер сети»).

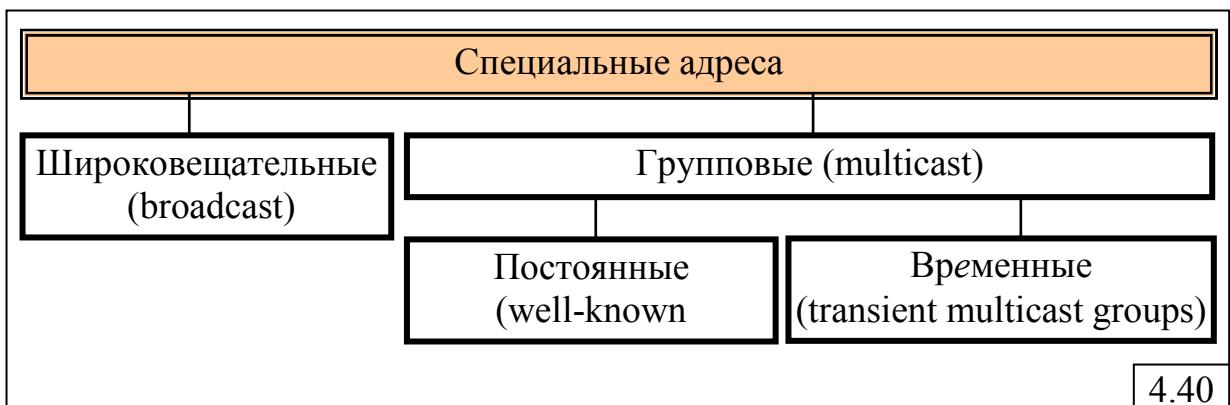
Поскольку IP-адрес идентифицирует сетевое соединение, а не узел, то отсюда вытекает принципиальное ограничение: *если компьютер переносится из одной подсети в другую, он должен обязательно изменить IP-адрес.*

#### 4.4.4.3. Специальные, автономные и групповые IP-адреса

IP-адресация поддерживает **специальные адреса** (рис.4.40), обращенные к множеству узлов и/или сетей и делящиеся на два класса:

- широковещательные (broadcast), обращенные ко всем;
- групповые (multicast), обращенные к заданному множеству объектов.

Адресная нотация при этом основывается на заполнении адресных полей нулями (обращение к данному объекту, this) или единицами (обращение ко всем объектам, all).



4.40

В табл.4.5 перечислены все возможные специальные адреса, трактовка которых раскрывается ниже.

Таблица 4.5

Тип	Номер сети	Номер узла
<b>Адрес 1</b>	0 0 0 ... 0	0 0 0 ... 0
<b>Адрес 2</b>	0 0 0 ... 0	X X X ... X
<b>Адрес 3</b>	X X X ... X	0 0 0 ... 0
<b>Адрес 4</b>	1 1 1 ... 1	1 1 1 ... 1
<b>Адрес 5</b>	X X X ... X	1 1 1 ... 1
<b>Адрес 6</b>	01111111	- - - - -

**Адрес 1** – "пустышка" или **неопределённый адрес**, используемый в инициализационной процедуре, когда рабочая станция не знает своего IP-адреса или хочет его согласовать; используется только как *адрес отправителя*, но никогда как адрес получателя.

**Адрес 2** – адрес конкретного узла (XXX...X) в той же сети, что и узел-отправитель; применяется в случае, когда узел-отправитель не знает идентификатора сети, в которой работает, например при инициализации бездисковой рабочей станции, которая при включении вообще ничего не знает ни о сети, ни о себе; используется только как *адрес получателя* и никогда как адрес отправителя.

**Адрес 3** – адрес сети (но не узла).

**Адрес 4** – **локальный** или **ограниченный широковещательный** адрес (limited или local broadcast address); используется, когда идентификатор сети по каким-либо причинам неизвестен; для использования не рекомендуется.

**Адрес 5** – **прямой широковещательный** адрес (direct broadcast address), обращенный ко всем узлам данной сети.

**Адрес 6** – **тестовый адрес**, в котором первый байт имеет значение 127, а оставшееся поле не специфицировано; используется для задач отладки и тестирования, не является адресом никакой сети, и маршрутизаторы никогда не обрабатывают его; также называется **адресом обратной петли** (loopback address), поскольку пакет с таким адресом, посланный на интерфейс loopback возвращается на тот же интерфейс, не выходя за пределы подсети.

Интерфейс loopback имеет несколько применений. Он может быть использован сетевым клиентским программным обеспечением, чтобы общаться с серверным приложением, расположенным на том же компьютере. Этот механизм полезен для тестирования служб, не подвергая их безопасность риску, как при удаленном сетевом доступе.

В стандартах Интернета определено несколько так называемых **автономных адресов**, рекомендуемых для автономного использования в пределах одной подсети и необрабатываемых маршрутизаторами:

- в классе A: 10.0.0.0 (1 сеть);

- в классе В: 172.16.0.0 – 172.31.0.0 (16 сетей);
- в классе С: 192.168.0.0 – 192.168.255.0 (256 сетей).

В качестве **группового адреса** используются адреса класса D. Групповая адресация в TCP/IP регламентируется входящим составной частью в IP протоколом *IGMP (Internet Group Management Protocol)*. Групповой адрес может объединять узлы из разных физических сетей путем использования в маршрутизаторах специальных протоколов групповой маршрутизации. Каждый узел может в любой момент подключиться к определенной адресной группе или выйти из нее.

Групповые адреса назначаются NIC и разделяются на два класса:

- **постоянные** – для непрерывно существующих групп (так называемые «всем известные адреса» – well-known addresses);
- **временные** – для организуемых на некоторый срок групп, которые существуют до тех пор, пока в группе сохраняется хотя бы один член (так называемые «временные адресные группы» – transient multicast groups).

Распространение групповых сообщений по интерсети ограничивается временем жизни (time-to-live) IP-пакета.

#### **4.4.4.4. Использование масок для IP-адресов**

**Маска** представляет собой 32-разрядный двоичный код, содержащий в *нескольких первых (старших) разрядах* «единицы», а в остальных – «нули». Количество единиц в маске определяет границу номера (идентификатора) сети. Другими словами, единичные значения маски позволяют выделить из IP-адреса номер сети, а оставшиеся младшие разряды IP-адреса определяют номер узла в этой сети.

Использование масок для IP-адресов позволяет *расширить адресное пространство* и сделать систему адресации более гибкой, не привязанной к классам IP-адресов (A, B или C).

**Пример.** Пусть заданы:

IP-адрес: **126.65.32.5** и маска: **255.192.0.0**.

IP-адрес **126.65.32.5** соответствует адресу узла **0.65.32.5** в сети **126.0.0.0**.

Запишем IP-адрес и маску в двоичном виде:

IP-адрес:	<b>01111110.01</b> 000001.00100000.00000101
маска:	<b>11111111.11</b> 000000.00000000.00000000

Тогда:

адрес сети: **01111110.01** или **126.64.0.0**

адрес узла: 000001.00100000.00000101 или **0.1.32.5**

Таким образом, вместо сети 126.0.0.0, принадлежащей к классу A, при наличии маски имеем сеть 126.64.0.0, которая не принадлежит ни одному из классов A, B или C. Максимальное количество узлов в этой сети определяется длиной поля адреса, используемого для нумерации узлов, то

есть количеством нулевых разрядов в маске. В нашем примере это 22 разряда, следовательно, максимальное количество узлов в сети будет равно  $2^{22} - 2 = 4\,194\,302$ .

Для стандартных классов сетей маски имеют вид:

**класс А:** 11111111.00000000.00000000.00000000 (255.0.0.0);

**класс В:** 11111111.11111111.00000000.00000000 (255.255.0.0);

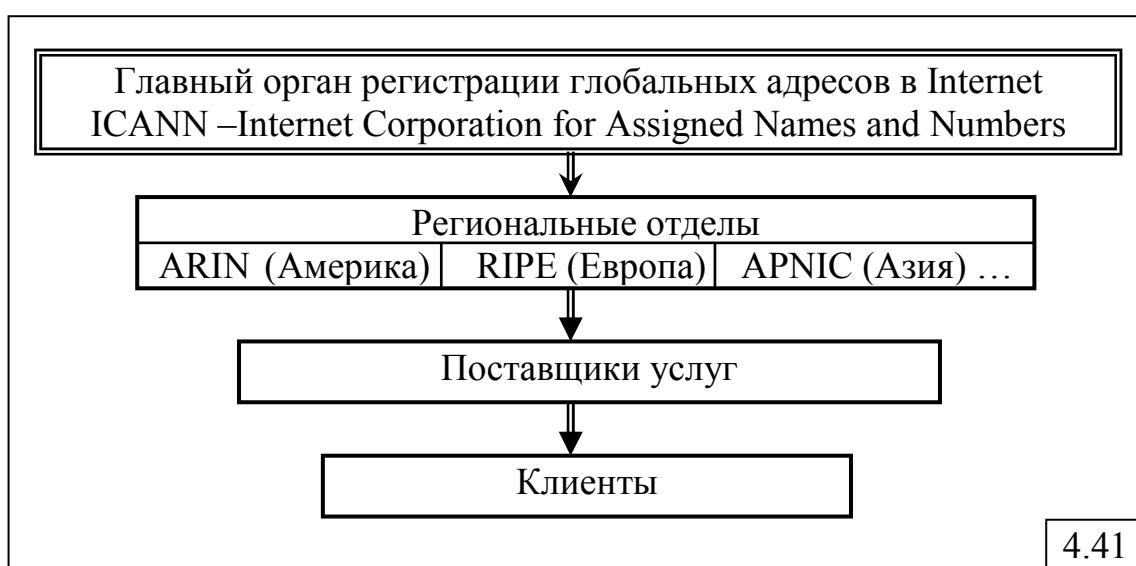
**класс С:** 11111111.11111111.11111111.00000000 (255.255.255.0).

Часто использование маски указывается в виде: 116.165.42.35/12, где число 12 определяет количество единичных разрядов в маске для IP-адреса 116.165.42.35.

#### 4.4.4.5. Распределение IP-адресов

Распределение IP-адресов может выполняться двумя способами:

- *централизованное распределение*, реализуемое специальными органами регистрации глобальных адресов, распределяющими адреса в сети Интернет и образующими иерархическую структуру, показанную на рис.4.41;
- *автоматизированное распределение*, реализуемое в сетях с единым административным управлением с использованием протокола назначения адресов DHCP.



Протокол для автоматического назначения IP-адресов – **Dynamic Host Configuration Protocol (DHCP)** – может поддерживать следующие способы распределения адресов (рис.4.42):

- *ручное распределение* – с участием администратора сети, причем DHCP-сервер всегда выдает определенному клиенту один и тот же назначенный ему администратором адрес;
- *автоматическое статическое распределение* – DHCP-сервер при первом подключении клиента выбирает из пула наличных IP-адресов произвольный IP-адрес, который при последующих подключениях клиента не меняется;

- автоматическое динамическое распределение – DHCP-сервер при каждом обращении клиента выдает IP-адрес на ограниченное время – **время аренды**, причем впоследствии этот адрес может быть предоставлен другому компьютеру; это позволяет строить IP-сеть с числом узлов, превышающим количество имеющихся в распоряжении администратора IP-адресов.

Кроме IP-адреса DHCP-сервер может назначить клиенту другие параметры стека TCP/IP, например:

- маску;
- IP-адрес маршрутизатора по умолчанию;
- IP-адрес сервера DNS;
- доменное имя компьютера и т.п.

#### Способы назначения IP-адресов

Ручное статическое

Автоматическое статическое

Автоматическое динамическое

4.42

Постоянный рост сети Интернет ведет к **дефициту IP-адресов**, особенно адресов класса А. Кроме того, имеющееся в распоряжении некоторой сети адресное пространство часто используется нерационально, например, используются не все адреса из 254 имеющихся в распоряжении сети класса С.

#### 4.4.4.6. Бесклассовая междоменная маршрутизация

Использование масок переменной длины для IP-адресов позволяет не только расширить адресное пространство за счет увеличения количества номеров сетей, но и экономно выделять IP-адреса.

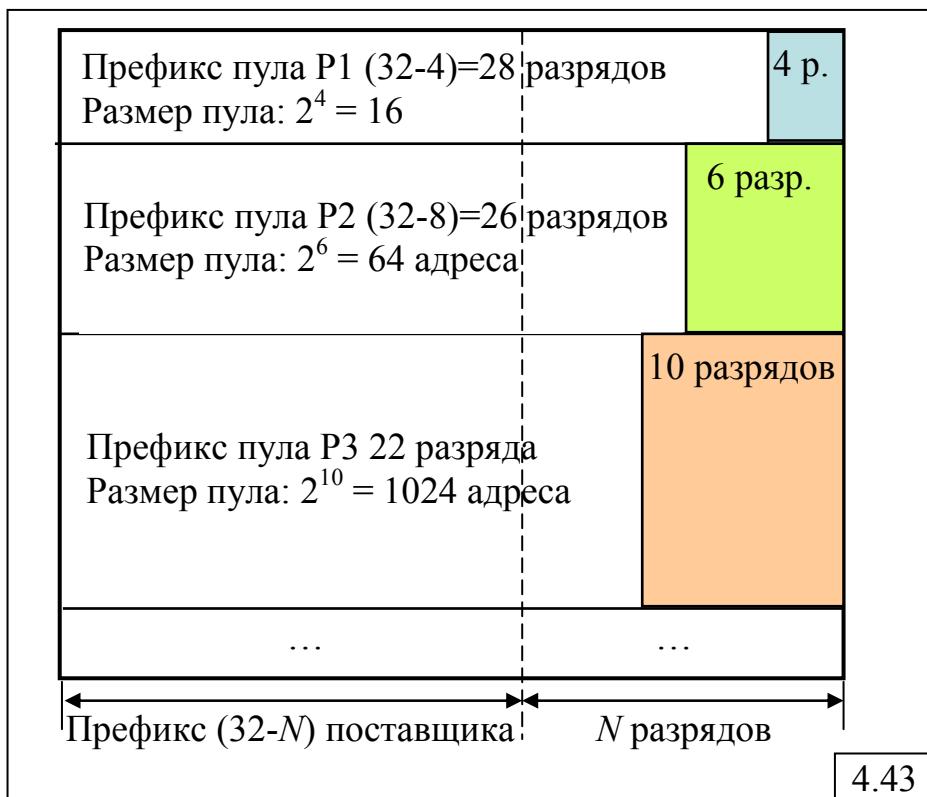
Например, если в какой-то небольшой сети находится десяток узлов, то очевидно, что неразумно выделять ей номер сети даже класса С, обеспечивающей нумерацию 254-х узлов. Гораздо более эффективным будет выделение для этой сети небольшого количества IP-адресов.

Для выделения ограниченного количества IP-адресов разработана технология **бесклассовой междоменной маршрутизации (CIDR – Classless Inter-Domain Routing)**, использующая **бесклассовую адресацию** и позволяющая гибко распределять IP-адреса.

Для реализации технологии CIDR необходимо, чтобы организация, распределяющая IP-адреса, имела в наличии непрерывный диапазон адресов. Это предоставляет возможность выделять сетям некоторое количество IP-адресов, имеющих *одинаковый префикс*, то есть одинаковые значения в нескольких старших разрядах. На рис.4.43 показан пример, иллюстрирующий принцип выделения адресов из общего пула адресов для сетей разных размеров. Так, например:

- пул Р1 имеет префикс длиной 28 двоичных разрядов и 4 разряда под нумерацию узлов, что позволяет пронумеровать 16 узлов небольшой сети;
- пул Р2 имеет префикс длиной 26 разрядов и 6 разрядов под нумерацию узлов, что позволяет пронумеровать 64 узла;

- пул Р3 с префиксом длиной 26 разрядов позволяет пронумеровать 1024 узла.



При таком выделении адресов необходимо, чтобы:

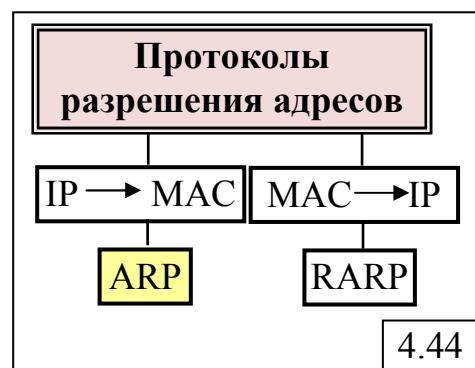
- количество выделяемых адресов было кратно степени двойки;
- начальная граница выделяемого пула адресов была кратна требуемому количеству узлов.

Благодаря технологии CIDR имеется возможность нарезать блоки адресов в соответствии с действительными потребностями каждой сети.

#### 4.4.4.7. Протоколы разрешения адресов ARP и RARP

Определение физического адреса устройства (MAC-адреса) по его IP-адресу и наоборот, IP-адреса по MAC-адресу, решают входящие в IP-стек два протокола:

- **ARP** (Address Resolution Protocol – Протокол разрешения адресов)
- **RARP** (Reverse Address Resolution Protocol – Протокол обратного определения адреса) соответственно рис.4.44.



**Протокол ARP** поддерживает в каждом узле (сетевом адаптере или порту маршрутизатора) **ARP-таблицу**, содержащую (рис.4.45):

- IP-адрес;
- MAC-адрес;
- тип записи (динамический, статический).

IP-адрес	MAC-адрес	Тип записи
195.36.210.12	12-43-F4-AB-5C-01	Динамический/статический
4.45		

По этой таблице узел может определить физический адрес (MAC-адрес) узла назначения, находящегося *в этой же сети*, по известному IP-адресу и указать его в заголовке кадра канального уровня. Если в ARP-таблице отсутствует запись для некоторого IP-адреса, то узел формирует *широковещательное сообщение – ARP-запрос*, в котором запрашивает физический адрес узла назначения. Все узлы сети принимают этот запрос, однако лишь один узел, IP-адрес которого совпадает с указанным в ARP-запросе, отвечает на него, высыпая *ARP-ответ* со своим физическим адресом *непосредственно* узлу, приславшему ARP-запрос. Последний записывает в ARP-таблицу найденное соответствие между IP-адресом и MAC-адресом и в дальнейшем не запрашивает его при повторных обращениях к этому узлу. Протокол ARP предполагает, что узлы знают свои IP-адреса.

Формат ARP-запроса (ответа) представлен на рис.4.46.

Поле	Значение
«Тип сети» канального уровня	1 (для Ethernet)
«Тип протокола» сетевого уровня	2048 (=0800 <sub>16</sub> для IP)
«Длина локального адреса»	6 (для Ethernet)
«Длина сетевого адреса»	4 (для IP)
«Опция»	(1 – для ARP-запроса и 2 – ответа)
«Локальный адрес отправителя»	008048EB6A15
«Сетевой адрес отправителя»	195.67.8.9
«Локальный адрес получателя»	000000000000 (для ARP-запроса)
«Сетевой адрес получателя»	195.67.8.12

4.46

В сети, объединяющей несколько локальных сетей (подсетей) с помощью маршрутизаторов, продвижение пакетов от узла, находящегося в одной подсети, к узлу, находящемуся в другой подсети, осуществляется на основе старшей части IP-адреса, то есть на основе номера сети. После того, как пакет поступит в конечный маршрутизатор, к которому подсоединенна вторая подсеть (сеть назначения), необходимо этот пакет упаковать в кадр и в качестве физического адреса узла назначения указать его MAC-адрес. Маршрутизатор просматривает свою ARP-таблицу и, если не находит соответствующего IP-адреса, формирует широковещательный ARP-запрос, посыпает его в локальную сеть и ожидает ARP-ответа. Если в сети нет

компьютера с указанным в ARP-запросе IP-адресом, то ARP-ответа не будет, и протокол IP уничтожит все пакеты, направляемые по этому адресу.

Статические записи создаются вручную и существуют, пока соответствующий узел (компьютер или маршрутизатор) не будет выключен.

Динамические записи создаются протоколом ARP как по собственным ARP-запросам, так и путем извлечения из широковещательных запросов IP- и MAC-адресов отправителя. Динамические записи периодически обновляются. Если в течение определенного интервала времени (порядка нескольких минут) адрес не использовался, то он исключается из таблицы.

В глобальных сетях, не поддерживающих широковещательные сообщения, ARP-таблицы формируются администратором вручную и помещаются на какой-либо хост, либо выделяется специальный маршрутизатор, который автоматически ведет ARP-таблицу для всех остальных узлов этой автономной сети.

**Протокол RARP** используется в случае, если узел – бездисковая рабочая станция, у которой только что включили питание и она не только ничего не знает о себе и окружающих, но и не может произвести дистанционную загрузку операционной системы, которая хранится на сетевом диске.

Узел широковещательно вызывает обслуживающий его сервер, закладывая в запрос свой физический адрес (при этом узел может даже не знать адреса сервера). В сети находится по меньшей мере один обслуживающий такие запросы сервер (RARP-сервер), который распознает запрос от рабочей станции, выбирает из некоторого списка свободный IP-адрес и шлет этому узлу сообщение с необходимой информацией:

- динамически выделенный узлу IP-адрес;
- свой физический адрес;
- IP-адрес и т.д.

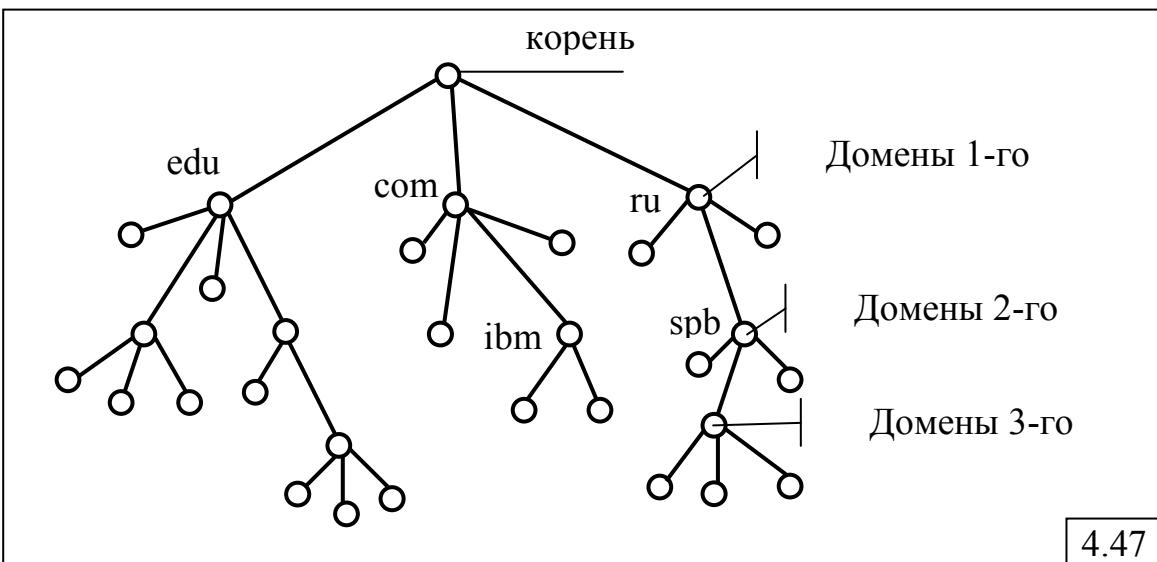
Поскольку при таком механизме отказ RARP-сервера очень критичен в том смысле, что без его услуг не заработает целый ряд рабочих станций, то обычно сеть конфигурируется так, чтобы протокол RARP поддерживало несколько серверов в сети.

#### **4.4.4.8. Система доменных имен DNS**

**Доменное имя** – символьное имя компьютера.

В стеке TCP/IP применяется система доменных имен с *иерархической древовидной структурой* (рис.4.47), допускающей использование в имени произвольного количества составных частей.

Совокупность имен, у которых несколько старших составных частей совпадают, образуют **домен (domain) имен**.



4.47

Примерами доменных имён организаций являются:

- com – коммерческие организации;
- edu – образовательные организации;
- gov – правительственные организации;
- org – некоммерческие организации;
- net –организации поддержки сетей.

Соответствие между доменными именами и IP-адресами может устанавливаться как средствами локального узла, так и средствами централизованной службы, реализуемой системой доменных имён.

**Система доменных имен (Domain Name System – DNS)** – централизованная служба, основанная на распределенной базе отображений «доменное имя – IP-адрес» (рис.4.48).

Служба DNS использует в своей работе протокол типа «клиент–сервер», в котором определены такие понятия как **DNS-сервер**, поддерживающий распределенную базу отображений, и **DNS-клиент**, обращающийся к DNS-серверу с запросом. DNS-сервер использует текстовые файлы формата «IP-адрес – доменное имя».

Доменное имя	IP-адрес
sota.park.org	213.45.7.12
abc.spb.ru	184.31.61.1
labor.uni.edu	159.1.26.34

4.48

Служба DNS является распределенной. Каждый DNS-сервер хранит имена следующего уровня иерархии и кроме таблицы отображений имен содержит ссылки на DNS-серверы своих поддоменов, что упрощает процедуру поиска.

Для ускорения поиска IP-адресов в DNS-серверах применяется процедура кэширования проходящих через них ответов на определенное время – от нескольких часов до нескольких дней.

#### 4.4.5. Коммуникационный протокол IPv4

Протокол IP специфицирует три основных элемента:

- блок данных – **пакет IP**, с которым работает протокол;
- механизмы распространения (маршрутизации) пакетов;
- способы обработки конфликтных ситуаций.

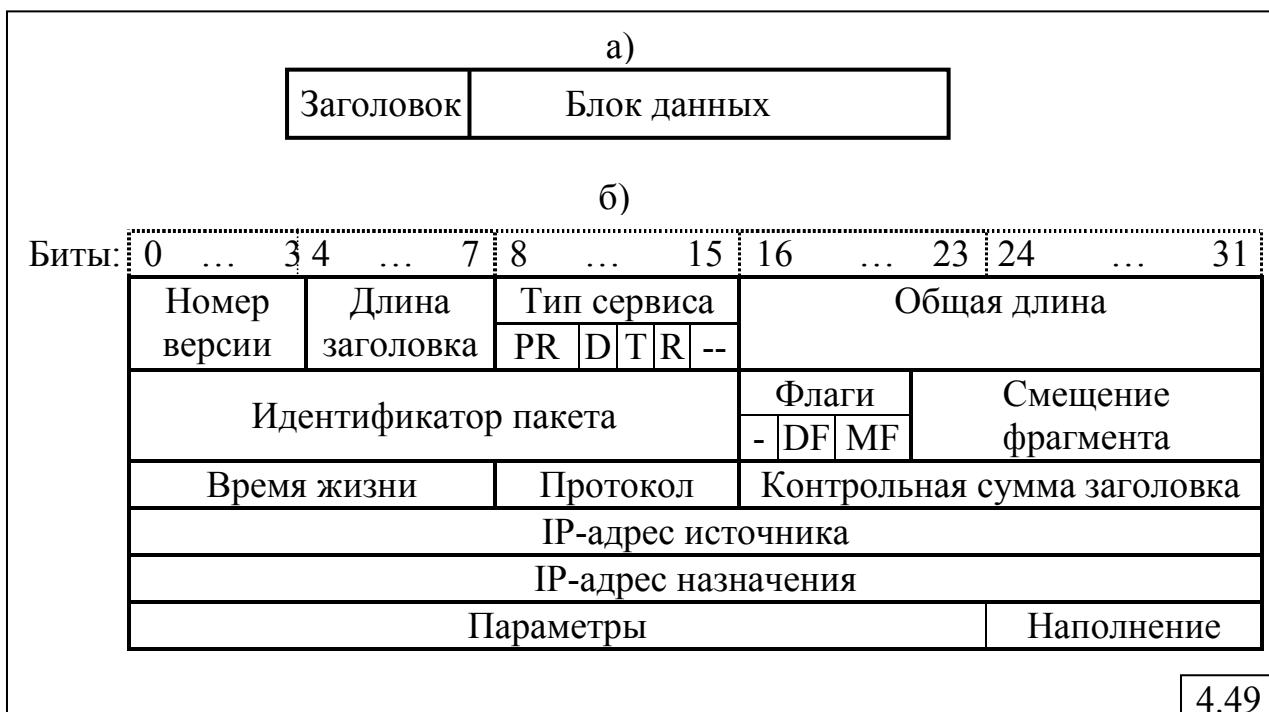
**Пакет IP** состоит из заголовка и блока данных (рис.4.49,а).

В настоящее время в сети Интернет могут циркулировать IP-пакеты двух версий:

- IP-пакет версии 4 (IPv4);
- IP-пакет версии 6 (IPv6).

Протокол IP обрабатывает и интерпретирует только поля заголовка.

**Формат заголовка пакета IPv4** показан на рис.4.49,б).



Рассмотрим назначения полей заголовка.

«**Номер версии**» (4 бита) – используется для указания версии протокола IP, который должен обрабатывать данный пакет. В настоящее время осуществляется постепенный переход от версии 4 к версии 6, и большинство узлов могут обрабатывать пакеты обеих версий. Если это поле содержит значение, отличное от указанных версий протокола, пакет уничтожается.

«**Длина заголовка**» (4 бита) – задает значение длины заголовка пакета, измеренной в 32-битовых (4-байтовых) словах. Минимальное значение длины (при отсутствии необязательных полей «Параметры» и «Наполнение») равно 5, что соответствует заголовку длиной 20 байт. Максимальное значение этого 4-битового поля равно 15, что соответствует

заголовку длиной 60 байт. Следовательно, максимальный размер необязательных полей «Параметры» и «Наполнение» равен 40 байтам.

«Тип сервиса» (Type of Service, ToS) – 8-битовое поле, предназначенное для оптимизации транспортной службы, содержащее:

- 3-битовое поле «Приоритет» принимает 8 значений: от 0 (нормальный приоритет) до 7 (сетевое управление);
- биты D,T,R задают тип транспортировки, который "запрашивает" пакет; установка этих битов в состояние "1" требует:
  - D=1 (*Delay – задержка*) – малой задержки при передаче пакета;
  - T=1 (*Throughput – пропускная способность*) – высокой пропускной способности;
  - R=1 (*Reliability – надежность, достоверность*) – высокой надежности;
- 2 резервных бита.

Стандарты, принятые в конце 90-х годов, дали новое название этому полю – *байт дифференцированное обслуживание* или *DS-байт* – и переопределене назначение его битов.

Поле «Тип сервиса» не всегда используется маршрутизаторами.

«Общая длина» (16 бит) – задает длину пакета, включая заголовок и данные, измеренную в байтах. Общая длина пакета IP может достигать 65 535 байт, однако в большинстве сетей столь большие пакеты не используются.

Протокол IP должен обеспечивать межсетевое взаимодействие между разными сетями, различающимися, в том числе, ограничением на *максимальную длину кадра*, разрешенным в той или иной физической сети (Maximum Transfer Unit, MTU). Поэтому протокол IP вынужден решать задачу, более свойственную транспортному протоколу, – разбивку больших пакетов на малые и наоборот – их сборку. Это требуется делать в тех случаях, когда на вход некоторой физической сети поступает пакет, превосходящий по длине MTU для данной сети. Такая операция называется *фрагментированием* (fragmentation) и осуществляется следующим образом.

Блок данных большого исходного пакета разделяется на *фрагменты* длиной MTU для физической сети, в которую направляются фрагменты. При этом фрагменты упаковываются в пакеты, заголовки которых похожи на заголовок исходного пакета.

В стандартах TCP/IP предусматривается, что все узлы должны принимать пакеты длиной не менее 576 байт, независимо от того, являются они фрагментами или целыми пакетами.

Следующие три поля заголовка пакета указывают на то, что данные пакеты являются фрагментами одного большого пакета.

«Идентификатор пакета» (16 бит) – общий для всех фрагментов идентификатор, указывающий на принадлежность фрагмента к одному большому пакету.

**«Флаги»** (3 бита) – содержат признаки (биты), связанные с фрагментацией:

- DF (Do not Fragment – не фрагментировать) – значение, равное 1, запрещает маршрутизатору фрагментировать пакет;
- MF (More Fragments – больше фрагментов) – значение, равное 1, означает, что фрагмент является промежуточным;
- один бит зарезервирован.

**«Смещение фрагмента»** (13 бит) – смещение в байтах поля данных этого фрагмента относительно начала поля данных исходного нефрагментированного пакета. Смещение используется при сборке фрагментов в пакет и должно быть кратно 8 байтам.

**«Время жизни»** (Time To Live, TTL) – 8-битовое поле, содержащее время, измеряемое в секундах, в течение которого пакет может существовать в сети. Хосты и маршрутизаторы, обрабатывающие данный пакет, уменьшают значение этого поля в период обработки и хранения пакета как минимум на 1 плюс время ожидания в очереди. Однако на практике в каждом маршрутизаторе обычно из этого времени просто вычитается 1. Таким образом, время жизни фактически измеряется количеством маршрутизаторов, через которые проходит пакет. Когда время жизни истекает, пакет уничтожается. При этом источник сообщения уведомляется о потере пакета. Наличие конечного времени жизни пакета, равное 255 (8 двоичных разрядов), обеспечивает, в частности, защиту от таких нежелательных событий, как передача пакета по циклическому маршруту, перегрузка сетей.

**«Протокол»** (8 бит) – указывает протокол вышележащего уровня, которому предназначена информация, содержащаяся в поле данных пакета IP. Например, значение 6 соответствует протоколу TCP, а значение 17 – протоколу UDP.

**«Контрольная сумма заголовка»** (16 бит) – используется для контроля целостности только заголовка пакета IP и вычисляется как сумма всех 16-битовых полуслов заголовка в дополнительном коде, преобразованная также в дополнительный код. Таким образом, вычисляемая получателем контрольная сумма заголовка вместе с этим полем должна быть равна нулю. Поскольку некоторые поля заголовка могут изменять свои значения в процессе передачи пакета по сети, контрольная сумма вычисляется и проверяется в каждом маршрутизаторе и в конечном узле.

**«IP-адрес источника»** (32 бита) – IP-адрес отправителя пакета.

**«IP-адрес назначения»** (32 бита) – IP-адрес получателя пакета.

**«Параметры»** – необязательное поле переменной длины, применяемое для указания параметров, используемых обычно при отладке сети и связанных, например, с режимами безопасности или маршрутизации.

**«Наполнение»** – поле переменной длины, необходимое для дополнения заголовка пакета до целого числа 32-битовых слов.

## 4.4.6. Коммуникационный протокол IPv6

Проблемы, с которыми в начале 90-х годов столкнулись разработчики и пользователи Интернета, базирующегося на протоколах TCP/IP, привели к осознанию необходимости разработки новой версии протокола IP – **протокола IPv6**, который должен обеспечить достижение следующих целей:

- создание масштабируемой системы адресации, обеспечивающей поддержку миллиардов хостов даже при неэффективном использовании адресного пространства;
- уменьшение таблиц маршрутизации и упрощение протокола для ускорения обработки пакетов маршрутизаторами;
- предоставление гарантий качества транспортных услуг при передаче неоднородного трафика, в частности, при передаче данных реального времени;
- более надёжное обеспечение безопасности - аутентификации и конфиденциальности;
- возможность существования старого и нового протоколов;
- возможность развития протокола в будущем.

Основными особенностями протокола IPv6 являются следующие.

1. Длина IP-адреса увеличена до 16 байт, что предоставляет пользователям практически неограниченное адресное пространство

2. Упрощена структура заголовка, содержащего всего 7 полей (вместо 13 в протоколе IPv4), что позволяет маршрутизаторам быстрее обрабатывать пакеты, то есть повышает их производительность.

3. Улучшена поддержка необязательных параметров, так как в новом заголовке требуемые прежде поля стали необязательными, а изменённый способ представления необязательных параметров ускоряет обработку пакетов в маршрутизаторах за счёт пропуска не относящихся к ним параметров.

4. Улучшена система безопасности.

5. Предусмотрена возможность расширения типов (классов) предоставляемых услуг, которые могут появиться в результате ожидаемого роста мультимедийного трафика.

### 4.4.6.1. Адресация в IPv6

Необходимость расширения адресного пространства в сетях TCP/IP была одной из основных целей перехода на новую версию протокола IP. Для этого длина IP-адреса была увеличена до **16 байт** или **128 бит**, что предоставляет пользователям практически *бесконечное адресное пространство* – более чем  $10^{38}$  адресов.

В протоколе IPv6 вместо двухуровневой (как в IPv4) иерархии адресов используется четырёхуровневая:

- 3 уровня используются для идентификации сетей;
- 1 уровень используется для идентификации узла сети.

Для записи 16-байтовых адресов используется *шестнадцатеричная форма* (вместо десятичной формы в протоколе IPv4), причём каждые 4 шестнадцатеричные цифры отделяются друг от друга *двоеточием*:

**AB25:164:0:E12B:6:0:C2C4:1234**

**BDA5::3217:19:0:F084**

Как видно из представленных примеров, при записи адреса допускается ряд упрощений:

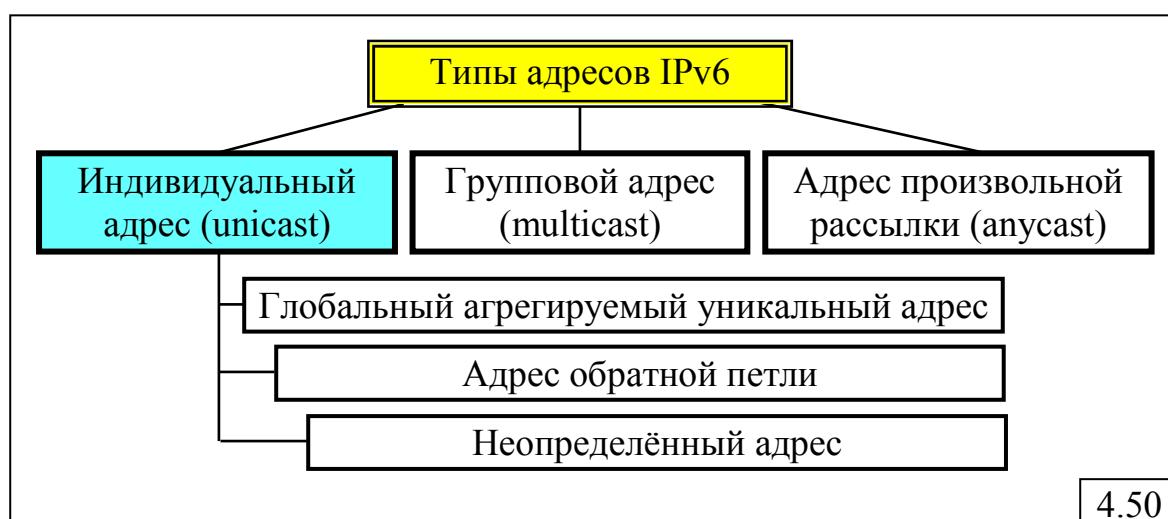
- вместо 4-х нулей записывается только один нуль: **0** вместо 0000;
- можно опускать незначащие нули в начале каждого четырёхсимвольного поля адреса: **164** вместо 0164 или **6** вместо 0006;
- если в адресе имеется длинная последовательность нулей, то запись можно сократить, заменив в ней все нули двоеточием, причём двоеточие может употребляться только один раз:

**CF18: 35::67:5**, что соответствует адресу **CF18: 35:0:0:0:67:5**;

• для сетей, использующих обе версии (IPv4 и IPv6) протокола разрешается использовать традиционную десятичную запись IPv4 в 4-х младших байтах, например: **::BAC2:192.85.1.6**.

В протоколе IPv6 предусмотрено 3 типа IP-адресов (рис.4.50):

- *индивидуальный адрес* (unicast), определяющий уникальный идентификатор отдельного интерфейса оконечного узла или маршрутизатора;
- *групповой адрес* (multicast), аналогичный групповому адресу IPv4, идентифицирует группу интерфейсов, относящихся, как правило, к разным узлам;
- *адрес произвольной рассылки* (anycast) – новый тип адреса, назначаемый только интерфейсам маршрутизатора и определяющий группу интерфейсов, к одному из которых доставляется пакет с таким адресом, как правило, «ближайшему» в соответствии с метрикой, используемой протоколами маршрутизации.

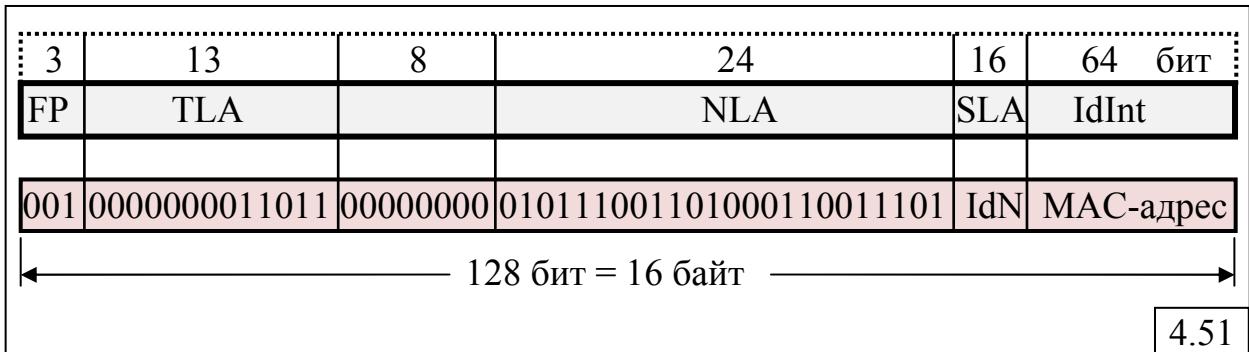


4.50

*Индивидуальные IP-адреса* могут быть трёх типов (рис.4.50):

- **глобальный агрегируемый уникальный адрес**, являющийся основным подтипов индивидуального адреса, основанные на агрегировании для упрощения маршрутизации;
- **адрес обратной петли**, играющий ту же роль, что и адрес 127.0.0.1 протокола IPv4 и имеющий вид: **0:0:0:0:0:0:0:1**;
- **неопределённый адрес**, состоящий из одних нулей и являющийся аналогом адреса 0.0.0.0 протокола IPv4.

Рассмотрим структуру глобального агрегируемого уникального адреса (рис.4.51).



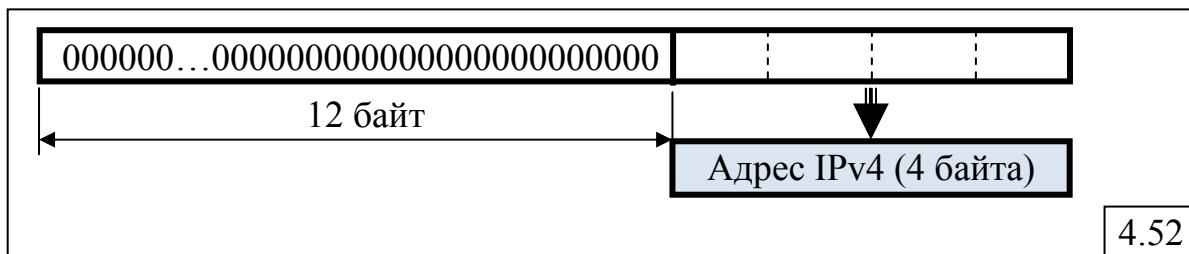
Поле **FP** (Format Prefix – **префикс формата**) определяет формат адреса и для рассматриваемого типа имеет значение 001.

Следующие поля описывают три уровня идентификации сетей:

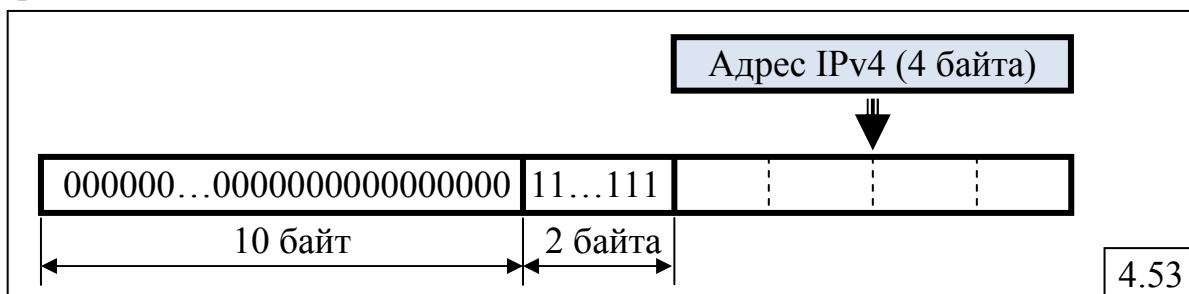
- **TLA** (Top-Level Aggregation – **агрегирование верхнего уровня**) предназначено для нумерации сетей самых крупных поставщиков услуг; небольшое количество разрядов (13 двоичных разрядов) позволяют ограничить количество таких сетей числом 8196 и, следовательно, ограничить размер таблиц маршрутизации и ускорить работу магистральных маршрутизаторов; следующие 8 разрядов за полем TLA зарезервированы на будущее для его расширения;
- **NLA** – (Next-Level Aggregation – **агрегирование следующего уровня**) предназначено для нумерации средних и мелких поставщиков услуг;
- **SLA** – (Site-Level Aggregation – **агрегирование местного уровня**) предназначено для нумерации подсетей, находящихся в распоряжении одного администратора, который может формировать адреса, состоящие из идентификатора подсети SLA и идентификатора интерфейса IdInt, без согласования с поставщиком услуг.

Поле **IdInt** – идентификатор интерфейса является аналогом номера узла в протоколе IPv4, но в отличие от него содержит физический (локальный) адрес интерфейса (например, MAC-адрес или адрес X.25), а не произвольно назначенный номер узла. В этом случае *отпадает необходимость в протоколе ARP* и в ручном конфигурировании конечных узлов. Кроме того, *теряет смысл использование масок для разделения сетей на подсети*, в то время как объединение сетей приобретает особое значение.

Для того чтобы узлы, поддерживающие протокол IPv6, могли передавать пакеты через сеть IPv4, разработан специальный подтип адресов, которые переносят адрес IPv4 в младших 4-х байтах адреса IPv6, а в 12 старших байтах содержат нули (рис.4.52).



Для передачи пакетов IPv4 через подсети, работающие по протоколу IPv6, предназначен **IPv4-отображённый IPv6-адрес** (рис.4.53), содержащий в первых десяти байтах нули, а в двух последующих байтах – единицы, которые показывают, что данный узел поддерживает только протокол IPv4.

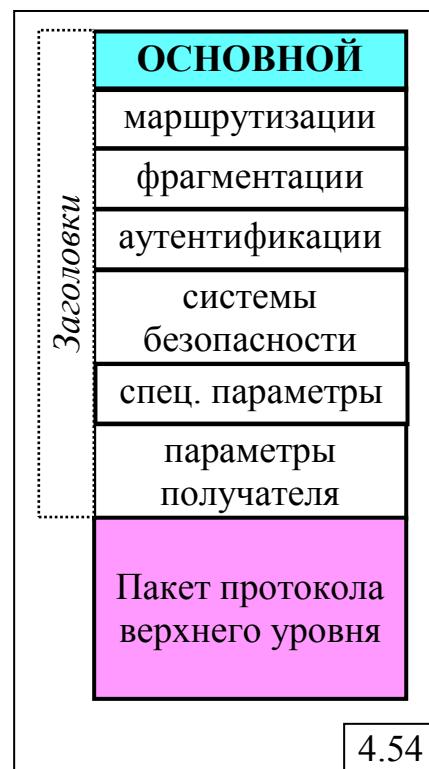


#### 4.4.6.2. Структура пакета IPv6

Структура пакета IPv6 (рис.4.54) существенно отличается от пакета IPv4. Это проявляется, прежде всего, в возможности наличия нескольких заголовков – кроме основного заголовка, который всегда присутствует, пакет может иметь несколько дополнительных заголовков, которые могут содержать информацию, необходимую для качественной передачи пакета.

В качестве дополнительных заголовков могут использоваться следующие:

- **заголовок маршрутизации**, содержащий полный маршрут при маршрутизации от источника;
- **заголовок фрагментации**, содержащий информацию о фрагментации исходного IP-пакета;
- **заголовок аутентификации**, содержащий информацию, необходимую для аутентификации конечных узлов и обеспечения целостности содержимого IP-пакетов;



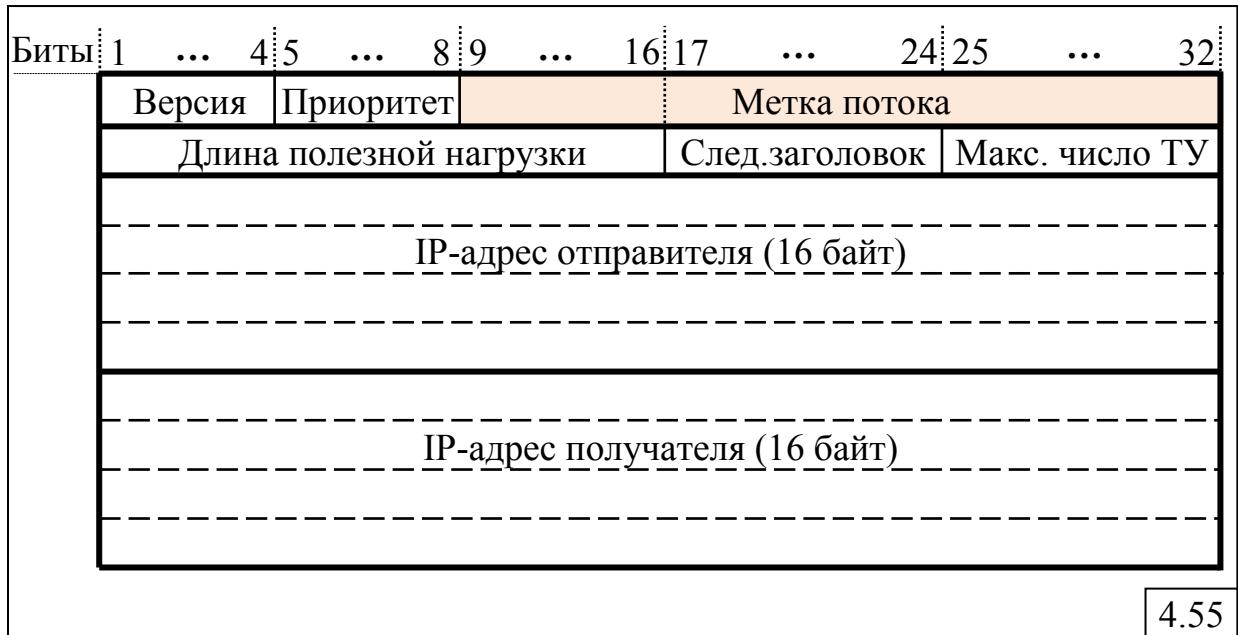
- **заголовок системы безопасности**, содержащий информацию, необходимую для обеспечения конфиденциальности передаваемых данных путём шифрования пакетов;
- **специальные параметры**, необходимые для обработки пакетов в процессе передачи по сети;
- **параметры получателя**, содержащие дополнительную информацию для узла назначения.

Такая структура пакета IPv6 обеспечивает следующие преимущества по сравнению с пакетом IPv4:

- *меньше нагрузка на маршрутизаторы*, поскольку все дополнительные заголовки обрабатываются только в конечных узлах;
- *большая функциональность и открытость* для внедрения новых механизмов протокола IP за счёт использования большого количества дополнительных параметров.

#### **4.4.6.3. Формат основного заголовка IPv6**

Формат основного заголовка IPv6 имеет фиксированную длину 40 байт (рис.4.55).



**Поле «Версия»** (4 бита) содержит число 6 для пакета IPv6.

**Поле «Приоритет»** (4 бита) используется для того, чтобы различать пакеты с разными требованиями к доставке в реальном времени.

**Поле «Метка потока»** предназначено для установления между отправителем и получателем псевдосоединения с определёнными свойствами и требованиями. Маршрутизаторы, в зависимости от метки потока в заголовке прибывшего пакета, определяют, какого рода особая обработка требуется пакету. С помощью этого поля протокол пытается объединить достоинства дейтаграммного способа передачи пакетов и способа «виртуальный канал».

**Поле «Длина полезной нагрузки»** указывает, сколько байт содержится в пакете без учета основного заголовка, длиной 40 байт. Аналогичное поле «Полная длина» в IPv4 определяло всю длину пакета с учётом заголовка.

**Поле «Следующий заголовок»** указывает, какой из дополнительных заголовков следует за основным. Все дополнительные заголовки содержат такие же поля, которые указывают на последующие заголовки. В последнем заголовке в этом поле указывается протокол транспортного уровня (TCP или UDP), которому следует передать содержимое пакета.

**Поле «Максимальное число транзитных участков (ТУ)»** определяет время жизни пакета. Значение поля, устанавливаемое узлом-отправителем, уменьшается на единицу на каждом транзитном участке.

Далее следуют 16-байтные IP-адреса отправителя и получателя.

Сравнение заголовка IPv6 с заголовком IPv4 показывает, что:

- поле «Длина заголовка» исчезло, так как основной заголовок IPv6 имеет фиксированную длину;
- поле «Протокол» отсутствует, поскольку поле «Следующий заголовок» указывает, что следует за последним заголовком (TCP-сегмент или UDP-пакет);
- удалены поля, относящиеся к фрагментации, так как все узлы, поддерживающие протокол IPv6, должны динамически определять нужный размер дейтаграммы, что делает фрагментацию маловероятной;
- минимальный размер пакета, который должен передаваться в сетях IPv6 без фрагментации, увеличен с 576 до 1280 байт;
- поле «Контрольная сумма» удалено, так как её подсчёт занимает много времени, что существенно снижает производительность узлов; к тому же всё шире используются надёжные линии связи, например волоконно-оптические.

Таким образом, протокол IPv6 является *простым, быстрым и гибким* протоколом сетевого уровня с огромным адресным пространством.

#### 4.4.7. Фрагментация

В объединяемых сетях разных технологий допустимая максимальная длина пакетов (**Maximum Transfer Unit, MTU**) различна и варьируется от 53 байт в ATM-сетях до 65 535 байт в IP-сетях. При объединении таких сетей возникает проблема, связанная необходимостью разбиения большого пакета при его передаче через сеть с меньшей допустимой длиной пакета. Если пакет проходит через последовательность сетей и попадает в сеть, у которой значение MTU оказывается меньше размера пакета, пограничный маршрутизатор разбивает пакет на две или более части.

Процесс разбиения длинного пакета на более короткие называется **фрагментацией**, а соответствующие короткие пакеты – **фрагментами**. При фрагментации каждый новый пакет получает свой IP-заголовок (20 байт), что увеличивает накладные расходы. После прохождения

фрагментов через соответствующую сеть необходимо восстановить исходный пакет из фрагментов.

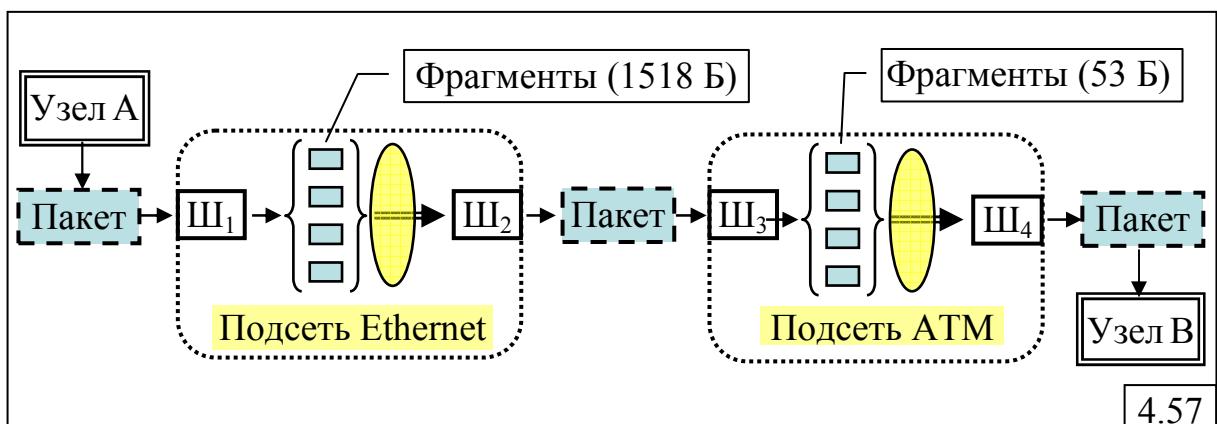
Фрагментация в сетях может быть реализована двумя способами (рис.4.56):

- прозрачная фрагментация;
  - сквозная фрагментация.



4.56

Принцип реализации *прозрачной фрагментации* на примере передачи длинного пакета от узла А к узлу В через две подсети (Ethernet и ATM) с меньшим значением MTU показан на рис.4.57.



4.57

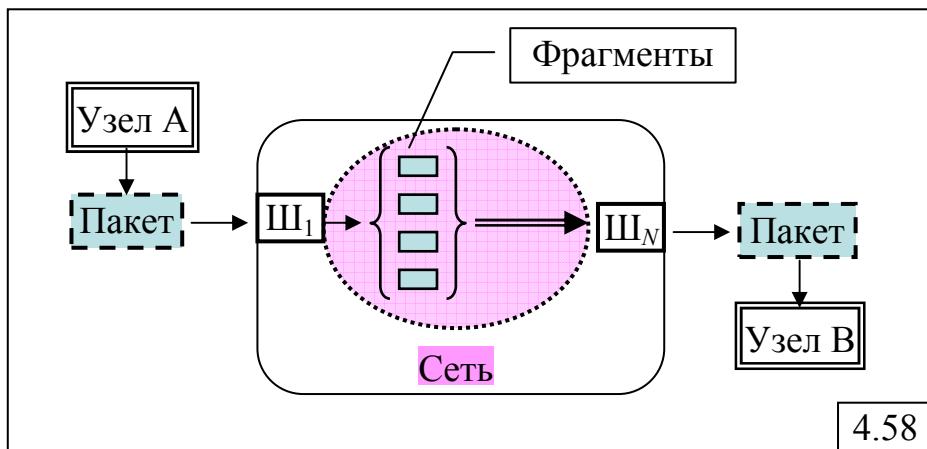
Подсети с разными MTU имеют шлюзы – специализированные маршрутизаторы, предоставляющие интерфейсы для связи с другими сетями. Если на такой шлюз приходит пакет слишком большого размера, он разбивается на фрагменты в соответствии с принятым в данной сети значением MTU. Каждый фрагмент адресуется одному и тому же выходному шлюзу, который восстанавливает из этих фрагментов исходный пакет и. Таким образом, прохождение данных через сети (подсети) с маленькими значениями MTU оказывается прозрачным для пользователей.

Прозрачная фрагментация обладает простотой, но при этом имеет ряд существенных недостатков:

- выходной шлюз должен собрать все фрагменты для восстановления исходного пакета, для чего в заголовках фрагментов необходимо иметь дополнительную информацию, например, номер фрагмента и признак последнего фрагмента;
  - все фрагменты одного пакета должны покидать подсеть через один и то же шлюз, что снижает эффективность маршрутизации;

- появляются дополнительные накладные расходы на фрагментацию и дефрагментацию, что снижает производительность сети и увеличивает время доставки пакетов.

**Сквозная фрагментация** (рис.4.58) является альтернативной по отношению к прозрачной фрагментации и состоит в отказе от восстановления пакета из фрагментов в каждой подсети. Пакет разбивается на фрагменты сразу же в узле-отправителе А или в шлюзе  $Ш_1$  сети. Эти фрагменты передаются по сети как самостоятельные пакеты независимо друг от друга и собираются только в конечном шлюзе  $Ш_N$  или узле-получателе В.



Недостатками такого способа фрагментации являются следующие:

- необходимо, чтобы каждый узел (или шлюз) могли восстанавливать пакеты из фрагментов;
- возрастают накладные расходы на передачу данных, так как каждый фрагмент должен иметь заголовок, который сохраняется на протяжении всего пути, что снижает пропускную способность сети;
- необходимо иметь информацию о том, какие значения MTU имеют подсети, через которые проходит путь передачи данных, чтобы задать размер фрагментов.

Для того чтобы правильно восстановить исходный пакет из фрагментов необходимо иметь эффективную систему нумерации фрагментов. Одна из таких систем основана на понятии **элементарного фрагмента**, имеющего небольшой размер, достаточный для его передачи через любую подсеть. Например, длина элементарного фрагмента может быть равна 8 байтам, как это показано на рис.4.59. Исходный пакет разбивается на множество элементарных фрагментов одинаковой длины (рис.4.59,а), кроме последнего, который может быть короче. Фрагменты, формируемые в некоторой подсети и называемые **межсетевыми пакетами**, могут состоять из нескольких элементарных фрагментов (рис.4.59,б), число которых определяется значением MTU, принятым для данной подсети. Заголовок таких фрагментов должен содержать (рис.4.59):

- номер исходного пакета (ИП);

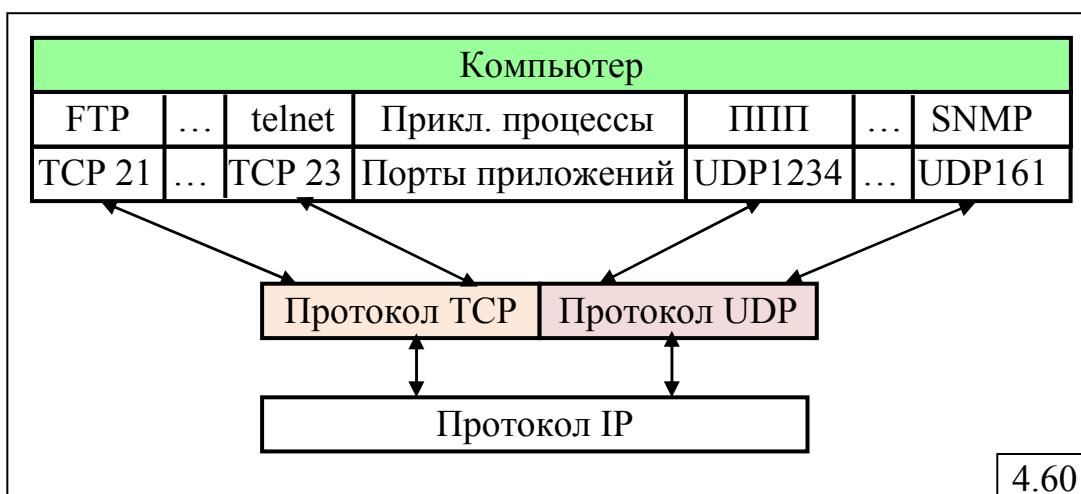
- номер первого элементарного фрагмента (нумерация начинается с нуля), содержащегося в нём, который в заголовке IP-пакета называется *смещением фрагмента* (СФ);
- признак конца (ПК) пакета.

Поскольку размер элементарного фрагмента выбирается таким образом, чтобы он мог пройти через любую сеть, дальнейшая фрагментация межсетевого пакета не составляет проблемы.



#### 4.4.8. Транспортные протоколы стека TCP/IP

Транспортные протоколы TCP и UDP стека протоколов TCP/IP обеспечивают передачу данных между любой парой *прикладных процессов*, выполняющихся в сети, и предоставляют интерфейс для протокола IP путем демультиплексирования нескольких процессов, использующих в качестве адресов транспортного уровня порты. Для каждого прикладного процесса (ПП) (приложения), выполняемого в компьютере, может быть сформировано *несколько точек входа*, выступающих в качестве *транспортных адресов*, называемых *портами* (рис.4.60).



- Существуют два способа присвоения порта приложению:
- централизованный** (присвоенные или назначенные номера от 0 до 1023), использующий стандартные номера, присвоенные

общедоступным службам (приложениям), например: FTP – 21, telnet – 23, SMTP – 25, DNS – 53, HTTP – 80.

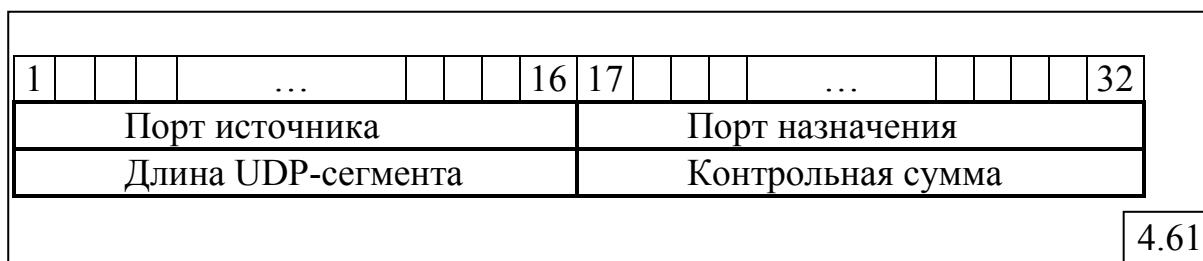
- **локальный** (динамические номера от 1024 до 65535), предоставляющий произвольный номер из списка свободных номеров при поступлении запроса от приложения пользователя.

Динамические номера портов приложений являются уникальными в пределах каждого компьютера, но могут совпадать с номерами портов в других компьютерах. Различие между ними определяется только различием интерфейсов каждого из компьютеров, задаваемых IP-адресами. Таким образом, пара «**IP-адрес; номер порта**», называемая **сокетом** (socket), однозначно определяет прикладной процесс в сети.

Номера UDP- и TCP-портов в пределах одного и того же компьютера могут совпадать, хотя и идентифицируют разные приложения. Поэтому при записи номера порта обязательно указывается тип протокола транспортного уровня, например 2345/TCP и 2345/UDP. В некоторых случаях, когда приложение может обращаться по выбору к протоколу UDP или TCP, ему могут быть назначены одинаковые номера UDP- и TCP-портов, например DNS-приложению назначен номер 53 – 53/UDP и 53/TCP.

#### 4.4.8.1. Транспортный протокол UDP

UDP – транспортный протокол, обеспечивающий передачу данных в виде *дейтаграмм* между любой парой *прикладных процессов*, выполняющихся в сети, *без установления соединения*. Сегменты состоят из 8-байтового заголовка, за которым следует поле данных. Заголовок UDP-сегмента показан на рис.4.61.



Наиболее широко UDP используется при выполнении клиент-серверных приложений (типа запрос-ответ).

При этом UDP не выполняет:

- контроль потока,
- контроль ошибок,
- повторной передачи после получения испорченного сегмента.

Примерами приложений, использующих протокол UDP для передачи данных, являются DHCP, DNS, SNMP.

В некоторых случаях на одном конечном узле может выполняться несколько копий одного и того же приложения. Возникает вопрос: каким образом различаются эти приложения?

Для этого рассмотрим на простом примере процесс формирования запроса и процедуру обращения DNS-клиента к DNS-серверу, когда на одном компьютере запущены два DNS-сервера, причём оба используют для передачи своих данных транспортный протокол UDP (рис.4.62). Для того чтобы различать DNS-серверы, им присваиваются разные IP-адреса – IP1 и IP2, которые вместе с номером порта образуют два разных сокета: «UDP-порт 53, IP1» и «UDP-порт 53, IP2».

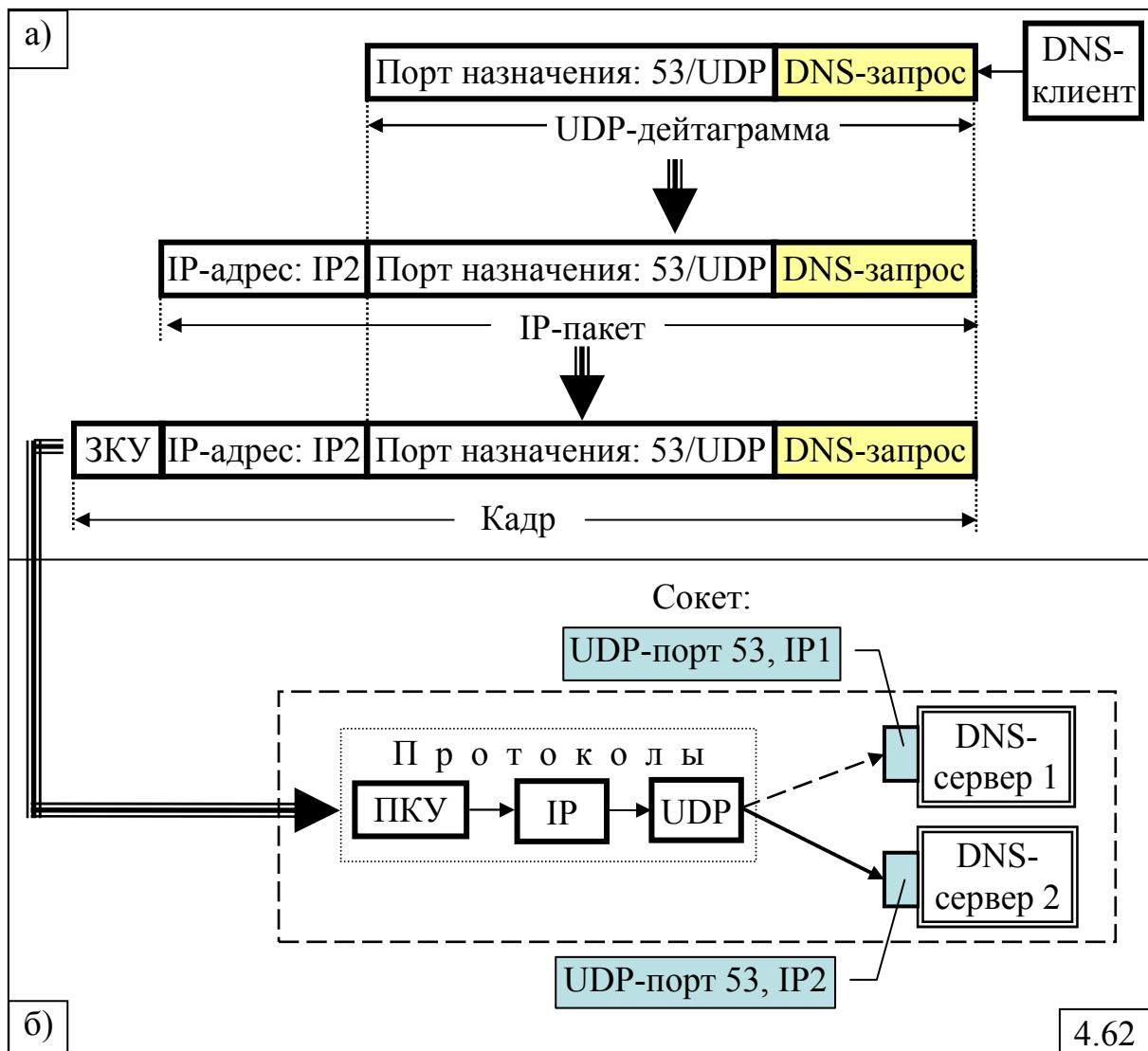


Рис.4.62,а) иллюстрирует процесс формирования DNS-клиентом запроса к DNS-серверу.

DNS-запрос транспортном уровне стека протоколов TCP/IP передаётся протоколу UDP, который вкладывает этот запрос в UDP-дейтаграмму и указывает в заголовке порт назначения 53/UDP. Затем UDP-дейтаграмма передаётся на межсетевой уровень, где она вкладывается в IP-пакет, заголовок которого содержит «IP-адрес: IP2». IP-пакет, в свою очередь, передаётся на уровень «межсетевой интерфейс», где он помещается в кадр канального уровня с соответствующим заголовком канального уровня (ЗКУ). Этот кадр передаётся по сети к компьютеру, содержащему два DNS-сервера (рис.4.62,б).

В этом компьютере протокол канального уровня (ПКУ) снимает заголовок ЗКУ и передаёт содержимое кадра на межсетевой уровень протоколу IP, который, в свою очередь, извлекает содержимое (UDP-дейтаграмму) из IP-пакета. Дальнейшие манипуляции с передаваемыми данными отличаются от принципов, заложенных в многоуровневую модель иерархии протоколов. Вместо того чтобы просто передать UDP-дейтаграмму, находящуюся в поле данных IP-пакета, транспортному уровню, *IP-протокол присоединяет к UDP-дейтаграмме* так называемый **псевдозаголовок**, содержащий среди прочего IP-адреса отправителя и получателя. Таким образом, протокол UDP, имея IP-адрес и порт назначения, однозначно определяет, что содержимое поля данных (то есть DNS-запрос), должно быть передано приложению «DNS-сервер 2».

Назначение и формат псевдозаголовка, который используется также и в TCP-сегменте, описаны в п.4.4.8.3.

#### 4.4.8.2. Транспортный протокол TCP

Протокол TCP обеспечивает надежную передачу данных между прикладными процессами за счет установления логических соединений между взаимодействующими процессами.

**Логическое соединение** между двумя прикладными процессами идентифицируется парой сокетов (IP-адрес, номер порта), каждый из которых описывает один из взаимодействующих процессов.

Информация, поступающая к протоколу TCP в рамках логического соединения от протоколов более высокого уровня, рассматривается протоколом TCP как *неструктурированный поток байтов* и заносится в буфер. Для передачи на сетевой уровень из буфера вырезается **сегмент**, не превосходящий 64 Кбайт (максимального размера IP-пакета). На практике обычно длина сегмента ограничивается значением 1460 байтами, что позволяет поместить его в кадр Ethernet с заголовками TCP и IP.

Соединение TCP ориентировано на *полнодуплексную передачу*.

Управление потоком данных в протоколе TCP осуществляется с использованием механизма **скользящего окна переменного размера**. При передаче сегмента узел-отправитель включает таймер и ожидает подтверждения. Отрицательные квитанции не посыпаются, а используется *механизм тайм-аута*. Узел назначения, получивший сегмент формирует и посыпает обратно сегмент (с данными, если они есть, или без данных) с номером подтверждения, равным следующему порядковому *номеру ожидаемого байта*. В отличие от многих других протоколов, протокол TCP подтверждает получение *не пакетов, а байтов* потока. Если время ожидания подтверждения истекает, отправитель посыпает сегмент еще раз.

Несмотря на кажущуюся простоту протокола, в нем имеется ряд нюансов, которые могут привести к некоторым проблемам.

Во-первых, поскольку сегменты при передаче по сети могут фрагментироваться, возможна ситуация, при которой часть переданного сегмента будет принята, а остальная часть окажется потерянной.

Во-вторых, сегменты могут прибывать в узел назначения в произвольном порядке, что может привести к ситуации, при которой байты с 2345 по 3456 уже прибыли, но подтверждение для них не может быть выслано, так как байты с 1234 по 2344 еще не получены.

В-третьих, сегменты могут задержаться в сети так долго, что у отправителя истечёт интервал ожидания, и он передаст их снова. Переданный повторно сегмент может пройти по другому маршруту и может быть иначе фрагментирован, или же сегмент может по дороге случайно попасть в перегруженную сеть. В результате для восстановления исходного сегмента потребуется достаточно сложная обработка

На рис.4.63 представлен формат заголовка TCP-сегмента. Первые 20-байт заголовка имеют строго фиксированный формат, за которым могут находиться дополнительные поля. После дополнительных полей заголовка размещается поле данных, содержащее не более 65 495 байт, которое вместе с TCP- и IP-заголовками размером по 20 байт даст максимально допустимый размер IP-пакета в 65 535 байт.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
																Порт отправителя								Порт получателя							
																Порядковый номер															
																Номер подтверждения (следующий ожидаемый байт)															
Длина TCP- загол.	Резерв	U	A	P	R	S	F	Размер окна																							
		R	C	S	S	Y	I													G	K	H	T	N	N						
Контрольная сумма																Указатель на срочные данные															
Параметры (0 или более 32-разрядных слов)																															

4.63

Не вдаваясь в детали, рассмотрим кратко назначение фиксированных полей заголовка TCP-сегмента.

Поля «Порт отправителя» (2 байта) и «Порт получателя» (2 байта) идентифицируют *процессы*, между которыми установлено логическое соединение.

Поле «Порядковый номер» (4 байта) содержит *номер первого байта* данных в сегменте, который определяет смещение сегмента относительно потока передаваемых данных

Поле «Номер подтверждения» (4 байта) содержит *номер следующего ожидаемого байта*, который используется в качестве квитанции, подтверждающей правильный приёма всех предыдущих байтов.

Поле «Длина TCP-заголовка» (4 бита) задаёт длину заголовка TCP-сегмента, измеренную в 32-битовых словах.

Поле «Резерв» длиной 6 бит зарезервировано на будущее.

Однобитовые **флаги** несут служебную информацию о типе сегмента и интерпретируются следующим образом:

URG=1 указывает на наличие *срочных данных*, что означает использование поля «Указатель на срочные данные»;

ACK=1 означает, что сегмент является *квитанцией* на принятый сегмент и поле «Номер подтверждения» содержит осмысленные данные. В противном случае данный сегмент не содержит подтверждения и поле «Номер подтверждения» просто игнорируется.

PSH=1 (PUSH-флаг) означает *запрос на отправку данных* без ожидания заполнения буфера;

RST=1 используется для *броса состояния соединения* при обнаружении проблем, а также для отказа от неверного сегмента или от попытки создать соединение;

SYN=1 используется для *установки соединения*, при этом если ACK=0, то это означает, что поле подтверждения не используется;

FIN=1 используется для *разрыва соединения*.

Поле «Размер окна» (2 байта) определяет, сколько байт может быть послано после байта, получившего подтверждение.

Поле «Контрольная сумма» (2 байта) содержит контрольную сумму, которая охватывает заголовок, данные и *псевдозаголовок*.

**Алгоритм вычисления контрольной суммы** выглядит следующим образом.

Перед началом вычисления контрольной суммы значение этого поля устанавливается равным нулю. Если поле данных содержит нечётное число байтов, то оно дополняется нулевым байтом, который используется при подсчёте контрольной суммы, но не вставляется в сегмент для передачи в сети. Необходимость такого добавления обусловлена тем, что TCP-сегмент, включающий заголовок, данные и псевдозаголовок, рассматривается как совокупность 16-разрядных двоичных чисел, которые складываются в дополнительном коде, а затем вычисляется дополнение для полученной суммы, которое заносится в поле «Контрольная сумма». Получатель сегмента аналогичным образом подсчитывает контрольную сумму для всего сегмента, включая поле «Контрольная сумма». Очевидно, что полученный таким образом результат должен быть равен 0. Отметим, что дополнительный нулевой байт

Поле «Указатель на срочные данные» (2 байта) содержит смещение в байтах от текущего порядкового номера байта до места расположения срочных данных, которые необходимо срочно принять, несмотря на переполнение буфера. Таким образом, в протоколе TCP реализуются прерывающие сообщения. Содержимым срочных данных занимается прикладной уровень. Протокол TCP лишь обеспечивает их доставку и не интересуется причиной прерывания.

Поле «Параметры» имеет переменную длину и может отсутствовать.

Примерами приложений, использующих протокол TCP для передачи данных, являются FTP, TFTP, DNS, POP3, IMAP, TELNET.

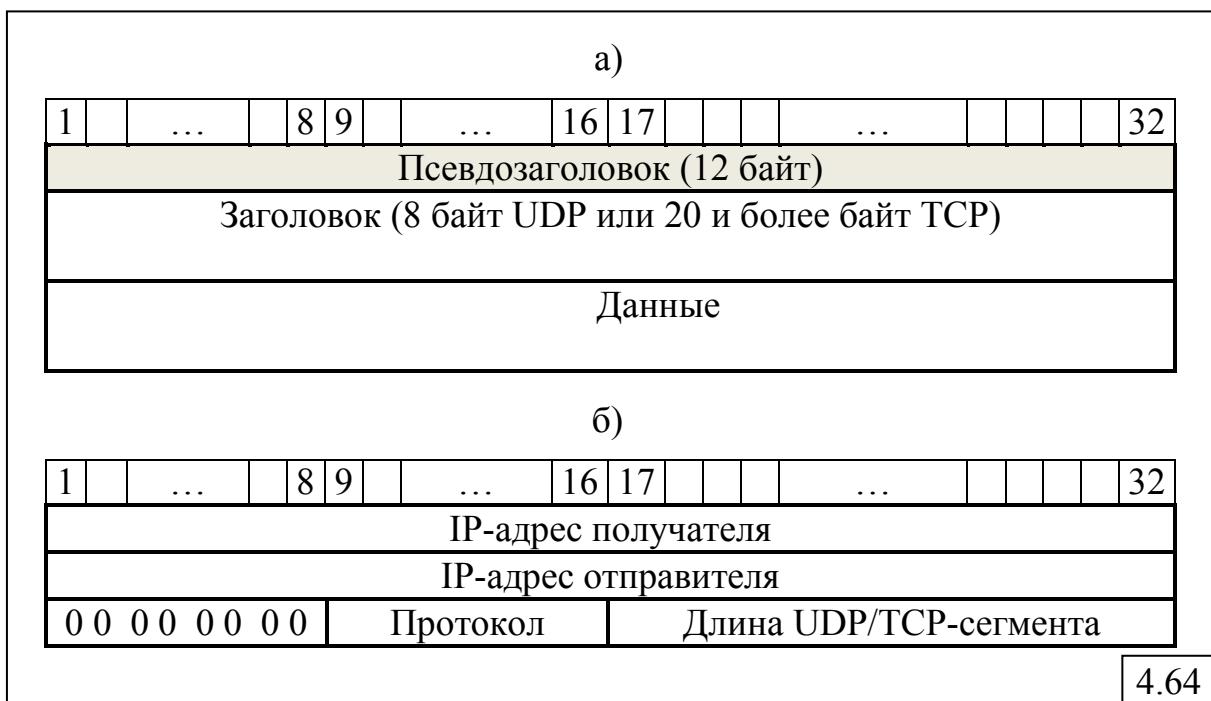
#### 4.4.8.3. Псевдозаголовок протоколов UDP и TCP

Как сказано выше, при передаче данных от нижележащего межсетевого уровня на транспортный уровень в заголовки UDP-дейтаграмм и TCP-сегментов включается псевдозаголовок, который располагается перед основным заголовком транспортного уровня. Таким образом, блок данных транспортного уровня (UDP-дейтаграмма или TCP-сегмент) будет содержать (рис.4.64,а):

- псевдозаголовок длиной 12 байт или 3 32-разрядных слова;
  - заголовок длиной 8 байт для UDP-дейтаграммы или 20 и более байт для TCP-сегмента;
  - данные

Псевдозаголовок, формат которого показан на рис.4.64,б, содержит:

- IP-адрес отправителя;
  - IP-адрес получателя;
  - нулевое поле, не используемое и заполненное нулями;
  - поле «Протокол», содержащее номер протокола транспортного уровня: 17 для протокола UDP и 6 для протокола TCP;
  - длина UDP-дейтаграммы или TCP-сегмента.



Включение псевдозаголовка в контрольную сумму блока данных транспортного протокола помогает обнаружить неверно доставленные пакеты за счёт двойной проверки, выполняемой протоколом IP и протоколами транспортного уровня. Кроме того, передача IP-адресов транспортному уровню позволяет однозначно разрешить ситуацию, показанную на рис.4.62, когда две копии одного и того же приложения используют одинаковый номер порта.

Узел-отправитель при формировании TCP-сегмента рассчитывает контрольную сумму сегмента с учётом псевдозаголовка. Однако при

передаче по сети псевдозаголовок не включается в сегмент, что позволяет уменьшить накладные расходы и, соответственно, повысить эффективную скорость передачи пользовательских данных. В узле-получателе протокол IP формирует псевдозаголовок и вставляет его в поступивший сегмент и передаёт транспортному уровню.

#### **4.4.9. Управляющий протокол ICMP**

Internet Control Message Protocol (ICMP) – **протокол межсетевых управляющих сообщений** предназначен для выявления и обработки нештатных событий (например, потеря пакета), заключающейся в определении типа ошибки, формировании сообщения о ней и передаче этого сообщения приложению, сформировавшему пакет.

К основным функциям протокола ICMP относятся:

- обмен тестовыми сообщениями для выяснения наличия и активности узлов сети;
- анализ достижимости узла-получателя и сброс пакетов, направляемых к недоступимым узлам;
- изменение маршрутов;
- уничтожение пакетов с истекшим временем жизни;
- синхронизация времени в узлах сети;
- управление потоком путем регулирования частоты посылки пакетов узлами-источниками.

Основные типы ICMP-сообщений:

- «адресат недоступен» – пакет не может быть доставлен;
- «время истекло» – время жизни пакета достигло нуля;
- «проблема с параметром» – ошибка в поле заголовка;
- «переадресовать» – научить маршрутизатор;
- «запрос отклика» – запрос: жив ли компьютер?;
- «отклик» – да, жив.

Одной из наиболее интересных среди перечисленных функций является изменение маршрутов: если некоторый маршрутизатор определяет, что хост использует неоптимальный путь для доставки пакета, он при помощи протокола ICMP может скорректировать маршрутную таблицу хоста. Это один из механизмов автоматической оптимизации и адаптации сетей TCP/IP к изменениям топологии.

ICMP-пакеты инкапсулируются в IP пакеты. ICMP является неотъемлемой частью IP, но при этом не делает протокол IP средством надёжной доставки сообщений. Для этих целей существует протокол TCP.

#### **4.4.10. Протоколы канального уровня для выделенных линий**

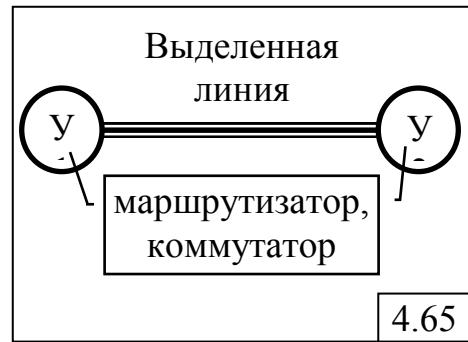
Протоколы канального уровня для выделенных линий (рис.4.65) должны:

- обеспечивать надежную передачу;

- предоставлять возможность управления потоком кадров для предотвращения переполнения соседних узлов.

Протоколы канального уровня:

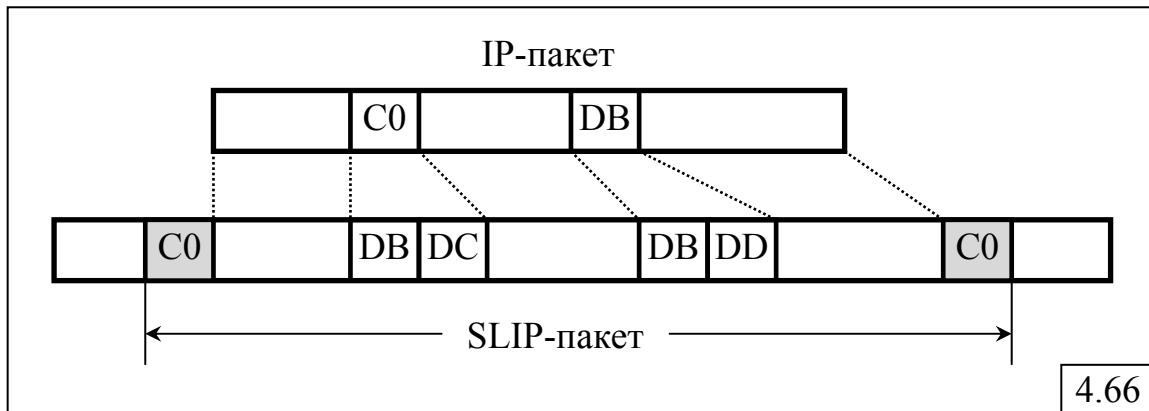
- SLIP;
- протоколы семейства HDLC;
- PPP.



#### 4.4.10.1. Протокол *SLIP*

**SLIP (Serial Line IP)** – первый стандарт для протоколов TCP/IP, который может использоваться как для коммутируемых, так и для выделенных каналов ввиду простоты.

SLIP поддерживается только протоколом сетевого уровня IP. Основная и единственная функция протокола SLIP – распознавание начала и конца IP-пакета в потоке бит. Для этого в качестве границ IP-пакета используется специальный символ END (шестнадцатеричный код – C0<sub>16</sub>). Если в IP-пакете встречается код C0<sub>16</sub>, то используется процедура *байт-страффинга* (рис.4.66), заключающаяся в следующем. Код C0<sub>16</sub> заменяется на коды DB<sub>16</sub> и DC<sub>16</sub>, а код DB<sub>16</sub> заменяется на DB<sub>16</sub> и DD<sub>16</sub>.



К недостаткам протокола SLIP относятся:

- отсутствие возможности обмениваться адресной информацией;
- использование только IP-пакетов в качестве содержимого SLIP-пакета;
- отсутствие процедур обнаружения и коррекции ошибок.

#### 4.4.10.2. Протоколы семейства *HDLC*

**HDLC (High-level Data Link Control Procedure)** – высокоуровневый протокол управления каналом – стандарт ISO для выделенных линий. Представляет собой *семейство протоколов LAP* (Link Access Protocol), включающее следующие протоколы:

- **LAP-B** – для сетей X.25 (B – Balanced);
- **LAP-D** – для сетей ISDN (D – D-channel);
- **LAP-M** – для модемов (M – Modem);

- **LAP-F** – для сетей Frame Relay (F – Frame Relay).

HDLC относится к бит-ориентированным протоколам и использует кадр, формат которого показан на рис.4.67.



В качестве обрамления кадра, служащих границами между передаваемыми кадрами, используется специальная последовательность из 8 бит (байт): 01111110, называемая **флагом**. Благодаря наличию флагов нет необходимости указывать длину кадра. Для того, чтобы отличать последовательность бит 01111110, находящуюся в поле данных от флага применяется процедура **бит-стаффинга**.

Поле **Адрес** имеет длину 1 или 2 байта и при наличии нескольких узлов-приёмников используется для идентификации конкретного узла, а в двухточечном соединении – для того, чтобы отличить команды от ответов, а также для указания направления передачи кадра по интерфейсу «пользователь – сеть».

Поле **Данные** может быть любой длины и содержать пакеты протоколов вышележащих уровней. Это поле может отсутствовать в управляющих кадрах и некоторых ненумерованных кадрах.

Поле **КС** (контрольная сумма) содержит *остаток избыточной циклической суммы*, вычисленной с помощью полиномов типа CRC.

Поле **У** (*управление*) имеет длину 1 или 2 байта и содержит служебную информацию. Структура и содержимое этого поля зависят от типа передаваемого HDLC-кадра.

Существуют 3 типа HDLC-кадров, различающиеся содержимым поля **У** (*управление*), показанного на рис.4.68:

- *информационные кадры* длиной 1 или 2 байта (рис.4.68,а), предназначенные для передачи данных пользователя;
- *управляющие* или *супервизорные кадры* длиной 1 или 2 байта (рис.4.68,б), предназначенные для передачи команд и ответов в процессе установленного логического соединения;
- *ненумерованные кадры* длиной 1 байт (рис.4.68,в), предназначенные для установления и разрыва логического соединения, а также информирования об ошибках.

Тип кадра определяется первыми битами поля управления: 0 – информационный кадр; 10 – управляющий кадр; 11 – ненумерованный кадр.

Протокол HDLC для обеспечения надёжности передачи данных использует механизм скользящего окна, ширина которого составляет:

- 7 кадров при длине поля управления в 1 байт;
- 127 кадров при длине поля управления в 2 байта.

a)	<table border="1"> <tr> <td>0</td><td>N(S)</td><td>P/F</td><td>N(R)</td></tr> </table>	0	N(S)	P/F	N(R)	1	3/7	1	3/7	бит	
0	N(S)	P/F	N(R)								
б)	<table border="1"> <tr> <td>1</td><td>0</td><td>Type</td><td>P/F</td><td>N(R)</td></tr> </table>	1	0	Type	P/F	N(R)	1	1	2/6	1	3/7
1	0	Type	P/F	N(R)							
в)	<table border="1"> <tr> <td>1</td><td>1</td><td>Type</td><td>P/F</td><td>Modifier</td></tr> </table>	1	1	Type	P/F	Modifier	1	1	2	1	3
1	1	Type	P/F	Modifier							

4.68

Для реализации механизма скользящего окна в **информационном кадре** предусмотрено 2 поля:

- поле **N(S)**, содержащее порядковый номер передаваемого кадра;
- поле **N(R)**, содержащее номер очередного ожидаемого кадра.

Наличие этих двух полей связано с реализацией дуплексной передачи данных, а их длина определяет ширину окна в 7 (при длине 3 бита) или 127 (при длине 7 бит) кадров.

Бит **P/F** (Poll/Final – Опрос/Финал) используется для указания промежуточного (P) или последнего передаваемого (F) кадра. В некоторых случаях этот бит может использоваться для указания другому узлу о необходимости передать управляющий кадр, не ожидая попутного потока данных.

**Управляющие кадры** могут быть 4-х типов, которые различаются значением поля **Type**:

- Type=0** – подтверждение (RESEIVE READY – к приёму готов) – передаёт в поле **N(R)** номер следующего ожидаемого кадра и используется при отсутствии попутного потока данных для передачи подтверждения;
- Type=1** – отрицательное подтверждение (REJECT – отказ) – передаёт в поле **N(R)** номер неверно полученного кадра, начиная с которого узел-отправитель должен повторить передачу кадров;
- Type=2** – отказ (RESEIVE NOT READY – к приёму не готов) – означает, что в узле-получателе возникли проблемы, не позволяющие принимать кадры (например, переполнена буферная память) и, соответственно, узел-отправитель должен приостановить передачу кадров, при этом в поле **N(R)** указывается номер кадра, начиная с которого узел-отправитель в дальнейшем (после устранения причины приостановки приёма кадров) должен будет повторить передачу кадров;
- Type=3** – выборочное подтверждение (SELECTIVE REJECT – выборочный отказ) – передаёт в поле **N(R)** номер только того кадра, передачу которого узел-отправитель должен повторить.

**Ненумерованные кадры** применяются в основном для служебных целей, но могут переносить и данные, когда требуется ненадёжный не требующий соединения сервис. Поля **Type** и **Modifier** определяют типы и

модификации команд, используемых двумя узлами на этапе установления соединения. Примерами таких команд могут служить:

- запрос на установление соединения с использованием двухбайтовых полей управления для информационных и управляющих кадров: SABME (Set Asynchronous Balanced Mode Extended – установить асинхронный сбалансированный расширенный режим);
- подтверждение установления или разрыва соединения: UA (Unnumbered Acknowledgment – ненумерованная положительная квитанция);
- запрос на разрыв соединения: REST (Resetting connection – сброс соединения).

Одна из основных функций протоколов семейства HDLC – восстановление искаженных и потерянных кадров (уменьшение вероятности искажения бита – BER с  $10^{-3}$  –  $10^{-4}$  до  $10^{-9}$ ). Для современных каналов высокого качества, обеспечивающих значение  $BER=10^{-8}$  –  $10^{-9}$ , использование протоколов семейства HDLC на уровне моста или маршрутизатора становится нецелесообразным.

#### 4.4.10.3. Протокол PPP

**PPP (Point-to-Point Protocol)** – протокол двухточечного соединения, заменивший протокол SLIP и построенный на основе формата кадров протоколов семейства HDLC с дополнением собственных полей.

Протокол PPP является стандартным протоколом Интернета и также, как протокол HDLC, представляет собой семейство протоколов, включающее в том числе:

- LCP (Link Control Protocol) – протокол управления соединением;
- NCP (Network Control Protocol) – протокол управления сетью;
- MLP PPP (Multi Link PPP) – многоканальный протокол PPP.

Протокол PPP основан на четырех принципах:

- переговорное принятие параметров соединения;
- многопротокольная поддержка;
- расширяемость протокола;
- независимость от глобальных служб.

В отличие от бит-ориентированного протокола HDLC, протокол PPP является *байт-ориентированным*, что означает посимвольное заполнение кадра, то есть все кадры состоят из целого числа байтов. Полный формат кадра PPP для работы в ненумерованном режиме показан на рис.4.69.

Флаг	Адрес	У	Протокол	Данные	КС	Флаг
01111110	11111111	00000011				01111110
1	1	1	1/2	-	2/4	1 байт

4.69

Характерными для PPP-кадра являются следующие особенности.

1. Если в поле **Данные** встречается байт 01111110, совпадающий с кодом флага, то используется процедура *байт-стаффинга*, рассмотренная выше.

2. Поле **Адрес** всегда содержит значение 11111111, что означает, что все станции должны принимать этот кадр и позволяет избежать необходимости назначения адресов для передачи данных.

3. Поле **управления У** по умолчанию содержит значение 00000011, означающее ненумерованный кадр.

4. Поле **Протокол** содержит код протокола вышележащего уровня, пакет которого вложен в поле данных. Длина этого поля по умолчанию составляет 2 байта, но путём переговоров длина может быть уменьшена до 1 байта.

5. Поле **Данные** может быть переменной длины, вплоть до некоторого установленного пользователями максимального значения, которое по умолчанию обычно составляет 1500 байт.

6. Поле **контрольной суммы КС** по умолчанию имеет длину 2 байта, которая в случае необходимости по договорённости может быть увеличена до 4-х байтов.

7. Установление соединения между двумя узлами сопровождается сложной переговорной процедурой принятия параметров соединения, таких как качество линии связи, размер передаваемых кадров, тип протокола аутентификации и т.д. Эта переговорная процедура реализуется протоколом управления линией связи LCP.

8. Протокол PPP реализует многопротокольную поддержку, обеспечивая внутри одного соединения передачу пакетов различных протоколов сетевого (IP, IPX, XNS и т.д.) и канального уровня ЛВС.

## 4.5. MPLS-технология

### 4.5.1. Основные принципы MPLS-технологии

**MPLS** – *MultProtocol Label Switching* – многопротокольная коммутация на основе меток объединяет два способа передачи пакетов: дейтаграммный и «виртуальный канал».

В основе MPLS-технологии лежит технология IP-коммутации (IP-Switching), предложенная в середине 90-х годов компанией IPSILON, которая для её реализации разработала специальное комбинированное устройство IP/ATM, представляющее собой ATM-коммутаторы со встроенными блоками IP-маршрутизации. Эти устройства были предназначены для уменьшения задержек при передаче кратковременных потоков данных за счёт отказа от предварительной процедуры установления виртуального канала, как это происходит в ATM-сетях. Для этого IP-пакет, принадлежащий кратковременному потоку, разбивался устройством IP/ATM на ATM-ячейки, которые передавались от одного устройства IP/ATM к другому. В то же время, долговременные потоки

передавались традиционным для ATM-технологии способом – с предварительным установлением виртуального канала.

Дальнейшие усовершенствования IP-коммутации привели в конце 90-годов прошлого века к созданию технологии MPLS, объединяющей достоинства техники виртуальных каналов и стека протоколов TCP/IP за счёт применения специального сетевого устройства – **коммутирующего по меткам маршрутизатора LSR (Label Switch Router)**, выполняющего функции *IP-маршрутизатора и коммутатора виртуальных каналов*.

#### 4.5.2. Маршрутизатор LSR и таблица продвижения

В основе MPLS лежит принцип передачи на основе меток. Любой передаваемый пакет ассоциируется с тем или иным *классом сетевого уровня* (Forwarding Equivalence Class, FEC), каждый из которых идентифицируется определенной меткой. Значение метки уникально лишь для участка пути между соседними узлами сети MPLS, которыми являются LSR. Метка передается в составе любого пакета, причем способ ее привязки к пакету зависит от используемой технологии канального уровня.

LSR получает топологическую информацию о сети, участвуя в работе алгоритма маршрутизации (OSPF, BGP, IS-IS). Затем он начинает взаимодействовать с соседними LSR, распределяя метки, которые в дальнейшем будут применяться для коммутации. Обмен метками может производиться с помощью как специального **протокола распределения меток LDP (Label Distribution Protocol)**, так и модифицированных версий протоколов сигнализации в сети (например, видоизмененных протоколов маршрутизации, резервирования ресурсов RSVP и др.).

Распределение меток между LSR приводит к установлению внутри домена MPLS **путей с коммутацией по меткам LSP (Label Switching Path)**, которые хранятся в каждом маршрутизаторе LSR в виде таблицы продвижения (рис.4.70), содержащей следующие столбцы:

- **входной интерфейс** – интерфейс (порт), по которому пакет поступил в LSR;
- **метка** – идентификатор (метка), который идентифицирует принадлежность поступившего пакета к конкретному трафику;
- **следующий хоп** – интерфейс (порт), в который должен быть направлен пакет;
- **действие** – указатель, определяющий, какое действие должно быть применено к метке (заменить, удалить).

Вх. интерфейс	Метка	След.хоп	Действие
I1	121	I2	211
I2	164	I3	274

4.70

В поле «Действие» таблицы продвижения указываются основные операции с метками:

- Push – поместить метку в стек;
- Swap – заменить текущую метку новой;
- Pop – удаление верхней метки.

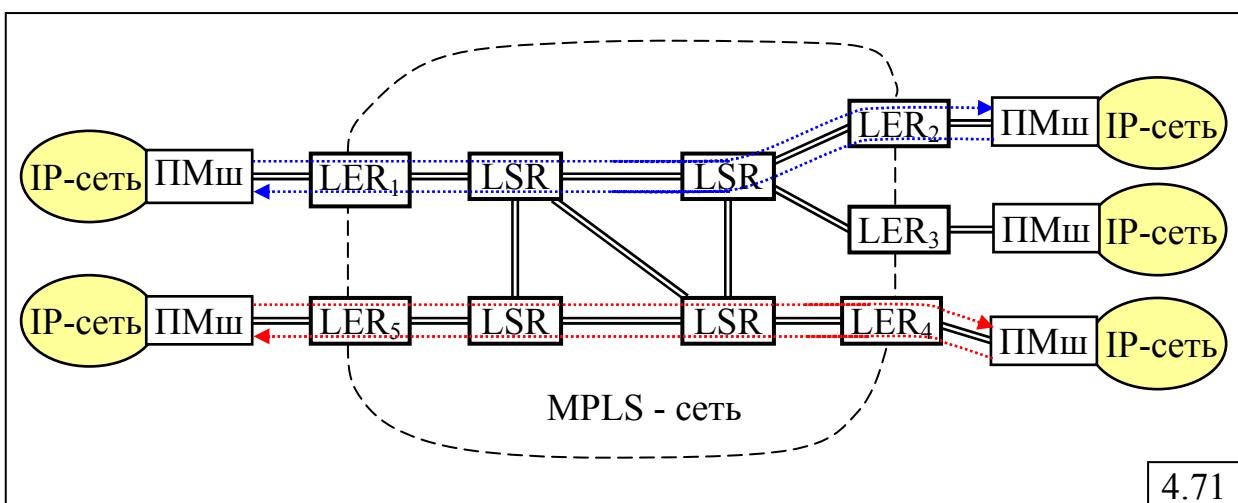
Получая пакет, LSR по номеру интерфейса, на который пришел пакет, и по значению привязанной к пакету метки определяет для него выходной интерфейс. Старое значение метки заменяется новым, содержащимся в поле «действие» таблицы, и пакет отправляется к следующему устройству на пути LSP.

Вся операция требует лишь одноразовой идентификации значений полей в одной строке таблицы. Это занимает гораздо меньше времени, чем сравнение IP-адреса отправителя с наиболее длинным адресным префиксом в таблице маршрутизации, которое используется при традиционной маршрутизации.

На рис.4.71 показан пример MPLS-сети, находящейся в окружении IP-сетей. Каждая IP-сеть соединяется через *пограничный маршрутизатор* (ПМш) с *пограничным коммутирующим по меткам маршрутизатором LER* (Label switch Edge Router), который выполняет следующие функции:

- классификация пакетов по различным *классам эквивалентного продвижения* (FEC – Forwarding Equivalence Class), имеющих один и тот же следующий хоп;
- реализация таких дополнительных сервисов, как фильтрация, явная маршрутизация, выравнивание нагрузки и управление трафиком.

В результате интенсивные вычисления приходятся на граничную область MPLS-сети, а высокопроизводительная коммутация выполняется в ядре, содержащем множество LSR.

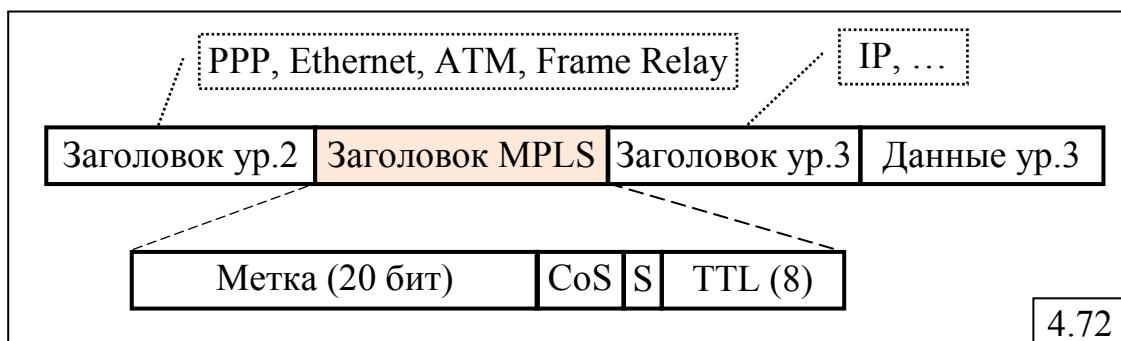


#### 4.5.3. Заголовок MPLS

Заголовок MPLS длиной 32 бита вставляется между заголовками 2-го и 3-го уровня OSI-модели, что даёт повод говорить, что MPLS – это технология уровня 2,5.

Заголовок MPLS содержит (рис.4.72) следующие поля:

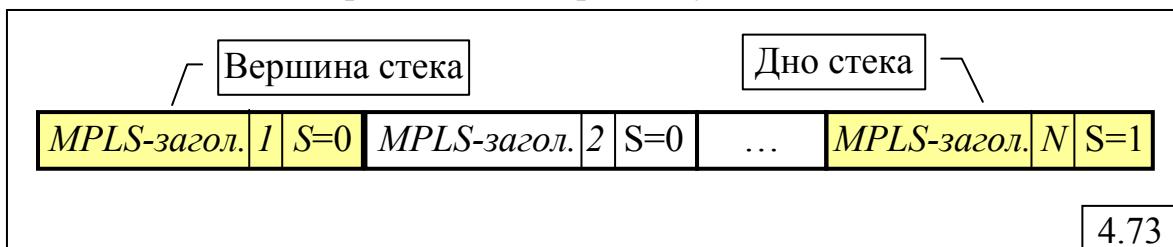
- **метка** (20 бит), на основе которой осуществляется коммутация пакетов в MPLS-сети;
- **CoS** (Class of Service) – класс обслуживания (3 бита), указывающий класс трафика, требующего определённого показателя QoS;
- **S** – признак дна стека меток (1 бит), используемый для организации агрегированных путей LSP при прохождении пакетом через несколько MPLS-сетей;
- **TTL** (Time To Live) – время жизни пакета (8 бит), дублирующее аналогичное поле IP-пакета, что позволяет маршрутизаторам LSR отбрасывать пакеты с истекшим временем жизни.



#### 4.5.4. Многоуровневая коммутация по меткам

Для создания системы агрегированных путей LSP с любым количеством уровней иерархии заголовок MPLS-кадра формируется в виде **стека меток**, включающего столько заголовков MPLS, сколько уровней иерархии содержит агрегированный путь (рис.4.73). При этом различают:

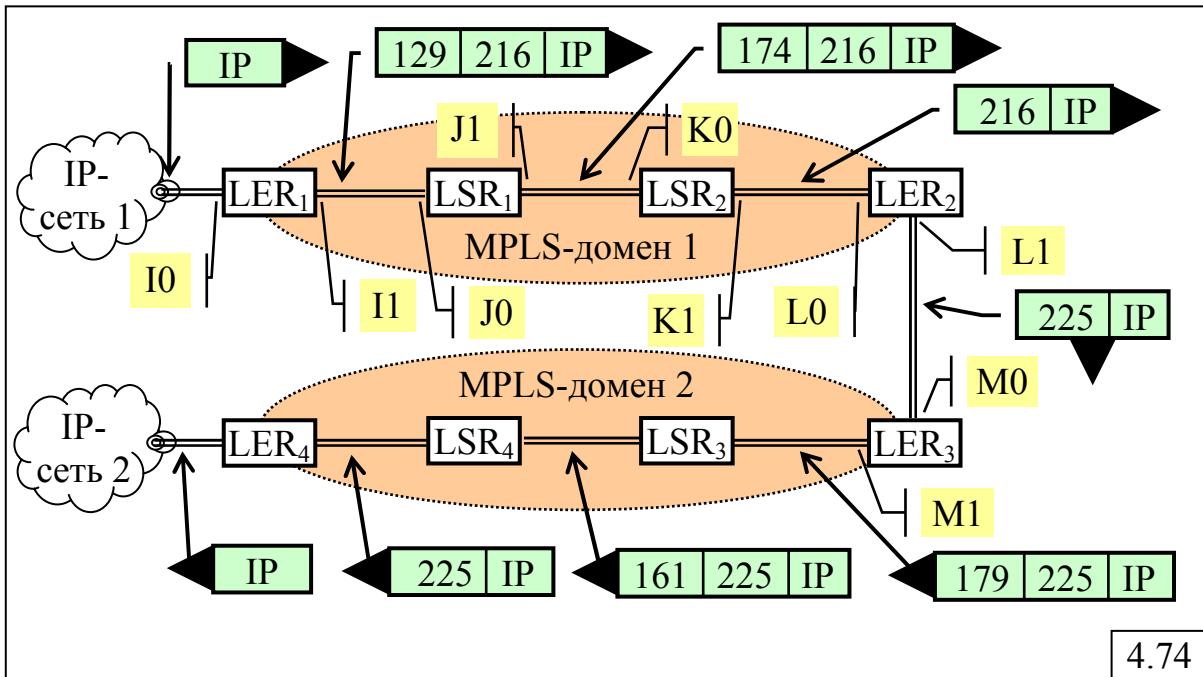
- **вершину стека**, над которым всегда выполняются действия, указанные в таблице продвижения;
- **дно стека**, признаком которого служит значение поля S=1.



Организация стека меток необходима для организации **многоуровневой коммутации по меткам**, когда пакеты передаются не только внутри каждого MPLS-домена, но и между разными MPLS-доменами, обслуживаемых разными поставщиками услуг. С помощью стека меток может быть реализован механизм *туннелирования*.

Рассмотрим механизм формирования многоуровневой коммутации с использованием стека меток на примере сети, показанной на рис.4.74.

Положим, что на пути передачи **IP-пакета из IP-сети 1 в IP-сеть2** имеются 2 **MPLS-домена**, в каждом из которых пакет проходит через 2 пограничных маршрутизатора LER и 2 маршрутизатора LSR.



Соответствующие фрагменты таблиц продвижения пакетов маршрутизаторов LER1, LSR1, LSR2 и LER2, для наглядности объединённые в одну таблицу, представлены на рис.4.75.

Маршрутизатор	Входной интерфейс	Метка	Следующий хоп	Действия
LER1	...			
	I0	-	I1	216   Push   129
	...			
LSR1	...			
	J0	129	J1	Swap 174
	...			
LSR2	...			
	K0	174	K1	Pop
	...			
LER2	...			
	L0	216	L1	Swap 225
	...			

4.75

IP-пакет из IP-сети 1 по интерфейсу I0 попадает в пограничный маршрутизатор LER1, где в заголовок IP-пакета будет вставлен MPLS-заголовок. В соответствии с таблицей продвижения маршрутизатора LER1 будет сформирован MPLS-заголовок, в поле метки которого будет установлено значение 216. Затем действие Push приведёт к формированию второго MPLS-заголовка, который станет вершиной стека, в поле метки которого будет установлено значение 129. Таким образом, появится стек из двух MPLS-заголовков (см. рис.4.74), причём во втором заголовке

признак дна стека S будет установлен в 1. Далее этот пакет направляется на интерфейс I1, через который он попадёт в маршрутизатор LSR1.

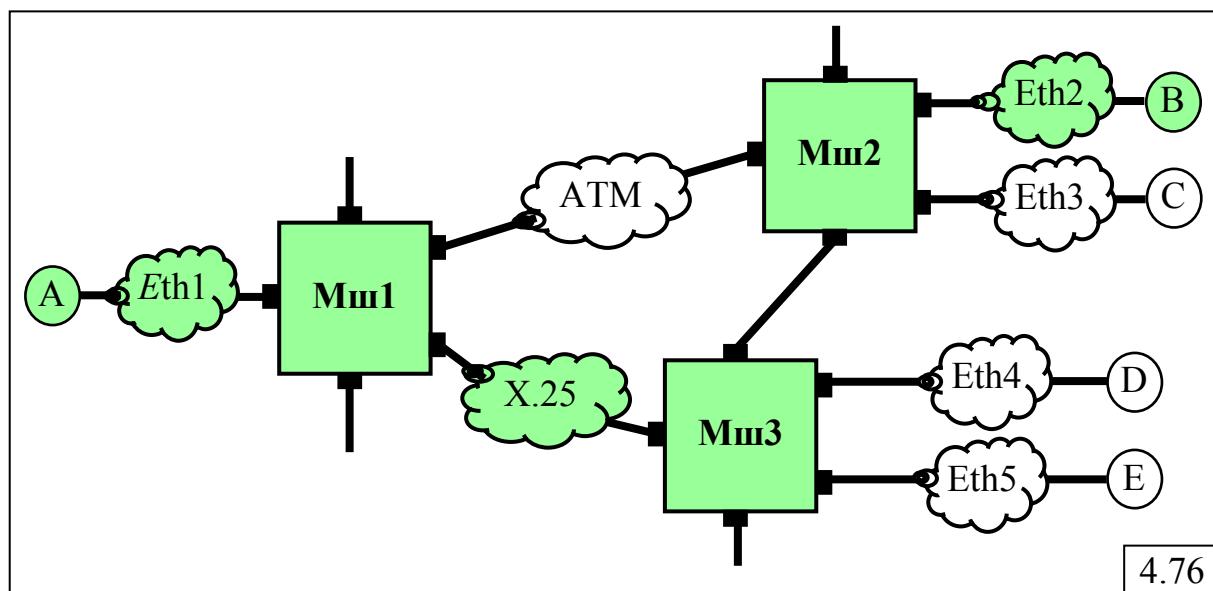
В соответствии с таблицей продвижения LSR1 поступивший по интерфейсу J0 пакет с меткой 129 должен быть направлен в выходной интерфейс J1, при этом метка 129, находящаяся в вершине стека, должна быть заменена на 174 (действие Swap 174).

В маршрутизаторе LSR2 будет удалена (действие Pop) верхняя метка 174, а в пограничном маршрутизаторе LER2 метка 216 будет заменена на 225 (действие Swap 225).

Дальнейшее продвижение пакета и изменения MPLS-заголовка происходят аналогичным образом (см. рис 4.74).

#### 4.6. Пример передачи данных в составной сети

В заключение рассмотрим подробный пример, иллюстрирующий процесс формирования протокольных блоков данных на разных уровнях управления передачей данных в составной сети (рис.4.76), использующей стеки протоколов TCP/IP.



Составная сеть с помощью трёх маршрутизаторов (Мш1, Мш2, Мш3) объединяет сеть ATM-сеть, X.25 и 5 локальных сетей Ethernet (Eth1, Eth2, Eth3, Eth4, Eth5), к которым подключены пользователи (компьютеры) A, B, C, D, E.

##### 4.6.1. Система обозначений

Введём следующие обозначения

- IP- и MAC-адрес *компьютера*:  
**IP.<имя компьютера>**  
**MAC.<имя компьютера>**
- IP- и MAC-адрес *порта маршрутизатора*:  
**IP.<номер маршрутизатора>.<номер порта>**  
**MAC.<номер маршрутизатора>.<номер порта>**

- заголовок используемого в сети *кадра* (пакета, ячейки):  
**3\_<имя сети>**

Например:

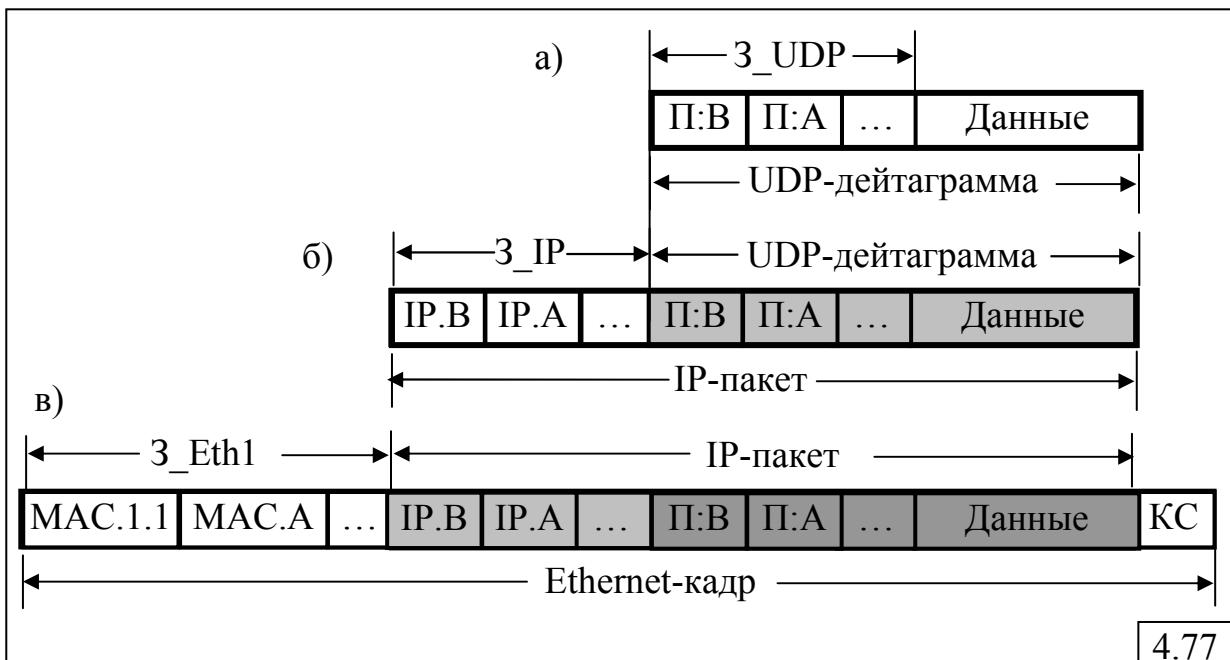
- IP- и MAC-адрес компьютера **A** будут иметь вид:  
**IP.A** и **MAC.A**,
- IP- и MAC-адрес порта 2 маршрутизатора **Мш1** будут иметь вид:  
**IP.1.2** и **MAC.1.2**
- заголовок используемого в сети **Eth1** кадра:  
**3\_Eth1**

Рассмотрим поэтапно, как изменяется протокольный блок данных в зависимости от среды передачи в процессе доставки данных от узла (компьютера) **A** к узлу **B**. Для определённости положим, что для передачи данных из конца в конец используется транспортный протокол UDP.

#### 4.6.2. Формирование данных в узле-источнике

1. Данные, подлежащие передаче, направляются от соответствующего приложения, реализуемого на прикладном уровне в компьютере **A**, на транспортный уровень, где формируется UDP-дейтаграмма (рис.4.77,а), в заголовке **3\_UDP** которой указываются номера двух портов – *получателя (П:В)* и *отправителя (П:А)*.

2. UDP-дейтаграмма передаётся протоколу IP, который вкладывает её в IP-пакет (рис.4.77,б), в заголовке **3\_IP** которого указываются IP-адреса *получателя (IP.В)* и *отправителя (IP.А)*.



4.77

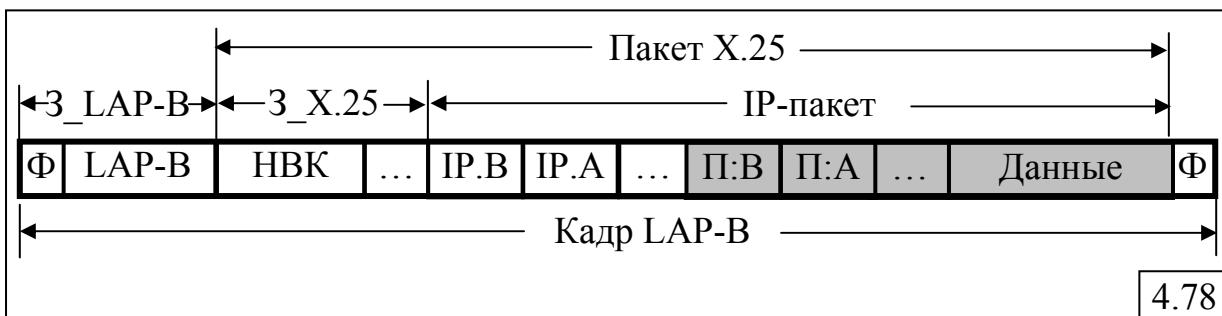
3. IP-пакет поступает на канальный уровень реализуемого в компьютере **A** стека протоколов, где вкладывается в кадр сети Ethernet, поскольку компьютер **A** принадлежит сети **Eth1**. Так как компьютер **B** не подключён к сети **Eth1**, компьютер **A** обращается к таблице маршрутизации и определяет, что для передачи кадра следует

использовать шлюз, которым является маршрутизатор Мш1. Тогда в заголовке кадра **З\_Eth1** в качестве MAC-адреса назначения указывается адрес порта 1 маршрутизатора Мш1 – **MAC.1.1**, с которым связана ЛВС Eth1, и MAC-адрес компьютера А – **MAC.A**, являющегося узлом-отправителем кадра (рис.4.77,в). Концевик кадра содержит контрольную сумму (**КС**) для проверки правильности доставки кадра.

#### 4.6.3. Передача данных

4. Сформированный таким образом кадр передаётся на физический уровень, который обеспечивает доставку кадра *от компьютера А через ЛВС Eth1 к маршрутизатору Msh1* в виде физических сигналов (электрических, оптических, ЭПИ), соответствующих среде передачи.

5. Маршрутизатор Мш1, получив кадр, передаёт его для обработки протоколу Ethernet, который подсчитывает контрольную сумму кадра и сравнивает её со значением КС в кадре. Если эти значения не совпадают, то кадр отбрасывается и не записывается в буферную память. В противном случае, если подсчитанное значение контрольной суммы совпадает со значением, указанным в концевике, протокол Ethernet освобождает кадр от заголовка и концевика и передаёт его содержимое, то есть IP-пакет, протоколу IP. Протокол IP анализирует IP-адрес назначения **IP.В** и, используя таблицу маршрутизации, определяет выходной порт и IP-адрес следующего хоста. Положим, что в нашем примере это порт 4 и IP-адрес **IP.3.1**. Поскольку порт 4 маршрутизатора Мш1 связан с сетью X.25 и, следовательно, принадлежит этой сети, протокол IP обращается к протоколу X.25, чтобы с помощью процедуры установления соединения создать виртуальный канал с определённым номером (**НВК**), который заносится в 3-байтовый заголовок пакета X.25. Затем пакет передаётся протоколу канального уровня LAP-B, который вкладывает пакет X.25 в соответствующий кадр LAP-B (рис.4.78), обрамляя его флагами (**Ф**).

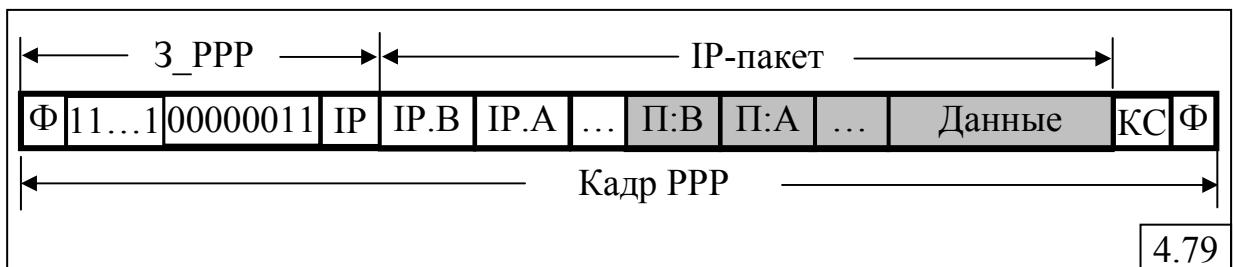


6. Сформированный таким образом кадр передаётся на физический уровень, который обеспечивает доставку кадра *через сеть X.25 от маршрутизатора МШ1 к маршрутизатору МШ3*.

7. Маршрутизатор Мш3, получив кадр, передаёт его для обработки протоколу LAP-B, который освобождает кадр от заголовка **З\_LAP-B** и передаёт его содержимое протоколу X.25. Протокол X.25, в свою очередь, извлекает из поля данных пакета X.25 содержимое (IP-пакет) и передаёт его протоколу IP, который, анализируя IP-адрес назначения **IP.В** и

используя свою таблицу маршрутизации, определяет выходной порт и IP-адрес следующего хоста. В нашем примере это порт 2 и IP-адрес **IP.2.5** маршрутизатора Мш2. Поскольку порт 2 маршрутизатора Мш3 напрямую связан с портом 5 маршрутизатора Мш2 выделенным каналом, образуя двухточечное соединение, передача данных осуществляется на основе протокола канального уровня PPP, которому протокол IP передаёт IP-пакет. Протокол PPP вкладывает его в кадр (формат которого показан на рис. 4.69), обрамлённый флагами **Ф** и содержащий три однобайтовых поля:

- **поле адреса (11...1)**, содержащее все единицы;
- **поле «Управление» с кодом 00000011**;
- **поле протокола (IP)**, указывающее, что в поле данных находится IP-пакет (рис.4.79).



8. Сформированный кадр PPP передаётся на физический уровень, который обеспечивает доставку кадра *по выделенному каналу от маршрутизатора МШ3 к маршрутизатору Мш2*.

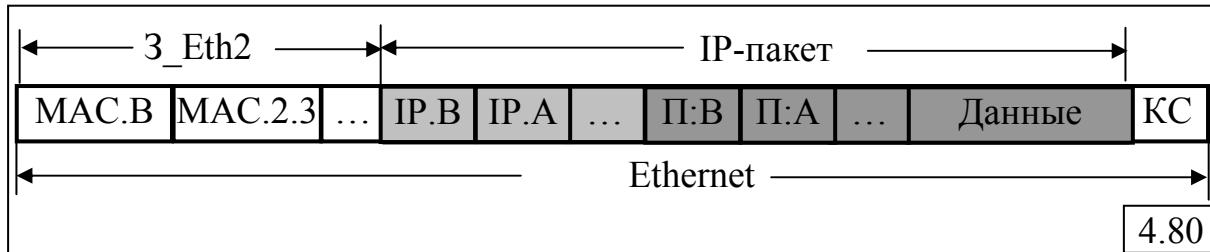
9. Маршрутизатор Мш1, получив кадр PPP, передаёт его для обработки протоколу PPP, который проверяет контрольную сумму и отбрасывает кадр, если рассчитанное значение контрольной суммы не совпадает со значением, указанным в поле КС кадра. Если КС совпадает с указанным в концевике значением, протокол PPP извлекает содержимое, то есть IP-пакет, и передаёт его протоколу IP. Протокол IP анализирует IP-адрес назначения и, используя свою таблицу маршрутизации, определяет, что адресат с IP-адресом **IP.B** находится в локальной сети Eth2, непосредственно подключённой к порту 3 этого маршрутизатора. Затем протокол IP обращается к протоколу ARP, чтобы узнать MAC-адрес, соответствующий IP-адресу IP.B. Протокол ARP находит в своей ARP-таблице MAC-адрес (**MAC.B**) и выдаёт его протоколу IP. Если протокол ARP не находит MAC-адреса, то он реализует процедуру его поиска, посылая в ЛВС Eth2 широковещательный ARP-запрос.

После того как найден MAC-адрес компьютера-получателя B, он вместе с IP-пакетом передаётся протоколу канального уровня Ethernet, который вкладывает его в кадр Ethernet (рис.4.80), указывая в качестве адреса назначения **MAC.B** и адреса отправителя – **MAC.2.3**.

10. Сформированный кадр передаётся на физический уровень, который обеспечивает доставку кадра *через локальную сеть Eth2 от маршрутизатора МШ2 к компьютеру B*.

11. **Компьютер B**, откликаясь на адрес **MAC.B**, записывает поступивший кадр в буфер сетевого адаптера. По завершении приёма кадр

передаётся протоколу Ethernet, который проверяет правильность доставки кадра, извлекает содержимое (IP-пакет) и передаёт его протоколу IP. Последний, в свою очередь, снимает IP-заголовок и передаёт содержимое пакета (UDP-дейтаграмму) протоколу UDP, который в соответствии с указанным в заголовке номером П:В порта назначения пересыпает содержимое, находящееся в поле данных, конкретному *прикладному процессу*.



## 4.7. Безопасность компьютерных сетей

Широкое применение компьютерных сетей во всех областях человеческой деятельности, оказывающее существенное влияние на нашу жизнь, делает весьма актуальной проблему информационной безопасности. Защита информации в компьютерных сетях является одной из наиболее важных задач, которые должны решаться в процессе их разработки и эксплуатации.

Средства защиты информации в компьютерных сетях можно разбить на два класса:

- средства *компьютерной безопасности*, обеспечивающие защиту информации, находящейся в локальной сети или на отдельном компьютере пользователя;
- средства *сетевой безопасности*, обеспечивающие защиту информации в процессе её передачи через сеть.

### 4.7.1. Средства компьютерной безопасности

Средства *компьютерной безопасности* должны обеспечить защиту от несанкционированного доступа всех находящихся внутри собственной локальной сети ресурсов:

- аппаратных – серверы, дисковые массивы, маршрутизаторы;
- программных – операционные системы, СУБД, почтовые службы и т. п.

Кроме того, необходимо обеспечить защиту данных, хранящихся в файлах и обрабатываемых в компьютерах. Для этого необходимо контролировать трафик, входящий в сеть обычно из Интернета, и стараться перекрыть доступ извне для любой информации, с помощью которой злоумышленник может попытаться использовать внутренние ресурсы сети во вред их владельцу.

Наиболее часто в качестве средства компьютерной безопасности используется брандмауэр, устанавливаемый в местах соединений внутренней локальной сети с Интернетом. **Брандмауэр** (firewall)

представляет собой межсетевой экран, который контролирует трафик между локальной сетью и Интернетом и не пропускает подозрительный трафик в сеть. Кроме того, в качестве средств компьютерной безопасности могут использоваться встроенные средства безопасности операционных систем, баз данных, а также встроенные аппаратные средства компьютера.

#### **4.7.2. Средства сетевой безопасности**

Для обеспечения **сетевой безопасности** необходимо защищать информацию, передаваемую в виде пакетов через сети поставщиков услуг Интернета, чтобы она не была искажена, уничтожена или перехвачена посторонними людьми. Для решения этой задачи сегодня широко используется механизм виртуальных частных сетей (VPN).

Автономно работающий компьютер можно более или менее эффективно защитить от внешних покушений. Гораздо сложнее это сделать, если компьютер работает в сети и общается с другими компьютерами. Обеспечение безопасности в этом случае сводится к тому, чтобы сделать проникновение посторонних к ресурсам компьютера контролируемым. Для этого каждому пользователю сети должны быть четко определены его права на доступ к информации, устройствам и на выполнение системных действий в каждом компьютере сети. Дополнительно необходимо обеспечить защиту от перехвата передаваемых по сети данных и создания «ложного» трафика, на что направлена большая часть средств обеспечения сетевой безопасности.

Вопросы сетевой безопасности приобретают особую значимость в связи с тем, что корпоративные сети всё чаще используют Интернет в качестве транспортного средства.

#### **4.7.3. Конфиденциальность, доступность, целостность**

Безопасная информационная система должна:

- защищать данные от несанкционированного доступа;
- быть всегда готовой предоставить данные своим пользователям;
- надежно хранить информацию и гарантировать неизменность данных.

Для этого система должна обладать следующими свойствами.

- **Конфиденциальность** (confidentiality) — гарантия того, что секретные данные будут доступны только авторизованным пользователям, которым этот доступ разрешен.

- **Доступность** (availability) — гарантия того, что авторизованные пользователи всегда получат доступ к данным.

- **Целостность** (integrity) — гарантия сохранности данных, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Требования безопасности могут меняться в зависимости от назначения системы, характера используемых данных и типа возможных угроз.

Если свойства целостности и доступности актуальны для всех систем, то свойство конфиденциальности может быть необязательным, например, если информация предназначена для широкого круга людей. В то же время, для того чтобы злоумышленник не смог изменить эту информацию, необходимо принять меры по обеспечению целостности данных.

Понятия конфиденциальности, доступности и целостности могут быть применены не только по отношению к информации, но и к другим ресурсам вычислительной сети (внешним устройствам, сетевому оборудованию или приложениям). Конфиденциальность, применительно к какому-либо устройству, обеспечивает доступ к нему только авторизованным пользователям, причем они могут выполнять только те операции, которые им разрешены. Свойство доступности устройства состоит в его готовности к использованию в момент возникновения такой необходимости. Благодаря свойству целостности злоумышленник не сможет изменить параметры настройки устройства, что могло бы привести к выходу его из строя.

#### 4.7.4. Сервисы сетевой безопасности

Для защиты данных используются средства, называемые *сервисами сетевой безопасности*, которые обеспечивают контроль доступа, включающий процедуры *шифрование информации, аутентификации, идентификации и авторизации, аудит, антивирусную защиту, контроль сетевого трафика* и т.д. Средства безопасности могут быть либо встроены в программное (операционные системы и приложения) и аппаратное (компьютеры и коммуникационное оборудование) обеспечение сети, либо реализованы в виде отдельных продуктов, созданных специально для решения проблем безопасности.

Рассмотрим основные сервисы сетевой безопасности.

**Шифрование** — процедура, превращающая информацию из обычного «понятного» вида в «непонятный» зашифрованный вид. Для расшифровки зашифрованной информации используется процедура дешифрирования. Пара процедур – шифрование и дешифрирование – называется **криптосистемой**. Шифрование может применяться в системах аутентификации или авторизации пользователей, а также в системах защиты канала связи и хранения данных.

**Аутентификация** (от греч. *authetikos* – подлинный, англ. *authentication* – опознавание, отождествление) – подтверждение подлинности – предотвращает несанкционированный доступ к сети посторонних лиц и разрешает доступ легальным пользователям.

В качестве объектов, требующих аутентификации, могут выступать не только пользователи, но и различные приложения, устройства, данные.

Примером аутентификации на уровне приложений может служить взаимная аутентификации клиента и сервера, когда клиент, доказавший серверу свою легальность, также должен убедиться, что ведет диалог

действительно со своим сервером. При установлении сеанса связи между двумя устройствами также может быть предусмотрена процедура взаимной аутентификации. Аутентификация данных означает доказательство целостности этих данных, а также факт их поступления именно от того человека, который объявил об этом. Для этого используется механизм **электронной подписи**.

Аутентификацию не следует путать с идентификацией и авторизацией.

**Идентификация** заключается в сообщении пользователем системе своего идентификатора, в то время как аутентификация — это процедура доказательства пользователем того, что он является тем, за кого себя выдает, в частности доказательство того, что именно ему принадлежит введенный им идентификатор. Идентификаторы пользователей применяются в системе с теми же целями, что и идентификаторы любых других объектов (файлов, процессов, структур данных), и они не всегда связаны непосредственно с обеспечением безопасности.

**Авторизация** — процедура контроля доступа легальных пользователей к ресурсам системы с предоставлением каждому из них именно тех прав, которые определены ему администратором. Помимо предоставления пользователям прав доступа к каталогам, файлам и принтерам, система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких как локальный доступ к серверу, установка системного времени, создание резервных копий данных, выключение сервера и т. п.

**Аудит** — фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам. Подсистема аудита современных операционных систем позволяет дифференцированно задавать перечень интересующих администратора событий с помощью удобного графического интерфейса. Средства учета и наблюдения обеспечивают возможность обнаружить и зафиксировать важные события, связанные с безопасностью; любые попытки (в том числе и неудачные) создать, получить доступ или удалить системные ресурсы.

#### 4.7.5. Технология защищённого канала

**Технология защищенного канала** обеспечивает безопасность передачи данных по открытой транспортной сети, например по Интернету, за счет:

- взаимной аутентификации абонентов при установлении соединения;
- защиты передаваемых по каналу сообщений от несанкционированного доступа;
- обеспечения целостности поступающих по каналу сообщений.

Защищенный канал можно построить с помощью протоколов, реализованных на разных уровнях модели OSI (табл.4.6).

Таблица 4.6

Уровни защищаемых протоколов	Протоколы защищенного канала
Прикладной уровень	S/MIME
Уровень представления	SSL, TLS
Сеансовый уровень	
Транспортный уровень	
Сетевой уровень	IPSec
Канальный уровень	PPTP
Физический уровень	

Защита данных средствами верхних уровней (прикладного, представления или сеансового) не зависит от технологий транспортировки данных (IP, Ethernet или ATM), однако приложения зависят от конкретного протокола защищенного канала, так как в них должны быть встроены явные вызовы функций этого протокола. Протоколы безопасности прикладного уровня защищают только вполне определенную сетевую службу, например протокол S/MIME защищает сообщения электронной почты. На уровне представления используется протокол SSL (Secure Socket Layer – слой защищенных сокетов) и его открытая реализация TLS (Transport Layer Security – безопасность транспортного уровня).

Средства защищенного канала становятся прозрачными для приложений в тех случаях, когда они защищают кадры протоколов сетевого и канального уровней. Однако при этом сервис защищенного канала становится зависимым от протокола нижнего уровня.

Компромиссным вариантом защищённого канала является работающий на сетевом уровне протокол IPSec. С одной стороны, он прозрачен для приложений, с другой – может работать практически во всех сетях, так как основан на протоколе IP и использует любую технологию канального уровня (PPP, Ethernet, ATM и т. д.).

#### 4.7.6. Протокол IPSec

IPSec (сокращение от IP Security) – набор протоколов, позволяющих обеспечить защиту данных, передаваемых по межсетевому протоколу IP за счёт подтверждение подлинности и шифрования IP-пакетов. Применение протокола IPSec гарантирует целостность, аутентичность и конфиденциальность данных на протяжении всего пути между двумя узлами сети, который получил название «**защищенный канал**».

IPSec-протоколы можно разделить на два класса:

- протоколы, отвечающие за защиту потока передаваемых пакетов, к которым относятся два протокола:

ESP (Encapsulating Security Payload — инкапсуляция зашифрованных данных), обеспечивающий шифрацию, целостность и конфиденциальность передаваемых данных;

AH (Authentication Header — заголовок аутентификации), гарантирующий только целостность и аутентичность данных (передаваемые данные не шифруются).

- протокол обмена криптографическими ключами IKE (Internet Key Exchange — обмен ключами Интернета), автоматически предоставляя конечным точкам защищенного канала секретные ключи, необходимые для работы протоколов аутентификации и шифрования данных.

Для шифрования данных в протоколе IPSec может быть применен любой симметричный алгоритм шифрования. В симметричных схемах шифрования конфиденциальность основана на том, что отправитель и получатель обладают общим, известным только им, параметром функции шифрования. Этот параметр называется *секретным ключом*. Секретный ключ используется как для шифрования текста, так и для его дешифрирования.

Протоколы AH и ESP могут защищать данные в двух режимах:

- транспортном;
- туннельном.

В **транспортном режиме** шифруется только содержимое IP-пакета, не затрагивая заголовок, который не изменяется.

В **туннельном режиме** IP-пакет шифруется целиком, помещается в новый IP-пакет, который передаётся по сети в соответствии с заголовком нового IP -пакета. Таким образом формируется *защищённый IP-туннель*. Туннельный режим может использоваться для подключения удалённых компьютеров к виртуальной частной сети или для организации безопасной передачи данных через открытые каналы связи (например, Интернет) между шлюзами для объединения разных частей виртуальной частной сети.

Режимы IPSec не являются взаимоисключающими – в одном и том же узле некоторые безопасные соединения могут использовать транспортный режим, а другие — туннельный.

Применение того или иного режима зависит:

- от требований, предъявляемых к защите данных;
- от типа узла, завершающего защищенный канал – хост (конечный узел) или шлюз (промежуточный узел).

Соответственно, имеются три схемы применения протокола IPSec:

- хост—хост;
- шлюз—шлюз;
- хост—шлюз.

В схеме **хост—хост**, использующей, как правило, транспортный режим защиты, защищенный канал устанавливается между двумя конечными узлами сети, и протокол IPSec, работая на конечных узлах, защищает передаваемые данные.

В схеме **шлюз—шлюз**, использующей только туннельный режим защиты, защищенный канал устанавливается между двумя промежуточными узлами, называемыми **шлюзами безопасности** (Security Gateway, SG), на каждом из которых работает протокол IPSec. Защищенный обмен данными может происходить между любыми двумя конечными узлами, подключенными к сетям, связанным со шлюзами безопасности. Конечные узлы передают трафик в незащищенном виде, направляя его в общедоступную сеть через шлюз безопасности, который и обеспечивает защиту трафика с помощью протокола IPSec.

Схема **хост—шлюз** применяется при удаленном доступе и позволяет надежно защитить трафик и внутренней сети. Защищенный канал организуется между удаленным хостом, на котором работает протокол IPSec, и шлюзом, защищающим трафик для всех хостов, входящих во внутреннюю сеть.

Протокол AH на приёмной стороне проверяет:

- был ли пакет отправлен тем абонентом, с которым установлено безопасное соединение;
- неискажено ли содержимое пакета;
- не является ли пакет дубликатом уже полученного пакета.

Протокол ESP, кроме перечисленных функций, обеспечивает защиту передаваемых данных от несанкционированного просмотра путем их шифрования.

## ЗАКЛЮЧЕНИЕ

«Удобство в доступе и обработке информации в сети обусловлено «бракосочетанием» двух огромных, но непохожих отраслей техники – техники связи и вычислительной техники. Технику связи лучше всего охарактеризовать как отрасль довольно консервативную.... Она в высшей степени регламентирована, включает в себя большие материальные ресурсы, имеет хорошо поставленные проблемы, которые решаются высококвалифицированными специалистами и основаны на хорошо продуманной теории. Вместе с тем вычислительная техника быстро меняется, является очень новой, также довольно широко распространена ..., слабо регламентирована, страдает от чрезвычайно быстрого старения оборудования, её фундаментальные проблемы плохо разработаны, она до сих пор не стала наукой, имеет плохо определённые цели и задачи и обслуживается, видимо, самыми плохими работниками (слабо подготовленными высокооплачиваемыми «специалистами» по программированию). Однако их союз является настоятельной необходимостью для задач обработки информации. При попытке «поженить» эти две системы возникают чрезвычайно сложные проблемы. Эти системы являются большими и дорогими, характеризуются наличием внешних пользователей, а также плохо понимаемыми критериями и параметрами, определяющими их работу, и, наконец, они оказывают значительное влияние на социальную, политическую и экономическую стороны нашего общества. Такова природа проблемы, с которой мы имеем дело.» (Клейнрок Л. Вычислительные системы с очередями. Пер. с англ. – М.: Мир, 1979. – с.327-328)

Это высказывание принадлежит одному из пионеров в области методов исследования эффективности функционирования вычислительных систем и сетей Леонарду Клейнроку, которое было опубликовано в конце 70-х годов прошлого века в указанной выше монографии. Несмотря на то, что с тех пор прошло более 30 лет, можно с уверенностью сказать, что сказанное выше сохраняет свою актуальность и сегодня.

Прообразом компьютерных сетей можно считать системы телеобработки, которые появились в середине 60-х годов прошлого века и представляли собой одну или несколько больших ЭВМ, доступ к которым осуществлялся от пользователей, находившихся на значительном удалении. Основное назначение таких систем – предоставление вычислительных ресурсов мощных ЭВМ для решения задач пользователей, находившихся порой в разных временных поясах, что обеспечивало высокую загрузку дорогостоящего вычислительного оборудования. Первая сеть с коммутацией пакетов ARPAnet появилась в США в 1969 году, а в середине 70-х была разработана локальная

вычислительная сеть Ethernet, протокол которой был стандартизирован в 1980 году.

За прошедшие 40 с небольшим лет компьютерные сети и сетевые технологии проделали огромный путь.

Если основной функцией первых сетей была обработка данных – решение задач удалённых пользователей, то современные сети охватывают практически весь земной шар и предназначены, прежде всего, для передачи данных на любые расстояния. При этом если первоначально в сетях передавались только компьютерные данные, то в современных сетях передаются все возможные виды данных, включая мультимедийные – речь, аудио, видео, в том числе видео высокой чёткости.

Если в начале 70-х годов скорости передачи данных составляли десятки килобит в секунду, то в современных сетях достигнуты скорости в сотни гигабит в секунду, и это не предел.

За эти годы появилось множество различных сетевых технологий, разнообразное сетевое оборудование. И сегодня компьютерные и телекоммуникационные технологии внедряются в самые разные области и становятся доступны миллионам людей во всём мире.

Несмотря на такие головокружительные успехи, вычислительная техника и сетевые технологии не стали наукой в полном смысле этого слова. Это проявляется, прежде всего, в отсутствии чётко сформулированных понятий и терминов, которые часто по-разному трактуются разными авторами, нет эффективного математического аппарата, призванного обоснованно на количественном уровне сравнивать различные методы построения компьютерных сетей и технические решения, позволяющие оценить эффективность тех или иных сетевых технологий. Правда, справедливо ради, следует отметить, что в последние годы при разработке стандартов и рекомендаций для сравнения тех или иных технических решений и вариантов построения сетей всё шире применяется имитационное моделирование, позволяющее объективно оценить эффективность предлагаемых вариантов и выбрать из них наилучший.

Различная трактовка ряда терминов в области вычислительной техники и телекоммуникационных систем, имеющих зачастую одинаковый или близкий смысл, подвигла автора к попытке разобраться в них и попытаться определить то иногда незначительное различие между близкими по смыслу терминами, которое отличает один термин от другого.

Такими терминами являются:

- «сеть ЭВМ», «компьютерная сеть» и «вычислительная сеть»;
- «телекоммуникационная сеть», «сеть связи» и «сеть передачи данных»;
- «ЭВМ», «вычислительный комплекс» и «вычислительная система»;
- «производительность» и «пропускная способность»;
- «данные» и «информация».

К сожалению, нечёткость определения терминов встречается даже в Государственном стандарте ГОСТ 15971-90 «Системы обработки информации, Термины и определения». Так определение термина «**Данные**» выглядит следующим образом: «*Информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека*» и тут же даётся определение термина «**Обработка информации**»: «*Систематическое выполнение операций над данными, представляющими предназначенную для обработки информацию*». Возникает вопрос: «Так что же мы обрабатываем – данные или информацию? И если мы обрабатываем информацию, то что же мы получаем на выходе после обработки информации – данные или другую информацию?». Найти ответ на этот вопрос не представляется возможным тем более, что сам термин «**Информация**» в ГОСТе не получил определения!

В настоящем пособии предлагается избавиться от такой неоднозначности этих и некоторых других терминов.

Хотелось бы обратить также внимание читателей на удивительно широко распространившуюся путаницу при использовании обозначений приставок кратных единиц в литературе по вычислительной технике и, в том числе, по компьютерным сетям. Речь идёт, прежде всего, о буквах «*K* (большое)» и «*k* (маленькое)», используемых в качестве обозначения приставок десятичных кратных единиц.

К сожалению, во многих книгах и пособиях, и что особенно неприятно, в учебниках по информатике утверждается, что «в вычислительной технике приставка «кило» означает не 1000, а 1024».

На самом же деле, это совсем не так. Следует различать «*K* (большое)» и «*k* (маленькое)».

В вычислительной технике действительно часто используется «*K* (большое)», обозначающее число  $1024 = 2^{10}$ . Это обозначение появилось в связи с адресацией оперативной памяти компьютера. Если под адрес отводится 16 двоичных разрядов, то всего может быть пронумеровано  $2^{16} = 2^6 * 2^{10}$  ячеек оперативной, то есть 64К слов или байт (при байтовой адресации памяти).

Однако скорость передачи данных по каналу связи, например при ИКМ-преобразовании, будет равна не 64 Кбит/с = 65 536 бит/с, а ровно 64 000 бит/с, то есть 64 кбит/с. Это следует из принципа ИКМ-преобразования, в соответствии с которым непрерывный голосовой сигнал квантуется по времени 8000 раз в секунду, при этом каждый отсчёт передаётся в виде 8-ми двоичных символов (битов), откуда получается  $8000 \text{ [раз/с]} * 8 \text{ [бит]} = 64\ 000 \text{ бит/с}$ , то есть скорость передачи двоичных данных будет составлять ровно 64 килобитов в секунду.

Поскольку обозначение «*K* (большое)» не означает 1000, то оно не может именоваться приставкой «кило». А вот «*k* (маленькое)» – это действительно является обозначением приставки «кило» и служит в

качестве множителя 1000. Это обозначение стандартизовано в Международной системой единиц СИ и в ГОСТ 8.417-2002 «Единицы величин», введённом в действие с 1 сентября 2003 г.

В некоторых случаях идут ещё дальше и утверждают, что «Мбит» – это один мегабит или  $1024 \times 1024 = 1048576$  бит!? Однако, если мы опять обратимся к системе СИ или вышеупомянутому ГОСТу, то увидим, что для обозначения приставки «мега» действительно используется большая буква «M», но она соответствует множителю 1 000 000, а не миллион с «хвостиком». Поэтому пропускная способность канала связи в ЛВС Ethernet 10 Мбит/с – это ровно 10 миллионов бит в секунду и длина битового интервала 100 нс, а 100 Мбит/с – это ровно 100 миллионов бит в секунду без всяких «хвостиков».

Возникает вопрос: как же избежать путаницы в этих обозначениях?

Во-первых, при использовании «*K* (большого)» и «*k* (маленького)» в принципе с самого начала никакой путаницы не было и нет:  $K=1024$ , а  $k=1000$ .

Во-вторых, в 2002 году опубликован стандарт **IEEE 1541—2002**, содержащий рекомендации по применению двоичных приставок единиц измерения в области цифровой и вычислительной техники.

Удивительное объяснение имеющейся путаницы в обозначениях можно найти в Интернете и некоторых книгах. Раньше якобы это **не было существенной проблемой**, «так как число  $2^{10}=1024$  достаточно близко к тысяче, и при объемах памяти, исчислявшихся кило- и мегабайтами, ошибка была незначительной. Однако, когда память стала исчисляться гигабайтами, ошибка стала значительной и заметной. В частности, разница между «двоичным» и «десятичным» килобайтом 2,4 %, в то время как между двоичным и десятичным гигабайтом — уже более 7%».

Очевидно, что Л.Клейнрок прав и сегодня – трудно после такого «железного довода» назвать вычислительную технику «наукой».

Следует отметить, что *при указании размерностей кратных и дольных величин, используемых в компьютерных сетях*, в основном применяются *десятичные приставки и их обозначения*. Это относится, прежде всего, к пропускной способности каналов связи и скорости передачи данных. Поэтому пропускная способность 2,048 Мбит/с = 2 048 кбит/с = 2 048 000 бит/с, а скорость передачи данных 51,84 Мбит/с (STS-1) в сетях SDH равна в точности 51 840 000 бит/с, поскольку кадр размером  $90 \times 9 = 810$  байт передаётся 8000 раз в секунду:

$$810 \text{ [байт]} \times 8 \text{ [бит]} \times 8000 \text{ [раз/с]} = 51\,840\,000 \text{ бит/с.}$$

Стандарт IEEE 1541–2002, утвержденный в 2008 году, рекомендует использовать для двоичных чисел приставки, схожие с СИ. Все они начинаются на те же слоги, но второй слог у всех двоичных приставок – «би» (binary – «двоичный»):

- *киби* (*kibi*) (обозн. 'Ki'):  $1Ki = 2^{10} = 1\,024$ ;
- *меби* (*mebi*) ('Mi')  $1Mi = 2^{20} = 1\,048\,576$ ;
- *гibi* (*gibi*) ('Gi')  $1Gi = 2^{30} = 1\,073\,741\,824$ ;

- *теби* (*tebi*) ('Ti')  $1\text{Ti} = 2^{40} = 1\ 099\ 511\ 627\ 776;$
- *пеби* (*pebi*) ('Pi')  $1\text{Pi} = 2^{50} = 1\ 125\ 899\ 906\ 842\ 624;$
- *эксиби* (*exbi*) ('Ei')  $1\text{Ei} = 2^{60} = 1\ 152\ 921\ 504\ 606\ 846\ 976.$

Ниже для справки приведена таблица, содержащая **множители и приставки, используемые для образования наименований и обозначений десятичных кратных и дольных единиц СИ** (ГОСТ 8.417-2002. Единицы величин).

Десятичный множитель	Приставка	Обозначение приставки		Десятичный множитель	Приставка	Обозначение приставки	
		Международное	русское			Международное	русское
$10^{24}$	йотта	Y	И	$10^{-1}$	деци	d	д
$10^{21}$	зетта	Z	З	$10^{-2}$	санти	c	с
$10^{18}$	екса	E	Э	$10^{-3}$	милли	m	м
$10^{15}$	пета	P	П	$10^{-6}$	микро	$\mu$	мк
$10^{12}$	тера	T	Т	$10^{-9}$	нано	n	н
$10^9$	гига	G	Г	$10^{-12}$	пико	p	п
$10^6$	мега	M	М	$10^{-15}$	фемто	f	ф
$10^3$	кило	k	к	$10^{-18}$	атто	a	а
$10^2$	гекто	h	г	$10^{-21}$	зепто	z	з
$10^1$	дека	da	да	$10^{-24}$	йокто	y	и

Большинство приставок образовано от греческих слов и означают: дека – «десять», гекто – «сто», кило – «тысяча», мега – «большой», гига – «гигантский», тера – «чудовищный». Пета и экса соответствуют пяти и шести разрядам по тысяче и переводятся, соответственно, как «пять» и «шесть». Дольные микро и нано переводятся как «малый» и «карлик». От одного слова októ, означающего «восемь», образованы приставки йотта ( $1000^8$ ) и йокто ( $1/1000^8$ ). Как «тысяча» переводится и приставка мили от латинского слова *mille*, санти – «сто» и деци – «десятый», зетта – «семь». Часть приставок происходят от французских, датских, норвежских и других слов: зепто – «семь», атто – «восемнадцать», фемто – «пятнадцать», пико – «маленький».

## **Вопросы и задания для самостоятельной работы**

### **Раздел 1. ОБЩИЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ СЕТЕЙ ЭВМ**

1. В чем различие между данными и информацией?
2. В каких единицах измеряются данные и информация?
3. В чем состоит отличие вычислительной системы от вычислительного комплекса и от ЭВМ?
4. Основная цель построения вычислительных комплексов.
5. Что понимается под архитектурой вычислительной сети?
6. Какие устройства относятся к АПД?
7. Нарисовать структуру сообщения.
8. Понятие звена передачи данных.
9. Перечислить основные функции узла связи.
10. В чем отличие маршрутизации от коммутации?
11. Понятия маршрутизации, коммутации и мультиплексирования.
12. Что такое PDU?
13. В чем отличие пакета от сообщения?
14. Что такое хост?
15. Классификация вычислительных сетей по размеру.
16. Что такое WAN, LAN, MAN, PAN.
17. Классификация вычислительных сетей по принадлежности.
18. Понятие виртуальной ЛВС.
19. Какие функции возлагаются на администрирование компьютерной сети?
20. Какие данные относятся к непрерывным, а какие – к дискретным?
21. В чём отличие аудиоданных от телефонных (голосовых) данных?
22. Какие типы данных относятся к мультимедийным?
23. Что понимается под каналом тональной частоты?
24. Перечислить требования к организации компьютерных сетей.
25. Что означает требование открытости вычислительных сетей?
26. Как называется промежуток времени, в течение которого взаимодействуют процессы?
27. За счет чего реализуются требования к организации компьютерных сетей?
28. Понятия схемного и программного интерфейса.
29. Назначение многоуровневой модели взаимодействия открытых систем.
30. В чем отличие ISO от OSI?
31. Нарисовать OSI-модель.
32. Перечислить уровни OSI-модели.
33. Основные функции каждого уровня OSI-модели.
34. На каком уровне OSI-модели реализуются функции доступа к среде передачи данных?
35. На каком уровне OSI-модели реализуются функции маршрутизации?
36. На каком уровне OSI-модели появляется свойство адресуемости?

37. Как изменяется структура данных при передаче между уровнями управления?
38. В чем отличие логической передачи от физической в OSI-модели?
39. Может ли сетевой уровень одной системы послать сообщение канальному уровню другой системы?
40. Что такое MAC-адрес?
41. В чём отличие MAC-адреса от сетевого адреса?
42. Что не может являться MAC-адресом?
  - 1) AF-90-02-0A-9B-9C
  - 2) AA-BB-CC-DD-EE
  - 3) 00-11-22-33-44-55
  - 4) 00-12-AA-CD-RH-34
  - 5) 0A-A1-B2-C3-D4-F5
  - 6) 00-00-02-0A-1B-0C
43. Могут ли два устройства иметь одинаковый MAC-адрес? Ответ обосновать.
44. Функции MAC и LLC-подуровней.
45. Чем отличается состав сетевой операционной системы от операционной системы компьютера?
46. Перечислить основные топологии компьютерных сетей.
47. Какими достоинствами и недостатками обладают разные топологии компьютерных сетей?
48. Какая топология СПД обладает максимальной (минимальной) надежностью?
49. Какая топология СПД обладает максимальным (минимальным) временем доставки сообщений?
50. Какая топология СПД обладает максимальной (минимальной) производительностью?
51. В чем отличие логической топологии от физической?
52. Чем определяется функциональная организация вычислительной сети?
53. Перечислите способы коммутации в вычислительных сетях.
54. Пояснить принцип коммутации каналов (пакетов, сообщений, ячеек).
55. Какими достоинствами и недостатками обладает коммутация каналов (пакетов, сообщений)?
56. При каком способе коммутации каналы связи должны иметь одинаковые пропускные способности на всем пути передачи?
57. Какой способ коммутации эффективен при передаче больших объемов данных?
58. Пояснить, почему при коммутации пакетов буферная память используется более эффективно, чем при коммутации сообщений?
59. Какими преимуществами обладает коммутация пакетов по сравнению с коммутацией сообщений?
60. Какой способ коммутации в компьютерных сетях является основным?
61. Пояснить принципы передачи данных при дейтаграммном способе и способе «виртуальный канал».

62. Какими достоинствами и недостатками обладают дейтаграммный способ передачи пакетов и "виртуальный канал"?
63. При каком способе передачи пакеты одного и того же сообщения передаются в сети по разным маршрутам?
64. Классификация алгоритмов маршрутизации.
65. Пояснить принцип маршрутизации "по предыдущему опыту".
66. Пояснить принципы локальной, распределенной, централизованной и адаптивной маршрутизации.
67. Что такое перегрузка в компьютерных сетях, и каковы её отрицательные последствия?
68. Что такое блокировка в компьютерной сети? Привести пример.
69. Нарисовать зависимость производительности сети передачи данных от числа пакетов.
70. Для чего используется механизм бит-стаффинга?
71. Пояснить идею механизма бит-стаффинга.
72. Пояснить принцип управления потоком сообщений на основе механизма квитанций.
73. Как называется интервал времени, в течение которого узел коммутации вычислительной сети, передавший пакет, ожидает подтверждения?
74. Чем положительная квитанция отличается от отрицательной?
75. Пояснить принцип управления потоком сообщений на основе механизма скользящего окна.
76. Какую цель преследует использование механизма скользящего окна?
77. Ширина окна равна 128. Узел, передавший 39-й кадр, получил подтверждение о приёме 31-го кадра. Какое максимальное число кадров может ещё передать узел без подтверждения?
78. Перечислить состав параметров и характеристик, описывающих компьютерную сеть.
79. Привести примеры структурных, функциональных и нагрузочных параметров вычислительной сети.
80. Что понимается под системной производительностью средств вычислительной техники?
81. В каких единицах измеряется системная производительность ВС?
82. В чем различие между отказами и сбоями?
83. Перечислить показатели надежности.
84. Что характеризует коэффициент загрузки устройства?
85. Краткая характеристика протоколов TCP/IP, XNS, IPX, AppleTalk, DECnet, SNA.

## **Раздел 2. СРЕДСТВА ТЕЛЕКОММУНИКАЦИЙ**

### **2.1. Основные понятия техники связи**

1. В чём различие между каналом и линией связи?
2. Что такое "децибел"?
3. Во сколько раз уменьшится мощность сигнала на расстоянии 100 м, если его ослабление равно:  $d=10 \text{ дБ/км}$ ?
4. В чём состоит удобство вычисления затухания сигнала в дБ?
5. Записать функцию, описывающую гармоническое колебание.
6. Нарисовать график гармонического колебания и показать на графике его параметры.
7. Каким соотношением связаны линейная и круговая частоты?
8. Записать и пояснить представление функции, отображающей непрерывные данные, в виде ряда Фурье.
9. Понятие сигнала (функции) с ограниченным спектром.
10. Какой спектр частот характерен для дискретных сигналов?
11. При каких условиях обеспечивается качественная передача сигнала?
12. Проиллюстрировать на графике понятие полосы пропускания (частот) линии связи.
13. Какую полосу пропускания имеет телефонный канал?
14. По каким каналам можно передавать дискретные сигналы в их естественном виде – без модуляции (в первичной полосе частот)?
15. Как передаются сигналы в высокоскоростных каналах связи с резко ограниченной полосой частот?
16. Что такое модуляция и для чего она нужна?
17. Чем манипуляция отличается от модуляции?
18. Пояснить принцип амплитудной, частотной и фазовой модуляции.
19. Что такое ИКМ?
20. Пояснить различие между АИМ и ИКМ.
21. Показать, за счет чего обеспечивается скорость передачи данных в 64 кбит/с (56 кбит/с) при ИКМ.
22. Пояснить принцип аддитивной разностной (дифференциальной) ИКМ.

### **2.2. Система связи**

1. Нарисовать обобщенную (каноническую) структуру системы связи.
2. Что такое линейный сигнал?
3. В чём различие между линейным и первичным сигналом?
4. В чём отличие системы связи на основе дискретного канала от системы связи на основе непрерывного канала?
5. В чём отличие выделенного канала связи от коммутируемого?
6. В чём отличие дуплексного канала связи от полудуплексного и от симплексного?
7. Перечислить характеристики цифрового канала связи.
8. От чего зависит пропускная способность канала связи?

9. Рассчитать максимально возможную пропускную способность (Мбит/с) канала связи при условии, что полоса пропускания равна 20 МГц, а отношение мощности сигнала к мощности шума равно 3.
10. В чем отличие пропускной способности от скорости передачи данных?
11. Какие скорости передачи данных обеспечивает телефонный канал?
12. Нарисовать схему многоканальной системы связи.
13. Перечислить методы уплотнения каналов.
14. Пояснить принципы частотного и временного уплотнения канала связи.
15. Какие методы мультиплексирования используются в вычислительных сетях?
16. В чем отличие частотного мультиплексирования от временного?
17. Что такое FDM, TDM, WDM?

### ***2.3. Методы модуляции и кодирования данных***

1. Как называется процесс представления непрерывных данных в виде физических сигналов для их передачи по каналам связи?
2. Как называется процесс представления дискретных данных в виде физических сигналов для их передачи по каналам связи?
3. От чего зависит спектр результирующего модулированного сигнала?
4. Как спектр результирующего модулированного сигнала зависит от скорости модуляции (скорости передачи данных)? Ответ пояснить.
5. Что такое потенциальное кодирование?
6. При каком кодировании скорость модуляции (бод) и скорость передачи данных (бит в секунду) совпадают?
7. Как изменяется спектр сигнала при потенциальном кодировании при передаче длинной последовательности нулей или единиц?
8. В каком случае при потенциальном кодировании в спектре сигнала отсутствует постоянная составляющая?
9. Почему потенциальные коды на каналах тональной частоты никогда не используются?
10. В чем отличие импульсных кодов от потенциальных?
11. Перечислить требования к методам цифрового кодирования.
12. Как битовая скорость связана со спектром результирующего сигнала?
13. В чем заключается проблема синхронизации при передаче цифровых сигналов?
14. Что такое самосинхронизирующийся код?
15. Какие методы кодирования относятся к самосинхронизирующемся?
16. От чего зависит стоимость реализации метода кодирования?
17. Что такое постоянная составляющая спектра сигнала и почему она нежелательна?
18. Какие методы кодирования имеют постоянную составляющую в спектре сигнала?
19. Почему проблема синхронизации в телекоммуникационных сетях решается сложнее, чем при обмене данными между компьютером и принтером?

20. Почему в телекоммуникационных сетях для синхронизации не используется схема, основанная на отдельной тактирующей линии связи?
21. Достоинства и недостатки методов кодирования NRZ, RZ, AMI, MLT-3, Манчестер 2, ....
22. Проиллюстрировать на диаграмме методы кодирования NRZ, RZ, AMI, MLT-3, Манчестер 2, ....
23. У какого из известных вам методов основная гармоника имеет наименьшую частоту?
24. Нарисовать диаграммы методов кодирования NRZ, RZ, AMI, MLT-3, Манчестер 2... для сообщения, заданного в шестнадцатеричном коде: C5.
25. Определить частоту основной гармоники для сообщения, заданного в шестнадцатеричном коде: C5, при использовании методов кодирования NRZ, RZ, AMI, MLT-3, Манчестер 2....
26. Какой метод кодирования применяется в ЛВС Ethernet и Token Ring.
27. Перечислить методы логического кодирования.
28. Для чего используются методы логического кодирования?
29. Пояснить принципы метода избыточного кодирования и скремблирования.
30. Какой метод логического кодирования используется в ЛВС Fast Ethernet и FDDI?
31. Пояснить суть методов логического кодирования 4B/5B, 5B/6B, 8B/10B, 8B/6T.
32. Что такое «запрещенные коды» в методах избыточного кодирования?
33. Какой метод избыточного кодирования обладает наибольшей (наименьшей) избыточностью и почему?
34. Сколько избыточных кодов содержит метод кодирования 4B/5B, 5B/6B, 8B/10B, 8B/6T.
35. Основной недостаток методов избыточного кодирования.
36. Что такое дескремблер?

#### **2.4. Кабельные линии связи**

1. Что понимается под кабельной линией связи?
2. В чем отличие кабеля связи от силового кабеля?
3. Перечислить типы электрических кабелей связи, применяемых в сетях передачи данных.
4. Перечислить основные электромагнитные характеристики электрических кабелей связи.
5. От чего зависит затухание в электрическом кабеле связи?
6. В каких единицах измеряется затухание, импеданс, NEXT?
7. Что характеризует NEXT для электрических кабелей связи?
8. Какое значение NEXT является предпочтительнее?
9. Что такое "активное сопротивление"?

10. Какое значение ёмкости для электрических кабелей связи является предпочтительным?
11. Для чего применяется скручивание электрических проводников?
12. Что представляют собой кабели UTP, FTP, STP?
13. В чём отличие FTP от STP?
14. Как зависит пропускная способность неэкранированной витой пары от её категории?
15. Какую полосу пропускания имеют кабели UTP категории 3 и 5?
16. Что представляет собой коаксиальный кабель?
17. Какие достоинства и недостатки присущи коаксиальным кабелям?
18. В чём состоят основные отличия толстого коаксиального кабеля от тонкого?
19. Перечислить основные компоненты ВОЛС.
20. Что представляет собой оптическое волокно?
21. Пояснить на рисунке разницу между одно- и многомодовым оптическим волокном.
22. Какие параметры оптического волокна являются важнейшими?
23. Чем обусловлено затухание в оптическом волокне?
24. На каких длинах волн осуществляется передача сигналов по оптическому волокну и почему?
25. Показать на графике характер зависимости затухания сигнала в оптическом волокне от длины волны.
26. Что такое дисперсия для оптического волокна и как она связана с полосой пропускания?
27. В каких единицах измеряется "полоса пропускания" для оптического волокна?
28. Какие достоинства и недостатки присущи одномодовым волокнам?
29. Какие оптические волокна имеют лучшие характеристики по затуханию и полосе пропускания и почему?
30. Какие оптические волокна имеют большую стоимость?
31. Для каких оптических волокон меньше потери сигнала при их сращивании?
32. Какие оптические волокна более удобны при монтаже и почему?
33. Что представляет собой волоконно-оптический кабель (ВОК)?
34. С помощью каких приборов световой поток вводится в ВОК?
35. На какие расстояния обеспечивают передачу данных без регенерации сигнала одномодовый и многомодовый ВОК?
36. Что такое коннекторы и для чего они предназначены?
37. Перечислить электронные компоненты систем оптической связи.
38. Достоинства и недостатки ВОЛС.
39. Основные преимущества применения ВОЛС в ЛВС.
40. Перечислить способы сращивания оптических волокон.
41. Какие возможности обеспечивает сварка оптических волокон специальным аппаратом?

- 42.Что представляет собой механический "сплайс" для сращивания оптических волокон?
- 43.Что представляет собой прецизионная втулка для сращивания оптических волокон?
- 44.Какой способ сращивания оптических волокон наиболее эффективен?
- 45.Какой способ сращивания оптических волокон наиболее простой?
- 46.Перечислить виды оборудования для диагностики и сертификации кабельных систем.
- 47.Что такая структурированная кабельная система (СКС).
- 48.Требования к современным кабельным системам.
- 49.Достоинства и недостатки структурированного подхода при построении кабельных систем.

## **2.5. Беспроводные линии связи**

1. Перечислить недостатки, присущие кабельным линиям связи.
2. Перечислить основные характеристики электромагнитного поля излучения (ЭПИ).
3. Какие фундаментальные физические процессы оказывают влияние на передачу ЭПИ в точке приема?
4. Пояснить на рисунке явления отражения ЭПИ от Земли, преломления лучей ЭПИ в ионизированных слоях атмосферы, дифракции ЭПИ.
5. Для каких радиоволн явление отражения проявляется в наибольшей степени?
6. Для каких радиоволн ионизированный слой атмосферы является практически "прозрачным"?
7. Для каких радиоволн явление дифракции проявляется в наибольшей степени?
8. Какие факторы необходимо принимать во внимание при выборе длины волны (частоты) для передачи по радиолиниям?
9. Что такое рефракция волн в атмосфере.
10. Для каких радиоволн начинает существенно сказываться явление рассеяния на малых неоднородностях атмосферы?
- 11.Какие радиоволны распространяются практически только в пределах прямой видимости?
- 12.Для передачи каких радиоволн используются специальные остронаправленные антенны?
- 13.В чем сложность применения инфракрасных и видимых волн в открытом пространстве?
- 14.Какие возможности предоставляет радиомодем?
- 15.Что такое чувствительность радиомодема?
- 16.Основной принцип организации радиорелейных линий связи (РРЛС)?
- 17.Нарисовать схему организации РРЛС.
- 18.На основе каких рассуждений может быть получено выражение для определения расстояния между антеннами РРЛС в случае гладкой поверхности Земли?

19. В чем основное различие между спутниковыми и наземными радиосистемами?
20. Как в ССС осуществляется контроль правильности доставки сообщений?
21. Чем геостационарная орбита отличается от высокоэллиптической?
22. Что означает синхронность геостационарной орбиты?
23. Под каким углом наклонена плоскость геостационарной орбиты по отношению к плоскости экватора?
24. На какой высоте расположен геостационарный спутник?
25. Чему равен период обращения геостационарного спутника?
26. Какие достоинства и недостатки присущи геостационарной орбите.
27. Почему связь с геостационарным спутником может осуществляться круглосуточно?
28. Почему ослабление сигнала на трассе между ЗС и спутником является стабильным?
29. Почему невозможна связь с геостационарным спутником в высоких широтах?
30. Чему равен период обращения ИСЗ на высокоэллиптической орбите?
31. В чём состоит основное достоинство высокоэллиптической орбиты?
32. Что означает аббревиатура VSAT в системах спутниковой связи?
33. Почему технология VSAT доступна мелким и средним фирмам?
34. На каких высотах размещаются низкоорбитальные спутники связи?
35. За счет чего в системах малых низкоорбитальных спутников связи обеспечивается значительный энергетический выигрыш по сравнению с системами связи через высокоорбитальные спутники связи?
36. Чему равен радиус действия сетей на ИК-лучах?
37. Почему связь на ИК-лучах устойчива к радиопомехам?
38. В каком диапазоне частот организована связь на ИК-лучах?
39. Недостатки сетей на ИК-лучах.

## **2.6. Телекоммуникационные сети**

1. Что представляет собой абонентская сеть, сеть доступа, магистральная сеть?
2. Какие требования предъявляются к современным магистральным телекоммуникационным сетям.
3. Что означает понятие «интеграция служб»?
4. За счет чего обеспечиваются высокие скорости передачи данных в магистральных сетях?
5. Что такое АТС?
6. В какой форме может осуществляться передача данных в современных телефонных сетях?
7. С помощью каких средств осуществляется передача цифровых данных по аналоговым каналам?
8. Перечислить основные функции модемов.

9. Какими способами могут быть реализованы протоколы контроля ошибок и сжатия данных?
10. Какой диапазон скоростей передачи обеспечивается при модемной связи?
11. Какая максимальная скорость передачи обеспечивается при модемной связи?
12. Назначение телеграфных, телефонных, сотовых, кабельных модемов, факс-модемов, модемов для голосовой почты.
13. Какая скорость обеспечивается при передаче данных с использованием кабельных модемов?
14. Что такое ISDN?
15. Какие преимущества обеспечивает ISDN по сравнению с обычной модемной связью?
16. В каких случаях целесообразно применять ISDN и почему?
17. В чем отличие канала **B** от канала **D** в ISDN-сетях?
18. Какая скорость обеспечивается в одном канале **B** в ISDN-сетях?
19. Что такое BRI (PRI, BISDN)?
20. Раскрыть обозначение (2B+D).
21. Какие пропускные способности обеспечиваются для базового, первичного и широкополосного интерфейса доступа к ISDN?
22. Что такое xDSL?
23. Какие скорости обеспечиваются в технологиях xDSL?
24. Раскрыть принцип организации ADSL.
25. Назначение DSLAM.
26. Что представляет собой сотовая связь в мобильной телефонной связи?
27. Показать на рисунке принцип организации сотовой связи.
28. В каких случаях соты разбиваются на микросоты?
29. В чём основные отличия мобильной сотовой связи 2-го поколения от 1-го, 3-го от 2-го и 4-го от 3-го?
30. Перечислить основные стандарты каждого поколения сотовой связи.
31. Дать краткую характеристику GSM.
32. На какие технологии ориентируется 4-е поколение мобильной сотовой связи?
33. Что такое PDH, SDH, SONET?
34. Что представляет собой канал E1/T1?
35. Нарисовать схему формирования канала E1 (T1).
36. Какие недостатки присущи PDH?
37. Какова цель разработки SDH?
38. Какие устройства входят в состав SDH?
39. Что в SDH используется в качестве среды передачи?
40. Сколько уровней содержит стек протоколов SDH?
41. Что такое виртуальный контейнер?

## **Раздел 3. ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ**

### **3.1. Принципы организации ЛВС**

1. Перечислить характерные особенности ЛВС.
2. Какие топологии наиболее широко применяются в ЛВС?
3. Почему в ЛВС отсутствует АПД?
4. Назначение сетевых адаптеров.
5. Алгоритм функционирования сетевых адаптеров при передаче и приеме пакетов.
6. Для чего необходима буферизация данных в сетевом адаптере?
7. Основные отличия одноранговых ЛВС от ЛВС типа "клиент-сервер".
8. Какие достоинства и недостатки присущи одноранговым ЛВС и ЛВС типа "клиент-сервер"?
9. Что такое сервер, служба, сервис?
10. Для чего предназначен файл-сервер?
11. Перечислить типы прикладных серверов.
12. Какие топологии ЛВС получили наиболее широкое распространение?
13. Что такое многосегментная организация ЛВС?
14. Назначение повторителей и концентраторов.
15. Что такое репитер и хаб?
16. Нарисовать структуру ЛВС с повторителем.
17. Достоинства и недостатки использования повторителей и концентраторов для увеличения размеров ЛВС.
18. На каком уровне OSI-модели работают повторители и концентраторы?
19. Что такое стек концентраторов?
20. На каком уровне OSI-модели реализуются методы управления доступом в ЛВС.
21. В чем отличие метода доступа CSMA/CA от CSMA/CD?
22. В чём суть маркерного метода доступа?
23. Что представляет собой маркер?
24. Какие способы передачи маркера используются в ЛВС?
25. В чём суть метода раннего освобождения маркера и в каких ЛВС он применяется?

### **3.2. ЛВС Ethernet**

1. Какой метод доступа используется в сетях Ethernet?
2. Сколько пакетов может передаваться в ЛВС Ethernet в один и тот же момент времени?
3. Нарисовать структуру ЛВС Ethernet на основе концентратора.
4. В чем отличие пассивного концентратора от активного?
5. Формат и краткое описание кадра Ethernet II и Ethernet 802.3.
6. Назначение и код поля преамбулы кадра Ethernet.
7. Структура поля адреса назначения кадра Ethernet.

8. Какими являются адреса назначения, заданные в шестнадцатеричном виде: 05412FD41906; 51A317B43456; 8100040D2107; E2E455462100?
9. Прокомментировать адреса отправителей, заданные в шестнадцатеричном виде: 05412FD41906; 51A317B43456; 8100040D2107; E2E455462100.
10. Чем широковещательный кадр отличается от группового?
11. Чему равны максимальная и минимальная длина поля данных в кадрах Ethernet II и Ethernet 802.3?
12. Из каких соображений выбирается максимальная и минимальная длина поля данных в кадрах Ethernet II и Ethernet 802.3?
13. В каком диапазоне находится длина кадра ЛВС Ethernet?
14. Почему длина кадра ЛВС Ethernet не может быть меньше 64 байт?
15. К каким отрицательным последствиям может привести передача кадра ЛВС Ethernet длиной в 46 байт?
16. Для каких полей кадра ЛВС Ethernet вычисляется контрольная сумма?
17. Что такое CRC-32?
18. Могут ли быть переданы данные длиной менее 46 байтов в стандарте Ethernet II?
19. Что определяют "точка доступа к услугам получателя" и "точка доступа к услугам источника" в кадре стандарта Ethernet 802.2?
20. Как обозначаются стандарты физического уровня ЛВС Ethernet?
21. Чему равны максимальное число рабочих станций и длина одного сегмента ЛВС стандартов 10Base2, 10Base5, 10BaseT, 10Base-F?
22. Чем основополосная передача отличается от широкополосной?
23. Когда целесообразно использование основополосной (широкополосной) передачи?
24. В каких сетях и почему обычно реализуется основополосная передача?
25. Нарисовать структуру сети Ethernet на толстом (тонком) коаксиальном кабеле с одним повторителем.
26. Кабели какого типа допускают (не допускают) отводы к рабочим станциям?
27. Нарисовать структуру сети Ethernet на основе неэкранированной витой пары.
28. Чему равно максимально допустимое число рабочих станций в ЛВС Ethernet? Нарисовать структуру сети Ethernet с максимально допустимым числом рабочих станций.
29. Какую топологию имеет сеть Ethernet в соответствии со спецификацией 10Base2 (10Base5, 10BaseT, 10Base-F)?
30. Что означает правило «5-4-3» (правило 4-х хабов)?
31. Для каких сетей применяется правило «5-4-3» (правило 4-х хабов)?
32. Нарисовать ЛВС Ethernet в соответствии с правилом «5-4-3» (правилом 4-х хабов).
33. Краткая характеристика стандартов 10Base-FL(10Base-FB, FOIRL)?
34. Сформулировать алгоритм передачи и приема данных в соответствии с протоколом CSMA/CD.

- 35.Что такое фрагмент и поздняя коллизия в ЛВС Ethernet?
- 36.Что представляет собой сигнал затора в ЛВС Ethernet?
- 37.О чём обычно свидетельствует наличие в сети Ethernet поздней коллизии?
- 38.В чём суть алгоритма отступления в ЛВС Ethernet?
- 39.Каковы действия рабочей станции после обнаружения коллизии в сети Ethernet?
- 40.На какое время откладывается передача кадра в ЛВС Ethernet после коллизии?
- 41.На какое время может быть отложена передача кадра в ЛВС Ethernet (100 Мбит/с) после второй коллизии?
- 42.На какое максимальное время может быть отложена передача кадра в ЛВС Ethernet (10 Мбит/с) после третьей коллизии?
- 43.После какого числа коллизий максимальное время, на которое будет отложена передача кадра в ЛВС Ethernet (10 Мбит/с), равно 102,4 мкс?
- 44.Рассчитать время, на которое будет отложена передача кадра в ЛВС Ethernet (10 Мбит/с) после второй коллизии, если известно, что генератор случайных чисел в интервале (0; 1) выдал значение 0,86?
- 45.Для чего необходим межкадровый интервал в ЛВС Ethernet и какова его величина?
- 46.Чему равно минимально допустимое значение межкадрового интервала в ЛВС Ethernet?
- 47.Чему равен межкадровый интервал (в микросекундах) в ЛВС Ethernet с пропускной способностью 100 Мбит/с?
- 48.Что произойдет, если межкадровый интервал в ЛВС Ethernet будет составлять 20 битовых интервалов?
- 49.В каком случае в ЛВС Ethernet кадр остается не переданным рабочей станцией?
- 50.Что является признаком фрагмента в ЛВС Ethernet?
- 51.Что включает в себя проверка целостности кадра данных в ЛВС Ethernet?
- 52.Когда кадр считается переполненным?
- 53.Что такое выравненность кадра.
- 54.Нарисовать и пояснить зависимость времени задержки кадров в ЛВС Ethernet от загрузки среды передачи.
- 55.Рассчитать пропускную способность среды передачи [кадров/с] ЛВС Ethernet (100 Мбит/с) при передаче кадров минимальной (максимальной) длины.
- 56.Рассчитать пропускную способность среды передачи [кадров/с] ЛВС Ethernet (100 Мбит/с) при передаче кадров с полем данных длиной в 494 байт.
- 57.Рассчитать эффективную пропускную способность ЛВС Ethernet (100 Мбит/с) при передаче кадров минимальной (максимальной) длины.
- 58.Рассчитать эффективную пропускную способность ЛВС Ethernet (100 Мбит/с) при передаче кадров с полем данных длиной в 494 байт.

59. Рассчитать коэффициент использования канала ЛВС Ethernet (100 Мбит/с) при передаче кадров минимальной (максимальной) длины.
60. Рассчитать коэффициент использования канала ЛВС Ethernet (10 Мбит/с) при передаче кадров с полем данных длиной в 494 байт.
61. Достоинства и недостатки сети Ethernet.

### **3.3. Высокоскоростные технологии Ethernet**

1. Какие методы доступа используются в ЛВС Fast Ethernet, в ЛВС 100VG-AnyLAN и в ЛВС Gigabit Ethernet?
2. Основные отличия Fast Ethernet от Ethernet-10.
3. Какие кабельные системы используются в Fast Ethernet?
4. Какую структуру имеет ЛВС Fast Ethernet?
5. Почему диаметр ЛВС Fast Ethernet сокращен до 200 метров? Как можно увеличить диаметр ЛВС Fast Ethernet?
6. Краткая характеристика ЛВС 100Base-TX (100Base-T4, 100Base-FX).
7. В каких сетях и для чего используется функция автопереговоров?
8. За счет чего обеспечивается пропускная способность в 100 Мбит/с при использовании витой пары категории 3 в ЛВС 100Base-T4?
9. В чем отличие повторителей Fast Ethernet класса I от повторителей класса II?
10. Раскрыть обозначения в спецификации 100VG-AnyLAN.
11. Краткое описание метода доступа Demand Priority.
12. Какие изменения имеются в технологии Gigabit Ethernet по сравнению Ethernet 10 Мбит/с и Fast Ethernet?
13. Как реализуется работа ЛВС Gigabit Ethernet в полнодуплексном режиме?
14. Для чего и на сколько в ЛВС Gigabit Ethernet увеличен минимальный размер кадра?
15. Какую длину имеет поле расширения в кадре ЛВС Gigabit Ethernet?
16. За счет чего уменьшаются накладные расходы при передаче коротких кадров в ЛВС Gigabit Ethernet?
17. В каких ЛВС и для чего используется режим передачи кадров Burst Mode?
18. В чем отличие спецификации 1000 Base-SX от 1000 Base-LX?
19. Каким образом технология Gigabit Ethernet реализована на витой паре категории 5?
20. Какой режим передачи данных используется в ЛВС 10GEthernet?
21. Какая среда передачи данных используется в ЛВС 10GEthernet?
22. В чем отличие ЛВС 10GBase-RS от ЛВС 10GBase-RL и ЛВС 10GBase-RE?
23. Какие максимальные расстояния обеспечиваются между передатчиком и приемником в ЛВС 10GEthernet?
24. Какую максимальную пропускную способность может иметь сеть Ethernet?

25. Рассчитать максимальный диаметр ЛВС Fast Ethernet, построенной с использованием повторителя класса I (со временем задержки в 70 bt), полагая, что скорость распространения сигнала в кабеле составляет треть от скорости света.
26. Рассчитать максимальный диаметр ЛВС Fast Ethernet, построенной с использованием двух повторителей класса II (со временем задержки в 33 bt), полагая, что скорость распространения сигнала в кабеле в три раза меньше скорости света.
27. Рассчитать максимальный диаметр ЛВС Gigabit Ethernet при минимальной длине кадра в 64 байта, полагая, что скорость распространения сигнала в кабеле составляет треть от скорости света. Задержкой в повторителе можно пренебречь.
28. Рассчитать пропускные способности среды передачи данных ЛВС Gigabit Ethernet при передаче кадров минимальной и максимальной длины.
29. Рассчитать эффективную пропускную способность канала связи ЛВС Gigabit Ethernet при передаче кадров в режиме «burst mode».

### **3.4. ЛВС Token Ring**

30. Назначение сетевой технологии Token Ring.
31. Какая пропускная способность обеспечивается в ЛВС Token Ring?
32. Что представляет собой устройство множественного доступа MSAU?
33. Нарисовать структуру и описать функционирование ЛВС Token Ring на основе одного и нескольких MSAU.
34. В чем отличие физической топологии ЛВС Token Ring от логической?
35. Нарисовать возможные варианты структурной организации ЛВС Token Ring.
36. Понятие и функции активного монитора в ЛВС Token Ring.
37. Какой режим (способ) передачи маркера используется в ЛВС Token Ring со скоростью 16 Мбит/с?
38. Перечислить типы кадров, используемых в ЛВС Token Ring.
39. Назначение кадра последовательности завершения.
40. Нарисовать и пояснить форматы маркера, кадра данных и последовательности завершения, используемых в ЛВС Token Ring.
41. Каково назначение битов приоритета, бита маркера, бита монитора и битов резервирования поля "управление доступом" в маркере ЛВС Token Ring.
42. Сколько уровней приоритета предусмотрено в ЛВС Token Ring (FDDI; 100VG-AnyLAN)?
43. В чем отличие кадров уровня MAC от кадров уровня LLC?
44. В каком поле кадра данных указывается принадлежность к типу MAC (LLC)?
45. Чему равна максимальная и минимальная длина поля данных в кадрах ЛВС Token Ring?

46. Из каких соображений выбирается максимальная длина поля данных в кадрах ЛВС Token Ring?
47. Рассчитать максимальную длину поля данных в кадре ЛВС Token Ring с пропускной способностью 4 (16) Мбит/с?
48. Какую дополнительную информацию и для чего содержит концевой разделитель кадра ЛВС Token Ring?
49. Как функционирует сеть Token Ring, если "бит обнаруженной ошибки" в концевом разделителе кадра имеет значение "1"?
50. О чём свидетельствует значение "бита распознавания адреса", равное 1 (0)?
51. О чём свидетельствует значение "бита копирования пакета в буфер"), равное 1 (0)?
52. Из каких соображений определяется максимальное число станций в одном кольце ЛВС Token Ring?
53. Основные достоинства и недостатки ЛВС Token Ring.

### **3.5. ЛВС FDDI**

1. Что означает аббревиатура FDDI?
2. Назначение сетевой технологии FDDI.
3. Какая пропускная способность обеспечивается в ЛВС FDDI?
4. Нарисовать и пояснить структуру ЛВС FDDI.
5. Пояснить на рисунке принцип реорганизации ЛВС FDDI при обрыве в кабеле и при отказе рабочей станции.
6. Для чего используется оптический обходной переключатель?
7. Функции связного концентратора в сети FDDI.
8. Какой метод доступа используется в сети FDDI?
9. Основные отличия метода доступа FDDI от Token Ring.
10. В чём отличие асинхронной станции от синхронной в сети FDDI?

### **3.6. Беспроводные ЛВС**

1. Какими преимуществами и недостатками обладают беспроводные ЛВС?
2. В чём состоит проблема «скрытого терминала»?
3. Какие методы доступа к среде передачи используются в беспроводных ЛВС?
4. Чему равен диаметр беспроводных ЛВС?
5. Для каких ЛВС разработана технология расширенного спектра?
6. В чём состоит идея технологии расширенного спектра?
7. В чём суть методов OFDM, FHSS и DSSS?
8. Проиллюстрировать на рисунке с необходимыми пояснениями идею методов OFDM и FHSS.
9. Как в методе FHSS формируется последовательность частот?
10. Что такое «чип» в методе FHSS?
11. В чём отличие режима медленного расширения спектра от режима быстрого расширения в методе FHSS?

12. При каком режиме расширения спектра в методе FHSS период передачи данных меньше (больше) периода передачи чипа?
13. Проиллюстрировать на рисунке с необходимыми пояснениями режимы медленного и быстрого расширения спектра в методе FHSS.
14. Какой режим расширения спектра в методе FHSS обеспечивает большую помехоустойчивость и почему?
15. Что такое расширяющая последовательность в методе DSSS?
16. Каким образом представляются в методе DSSS единичный и нулевой биты?
17. Что такое «коэффициент расширения» в методе DSSS, и в каких пределах он находится?
18. Раскрыть аббревиатуру CDMA.
19. Проиллюстрировать на примере идею метода CDMA.
20. Перечислить достоинства и недостатки беспроводных ЛВС.
21. Нарисовать и пояснить топологии беспроводных ЛВС.
22. В каком частотном диапазоне работают беспроводные ЛВС 802.11?
23. Какие скорости передачи данных обеспечиваются в беспроводных ЛВС 802.11?
24. Сформулировать основные отличия технологии WiMax от WiFi/
25. Назначение и особенности персональных сетей.
26. Какие устройства могут входить в состав персональных сетей?
27. Что такое Bluetooth?
28. Сколько устройств может входить в состав сети Bluetooth?
29. Сколько устройств в сети Bluetooth одновременно могут быть активными?
30. Чему равна область покрытия сети Bluetooth?
31. Что представляет собой технология ZigBee?
32. Основные отличия технологии ZigBee от Bluetooth?
33. Назначения координатора, маршрутизатора и конечного устройства в сетях ZigBee.
34. Что такое сенсорные сети?
35. Что представляет собой сенсор?
36. Сколько устройств может быть подключено к сенсорной сети?

## **Раздел 4. ГЛОБАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ**

### **4.1. Принципы организации глобальных сетей**

1. Что такое территориально-распределённая сеть?
2. Характерные особенности глобальных сетей.
3. Какое оборудование используется для объединения сетей?
4. Какая топология характерна для глобальных сетей?
5. Какие достоинства присущи глобальным сетям?

### **4.2. Технические средства объединения сетей**

1. Назначение мостов, маршрутизаторов, коммутаторов и шлюзов.
2. Нарисовать пример сети с использованием мостов.
3. Сформулировать алгоритм функционирования моста.
4. Какие достоинства и недостатки присущи мостам (маршрутизаторам)?
5. На каком уровне OSI-модели работают мосты (маршрутизаторы)?
6. Краткая характеристика прозрачных, транслирующих и инкапсулирующих мостов.
7. Принцип обнаружения маршрута в мостах с маршрутизацией от источника.
8. Перечислить характерные особенности мостов и маршрутизаторов.
9. Выполнить сравнительный анализ мостов и маршрутизаторов.
10. Основные отличия коммутатора от моста и маршрутизатора.
11. В чём заключается основное преимущество коммутатора по сравнению с маршрутизатором?
12. Что такое автономная система?
13. Какие протоколы используются для внутренней маршрутизации?
14. Что такое DVA и LSA?
15. Какой протокол основан на алгоритме обмена DVA (LSA)?
16. В чём состоит основное отличие протокола OSPF от протокола RIP?
17. Нарисовать каноническую структуру коммутатора.
18. Режимы работы коммутатора и их краткая характеристика.
19. Что такое микросегментация?
20. Для чего необходим механизм управления потоками кадров в коммутаторе?
21. Как реализуется механизм управления потоками кадров в дуплексном и полудуплексном режимах коммутации?
22. В чём суть методов обратного давления и агрессивного поведения в коммутаторах?
23. Основные способы технической реализации коммутаторов.
24. Перечислить дополнительные функции коммутаторов.
25. Для чего в мостах и коммутаторах используется «алгоритм покрывающего дерева»?
26. Показать на примере идею алгоритма «Spanning Tree».
27. Что представляет собой шлюз?

### **4.3. Сети с установлением соединений**

1. В чем отличие каналов PVC от SVC?
2. Какие сети используют технологию «виртуального канала»?
3. Проиллюстрировать на примере принцип коммутации пакетов на основе виртуального канала.
4. Что представляет собой пакет «Call Request»?
5. Какая информация содержится в таблице коммутации?
6. Чем таблица коммутации отличается от таблицы маршрутизации?
7. Перечислить достоинства принципа коммутации пакетов на основе виртуального канала.
8. Назначение стандарта X.25.
9. Специфические особенности сетей X.25.
10. Что такое PAD и ЦКП в сетях X.25?
11. Какие основные функции присущи PAD и ЦКП в сетях X.25?
12. Кадры какой длины предпочтительней в случае качественного (некачественного) канала связи в сетях X.25?
13. Может ли в сети X.25 пакет быть длиннее кадра? Ответ обосновать.
14. Какими достоинствами обладают сети X.25?
15. Для чего предназначены сети Frame Relay?
16. Перечислить особенности сетей Frame Relay.
17. В чем основное отличие стандарта Frame Relay от X.25?
18. За счет чего в сети Frame Relay обеспечивается более высокая скорость доставки пакетов, чем в X.25?
19. В каких случаях протокол X.25 более эффективен, чем Frame Relay?
20. Перечислить параметры качества обслуживания в сетях Frame Relay.
21. Что такое CIR?
22. Что такое согласованная информационная скорость, согласованный объем пульсации и дополнительный объем пульсации?
23. Каким соотношением связаны согласованная информационная скорость и согласованный объем пульсации?
24. Проиллюстрировать на графике процедуру поддержки качества обслуживания в сети Frame Relay.
25. За счёт чего в сети Frame Relay обеспечивается поддержка качества обслуживания?
26. Что такое ATM ?
27. В чём отличие пульсирующего трафика от потокового?
28. Какие базовые принципы лежат в основе ATM-технологии?
29. Почему размер ячейки в ATM-сетях не должен быть слишком большим и слишком маленьким?
30. Основные преимущества ячеек перед кадрами.
31. Почему ячейки требуют меньших затрат на буферизацию, чем кадры?
32. Почему обработка ячеек происходит быстрее, чем обработка кадров?
33. Что такое QoS?
34. Чем интерфейс UNI отличается от интерфейса NNI в ATM-сетях?

35. Основные функции ATM-коммутатора.
36. В чем отличие ATM-коммутатора от маршрутизатора?
37. Нарисовать и пояснить многоуровневую модель ATM.
38. Перечислить уровни ATM-модели.
39. Нарисовать и пояснить формат заголовка ATM-ячейки.
40. Назначение поля "Управление потоком" в заголовке ATM-ячейки.
41. Назначение поля "Тип полезной нагрузки" в заголовке ATM-ячейки.
42. Назначение поля "Приоритет потери" в заголовке ATM-ячейки.
43. Понятие виртуального соединения (виртуального пути, виртуального канала).
44. В чем отличие виртуального пути от виртуального канала?
45. Может ли один виртуальный путь содержать несколько виртуальных каналов?
46. Чему равно максимально возможное число виртуальных путей в ATM-сетях?
47. Чему равно максимально возможное число виртуальных каналов в пределах одного виртуального пути в ATM-сетях?
48. Какую информацию содержат маршрутные (адресные) таблицы ATM-коммутаторов?
49. Проиллюстрировать на рисунке формирование маршрутной таблицы ATM-коммутаторов, сопроводив необходимыми пояснениями.

#### **4.4. Глобальная сеть Internet**

1. Особенности протоколов TCP/IP.
2. Нарисовать многоуровневую модель управления в TCP/IP-сетях.
3. Что обеспечивает протокол IP?
4. Перечислить наиболее известные протоколы прикладного, транспортного, межсетевого и канального уровня стека TCP/IP.
5. Назначение протоколов FTP, BGP, HTTP, SNMP, SIP, SMTP, POP3, TELNET, PPTP, RTP, ICMP, IGMP.
6. Какие типы адресов используются в стеке TCP/IP?
7. Что представляют собой локальные (сетевые, доменные) адреса?
8. Сколько IP-адресов может иметь компьютер?
9. Чему равна длина IP-адреса версии 4 (версии 6)?
10. Классы IP-адресов и их краткое описание.
11. Сколько узлов может иметь сеть с адресом 118.x.x.x?
12. Изменится ли IP-адрес, если хост переносится из одной подсети в другую?
13. Примеры специальных, автономных и групповых адресов.
14. Назначение масок для IP-адресов.
15. Определить адрес сети и узла для IP-адреса 126.65.32.5 с маской 255.192.0.0.
16. Чему равно максимальное количество хостов в сети с маской 255.255.248.0?
17. Какой вид имеют маски для сетей классов A, B и C?

18. Какие адреса в Интернете используются автономно и не обрабатываются маршрутизаторами?
19. Два способа назначения IP-адресов.
20. Какие IP-адреса являются некорректными?
  - 1) 192.164.265.34
  - 2) 145.1.0.1
  - 3) 5.64.111.256
  - 4) 13.0.0.1.1
  - 5) 126.14.65.34
21. Назначение протокола DHCP.
22. В чем отличие динамического IP-адреса от статического?
23. Что такое CIDR?
24. В чем состоит основная идея технологии CIDR?
25. Что понимается под пулом адресов и префиксом в технологии CIDR?
26. Сколько адресов содержит пул с префиксом длиной 20 бит?
27. Чему равен префикс пула, содержащего 1024 адреса?
28. Как определяется физический адрес устройства (MAC-адрес) по его IP-адресу?
29. Назначение протоколов ARP и RARP.
30. Что представляет собой доменное имя?
31. Что такое DNS?
32. Чему равен минимальный (максимальный) размер заголовка IP-пакета?
33. Какая информация содержится в заголовке IP-пакета?
34. Чему равна минимальная и максимальная длина IP-заголовка?
35. Чему равна максимально возможная длина IP-пакета?
36. Назначение полей «номер версии», «тип сервиса», «идентификатор пакета» в заголовке IP-пакета?
37. Основная цель перехода с протокола IPv4 на IPv6?
38. Какие особенности присущи протоколу IPv6?
39. Какую длину имеет адрес в протоколе IPv6?
40. Сколько уровней иерархии адреса предусмотрено в протоколе IPv6?
41. В чём отличие в записи адресов протокола IPv6 от IPv4?
42. Для чего нужен адрес произвольной рассылки в протоколе IPv6?
43. Что представляет собой глобальный агрегируемый уникальный адрес в протоколе IPv6?
44. Какие дополнительные заголовки могут использоваться в IPv6?
45. Какую длину имеет основной заголовок IPv6?
46. Для чего необходимо поле «Максимальное число транзитных участков» в основном заголовке IPv6?
47. Как называется процесс разбиения длинных пакетов на более короткие в процессе передачи по сети?
48. Что такое MTU?
49. Чем сквозная фрагментация отличается от прозрачной?
50. Что такое элементарный фрагмент и для чего он используется?

51. Что используется на транспортном уровне стека TCP/IP в качестве адреса?
52. Сколько портов может быть сформировано для одного прикладного процесса?
53. В чем отличие централизованного способа присвоения порта приложению от локального?
54. Назначение протоколов UDP, TCP и ICMP.
55. В чем отличие протокола UDP от TCP?
56. Нарисовать и пояснить формат заголовка UDP-сегмента.
57. Что представляет собой сокет?
58. Сколько сокетов необходимо для описания логического соединения?
59. Привести пример описания логического соединения с помощью сокетов.
60. Что представляет собой сегмент в протоколе TCP?
61. Какой механизм используется для управления потоком данных в протоколе TCP?
62. За счет чего в протоколе TCP обеспечивается надежная передача данных?
63. Как вычисляется контрольная сумма в протоколе TCP?
64. Что такое псевдозаголовок в протоколах UDP и TCP и для чего он используется?
65. Какие функции возложены на протокол ICMP?
66. Какие требования предъявляются к протоколам канального уровня для выделенных линий?
67. Перечислить протоколы канального уровня для выделенных линий.
68. Основная функция протокола SLIP.
69. Какие недостатки присущи протоколу SLIP?
70. Основная функция протоколов семейства HDLC.
71. Какие протоколы включает в себя семейство протоколов HDLC?
72. Для каких сетей предназначены протоколы LAP-B, LAP-D и LAP-F?
73. Нарисовать формат и пояснить назначение полей кадра HDLC.
74. Для чего в HDLC предназначены информационные, управляющие и ненумерованные кадры?
75. Чему равна ширина окна в протоколе HDLC?
76. Назначение протокола PPP.
77. Какие протоколы включает в себя семейство протоколов PPP?
78. На каких принципах основан протокол PPP?
79. Что используется в качестве флага в кадрах PPP?

#### **4.5. MPLS-технология**

1. Краткая характеристика MPLS-технологии.
2. В чем различие между LSR и LER?
3. Перечислить основные функции LSR и LER.
4. Какие данные содержат таблицы продвижения в MPLS-сетях?
5. Нарисовать пример MPLS-сети.

6. Нарисовать и пояснить структуру кадра с MPLS-заголовком.
7. Нарисовать и пояснить структуру MPLS-заголовка.
8. Чему равна длина метки в MPLS-сетях?
9. Какие поля содержит MPLS-заголовок?
10. Что такое и для чего используется стек меток в MPLS-сетях?
11. Нарисовать структуру стека меток, используемых в MPLS-сетях?
12. Что является признаком «дна стека меток» в MPLS-сетях?
13. Пояснить на примере использование стека меток в MPLS-сетях.
14. Какие операции с метками используются в MPLS-сетях?

#### **4.6. Пример передачи данных в составной сети**

1. На каком уровне формируется UDP-дейтаграмма?
2. Что указывается в заголовке UDP-дейтаграммы в качестве адресов?
3. Что указывается в заголовке IP-пакета в качестве адресов?
4. Что указывается в заголовке кадра в качестве адресов?
5. Что делает маршрутизатор, если контрольная сумма кадра совпадает с рассчитанным значением?
6. Что делает маршрутизатор, если не совпадает контрольная сумма кадра?

#### **4.7. Безопасность компьютерных сетей**

1. Для чего предназначены средства компьютерной безопасности?
2. Что такое брандмауэр и для чего он нужен?
3. Для чего предназначены средства сетевой безопасности?
4. Какими свойствами должна обладать безопасная информационная система?
5. Определить понятия «конфиденциальность», «доступность» и «целостность».
6. Что обеспечивают сервисы сетевой безопасности?
7. Что относится к основным сервисам сетевой безопасности?
8. Что представляет собой криптосистема?
9. В чём отличие идентификации от аутентификации?
10. В чём отличие идентификации от авторизации?
11. Что такое аудит?
12. Назначение технологии защищённого канала.
13. За счёт чего технология защищённого канала обеспечивает безопасность передачи данных по открытой транспортной сети?
14. Для чего предназначен протокол IPSec?
15. В чём различие между транспортным и туннельным режимами защиты данных?
16. Назначение протоколов AH и ESP.
17. Для чего используется секретный ключ?
18. Что такое защищённый IP-туннель?
19. Что представляет собой шлюз безопасности?

## Используемые аббревиатуры

### А

<b>АДИКМ</b>	адаптивная дифференциальная импульсно-кодовая модуляция
<b>АИ</b>	адрес источника
<b>АИМ</b>	амплитудно-импульсная модуляция
<b>АМ</b>	амплитудная модуляция
<b>АН</b>	адрес назначения
<b>АП</b>	абсолютный приоритет
<b>АПД</b>	аппаратура передачи данных
<b>АРД</b>	асинхронный режим доставки (передачи) (англ.аббр. - <i>ATM</i> )

### Б

<b>БД</b>	база данных
<b>БМ</b>	базовая модель
<b>БП</b>	бесприоритетное обслуживание

### В

<b>ВЗУ</b>	внешние запоминающие устройства
<b>ВК</b>	вычислительный комплекс
<b>ВО</b>	внешний объект
<b>ВОК</b>	волоконно-оптический кабель
<b>ВОЛС</b>	волоконно-оптическая линия связи
<b>ВОС</b>	взаимодействие открытых систем
<b>ВС</b>	вычислительная система
<b>ВТ</b>	вычислительная техника
<b>ВУ</b>	внешнее устройство

### Г

<b>ГВМ</b>	главная ЭВМ (хост-машина)
<b>ГВС</b>	глобальная вычислительная сеть
<b>ГМ</b>	глобальная модель

### Д

<b>ДБ</b>	дисциплина буферизации
<b>ДО</b>	дисциплина обслуживания

### З

<b>ЗСт</b>	земная станция
<b>ЗСеМО</b>	замкнутая сеть массового обслуживания

### И

<b>ИКМ</b>	импульсно-кодовая модуляция (англ.аббр. – <i>PCM</i> )
<b>ИМ</b>	имитационная модель
<b>ИММ</b>	иерархическое многоуровневое моделирование
<b>ИС</b>	источник сообщения
<b>ИСЗ</b>	искусственный спутник земли

### К

<b>КВВ</b>	канал ввода-вывода
<b>КС</b>	канал связи

---

<b>КСм</b>	контрольная сумма
<b>КСт</b>	космическая станция
	<b>Л</b>
<b>ЛА</b>	линейный адаптер
<b>ЛВС</b>	локальная вычислительная сеть
<b>ЛМ</b>	локальная модель
<b>ЛС</b>	линия связи
	<b>М</b>
<b>МК СМО</b>	многоканальная система массового обслуживания
<b>ММВК</b>	многомашинный вычислительный комплекс
<b>ММО</b>	модель массового обслуживания
<b>МП</b>	матрица приоритетов
<b>МПД</b>	мультиплексор передачи данных
<b>МПВК</b>	многопроцессорный вычислительный комплекс
	<b>О</b>
<b>ОК СМО</b>	одноканальная система массового обслуживания
<b>ООД</b>	оконечное оборудование данных
<b>ОП</b>	оперативная (основная) память
<b>ОПр</b>	относительный приоритет
<b>ОС</b>	операционная система
	<b>П</b>
<b>ПВВ</b>	процессор ввода-вывода
<b>ПК</b>	персональный компьютер
<b>ПП</b>	прикладная программа
<b>ПС</b>	приемник сообщения
<b>ПСр</b>	программные средства
	<b>Р</b>
<b>РРС</b>	радиорелейная станция
<b>РС</b>	рабочая станция
<b>РСеМО</b>	разомкнутая сеть массового обслуживания
<b>РРЛС</b>	радиорелейная линия связи
	<b>С</b>
<b>СА</b>	сетевой адаптер
<b>СВ</b>	сеть вычислительная
<b>СВТ</b>	средства вычислительной техники
<b>СеМО</b>	сеть массового обслуживания
<b>СКС</b>	структурированная кабельная система
<b>СМО</b>	система массового обслуживания
<b>СП</b>	смешанный приоритет
<b>СПД</b>	сеть передачи данных
<b>ССС</b>	спутниковая система связи
<b>СТК</b>	средства телекоммуникаций
<b>СТО</b>	система телеобработки
<b>СУБД</b>	система управления базами данных

---

<b>СХД</b>	сеть хранения данных
	<b>Т</b>
<b>ТВМ</b>	терминальная ЭВМ
<b>ТКС</b>	телекоммуникационная сеть
<b>ТРВС</b>	территориально-распределенная вычислительная сеть
<b>ТСр</b>	технические средства
<b>ТфКС</b>	телефонный канал связи
	<b>У</b>
<b>УВВ</b>	устройства ввода-вывода
<b>УК</b>	узел коммутации
<b>УМПД</b>	удаленный мультиплексор передачи данных
<b>УП</b>	управляющая программа
<b>УС</b>	узел связи
	<b>Ф</b>
<b>ФМ</b>	фазовая модуляция
	<b>Ц</b>
<b>ЦП</b>	центральный процессор
<b>ЦСИО</b>	цифровые сети интегрального обслуживания ( <i>ISDN</i> )
<b>ЦРРЛС</b>	цифровая радиорелейная линия связи
	<b>Ч</b>
<b>ЧП</b>	чредующийся приоритет
<b>ЧМ</b>	частотная модуляция
	<b>Э</b>
<b>ЭВМ</b>	электронная вычислительная машина
<b>ЭПИ</b>	электромагнитное поле излучение

**A**

- ADPCM** (*Adaptive Differential Pulse Code Modulation*) – Адаптивная дифференциальная (разностная) импульсно-кодовая модуляция (АДИКМ)
- ADSL** (*Asymmetrical Digital Subscriber Line*) – Асимметричная цифровая абонентская линия
- AMI** (*Bipolar Alternate Mark Inversion*) – Биполярное кодирование с альтернативной инверсией
- ANSI** (*American National Standards Institute*) – Американский национальный институт стандартов
- API** (*Application Programming Interface*) – Интерфейс прикладного программирования
- ARP** (*Address Resolution Protocol*) – Протокол разрешения адресов
- ASK** (*Amplitude Shift Keying*) – Амплитудная манипуляция
- ATM** (*Asynchronous Transfer Mode*) – Режим асинхронной передачи (доставки)

**B**

- BER** (*Bit Error Rate*) – Интенсивность битовых ошибок
- B-ISDN** (*Broadband Integrated Services Digital Network*) – Широкополосная ISDN

**C**

- CIR** (*Committed Information Rate*) – Согласованная информационная скорость
- CoS** (*Class of Service*) – Класс услуги (сервиса)
- CRC** (*Cyclic Redundancy Check*) – Циклический контрольный код
- CDMA** (*Code Division Multiple Access*) – Множественный доступ с кодовым разделением
- CSMA/CA** (*Carrier Sense Multiple Access Collision Avoidance*) – Множественный доступ с проверкой несущей и предотвращением столкновений
- CSMA/CD** (*Carrier Sense Multiple Access Collision Detection*) – Множественный доступ с проверкой несущей и обнаружением столкновений
- CSU** (*Channel Service Unit*) – Устройство обслуживания канала

**D**

- DARPA** (*Defence Advanced Research Projects Agency*) – Управления перспективных исследований Министерства обороны США
- DAS** (*Dual Attach Station*) – Станция с двойным подключением
- DCE** (*Data Communication Equipment*) – Аппаратура передачи данных (АПД)
- DHCP** (*Dynamic Host Configuration Protocol*) – Протокол динамического конфигурирования хостов (автоматического назначения IP-адресов)
- DNS** (*Domain Name System*) – Система доменных имен
- DQDB** (*Distributed Queue Dual Bus*) – Двойная шина с распределенной очередью

---

<b>DSAP</b>	<i>(Destination Service Access Point)</i> – Точка доступа к услугам получателя
<b>DSL</b>	<i>(Digital Subscriber Line)</i> – Цифровая абонентская линия
<b>DSLAM</b>	<i>(DSL Access Multiplexer)</i> – Мультиплексор доступа к цифровой абонентской линии
<b>DSSS</b>	<i>(Direct Sequence Spread Spectrum)</i> – Прямое последовательное расширение спектра
<b>DSU</b>	<i>(Data Service Unit)</i> – Устройство обслуживания данных
<b>DTE</b>	<i>(Data Terminal Equipment)</i> – Оконечное (терминальное) оборудование данных (ООД)
	<b>E</b>
<b>ETR</b>	<i>(Early Token Release)</i> – Раннее освобождение маркера
	<b>F</b>
<b>FDDI</b>	<i>(Fiber Distributed Data Interface)</i> – Оптоволоконный интерфейс распределения данных
<b>FDM</b>	<i>(Frequency Division Multiplexing)</i> – Частотное мультиплексирование (уплотнение)
<b>FEXT</b>	<i>(Far End Crosstalk)</i> – Перекрестные наводки на дальнем конце
<b>FHSS</b>	<i>(Frequency Hopping Spread Spectrum)</i> – Расширение спектра скачкообразной перестройкой частоты
<b>FSK</b>	<i>(Frequency Shift Keying)</i> – Частотная манипуляция
<b>FTP</b>	1. <i>(File Transfer Protocol)</i> – Протокол передачи файлов 2. <i>(Foiled Twisted Pair)</i> – Экранированная витая пара
	<b>G</b>
<b>GAN (GN)</b>	<i>(Global (Area) Network)</i> – Глобальная вычислительная сеть (ГВС)
	<b>H</b>
<b>HTTP</b>	<i>(HyperText Transfer Protocol)</i> – Протокол передачи гипертекстовой информации
	<b>I</b>
<b>ICANN</b>	<i>(Internet Corporation for Assigned Names and Numbers)</i> – Интернет-корпорация по регистрации глобальных IP-адресов
<b>ICMP</b>	<i>(Internet Control Message Protocol)</i> – Протокол управляющих сообщений Интернета
<b>IEEE</b>	<i>(The Institute of Electrical and Electronics Engineers)</i> – Институт инженеров по электротехнике и электронике
<b>IGMP</b>	<i>(Internet Group Management Protocol)</i> – Протокол управления групповой IP-адресацией
<b>IP</b>	<i>(Internet Protocol)</i> – Межсетевой протокол
<b>IPG</b>	<i>(Inter Package Gap)</i> – Межкадровый интервал
<b>IPX</b>	<i>(Internetwork Packet eXchange)</i> – Протокол межсетевого обмена пакетами
<b>ISDN</b>	<i>(Integrated Services Digital Network)</i> – Цифровая сеть интегрального обслуживания (ЦСИО)

---

<b>ITU</b>	<i>(International Telecommunications Union)</i> – Международный телекоммуникационный союз
	<b>L</b>
<b>LAN</b>	<i>(Local Area Network)</i> – Локальная вычислительная сеть (ЛВС)
<b>LCP</b>	<i>(Link Control Protocol)</i> – Протокол управления соединением
<b>LDP</b>	<i>(Label Distribution Protocol)</i> – Протокол распределения меток
<b>LER</b>	<i>(Label switch Edge Router)</i> – Пограничный коммутирующий по меткам маршрутизатор
<b>LSP</b>	<i>(Label Switching Path)</i> – Путь коммутации по меткам
<b>LSR</b>	<i>(Label Switch Router)</i> – Коммутирующий по меткам маршрутизатор
	<b>M</b>
<b>MAC</b>	<i>(Media Access Control)</i> – Управление доступом к среде
<b>MAN</b>	<i>(Metropolitan Area Network)</i> – Городская вычислительная сеть (ГВС)
<b>MAU</b>	<i>(Media Attachment Unit)</i> – Приемопередатчик Ethernet
<b>MLPPP</b>	<i>(Multi Link PPP)</i> – Многоканальный протокол PPP
<b>MLT-3</b>	<i>(Multi Level Transmission-3)</i> – Код трехуровневой передачи
<b>MPLS</b>	<i>(MultiProtocol Label Switching)</i> – Многопротокольная коммутация по меткам
<b>MSAU</b>	<i>(Multistation Access Unit)</i> – Устройство множественного доступа (концентратор в сети TokenRing)
<b>MTU</b>	<i>(Maximum Transfer Unit)</i> – Максимально допустимая длина блока данных
	<b>N</b>
<b>NAS</b>	<i>(Network Attached Storage)</i> – Сетевая система хранения данных
<b>NCP</b>	1. <i>(Network Control Protocol)</i> – Протокол управления сетью 2. <i>([Nowell] NetWare Core Protocol)</i> – Протокол ядра NetWare
<b>NEXT</b>	<i>(Near End Crosstalk)</i> – Перекрестные наводки на ближнем конце
<b>NIC</b>	<i>(Network Interface Card/Controller)</i> – Сетевой адаптер/контроллер [сетевая интерфейсная плата]
<b>NLA</b>	<i>(Next-Level Aggregation)</i> – Агрегирование следующего уровня
<b>NNI</b>	<i>(Network-Network Interface)</i> – Интерфейс «сеть-сеть»
<b>NRZ</b>	<i>(Non-Return to Zero)</i> – Кодирование без возврата к нулю
<b>NRZI</b>	<i>(Non-Return to Zero Inverted)</i> – Кодирование без возврата к нулю с инверсией
	<b>O</b>
<b>OBS</b>	<i>(Optical Bypass Switch)</i> – Оптический обходной переключатель
<b>OFDM</b>	<i>(Orthogonal Frequency Division Multiplexing)</i> – Ортогональное частотное мультиплексирование
<b>OSI</b>	<i>(Open Systems Interconnection)</i> – Взаимодействие открытых систем
<b>OUI</b>	<i>(Organizationally Unique Identifier)</i> – Организационно уникальные идентификаторы

---

<b>P</b>	
<b>PAM</b>	<i>(Pulse Amplitude Modulation)</i> – Амплитудно-импульсная модуляция (АИМ)
<b>PAN</b>	<i>(Personal Area Networks)</i> – Персональные сети
<b>PCM</b>	<i>(Pulse Code Modulation)</i> – Импульсно-кодовая модуляция (ИКМ)
<b>PDH</b>	<i>(Plesiochronous Digital Hierarchy)</i> – Плазиохронная цифровая иерархия
<b>PDV</b>	<i>(Path Delay Value)</i> – Значение задержки пути (время двойного оборота)
<b>PDU</b>	<i>(Protocol Data Unit)</i> – Протокольный блок данных (ПБД)
<b>PSK</b>	<i>(Phase Shift Keying)</i> – Фазовая манипуляция
<b>PVC</b>	<i>(Permanent Virtual Circuit (Connect))</i> – Постоянный виртуальный канал (соединение)
<b>PVV</b>	<i>(Path Variability Value)</i> – Значение изменчивости пути (сокращение межкадрового интервала)
<b>Q</b>	
<b>QAM</b>	<i>(Quadrature Amplitude Modulation)</i> – Квадратурная амплитудная модуляция
<b>QoS</b>	<i>(Quality of Service)</i> – Качество сервиса
<b>R</b>	
<b>RARP</b>	<i>(Reverse Address Resolution Protocol)</i> – Протокол обратного определения адреса
<b>RMON</b>	<i>(Remote Monitoring)</i> – Удаленный мониторинг
<b>RZ</b>	<i>(Return to Zero)</i> – Метод кодирования с возвратом к нулю
<b>S</b>	
<b>SAN</b>	<i>(Storage Area Network)</i> – Сеть хранения данных (СХД)
<b>SAP</b>	<i>(Service Advertising Protocol)</i> – Протокол извещения об услугах
<b>SDH</b>	<i>(Synchronous Digital Hierarchy)</i> – Синхронная цифровая иерархия
<b>SIP</b>	<i>(Session Initiation Protocol)</i> – Протокол инициализации сессии
<b>SLA</b>	<i>(Site-Level Aggregation)</i> – Агрегирование местного уровня
<b>SMTP</b>	<i>(Simple Mail Transfer Protocol)</i> – Простой протокол передачи почты
<b>SNAP</b>	<i>(SubNetwork Access Protocol)</i> – Протокол доступа к подсети
<b>SNMP</b>	<i>(Simple Network Management Protocol)</i> – Простой протокол управления сетью
<b>SNR</b>	<i>(Signal-to-Noise Ratio)</i> – Отношение сигнал/шум
<b>SONET</b>	<i>(Synchronous Optical NETwork)</i> – Синхронная оптическая сеть
<b>SPVC</b>	<i>(Smart Permanent Virtual Circuit)</i> – Интеллектуальный постоянный виртуальный канал
<b>SPX</b>	<i>(Sequenced Packet Exchange)</i> – Последовательный обмен пакетами
<b>SSAP</b>	<i>(Source Service Access Point)</i> – Точка доступа к услугам источника
<b>STM</b>	<i>(Statistical Multiplexing)</i> – Статистическое мультиплексирование (уплотнение)
<b>STM-n</b>	<i>(Synchronous Transport Module-n)</i> – Синхронный транспортный модуль – n

---

<b>STP</b>	<i>(Shielded Twisted Pair)</i> – Экранированная витая пара
<b>STS-n</b>	<i>(Synchronous Transport Signal - n)</i> – Синхронный транспортный сигнал – n
<b>SVC</b>	<i>(Switched Virtual Circuit (Connect))</i> – Коммутируемый виртуальный канал (соединение)
	<b>T</b>
<b>TAPI</b>	<i>(Telephony Application Programming Interface)</i> – Интерфейс программирования приложений телефонной связи
<b>TCP</b>	<i>(Transmission Control Protocol)</i> – Протокол управления передачей (протокол транспортного уровня)
<b>TCP/IP</b>	<i>(Transmission Control Protocol/Internet Protocol)</i> – Протокольный набор (стек протоколов) TCP/IP
<b>TDM</b>	<i>(Time Division Multiplexing)</i> – Временное мультиплексирование (уплотнение)
<b>TLA</b>	<i>(Top-Level Aggregation)</i> – Агрегирование верхнего уровня
<b>TSAPI</b>	<i>(Telephony Services Application Programming Interface)</i> – Интерфейс прикладного программирования для управления телефонной связью
<b>TTL</b>	<i>(Time To Live)</i> – Время жизни
	<b>U</b>
<b>UART</b>	<i>(Universal Asynchronous Receiver/Transmitter)</i> – Универсальный асинхронный приемопередатчик
<b>UDP</b>	<i>(User Datagram Protocol)</i> – Протокол пользовательских дейтаграмм
<b>UNI</b>	<i>(User-Network Interface)</i> – Интерфейс «пользователь-сеть»
<b>UTP</b>	<i>(Unshielded Twisted Pair)</i> – Экранированная витая пара
	<b>V</b>
<b>VCI</b>	<i>(Virtual Circuit Identifier)</i> – Идентификатор виртуального канала (ИВК)
<b>VLAN</b>	<i>(virtual LAN)</i> – Виртуальная ЛВС
<b>VPI</b>	<i>(Virtual Path Identifier)</i> – Идентификатор виртуального пути (ИВП)
<b>VPN</b>	<i>(Virtual Private Network)</i> – Виртуальная частная сеть
<b>VSAT</b>	<i>(Very Small Aperture Terminal)</i> – Технология малоапертурных спутниковых терминалов
	<b>W</b>
<b>WAN</b>	<i>(Wide Area Network)</i> – Территориально-распределенная сеть
<b>WDM</b>	<i>(Wave Division Multiplexing)</i> – Волновое мультиплексирование
<b>WLAN</b>	<i>(wireless LAN)</i> – Беспроводная ЛВС
<b>WWW</b>	<i>(World Wide Web)</i> – Всемирная паутина
	<b>X</b>
<b>xDSL</b>	<i>(x Digital Subscriber Line)</i> – Цифровая абонентская линия типа «x»

## **Список литературы**

1. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. / В.Г.Олифер, Н.А.Олифер. – СПб: Питер, 2006. – 958 с.: ил.
2. Таненбаум Э. Компьютерные сети. 4-е изд. – СПб.: Питер, 2003. – 992 с.: ил.
3. Столингс В. Современные компьютерные сети. – СПб.: Питер, 2003. – 783 с.: ил.
4. Хелд Г. Технологии передачи данных. 7-е изд. – СПб.: Питер, К.: Издательская группа BHV, 2003. – 720 с.: ил.
5. Новиков Ю.В., Карпенко Д.Г. Аппаратура локальных сетей: функции, выбор, разработка. - М.: Изд-во ЭКОМ, 1998. - 288 с.: ил.
6. Лаура А.Чапpell, Дэн Е.Хейкс. Анализ локальных сетей NetWare: Пер.с англ. – М.: ЛОРИ, 1995. - 596 с.
7. Барри Нанс. Компьютерные сети: Пер. с англ. – М.: Восточная книжная компания, 1996. - 400 с.: ил.
8. Ларионов А.М., Майоров С.А., Новиков Г.И. Вычислительные комплексы, системы и сети/ Учебник для вузов. - Л.: Энергоатомиздат, Ленингр. отд-ние, 1987. - 288 с.: ил.

## Алфавитный указатель

- !**  
100VG-AnyLAN, 212
- A**  
AAL, 282  
ADSL, 157  
ARP, 293, 302  
ARP-запрос, 303  
ARP-ответ, 303  
ARP-таблица, 302  
ATM, 279
- B**  
BGP, 290  
B-ISDN, 156  
Bluetooth, 241
- C**  
CDMA, 236  
CIDR, 301  
CIR, 275  
CSMA/CA, 186  
CSMA/CD, 186  
CSU, 171
- D**  
DHCP, 290, 300  
DNS, 291, 305  
DNS-клиент, 305  
DNS-сервер, 305  
DSAP, 198  
DSSS, 235  
DSU, 171  
DS-байт, 307  
DVA, 257
- E**  
Ethernet, 188  
    Terabit, 218  
    быстрый, 209  
    тонкий, 192  
ETR, 187
- F**  
Fast Ethernet, 209  
FDDI, 227  
FHSS, 234  
Frame Relay, 274  
FTP, 290
- H**  
HDLC, 293, 325  
HTTP, 290  
Hub, 184
- I**  
ICMP, 292  
IEEE-модель, 29  
IGMP, 293  
IMAP, 291  
IP, 292  
IPsec, 342  
IP-адрес, 295  
ISDN, 154
- J**  
Jam-последовательность, 202
- L**  
LAN, 177  
LCN, 273  
LDP, 330  
LER, 331  
LGN, 273  
LLC-кадры, 224  
LLC-подровень, 29  
Loopback, 298  
LSA, 259  
LSP, 330  
LSR, 330  
LTE, 170
- M**  
MAC-адрес, 25  
MAC-кадры, 224  
MAC-подровень, 29  
MPLS, 329  
MSAU, 219  
MTU, 314
- N**  
NLA, 311
- O**  
OFDM, 233  
OSI-модель, 24  
    высшие уровни, 28  
    низшие уровни, 28  
OSPF, 259, 293

**P**  
PAD, 271  
PDV, 205  
Peer-to-peer, 181  
POP3, 291  
PPP, 293, 328  
PPTP, 291  
PVV, 207  
**R**  
RARP, 293, 304  
Repeater, 183  
RIP, 293  
RTP, 292  
**S**  
SDH, 173  
SIP, 291  
SLA, 311  
SLIP, 293, 325  
SMTP, 291  
SNAP, 199  
SNMP, 291  
SONET, 173  
SSAP, 198  
**T**  
TCP, 292  
TELNET, 291  
TFTP, 290  
TLA, 311  
Token Ring, 218  
**U**  
UDP, 292  
**V**  
VCI, 281  
VPI, 281  
**W**  
WAN, 246  
WiFi, 238  
WiMax, 169, 239  
**X**  
xDSL, 156  
**Z**  
ZigBee, 242

**A**  
Автономная система, 256  
Авторизация, 341  
Администрирование, 20  
Адрес  
автономный, 298  
глобальный агрегируемый  
уникальный, 311  
групповой, 297  
локальный, 294  
машинный, 25  
неопределённый, 298, 311  
обратной петли, 298, 311  
ограниченный  
широковещательный, 298  
порта, 26  
произвольной рассылки, 310  
прямой широковещательный,  
298  
сетевой, 26  
специальный, 297  
тестовый, 298  
транспортный, 317  
физический, 25, 294  
широковещательный, 297  
Активное сопротивление, 119  
Активный монитор, 221  
Алгоритм  
«Spanning Tree», 265  
отступления, 202  
предпочтения кратчайшего  
пути, 259  
Амплитуда, 84  
Апогей, 143  
Аппаратура  
передачи данных, 14  
уплотнения, 91  
Архитектура компьютерной сети,  
14  
Асинхронный режим передачи,  
279  
АТС, 147  
декадно-шаговая, 147  
квазиэлектронная, 148  
координатная, 148

- цифровая, 148  
электронная, 148
- Аудиоданные, 21
- Аудит, 341
- Аутентификация, 340
- Б**
- База данных, 12
- Байт дифференцированное обслуживание, 307
- Байт-стаффинг, 325
- Бит
- копирования пакета, 226
  - обнаруженной ошибки, 223
  - промежуточного кадра, 223
  - распознавания адреса, 226
- Битовый интервал, 99, 200
- Битрейт, 99
- Бит-стаффинг, 63
- Брандмауэр, 338
- В**
- Вектор, 258
- Вероятность безотказной работы, 74
- Вершина стека, 332
- Видеоданные, 21
- Видеоконференцсвязь, 21
- Виртуальный канал
- коммутируемый, 266
  - постоянный, 266
- Виртуальный контейнер, 175
- Виртуальный текстовый терминал, 291
- Витая пара, 119
- неэкранированная, 119
  - экранированная, 120
- Время
- восстановления, 74
  - двойного оборота, 205
  - доставки, 73
  - задержки, 73
  - наработки на отказ, 74
  - ответа, 73
  - отклика, 73
- Высокоуровневый протокол управления каналом, 293
- Вычислительная сеть
- городская, 17
  - локальная, 17
- Вычислительная система, 10
- многомашинная, 11
  - многопроцессорная, 11
- Вычислительный комплекс, 10
- многомашинный, 10
  - многопроцессорный, 10
- Г**
- Гальваническая развязка, 108
- Геркон, 148
- Гибкость, 22, 71
- Глобальная сеть, 246
- Д**
- Данные, 8
- голосовые, 21
  - мультимедийные, 21
  - телеграфные, 21
  - телефонные, 21
  - факсимильные, 21
- Дейтаграмма, 31, 51
- Дейтаграммный протокол передачи данных, 292
- Дескремблер, 115
- Дебибел, 82
- Джиттер, 86
- Диаметр сети, 182
- Дисперсия, 123
- Дифракция, 134
- Длина
- вектора, 258
  - волны, 133
- Дно стека, 332
- Домен
- имен, 304
  - коллизий, 189
- Доменное имя, 304
- Достоверность передачи, 25, 91
- Доступ
- маркерный, 186
  - множественный, 184
  - случайный, 185
  - тактированный, 185
- Доступность, 339

## Ё

Ёмкость, 119

## З

Загрузка, 75

Задание, 12

Задача, 12

Затухание, 118

в оптическом волокне, 122

Защищённый

IP-туннель, 343

канал, 342

Звено передачи данных, 16

## И

Идентификатор

виртуального канала, 267, 281

виртуального пути, 281

Идентификация, 341

Импеданс, 118

Интегративность, 11

Интенсивность

битовых ошибок, 91

отказов, 74

Интерфейс, 30

BRI, 156

PRI, 156

программный, 30

схемный, 30

Информационное обеспечение, 12

Информация, 8

Ионизированный слой, 133

## К

Кабель, 117

волоконно-оптический, 125

коаксиальный, 120

коаксиальный толстый, 121

коаксиальный тонкий, 121

медный, 117

связи, 117

электрический, 117

Кабельная система, 130

Кадр, 25, 31

ненумерованный, 327

управляющий, 327

Канал В, 155

Канал D, 155

Канал связи, 13, 82

аналоговый, 88

временный, 43, 90

выделенный, 43, 90

двухточечный, 90

дискретный, 89

дуплексный, 89

коммутируемый, 43, 90

многоточечный, 90

некоммутируемый, 43, 90

непрерывный, 88, 89

полудуплексный, 90

симплексный, 89

тональной частоты, 88

цифровой, 89

Квитанция

отрицательная, 64

положительная, 65

Клиент, 181

Код

AMI, 111

MLT-3, 113

NRZ, 109

RZ, 110

без возврата к нулю, 109

биполярный импульсный, 110

дифференциальный

манчестерский, 112

манчестерский, 112

потенциальный с инверсией

при единице, 112

пятиуровневый РАМ-5, 113

с возвратом к нулю, 110

трехуровневой передачи, 113

Кодирование, 81

биполярное с альтернативной  
инверсией, 111

избыточное, 114

логическое, 113

потенциальное, 99

физическое, 96

цифровое, 96

Коммутатор, 262

корневой, 265

Коммутация, 41

- каналов, 42  
пакетов, 45  
сообщений, 44  
ячеек, 49
- Компьютер, 9  
Конфиденциальность, 339  
Концентратор, 184  
Коррекция ошибок, 151  
Космическая станция, 139  
Коэффициент готовности, 74  
загрузки, 75  
затухания, 83, 118  
передачи, 82  
простоя, 75  
расширения, 236  
усиления, 83
- Л**
- ЛВС, 177  
Линия связи, 13, 81  
кабельная, 116  
радиорелейная, 138  
цифровая радиорелейная, 139
- Локальная вычислительная сеть, 177
- М**
- Магистраль, 179  
Максимальная длина пакетов, 314  
Манипуляция, 96, 99  
амплитудная, 100  
фазовая, 100  
частотная, 100
- Маркер, 220  
Маркерное кольцо, 218  
Маршрутизатор, 252  
коммутирующий по меткам, 330  
магистральный, 255  
периферийный, 254  
пограничный коммутирующий по меткам, 331  
удаленного доступа, 254
- Маршрутизация, 54  
адаптивная, 60  
бесклассовая междоменная, 301
- динамическая, 256  
лавинообразная, 57  
локальная, 60  
многопутевая, 59  
однопутевая, 59  
по предыдущему опыту, 57  
простая, 56  
распределённая, 60  
случайная, 56  
статическая, 256  
фиксированная, 59  
централизованная, 60
- Маска, 299  
Масштабируемость, 22, 71  
Межсетевой протокол  
управляющих сообщений, 292  
Межсетевые пакеты, 316  
Метод доступа  
Demand Priority, 212  
детерминированный, 212
- Метод прямого  
последовательного расширения спектра, 235
- Метод раннего освобождения маркера, 187
- Метод уплотнения  
временной, 92  
частотный, 92
- Метод  
агрессивного поведения, 264  
обратного давления, 264  
управления доступом, 184
- Методы опроса, 233  
Метрика, 253  
Механизм  
квитирования, 64  
скользящего окна, 67  
тайм-аута, 65  
управления потоками кадров, 263
- Микросегментация, 263  
Микросота, 160  
Многопротокольная коммутация на основе меток, 329

- Многоуровневая коммутация по меткам, 332
- Множественный доступ с кодовым разделением, 236
- Множественный доступ с контролем несущей и обнаружением конфликтов, 186 предотвращением конфликтов, 186
- Мобильная сотовая связь, 159
- Модем, 86
- Модуляция, 87
- адаптивная дифференциальная импульсно-кодовая, 98
  - амплитудная, 96
  - амплитудно-импульсная, 97
  - аналоговая, 95, 96
  - импульсная, 95, 97
  - импульсно-кодовая, 97
  - квадратурная амплитудная, 100
  - цифровая, 95
  - частотная, 96
- Мост, 247
- инкапсулирующий, 250
  - прозрачный, 249
  - с маршрутизацией от источника, 251
  - транслирующий, 250
- Мот, 244
- Мультиплексирование, 14, 92
- асинхронное, 94
  - волновое, 94
  - временное, 93
  - синхронное, 93
  - статистическое, 94
  - статическое, 93
  - уплотнённое волновое, 95
  - частотное, 92
- Н**
- Надежность, 73
- Несущая, 87
- Номер виртуального канала, 267
- О**
- Оборудование канaloобразующее, 14
- Обрамление сообщения, 28
- Объём, 9
- Объём пульсации
- дополнительный, 276
  - согласованный, 276
- Операционная система
- клиентская часть, 33
  - коммуникационная часть, 33
  - серверная часть, 33
- Операционные возможности, 70
- Оптический обходной переключатель, 228
- Оптическое волокно, 122
- многомодовое, 122
  - одномодовое, 122
- Орбита, 141
- высокоэллиптическая, 143
  - геостационарная, 142
- Организация
- многоуровневая, 22
  - структурная, 34
  - функциональная, 41
- Ортогональное частотное мультиплексирование, 233
- Основная гармоника, 105
- Отказ, 73
- Открытость, 22
- Отражение, 133
- П**
- ПАД, 271
- Пакет, 31, 45
- Пакетный адаптер данных, 271
- Параметры, 69
- нагрузочные, 70
  - структурные, 69
  - функциональные, 70
- Передача
- немодулированная, 190
  - основополосная, 190
  - прямая, 190
  - широкополосная, 190
- Перекрестные наводки
- на ближнем конце, 118
  - на дальнем конце, 118
- Перигей, 143

- Период отсечки, 234  
Персональная сеть, 17  
Пикосеть, 241  
Повторитель, 183  
Подсеть, 293  
Подуровень управления  
    доступом к среде передачи, 29  
    логическим соединением, 29  
Поздняя коллизия, 202  
Поле расширения, 215  
Полоса пропускания  
    оптического волокна, 123  
    частот, 85  
Помехоустойчивость, 88  
Порт, 23  
    корневой, 265  
    назначенный, 265  
Последовательность завершения, 222  
Постоянная составляющая, 107  
Правило "5-4-3", 192  
Преамбула, 196  
Префикс, 301  
Принцип ретрансляции, 138  
Программное обеспечение  
    прикладное, 10  
    системное, 10  
Производительность  
    компьютерной сети, 71  
    реальная, 72  
    сети передачи данных, 72  
    системная, 72  
    средств обработки данных, 72  
    фактическая, 72  
Пропускная способность канала связи, 90, 208  
    полезная, 208  
    эффективная, 208  
Пропускная способность  
    среды передачи, 208  
    сети передачи данных, 72  
Простой протокол передачи почты, 291  
    файлов, 290  
Протокол, 30  
IPsec, 342  
IPv6, 309  
границного шлюза, 290  
двухточечного соединения, 293  
динамической конфигурации узла, 290  
доступа к электронной почте Интернета, 291  
маршрутизации типа DVA, 293  
маршрутизации типа LSA, 293  
обратного определения адреса, 293  
передачи гипертекста, 290  
передачи трафика реального времени, 292  
передачи файлов, 290  
почтового отделения, 291  
простого управления сетями, 291  
разрешения адресов, 293  
распределения меток, 330  
управления группами Интернета, 293  
управления передачей данных с установлением соединения, 292  
установления сеанса, 291  
Протокольный блок данных, 31  
Процедура заказа качества обслуживания, 275  
Процесс, 23  
    вычислительный, 12  
    прикладной, 23  
    системный, 23  
Псевдозаголовок, 323  
Путь с коммутацией по меткам, 330  
**P**  
Рабочая станция, 177  
Радиомодем, 137  
Радиотелефон, 159  
Размер окна, 67  
Расширение спектра скачкообразной перестройкой частоты, 234

- Расширяющая последовательность, 235  
Регенератор, 88  
Режим асинхронной передачи, 50  
ранней передачи маркера, 221  
Роумер, 165  
Ряд Фурье, 84
- С**
- Самосинхронизирующиеся коды, 103  
Сбой, 73  
Сборщик-разборщик пакетов, 271  
Световод, 121  
Сеанс, 23  
Сегмент, 32  
Сенсор, 243  
Сервер, 181  
    прикладной, 182  
Серверная ферма, 19  
Сервис сетевой безопасности, 340  
Сессия, 23  
Сетевая система хранения данных, 19  
Сетевой адаптер, 177  
Сеть связи  
    вторичная, 145  
    первичная, 144  
Сеть  
    X.25, 270  
    абонентская, 146  
    беспроводная, 19  
    беспроводная сенсорная, 243  
    ведомственная, 18  
    виртуальная, 19  
    вычислительная, 18  
    глобальная, 18  
    доступа, 146  
    иерархическая, 19  
    информационная, 18  
    информационно-вычислительная, 19  
    информационно-управляющая, 19  
    корпоративная, 18  
    магистральная, 146  
    одноранговая, 181  
    офисная, 18  
    пакетной коммутации, 270  
    передачи данных, 8, 13  
    связи, 13  
    сотовой связи, 160  
    телекоммуникационная, 13, 80  
    хранения данных, 19  
    частная, 18  
    ЭВМ, 7  
Сжатие данных, 151  
Сигнал, 82  
    аналоговый, 83  
    дискретный, 83  
    запрещенный, 111  
    затора, 201  
    информационный, 83  
    непрерывный, 83  
    оптический, 121  
    с ограниченным спектром, 85  
    цифровой, 83  
Система  
    доменных имён, 291  
    управления базами данных, 12  
    связи, 87  
Система связи  
    многоканальная, 91  
    спутниковая, 139  
Системная производительность, 11  
Скорость модуляции, 90  
Скорость передачи данных  
    реальная, 208  
    фактическая, 208  
Скремблер, 115  
Скремблирование, 115  
Смещение фрагмента, 317  
Совместимость, 22  
Согласованная информационная скорость, 275  
Сокет, 318  
Солитон, 123  
Сообщение, 16, 31  
Спектр, 85

- Способ передачи пакетов  
виртуальный канал, 53  
дейтаграммный, 51
- Спутник  
нерегенеративный, 141  
регенеративный, 141
- Спутниковая связь, 139
- Спутник-ретранслятор  
активный, 141  
пассивный, 141
- Средства  
вычислительной техники, 9  
компьютерной безопасности,  
338  
сетевой безопасности, 339  
телекоммуникаций, 13, 80
- Стандарт  
10Base-FB, 195  
10Base-FL, 195  
AMPS, 162  
CDMA, 166  
CDMA2000, 168  
D-AMPS, 163  
FOIRL, 195  
GPRS, 166  
GSM, 163  
HSDPA, 168  
NMT, 162  
TAPI, 151  
TDMA, 162  
UMTS, 167  
WCDMA, 168
- Станция с двойным  
подключением, 227
- Статус кадра, 226
- Стек протоколов, 31
- Структурированная кабельная  
система, 131
- T**
- Таблица адресов, 248
- Тайм-аут, 65
- Телекоммуникация, 80
- Теорема Котельникова, 97
- Терминатор, 179
- Территориально-распределенная  
сеть, 246
- Технология защищенного канала,  
341
- Технология компьютерной сети,  
14
- Технология расширенного  
спектра, 233
- Топология, 13  
активная, 180  
дерево, 36  
звезда, 36  
кольцо, 36  
логическая, 34  
многосвязная, 36  
общая шина, 34  
пассивная, 180  
полносвязная, 36  
смешанная, 37  
физическая, 34  
ячеистая, 36
- Туннелирование, 332
- Туннельный протокол типа точка-  
точка, 291
- У**
- Узел  
коммутации, 15  
обработки данных, 15  
передачи данных, 15  
сети, 15
- Узкое место, 61
- Уменьшение межкадрового  
интервала, 207
- Уплотнение, 91  
спектральное, 94
- Управление доступом, 223
- Управляемость, 20, 71
- Управляющие программы, 12
- Уровень, 24  
адаптации, 282  
канальный, 25  
представления, 27  
прикладной, 28  
сеансовый, 27  
сетевой, 26

- транспортный, 26  
физический, 24
- Усилитель, 88
- Устройство множественного доступа, 219
- Ф**
- Фаза, 84
- Файл-сервер, 182
- Фильтр, 88
- Фрагмент, 201, 307, 314  
    элементарный, 316
- Фрагментация, 314  
    прозрачная, 315  
    сквозная, 316
- Фрагментирование, 307
- Фронт, 109
- Фтороцирконатные волокна, 122
- Х**
- Хаб, 184
- Характеристики, 69  
    глобальные, 71  
    каналов связи, 90  
    качественные, 70  
    количественные, 71  
    локальные, 71  
    надежности, 73  
    оперативности, 72  
    производительности, 71  
    стоимостные, 74
- Хоп, 37
- Хост, 15
- Ц**
- Целостность, 339
- Центр  
    коммутации пакетов, 270  
    обработки данных, 15
- Цифровая иерархия  
    плезиохронная, 170  
    синхронная, 173
- Цифровые сети с интегральным обслуживанием, 154
- ЦКП, 270
- Ч**
- Частота, 84
- Чип, 234
- Чиповая скорость, 236
- Чувствительность, 137
- Ш**
- Ширина окна, 67
- Шифрование, 340
- Шлюз, 266  
    безопасности, 344
- Э**
- Электромагнитное поле излучения, 132
- Электронная вычислительная машина, 9
- Энтропия, 9
- Эффективность, 22
- Я**
- Ячейка, 50

# **СОДЕРЖАНИЕ**

<b>Введение .....</b>	<b>3</b>
<b>Раздел 1. ОБЩИЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ СЕТЕЙ ЭВМ .....</b>	<b>7</b>
<b>    1.1. Основные понятия и терминология .....</b>	<b>7</b>
1.1.1. Понятие сети ЭВМ .....	7
1.1.2. Данные и информация.....	8
1.1.3. Средства вычислительной техники .....	9
1.1.4. Средства телекоммуникаций.....	13
1.1.5. Понятия архитектуры и технологии компьютерной сети .....	14
<b>    1.2. Состав и типы компьютерных сетей .....</b>	<b>15</b>
1.2.1. Состав компьютерной сети.....	15
1.2.2. Классификация сетей ЭВМ .....	16
1.2.3. Администрирование компьютерных сетей.....	20
1.2.4. Типы данных .....	20
<b>    1.3. Многоуровневая организация вычислительных сетей.....</b>	<b>22</b>
1.3.1. Требования к организации компьютерных сетей.....	22
1.3.2. Понятия процесса и уровня .....	23
1.3.3. Модель взаимодействия открытых систем (OSI-модель) .....	24
1.3.3.1. Физический уровень .....	24
1.3.3.2. Канальный уровень .....	25
1.3.3.3. Сетевой уровень .....	26
1.3.3.4. Транспортный уровень .....	26
1.3.3.5. Сеансовый уровень .....	27
1.3.3.6. Уровень представления .....	27
1.3.3.7. Прикладной уровень .....	28
1.3.3.8. Процесс передачи сообщений в OSI-модели .....	28
1.3.4. IEEE-модель локальных сетей .....	29
1.3.5. Понятия интерфейса и протокола .....	30
1.3.6. Протокольные блоки данных (PDU).....	31
1.3.7. Сетевая операционная система .....	32
<b>    1.4. Принципы структурной организации компьютерных сетей....</b>	<b>34</b>
1.4.1. Сетевые топологии .....	34
1.4.2. Сравнительный анализ топологий.....	37
<b>    1.5. Принципы функциональной организации компьютерных сетей .....</b>	<b>41</b>
1.5.1. Коммутация .....	41
1.5.1.1. Коммутация каналов .....	42
1.5.1.2. Коммутация сообщений .....	44
1.5.1.3. Коммутация пакетов .....	45
1.5.1.4. Коммутация ячеек .....	49
1.5.2. Способы передачи пакетов .....	50
1.5.2.1. Дейтаграммная передача .....	51
1.5.2.2. Виртуальный канал .....	53
1.5.3. Маршрутизация .....	54

1.5.3.1. Таблица маршрутизации .....	54
1.5.3.2. Модель маршрутизатора .....	55
1.5.3.3. Классификация методов маршрутизации.....	56
1.5.3.4. Простые методы маршрутизации .....	56
1.5.3.5. Методы фиксированной маршрутизации .....	59
1.5.3.6. Методы адаптивной маршрутизации.....	60
1.5.4. Задачи управления трафиком.....	61
1.5.5. Методы управления трафиком на физическом уровне .....	63
1.5.5.1. Способы разделения кадров.....	63
1.5.5.2. Бит-страффинг.....	63
1.5.6. Управление трафиком на канальном уровне.....	64
1.5.6.1. Квитирование .....	64
1.5.6.2. Тайм-аут .....	65
1.5.6.3. Скользящее окно .....	67
1.5.7. Управление трафиком на высших уровнях OSI-модели .....	68
<b>1.6. Параметры и характеристики компьютерных сетей.....</b>	<b>69</b>
1.6.1. Параметры компьютерных сетей.....	69
1.6.2. Характеристики компьютерных сетей .....	70
1.6.2.1. Характеристики производительности.....	71
1.6.2.2. Характеристики оперативности.....	72
1.6.2.3. Характеристики надежности.....	73
1.6.2.4. Стоимостные характеристики .....	74
1.6.2.5. Локальные характеристики СВ .....	74
<b>1.7. Сетевые протоколы.....</b>	<b>75</b>
1.7.1. TCP/IP .....	75
1.7.2. XNS .....	76
1.7.3. IPX.....	77
1.7.4. AppleTalk .....	77
1.7.5. DECnet .....	77
1.7.6. SNA .....	78
1.7.7. Сопоставление коммуникационных моделей и протоколов ..	78
<b>Раздел 2. СРЕДСТВА ТЕЛЕКОММУНИКАЦИЙ.....</b>	<b>80</b>
<b>2.1. Основные понятия техники связи .....</b>	<b>80</b>
2.1.1. Телекоммуникация .....	80
2.1.2. Сигналы .....	82
2.1.3. Спектр .....	84
2.1.4. Полоса пропускания.....	85
2.1.5. Модуляция.....	86
<b>2.2. Система связи .....</b>	<b>87</b>
2.2.1. Системы связи на основе непрерывного канала .....	88
2.2.2. Системы связи на основе дискретного канала .....	89
2.2.3. Классификация каналов связи.....	89
2.2.4. Характеристики каналов связи .....	90
2.2.5. Многоканальные системы связи .....	91
2.2.6. Методы мультиплексирования .....	92

2.2.6.1. Частотное мультиплексирование .....	92
2.2.6.2. Временное мультиплексирование .....	93
2.2.6.3. Волновое мультиплексирование.....	94
<b>2.3. Методы модуляции и кодирования данных .....</b>	<b>95</b>
2.3.1. Методы модуляции непрерывных данных .....	96
2.3.1.1. Аналоговая модуляция .....	96
2.3.1.2. Импульсная модуляция .....	97
2.3.2. Методы модуляции дискретных данных .....	99
2.3.3. Цифровое кодирование .....	100
2.3.3.1. Особенности передачи цифровых сигналов.....	101
2.3.3.2. Требования к методам цифрового кодирования.....	108
2.3.3.3. Потенциальный код без возврата к нулю (NRZ) .....	109
2.3.3.4. Биполярный импульсный код (RZ) .....	110
2.3.3.5. Биполярное кодирование с альтернативной инверсией (AMI) .....	111
2.3.3.6. Потенциальный код с инверсией при единице (NRZI) .....	112
2.3.3.7. Манчестерский код .....	112
2.3.3.8. Дифференциальный манчестерский код.....	112
2.3.3.9. Код трехуровневой передачи MLT-3 .....	113
2.3.3.10. Пятиуровневый код PAM-5 .....	113
2.3.4. Логическое кодирование.....	113
2.3.4.1. Избыточное кодирование .....	114
2.3.4.2. Скремблирование .....	115
<b>2.4. Кабельные линии связи .....</b>	<b>116</b>
2.4.1. Электрические кабельные линии связи.....	117
2.4.1.1. Основные электромагнитные характеристики электрических кабелей связи .....	117
2.4.1.2. Витая пара .....	119
2.4.1.3. Коаксиальный кабель.....	120
2.4.2. Волоконно-оптические линии связи (ВОЛС) .....	121
2.4.2.1. Оптическое волокно.....	122
2.4.2.2. Волоконно-оптический кабель .....	125
2.4.2.3. Оптические компоненты .....	125
2.4.2.4. Особенности ВОЛС .....	126
2.4.2.5. Применение ВОЛС в ЛВС .....	128
2.4.2.6. Способы сращивания оптических волокон .....	128
2.4.2.7. Перспективы ВОЛС .....	129
2.4.3. Кабельные системы .....	130
2.4.4. Структурированные кабельные системы.....	130
<b>2.5. Беспроводные системы связи .....</b>	<b>132</b>
2.5.1. Общие принципы организации беспроводной связи.....	132
2.5.1.1. Виды беспроводной связи .....	132
2.5.1.2. Характеристики ЭПИ.....	133
2.5.1.3. Условия распространения ЭПИ разных частот .....	133

2.5.1.4. Диапазоны радиоволн.....	134
2.5.1.5. Свойства радиоволн разных диапазонов .....	134
2.5.2. Наземная радиосвязь.....	137
2.5.3. Радиорелейные линии связи.....	138
2.5.4. Спутниковые системы связи .....	139
2.5.4.1. Общие сведения .....	139
2.5.4.2. Классификация спутниковых систем по типу орбиты .....	141
2.5.4.3. Геостационарная орбита.....	142
2.5.4.4. Высокоэллиптическая орбита.....	143
2.5.4.5. Низкоорбитальные ССС .....	144
2.5.5. Беспроводные сети на ИК-лучах .....	145
<b>2.6. Телекоммуникационные сети.....</b>	<b>145</b>
2.6.1. Классификация телекоммуникационных сетей .....	145
2.6.2. Передача данных на основе телефонных сетей .....	147
2.6.3. Модемная связь.....	151
2.6.3.1. Принципы организации модемной связи .....	151
2.6.3.2. Модемные стандарты .....	151
2.6.3.3. Классификация модемов .....	152
2.6.4. Цифровые сети с интегральным обслуживанием (ISDN- технология) .....	153
2.6.5. Технологии xDSL .....	156
2.6.6. Мобильная телефонная связь.....	159
2.6.6.1. Принципы организации сотовой связи .....	159
2.6.6.2. Поколения мобильной сотовой связи .....	161
2.6.6.3. Поколение 1G .....	161
2.6.6.4. Поколение 2G .....	162
2.6.6.5. Поколение 2.5G .....	166
2.6.6.6. Поколение 3G .....	167
2.6.6.7. Поколение 3.5G .....	168
2.6.6.8. Поколение 4G .....	169
2.6.7. Цифровые выделенные линии.....	170
2.6.7.1. Плэзиохронная цифровая иерархия .....	170
2.6.7.2. Синхронная цифровая иерархия.....	173
<b>Раздел 3. ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ.....</b>	<b>177</b>
<b>3.1. Принципы организации ЛВС .....</b>	<b>177</b>
3.1.1. Характерные особенности ЛВС .....	177
3.1.2. Состав ЛВС .....	177
3.1.3. Топологии ЛВС.....	179
3.1.4. Архитектуры ЛВС .....	180
3.1.4.1. Одноранговые (равноранговые) сети.....	181
3.1.4.2. Сети типа "клиент-сервер" .....	181
3.1.4.3. Серверы ЛВС .....	182
3.1.5. Многосегментная организация ЛВС .....	182
3.1.5.1. Использование нескольких сетевых адаптеров .....	182

3.1.5.2. Повторители.....	183
3.1.5.3. Концентраторы .....	184
3.1.6. Методы управления доступом в ЛВС .....	184
3.1.7. Стандарты локальных сетей .....	187
<b>3.2. ЛВС Ethernet .....</b>	<b>188</b>
3.2.1. Общие сведения .....	188
3.2.2. Физический уровень ЛВС Ethernet .....	190
3.2.2.1. Спецификация 10Base-5 .....	190
3.2.2.2. Спецификация 10Base-2 .....	192
3.2.2.3. Спецификация 10Base-T .....	193
3.2.2.4. Спецификация 10Base-F .....	195
3.2.3. Канальный уровень ЛВС Ethernet.....	196
3.2.3.1. Кадр Ethernet II (Ethernet DIX).....	196
3.2.3.2. Кадр Raw 802.3 (IEEE 802.3/Novell).....	198
3.2.3.3. Кадр 802.3/LLC (кадр 802.3/802.2) .....	199
3.2.3.4. Кадр Ethernet SNAP.....	199
3.2.3.5. Алгоритм определения типа кадра.....	200
3.2.3.6. Протокол CSMA/CD .....	201
3.2.4. Многосегментные ЛВС Ethernet .....	204
3.2.4.1. Условие корректности ЛВС .....	204
3.2.4.2. Расчёт времени двойного оборота (PDV) .....	206
3.2.4.3. Расчёт уменьшения межкадрового интервала (PVV)....	207
3.2.5. Расчет показателей производительности ЛВС Ethernet .....	208
3.2.6. Достоинства и недостатки ЛВС Ethernet .....	209
<b>3.3. Высокоскоростные технологии Ethernet.....</b>	<b>209</b>
3.3.1. Fast Ethernet .....	209
3.3.1.1. Спецификации 100Base-TX и 100Base-FX .....	210
3.3.1.2. Спецификация 100Base-T4.....	211
3.3.1.3. Правила построения многосегментных ЛВС Fast Ethernet.....	211
3.3.2. 100VG-AnyLAN .....	212
3.3.3. Gigabit Ethernet.....	215
3.3.4. 10Gigabit Ethernet.....	216
3.3.5. 40Gigabit Ethernet и 100Gigabit Ethernet.....	217
<b>3.4. ЛВС Token Ring .....</b>	<b>218</b>
3.4.1. Общие сведения .....	218
3.4.2. Структурная организация Token Ring .....	219
3.4.3. Функциональная организация Token Ring.....	220
3.4.4. Форматы кадров.....	222
3.4.4.1. Начальный и концевой разделители .....	223
3.4.4.2. Управление доступом .....	223
3.4.4.3. Управление кадром .....	224
3.4.4.4. Адреса.....	225
3.4.4.5. Данные.....	225
3.4.4.6. Контрольная сумма .....	225

3.4.4.7. Статус кадра.....	226
3.4.5. Достоинства и недостатки ЛВС Token Ring.....	226
<b>3.5. ЛВС FDDI.....</b>	<b>227</b>
3.5.1. Общие сведения.....	227
3.5.2. Структурная организация сети FDDI .....	227
3.5.3. Функциональная организация FDDI .....	229
3.5.4. Форматы кадров.....	230
3.5.5. Технические характеристики FDDI.....	231
3.5.6. Достоинства и недостатки FDDI.....	232
<b>3.6. Беспроводные ЛВС .....</b>	<b>232</b>
3.6.1. Общие принципы построения беспроводных ЛВС .....	232
3.6.2. Методы передачи данных .....	233
3.6.2.1. Ортогональное частотное мультиплексирование .....	233
3.6.2.2. Расширение спектра скачкообразным изменением частоты .....	234
3.6.2.3. Прямое последовательное расширение спектра .....	235
3.6.2.4. Множественный доступ с кодовым разделением.....	236
3.6.3. Технология WiFi .....	238
3.6.4. Технология WiMax .....	239
3.6.5. Беспроводные персональные сети .....	241
3.6.5.1. Технология Bluetooth.....	241
3.6.5.2. Технология ZigBee .....	242
3.6.6. Беспроводные сенсорные сети .....	243
3.6.7. Сравнение беспроводных технологий .....	244
<b>Раздел 4. ГЛОБАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ .....</b>	<b>246</b>
<b>4.1. Принципы организации глобальных сетей .....</b>	<b>246</b>
4.1.1. Характерные особенности ГВС .....	246
4.1.2. Достоинства ГВС .....	247
<b>4.2. Технические средства объединения сетей.....</b>	<b>247</b>
4.2.1. Мосты .....	247
4.2.1.1. Прозрачные мосты .....	249
4.2.1.2. Транслирующие мосты.....	250
4.2.1.3. Инкапсулирующие мосты .....	250
4.2.1.4. Мосты с маршрутизацией от источника.....	251
4.2.2. Маршрутизаторы .....	252
4.2.2.1. Периферийные маршрутизаторы .....	254
4.2.2.2. Маршрутизаторы удаленного доступа .....	254
4.2.2.3. Магистральные маршрутизаторы.....	255
4.2.2.4. Методы маршрутизации .....	255
4.2.2.5. Протоколы маршрутизации .....	257
4.2.3. Коммутаторы .....	261
4.2.3.1. Каноническая структура коммутатора.....	262
4.2.3.2. Техническая реализация коммутаторов.....	264
4.2.3.3. Дополнительные функции коммутаторов .....	265
4.2.4. Шлюзы .....	266

<b>4.3. Сети с установлением соединений.....</b>	<b>266</b>
4.3.1. Принцип передачи пакетов на основе виртуальных каналов ..	266
4.3.2. Сети X.25 .....	270
4.3.2.1. Назначение и структура сетей X.25 .....	270
4.3.2.2. Стек протоколов сети X.25.....	271
4.3.2.3. Установление виртуального соединения.....	272
4.3.3. Сети Frame Relay .....	274
4.3.3.1. Особенности технологии Frame Relay .....	274
4.3.3.2. Поддержка качества обслуживания .....	275
4.3.3.3. Использование сетей Frame Relay .....	278
4.3.4. Технология ATM .....	279
4.3.4.1. Общие принципы технологии ATM .....	280
4.3.4.2. Стек протоколов ATM .....	282
4.3.4.3. Формат ATM-ячейки.....	283
4.3.4.4. Принцип работы коммутаторов ATM .....	284
4.3.4.5. Обеспечение качества обслуживания .....	286
4.3.4.6. Использование технологии ATM .....	287
<b>4.4. Глобальная сеть Internet.....</b>	<b>287</b>
4.4.1. Краткая история создания и организационные структуры Internet.....	287
4.4.2. Стек протоколов TCP/IP .....	288
4.4.2.1. Протоколы прикладного уровня.....	290
4.4.2.2. Протоколы транспортного уровня .....	292
4.4.2.3. Протоколы межсетевого уровня .....	292
4.4.2.4. Протоколы канального уровня («сетевой интерфейс»).....	293
4.4.3. Архитектурная концепция Internet .....	293
4.4.4. Адресация в IP-сетях .....	294
4.4.4.1. Сетевые IP-адреса.....	295
4.4.4.2. Сетевые IP-адреса.....	295
4.4.4.3. Специальные, автономные и групповые IP-адреса .....	297
4.4.4.4. Использование масок для IP-адресов.....	299
4.4.4.5. Распределение IP-адресов .....	300
4.4.4.6. Бесклассовая междоменная маршрутизация .....	301
4.4.4.7. Протоколы разрешения адресов ARP и RARP .....	302
4.4.4.8. Система доменных имен DNS .....	304
4.4.5. Коммуникационный протокол IPv4.....	306
4.4.6. Коммуникационный протокол IPv6.....	309
4.4.6.1. Адресация в IPv6 .....	309
4.4.6.2. Структура пакета IPv6 .....	312
4.4.6.3. Формат основного заголовка IPv6.....	313
4.4.7. Фрагментация.....	314
4.4.8. Транспортные протоколы стека TCP/IP .....	317
4.4.8.1. Транспортный протокол UDP .....	318
4.4.8.2. Транспортный протокол TCP .....	320

4.4.8.3. Псевдозаголовок протоколов UDP и TCP .....	323
4.4.9. Управляющий протокол ICMP .....	324
4.4.10. Протоколы канального уровня для выделенных линий.....	324
4.4.10.1. Протокол SLIP .....	325
4.4.10.2. Протоколы семейства HDLC .....	325
4.4.10.3. Протокол PPP .....	328
<b>4.5. MPLS-технология.....</b>	<b>329</b>
4.5.1. Основные принципы MPLS-технологии.....	329
4.5.2. Маршрутизатор LSR и таблица продвижения .....	330
4.5.3. Заголовок MPLS .....	331
4.5.4. Многоуровневая коммутация по меткам .....	332
<b>4.6. Пример передачи данных в составной сети .....</b>	<b>334</b>
4.6.1. Система обозначений .....	334
4.6.2. Формирование данных в узле-источнике .....	335
4.6.3. Передача данных .....	336
<b>4.7. Безопасность компьютерных сетей.....</b>	<b>338</b>
4.7.1. Средства компьютерной безопасности .....	338
4.7.2. Средства сетевой безопасности .....	339
4.7.3. Конфиденциальность, доступность, целостность.....	339
4.7.4. Сервисы сетевой безопасности .....	340
4.7.5. Технология защищённого канала .....	341
4.7.6. Протокол IPsec .....	342
<b>Заключение.....</b>	<b>345</b>
<b>Вопросы и задания для самостоятельной работы .....</b>	<b>350</b>
<b>Используемые аbbревиатуры .....</b>	<b>373</b>
<b>Список литературы .....</b>	<b>381</b>
<b>Алфавитный указатель .....</b>	<b>382</b>