12. ПРИНЦИПЫ ПОСТРОЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

12.1. Характеристика телекоммуникационных вычислительных сетей

Телекоммуникационная вычислительная сеть (ТВС) *— это сеть обмена и распределенной обработки информации, образуемая множеством взаимосвязанных абонентских систем и средствами связи; средства передачи и обработки информации ориентированы в ней на коллективное использование общесетевых ресурсов — аппаратных, информационных, программных.*

Абонентская система (АС) *— это совокупность ЭВМ, программного обеспечения, периферийного оборудования, средств связи с коммуникационной подсетью вычислительной сети, выполняющих прикладные процессы.*

Коммуникационная подсеть, *или телекоммуникационная система (ТКС), представляет собой совокупность физической среды передачи информации, аппаратных и программных средств, обеспечивающих взаимодействие АС.*

Прикладной процесс *— это различные процедуры ввода, хранения, обработки и выдачи информации, выполняемые в интересах пользователей и описываемые прикладными программами.*

С появлением ТВС удалось разрешить две очень важные проблемы: обеспечение в принципе неограниченного доступа к ЭВМ пользователей независимо от их территориального расположения и возможность оперативного перемещения больших массивов информации на любые расстояния, позволяющая своевременно получать данные для принятия тех или иных решений.

Для ТВС принципиальное значение имеют следующие обстоятельства:

- ЭВМ, находящиеся в составе разных абонентских систем одной и той же сети или различных взаимодействующих сетей, связываются между собой автоматически (в этом заключается сущность протекающих в сети процессов);
- каждая ЭВМ сети должна быть приспособлена как для работы в автономном режиме под управлением своей операционной системы (ОС), так и для работы в качестве составного звена сети. ТВС могут работать в различных режимах: обмена данными между АС, запроса и выдачи информации, сбора информации, пакетной обработки данных по запросам пользователей с удаленных терминалов, в диалоговых режимах.

По сравнению с адекватной по вычислительной мощности совокупностью автономно работающих ЭВМ сеть имеет ряд преимуществ:

- обеспечение распределенной обработки данных и параллельной обработки многими ЭВМ;
- возможность создания распределенной базы данных (РБД), размещаемой в памяти различных ЭВМ;
- возможность обмена большими массивами информации между ЭВМ, удаленными друг от друга на значительные расстояния;
- коллективное использование дорогостоящих ресурсов: прикладных программных продуктов (ППП), баз данных (БД), баз знаний (БЗ), запоминающих устройств (ЗУ), печатающих устройств;

- предоставление большего перечня услуг, в том числе таких, как электронная почта (ЭП), телеконференции, электронные доски объявлений (ЭДО), дистанционное обучение;
- повышение эффективности использования средств вычислительной техники и информатики (СВТИ) за счет более интенсивной и равномерной их загрузки, а также надежности обслуживания запросов пользователей;
- возможность оперативного перераспределения вычислительных мощностей между пользователями сети в зависимости от изменения их потребностей, а также резервирования этих мощностей и средств передачи данных на случай выхода из строя отдельных элементов сети;
- сокращение расходов на приобретение и эксплуатацию СВТИ (за счет коллективного их использования);
- облегчение работ по совершенствованию технических, программных и информационных средств.

Характеризуя возможности той или иной ТВС, следует оценивать ее аппаратное, информационное и программное обеспечение.

Аппаратное обеспечение составляют ЭВМ различных типов, средства связи, оборудование абонентских систем, оборудование узлов связи, аппаратура связи и согласования работы сетей одного и того же уровня или различных уровней. Основные требования к ЭВМ сетей — это универсальность, т.е. возможность выполнения практически неограниченного круга задач пользователей, и модульность, обеспечивающая возможность изменения конфигурации ЭВМ. В сетях в зависимости от их назначения используются ЭВМ в широком диапазоне по своим характеристикам: от суперЭВМ до ПЭВМ. ЭВМ могут размещаться либо в непосредственной близости от пользователей (например, ПЭВМ в составе абонентской системы, т.е. на рабочем месте пользователя), либо в центре обработки информации (ЦОИ), который является звеном сети и к которому пользователи обращаются с запросами со своих АС.

Информационное обеспечение сети представляет собой единый информационный фонд, ориентированный на решаемые в сети задачи и содержащий массивы данных общего применения, доступные для всех пользователей (абонентов) сети, и массивы индивидуального пользования, предназначенные для отдельных абонентов. В состав информационного обеспечения входят базы знаний, автоматизированные базы данных — локальные и распределенные, общего и индивидуального назначения.

Программное обеспечение (ПО) вычислительных сетей отличается большим многообразием как по своему составу, так и по выполняемым функциям. Оно автоматизирует процессы программирования задач обработки информации, осуществляет планирование и организацию коллективного доступа к телекоммуникационным, вычислительным и информационным ресурсам сети, динамическое распределение и перераспределение этих ресурсов с целью повышения оперативности и надежности удовлетворения запросов пользователей и т.д.

Выделяются следующие группы ПО сетей:

- общесетевое ПО, образуемое распределенной операционной системой (РОС) сети и программными средствами, входящими в состав КПТО — комплект программ технического обслуживания сети (это контролирующие

тест-программы для контроля работоспособности элементов и звеньев сети и ее ТКС и диагностические тест-программы для локализации неисправностей в сети);

- специальное ПО, представленное прикладными программными средствами: функциональными и интегрированными пакетами прикладных программ и прикладными программами сети, библиотеками стандартных программ, а также прикладными программами, отражающими специфику предметной области пользователей при реализации своих задач;
- базовое программное обеспечение ЭВМ абонентских систем, включающее операционные системы ЭВМ, системы автоматизации программирования, контролирующие и диагностические тест-программы.

Распределенная операционная система сети управляет работой сети во всех ее режимах, обеспечивает реализацию запросов пользователей, координирует функционирование звеньев сети. Она имеет иерархическую структуру, соответствующую стандартной семиуровневой модели взаимодействия открытых систем. РОС представляет собой систему программных средств, реализующих процессы взаимодействия АС и объединенных общей архитектурой и коммуникационными протоколами. Взаимодействие асинхронных параллельных процессов в сети, обеспечиваемое РОС, сопровождается применением средств передачи сообщений между одновременно реализуемыми процессами и средств синхронизации этих процессов.

Набор управляющих и обслуживающих программ РОС обеспечивает:

- удовлетворение запросов пользователей по использованию общесетевых ресурсов, т.е. обеспечение доступа отдельных прикладных программ к ресурсам сети;
- организацию связи между отдельными прикладными программами комплекса пользовательских программ, реализуемыми в различных АС сети, т.е. обеспечение межпрограммных методов доступа;
- синхронизацию работы пользовательских программ при их одновременном обращении к одному и тому же общесетевому ресурсу;
- удаленный ввод заданий с любой АС сети и их выполнение в любой другой АС сети в пакетном или оперативном режиме;
- обмен файлами между АС сети, доступ к файлам, хранимым в удаленных ЭВМ, и их обработку;
- передачу текстовых сообщений пользователям в порядке реализации функций службы электронной почты, телеконференций, электронных досок объявлений, дистанционного обучения;
- защиту информации и ресурсов сети от несанкционированного доступа, т.е. реализацию функций служб безопасности сети;
- выдачу справок, характеризующих состояние и использование аппаратных, информационных и программных ресурсов сети. С помощью РОС осуществляется планирование использования общесетевых ресурсов: планирование сроков и очередности получения и выдачи информации пользователям, распределение решаемых задач по ЭВМ сети, распределение информационных ресурсов для этих задач, присвоение приоритетов задачам и выходным сообщениям, изменение конфигурации сети и т.д. В ТВС

применяются различные методы планирования, которые классифицируются по ряду признаков, основные из них: качество решения задачи планирования (по этому признаку различают методы, позволяющие получить оптимальный в отношении выбранного критерия план, и методы составления приближенных планов), степень связности решаемых задач (составление планов реализации связанных задач обычно сложнее, чем в случае несвязанных задач), степень адаптивности процесса планирования к возмущающим факторам, воздействующим на вычислительный процесс (методы адаптивного и неадаптивного планирования).

Кроме того, различают статическое и динамическое планирование. ***Статическое планирование*** осуществляется заранее, до начала решения поступившей в систему к данному времени группы задач. Оно целесообразно, когда перечень задач стабилен и ограничен, для каждой задачи известны потребности в ресурсах сети и частота решения, а надобность в выполнении этих задач возникает неоднократно. Затраты на статическое планирование могут быть большими, зато сами планы — оптимальными в заданном смысле.

Динамическое планирование производится в процессе функционирования сети непосредственно перед началом решения групп задач. С поступлением в систему каждой новой задачи составленный план обычно корректируется с учетом складывающейся ситуации по свободным и занятым ресурсам сети, наличию очередей задач и т.д. Для динамического планирования, как правило, используются методы получения приближенных планов, что объясняется недостатком информации о характеристиках решаемых задач и ограниченностью ресурсов, выделяемых на цели планирования.

Основным показателем эффективности организации вычислительного процесса в сети, планирования использования общесетевых ресурсов является время решения комплекса задач.

Оперативное управление процессами удовлетворения запросов пользователей и обработки информации с помощью РОС сети дает возможность организовать учет выполнения запросов и заданий, выдачу справок об их прохождении в сети, сбор данных о выполняемых в сети работах.

Создание ТВС — сложная комплексная задача, требующая согласованного решения ряда вопросов: выбора рациональной структуры сети, соответствующей ее назначению и удовлетворяющей определенным требованиям (определяется состав элементов и звеньев сети, их расположение, способы соединения); выбора типа линий и каналов связи между звеньями сети и оценки их пропускной способности; обеспечения способности доступа пользователей к общесетевым ресурсам, в частности, за счет оптимального решения задач маршрутизации; распределения аппаратных, информационных и программных ресурсов по звеньям сети; защиты информации, циркулирующей в сети, от несанкционированного доступа и др. Все эти вопросы решаются с учетом требований, предъявляемых к сети по главным показателям: временным — для оценки оперативности удовлетворения запросов пользователей; надежностным — для оценки надежности своевременного удовлетворения этих запросов; экономическим — для оценки капитальных вложений на создание и внедрение сети и текущих затрат при эксплуатации и использовании.

В основу ***классификации ТВС*** положены наиболее характерные функциональные, информационные и структурные признаки.

По степени территориальной рассредоточенности элементов сети (абонентских систем, узлов связи) различают глобальные, региональные и локальные вычислительные сети.

Глобальная вычислительная сеть (ГВС) объединяет абонентские системы, рассредоточенные на большой территории, охватывающей различные страны и континенты. ГВС решают проблему объединения информационных ресурсов всего человечества и организации доступа к ним. Взаимодействие АС осуществляется на базе различных территориальных сетей связи, в которых используются телефонные линии связи, радиосвязь, системы спутниковой связи.

Региональная вычислительная сеть (РВС) объединяет абонентские системы, расположенные друг от друга на значительном расстоянии: в пределах отдельной страны, региона, большого города.

Локальная вычислительная сеть (ЛВС) связывает абонентские системы, расположенные в пределах небольшой территории. К классу ЛВС относятся сети предприятий, фирм, банков, офисов, учебных заведений и т.д. Протяженность ЛВС ограничивается несколькими километрами.

Отдельный класс составляют ***корпоративные вычислительные сети (КВС).*** Корпоративная сеть является технической базой корпорации. Ей принадлежит ведущая роль в реализации задач планирования, организации и осуществления производственно-хозяйственной деятельности корпорации.

Объединение локальных, региональных, корпоративных и глобальных сетей позволяет создавать сложные многосетевые иерархии.

По способу управления ТВС делятся на сети с централизованным (в сети имеется один или несколько управляющих органов), децентрализованным (каждая АС имеет средства для управления сетью) и смешанным управлением, в которых в определенном сочетании реализованы принципы централизованного и децентрализованного управления (например, под централизованным управлением решаются только задачи с высшим приоритетом, связанные с обработкой больших объемов информации).

По организации передачи информации сети делятся на сети с селекцией информации и маршрутизацией информации. В сетях с селекцией информации, строящихся на основе моноканала, взаимодействие АС производится выбором (селекцией) адресованных им блоков данных (кадров): всем АС сети доступны все передаваемые в сети кадры, но копию кадра снимают только АС, которым они предназначены. В сетях с маршрутизацией информации для передачи кадров от отправителя к получателю может использоваться несколько маршрутов. Поэтому с помощью коммуникационных систем сети решается задача выбора оптимального (например, кратчайшего по времени доставки кадра адресату) маршрута.

По типу организации передачи данных сети с маршрутизацией информации делятся на сети с коммутацией цепей (каналов), коммутацией сообщений и коммутацией пакетов. В эксплуатации находятся сети, в которых используются смешанные системы передачи данных.

По топологии, т.е. конфигурации элементов в ТВС, сети могут делиться на два класса: широковещательные (рис. 12.1) и последовательные (рис. 12.2).

Широковещательные конфигурации и значительная часть последовательных конфигураций (кольцо, звезда с «интеллектуальным центром», иерархическая) характерны для ЛВС. Для глобальных и региональных сетей наиболее распространенной является произвольная (ячеистая) топология. Нашли применение также иерархическая конфигурация и звезда.

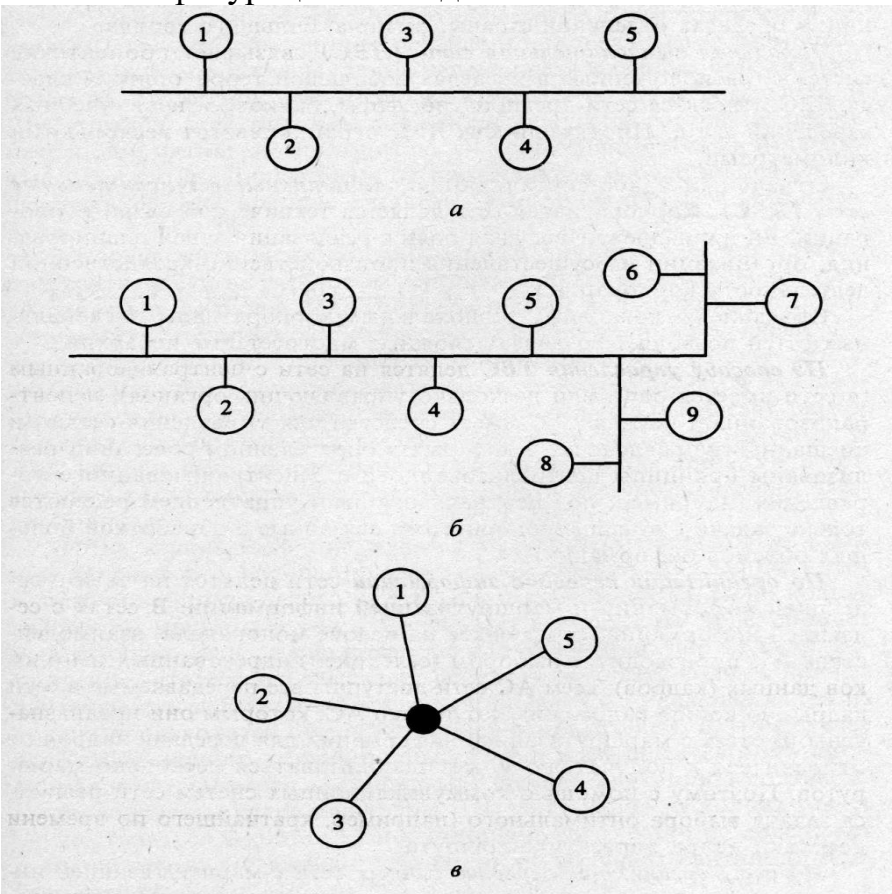

Рис. 12.1. Широковещательные конфигурации сетей: *а* — общая шина; *б* — дерево; *в* — звезда с пассивным центром

В широковещательных конфигурациях в любой момент времени на передачу кадра может работать только одна рабочая станция (абонентная система). Остальные рабочие станции (РС) сети могут принимать этот кадр, т.е. такие конфигурации характерны для ЛВС с селекцией информации. Основные типы широковещательной конфигурации — общая шина, дерево, звезда с пассивным центром. Главные достоинства ЛВС с общей шиной — простота расширения сети, простота используемых методов управления, минимальный расход кабеля. ЛВС с топологией типа дерево — это более развитый вариант сети с шинной топологией. Дерево образуется путем соединения нескольких шин активными повторителями или пассивными размножителями («хабами»), каждая ветвь дерева представляет собой сегмент. Отказ одного сегмента не приводит к выходу из строя остальных. В ЛВС с топологией типа звезда в центре находится пассивный соединитель или активный повторитель — достаточно простые и надежные устройства. Для защиты от нарушений в кабеле используется центральное реле, которое отключает вышедшие из строя кабельные лучи.

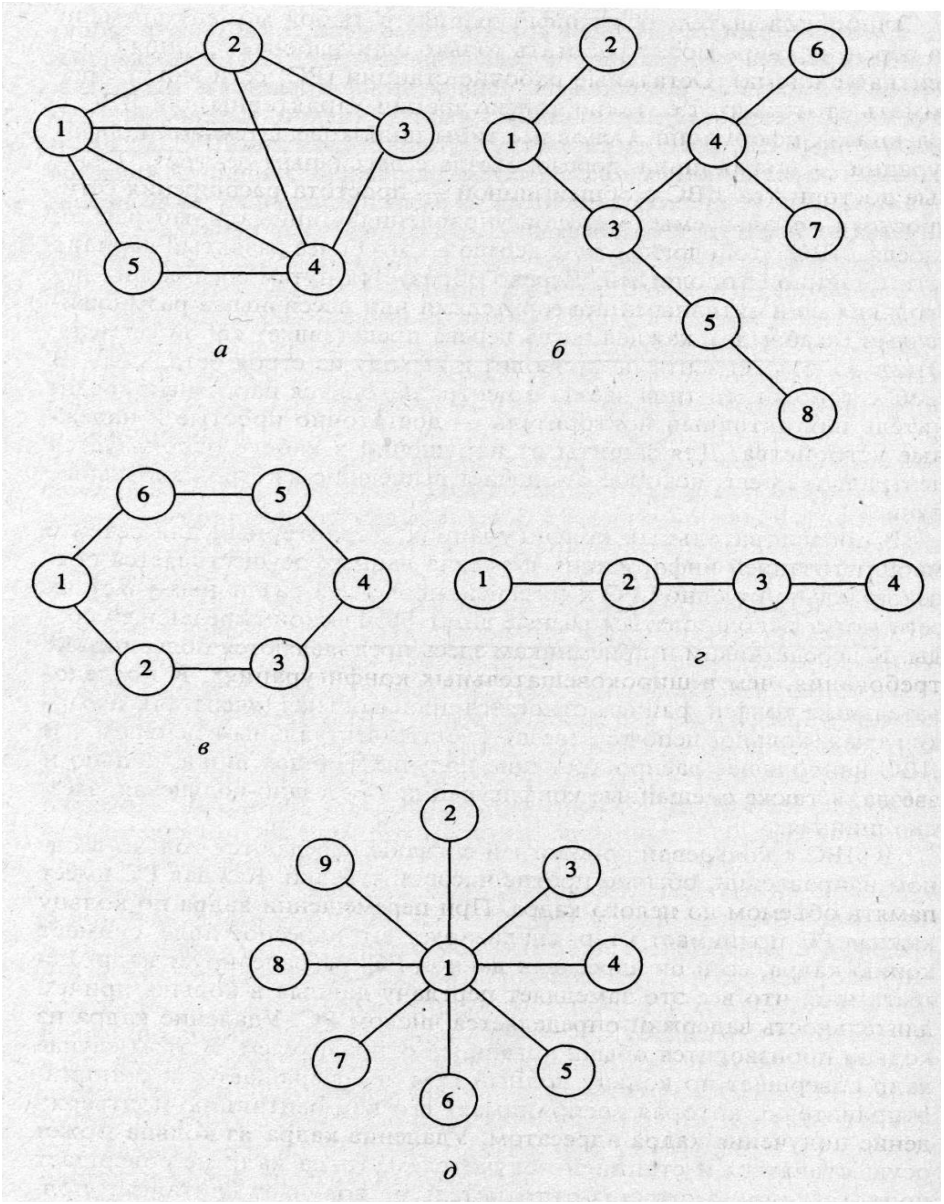

Рис. 12.2. Последовательные конфигурации сетей:
а — произвольная (ячеистая); *б* — иерархическая; *в* — кольцо; *г* — цепочка; I *д* — звезда с «интеллектуальным» центром

В последовательных конфигурациях, характерных для сетей с маршрутизацией информации, передача данных осуществляется последовательно от одной РС к соседней, причем на различных участках сети могут использоваться разные виды физической передающей среды. К передатчикам и приемникам здесь предъявляются более низкие требования, чем в широковещательных конфигурациях. К последовательным конфигурациям относятся произвольная (ячеистая), иерархическая, кольцо, цепочка, звезда с «интеллектуальным центром». В ЛВС наибольшее распространение получили общая шина, кольцо и звезда, а также смешанные конфигурации — звездно-кольцевая, звездно-шинная.

В ЛВС с кольцевой топологией сигналы передаются только в одном направлении, обычно против часовой стрелки. Каждая РС имеет память объемом до целого кадра. При перемещении кадра по кольцу каждая РС принимает кадр, анализирует его адресное поле, снимает копию кадра, если он адресован данной РС, ретранслирует кадр. Естественно, что все это замедляет передачу данных в кольце,

причем длительность задержки определяется числом РС. Удаление кадра из кольца производится обычно станцией-отправителем. В этом случае кадр совершает по кольцу полный круг и возвращается к станции-отправителю, которая воспринимает его как квитанцию-подтверждение получения кадра адресатом. Удаление кадра из кольца может осуществляться и станцией-получателем, тогда кадр не совершает полного круга, а станция-отправитель не получает квитанции-подтверждения.

Кольцевая структура обеспечивает довольно широкие функциональные возможности ЛВС при высокой эффективности использования моноканала, низкой стоимости, простоте методов управления, возможности контроля работоспособности моноканала.

В широковещательных и большинстве последовательных конфигураций (за исключением кольца) каждый сегмент кабеля должен обеспечивать передачу сигналов в обоих направлениях, что достигается: в полудуплексных сетях связи — использованием одного кабеля для поочередной передачи в двух направлениях; в дуплексных сетях — с помощью двух однонаправленных кабелей; в широкополосных системах — применением различной несущей частоты для одновременной передачи сигналов в двух направлениях.

Глобальные и региональные сети, как и локальные, в принципе могут быть однородными (гомогенными), в которых применяются программно-совместимые ЭВМ, и неоднородными (гетерогенными), включающими программно-несовместимые ЭВМ. Однако, учитывая протяженность ГВС и РВС и большое количество используемых в них ЭВМ, такие сети чаще бывают неоднородными.

12.2. Управление взаимодействием прикладных процессов

Реализация рассредоточенных и взаимодействующих процессов в сетях осуществляется на основе двух концепций, одна из которых устанавливает связи между процессами без функциональной среды между ними, а другая определяет связь только через функциональную среду. В первом случае правильность понимания действий, происходящих в рамках соединяемых процессов взаимодействующих АС, обеспечивается соответствующими средствами теледоступа в составе сетевых операционных систем (СОС). Однако предусмотреть такие средства на все случаи соединения процессов нереально. Поэтому взаимодействующие процессы в сетях соединяются с помощью функциональной среды, обеспечивающей выполнение определенного свода правил — протоколов связи процессов. Обычно эти протоколы реализуются с учетом принципа пакетной коммутации, в соответствии с которым перед передачей сообщение разбивается на блоки — пакеты определенной длины. Каждый пакет представляет собой независимую единицу передачи информации, содержащую, кроме собственно данных, служебную информацию (адреса отправителя и получателя, номер пакета в сообщении, информацию для контроля правильности принятых данных).

Практика создания и развития ТВС привела к необходимости разработки стандартов по всему комплексу вопросов организации сетевых систем. В 1978 г. Международная организация по стандартизации (МОС) ***предложила семиуровневую эталонную модель взаимодействия открытых систем (ВОС),*** которая получила широкое распространение и признание. Она создает основу для анализа существующих ТВС и определения новых сетей и стандартов.

В соответствии с эталонной моделью ВОС абонентская система представляется прикладными процессами и процессами взаимодействия АС (рис. 12.3). Последние разбиваются на семь функциональных уровней. Функции и процедуры, выполняемые в рамках одного функционального уровня, составляют соответствующий уровневый протокол. Нумерация уровневых протоколов идет снизу вверх, а их названия указаны на рис. 12.3. Функциональные уровни взаимодействуют на строго иерархической основе: каждый уровень пользуется услугами нижнего уровня и, в свою очередь, обслуживает уровень, расположенный выше. Стандартизация распространяется на протоколы связи одноименных уровней взаимодействующих АС. Создание ТВС в соответствии с эталонной моделью ВОС открывает возможность использования сети ЭВМ различных классов и типов. Поэтому сеть, удовлетворяющая требованиям эталонной модели, называется открытой.

Рис.12.3. Семиуровневая модель протоколов взаимодействия открытых систем

Функциональные уровни рассматриваются как составные независимые части процессов взаимодействия АС. Основные функции, реализуемые в рамках уровневых протоколов, состоят в следующем.

Физический уровень непосредственно связан с каналом передачи данных, обеспечивает физический путь для электрических сигналов, несущих информацию. На этом уровне осуществляется установление, поддержка и расторжение соединения с физическим каналом, определение электрических и функциональных параметров взаимодействия ЭВМ с коммуникационной подсетью.

Канальный уровень определяет правила совместного использования физического уровня узлами связи. Главные его функции: управление передачей данных по информационному каналу (генерация стартового сигнала и организация

начала передачи информации, передача информации по каналу, проверка получаемой информации и исправление ошибок, отключение канала при его неисправности и восстановление передачи после ремонта, генерация сигнала окончания передачи и перевода канала в пассивное состояние) и управление доступом к передающей среде, т.е. реализация выбранного метода доступа к общесетевым ресурсам. Физический и канальный уровни определяют характеристики физического канала и процедуру передачи по нему кадров, являющихся контейнерами, в которых транспортируются пакеты.

Сетевой уровень реализует функции буферизации и маршрутизации, т.е. прокладывает путь между отправителем информации и адресатом через всю сеть. Основная задача сетевого протокола — прокладка в каждом физическом канале совокупности логических каналов. Два пользователя, соединенные логическим каналом, работают так, как будто только в их распоряжении имеется физический канал.

Транспортный уровень занимает центральное место в иерархии уровней сети. Он обеспечивает связь между коммуникационной подсетью и верхними тремя уровнями, отделяет пользователя от физических и функциональных аспектов сети. Главная его задача — управление трафиком (данными пользователя) в сети. При этом выполняются такие функции, как деление длинных сообщений, поступающих от верхних уровней, на пакеты данных (при передаче информации) и формирование первоначальных сообщений из набора пакетов, полученных через канальный и сетевой уровни, исключая их потери или смещение (при приеме информации). Транспортный уровень есть граница, ниже которой пакет данных является единицей информации, управляемой сетью. Выше этой границы в качестве единицы информации рассматривается только сообщение. Транспортный уровень обеспечивает также сквозную отчетность в сети.

Сеансовый уровень предназначен для организации и управления сеансами взаимодействия прикладных процессов пользователей (сеанс создается по запросу процесса пользователя, переданному через прикладной и представительный уровни). Основные функции: управление очередностью передачи данных и их приоритетом, синхронизация отдельных событий, выбор формы диалога пользователей (полудуплексная, дуплексная передача).

Представительный уровень (уровень представления данных) преобразует информацию к виду, который требуют прикладные процессы пользователей (например, прием данных в коде ASCII и выдача их на экран дисплея в виде страницы текста с заданным числом и длиной строк). Представительный уровень занимается синтаксисом данных. Выше этого уровня поля данных имеют явную смысловую форму, а ниже его поля рассматриваются как передаточный груз, и их смысловое значение не влияет на обработку.

Прикладной уровень занимается поддержкой прикладного процесса пользователя и имеет дело с семантикой данных. Он является границей между процессами сети и прикладными (пользовательскими) процессами. На этом уровне выполняются вычислительные, информационно-поисковые и справочные работы, осуществляется логическое преобразование данных пользователя.

Работы по совершенствованию эталонной модели ВОС для ЛВС привели к декомпозиции уровней 1 и 2. Канальный уровень разделен на два подуровня:

подуровень управления логическим каналом (передача кадров между РС, включая исправление ошибок, диагностика работоспособности узлов сети) и подуровень управления доступом к передающей среде (реализация алгоритма доступа к среде и адресация станций сети). Физический уровень делится на три подуровня: передачи физических сигналов, интерфейса с устройством доступа и подключения к физической среде.

В ЛВС процедуры управления на физическом, канальном и транспортном уровнях не отличаются сложностью, в связи с чем эти уровни управления реализуются в основном техническими средствами, называемыми станциями локальной сети (СЛС) и адаптерами ЛВС. По существу, адаптер вместе с физическим каналом образует информационный моноканал, к которому подключаются системы сети, выступающие в качестве абонентов моноканала.

12.3. Протоколы передачи данных нижнего уровня. Управление доступом к передающей среде

Существуют различные процедуры обмена данными между рабочими станциями абонентских систем сети, реализующие при этом те или иные методы доступа к передающей среде. Эти процедуры называются протоколами передачи данных (ППД). Речь идет о ППД, которые относятся к категории линейных (канальных) протоколов, или протоколов управления каналом. Такое название они получили потому, что управляют потоками трафика (данных пользователя) между станциями на одном физическом канале связи. Это также протоколы нижнего уровня, так как их реализация осуществляется на нижних уровнях семиуровневой эталонной модели ВОС.

Между понятиями «протокол передачи данных нижнего уровня» и «метод доступа к передающей среде» существуют определенные различия и связь.

Метод доступа — это способ «захвата» передающей среды, способ определения того, какая из рабочих станций сети может следующей использовать ресурсы сети. Но так же называется и набор правил (алгоритм), используемых сетевым оборудованием, чтобы направлять поток сообщений через сеть, и один из основных признаков, по которым различают сетевое оборудование.

Протокол в общем виде — это набор правил для связи между рабочими станциями (компьютерами) сети, которые управляют форматом сообщений, временными интервалами, последовательностью работы и контролем ошибок. Протокол передачи данных нижнего уровня (протокол управления каналом) — это совокупность процедур, выполняемых на нижних уровнях семиуровневой эталонной модели ВОС по управлению потоками данных между рабочими станциями сети на одном физическом канале связи.

Методы доступа к передающей среде, определяющие правила ее «захвата», могут быть разделены на следующие классы [26]:

- селективные методы, при реализации которых с помощью соответствующего ППД рабочая станция осуществляет передачу только после получения разрешения, которое либо направляется каждой РС по очереди центральным управляющим органом сети (такой алгоритм называется циклическим опросом), либо передается от станции к станции (алгоритм передачи маркера);

- методы, основанные на соперничестве (методы случайного доступа, методы «состязаний» абонентов), когда каждая РС пытается «захватить» передающую среду. При этом могут использоваться несколько способов передачи данных: базовый асинхронный, синхронизация режима работы канала путем тактирования моментов передачи кадров, прослушивание канала перед началом передачи данных по правилу «слушай, прежде чем говорить», прослушивание канала во время передачи данных по правилу «слушай, пока говоришь». Эти способы используются вместе или раздельно, обеспечивая различные варианты загруженности канала и стоимости сети;
- методы, основанные на резервировании времени, принадлежат к числу наиболее ранних и простых. Любая РС осуществляет передачу только в течение временных интервалов (слотов), заранее для нее зарезервированных. Все слоты распределяются между станциями либо поровну (в неприоритетных системах), либо с учетом приоритетов АС, когда некоторые РС за фиксированный интервал времени получают большее число слотов. Станция, владеющая слотом, получает канал в свое полное распоряжение. Такие методы целесообразно применять в сетях с малым числом АС, так как канал используется неэффективно;
- кольцевые методы предназначены специально для ЛВС с кольцевой топологией (хотя большинство указанных методов могут использоваться в таких сетях). К ним относятся два метода — вставка регистров и сегментированная передача (метод временных сегментов).

При реализации метода вставки регистра рабочая станция содержит регистр (буфер), подключаемый параллельно к кольцу. В регистр записывается кадр для передачи, и станция ожидает межкадрового промежутка в моноканале. С его появлением регистр включается в кольцо (до этого он был отключен от кольца) и содержимое регистра передается в линию. Если во время передачи станция получает кадр, он записывается в буфер и передается вслед за кадром, передаваемым этой станцией. Такой метод допускает «подсадку» в кольцо нескольких кадров.

При использовании в ЛВС с кольцевой топологией сегментированной передачи временные сегменты формируются управляющей станцией сети. Они имеют одинаковую протяженность и циркулируют по кольцу. Каждая станция, периодически обращаясь в сеть, может дождаться временного сегмента, помеченного меткой «свободный». В этот сегмент станция помещает свой кадр фиксированной длины, при этом в сегменте метка «свободный» заменяется меткой «занятый». После доставки кадра адресату сегмент вновь освобождается. Важным преимуществом такого метода является возможность одновременной передачи кадров несколькими РС. Однако передача допускается только кадрами фиксированной длины.

Используется и другая классификационная структура, предложенная в [3]. Все ППД делятся на два класса: ППД типа первичный/вторичный и равноранговые ППД. При реализации ППД первого класса в сети выделяется первичный (главный) узел, который управляет всеми остальными (вторичными) узлами, подключенными к каналу, и определяет, когда и какие узлы могут производить обмен данными. В сетях, где реализуются равноранговые (одноуровневые, одноранговые) протоколы,

все узлы имеют одинаковый статус. Однако если предварительно узлам присвоить разные приоритеты, то для них устанавливается неравноправный доступ в сеть.

Рассмотрим более подробно ППД в соответствии с их классификационной структурой, приведенной на рис. 12.4.

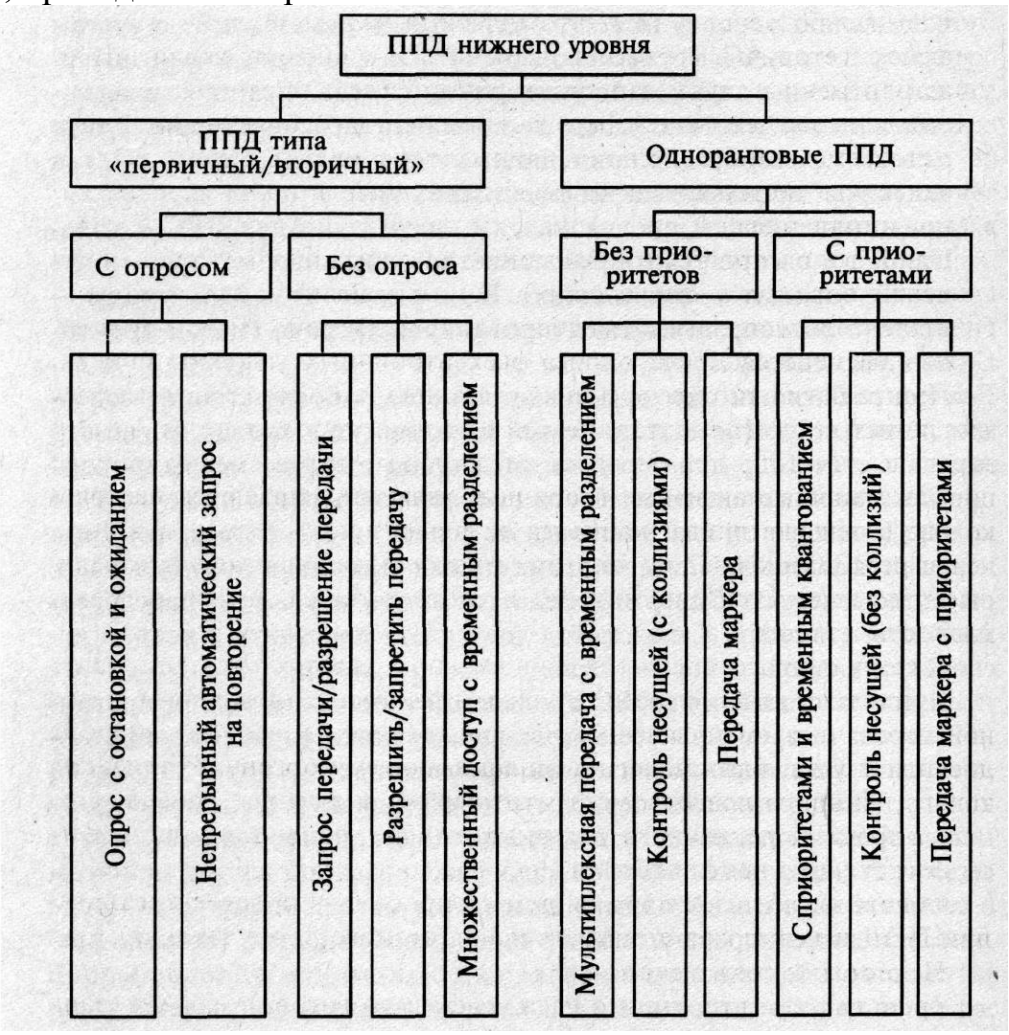

Рис. 12.4. Классификация ППД нижнего уровня

Один из широко распространенных подходов к управлению каналом связи основан на использовании протокола типа «первичный/вторичный» или «главный/подчиненный», когда первичный (главный) узел системы определяет для всех других узлов (вторичных, подчиненных), подключенных к каналу, порядок (очередность) обмена данными.

ППД типа «первичный/вторичный» могут быть реализованы на основе нескольких технологий, образующих две группы: с опросом и без опроса.

В сетях с опросом распространение получили протоколы, которые называются «опрос с остановкой и ожиданием» и «непрерывный автоматический запрос на повторение». Оба протокола относятся к классу ППД, реализующих селективные методы доступа к передающей среде. Технология доступа к передающей среде хорошо известна по применению в многоточечных линиях глобальных сетей.

Суть ее заключается в том, что первичный узел последовательно предлагает вторичным узлам подключиться к общему каналу передачи. В ответ на такой запрос вторичный узел, имея подготовленные данные, осуществляет передачу. Если подготовленных данных нет, выдается короткий пакет данных типа «данных нет»,

хотя в современных системах, как правило, реакцией в таких случаях является «молчание».

Наиболее распространенный способ организации запроса — циклический опрос, т.е. последовательное обращение к каждому вторичному узлу в порядке очередности, определяемой списком опроса. Цикл завершается после опроса всех вторичных узлов из списка. Для сокращения потерь времени, связанных с опросом неактивных вторичных узлов (т.е. узлов, по той или иной причине не готовых к передаче данных), применяются специальные варианты процедуры опроса: наиболее активные вторичные узлы опрашиваются несколько раз в течение цикла; наименее активные узлы — один раз в течение нескольких циклов; частота, с которой опрашиваются отдельные узлы, меняется динамически в соответствии с изменением активности узлов.

В сетях с многоточечными линиями применяется также опрос по принципу «готов — вперед». В каждой многоточечной линии опрос начинается с самого удаленного вторичного узла к другому, пока не достигнет узла, ближайшего к опрашивающему органу. Реализация такого принципа позволяет сократить время на распространение сигнала опроса от первичного узла к вторичным, однако это достигается за счет усложнения системы.

Основные преимущества систем с опросом — простота реализации ППД и невысокая стоимость используемого оборудования.

Недостатки таких систем:

- простаивание вторичного узла, имеющего готовые для передачи данные, в ожидании поступления сигнала «опрос»;
- неэффективное потребление дорогостоящих ресурсов канала, связанное с передачей служебной информации (сигналов опроса, сигналов ответной реакции);
- наличие узкого места по надежности (отказ первичного узла приводит к отказу всей сети) и по пропускной способности, так как обмен данными между вторичными звеньями осуществляется только через первичный узел.

Одной из простейших модификаций ППД типа «первичный/вторичный» с опросом является протокол ***«опрос с остановкой и ожиданием».*** **В** системах с таким протоколом узел после передачи кадра ожидает от адресата подтверждения в правильности его пересылки, что сопряжено с дополнительными затратами времени.

Непрерывный автоматический запрос на повторение передачи данных в дуплексных системах (точнее, в системах передачи данных с решающей обратной связью), которые допускают передачу данных в обоих направлениях между узлами, поддерживающими связь. В системах с таким протоколом (он называется также протоколом ARQ) узел связи может автоматически запрашивать другой узел и повторно производить передачу данных.

В системах с протоколом ARQ на передающей и принимающей станциях устанавливаются так называемые ***передающие*** **и** ***принимающие окна.*** При установке окна выделяется время на непрерывную передачу (прием) фиксированного числа кадров и резервируются необходимые для такого протокола ресурсы. Кадры, принадлежащие данному окну, передаются без периодических подтверждений со стороны адресата о приеме очередного кадра. Подтверждение передается после получения всех кадров окна, что обеспечивает экономию времени

на передачу фиксированного объема информации по сравнению с предыдущим протоколом. Однако приемник должен иметь достаточный объем зарезервированного буферного ЗУ для обработки непрерывно поступающего трафика.

В системах ARQ важное значение имеет размер окна (количество кадров в окне). Чем больше окно, тем большее число кадров может быть передано без ответной реакции со стороны приемника и, следовательно, тем большая экономия времени достигается за счет сокращения передачи служебной информации. Но увеличение размера окна сопровождается выделением больших ресурсов и буферной памяти для обработки поступающих сообщений. Кроме того, это отражается на эффективности реализуемых способов защиты от ошибок. В настоящее время в сетях, где используется протокол ARQ, предусматриваются семикадровые окна, т.е. передатчик может посылать семь кадров без получения ответного подтверждения после каждого кадра.

Концепция скользящих окон, реализованная в протоколе ARQ, является достаточно простой. Сложность заключается лишь в том, что первичный узел, связанный с десятками и даже сотнями вторичных узлов, должен поддерживать окно с каждым из них, обеспечивая эффективность передачи данных, управление потоками данных.

К ППД типа «первичный/вторичный» без опроса, используемым в ТВС, относятся:

- запрос передачи/разрешение передачи;
- разрешить/запретить передачу;
- множественный доступ с временным разделением.

Первые два протокола реализуют селективные методы доступа к передающей среде, а третий — методы, основанные на резервировании времени. Общим для этих протоколов является то, что инициатива в подаче запроса на обслуживание принадлежит, как правило, вторичному органу, причем запрос подается первичному органу, если действительно имеется необходимость в передаче данных или в получении данных от другого органа. Эффективность этого протокола по сравнению с ППД с опросом будет тем выше, чем в большей степени вторичные органы отличаются друг от друга по своей активности, т.е. по частоте подачи запросов на обслуживание.

Протокол типа «запрос передачи/разрешение передачи» применяется довольно широко в полудуплексных каналах связи ЛВС, так как взаимосвязан с распространенным короткодистанционным физическим интерфейсом RS-232-C. В соответствии с этим протоколом организация передачи данных между терминалом (вторичным органом) и ЭВМ (первичным органом) производится в такой последовательности: выдача терминалом запроса на передачу — выдача ЭВМ сигнала разрешения на передачу терминалом — передача данных от терминала к ЭВМ — сброс сигнала машиной — прекращение передачи терминалом.

Протокол типа «разрешить/запретить передачу» часто используется периферийными устройствами (печатающими устройствами, графопостроителями) для управления входящим в них трафиком. Главный орган (обычно ЭВМ) посылает данные в удаленный периферийный узел, скорость работы которого существенно меньше скорости работы ЭВМ и скорости передачи данных каналом. В связи с этим

возможно переполнение буферного ЗУ периферийного узла. Для предотвращения переполнения периферийный узел посылает к ЭВМ сигнал «передача выключена». Получив такой сигнал, ЭВМ прекращает передачу и сохраняет данные до тех пор, пока не получит сигнал «разрешить передачу», означающий, что периферийный узел готов принять новые данные, так как буферное ЗУ освободилось.

Множественный доступ с временным разделением широко используется в спутниковых сетях связи. Главная (эталонная) станция принимает запросы от вторичных (подчиненных) станций на предоставление канала связи и, реализуя ту или иную дисциплину обслуживания запросов, определяет, какие именно станции и когда могут использовать канал в течение заданного промежутка времени, т.е. предоставляет каждой станции слот. Получив слот, вторичная станция осуществляет временную подстройку, чтобы произвести передачу данных за заданный слот.

Одноранговые ППД разделяются на две группы: без приоритетов (в неприоритетных системах) и с учетом приоритетов (в приоритетных системах).

Мультиплексная передача с временным разделением — наиболее простая равноранговая неприоритетная система, где реализуются методы доступа к передающей среде, основанные на резервировании времени. Здесь используется жесткое расписание работы абонентов: каждой станции выделяется интервал времени (слот) использования канала связи, и все интервалы распределяются поровну между станциями. Во время слота станция получает канал в свое полное распоряжение. Такой протокол отличается простотой в реализации и широко применяется в глобальных и локальных сетях. Недостатки протокола:

- возможность неполного использования канала, когда станция, получив слот, не может загрузить канал полностью из-за отсутствия необходимого объема данных для передачи;
- нежелательные задержки в передаче данных, когда станция, имеющая важную и срочную информацию, вынуждена ждать своего слота или когда выделенного слота недостаточно для передачи подготовленных данных и необходимо ждать следующего слота.

Система с контролем несущей (с коллизиями) реализует метод случайного доступа к передающей среде (метод множественного доступа с прослушиванием несущей и разрешением коллизий, CSMA/CD — Caner Sense Maltiple Access with Collision Detection) и применяется в основном в локальных сетях. Все станции сети, будучи равноправными, перед началом передачи работают в режиме прослушивания канала. Если канал свободен, станция начинает передачу; если занят, — станция ожидает завершения передачи. Через некоторое случайное время она снова обращается к каналу.

Поскольку сеть CSMA/CD является равноранговой, в результате соперничества за канал могут возникнуть коллизии: станция В может передать свой кадр, не зная, что станция А уже захватила канал, поскольку от станции А к станции В сигнал распространяется за конечное время. В результате станция В, начав передачу, вошла в конфликт со станцией А (коллизия со станцией А).

Каждая станция способна одновременно и передавать данные, и «слушать» канал. При наложении двух сигналов в канале начинаются аномалии (в виде аномального изменения напряжения), которые обнаруживаются станциями, участвующими в коллизии.

Важным аспектом коллизии является окно коллизий, представляющее собой интервал времени, необходимый для распространения сигнала по каналу и обнаружения его любой станцией сети. В наихудших для одноканальной сети условиях время, необходимое для обнаружения столкновения сигналов (коллизии), в два раза больше задержки распространения, так как сигнал, образовавшийся в результате коллизии, должен распространяться обратно к передающим станциям. Чтобы окно коллизии было меньше, такой способ доступа целесообразно применять в сетях с небольшими расстояниями между станциями, т.е. в локальных сетях. Кроме того, вероятность появления коллизий возрастает с увеличением расстояния между станциями сети.

Коллизия является нежелательным явлением, так как приводит к ошибкам в работе сети и поглощает много канального времени для ее обнаружения и ликвидации последствий. Поэтому желательно реализовать некоторый алгоритм, позволяющий либо избежать коллизий, либо минимизировать их последствия.

В сети CSMA/CD эта проблема решается на уровне управления доступом к среде путем прекращения передачи кадра сразу же после обнаружения коллизии.
При обработке коллизии компонент управления доступом к среде передающей станции выполняет две функции:

- усиливает эффект коллизии путем передачи специальной последовательности битов, называемой ***затором.*** Цель затора — сделать коллизию настолько продолжительной, чтобы ее смогли заметить все другие передающие станции, которые вовлечены в коллизию. В ЛВС CSMA/CD затор состоит по меньшей мере из 32 бит, но не более 48 бит. Ограничение длины затора сверху необходимо для того, чтобы станции ошибочно не приняли его за действительный кадр. Любой кадр длиной менее 64 байт считается фрагментом испорченного сообщения и игнорируется принимающими станциями сети;
- после посылки затора прекращает передачу и планирует ее на более позднее время, определяемое на основе случайного выбора интервала ожидания.

Системы с доступом в режиме соперничества реализуются достаточно просто и при малой загрузке обеспечивают быстрый доступ к передающей среде, а также позволяют легко подключать и отключать станции. Они обладают высокой живучестью, поскольку большинство ошибочных и неблагоприятных условий приводит либо к молчанию, либо к конфликту (а обе эти ситуации поддаются обработке) и, кроме того, нет необходимости в центральном управляющем органе сети. Их основной недостаток: при больших нагрузках время ожидания доступа к передающей среде становится большим и меняется непредсказуемо, следовательно, не гарантируется обеспечение предельно допустимого времени доставки кадров. Такие системы применяются в незагруженных локальных сетях с небольшим числом абонентских станций (с увеличением числа станций увеличивается вероятность возникновения конфликтных ситуаций).

Метод передачи маркера широко используется в неприоритетных и приоритетных сетях с магистральной (шинной), звездообразной и кольцевой топологией. Он относится к классу селективных методов: право на передачу данных станции получают в определенном порядке, задаваемом с помощью маркера,

который представляет собой уникальную последовательность бит информации (уникальный кадр). Магистральные сети, использующие этот метод, называются сетями типа «маркерная шина», а кольцевые сети — сетями типа «маркерное кольцо».

В сетях типа «маркерная шина» (рис. 12.5) доступ к каналу обеспечивается таким образом, как если бы канал был физическим кольцом, причем допускается использование канала некольцевого типа (шинного, звездообразного).

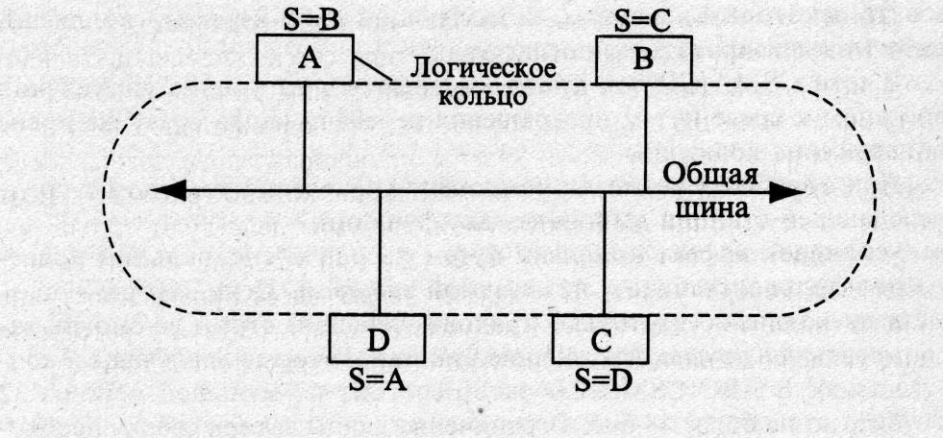

Рис.12.5 Протокол типа «маркерная шина»

Право пользования каналом передается организованным путем. Маркер (управляющий кадр) содержит адресное поле, где записывается адрес станции, которой предоставляется право доступа в канал. Станция, получив маркер со своим адресом, имеет исключительное право на передачу данных (кадра) по физическому каналу. После передачи кадра станция отправляет маркер другой станции, которая является очередной по установленному порядку владения правом на передачу. Каждой станции известен идентификатор следующей станции. Станции получают маркер в циклической последовательности, при этом в физической шине формируется так называемое логическое кольцо. Все станции «слушают» канал, но ***захватить*** канал для передачи данных может только та станция, которая указана в адресном поле маркера. Работая в режиме прослушивания канала, ***принять*** переданный кадр может только та станция, адрес которой указан в поле адреса получателя этого кадра.

В сетях типа «маркерная шина», помимо передачи маркера, решается проблема потери маркера из-за повреждения одного из узлов сети и реконфигурации логического кольца, когда в кольцо добавляется или из него удаляется один из узлов.

Преимущества такого метода доступа очевидны:

- не требуется физического упорядочения подключенных к шине станций, так как с помощью механизма логической конфигурации может быть обеспечен любой порядок передачи маркера станции, т. е. с помощью этого механизма осуществляется упорядочение использования канала станциями;
- имеется возможность использования в загруженных сетях;
- возможна передача кадров произвольной длины.

Протокол типа «маркерное кольцо» применяется в сетях с кольцевой топологией, которые относятся к типу сетей с последовательной конфигурацией, где широковещательный режим работы невозможен. В таких сетях сигналы

распространяются через однонаправленные двухточечные пути между узлами. Узлы и однонаправленные звенья соединяются последовательно, образуя физическое кольцо (рис. 12.6). В отличие от сетей с шинной структурой, где узлы действуют только как передатчики или приемники и отказ узла или удаление его из сети не влияет на передачу сигнала к другим узлам, здесь при распространении сигнала все узлы играют активную роль, участвуя в ретрансляции, усилении, анализе и модификации приходящих сигналов.

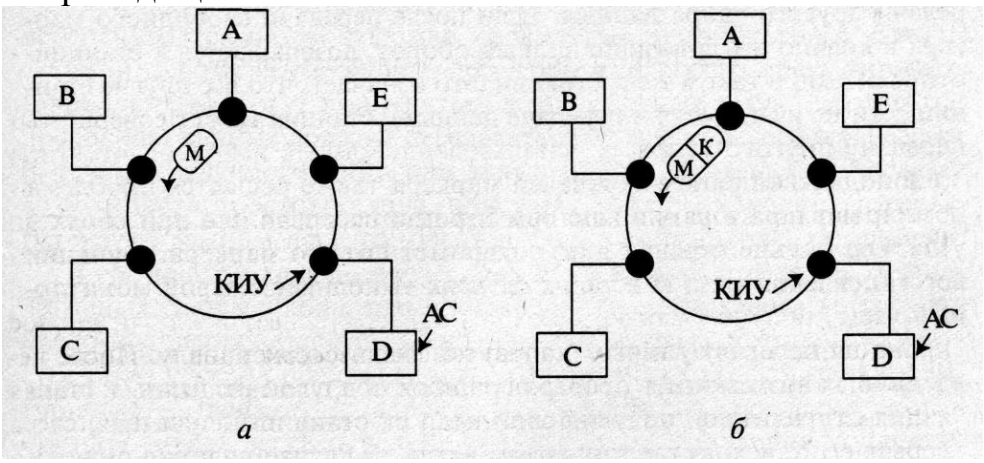

Рис. 12.6. Протокол типа «маркерное кольцо»:
а — маркер свободен; *б* — маркер занят; М - маркер; К - кадр; КИУ — кольцевое интерфейсное устройство

Как и в случае маркерной шины, в протоколе типа «маркерное кольцо» в качестве маркера используется уникальная последовательность битов. Однако маркер не имеет адреса. Он снабжается полем занятости, в котором записывается один из кодов, обозначающих состояние маркера — свободное или занятое. Если ни один из узлов сети не имеет данных для передачи, свободный маркер циркулирует по кольцу, совершая однонаправленное (обычно против часовой стрелки) перемещение (рис. 12.6, *а).* В каждом узле маркер задерживается на время, необходимое для его приема, анализа (с целью установления занятости) и ретрансляции. В выполнении этих функций задействованы кольцевые интерфейсные устройства (КИУ).

Свободный маркер означает, что кольцевой канал свободен и что любая станция, имеющая данные для передачи, может его использовать. Получив свободный маркер, станция, готовая к передаче кадра с данными, меняет состояние маркера на «занятый», передает его дальше по кольцу и добавляет к нему кадр (рис. 12.6, *б)*. Занятый маркер вместе с кадром совершает полный оборот по кольцу и возвращается к станции-отправителю. По пути станция-получатель, удостоверившись по адресной части кадра, что именно ей он адресован, снимает копию с кадра. Изменить состояние маркера снова на свободное может тот узел, который изменил его на занятое. По возвращении занятого маркера с кадром данных к станции-отправителю кадр удаляется из кольца, а состояние маркера меняется на свободное, после чего любой узел может захватить маркер и начать передачу данных. С целью предотвращения монополизации канала станция-отправитель не может повторно использовать возвращенный к ней маркер для передачи другого кадра данных. Если после передачи свободного маркера в кольцо он, совершив полный оборот, возвращается к станции-отправителю в таком же состоянии (это означает, что все

другие станции сети не нуждаются в передаче данных), станция может совершить передачу другого кадра.

В кольцевой сети с передачей маркера также решается проблема потери маркера в результате ошибок при передаче или при сбоях в узле. Отсутствие передач в сети означает потерю маркера. Функции восстановления кольца в таких случаях выполняет сетевой мониторный узел.

Основные преимущества протокола типа «маркерное кольцо»:

- имеется возможность проверки ошибок при передаче данных: станция-отправитель, получив свой кадр от станции-получателя, сверяет его с исходным вариантом кадра. В случае наличия ошибки кадр передается повторно;
- канал используется полностью, его простои отсутствуют;
- протокол может быть реализован в загруженных сетях;
- имеется принципиальная возможность (и в некоторых сетях она реализована) осуществлять одновременную передачу несколькими станциями сети. Недостатки такого протокола:
- невозможность передачи кадров произвольной длины;
- в простейшем (описанном выше) исполнении не предусматривает- . ся использование приоритетов, вследствие чего станция, имеющая для передачи важную информацию, вынуждена ждать освобождения маркера, что сопряжено с опасностью несвоевременной доставки данных адресату;
- протокол целесообразно использовать только в локальных сетях с относительно небольшим количеством узлов, так как в противном случае время на передачу данных может оказаться неприемлемо большим.

Равноранговые приоритетные системы представлены тремя подходами, реализованными в приоритетных слотовых системах (в системах с приоритетами и временным квантованием), в системах с контролем несущей без коллизий и в системах с передачей маркера с приоритетами.

Приоритетные слотовые системы подобны бесприоритетным системам, в которых осуществляется мультиплексная передача с временным разделением. Однако использование канала производится здесь на приоритетной основе. В качестве критериев для установления приоритетов применяются следующие: предшествующее владение слотом; время ответа, которое удовлетворяет станцию-отправителя; объем передаваемых данных (чем меньше объем, тем выше приоритет) и др.

Приоритетные слотовые системы могут быть реализованы без главной станции, управляющей использованием слотов. Управление обеспечивается путем загрузки параметров приоритетов в каждой станции. Кроме возможности децентрализованного обслуживания, такие системы могут применяться в загруженных сетях. Недостатки протокола: данные должны передаваться строго определенной длины (в течение заданного слота они должны быть переданы); существует возможность простоя канала, присущая всем протоколам, которые реализуют методы доступа, основанные на резервировании времени.

В системах с контролем несущей без коллизий, в отличие от аналогичных систем с коллизиями, используется специальная логика для предотвращения коллизий. Каждая станция сети, в которой реализуется такая система обслуживания

запросов, имеет дополнительное устройство — ***таймер*** или ***арбитр.*** Это устройство определяет, когда станция может вести передачу без опасности появления коллизий. Главная станция для управления использованием канала не предусматривается.

Установка времени на таймере, по истечении которого станция может вести передачу данных, осуществляется на приоритетной основе. Для станции с наивысшим приоритетом переполнение таймера наступает раньше. Если станция с высоким приоритетом не намерена вести передачу, канал будет находиться в состоянии покоя, т.е. свободен, и тогда следующая по приоритету станция может захватить канал.

Системы с контролем несущей без коллизий могут использоваться в более загруженных и протяженных сетях. Уменьшается также время простоя канала. Все это достигается за счет усложнения оборудования системы.

Приоритетные системы с передачей маркера применяются обычно в кольцевых локальных сетях. Здесь преодолен недостаток, характерный для неприоритетных систем с передачей маркера.

Каждой станции сети определен свой уровень приоритета, причем чем выше уровень приоритета, тем меньше его номер. Назначение приоритетной схемы состоит в том, чтобы дать возможность каждой станции зарезервировать использование канала для следующей пере- дачи по кольцу. Каждый узел анализирует перемещающийся по кольцу маркер, который содержит поле резервирования (ПР). Если собственный приоритет выше, чем значение приоритета в ПР маркера, станция увеличивает значение приоритета в ПР до своего уровня, резервируя тем самым маркер на следующий цикл. Если в данном цикле какой-то другой узел не увеличит еще больше значение уровня приоритета в ПР, этой станции разрешается использовать маркер и канал во время следующего цикла передачи по кольцу (за время цикла маркер совершает полный оборот по кольцу).

Для того чтобы запросы на обслуживание со стороны станций с низким приоритетом не были потеряны, станция, захватившая маркер, должна запомнить предыдущее значение ПР в своем ЗУ. После «высвобождения» маркера, когда он завершит полный оборот по кольцу, станция восстанавливает предыдущий запрос к сети, имеющий более низкий приоритет.

12.4. Обеспечение безопасности информации в сетях

Существует постоянная опасность несанкционированных (преднамеренных и непреднамеренных) действий над циркулирующей в сетях информацией, следствием чего стали все возрастающие расходы и усилия на ее защиту.

По мере развития ПЭВМ, увеличения их количества и доступности все больший размах приобретает информационное пиратство: несанкционированное копирование программных продуктов и данных, финансовые преступления с применением ЭВМ, компьютерные диверсии (вирусы, «логические бомбы», «черви», «троянские кони» и т.п.). Появление ТВС, особенно сети Интернет, еще в большей степени стимулировало такое пиратство, значительно увеличив количество доступных пирату компьютеров за счет исключения необходимости физического доступа к ним и сделав сам процесс более увлекательным в силу его интерактивности.

Защита информации в компьютерных сетях становится одной из самых острых проблем в современной информатике. Сформулировано ***три базовых принципа информационной безопасности,*** которая должна обеспечивать [16; 17]:

- целостность данных (защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных);
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей. В рамках комплексного рассмотрения вопросов обеспечения безопасности информации различают ***угрозы безопасности, службы безопасности (СБ)*** **и** ***механизмы реализации функций служб безопасности.***

Характер проникновения (несанкционированного доступа) в сеть может быть классифицирован по таким показателям: преднамеренность, продолжительность проникновения, воздействие проникновения на информационную среду сети, фиксированность проникновения в регистрационных и учетных данных сети.

По первому показателю проникновение может быть случайным или преднамеренным. ***Случайное проникновение*** происходит из-за ошибок или сбоев программ или оборудования, оно может быть связано с недостаточной надежностью используемых линий связи. Такое проникновение редко бывает опасным, если не оказывается разрушающее воздействие на информационную среду. ***Преднамеренное проникновение*** происходит в результате сознательно предпринимаемых действий со стороны злоумышленника и свидетельствует о его серьезных интересах. Это наиболее опасное проникновение.

По *продолжительности проникновения* они могут быть кратковременными и долговременными. ***Кратковременное проникновение*** свидетельствует о случайности или нежелании злоумышленника привлечь к себе внимание. Оно менее опасно, но зато имеет больше шансов остаться незамеченным. ***Долговременное проникновение,*** как правило, связано с устойчивой заинтересованностью в чужом информационном пространстве с целью изучения его структуры и содержания.

Воздействие проникновения на информационную среду может быть:

- неразрушающим, когда сеть продолжает функционировать нормально, так как в результате проникновения не пострадали ни программы, ни данные. Если оно не случайное, то является весьма опасным и свидетельствует о намерении злоумышленника использовать в дальнейшем найденный канал доступа к чужой информации;
- разрушающим, когда в результате проникновения внесены какие-либо изменения в программы и/или данные, что сказывается на работе сети. Его последствия при надлежащем ведении архивов могут быть сравнительно легко устранены;
- разовым или многократным, что свидетельствует о серьезности намерений и требует решительных действий.

По *фиксированности проникновении* в регистрационных и учетных данных сети они могут быть:

- зарегистрированными администратором сети при проведении периодического анализа регистрационных данных. Они свидетельствуют о необходимости совершенствования или модификации системы защиты;
- незарегистрированными администратором сети.

Различают следующие ***виды воздействия*** на информацию в случае преднамеренного проникновения в сеть [17]:

- уничтожение, т.е. физическое удаление информации (файлов) с носителей информации. Оно выявляется при первой же попытке обращения к этой информации, а все потери легко восстанавливаются при налаженной системе резервирования и архивации;
- разрушение — нарушение целостности программ и структур данных, вызывающих невозможность их использования: программы не запускаются, а при обращении к структурированным данным происходит (хотя и не всегда) сбой;
- искажение — нарушение логики работы программ или связей в структурированных данных, не вызывающих отказа в их работе или использовании. Это один из опасных видов воздействия, так как его нельзя обнаружить;
- подмена, т.е. замена существующих программ или данных другими под тем же именем и так, что внешне это никак не проявляется. Это очень опасный вид воздействия. Единственно надежным способом защиты от такого воздействия для программ является побитовое сравнение с эталонной версией программы;
- копирование, т.е. получение копии программ или данных на другом компьютере. Это воздействие не является опасным, поскольку не угрожает нормальному функционированию сети, однако оно наносит наибольший ущерб в случаях промышленного шпионажа;
- добавление новых компонентов, т.е. запись в память компьютера других программ или данных, ранее в ней отсутствовавших. Такое воздействие опасно, так как функциональное назначение добавляемых компонентов неизвестно;
- заражение вирусом — это такое однократное воздействие на программы или данные, при котором они изменяются и, кроме того, при обращении к ним вызываются подобные изменения в других, как правило аналогичных, компонентах (происходит «цепная реакция», распространение вируса в компьютере или локальной сети).

К перечисленным видам воздействия на информацию в сети следует добавить следующие ***угрозы безопасности:*** несанкционированный обмен информацией между пользователями (может привести к получению одним из них не предназначенных ему сведений); отказ от информации, т.е. непризнание получателем (отправителем) этой информации факта ее получения (отправления), что может привести к различным злоупотреблениям; отказ в обслуживании, который может сопровождаться тяжелыми последствиями для пользователя, обратившегося с запросом на предоставление сетевых услуг.

Величина наносимого ущерба определяется как видом несанкционированного воздействия, так и тем, какой именно объект информационных ресурсов ему подвергся.

В качестве возможных ***объектов воздействия*** могут быть:

- операционная система, обслуживающая сеть (в настоящее время только отдельные операционные системы сертифицированы на определенный класс

защиты, предусматривающий требование защиты самой себя от изменений);
- служебные, регистрационные таблицы и файлы обслуживания сети — это файлы паролей, прав доступа пользователей к ресурсам, ограничения по времени, функциям и т.д.;
- программы и таблицы шифровки информации, циркулирующей в сети.

Любое воздействие на эти компоненты вызовет отказ в работе или серьезные сбои, но наиболее опасно копирование, которое может открыть возможность дешифровки информации;
- операционные системы компьютеров конечных пользователей;
- специальные таблицы и файлы доступа к данным на компьютерах конечных пользователей — это пароли файлов или архивов, индивидуальные таблицы шифровки / дешифровки данных, таблицы ключей и т.д. Степень опасности воздействия на них зависит от принятой системы защиты и от ценности защищаемой информации. Наиболее опасным воздействием является копирование этой информации;
- прикладные программы на компьютерах сети и их настроечные таблицы (здесь для разработчиков новых прикладных программ серьезную угрозу представляет копирование, так как в ходе разработки большинство программ существуют в незащищенном виде);
- информационные файлы компьютеров сети, базы данных, базы знаний экспертных систем и т.д. Наибольший ущерб наносит копирование и последующее распространение этой информации;
- текстовые документы, электронная почта и т.д.;
- параметры функционирования сети — это главным образом ее производительность, пропускная способность, временные показатели обслуживания пользователей. Здесь признаками возможного несанкционированного воздействия на сеть, сопровождаемого ухудшением параметров ее функционирования, являются: замедление обмена информацией в сети или возникновение необычно больших очередей обслуживания запросов пользователей, резкое увеличение трафика (данных пользователей) в сети или явно преобладающее время загрузки процессора сервера каким-либо отдельным процессором. Все эти признаки могут быть выявлены и обслужены только при четко отлаженном аудите и текущем мониторинге работы сети.

Основными ***источниками преднамеренного проникновения*** в сеть являются:
- взломщики сетей — хакеры, в действиях которых почти всегда есть состав преступления, независимо от того, осознают они это или нет. Наибольшую угрозу представляют сформировавшиеся виртуальные банды хакеров, цель которых — сделать всю информацию в мире свободной и доказать каждому, что их нельзя остановить. Они хорошо организованы и даже создали всемирные объединения с регулярными встречами и съездами;
- уволенные или обиженные сотрудники сети — эта категория людей наиболее опасна и способна нанести существенный ущерб, особенно если речь идет об администраторах сети, так как они обладают знаниями системы и принципами защиты информации и по долгу службы имеют доступ к программам сниффинга (перехвата паролей и имен пользователей в сети, ключей, пакетов и т.д.);

• профессионалы — специалисты по сетям, посвятившие себя промышленному шпионажу;
• конкуренты, степень опасности которых зависит от ценности информации, к которой осуществляется несанкционированный доступ, и от уровня их профессионализма.

Что же касается источников непреднамеренного проникновения в сеть, то здесь речь должна идти скорее о причинах случайного проникновения. Помимо упоминавшихся выше сбоев программ и оборудования, причинами такого проникновения являются неправильные установка и конфигурирование сетевых операционных систем и средств защиты (особенно в неоднородных и многопротокольных сетях), а также ошибки, беспечность или халатность конечных пользователей. Особую опасность представляют недостаточно обученные и недостаточно контролируемые пользователи с привилегированными правами.

Нейтрализация перечисленных и других угроз безопасности осуществляется службами безопасности сети и механизмами реализации функций этих служб. Документами Международной организации стандартизации (МОС) определены следующие ***службы безопасности:***

• аутентификация (подтверждение подлинности);
• обеспечение целостности передаваемых данных;
• засекречивание данных;
• контроль доступа;
• защита от отказов.

Первые три службы характеризуются различиями для виртуальных и дейтаграммных сетей, а последние две службы инварианты по отношению к этим сетям.

В *виртуальных сетях* используются протоколы информационного обмена типа виртуального соединения. Передача информации между абонентами организуется по виртуальному каналу и происходит в три этапа: создание (установление) канала, собственно передача и уничтожение (разъединение) канала. При этом сообщения разбиваются на одинаковые части (пакеты). Пакеты передаются по виртуальному каналу в порядке их следования в сообщении.

В *дейтаграммных сетях* реализуются дейтаграммные протоколы информационного обмена. Пакеты, принадлежащие одному и тому же сообщению, передаются от отправителя к получателю в составе дейтаграмм независимо друг от друга и в общем случае по различным маршрутам, т.е. в сети они являются самостоятельными единицами информации. На приемном пункте из пакетов, поступивших по различным маршрутам и в разное время, составляется первоначальное сообщение.

Службы и механизмы безопасности используются на определенных уровнях эталонной модели ВОС [26].

В табл. 12.1 представлено распределение служб безопасности (СБ) по уровням эталонной модели ВОС, а в табл. 12.2 — механизмы реализации служб безопасности.

Служба аутентификации, в виртуальных сетях называемая службой аутентификации одноуровневого объекта, обеспечивает подтверждение (опровержение) того, что объект, предлагающий себя в качестве отправителя

сообщения по виртуальному каналу, является именно таковым как на этапе установления связи между абонентами, так и на этапе передачи сообщения. В дейтаграммных сетях эта служба называется службой аутентификации источника данных, передаваемых в виде дейтаграмм.

Таблица 12.1 **Распределение СБ по уровням эталонной модели ВОС**

№ п/п	Наименование СБ	Уровни модели						
		1	2	3	4	5	6	7
	СБ виртуальных сетей							
1	Аутентификация одноуровневого объекта			+	+			+
2	*Целостность соединения* с восстановлением				+			+
3	Целостность соединения без восстановления			+	+			+
4	Целостность выборочных полей соединения							+
5	Засекречивание соединения	+	+	+	+			+
6	Засекречивание выборочных полей соединения							+
	СБ дейтаграммных сетей							
7	Аутентификация источника данных			+	+			+
8	Целостность без соединения			+	+			+
9	Целостность выборочных полей без соединения							+
10	Засекречивание без соединения		+	+	+			+
11	Засекречивание выборочных полей без соединения							+
	Общие СБ							
12	*Засекречивание потока данных*	+		+				+
13	Контроль доступа			+	+			+
14	Защита от отказов с подтверждением источника							+
15	Защита доступа с подтверждением доставки							+

-

Таблица 12.2. **Механизмы реализации СБ**

№ п/п	Наименование механизма	СБ виртуальных сетей					СБ дейтаграммных сетей					Общие службы безопасности				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Шифрование	+	+	+	+	+	+	+	+	+	+	+	+			
2	Цифровая подпись	+						+	+	+					+	+
3	Контроль доступа													+		
4	Обеспечение целостности данных		+	+	+				+	+					+	+
5	Обеспечение аутентификации	+														
6	Подстановка трафика												+			
7	Управление маршрутизацией					+					+		+			
8	Арбитраж															+

Службы целостности обеспечивают выявление искажений в передаваемых данных, вставок, повторов и уничтожение данных. Они разделяются по виду сетей, в которых они применяются (СБ в виртуальных и дейтаграммных сетях), по действиям, выполняемым при обнаружении аномальных ситуаций (с восстановлением данных или без восстановления), по степени охвата передаваемых данных (сообщение или дейтаграмма в целом либо их части, называемые выборочными полями).

Службы засекречивания обеспечивают секретность передаваемых данных: в виртуальных сетях — всего пересылаемого сообщения или только его выборочных полей, в дейтаграммных — каждой дейтаграммы или только отдельных ее элементов.

Служба засекречивания потока данных (трафика), являющаяся общей для виртуальных и дейтаграммных сетей (как и службы 13-я, 14-я, 15-я табл. 12.1), предотвращает возможность получения сведений об абонентах сети и характере использования сети.

Служба контроля доступа обеспечивает нейтрализацию попыток несанкционированного использования общесетевых ресурсов.

Службы защиты от отказов нейтрализуют угрозы отказов от информации со стороны ее отправителя и/или получателя.

Механизмы реализации указанных СБ представлены соответствующими, преимущественно программными, средствами. Некоторые из механизмов, перечисленных в табл. 12.2, используются для реализации не одной, а ряда служб безопасности. Это относится к шифрованию, цифровой подписи, обеспечению целостности данных, управлению маршрутизацией.

Для использования механизмов шифрования необходима специальная служба генерации ключей и их распределения между абонентами сети.

Механизмы цифровой подписи основываются на алгоритмах асимметричного шифрования. Они включают процедуры формирования подписи отправителем и ее опознавание (верификацию) получателем.

Механизмы контроля доступа, реализующие функции одноименной СБ, отличаются многообразием. Они осуществляют проверку полномочий объектов сети (пользователей и программ) на доступ к ее ресурсам.

Механизмы обеспечения целостности данных, реализуя функции одноименных служб, выполняют взаимосвязанные процедуры шифрования и дешифрования данных отправителем и получателем.

Механизмы обеспечения аутентификации, на практике обычно совмещаемые с шифрованием, цифровой подписью и арбитражем, реализуют одностороннюю или взаимную аутентификацию, когда проверка подписи осуществляется либо одним из взаимодействующих одноуровневых объектов, либо она является взаимной.

Механизмы подстановки трафика, используемые для реализации службы засекречивания потока данных, основываются на генерации объектами сети фиктивных блоков, их шифрования и передаче по каналам связи. Этим затрудняется и даже нейтрализуется возможность получения информации об абонентах сети и характере потоков информации в ней.

Механизмы управления маршрутизацией, используемые для реализации служб засекречивания, обеспечивают выбор безопасных, физически надежных маршрутов для передачи секретных сведений.

Механизмы арбитража обеспечивают подтверждение третьей стороной (арбитром) характеристик данных, передаваемых между абонентами.