

Учреждение образования  
«Белорусский государственный университет информатики и  
радиоэлектроники»

Факультет вечернего, заочного и дистанционного обучения  
Кафедра ЭВМ

Контрольная работа №2  
по дисциплине «Вычислительные комплексы, системы и сети».  
Вариант №1  
студента 5 курса 500503 учебной группы  
Авсеева С.П.

Минск 2009

# Содержание

1. Структура сети и особенности метода доступа к среде передачи в сетях технологии FDDI . . . . .	2
2. Структурная организация корпоративных сетей. Способы структуризации корпоративных сетей . . . . .	4
3. Отбражение IP-адресов на локальные (MAC) адреса и обратно (ARP и RARP-протоколы) . . . . .	5
4. Протокол дейтаграмм пользователя UDP . . . . .	7
5. Функциональные группы задач управления. Многоуровневое представление задач управления . . . . .	10
6. Протокол взаимодействия сервера с клиентской станцией (NCP) . . . . .	12
7. Многопроцессорные вычислительные комплексы (МПК) с общей шиной . . . . .	14
8. Принципы построения и структуры ассоциативных ВС .	16
9. Литература . . . . .	18

# 1 Структура сети и особенности метода доступа к среде передачи в сетях технологии FDDI

FDDI явился первой технологией локальных сетей со скоростью передачи данных 100Мбит/с.

В качестве сети передачи данных используется волоконно-оптический кабель, впервые эта технология была опубликована в 1985г. комитетом ХЗТ9.5. В 1986 году стандарт был усовершенствован — FDDI-II. В последствии стандарт был доработан и принят IEEE 802.8 и ISO 9314.

FDDI развивает технологию сетей Token Ring, совершенствует некоторые характеристики этой сети, в ней используется не просто маркерный способ, а маркерно-временной, т.е. время удержания маркера не фиксировано, а зависит от времени прохождения маркером кольца.

Пакеты могут передаваться в синхронном и асинхронном режимах. В асинхронном режиме возможно использование приоритетов передаваемых данных.

Кадр маркер выдается очередной станцией сразу после передачи кадра данные.

Сеть строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных.

Структура канального и физического уровня управления, примерно соответствует стандарту локальных сетей предложенному IEEE.

OSI/ISO	FDDI
...	
Транспортный уровень	
Сетевой уровень	
Канальный уровень	УЛЗ (LLC) УДС (MAC)
Физический уровень	УФС (PHY) ПФС (PMD)

LLC уровень выполняет те же функции, что и в сетях Token Ring, задачей этого уровня является реализация обмена пакетами между станциями.

Возможно 3 режима:

- без установления соединения, без подтверждения приема;
- без установки соединения, с подтверждением приема;
- с установлением соединения и подтверждением приема.

MAC уровень определяет метод доступа к среде передачи данных, в данной технологии используется маркерно-временной метод.

PHY (physical layer device) подуровень управления физическим сигналом, использует следующие функции:

- логическое кодирование путем замены четырех бит исходного кода пятибитовым кодом;
- кодирование сигнала с помощью циклического кода, при передаче, и обнаружении ошибки, при приеме.

PMД (physical media dependent) подуровень физического представления, выполняет следующие функции:

- формирование NRZI кода;
- характеристика среды передачи данных;
- требования к T-коннектору;
- требования к приемо-передатчику.

Особенностью этих сетей является наличие на первом и втором уровне, протокола управления станцией (SMT), с его помощью обеспечивается взаимодействие подуровней между собой, а так же между станциями. SMT предусматривает ряд пакетов – внутренние пакеты управления.

## 2 Структурная организация корпоративных сетей. Способы структуризации корпоративных сетей

Корпоративные сети называют также сетями масштаба предприятия, что соответствует дословному переводу термина «enterprise-wide networks», используемого в англоязычной литературе для обозначения этого типа сетей. Сети масштаба предприятия (корпоративные сети) объединяют большое количество компьютеров на всех территориях отдельного предприятия. Они могут быть сложно связаны и покрывать город, регион или даже континент. Число пользователей и компьютеров может измеряться тысячами, а число серверов - сотнями, расстояния между сетями отдельных территорий могут оказаться такими, что становится необходимым использование глобальных связей (рис. 2.1). Для соединения удаленных локальных сетей и отдельных компьютеров в корпоративной сети применяются разнообразные телекоммуникационные средства, в том числе телефонные каналы, радиоканалы, спутниковая связь. Корпоративную сеть можно представить в виде «островков локальных сетей», плавающих в телекоммуникационной среде.

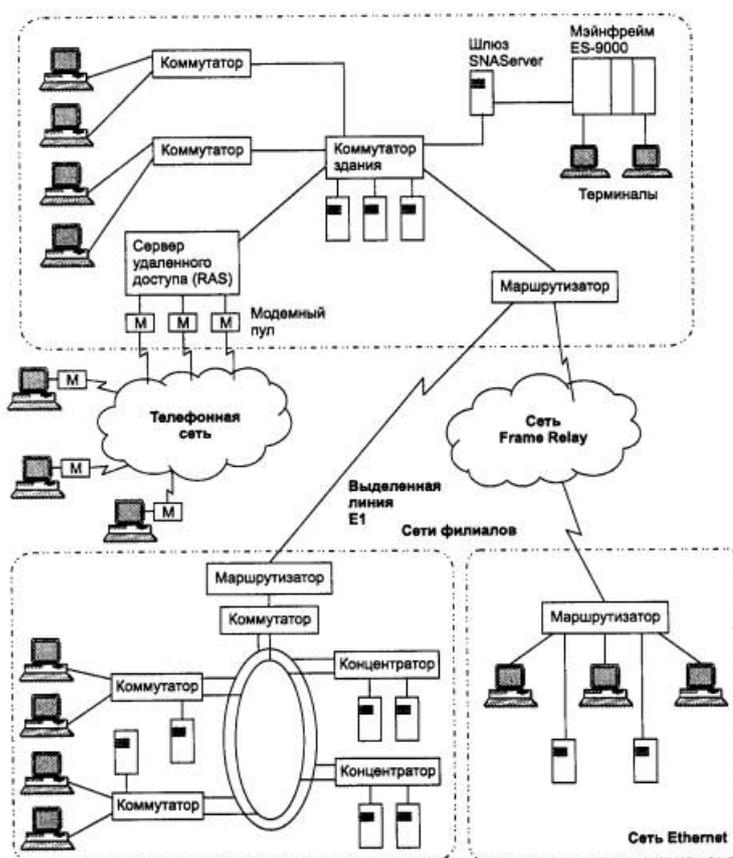


Рис. 2.1. Пример корпоративной сети

### 3 Отбражение IP-адресов на локальные (MAC) адреса и обратно (ARP и RARP-протоколы)

Для определения локального адреса по IP-адресу используется протокол разрешения адреса (Address Resolution Protocol, ARP). Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети - протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети или же протокол глобальной сети (X.25, frame relay), как правило не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу — нахождение IP-адреса по известному локальному адресу. Он называется реверсивным ARP (Reverse Address Resolution Protocol, RARP) и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

Существует четыре типа ARP-сообщений: ARP-запрос (ARP request), ARP-ответ (ARP reply), RARP-запрос (RARP-request) и RARP-ответ (RARP-reply). Локальный хост при помощи ARP-запроса запрашивает физический адрес хоста-получателя. Ответ (физический адрес хоста-получателя) приходит в виде ARP-ответа. Хост-получатель, вместе с ответом, шлёт также RARP-запрос, адресованный отправителю, для того, чтобы проверить его IP-адрес. После проверки IP-адреса отправителя начинается передача пакетов данных.

#### 3.1 Структура пакета

Ниже представлена структура пакета, используемого в ARP-запросах и ответах. В сетях Ethernet эти пакеты используют EtherType 0x0806, и рассылаются широковещательно MAC-адрес — FF:FF:FF:FF:FF:FF. Отметим, что в структуре пакета, показанной ниже в качестве SHA, SPA, THA, TRA условно используются 32-битные слова — реальная длина определяется физическим устройством и протоколом.

Биты	Значение
0-15	HTYPE
16-31	PTYPE
32-47	HLEN
48-63	PLEN
48-63	OPER
64-...	SHA
...	SPA

Биты	Значение
...	ТНА
...	ТРА

Hardware type (HTYPE). Каждый транспортный протокол передачи данных имеет свой номер, который хранится в этом поле. Например, Ethernet имеет номер 0x0001.

Protocol type (PTYPE). Код протокола. Например, для IPv4 будет записано 0x0800.

Hardware length (HLEN). Длина физического адреса в байтах. Ethernet адреса имеют длину 6 байт.

Protocol length (PLEN). Длина логического адреса в байтах. IPv4 адреса имеют длину 4 байта.

Operation. Код операции отправителя: 1 в случае запроса и 2 в случае ответа.

Sender hardware address (SHA). Физический адрес отправителя.

Sender protocol address (SPA). Логический адрес отправителя.

Target hardware address (THA). Физический адрес получателя. Поле пусто при запросе.

Target protocol address (TPA). Логический адрес получателя.

## 4 Протокол дейтаграмм пользователя UDP

UDP (англ. User Datagram Protocol — протокол пользовательских дейтаграмм) — это транспортный протокол для передачи данных в сетях IP без установления соединения. Он является одним из самых простых протоколов транспортного уровня модели OSI. Его IP-идентификатор — 0x11.

В отличие от TCP, UDP не гарантирует доставку пакета. Это позволяет ему гораздо быстрее и эффективнее доставлять данные для приложений, которым требуется большая пропускная способность линий связи, либо требуется малое время доставки данных.

Недостаточная надёжность протокола может выражаться как в потере отдельных пакетов, так и в их дублировании. UDP используется при передаче потокового видео, игр реального времени, а также некоторых других типов данных.

Ненадёжность протокола UDP надо понимать в том смысле, что в случаях влияния внешних факторов, приводящих к сбоям, протокол UDP не предусматривает стандартного механизма повторения передачи потерянных пакетов. В этом смысле он настолько же надёжен, как и протокол ICMP.

Если приложению требуется большая надёжность, то используется протокол TCP или SCTP, либо реализуется какой-нибудь свой нестандартный алгоритм повторения передач в зависимости от условий.

### 4.1 Формат UDP-дейтаграммы

Единица данных протокола UDP называется UDP-дейтаграммой, или пользовательской дейтаграммой. Каждая дейтаграмма переносит отдельное пользовательское сообщение. Это приводит к естественному ограничению: длина дейтаграммы UDP не может превышать длины поля данных протокола IP, которое, в свою очередь, ограничено размером кадра технологии нижнего уровня. Поэтому если UDP-буфер переполняется, то данные приложения отбрасываются. Первый 64 бита дейтаграммы представляют собой UDP-заголовок, остальные биты — данные сообщения.

Биты	Значение
0-15	Порт отправителя
16-31	Порт получателя
32-47	Длина дейтаграммы
48-63	Контрольная сумма
64-...	Данные

Значение поля «длина дейтаграммы» указывает на длину всего UDP-сообщения, то есть включая и UDP-заголовок. Измеряется в октетах (бай-

тах). Для вычисления максимальной длины данных в UDP-сообщении необходимо учесть, что UDP-сообщение в свою очередь является содержимым области данных IP-сообщения. Максимальная длина IP-сообщения (с учетом заголовка) равна 65535 октетов. Потому максимальная длина UDP-сообщения (за вычетом минимального IP-заголовка) равна  $65535 - 20 = 65515$  октетов. Длина заголовка UDP-сообщения равна 8 октетам, следовательно, максимальная длина данных в UDP-сообщении равна  $65515 - 8 = 65507$  октетов. На практике сообщения максимальной длины не используются — ограничиваются 8192 октетами данных.

UDP-заголовок не содержит информации об адресе отправителя и получателя, поэтому даже при совпадении порта получателя нельзя с точностью сказать, что сообщение пришло в нужное место. Для проверки того, что UDP-сообщение достигло пункта своего назначения, используется дополнительный псевдозаголовок:

Биты	Значение
0-31	IP-адрес отправителя
32-63	IP-адрес получателя
64-71	0
71-79	Протокол (0x11)
80-95	Длина UDP-дейтаграммы

## 4.2 Расчёт контрольной суммы

Перед расчетом контрольной суммы UDP-сообщение дополняется в конце нулевыми битами до длины, кратной 16 битам (псевдозаголовки и добавочные нулевые биты не отправляются вместе с сообщением). Поле контрольной суммы в UDP-заголовке во время расчета контрольной суммы отправляемого сообщения принимается нулевым.

Для расчета контрольной суммы псевдозаголовки и UDP-сообщение разбивается на слова (1 слово = 2 байта (октета) = 16 бит). Затем рассчитывается поразрядное дополнение до единицы суммы всех слов с поразрядным дополнением. Результат записывается в соответствующее поле в UDP-заголовке.

В том случае, если контрольная сумма получилась равной нулю, поле заполняют единицами. Если контрольную сумму не требуется рассчитывать, значение поля оставляют нулевым.

При получении сообщения получатель считает контрольную сумму заново (уже учитывая поле контрольной суммы), и, если в результате получится двоичное число из шестнадцати единиц (то есть 0xffff), то контрольная сумма считается сошедшейся, и сообщение принимается.

### 4.3 Применение

UDP используется в следующих протоколах:

- DNS (Domain Name System)
- RTP (Real-time Transport Protocol) и RTCP (Real Time Control Protocol)
- TFTP (Trivial File Transfer Protocol)
- SNTP (Simple Network Time Protocol)
- NTP (Network Time Protocol)
- NFS (Network File System)

## 5 Функциональные группы задач управления. Многоуровневое представление задач управления

Существуют рекомендации ITU-T X.700 и близкий к ним стандарт ISO 7498-4, которые делят задачи системы управления на пять функциональных групп:

1. Управление конфигурацией сети и именовани<sup>ем</sup>. Эти задачи заключаются в конфигурировании параметров как элементов сети, так и сети в целом. Для элементов сети, таких как маршрутизаторы, мультиплексоры и т.п., с помощью этой группы задач определяются сетевые адреса, идентификаторы (имена), географическое положение и пр. Для сети в целом управление конфигурацией обычно начинается с построения карты сети, то есть отображении реальных связей между элементами сети и изменении связей между элементами сети — образование новых физических или логических каналов, изменение таблиц коммутации и маршрутизации.
2. Обработка ошибок. Эта группа задач включает выявление, определение и устранение последствий сбоев и отказов в работе сети. На этом уровне выполняется не только регистрация сообщений об ошибках, но и их фильтрация, маршрутизация и анализ на основе некоторой корреляционной модели. Фильтрация позволяет выделить из весьма интенсивного потока сообщений об ошибках, который обычно наблюдается в большой сети, только важные сообщения, маршрутизация обеспечивает их доставку нужному элементу системы управления, а корреляционный анализ позволяет найти причину, породившую поток взаимосвязанных сообщений (например, обрыв кабеля может быть причиной большого количества сообщений о недоступности сетей и серверов).
3. Анализ производительности и надежности. Задачи этой группы связаны с оценкой на основе накопленной статистической информации таких параметров, как время реакции системы, пропускная способность реального или виртуального канала связи между двумя конечными абонентами сети, интенсивность трафика в отдельных сегментах и каналах сети, вероятность искажения данных при их передаче через сеть, а также коэффициент готовности сети или ее определенной транспортной службы. Функции анализа производительности и надежности сети нужны как для оперативного управления сетью, так и для планирования развития сети.

4. Управление безопасностью. Задачи этой группы включают в себя контроль доступа к ресурсам сети (данным и оборудованию) и сохранение целостности данных при их хранении и передаче через сеть. Базовыми элементами управления безопасностью являются процедуры аутентификации пользователей, назначение и проверка прав доступа к ресурсам сети, распределение и поддержка ключей шифрования, управления полномочиями и т.п. Часто функции этой группы не включаются в системы управления сетями, а реализуются либо в виде специальных продуктов (например, системы аутентификации и авторизации Kerberos, различных защитных экранов, систем шифрования данных), либо входят в состав операционных систем и системных приложений.
5. Учет работы сети. Задачи этой группы занимаются регистрацией времени использования различных ресурсов сети — устройств, каналов и транспортных служб. Эти задачи имеют дело с такими понятиями, как время использования службы и плата за ресурсы.

Кроме описанного выше разделения задач управления на несколько функциональных групп, полезно разделять задачи управления на уровни в соответствии с иерархической организацией корпоративной сети. Корпоративная сеть строится иерархически, отражая иерархию самого предприятия и его задач. Нижний уровень сети составляют элементы сети — отдельные компьютеры, коммуникационные устройства, каналы передачи данных. На следующем уровне иерархии эти элементы образуют сети разного масштаба — сеть рабочей группы, сеть отдела, сеть отделения и, наконец, сеть предприятия в целом.

## 6 Протокол взаимодействия сервера с клиентской станцией (NCP)

В NetWare протокол NCP (NetWare Core Protocol) является надстройкой над протоколом IPX и используется для организации обмена между рабочей станцией и файловым сервером.

Связь между рабочей станцией и файловым сервером, которые используют API-интерфейс к протоколу NCP, обычно организуется по следующей схеме:

- NLM-модуль регистрирует какую-либо свою функцию как расширение NCP;
- программа на рабочей станции или файловом сервере связывается с NetWare и получает требуемый идентификатор расширения NCP;
- программа на рабочей станции или файловом сервере использует зарегистрированную функцию NLM-модуля как удалённую процедуру, передавая ей исходные данные и получая результаты обработки.

### 6.1 Формат заголовка

Формат заголовка пакета в NCP представляется следующим образом:

Биты	Значение
0-15	Тип запроса
16-23	Номер по порядку
24-31	Младшая часть номера канала
32-39	Номер задачи
40-47	Старшая часть номера канала
48-55	Код запроса
56-...	Данные

Поле тип запроса характеризует запрос, передаваемый от клиента к серверу, возможные значения кодов этого поля приведены ниже.

Код	Описание
0x1111	Запрос на выделение слота
0x2222	Запрос к файловому серверу
0x3333	Ответ файл-сервера

Код	Описание
0x5555	Запрос на освобождение слота
0x7777	Пересылка в пакетном режиме
0x9999	Подтверждение приёма

Поле порядковый номер используется для отслеживания последовательности связи между клиентом и сервером. Клиент записывает в это поле код, равный номеру по порядку плюс единица. В полях номера канала записан номер, присвоенный клиенту при его регистрации сервером. Поле номер задачи идентифицирует каждую из задач, сделавших запрос. Сервер следит за выполнением задачи и освобождает ресурсы при завершении выполнения. Номер задачи равный нулю говорит серверу, что все задания окончены. Старшая часть номера канала используется лишь при наличии более чем 1000 пользователей, в остальных вариантах это субполе содержит нуль. Сервер в своем отклике сообщает клиенту результаты выполнения его запроса. Отклик, также как и запрос, вкладывается в IPX/SPX-пакет. Формат пакета-отклика:

Биты	Значение
0-15	Тип запроса
16-23	Номер по порядку
24-31	Младшая часть номера канала
32-39	Номер задачи
40-47	Старшая часть номера канала
48-55	Код завершения
56-63	Статус соединения

Нулевое значение кода завершения показывает, что запрос был обработан без ошибок. Любое другое значение говорит об ошибке при обработке запроса.

## 7 Многопроцессорные вычислительные комплексы (МПВК) с общей шиной

Существует три типа структурной организации МПВК: с общей шиной; с перекрестной коммутацией; с многоходовыми ОЗУ.

В комплексах с общей шиной проблема связей всех устройств между собой решается крайне просто: все они соединяются общей шиной, выполненной в виде совокупности проводов или кабелей, по которым передаются информация, адреса и сигналы управления (рис. 7.1). Интерфейс является односвязным, т. е. обмен информацией в любой момент времени может происходить только между двумя устройствами. Если потребность в обмене существует более чем у двух устройств, то возникает конфликтная ситуация, которая разрешается с помощью системы приоритетов и организации очередей в соответствии с этим. Обычно функции арбитра выполняет либо процессор, либо специальное устройство, которое регистрирует все обращения к общей шине и распределяет шину во времени между всеми устройствами комплекса.

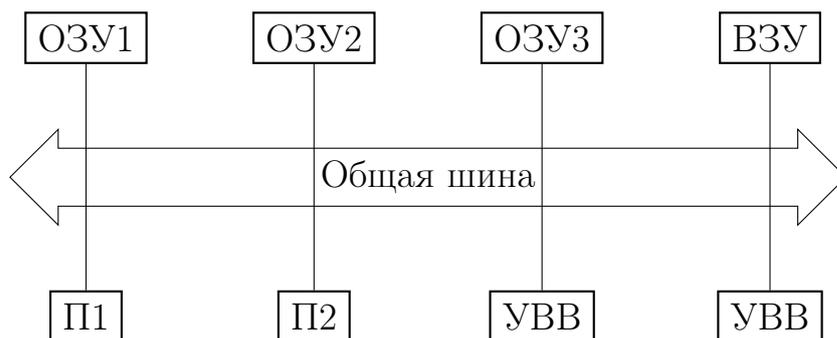


Рис. 7.1. МПВК с общей шиной

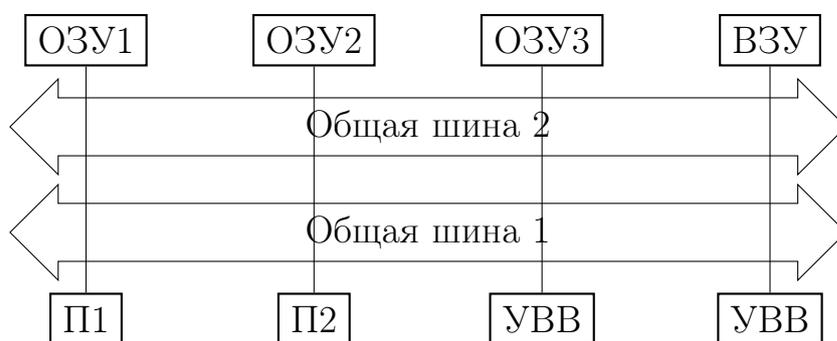


Рис. 7.2. МПВК с общей шиной

Несомненные достоинства структуры с общей шиной — простота, в том числе изменения комплекса, добавления или изъятия отдельных устройств, а также доступность модулей ОЗУ для всех остальных устройств. Следствием всего этого является достаточно низкая стоимость комплекса.

Вместе с тем комплексы с общей шиной не лишены определенных недостатков. Первый — невысокое быстродействие, так как одновременный обмен информацией возможен между двумя устройствами, не более. По этой причине в комплексах с общей шиной число процессоров не превосходит двух-четырех. Этот недостаток может быть несколько компенсирован путем использования общей шины с высоким быстродействием, большим, чем быстродействие входящих в комплекс устройств. Однако этот путь приводит к усложнению и удорожанию комплекса. Вторым недостатком МПВК с общей шиной является относительно низкая надежность системы из-за наличия общего элемента — шины. Надо иметь в виду, что надежность общей шины определяется не только надежностью проводов и кабелей (их собственная надежность достаточно высока), но и надежностью всех соединений, входных и выходных цепей устройства. Отказ хотя бы одного из элементов приводит к отказу всего комплекса. Этот недостаток можно компенсировать за счет введения резервной шины (рис. 7.2). Хотя это несколько усложняет комплекс, однако надежность его существенно возрастает. Если же резервную шину сделать активной, т. е. работающей одновременно с основной, то можно не только повысить надежность, но и увеличить производительность комплекса за счет того, что обмен информацией может осуществляться одновременно между двумя парами устройств.

## 8 Принципы построения и структуры ассоциативных ВС

К числу систем класса ОКМД относятся ассоциативные системы. Эти системы, как и матричные, характеризуются большим числом операционных устройств, способных одновременно, по командам одного управляющего устройства вести обработку нескольких потоков данных. Но эти системы существенно отличаются от матричных способами формирования потоков данных. В матричных системах данные поступают на обработку от общих или отдельных запоминающих устройств с адресной выработкой информации либо непосредственно от устройств – источников данных. В ассоциативных системах информация на обработку поступает от ассоциативных запоминающих устройств (АЗУ), характеризующихся тем, что информация из них выбирается не по определенному адресу, а по ее содержанию.

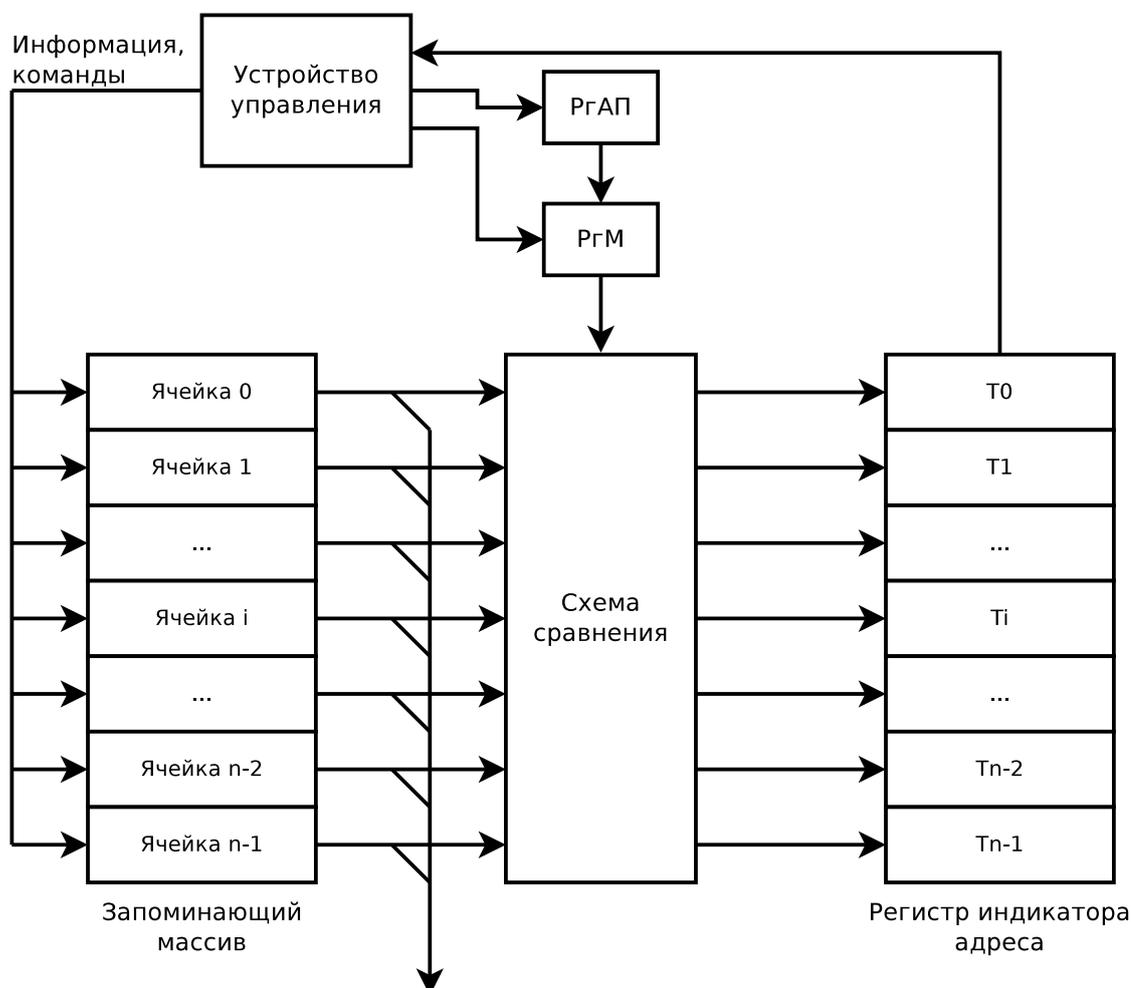


Рис. 8.1. Ассоциативное запоминающее устройство

Принцип работы АЗУ поясняет схема, представленная на рис. 8.1. Запоминающий массив, как и в адресных ЗУ, разделен на  $m$ -разрядные ячейки, число которых  $n$ . Практически для любого типа АЗУ характерно наличие

следующих элементов: запоминающего массива; регистра ассоциативных признаков (РГАП); регистра маски (РГМ); регистра индикаторов адреса со схемами сравнения на входе. В АЗУ могут быть и другие элементы, наличие и функции которых определяются способом использования АЗУ.

Выборка информации из АЗУ происходит следующим образом. В РГАП из устройства управления передается код признака искомой информации (иногда его называют компарандом). Код может иметь произвольное число разрядов — от 1 до  $m$ . Если код признаков используется полностью, то он без изменения поступает на схему сравнения, если же необходимо использовать только часть кода, тогда ненужные разряды маскируются с помощью РГМ. Перед началом поиска информации в АЗУ все разряды регистра индикаторов адреса устанавливаются в состояние 1. После этого производится опрос первого разряда всех ячеек ЗМ и содержимое сравнивается с первым разрядом РГАП. Если содержимое первого разряда  $i$ -й ячейки не совпадает с содержимым первого разряда РГАП, то соответствующий этой ячейке разряд регистра индикаторов адреса  $T_i$  сбрасывается в состояние 0, если совпадает, — на  $T_i$  остается 1. Затем эта операция повторяется со вторым, третьим и последующими разрядами до тех пор, пока не будет произведено сравнение со всеми разрядами РГАП. После поразрядного опроса и сравнения в состоянии 1 останутся те разряды регистра индикаторов адреса, которые соответствуют ячейкам, содержащим информацию, совпадающую с записанной в РГАП. Эта информация может быть считана в той последовательности, которая определяется устройством управления.

Время поиска информации в ЗМ по ассоциативному признаку зависит только от числа разрядов признака и от скорости опроса разрядов, но совершенно не зависит от числа ячеек ЗМ. Этим и определяется главное преимущество АЗУ перед адресными ЗУ: в адресных ЗУ при операции поиска необходим перебор всех ячеек запоминающего массива.

Запись новой информации в ЗМ производится без указания номера ячейки. Обычно один из разрядов каждой ячейки используется для указания ее занятости, т.е. если ячейка свободна для записи, то в этом разряде записан 0, а если занята, — 1. Тогда при записи в АЗУ новой информации устанавливается признак 0 в соответствующем разряде РГАП и определяются все ячейки ЗМ, которые свободны для записи. В одну из них устройство управления помещает новую информацию.

## 9 Литература

1. Ларионов А.М., Майоров С.А., Новиков Г.И., Вычислительные комплексы, системы и сети: Учебник для вузов — Л.: Энергоатомиздат, 1987 — 285 с.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы.
3. Компьютерные сети. 4-е изд. / Э. Таненбаум. — СПб.: Питер, 2003. — 992 с.