

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кафедра «Информационная безопасность»

**АППАРАТНЫЕ СРЕДСТВА
ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ
ДЛЯ ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Учебно-методическое пособие
для обучающихся по направлению
10.03.01 «Информационная безопасность»
очной и очно-заочной формы обучения

Севастополь
СевГУ
2022

УДК 004.056(075.8)
ББК 16.8я73
А76

Рецензент:
Ю.Ю. Гончаренко – д-р техн. наук, профессор,
профессор кафедры «Информационная безопасность»

Составитель: Е.А. Контылева

А76 Аппаратные средства вычислительной техники для обеспечения информационной безопасности: учебно-методическое пособие для обучающихся по направлению 10.03.01 «Информационная безопасность» очной и очно-заочной формы обучения / Севастопольский государственный университет, Институт радиоэлектроники и информационной безопасности, кафедра «Информационная безопасность» : сост. Е.А. Контылева. – Севастополь: СевГУ, 2022. – 63 с. – Текст: электронный.

Целью пособия является оказание помощи студентам очной и очно-заочной формы обучения в подготовке к практическим занятиям и написанию отчета по дисциплине «Аппаратные средства вычислительной техники для обеспечения информационной безопасности».

УДК 004.056(075.8)
ББК 16.8я73

Рассмотрено и утверждено на заседании кафедры «Информационная безопасность», протокол № 8 от 18 февраля 2022 г.

© ФГАОУ ВО «Севастопольский
государственный университет», 2022

СОДЕРЖАНИЕ

Введение	4
1. Аппаратные средства защиты информации	5
2. Характеристики основных параметров компьютера	10
3. Логические основы ЭВМ	13
4. Классификация основных элементов компьютера	16
5. Назначение и принцип работы элементов ЭВМ	26
6. Общая структура микропроцессора	33
7. Запоминающие устройства: классификация, принцип работы, основные характеристики	41
8. Постоянное энергонезависимое запоминающее устройство ROM	51
9. Виды накопителей информации	58
Литература	63

ВВЕДЕНИЕ

Большинство современных систем автоматики, вычислительной техники, системы передачи и обработки информации выполняются на цифровых устройствах. Поэтому знание принципов применения цифровых устройств и построения на их основе систем различного назначения имеет актуальное значение и большую практическую ценность, как в инженерной деятельности, так и при исследованиях методологического характера.

Дисциплина «Аппаратные средства вычислительной техники обеспечения информационной безопасности» относится к базовой части профессионального цикла. Целью дисциплины является формирование основополагающих знаний, умений, навыков и компетенций у студентов по аппаратным средствам вычислительной техники.

Основные задачи методических указаний к практическим занятиям по дисциплине «Аппаратные средства вычислительной техники обеспечения информационной безопасности» следующие:

- изучение характеристик основных параметров компьютера;
- изучение логических основ вычислительной техники;
- изучить классификацию, назначение и принцип работы основных элементов компьютера.
- изучение запоминающих устройств;
- ознакомление с видами накопителей информации.

Студенту необходимо знать математические методы для решения задач обеспечения защиты информации, чтобы владеть не только навыками применения данных методов, но и уметь их применять для решения задач по обеспечению защиты информации.

Практические работы проводятся на персональном компьютере с использованием метода беседы.

Защита отчета осуществляется на проводимом занятии.

1 АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

В последние десятилетия в связи с развитием, усложнением и появлением новых средств автоматизации процессов обработки информации появляются новые виды уязвимостей в защите информации. Основными факторами, приводящие к увеличению рисков, являются:

- повальное увеличение обрабатываемой с помощью ВС информации;
- собрание в базах данных информации не ограниченной узкими областями применения;
- расширение круга пользователей, имеющих доступ к хранимой информации;
- усложнение алгоритмов работы ВС, хранящих и обрабатывающих информацию, в т.ч. распределённых на больших территориях ВС.

В этих условиях возникает два общих класса уязвимостей информации: информация может быть искажена в силу несовершенства программного обеспечения ВС и ошибок в нём, а также, помимо этого, возможно несанкционированное получение той или иной хранимой информации. Основными способами несанкционированного получения информации являются прямое получение доступа к носителям информации, её копирование и подключение к каналам передачи информации, как с использованием законной аппаратуры, так и с применением специально изготовленных средств.

В целом аппаратные либо технические СЗИ это различные устройства, которые аппаратными средствами решают задачи защиты информации. К ним можно отнести как и классические организационные средства, такие как различные меры противодействия проникновению на объекты, так и специализированные средства противодействия конкретным способам получения доступа к информации в процессе хранения либо передачи.

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

- специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных;
- устройства для шифрования информации (криптографические методы).

Для защиты периметра информационной системы создаются:

- системы охранной и пожарной сигнализации;
- системы цифрового видеонаблюдения;
- системы контроля и управления доступом.

Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:

- использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;
- установкой на линиях связи высокочастотных фильтров;
- построение экранированных помещений («капсул»);
- использование экранированного оборудования;
- установка активных систем шумления;
- создание контролируемых зон.

Задачи аппаратного обеспечения защиты информации Использование аппаратных средств защиты информации позволяет решать следующие задачи:

- проведение специальных исследований технических средств на наличие возможных каналов утечки информации;
- выявление каналов утечки информации на разных объектах и в помещениях;
- локализация каналов утечки информации;
- поиск и обнаружение средств промышленного шпионажа;
- противодействие НСД к источникам конфиденциальной информации и другим действиям.

По назначению аппаратные средства классифицируют на средства обнаружения, средства поиска и детальных измерений, средства активного и пассивного противодействия. При этом по техническим возможностям средства защиты информации могут быть общего назначения, рассчитанные на использование непрофессионалами с целью получения общих оценок, и профессиональные комплексы, позволяющие проводить тщательный поиск, обнаружение и измерения все характеристик средств промышленного шпионажа.

Поисковую аппаратуру можно подразделить на аппаратуру поиска средств съема информации и исследования каналов ее утечки. Аппаратура первого типа направлена на поиск и локализацию уже внедренных злоумышленниками средств НСД. Аппаратура второго типа предназначена для выявления каналов утечки информации. Определяющими для такого рода систем являются оперативность исследования и надежность полученных результатов. Профессиональная поисковая аппаратура, как правило, очень дорога, и требует высокой квалификации работающего с ней специалиста. В связи с этим, позволить ее могут себе организации, постоянно проводящие соответствующие обследования. Так что если Вам нужно провести полноценное обследование – прямая дорога к ним. Конечно, это не значит, что нужно отказаться от использования средств поиска самостоятельно. Но доступные поисковые средства достаточно просты и позволяют проводить профилактические мероприятия в промежутке между серьезными поисковыми обследованиями.

Виды аппаратных средств защиты информации.

Для обеспечения сохранности данных разработаны специализированные аппаратные решения, способные обеспечивать как быстрый доступ к данным, так и их надёжное компактное хранение. Базово их можно классифицировать на следующие виды.

1. Специализированная сеть хранения SAN (Storage Area Network) обеспечивает данным гарантированную полосу пропускания, исключает возникновение единой точки отказа системы, допускает практически неограниченное масштабирование как со стороны серверов, так и со стороны информационных ресурсов.

2. Для реализации сетей хранения наряду с популярной технологией Fiber Channel в последнее время все чаще используются устройства iSCSI. Дисковые хранилища отличаются высочайшей скоростью доступа к данным за счет распределения запросов чтения/записи между несколькими дисковыми накопителями.

3. Ленточные накопители (стримеры, автозагрузчики и библиотеки) попрежнему считаются самым экономичным и популярным решением создания резервных копий. Они изначально созданы для хранения данных, предоставляют практически неограниченную емкость за счет добавления ленточных картриджей, обеспечивают высокую надежность, имеют низкую стоимость хранения, позволяют организовать ротацию любой сложности и глубины, архивацию данных, эвакуацию носителей в защищенное место за пределами основного офиса.

Помимо рассмотренных технологий следует также упомянуть обеспечение физической защиты данных (разграничение и контроль доступа в помещения, видеонаблюдение, охранная и пожарная сигнализация), организация бесперебойного электроснабжения оборудования.

Рассмотрим примеры аппаратных средств.

1) Электронный ключ eToken - персональное средство авторизации, аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП).

2) Смарт-карты доступа – аппаратный декодер, применяемый для генерирования ключей декодирования на основе публично доступных данных. Чип смарт-карты (либо иного аппаратного форм-фактора) содержит в себе специализированную микропрограмму и микроаппаратное обеспечение, задачей которого является вычисление ключа декодирования зашифрованных данных на основе предоставляемых в открытый доступ зашифрованных версий ключа. Область применения не ограничена, на сегодняшний день применяется в основном для организации условного доступа к потоковым данным, таким как системы цифрового телевидения.

3) Шифрование - обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.

4) Специализированная сеть хранения SAN (Storage Area Network) обеспечивает данным гарантированную полосу пропускания, исключает

возникновение единой точки отказа системы, допускает практически неограниченное масштабирование как со стороны серверов, так и со стороны информационных ресурсов.

5) Для реализации сетей хранения наряду с популярной технологией Fiber Channel в последнее время все чаще используются устройства iSCSI. Дисковые хранилища отличаются высочайшей скоростью доступа к данным за счет распределения запросов чтения/записи между несколькими дисковыми накопителями.

6) Ленточные накопители (стримеры, автозагрузчики и библиотеки) попрежнему считаются самым экономичным и популярным решением создания резервных копий. Они изначально созданы для хранения данных, предоставляют практически неограниченную емкость за счет добавления ленточных картриджей, обеспечивают высокую надежность, имеют низкую стоимость хранения, позволяют организовать ротацию любой сложности и глубины, архивацию данных, эвакуацию носителей в защищенное место за пределами основного офиса.

7) Криптопровайдер – это программное обеспечение, то есть посредник, который позволяет операционной системе выполнять шифровальные функции. Еще проще можно сказать, что это специальная программа для работы с ЭП, обеспечивающая соблюдение стандартов (ГОСТ).

8) Средства электронной цифровой подписи — аппаратные программные средства, обеспечивающие реализацию хотя бы одной из следующих функций — создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

9) Ключевые носители - использование технологий ЭЦП для сотрудников подразумевает наличие надежного места для хранения закрытой части ЭЦП, а именно персональных носителей ключевой информации. Они в отличие от жесткого диска или флэшки пользователя обеспечивают защиту от несанкционированного считывания ЭЦП. Самые популярные из них – Рутокен (компания «Актив»), JaCarta от «Алладин РД» и Esmart USB от компании ISBC.

10) VPN – технология, которая позволяет подключаться к корпоративной сети компании через интернет, но по принципу доверенной частной сети по зашифрованному VPN каналу связи. Комплексное решение в области VPN технологий предлагает компания ИнфоТеКС. Ее ViPNet Client - это программный комплекс, выполняющий на рабочем месте пользователя или сервере с прикладным ПО функции VPN-клиента, персонального сетевого экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования.

11) Системы защищённой электронной почты могут быть реализованы как: самостоятельные системы – Дипост, Диопост от компании Фактор-ТС; Почтовый клиент Диопост предназначен для обмена зашифрованными и подписанными письмами по протоколам SMTP, POP3, TELNET. в составе пакета для организации защищенной сети, например ViPNet «Деловая почта».

12) Аппаратные криптомаршрутизаторы - Криптографический шлюз (криптошлюз, криптомаршрутизатор, VPN-шлюз) – это программноаппаратный комплекс для криптографической защиты трафика, передаваемого по открытым каналам связи, путем шифрования пакетов по различным протоколам.

13) Антивирусные программы. Современные антивирусные средства кроме своих «основных обязанностей» умеют управлять доступом к съемным устройствам (запрет, белый список), сообщать об уязвимостях в установленном ПО, производить удаленную установку и удаление программ, шифровать данные на жестких дисках и съемных устройствах.

14) Межсетевой экран - программа, контролирующая и фильтрующая на основе заданных правил входящий и исходящий сетевой трафик – пропускать его или нет. Помимо этого, сетевой экран используется для защиты сети или рабочих станций от несанкционированного проникновения через уязвимости программного обеспечения или протоколов сети. Таким образом межсетевой экран – это барьер между внутренней сетью компании, содержащей конфиденциальные или персональные данные и глобальными информационными сетями.

- Прокси-сервер – это компьютер, выполняющий роль посредника между пользователем и запрашиваемым адресом в сети интернет.

Распространенные варианты использования прокси в компании: 1) для повышения безопасности сети - шифрования запросов и скрывание адреса клиента, так как конечный сервер будет знать только адрес прокси ; 2) для увеличения производительности сети и экономии трафика за счет кэширования (запоминания на прокси) просмотренной информации и фильтрации трафика, например, блокировки рекламных блоков; 3) для блокировки вредоносных и развлекательных сайтов и рекламы; 4) для контроля использования сетевого канала; 5) для мониторинга и регистрации веб-запросов пользователей.

2 ХАРАКТЕРИСТИКИ ОСНОВНЫХ ПАРАМЕТРОВ КОМПЬЮТЕРА

Система счисления - совокупность приёмов и правил изображения чисел цифровыми знаками. Системы счисления делятся на непозиционные и позиционные

Непозиционная система счисления — система, в которой, значение символа не зависит от его положения в числе. Непозиционные системы счисления возникли раньше позиционных систем. Они использовались в древности римлянами, египтянами, славянами и другими народами. Примером непозиционной системы счисления, дошедшей до наших дней, служит римская система счисления.

Цифры в римской системе обозначаются различными знаками: 1—I; 3—III; 5—V; 10—X; 50—L; 100—C; 500—D; 1000—M. Для записи промежуточных значений существует правило: каждый меньший знак, поставленный справа от большего, прибавляется к его значению, а слева — вычитается из него. Так, IV обозначает 4, VI—6, LX— 60, XC—90 и т.д. Основной недостаток непозиционных систем — большое число различных знаков и сложность выполнения арифметических операций.

Позиционная система счисления — система, в которой значение символа зависит от его места в ряду цифр, изображающих число. Например, в числе 7382 первая цифра слева означает количество тысяч, вторая — количество сотен, третья — количество десятков и четвёртая количество единиц. Позиционные системы счисления (ПСС) более удобны для вычислительных операций, поэтому они получили более широкое распространение. Позиционная система счисления характеризуется основанием.

Основание (базис) ПСС - количество знаков или символов, используемых в разрядах для изображения числа в данной системе счисления.

Таблица 1 - Значения первых 16 целых чисел в различных СС

10	2	8	16	10	2	8	16
0	0	0	0	8	1000	10	8
1	1	1	1	9	1001	11	9
2	10	2	2	10	1010	12	A
3	11	3	3	11	1011	13	B
4	100	4	4	12	1100	14	C
5	101	5	5	13	1101	15	D
6	110	6	6	14	1110	16	E
7	111	7	7	15	1111	17	F

Двоичная система счисления. Правила двоичной арифметики.

В двоичной системе счисления для записи чисел используется две цифры 0 и 1. Основание системы $q = 2$ записывается как $10_2 = (1 \cdot 2^1 + 0 \cdot 2^0)_{10}$.

В данной СС любое число может быть представлено последовательностью двоичных цифр. Эта запись соответствует сумме степеней цифры 2, взятых с указанными в ней коэффициентами. Например, двоичное число $(0101101)_2 = 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 173_{10}$.

Арифметические операции над двоичными числами отличаются простотой и легкостью технического выполнения.

Правила двоичной арифметики:

Сложение:

$$0+0=0;$$

$$1+0=1;$$

$$0+1=1;$$

$$1+1=10 \text{ (происходит перенос единицы в старший разряд);}$$

Вычитание:

$$0-0=0;$$

$$1-1=0;$$

$$1-0=1;$$

$$10-1=1 \text{ (происходит заем единицы в старшем разряде);}$$

Умножение:

$$0 \times 0 = 0;$$

$$1 \times 0 = 0;$$

$$0 \times 1 = 0;$$

$$1 \times 1 = 1;$$

Двоичная система счисления является основной для использования в ЭВМ, удобной из-за простоты выполнения арифметических операций над двоичными числами. С точки зрения затрат оборудования на создание ЭВМ эта система уступает только троичной системе счисления.

В двоично-кодированных системах счисления, имеющих основания q , отличные от 2 ($q > 2$), каждая цифра числа представляется в двоичной системе счисления. Наибольшее применение в ЭВМ получили шестнадцатеричная система счисления и десятичная двоично-кодированная система счисления.

Восьмеричная и шестнадцатеричная системы счисления.

Восьмеричная и шестнадцатеричная системы счисления являются вспомогательными системами при подготовке задачи к решению. Удобство их использования состоит в том, что числа соответственно в 3 и 4 раза короче двоичной системы, а перевод в двоичную систему счисления и наоборот несложен и выполняется простым механическим способом.

Пример 1:

Число $137,45_8$ перевести в двоичную систему счисления. Перевод осуществляется заменой каждой восьмеричной цифры трехзначным двоичным числом (триадой):

$$137,45_8 = 001011111,100101_2.$$

И наоборот, заменой каждой триады слева и справа от запятой эквивалентным значением восьмеричной цифры образуется восьмеричное число.

Если в крайней слева или крайней справа триаде окажется меньше трех двоичных чисел, то эти тройки дополняют нулями.

Пример 2:

Число $5F,94_{16}$ перевести в двоичную систему счисления. Перевод осуществляется заменой каждой шестнадцатеричной цифры четырехзначным двоичным числом (тетрадой):

$$5F,94_{16} = 01011111,10010100_2.$$

В десятичной двоично-кодированной системе счисления, часто называемой двоично-десятичной системой, используются десятичные числа. В ней каждую цифру десятичного числа (от 0 до 9) заменяют тетрадой.

Пример 3:

Число $273,59_{10}$ перевести в двоично-десятичную систему счисления. Перевод осуществим следующим образом:

$$273,59_{10} = 001001110011,01011001_{2-10}$$

Двоично-десятичную запись числа используют непосредственно или как промежуточную форму записи между обычной десятичной его записью и машинной двоичной. Вычислительная машина сама по специальной программе переводит двоично-десятичные числа в двоичные и обратно.

3 ЛОГИЧЕСКИЕ ОСНОВЫ ЭВМ

Алгебра логики возникла в середине XIX века в трудах английского математика Джорджа Буля. Ее создание представляло собой попытку решать традиционные логические задачи алгебраическими методами.

Совокупность логических переменных $x_1, \dots, x_n$ называется **набором переменных**.

Логической функцией (функцией алгебры логики) от набора логических переменных $F(x_1, \dots, x_n)$ называется функция, которая может принимать только два значения: истина или ложь (1 или 0). Любая логическая функция может быть задана с помощью таблицы истинности, в левой части которой записываются возможные наборы значений аргументов, а в правой - соответствующие им значения функции.

Связь между алгеброй логики и двоичным кодированием

Математический аппарат алгебры логики очень удобен для описания того, как функционируют аппаратные средства компьютера, поскольку основной системой счисления в компьютере является двоичная, в которой используются цифры 1 и 0, а значений логических переменных тоже два: “1” и “0”.

Из этого следует два вывода:

1. Одни и те же устройства компьютера могут применяться для обработки и хранения как числовой информации, представленной в двоичной системе счисления, так и логических переменных;

2. На этапе конструирования аппаратных средств алгебра логики позволяет значительно упростить логические функции, описывающие функционирование схем компьютера, и, следовательно, уменьшить число элементарных логических элементов, из десятков тысяч которых состоят основные узлы компьютера.

Запись данных и команд в памяти компьютера и в регистрах процессора.

Данные и команды представляются в виде двоичных последовательностей различной структуры и длины. Существуют различные физические способы кодирования двоичной информации. В электронных устройствах компьютера двоичные единицы чаще всего кодируются более высоким уровнем напряжения, чем двоичные нули (или наоборот)/

Логический элемент компьютера - это часть электронной логической схемы, которая реализует элементарную логическую функцию.

Логическими элементами компьютеров являются электронные схемы И, ИЛИ, НЕ, И—НЕ, ИЛИ—НЕ и другие (называемые также **вентиллями**), а также **триггер**.

С помощью этих схем можно реализовать любую логическую функцию, описывающую работу устройств компьютера. Обычно у вентилей бывает от двух до восьми входов и один или два выхода.

Чтобы представить два логических состояния — “1” и “0” в вентиллях, соответствующие им входные и выходные сигналы имеют один из двух

установленных уровней напряжения. Например, +5 вольт и 0 вольт. Высокий уровень обычно соответствует значению “истина” (“1”), а низкий — значению “ложь” (“0”).

Каждый логический элемент имеет свое условное обозначение, которое выражает его логическую функцию, но не указывает на то, какая именно электронная схема в нем реализована. Это упрощает запись и понимание сложных логических схем.

Работу логических элементов описывают с помощью таблиц истинности.

Таблица истинности - это табличное представление логической схемы (операции), в котором перечислены все возможные сочетания значений истинности входных сигналов (операндов) вместе со значением истинности выходного сигнала (результата операции) для каждого из этих сочетаний.

Что такое схемы И, ИЛИ, НЕ, И-НЕ, ИЛИ-НЕ?

Схема И реализует конъюнкцию двух или более логических значений.

Таблица 2 –Таблица истинности схемы И

x	y	$x \& y$
0	0	0
0	1	0
1	0	0
1	1	1

Единица на выходе схемы И будет тогда и только тогда, когда на всех входах будут единицы. Когда хотя бы на одном входе будет ноль, на выходе также будет ноль.

Схема ИЛИ реализует дизъюнкцию двух или более логических значений. Когда хотя бы на одном входе схемы ИЛИ будет единица, на её выходе также будет единица.

Таблица 3 - Таблица истинности схемы ИЛИ

x	y	$x \vee y$
0	0	0
0	1	1
1	0	1
1	1	1

Схема НЕ (инвертор) реализует операцию отрицания.

Таблица 4 - Таблица истинности схемы НЕ

x	$\bar{x}$
0	1
1	0

Схема И—НЕ состоит из элемента И и инвертора и осуществляет отрицание результата схемы И.

Таблица5 - Таблица истинности схемы И—НЕ

x	y	$\overline{x \cdot y}$
0	0	1
0	1	1
1	0	1
1	1	0

Схема ИЛИ—НЕ состоит из элемента ИЛИ и инвертора и осуществляет отрицание результата схемы ИЛИ.

Таблица 6 - Таблица истинности схемы ИЛИ—НЕ

x	y	$\overline{x \vee y}$
0	0	1
0	1	0
1	0	0
1	1	0

4 КЛАССИФИКАЦИЯ ОСНОВНЫХ ЭЛЕМЕНТОВ КОМПЬЮТЕРА

В настоящее время в базовой конфигурации рассматривают четыре устройства:

1. Системный блок представляет собой основной узел, внутри которого установлены наиболее важные компоненты. Устройства, находящиеся внутри системного блока, называют внутренними, а устройства, подключаемые к нему снаружи, — внешними. Внешние дополнительные устройства, предназначенные для ввода, вывода и длительного хранения данных, также называют периферийными.

2. Монитор — устройство визуального представления данных. Это не единственно возможное, но главное устройство вывода. Его основными потребительскими параметрами являются: тип, размер и шаг маски экрана, максимальная частота регенерации изображения, класс защиты.

Сейчас наиболее распространены мониторы двух основных типов на основе электронно-лучевой трубки (ЭЛТ) и плоские жидкокристаллические (ЖК). ЭЛТ-мониторы обеспечивают лучшее качество изображения, но в пользу жидкокристаллических мониторов говорит их компактность, небольшой вес, идеально плоская поверхность экрана.

Размер монитора измеряется между противоположными углами видимой части экрана по диагонали. Единица измерения — дюймы. Стандартные размеры: 14"; 15"; 17"; 19"; 20"; 21".

Шаг маски. Изображение на экране ЭЛТ-монитора получается в результате облучения люминофорного покрытия остронаправленным пучком электронов, разогнанных в вакуумной колбе. Для получения цветного изображения люминофорное покрытие имеет точки или полосы трех типов, светящиеся красным, зеленым и синим цветом. Чтобы на экране все три луча сходились строго в одну точку и изображение было четким, перед люминофором ставят маску — панель с регулярно расположенными отверстиями или щелями. Часть мониторов оснащена маской из вертикальных проволочек, что усиливает яркость и насыщенность изображения. Чем меньше шаг между отверстиями или щелями (шаг маски), тем четче и точнее полученное изображение.

Шаг маски измеряют в долях миллиметра. В настоящее время наиболее распространены мониторы с шагом маски 0,24-0,26 мм.

На экране жидкокристаллического монитора изображение образуется в результате прохождения белого света лампы подсветки через ячейки, прозрачность которых зависит от приложенного напряжения. Элементарная триада состоит из трех ячеек зеленого, красного и синего цвета и соответствует одному пикселу экрана. Размер монитора по диагонали и разрешение экрана однозначно определяет размер такой триады и, тем самым, зернистость изображения.

Частота регенерации (обновления) изображения показывает, сколько раз в течение секунды монитор может полностью сменить изображение

(поэтому ее также называют частотой кадров). Этот параметр зависит не только от монитора, но и от свойств и настроек видеоадаптера хотя предельные возможности определяет все-таки монитор. Частоту регенерации изображения измеряют в герцах (Гц). Чем она выше, тем четче и устойчивее изображение, тем меньше утомление глаз, тем больше времени можно работать с компьютером непрерывно. При частоте регенерации порядка 60 Гц мелкое мерцание изображения может быть заметно невооруженным глазом. Сегодня такое значение считается недопустимым. Для ЭЛТ-мониторов минимальным считают значение 75 Гц, нормативным — 85 Гц и комфортным — 100 Гц и более. У жидкокристаллических мониторов изображение более инерционно, так что мерцание подавляется автоматически. Для них частота обновления в 75 Гц уже считается комфортной.

Класс защиты монитора определяется стандартом, которому соответствует монитор с точки зрения требований техники безопасности.

3. Клавиатура — клавишное устройство управления персональным компьютером. Служит для ввода алфавитно-цифровых (знаковых) данных, а также команд управления. Комбинация монитора и клавиатуры обеспечивает простейший интерфейс пользователя. С помощью клавиатуры управляют компьютерной системой, а с помощью монитора получают от нее отклик.

Клавиатура относится к стандартным средствам персонального компьютера. Ее основные функции не нуждаются в поддержке специальными системными программами (драйверами). Необходимое программное обеспечение для начала работы с компьютером уже имеется в микросхеме ПЗУ в составе базовой системы ввода-вывода (BIOS), и потому компьютер реагирует на нажатия клавиш сразу после включения.

4. Мышь — устройство управления манипуляторного типа. Перемещение мыши по плоской поверхности синхронизировано с перемещением графического объекта (указателя мыши) на экране монитора.

В отличие от рассмотренной ранее клавиатуры мышь не является стандартным органом управления, и персональный компьютер не имеет для нее выделенного порта. Она нуждается в поддержке специальной системной программы — драйвера мыши. Драйвер устанавливается либо при первом подключении мыши, либо при установке операционной системы компьютера.

К числу регулируемых параметров мыши относятся: чувствительность (выражает величину перемещения указателя на экране при заданном линейном перемещении мыши), функции левой и правой кнопок, а также чувствительность к двойному нажатию (максимальный интервал времени, при котором два щелчка кнопкой мыши расцениваются как один двойной щелчок).

Комбинация монитора и мыши обеспечивает наиболее современный тип интерфейса пользователя, который называется графическим

Внутренние устройства системного блока.

1. Материнская плата — основная плата персонального компьютера. На ней размещаются:

- процессор — основная микросхема, выполняющая большинство математических и логических операций;
- микропроцессорный комплект (чипсет) — набор микросхем, управляющих работой внутренних устройств компьютера и определяющих основные функциональные возможности материнской платы;
- шины — наборы проводников, по которым происходит обмен сигналами между внутренними устройствами компьютера;
- оперативная память (оперативное запоминающее устройство, ОЗУ) — набор микросхем, предназначенных для временного хранения данных, когда компьютер включен;
- ПЗУ (постоянное запоминающее устройство) — микросхема, предназначенная для длительного хранения данных, в том числе и когда компьютер выключен;
- разъемы для подключения дополнительных устройств (слоты).

2. Жесткий диск — основное устройство для долговременного хранения больших объемов данных и программ.

Управление работой жесткого диска выполняет специальное аппаратно-логическое устройство —

контроллер жесткого диска

К основным параметрам жестких дисков относятся:

- емкость
- производительность.

3. Дисковод гибких дисков. В новейших компьютерах происходит постепенный отказ и от этого типа носителей, которые вытесняются записывающими дисководами CD-RW.

4. Дисковод компакт-дисков CD-ROM (*Compact Disc Read-Only Memory*) переводится на русский язык как *постоянное запоминающее устройство на основе компакт-диска*. Принцип действия этого устройства состоит в считывании числовых данных с помощью лазерного луча, отражающегося от поверхности диска. Цифровая запись на компакт-диске отличается от записи на магнитных дисках очень высокой плотностью, и стандартный компакт-диск может хранить примерно 650 Мбайт данных.

Основным недостатком стандартных дисководов CD-ROM является невозможность записи данных (предназначен только для многократного чтения).

5. Видеокарта (видеоадаптер). Совместно с монитором *видеокарта* образует *видеоподсистему* персонального компьютера.

Физически видеоадаптер выполнен в виде отдельной *дочерней платы*, которая вставляется в один из слотов материнской платы и называется *видеокартой*. Видеоадаптер взял на себя функции *видеоконтроллера, видеопроцессора и видеопамати*.

За время существования персональных компьютеров сменилось несколько стандартов видеоадаптеров: MDA (монохромный); CGA (4

цвета); EGA (16 цветов); VGA (256 цветов). В настоящее время применяются видеоадаптеры SVGA, обеспечивающие по выбору воспроизведение до 16,7 миллионов цветов с возможностью произвольного выбора разрешения экрана из стандартного ряда значений (640x480, 800x600, 1024x768, 1152x864; 1280x1024 точек и далее).

Параметры видеоподсистемы:

- Разрешение экрана (является одним из важнейших). Для каждого размера монитора существует свое оптимальное разрешение экрана, которое должен обеспечивать видеоадаптер.

- Цветовое разрешение (глубина цвета) определяет количество различных оттенков, которые может принимать отдельная точка экрана.

- Видеоускорение — одно из свойств видеоадаптера, которое заключается в том, что часть операций по построению изображений может происходить без выполнения математических вычислений в основном процессоре компьютера, а чисто аппаратным путем — преобразованием данных в микросхемах видеоускорителя.

6. Звуковая карта. Качество звука, оцифрованного звуковой картой, определяется такими параметрами, как:

- частота дискретизации звука;
- глубина кодирования.

Важнейшим параметром кодирования звука является частота дискретизации звука, то есть количество преобразований аналогового звука в цифровую форму, выполняемых за одну секунду. При квантовании звука определяется номер подуровня квантования, в который попадает дискретное значение звукового давления. Количество бит, используемых для записи номеров подуровней, называется глубиной кодирования звука.

Чем больше частота дискретизации и глубина кодирования, тем выше качество звука и тем больше при воспроизведении он будет похож на оригинал.

Основным параметром звуковой карты является разрядность, определяющая количество битов, используемых при преобразовании сигналов из аналоговой в цифровую форму и наоборот. Чем выше разрядность, тем меньше погрешность, связанная с оцифровкой, тем выше качество звучания. Минимальным требованием сегодняшнего дня являются 16 разрядов, а наибольшее распространение имеют 32-разрядные и 64-разрядные устройства.

Системы, расположенные на материнской плате.

Оперативная память (RAM — *Random Access Memory*) — это массив кристаллических ячеек, способных хранить данные. Существует много различных типов оперативной памяти, но с точки зрения физического принципа действия различают:

- динамическую память (DRAM);
- статическую память (SRAM).

Ячейки динамической памяти (DRAM) можно представить в виде микроконденсаторов, способных накапливать заряд на своих обкладках. Это

наиболее распространенный и экономически доступный тип памяти. Недостатки этого типа связаны, во-первых, с тем, что как при заряде, так и при разряде конденсаторов неизбежны переходные процессы, то есть запись данных происходит сравнительно медленно. Второй важный недостаток связан с тем, что заряды ячеек имеют свойство рассеиваться в пространстве, причем весьма быстро. Если оперативную память постоянно не «подзаряжать», утрата данных происходит через несколько сотых долей секунды.

Для борьбы с этим явлением в компьютере происходит постоянная регенерация (освежение, подзарядка) ячеек оперативной памяти. Регенерация осуществляется несколько десятков раз в секунду и вызывает непроизводительный расход ресурсов вычислительной системы.

Ячейки статической памяти (SRAM) можно представить как электронные микросхемы — триггеры, состоящие из нескольких транзисторов. В триггере хранится не заряд, а состояние (включен/выключен), поэтому этот тип памяти обеспечивает более высокое быстродействие, хотя технологически он сложнее и, соответственно, дороже.

Микросхемы динамической памяти используют в качестве основной оперативной памяти компьютера. Микросхемы статической памяти используют в качестве вспомогательной памяти (так называемой *кэш-памяти*), предназначенной для оптимизации работы процессора.

Каждая ячейка памяти имеет свой адрес, который выражается числом. В большинстве современных процессоров предельный размер адреса обычно составляет 32 разряда, а это означает, что всего независимых адресов может быть 2^{32} . Одна адресуемая ячейка содержит один байт данных. Таким образом, в современных компьютерах возможна непосредственная адресация к полю памяти размером 2^{32} байт = 4 Гбайт. Однако это отнюдь не означает, что именно столько оперативной памяти непременно должно быть в компьютере. Предельный размер поля оперативной памяти, установленной в компьютере, определяется микропроцессорным комплектом (чипсетом) материнской платы и обычно не может превосходить нескольких Гбайт. Минимальный объем памяти определяется требованиями операционной системы и для современных компьютеров составляет 128 Мбайт.

Процессор — основная микросхема компьютера, в которой и производятся все вычисления. Конструктивно процессор состоит из ячеек, похожих на ячейки оперативной памяти, но в этих ячейках данные могут не только храниться, но и изменяться.

Внутренние ячейки процессора называют регистрами. Важно также отметить, что данные, попавшие в некоторые регистры, рассматриваются не как данные, а как команды, управляющие обработкой данных в других регистрах. Таким образом, управляя засылкой данных в разные регистры процессора, можно управлять обработкой данных. На этом и основано исполнение программ.

С остальными устройствами компьютера, и в первую очередь с оперативной памятью, процессор связан несколькими группами проводников, называемых **шинами**. Основных шин три:

Адресная шина. У процессоров семейства Pentium (а именно они наиболее распространены в персональных компьютерах) адресная шина 32-разрядная, то есть состоит из 32 параллельных проводников. В зависимости от того, есть напряжение на какой-то из линий или нет, говорят, что на этой линии выставлена единица или ноль.

Комбинация из 32 нулей и единиц образует 32-разрядный адрес, указывающий на одну из ячеек оперативной памяти. К ней и подключается процессор для копирования данных из ячейки в один из своих регистров.

Шина данных. По этой шине происходит копирование данных из оперативной памяти в регистры процессора и обратно. В современных персональных компьютерах шина данных, как правило, 64-разрядная, то есть состоит из 64 линий, по которым за один раз на обработку поступают сразу 8 байтов.

Шина команд. Для того чтобы процессор мог обрабатывать данные, ему нужны команды. Он должен знать, что следует сделать с теми байтами, которые хранятся в его регистрах. Эти команды поступают в процессор тоже из оперативной памяти, но не из тех областей, где хранятся массивы данных, а оттуда, где хранятся программы. Команды тоже представлены в виде байтов.

Система команд процессора.

Совокупность всех возможных команд, которые может выполнить процессор над данными, образует так называемую систему команд процессора. Процессоры, относящиеся к одному семейству, имеют одинаковые или близкие системы команд.

Процессоры, относящиеся к разным семействам, различаются по системе команд и невзаимозаменяемые.

Процессоры с расширенной (CISC-процессоры) и сокращенной системой команд (RISC- процессоры).

Персональные компьютеры платформы IBM PC ориентированы на использование CISC-процессоров.

Совместимость процессоров. Если два процессора имеют одинаковую систему команд, то они полностью совместимы на программном уровне. Это означает, что программа, написанная для одного процессора, может исполняться и другим процессором. Процессоры, имеющие разные системы команд, как правило, несовместимы или ограниченно совместимы на программном уровне.

Группы процессоров, имеющих ограниченную совместимость, рассматривают как *семейства процессоров*.

Основные параметры процессоров.

Основными параметрами процессоров являются:

- рабочее напряжение;
- разрядность;

- рабочая тактовая частота;
- коэффициент внутреннего умножения тактовой частоты;
- размер кэш-памяти.

Микросхема ПЗУ и система BIOS

В момент включения компьютера в его оперативной памяти нет ничего — ни данных, ни программ, поскольку оперативная память не может ничего хранить без подзарядки ячеек более сотых долей секунды, но процессору нужны команды, в том числе и в первый момент после включения. Поэтому сразу после включения на адресной шине процессора выставляется стартовый адрес. Это происходит аппаратно, без участия программ (всегда одинаково). Процессор обращается по выставленному адресу за своей первой командой и далее начинает работать по программам. Этот исходный адрес не может указывать на оперативную память, в которой пока ничего нет. Он указывает на другой тип памяти — постоянное запоминающее устройство (ПЗУ). Микросхема ПЗУ способна длительное время хранить информацию, даже когда компьютер выключен. Программы, находящиеся в ПЗУ, называют «защитыми» — их записывают туда на этапе изготовления микросхемы.

Комплект программ, находящихся в ПЗУ, образует базовую систему ввода-вывода (BIOS — Basic Input Output System). Основное назначение программ этого пакета состоит в том, чтобы проверить состав и работоспособность компьютерной системы и обеспечить взаимодействие с клавиатурой, монитором, жестким диском и дисководом гибких дисков. Программы, входящие в BIOS, позволяют нам наблюдать на экране диагностические сообщения, сопровождающие запуск компьютера, а также вмешиваться в ход запуска с помощью клавиатуры.

Энергонезависимая память CMOS

Выше мы отметили, что работа таких стандартных устройств, как клавиатура, может обслуживаться программами, входящими в BIOS, но такими средствами нельзя обеспечить работу со всеми возможными устройствами. Так, например, изготовители BIOS абсолютно ничего не знают о параметрах наших жестких и гибких дисков, им не известны ни состав, ни свойства произвольной вычислительной системы. Для того чтобы начать работу с другим оборудованием, программы, входящие в состав BIOS, должны знать, где можно найти нужные параметры. По очевидным причинам их нельзя хранить ни в оперативной памяти, ни в постоянном запоминающем устройстве.

Специально для этого на материнской плате есть микросхема «энергонезависимой памяти», по технологии изготовления называемая CMOS. От оперативной памяти она отличается тем, что ее содержимое не стирается во время выключения компьютера, а от ПЗУ она отличается тем, что данные в нее можно заносить и изменять самостоятельно, в соответствии с тем, какое оборудование входит в состав системы. Эта микросхема постоянно подпитывается от небольшой аккумуляторной батарейки, расположенной на материнской плате. Заряда этой батарейки

хватает на то, чтобы микросхема не теряла данные, даже если компьютер не будут включать месяцами.

В микросхеме CMOS хранятся данные о гибких и жестких дисках, о процессоре, о некоторых других устройствах материнской платы. Тот факт, что компьютер четко отслеживает время и календарь (даже и в выключенном состоянии), тоже связан с тем, что показания системных часов постоянно хранятся (и изменяются) в CMOS.

Таким образом, программы, записанные в BIOS, считывают данные о составе оборудования компьютера из микросхемы CMOS, после чего они могут выполнить обращение к жесткому диску, а в случае необходимости и к гибкому, и передать управление тем программам, которые там записаны.

Периферийные устройства персонального компьютера

Периферийные устройства персонального компьютера подключаются к его интерфейсам и выполняют функцию ввода-вывода информации.

По назначению периферийные устройства можно разделить на:

1. Устройства ввода данных:

- клавиатура,
- мышь,
- специальные манипуляторы;
- устройства ввода графических данных;
- сенсорный экран;
- веб-камера;
- световое перо.

2. Устройства вывода данных:

- дисплей (монитор),
- принтеры,
- графопостроители

3. Устройства хранения данных:

- внешние запоминающие устройства, накопители информации;
- накопители на магнитных дисках;
- CD – привод;
- DVD – привод;
- стримеры – накопители на магнитных лентах;
- флэш-диски.

4. Устройства обмена данными.

- модем

Аппаратное подключение внешних устройств к компьютеру осуществляется через контроллер (адаптер).

Контроллер - это электронная схема, которая управляет внешним устройством. Все контроллеры или адаптеры взаимодействуют с микропроцессором и оперативной памятью через системную магистраль передачи данных, которую называют шиной. Системная шина является каналом соединения микропроцессора, оперативной памяти и интегральных устройств. Физически шина находится на материнской плате.

Контроллер периферийного устройства подключается к общей шине

ПК. Соответственно, получается, что все периферийные устройства персонального компьютера подключены компьютера через контроллеры. И к этой же общей шине подключаются процессор и оперативная память ПК.

Контроллер осуществляет постоянное взаимодействие с процессором и оперативной памятью ПК через общую шину ПК. Контроллер отвечает за получение информации от процессора и из оперативной памяти, и за передачу данных процессору или в оперативную память.

Периферийные устройства персонального компьютера бывают внутренние и внешние. Внутренние устройства устанавливаются внутрь ПК (внутри системного блока). Примеры внутренних периферийных устройств персонального компьютера – это жесткие диски, встроенный привод CD-/DVD- дисков и т.п.

Внешние устройства подключаются к портам ввода-вывода, при этом за взаимодействие этих устройств внутри ПК отвечают порты ввода-вывода. Примеры внешних периферийных устройств персонального компьютера – это принтеры, сканеры, внешние (подключаемые извне ПК) приводы CD-/DVD- дисков, камеры, манипулятор «мышь», клавиатура и т.п.

Каждое внутреннее устройство имеет контроллер (от английского слова controller – устройство управления). Для внешних устройств эту функцию выполняет контроллер порта, к которому это устройство подключено.

Во всем остальном внутренние и внешние периферийные устройства персонального компьютера работают по одним и тем же принципам.

Устройства ввода графических данных.

Для ввода графической информации используют *сканеры, графические планшеты (дигитайзеры) и цифровые фотокамеры*. Интересно отметить, что с помощью сканеров можно вводить и знаковую информацию. В этом случае исходный материал вводится в графическом виде, после чего обрабатывается специальными программными средствами (*программами распознавания образов*).

Устройства вывода данных.

1. Принтеры.

В качестве устройств вывода данных, дополнительных к монитору, используют печатающие устройства (принтеры), позволяющие получать копии документов на бумаге или прозрачном носителе. По принципу действия различают матричные, лазерные, светодиодные и струйные принтеры.

2. Плоттер (графопостроитель).

Устройство для вывода на бумагу больших рисунков, чертежей и другой графической информации. Плоттер может выводить графическую информацию на бумагу формата A2 и больше. Конструктивно в нем может использоваться или барабан рулонной бумаги, или горизонтальный планшет.

3. Внешние запоминающие устройства.

В основе работы запоминающего устройства может лежать любой

физический эффект, обеспечивающий приведение системы к двум или более устойчивым состояниям.

В современной компьютерной технике часто используются физические свойства полупроводников, когда прохождение тока через полупроводник или его отсутствие трактуются как наличие логических сигналов 0 или 1 (полупроводниковая память). Во флэш-накопителях применяется полупроводниковая память.

Устойчивые состояния, определяемые направлением намагниченности, позволяют использовать для хранения данных разнообразные магнитные материалы (магнитная память). Принцип изменения магнитной индукции поверхности носителя используется в накопителях типа винчестер.

Наличие или отсутствие заряда в конденсаторе также может быть положено в основу системы хранения (емкостная память).

Быстродействие накопителя информации – скорость чтения/записи данных в накопителе. Оно характеризуется двумя параметрами:

1. Средним временем доступа.
2. Скоростью передачи данных.

5. НАЗНАЧЕНИЕ И ПРИНЦИП РАБОТЫ ЭЛЕМЕНТОВ ЭВМ

Классификация элементов и узлов ЭВМ.

При рассмотрении структуры любой ЭВМ обычно проводят ее детализацию.

Как правило, в структуре ЭВМ выделяют следующие структурные единицы:

- устройства;
- узлы;
- блоки;
- элементы.

Такая детализация соответствует вполне определенным операциям преобразования информации, заложенным в программах пользователей.

Нижний уровень обработки реализуют элементы. Каждый элемент предназначен для обработки единичных электрических сигналов, соответствующих битам информации.

Узлы обеспечивают одновременную обработку группы сигналов - информационных слов.

Блоки реализуют некоторую последовательность в обработке информационных слов — функционально обособленную часть машинных операций (блок выборки команд, блок записи-чтения и др.).

Устройства предназначены для выполнения отдельных машинных операций и их последовательностей (АЛУ, УУ...).

Все современные вычислительные машины строятся на комплексах (системах) интегральных микросхем (ИС). Электронная микросхема называется **интегральной**, если ее компоненты и соединения между ними выполнены

- в едином технологическом цикле,
- на едином основании и
- имеют общую герметизацию и защиту от механических воздействий.

Каждая микросхема представляет собой миниатюрную электронную схему, сформированную послойно в кристалле полупроводника: кремния, германия, арсениде галлия и т.д. В состав микропроцессорных наборов включаются различные типы микросхем, но все они должны иметь единый тип межмодульных связей, основанный на стандартизации параметров сигналов взаимодействия (амплитуда, полярность, длительность импульсов и т.п.). Основу набора обычно составляют большие ИС (БИС) и даже сверхбольшие интегральные схемы (СБИС). На очереди следует ожидать появления ультра больших ИС (УБИС). Кроме них обычно используются микросхемы с малой и средней степенью интеграции (СИС).

Функционально **микросхемы** могут соответствовать **устройству**, **узлу** или **блоку**, но каждая из них состоит из комбинации простейших **логических элементов**, реализующих функции формирования, преобразования, запоминания сигналов и т.д.

Элементы ЭВМ можно классифицировать по различным признакам.

Наиболее часто такими признаками являются:

- тип сигналов;
- назначение элементов;
- технология их изготовления и т.д.

В ЭВМ широко применяют два способа физического представления сигналов: импульсный и потенциальный. При импульсном способе представления сигналов единичному значению некоторой двоичной переменной ставится в соответствие наличие импульса (тока или напряжения), нулевому значению — отсутствие импульса. Длительность импульсного сигнала не превышает один такт синхроимпульсов. При потенциальном или статическом представлении сигналов единично значение двоичной переменной отображается высоким уровнем напряжения, а нулевое значение - низким уровнем.

Независимо от вида сигналов различают последовательный и параллельный коды передачи и представления информации в ЭВМ.

При последовательном коде представления данных используются одиночные шины или линии передачи, в которых сигналы, соответствующие отдельным разрядам данных, разнесены во времени. Обработка такой информации производится последовательно разряд за разрядом. Такой вид представления и передачи данных требует весьма экономичных по аппаратурным затратам схем обработки данных. Время же обработки определяется числом обрабатываемых сигналов (разрядов).

Параллельный код отображения и передачи информации предполагает параллельную и одновременную фиксацию всех разрядов данных на различных шинах, т.е. параллельный код данных развернут в пространстве. Это дает возможность ускорить обработку во времени, но затраты на аппаратурные средства при этом возрастают пропорционально числу обрабатываемых разрядов.

По своему назначению элементы делятся на:

- формирующие;
- логические;
- запоминающие.

К формирующим элементам относятся различные формирователи, усилители, усилители-формирователи и т.п. Данные элементы служат для выработки определенных электрических сигналов, восстановления их параметров (амплитуды, полярности, мощности, длительности).

Простейшие логические элементы преобразуют входные сигналы в соответствии с элементарными логическими функциями, рассмотренными ранее. В свою очередь, полученные сигналы могут формировать следующий уровень сигналов и т. д. Сложные преобразования в соответствии с требуемыми логическими зависимостями могут приводить к построению многоуровневых схем. Каждая такая схема представляет собой композицию простейших логических схем.

Запоминающим элементом называется элемент, который способен принимать и хранить код двоичной цифры (единицы или нуля). Элементы

памяти могут запоминать и сохранять исходные значения некоторых величин, промежуточные значения обработки и окончательные результаты вычислений.

Только запоминающие элементы в схемах ЭВМ позволяют проводить обработку информации с учетом ее развития.

Комбинационные схемы.

Обработка входной информации X в выходную Y в любых схемах ЭВМ обеспечивается преобразователями или цифровыми автоматами двух видов: *комбинационными схемами и схемами с памятью*.

Комбинационные схемы (КС) - это схемы, у которых выходные сигналы $Y = (y_1, y_2, \dots, y_m)$ в любой момент дискретного времени однозначно определяются совокупностью входных сигналов $X = (x_1, x_2, \dots, x_n)$, поступающих в тот же момент времени t . Реализуемый в КС способ обработки информации называется комбинационным потому, что результат обработки зависит только от комбинации входных сигналов и формируется сразу при поступлении входных сигналов.

Поэтому одним из достоинств комбинационных схем является их высокое быстродействие. Преобразование информации однозначно описывается логическими функциями вида $Y = f(X)$.

Логические функции и соответствующие им комбинационные схемы подразделяют на:

- регулярные;
- нерегулярные.

Регулярные структуры предполагают построение схемы таким образом, что каждый из ее выходов строится по аналогии с предыдущими. В нерегулярных структурах такая аналогия отсутствует. Примером построения нерегулярной структуры может служить разработка схемы в примере схемы, фиксирующей появление “неправильной” тетрады в двоично-десятичном представлении чисел (см. предыдущую лекцию).

Дешифраторы и шифраторы

Дешифраторы (ДШ) — это комбинационные схемы с n входами и $m = 2^n$ выходами. Единичный сигнал, формирующийся на одном из n выходов, однозначно соответствует комбинации входных сигналов.

Дешифраторы широко используются в ЭВМ для выбора информации по определенному адресу, для расшифровки кода операции и др. Логические зависимости дешифратора:

$$\begin{aligned} y_0 &= \overline{x_1} \overline{x_2} \overline{x_3}, y_4 = x_1 \overline{x_2} \overline{x_3}, \\ y_1 &= \overline{x_1} \overline{x_2} x_3, y_5 = x_1 \overline{x_2} x_3, \\ y_2 &= \overline{x_1} x_2 \overline{x_3}, y_6 = x_1 x_2 \overline{x_3}, \\ y_3 &= \overline{x_1} x_2 x_3, y_7 = x_1 x_2 x_3. \end{aligned}$$

Шифратор (ШР) решает задачу, обратную схемам ДШ, т. е. по номеру входного сигнала формирует однозначную комбинацию выходных сигналов. Логические зависимости, соответствующие таблице истинности:

$$y_2 = x_1 \vee x_3 \vee x_5 \vee x_7,$$

$$y_1 = x_2 \vee x_3 \vee x_6 \vee x_7,$$

$$y_0 = x_4 \vee x_5 \vee x_6 \vee x_7.$$

Компараторы и сумматоры

Схемы сравнения или компараторы обычно строятся как поразрядные. Они широко используются и автономно, и в составе более сложных схем, например, при построении сумматоров.

Таблица истинности (см. табл.7) отражает логику работы 1-го разряда схемы сравнения при сравнении двух двоичных векторов А и В.

Таблица 7 - Таблица истинности компаратора

Входы		Выходы
a_i	b_i	Y_i
0	0	1
0	1	0
1	0	0
1	1	1

Логическая зависимость в соответствие с таблицей истинности:

$$Y_i = \bar{a}_i \bar{b}_i \vee a_i b_i = \bar{a}_i b_i \vee a_i \bar{b}_i = a_i \oplus b_i.$$

Комбинационный сумматор. Принципы построения и работы сумматора вытекают из правил сложения двоичных цифр. Схема сумматора также является регулярной и широко используется в ЭВМ. При сложении одноразрядных двоичных цифр можно выявить закономерности в построении и многоразрядных сумматоров.

Сначала рассмотрим сумматор, обеспечивающий сложение двух двоичных цифр a_i и b_i , считая, что переносы из предыдущего разряда не поступают. Этой логике отвечает сложение младших разрядов двоичных чисел. Процесс сложения описывается таблицей истинности (см. табл. 8) и соответствующими логическими зависимостями, где S_i - функция одноразрядной суммы и p_i - функция формирования переноса. Перенос формируется в том случае, когда $a_i = 1$ и $b_i = 1$.

Таблица 8 – Таблица истинности комбинационного полусумматора

Входы		Выходы	
a_i	b_i	S_i	p_i
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Логические зависимости:

$$S_i = \bar{a}_i b_i \vee a_i \bar{b}_i = a_i \oplus b_i,$$

$$p_i = a_i \cdot b_i.$$

Приведенные зависимости соответствуют логике работы самого

младшего разряда любого сумматора.

Логические зависимости полусумматора S_i и компаратора очень похожи, так как они инверсны по отношению друг к другу.

Уравнения, положенные в основу одноразрядного сумматора, используются и при построении многоразрядных сумматоров. Логика работы каждого разряда сумматора описывается таблицей 9, которую можно считать его таблицей истинности.

Таблица 9 - Правила сложения двоичных цифр

Значения двоичных чисел a и b			Разряд суммы S_i	Перенос в следующий разряд p_i
a_i	b_i	p_{i-1}		
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Таблица истинности сумматора, учитывающего сигналы переноса, отличается от таблицы полусумматора (табл.8) дополнительным входом p — переносом из предыдущих разрядов.

Исходные логические зависимости, формируемые по табл.9, имеют следующие совершенные ДНФ:

$$S_i = \bar{a}\bar{b}p \vee \bar{a}b\bar{p} \vee a\bar{b}\bar{p} \vee abp,$$

$$p_i = \bar{a}bp \vee \bar{a}\bar{b}p \vee ab\bar{p} \vee abp.$$

Преобразование этих выражений приводит к следующим зависимостям:

$$S_i = p(\bar{a}\bar{b} \vee ab) \vee b(\bar{a}\bar{p} \vee ap) \vee a(\bar{b}\bar{p} \vee bp) = p(\bar{a} \oplus \bar{b}) \vee b(\bar{a} \oplus p) \vee a(\bar{b} \oplus p),$$

$$p_i = ab \vee ap \vee bp.$$

В приведенных выражениях индексы у переменных в правых частях уравнений опущены.

Сумматор параллельного действия.

Можно построить сумматор, в котором сложение производится как поразрядная операция и на распространение переноса не требуется дополнительного времени.

Для описания работы такого сумматора удобно ввести две функции: γ — функция генерации переноса, $\gamma = x \& y$.

Функция равна 1, когда перенос в этом разряде возникает независимо от переноса на его входе.

π — функция прозрачности, $\pi = x \vee y$.

Функция равна 1, когда при возникновении переноса на входе данного

разряда, на его выходе также возникает перенос, т.е. тракт разряда прозрачен для входного переноса.

С помощью введенных функций можно представить работу тракта переноса одного разряда сумматора

$$C_{i+1} = \gamma_i \vee C_i \wedge \pi_i,$$

где C_i – перенос из предыдущего разряда, C_{i+1} – перенос в следующий разряд. Тогда перенос на входе $(i+1)$ разряда сумматора можно представить так:

$$C_{i+1} = \gamma_i \vee \gamma_{i-1} \cdot \pi_i \vee \gamma_{i-2} \cdot \pi_{i-1} \cdot \pi_i \vee \gamma_{i-3} \cdot \pi_{i-2} \cdot \pi_{i-1} \cdot \pi_i \vee \dots$$

Затраты оборудования на реализацию такого сумматора, особенно при большом количестве разрядов, достаточно велики.

Сумматор с групповым переносом

Сумматор разбивают на несколько групп. Каждая такая группа — мини сумматор — имеет свой штатный вход переноса.

Суть группового переноса заключается в том, что в дополнении к тракту переноса внутри группы, строят тракт переноса второго уровня между группами, который вырабатывает сигналы групповых переносов, подаваемые на входы «мини сумматоров».

Параллельный перенос между группами в сочетании с параллельным переносом внутри группы позволяет создавать быстрые сумматоры.

Регистр

Регистром называется узел, предназначенный для приема, временного хранения и выдачи машинного слова. Регистры могут также использоваться для некоторых операций преобразования данных: для сдвига кода числа (слова) на определенное число разрядов влево или вправо, для преобразования последовательного кода числа в параллельный и наоборот и т.д. Эти дополнительные функции регистров обеспечиваются путем усложнения схем хранения, выбора более сложных триггеров и подключения дополнительных логических схем на их входах и выходах.

Таким образом, регистры представляют собой совокупность триггеров, число которых соответствует числу разрядов в слове, и вспомогательных схем, обеспечивающих выполнение различных операций над словом.

Счетчик

Счетчик — узел ЭВМ, позволяющий осуществлять подсчет поступающих на его вход сигналов и фиксацию результата в виде многоразрядного двоичного числа. Счетчик, состоящий из n -триггеров, дает возможность подсчитывать до N сигналов, связанных зависимостью:

$$n = \log_2 N \text{ или } N = 2^n.$$

Счетчики используются для подсчета импульсов, сдвигов, формирования адресов и т.д. Функционально различают суммирующие, вычитающие, реверсивные счетчики. Они также отличаются друг от друга логикой работы дополнительных логических элементов, подключаемых к триггерам.

В основу построения любого счетчика положено свойство Т-триггеров изменять свое состояние при подаче очередного сигнала на счетный вход Т.

Рассмотрим работы трехразрядного суммирующего счетчика. В табл. 10 представлена логика его работы.

Таблица 10 - Таблица переходов трехразрядного счетчика

Вход x	Состояние								Режим
	000	001	010	011	100	101	110	111	
0	000	001	010	011	100	101	110	111	Хранение
1	001	010	011	100	101	110	111	000	Счет

6. ОБЩАЯ СТРУКТУРА МИКРОПРОЦЕССОРА

Микропроцессор — главный вычислительный элемент компьютера, его «сердце».

На первый взгляд, процессор — просто выращенный по специальной технологии кристалл кремния. Процессор содержит в себе множество отдельных элементов — транзисторов, которые в совокупности и наделяют компьютер способностью «думать». Точнее, вычислять, производя определенные математические операции с числами, в которые преобразуется любая поступающая в компьютер информация. Безусловно, один транзистор никаких особых вычислений произвести не может. Единственное, на что способен этот электронный переключатель — это пропустить сигнал дальше или задержать его. Наличие сигнала дает логическую единицу (да); его отсутствие — логический же ноль (нет).

Каждый процессор включает в себя миллионы транзисторов, но и самих процессоров для работы компьютера требуется немало. Помимо центрального процессора, который во всем мире принято обозначать аббревиатурой CPU (Central Processor Unit), схожими микросхемами оборудована практически каждая компьютерная «железяка».

Процессор — это не просто скопище транзисторов, а целая система множества важных устройств. На любом процессорном кристалле находятся:

Состав микропроцессора.

Собственно процессор, главное вычислительное устройство, состоящее из миллионов логических элементов — транзисторов.

Сопроцессор — специальный блок для операций с «плавающей точкой» (или запятой). Применяется для особо точных и сложных расчетов, а также для работы с рядом - графических программ.

Кэш-память первого уровня — небольшая (несколько десятков килобайт) сверхбыстрая память, предназначенная для хранения промежуточных результатов вычислений.

Кэш-память второго уровня — эта память чуть помедленнее, зато больше — от 128 килобайт до 2 Мб.

Арифметико-логическое устройство - часть процессора, которая выполняет команды.

Устройство управления - часть процессора, выполняющая функции управления устройствами.

Основные характеристики.

Тактовая частота. Самый важный показатель, определяющий скорость работы процессора. Тактовая частота, измеряемая в мегагерцах (МГц) и гигагерцах (ГГц), обозначает лишь то количество циклов, которые совершает работающий процессор за единицу времени (секунду).

Разрядность процессора. Если тактовую частоту процессора можно уподобить скорости течения воды в реке, то разрядность процессора — ширину ее русла. Понятно, что процессор со вдвое большей разрядностью может «заглотнуть» вдвое больше данных в единицу времени — в том

случае, конечно, если это позволяет сделать специально оптимизированное программное обеспечение.

Размер кэш-памяти. В эту встроенную память процессор помещает все часто используемые данные, чтобы не обращаться каждый раз — к более медленной оперативной памяти и жесткому диску.

Кэш-память в процессоре имеется двух видов. Самая быстрая — кэш-память первого уровня (32 кб у процессоров Intel и до 128 кб — в последних моделях AMD).

Существует еще чуть менее быстрая, но зато более объемная кэш-память второго уровня — и именно ее объемом отличаются различные модификации процессоров.

Тип ядра и технология производства. Технология определяется толщиной минимальных элементов процессора, — чем более «тонкой» становится технология, тем больше транзисторов может уместиться на кристалле. Кроме этого, переход на новую технологию помогает снизить энергопотребление и тепловыделение процессора, что очень важно для его стабильной работы.

Переход на новую технологию, как правило, влечет за собой и смену процессорного «ядра»

Частота системной шины. Шиной называется та аппаратная магистраль, по которой перемещаются от устройства к устройству данные. Чем выше частота шины, тем больше данных поступает за единицу времени к процессору.

Частота системной шины прямо связана и с частотой самого процессора через так называемый «коэффициент умножения». Процессорная частота — это и есть частота системной шины, умноженная процессором на некую заложенную в нем величину.

Дополнительные возможности. Большинство современных процессоров оснащены также рядом эксклюзивных возможностей, которые влияют на скорость обработки информации. В их числе можно назвать специальные системы «мультимедийных команд», предназначенных для оптимизации работы с графикой, видео и звуком.

Устройства внутренней памяти и их назначение.

В состав внутренней памяти входят оперативная память, кэш-память и специальная память.

1. Оперативная память

Оперативная память — это быстрое запоминающее устройство не очень большого объема, непосредственно связанное с процессором и предназначенное для записи, считывания и хранения выполняемых программ и данных, обрабатываемых этими программами.

Оперативная память используется только для временного хранения данных и программ, так как, когда машина выключается, все, что находилось в ОЗУ, пропадает.

Модули памяти характеризуются такими параметрами, как объем — (16, 32, 64, 128, 256 или 512 Мбайт), число микросхем, паспортная

частота(100 или 133 МГц), время доступа к данным (6 или 7 наносекунд) и число контактов (72, 168 или 184).

2. Кэш-память

Кэш (англ. cache), или сверхоперативная память — очень быстрое ЗУ небольшого объёма, которое используется при обмене данными между микропроцессором и оперативной памятью для компенсации разницы в скорости обработки информации процессором и несколько менее быстродействующей оперативной памятью.

Кэш-памятью управляет специальное устройство — контроллер, который, анализируя выполняемую программу, пытается предвидеть, какие данные и команды вероятнее всего понадобятся в ближайшее время процессору, и подкачивает их в кэш-память. При этом возможны как "попадания", так и "промахи". В случае попадания, то есть, если в кэш подкачаны нужные данные, извлечение их из памяти происходит без задержки. Если же требуемая информация в кэше отсутствует, то процессор считывает её непосредственно из оперативной памяти. размером 8, 16 или 32 Кбайт.

3. Специальная память

К устройствам специальной памяти относятся постоянная память (ROM), перепрограммируемая постоянная память (Flash Memory), память CMOS RAM, питаемая от батарейки, видеопамять и некоторые другие виды памяти.

Постоянная память (ПЗУ, англ. ROM, Read Only Memory — память только для чтения) — энергонезависимая память, используется для хранения данных, которые никогда не потребуют изменения. Содержание памяти специальным образом "зашивается" в устройстве при его изготовлении для постоянного хранения. Из ПЗУ можно только читать.

Перепрограммируемая постоянная память (Flash Memory) — энергонезависимая память, допускающая многократную перезапись своего содержимого с дискеты.

Прежде всего в постоянную память записывают программу управления работой самого процессора. В ПЗУ находятся программы управления дисплеем, клавиатурой, принтером, внешней памятью, программы запуска и остановки компьютера, тестирования устройств.

Важнейшая микросхема постоянной или Flash-памяти — модуль BIOS. Роль BIOS двоякая: с одной стороны это неотъемлемый элемент аппаратуры, а с другой стороны — важный модуль любой операционной системы.

BIOS (Basic Input/Output System — базовая система ввода-вывода) — совокупность программ, предназначенных для автоматического тестирования устройств после включения питания компьютера и загрузки операционной системы в оперативную память.

4. Видеопамять

Для хранения графической информации используется видеопамять.

Видеопамять (VRAM) — разновидность оперативного ЗУ, в котором хранятся закодированные изображения. Это ЗУ организовано так, что его

содержимое доступно сразу двум устройствам — процессору и дисплею. Поэтому изображение на экране меняется одновременно с обновлением видеоданных в памяти.

Описание набора регистров микропроцессора.

Программная модель микропроцессора содержит 32 регистра, которые можно разделить на две группы:

- 16 пользовательских регистров;
- 16 системных регистров.

Пользовательские регистры

Пользовательскими регистры называются потому, что программист может их использовать при разработке программ.

К пользовательским регистрам относятся:

1)восемь 32-битных регистров, которые могут использоваться программистами для хранения данных и адресов (регистры общего назначения)

eax/ax/ah/al
 ebx/bx/bh/bl
 edx/dx/dh/dl
 ecx/cx/ch/cl
 esi/si
 edi/di
 ebp/bp
 esp/sp

2) шесть регистров сегментов: cs, ds, ss, es, fs, gs

3) регистр состояния (регистр флагов) eflags/flags;

4) регистр управления (регистр указателя команды) eip/ip.

Регистры общего назначения

Регистры общего назначения физически находятся в микропроцессоре внутри арифметико-логического устройства (АЛУ), поэтому их еще называют регистрами АЛУ.

eax/ax/ah/al (Accumulator register) — регистр-аккумулятор.

Применяется для хранения промежуточных данных.

ebx/bx/bh/bl (Base register) — базовый регистр.

Применяется для хранения базового адреса некоторого объекта в памяти.

ecx/cx/ch/cl (Count register) — регистр-счетчик.

Применяется в командах, производящих некоторые повторяющиеся действия.

Его использование часто неявно и скрыто в алгоритме работы соответствующей команды. Например, команда организации цикла loop кроме передачи управления команде, находящейся по некоторому адресу, анализирует и уменьшает на единицу значение регистра ecx/cx.

edx/dx/dh/dl (Data register) — регистр данных.

Применяется для хранения промежуточных данных.

Обратим внимание, можно использовать только весь регистр целиком (например, `eax`), младшую 16-битную часть (например, `ax`) и 8-битные части этих регистров (например, `ah`, `al`).

!!! Старшие 16 бит этих регистров как самостоятельные объекты недоступны.

Регистры **esi/si** и **edi/di** используются для поддержки так называемых цепочечных операций, то есть операций, производящих последовательную обработку цепочек элементов (можно сравнить со строками в языке Pascal).

esi/si (Source Index register) — индекс источника.

Этот регистр в цепочечных операциях содержит текущий адрес элемента в цепочке-источнике (первоначальная строка).

edi/di (Destination Index register) — индекс приемника (получателя).

Этот регистр в цепочечных операциях содержит текущий адрес в цепочке-приемнике (результатирующая строка).

Регистры **ebp/bp** и **esp/sp** предназначены для работы со стеком.

esp/sp (Stack Pointer register) — регистр указателя стека.

Содержит указатель вершины стека в текущем сегменте стека.

ebp/bp (Base Pointer register) — регистр указателя базы кадра стека.

Регистр предназначен для организации произвольного доступа к данным внутри стека.

Сегментные регистры

В программной модели микропроцессора имеется шесть сегментных регистров:

cs, ss, ds, es, gs, fs.

Все сегментные регистры $\frac{3}{4}$ 16-разрядные.

Их существование обусловлено спецификой организации и использования оперативной памяти: микропроцессоры Intel в любом режиме работы (реальный режим, защищенный режим) поддерживают сегментную модель организации оперативной памяти.

Она заключается в том, что микропроцессор аппаратно поддерживает структурную организацию программы в виде частей (фрагментов), которые называются сегментами. Соответственно, такая организация памяти называется сегментной.

Сегментные регистры предназначены для того, чтобы указать на сегменты, к которым программа имеет доступ в конкретный момент времени.

Фактически в этих регистрах содержатся адреса ячеек памяти, с которых начинаются соответствующие сегменты.

Микропроцессор поддерживает следующие типы сегментов.

1. Сегмент кода (содержит команды программы).

Для доступа к этому сегменту служит регистр **cs** (code segment register) — сегментный регистр кода.

Он содержит адрес сегмента кода, к которому в данный момент имеет доступ микропроцессор.

2. Сегмент данных (содержит обрабатываемые программой данные).

Для доступа к этому сегменту служит регистр ds (data segment register) — сегментный регистр данных.

Он содержит адрес сегмента данных текущей программы.

3. Сегмент стека (область памяти, называемая стеком).

Работу со стеком микропроцессор организует по следующему принципу: последний записанный в эту область элемент выбирается первым (LIFO).

Для доступа к этому сегменту служит регистр ss (stack segment register) — сегментный регистр стека.

Он содержит адрес сегмента стека.

4. Дополнительные сегменты данных.

Если программе недостаточно одного сегмента данных, то она имеет возможность использовать еще три дополнительных сегмента данных.

Адреса дополнительных сегментов данных должны содержаться в регистрах es, gs, fs (extension data segment registers).

es ³/₄ дополнительный сегментный регистр данных или экстракодов (Extra Segment).

Начиная с микропроцессора 80386, появились два дополнительных регистра fs,gs (следующие буквы в латинском алфавите после e).

При использовании дополнительных сегментов данных их адреса требуется указывать с помощью специальных префиксов переопределения сегментов в команде (например, fs:).

Регистр состояния

Регистр состояния **eflags/flags** содержит информацию о состоянии микропроцессора.

eflags/flags (flag register) — регистр флагов.

Разрядность eflags/flags — 32/16 бит.

Отдельные биты данного регистра имеют определенное функциональное назначение и называются флагами.

Младшая часть этого регистра полностью аналогична регистру flags для i8086.

Флаги регистра eflags/flags подразделяются на три группы.

1) Флаги состояния

Эти флаги отражают особенности результата исполнения арифметических или логических операций и могут изменяться после выполнения машинных команд.

Это позволяет анализировать состояние вычислительного процесса и реагировать на него (например, с помощью команд условных переходов и вызовов подпрограмм).

cf - флаг переноса (Carry Flag)

pf - флаг паритета (Parity Flag)

af - вспомогательный флаг переноса (Auxiliary carry Flag)

zf - флаг нуля (Zero Flag) (1 - результат нулевой; 0 - результат ненулевой)

sf - флаг знака (Sign Flag)

(1 - старший бит результата = 1; 0 - старший бит результата = 0)

of - Флаг переполнения (Overflow Flag)

Используется для фиксирования факта потери значащего бита при арифметических операциях.

iopl - уровень привилегий ввода-вывода (Input/Output Privilege Level)

Используется в защищенном режиме работы микропроцессора для контроля доступа к командам ввода-вывода в зависимости от привилегированности задачи.

nt - флажок вложенности задачи (Nested Task)

Используется в защищенном режиме работы микропроцессора для фиксации того факта, что одна задача вложена в другую

2) Флаг направления df (Directory Flag).

Он находится в 10-м бите регистра eflags и используется цепочечными командами. Значение флага df определяет направление обработки в цепочечных операциях: от начала строки к концу (df = 0) или от конца строки к ее началу (df = 1).

3) Системные флаги

Управляют вводом/выводом, маскируемыми прерываниями, отладкой, переключением между задачами и виртуальным режимом 8086.

tf - флаг трассировки (Trace Flag)

Предназначен для организации пошаговой работы микропроцессора.

if - Флаг прерывания (Interrupt enable Flag)

Предназначен для разрешения или запрещения (маскирования) аппаратных прерываний.

(1 — аппаратные прерывания разрешены; 0 — аппаратные прерывания запрещены)

rf - флаг возобновления (Resume Flag)

Используется при обработке прерываний от регистров отладки.

Vm - флаг виртуального 8086 (Virtual 8086 Mode)

Признак работы микропроцессора в режиме виртуального 8086.

(1 - процессор работает в режиме виртуального 8086; 0 - процессор работает в реальном или защищенном режиме)

ac - флаг контроля выравнивания (Alignment Check)

Предназначен для разрешения контроля выравнивания при обращениях к памяти.

Регистр управления

Регистр управления **eip/ip** содержит информацию о состоянии программы, команды которой в данный момент загружены на конвейер.

eip/ip (Instruction Pointer register) — регистр-указатель команд.

Содержит смещение следующей подлежащей выполнению команды (относительно текущего сегмента кода).

Регистр **eip/ip** имеет разрядность 32/16 бит.

Загрузка и изменение его значения производятся различными командами условных и безусловных переходов, вызова процедур и возврата

из процедур. Возникновение прерываний также приводит к модификации регистра ip/ip .

Арифметико-логическое устройство

(АЛУ) предназначено для выполнения арифметических и логических операций преобразования информации. Функционально АЛУ состоит обычно из двух регистров, сумматора и схем управления (местного устройства управления).

Сумматор - вычислительная схема, выполняющая процедуру сложения поступающих на ее вход двоичных кодов; сумматор имеет разрядность двойного машинного слова.

Регистры - быстродействующие ячейки памяти различной длины: регистр 1 имеет разрядность двойного слова, а регистр 2 — разрядность слова. При выполнении операций в регистр 1 помещается первое число, участвующее в операции, а по завершении операции — результат; в регистр 2 — второе число, участвующее в операции (по завершению операции информация в нем не изменяется). Регистр 1 может и принимать информацию с кодовых шин данных и выдавать информацию на них; регистр 2 только получает информацию с этих шин.

Схемы управления принимают по кодовым шинам инструкций управляющие сигналы от устройства управления и преобразуют их в сигналы для управления работой регистров и сумматора АЛУ.

АЛУ выполняет арифметические операции «+», «-», «х» и «>» только над двоичной информацией с запятой, фиксированной после последнего разряда, то есть только над целыми двоичными числами. Выполнение операций над двоичными числами с плавающей запятой и над двоично-кодированными десятичными числами осуществляется с привлечением математического сопроцессора или по специально составленным программам.

7. ЗАПОМИНАЮЩИЕ УСТРОЙСТВА: КЛАССИФИКАЦИЯ, ПРИНЦИП РАБОТЫ, ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

Запоминающее устройство - носитель информации, предназначенный для записи и хранения данных. В основе работы запоминающего устройства может лежать любой физический эффект, обеспечивающий приведение системы к двум или более устойчивым состояниям.

Классификация запоминающих устройств

По устойчивости записи и возможности перезаписи ЗУ делятся на:

- постоянные ЗУ (ПЗУ), содержание которых не может быть изменено конечным пользователем (например, DVD-ROM). ПЗУ в рабочем режиме допускает только считывание информации.
- записываемые ЗУ, в которые конечный пользователь может записать информацию только один раз (например, DVD-R).
- многократно перезаписываемые ЗУ (например, DVD-RW).
- оперативные ЗУ (ОЗУ) обеспечивает режим записи, хранения и считывания информации в процессе её обработки.

По типу доступа ЗУ делятся на:

- устройства с последовательным доступом (например, магнитные ленты).
- устройства с произвольным доступом (RAM) (например, оперативная память).
- устройства с прямым доступом (например, жесткие магнитные диски).
- устройства с ассоциативным доступом (специальные устройства, для повышения производительности БД)

По геометрическому исполнению:

- дисковые (магнитные диски, оптические, магнитооптические);
- ленточные (магнитные ленты, перфоленты);
- барабанные (магнитные барабаны);
- карточные (магнитные карты, перфокарты, флэш-карты, и др.)
- печатные платы (карты DRAM).

По физическому принципу:

- перфорационные (перфокарта; перфолента);
- с магнитной записью (ферритовые сердечники, магнитные диски, магнитные ленты, магнитные карты);
- оптические (CD, DVD, HD-DVD, Blu-ray Disc);
- использующие эффекты в полупроводниках (флэш-память) и другие.

По форме записанной информации выделяют аналоговые и цифровые запоминающие устройства.

Постоянное запоминающее устройство

ПЗУ предназначено для хранения постоянной программной и справочной информации. Данные в ПЗУ заносятся при изготовлении. Информацию, хранящуюся в ПЗУ, можно только считывать, но не изменять.

В ПЗУ находятся:

- программа управления работой процессора;
 - программа запуска и останова компьютера;
 - программы тестирования устройств, проверяющие при каждом включении компьютера правильность работы его блоков;
 - программы управления дисплеем, клавиатурой, принтером, внешней памятью;
 - информация о том, где на диске находится операционная система.
- ПЗУ является энергонезависимой памятью, при отключении питания информация в нем сохраняется.

Оперативное запоминающее устройство

Оперативная память (также оперативное запоминающее устройство, ОЗУ) - предназначена для временного хранения данных и команд, необходимых процессору для выполнения им операций. Оперативная память передаёт процессору данные непосредственно, либо через кэш-память. Каждая ячейка оперативной памяти имеет свой индивидуальный адрес.

ОЗУ может изготавливаться как отдельный блок или входить в конструкцию однокристальной ЭВМ или микроконтроллера.

На сегодня наибольшее распространение имеют два вида ОЗУ: SRAM (Static RAM) и DRAM (Dynamic RAM).

SRAM - ОЗУ, собранное на триггерах, называется статической памятью с произвольным доступом или просто статической памятью. Достоинство этого вида памяти - скорость. Поскольку триггеры собраны на вентилях, а время задержки вентиля очень мало, то и переключение состояния триггера происходит очень быстро. Данный вид памяти не лишён недостатков. Во-первых, группа транзисторов, входящих в состав триггера, обходится дороже, даже если они вытравляются миллионами на одной кремниевой подложке. Кроме того, группа транзисторов занимает гораздо больше места, поскольку между транзисторами, которые образуют триггер, должны быть вытравлены линии связи.

DRAM - более экономичный вид памяти. Для хранения разряда (бита или трита) используется схема, состоящая из одного конденсатора и одного транзистора (в некоторых вариациях конденсаторов два). Такой вид памяти решает, во-первых, проблему дороговизны (один конденсатор и один транзистор дешевле нескольких транзисторов) и во-вторых, компактности (там, где в SRAM размещается один триггер, то есть один бит, можно уместить восемь конденсаторов и транзисторов). Есть и свои минусы. Во-первых, память на основе конденсаторов работает медленнее, поскольку если в SRAM изменение напряжения на входе триггера сразу же приводит к изменению его состояния, то для того чтобы установить в единицу один разряд (один бит) памяти на основе конденсатора, этот конденсатор нужно зарядить, а для того чтобы разряд установить в ноль, соответственно, разрядить. А это гораздо более длительные операции (в 10 и более раз), чем переключение триггера, даже если конденсатор имеет весьма небольшие размеры. Второй существенный минус - конденсаторы склонны к «стеканию» заряда; проще говоря, со временем конденсаторы разряжаются.

Причём разряжаются они тем быстрее, чем меньше их ёмкость. В связи с этим обстоятельством, дабы не потерять содержимое памяти, заряд конденсаторов необходимо регенерировать через определённый интервал времени - для восстановления. Регенерация выполняется путём считывания заряда (через транзистор). Контроллер памяти периодически приостанавливает все операции с памятью для регенерации её содержимого, что значительно снижает производительность данного вида ОЗУ. Память на конденсаторах получила своё название Dynamic RAM (динамическая память) как раз за то, что разряды в ней хранятся не статически, а «стекают» динамически во времени.

Жесткий магнитный диск

Накопитель на жёстких магнитных дисках или НЖМД (англ. Hard (Magnetic) Disk Drive), жёсткий диск - устройство хранения информации, основанное на принципе магнитной записи. Является основным накопителем данных в большинстве компьютеров.

Информация в НЖМД записывается на жёсткие (алюминиевые, керамические или стеклянные) пластины, покрытые слоем ферромагнитного материала, чаще всего двуокиси хрома. В НЖМД используется от одной до нескольких пластин на одной оси. Считывающие головки в рабочем режиме не касаются поверхности пластин благодаря прослойке набегающего потока воздуха, образующейся у поверхности при быстром вращении. Расстояние между головкой и диском составляет несколько нанометров, а отсутствие механического контакта обеспечивает долгий срок службы устройства. При отсутствии вращения дисков головки находятся у шпинделя или за пределами диска в безопасной зоне, где исключён их нештатный контакт с поверхностью дисков.

Основные характеристики жестких дисков:

Интерфейс (англ. interface) - совокупность линий связи, сигналов, посылаемых по этим линиям, технических средств, поддерживающих эти линии, и правил (протокола) обмена. Серийно выпускаемые жёсткие диски могут использовать интерфейсы ATA (он же IDE и PATA), SATA, SCSI, SAS, FireWire, USB, SDIO и Fibre Channel.

Ёмкость (англ. capacity) - количество данных, которые могут храниться накопителем. Ёмкость современных устройств достигает 2000 Гб (2 Тб). В отличие от принятой в информатике системы приставок, обозначающих кратную 1024 величину, производителями при обозначении ёмкости жёстких дисков используются величины, кратные 1000.

Физический размер (форм-фактор) (англ. dimension). Почти все современные накопители для персональных компьютеров и серверов имеют ширину либо 3,5, либо 2,5 дюйма. Также получили распространение форматы 1,8 дюйма, 1,3 дюйма, 1 дюйм и 0,85 дюйма. Прекращено производство накопителей в форм-факторах 8 и 5,25 дюймов.

Время произвольного доступа (англ. random access time) - время, за которое винчестер гарантированно выполнит операцию чтения или записи на

любом участке магнитного диска. Диапазон этого параметра невелик - от 2,5 до 16 мс.

Скорость вращения шпинделя (англ. spindle speed) - количество оборотов шпинделя в минуту. От этого параметра в значительной степени зависят время доступа и средняя скорость передачи данных. В настоящее время выпускаются винчестеры со следующими стандартными скоростями вращения: 4200, 5400 и 7200 (ноутбуки), 5400, 7200 и 10 000 (персональные компьютеры), 10 000 и 15 000 об/мин (серверы и высокопроизводительные рабочие станции).

Надёжность (англ. reliability) - определяется как среднее время наработки на отказ (MTBF).

Количество операций ввода-вывода в секунду - у современных дисков это около 50 оп./с при произвольном доступе к накопителю и около 100 оп./с при последовательном доступе.

Потребление энергии - важный фактор для мобильных устройств.

Уровень шума - шум, который производит механика накопителя при его работе. Указывается в децибелах. Тихими накопителями считаются устройства с уровнем шума около 26 дБ и ниже. Шум состоит из шума вращения шпинделя (в том числе аэродинамического) и шума позиционирования.

Сопrotивляемость ударам (англ. G-shock rating) - сопротивляемость накопителя резким скачкам давления или ударам, измеряется в единицах допустимой перегрузки во включённом и выключенном состоянии.

Скорость передачи данных (англ. Transfer Rate) при последовательном доступе:

- внутренняя зона диска: от 44,2 до 74,5 Мб/с;
- внешняя зона диска: от 60,0 до 111,4 Мб/с.

Объём буфера - буфером называется промежуточная память, предназначенная для сглаживания различий скорости чтения/записи и передачи по интерфейсу. В современных дисках он обычно варьируется от 8 до 64 Мб.

Жёсткий диск состоит из гермозоны и блока электроники.

Гермозона включает в себя корпус из прочного сплава, собственно диски (пластины) с магнитным покрытием, блок головок с устройством позиционирования, электропривод шпинделя.

Блок головок - пакет рычагов из пружинистой стали (по паре на каждый диск). Одним концом они закреплены на оси рядом с краем диска. На других концах (над дисками) закреплены головки.

Диски (пластины), как правило, изготовлены из металлического сплава. Хотя были попытки делать их из пластика и даже стекла, но такие пластины оказались хрупкими и недолговечными. Обе плоскости пластин, подобно магнитофонной ленте, покрыты тончайшей пылью ферромагнетика - окислов железа, марганца и других металлов. Точный состав и технология нанесения держатся в секрете. Большинство бюджетных устройств содержит 1 или 2 пластины, но существуют модели с большим числом пластин.

Диски жёстко закреплены на шпинделе. Во время работы шпиндель вращается со скоростью несколько тысяч оборотов в минуту. При такой скорости вблизи поверхности пластины создаётся мощный воздушный поток, который приподнимает головки и заставляет их парить над поверхностью пластины. Форма головок рассчитывается так, чтобы при работе обеспечить оптимальное расстояние от пластины. Пока диски не разогнались до скорости, необходимой для «взлёта» головок, парковочное устройство удерживает головки в зоне парковки. Это предотвращает повреждение головок и рабочей поверхности пластин. Шпиндельный двигатель жёсткого диска трехфазный, что обеспечивает стабильность вращения магнитных дисков, смонтированных на оси (шпинделе) двигателя. Статор двигателя содержит три обмотки, включенные звездой с отводом посередине, а ротор – постоянный секционный магнит. Для обеспечения малого биения на высоких оборотах в двигателе используются гидродинамические подшипники.

Устройство позиционирования головок состоит из неподвижной пары сильных неодимовых постоянных магнитов, а также катушки на подвижном блоке головок. Вопреки расхожему мнению, внутри гермозоны нет вакуума. Одни производители делают её герметичной (отсюда и название) и заполняют очищенным и осушенным воздухом или нейтральными газами, в частности, азотом; а для выравнивания давления устанавливают тонкую металлическую или пластиковую мембрану. Другие производители выравнивают давление через небольшое отверстие с фильтром, способным задерживать очень мелкие (несколько микрометров) частицы. Однако в этом случае выравнивается и влажность, а также могут проникнуть вредные газы. Выравнивание давления необходимо, чтобы предотвратить деформацию корпуса гермозоны при перепадах атмосферного давления и температуры, а также при прогреве устройства во время работы.

Пылинки, оказавшиеся при сборке в гермозоне и попавшие на поверхность диска, при вращении сносятся на ещё один фильтр – пылеуловитель.

Интерфейсный блок обеспечивает сопряжение электроники жёсткого диска с остальной системой.

Блок управления представляет собой систему управления, принимающую электрические сигналы позиционирования головок, и вырабатывающую управляющие воздействия приводом типа «звуковая катушка», коммутации информационных потоков с различных головок, управления работой всех остальных узлов (к примеру, управление скоростью вращения шпинделя), приёма и обработки сигналов с датчиков устройства (система датчиков может включать в себя одноосный акселерометр, используемый в качестве датчика удара, трёхосный акселерометр, используемый в качестве датчика свободного падения, датчик давления, датчик угловых ускорений, датчик температуры).

Блок ПЗУ хранит управляющие программы для блоков управления и цифровой обработки сигнала, а также служебную информацию винчестера.

Буферная память сглаживает разницу скоростей интерфейсной части и накопителя. Увеличение размера буферной памяти в некоторых случаях позволяет увеличить скорость работы накопителя.

Блок цифровой обработки сигнала осуществляет очистку считанного аналогового сигнала и его декодирование (извлечение цифровой информации). Для цифровой обработки применяются различные методы, например, метод PRML (Partial Response Maximum Likelihood - максимальное правдоподобие при неполном отклике). Осуществляется сравнение принятого сигнала с образцами. При этом выбирается образец, наиболее похожий по форме и временным характеристикам с декодируемым сигналом.

На заключительном этапе сборки устройства поверхности пластин форматируются - на них формируются дорожки и секторы. Конкретный способ определяется производителем и/или стандартом, но, как минимум, на каждую дорожку наносится магнитная метка, обозначающая её начало.

С целью адресации пространства поверхности пластин диска делятся на дорожки - концентрические кольцевые области. Каждая дорожка делится на равные отрезки - секторы.

Цилиндр - совокупность дорожек, равноотстоящих от центра, на всех рабочих поверхностях пластин жёсткого диска. Номер головки задает используемую рабочую поверхность (то есть конкретную дорожку из цилиндра), а номер сектора - конкретный сектор на дорожке.

При способе адресации CHS сектор адресуется по его физическому положению на диске 3 координатами - номером цилиндра, номером головки и номером сектора

При способе адресации LBA адрес блоков данных на носителе задаётся с помощью логического линейного адреса.

Оптические диски

Оптический диск (англ. optical disc) - собирательное название для носителей информации, выполненных в виде дисков, чтение с которых ведётся с помощью оптического излучения. Диск обычно плоский, его основа сделана из поликарбоната, на который нанесён специальный слой, который и служит для хранения информации. Для считывания информации используется обычно луч лазера, который направляется на специальный слой и отражается от него. При отражении луч модулируется мельчайшими выемками (питами, от англ. pit - ямка, углубление, рисунок 22) на специальном слое, на основании декодирования этих изменений устройством чтения восстанавливается записанная на диск информация. Информация на диске записывается в виде спиральной дорожки так называемых питов (углублений), выдавленных в поликарбонатной основе. Каждый пит имеет примерно 100 нм в глубину и 500 нм в ширину. Длина пита варьируется от 850 нм до 3,5 мкм. Промежутки между питами называются лендом. Шаг дорожек в спирали составляет 1,6 мкм.

Существует несколько видов оптических дисков: CD, DVD, Blu-Ray и др..

CD-ROM (англ. compact disc read-only memory) - разновидность компакт-дисков с записанными на них данными, доступными только для чтения. Изначально диск был разработан для хранения аудиозаписей, но впоследствии был доработан для хранения и других цифровых данных. В дальнейшем на базе CD-ROM были разработаны диски как с однократной, так и с многократной перезаписью (CD-R и CD-RW).

Компакт-диск представляет собой поликарбонатную подложку толщиной 1,2мм, покрытого тончайшим слоем металла (алюминий, золото, серебро и др.) и защитным слоем лака, на котором обычно наносится графическое представление содержания диска. Принцип считывания через подложку был принят, поскольку позволяет весьма просто и эффективно осуществить защиту информационной структуры и удалить её от внешней поверхности диска. Диаметр пучка на внешней поверхности диска составляет порядка 0,7 мм, что повышает помехоустойчивость системы к пыли и царапинам. Кроме того, на внешней поверхности имеется кольцевой выступ высотой 0,2 мм, позволяющий диску, положенному на ровную поверхность, не касаться этой поверхности. В центре диска расположено отверстие диаметром 15 мм. Вес диска без коробки составляет приблизительно 15,7 гр. Вес диска в обычной коробке приблизительно равен 74 гр.

Компакт-диски имеют в диаметре 12 см и изначально вмещали до 650 Мбайт информации. Однако, начиная приблизительно с 2000 года, всё большее распространение стали получать диски объёмом 700 Мбайт, впоследствии полностью вытеснившие диск объёмом 650 Мбайт. Встречаются и носители объёмом 800 мегабайт и даже больше, однако они могут не читаться на некоторых приводах компакт-дисков. Бывают также 8-сантиметровые диски, на которые вмещается около 140 или 210 Мб данных.

Различают диски только для чтения («алюминиевые»), CD-R - для однократной записи, CD-RW - для многократной записи. Диски последних двух типов предназначены для записи на специальных пишущих приводах.

Дальнейшим развитием CD-ROM-дисков стали диски DVD-ROM.

DVD (англ. Digital Versatile Disc) - цифровой многоцелевой диск - носитель информации, выполненный в виде диска, внешне схожий с компакт-диском, однако имеющий возможность хранить бóльший объём информации за счёт использования лазера с меньшей длиной волны, чем для обычных компакт-дисков.

Blu-ray Disc, BD (англ. blue ray disk) - формат оптического носителя, используемый для записи и хранения цифровых данных, включая видео высокой чёткости с повышенной плотностью. Стандарт Blu-ray был совместно разработан консорциумом BDA.

Blu-ray (буквально «синий-луч») получил своё название от использования для записи и чтения коротковолнового (405 нм) «синего» (технически сине-фиолетового) лазера. Однослойный диск Blu-ray (BD) может хранить 23,3/25/27 или 33 Гб, двухслойный диск может вместить 46,6/50/54 или 66 Гб.

Твердотельный накопитель

Твердотельный накопитель (англ. SSD, Solid State Drive, Solid State Disk) - энергонезависимое, перезаписываемое компьютерное запоминающее устройство без движущихся механических частей. Следует различать твердотельные накопители, основанные на использовании энергозависимой (RAM SSD) и энергонезависимой (NAND или Flash SSD) памяти.

Накопители RAM SSD, построенные на использовании энергозависимой памяти (такой же, какая используется в ОЗУ персонального компьютера) характеризуются сверхбыстрым чтением, записью и поиском информации. Основным их недостатком является чрезвычайно высокая стоимость. Используются, в основном, для ускорения работы крупных систем управления базами данных и мощных графических станций. Такие накопители, как правило, оснащены аккумуляторами для сохранения данных при потере питания, а более дорогие модели - системами резервного и/или оперативного копирования.

Накопители NAND SSD, построенные на использовании энергонезависимой памяти появились относительно недавно, но в связи с гораздо более низкой стоимостью начали уверенное завоевание рынка. До недавнего времени существенно уступали традиционным накопителям в чтении и записи, но компенсировали это (особенно при чтении) высокой скоростью поиска информации (сопоставимой со скоростью оперативной памяти). Сейчас уже выпускаются твердотельные накопители Flash со скоростью чтения и записи, сопоставимой с традиционными, и разработаны модели, существенно их превосходящие. Характеризуются относительно небольшими размерами и низким энергопотреблением. Уже практически полностью завоевали рынок ускорителей баз данных среднего уровня и начинают теснить традиционные диски в мобильных приложениях.

Преимущества по сравнению с жёсткими дисками:

- меньше время загрузки системы;
- отсутствие движущихся частей;
- производительность: скорость чтения и записи до 270 МБ/с;
- низкая потребляемая мощность;
- полное отсутствие шума от движущихся частей и охлаждающих вентиляторов;
- высокая механическая стойкость;
- широкий диапазон рабочих температур;
- практически устойчивое время считывания файлов вне зависимости от их расположения или фрагментации;
- малый размер и вес.

Флеш-память

Флеш-память (англ. Flash-Memory) - разновидность твердотельной полупроводниковой энергонезависимой перезаписываемой памяти.

Она может быть прочитана сколько угодно раз, но писать в такую память можно лишь ограниченное число раз (максимально - около миллиона циклов). Распространена флеш-память, выдерживающая около 100 тысяч

циклов перезаписи - намного больше, чем способна выдержать дискета или CD-RW.

Флеш-память хранит информацию в массиве транзисторов с плавающим затвором, называемых ячейками. В традиционных устройствах с одноуровневыми ячейками, каждая из них может хранить только один бит. Некоторые новые устройства с многоуровневыми ячейками могут хранить больше одного бита, используя разный уровень электрического заряда на плавающем затворе транзистора.

В основе типа флеш-памяти NOR лежит ИЛИ-НЕ элемент (англ. NOR), потому что в транзисторе с плавающим затвором низкое напряжение на затворе обозначает единицу.

Транзистор имеет два затвора: управляющий и плавающий. Последний полностью изолирован и способен удерживать электроны до 10 лет. В ячейке имеются также сток и исток. При программировании напряжением на управляющем затворе создаётся электрическое поле и возникает туннельный эффект. Некоторые электроны туннелируют через слой изолятора и попадают на плавающий затвор, где и будут пребывать. Заряд на плавающем затворе изменяет «ширину» канала сток-исток и его проводимость, что используется при чтении.

Программирование и чтение ячеек сильно различаются в энергопотреблении: устройства флеш-памяти потребляют достаточно большой ток при записи, тогда как при чтении затраты энергии малы.

Для стирания информации на управляющий затвор подаётся высокое отрицательное напряжение, и электроны с плавающего затвора переходят (туннелируют) на исток.

В NOR-архитектуре к каждому транзистору необходимо подвести индивидуальный контакт, что увеличивает размеры схемы. Эта проблема решается с помощью NAND-архитектуры.

В основе NAND-типа лежит И-НЕ элемент (англ. NAND). Принцип работы такой же, от NOR-типа отличается только размещением ячеек и их контактами. В результате уже не требуется подводить индивидуальный контакт к каждой ячейке, так что размер и стоимость NAND-чипа может быть существенно меньше. Также запись и стирание происходит быстрее. Однако эта архитектура не позволяет обращаться к произвольной ячейке.

NAND и NOR-архитектуры сейчас существуют параллельно и не конкурируют друг с другом, поскольку находят применение в разных областях хранения данных.

Существуют несколько типов карт памяти, используемых в портативных устройствах:

Compact Flash - карты памяти CF являются старейшим стандартом карт флеш-памяти. Первая CF карта была произведена корпорацией SanDisk в 1994 году. Чаще всего в наши дни он применяется в профессиональном фото и видео оборудовании, так как ввиду своих размеров (43×36×3,3 мм) слот расширения для Compact Flash-карт физически проблематично разместить в мобильных телефонах или MP3-плеерах.

Multimedia Card. Карта в формате MMC имеет небольшой размер - 24×32×1,4 мм. Разработана совместно компаниями SanDisk и Siemens. MMC содержит контроллер памяти и обладает высокой совместимостью с устройствами самого различного типа. В большинстве случаев карты MMC поддерживаются устройствами со слотом SD.

MMCmicro - миниатюрная карта памяти для мобильных устройств с размерами 14×12×1,1 мм. Для обеспечения совместимости со стандартным слотом MMC необходимо использовать переходник.

SD Card (Secure Digital Card) является дальнейшим развитием стандарта MMC. По размерам и характеристикам карты SD очень похожи на MMC, только чуть толще (32×24×2,1 мм). Основное отличие от MMC - технология защиты авторских прав: карта имеет криптозащиту от несанкционированного копирования, повышенную защиту информации от случайного стирания или разрушения и механический переключатель защиты от записи.

SDHC (SD High Capacity): Старые карты SD (SD 1.0, SD 1.1) и новые SDHC (SD 2.0) (SD High Capacity) и устройства их чтения различаются ограничением на максимальную ёмкость носителя, 4 Гб для SD и 32 Гб для SD High Capacity (Высокой Ёмкости). Устройства чтения SDHC обратно совместимы с SD, то есть SD-карта будет без проблем прочитана в устройстве чтения SDHC, но в устройстве SD карта SDHC не будет читаться вовсе. Оба варианта могут быть представлены в любом из трёх форматов физических размеров (стандартный, mini и micro).

MiniSD (Mini Secure Digital Card): От стандартных карт Secure Digital отличаются меньшими размерами 21,5×20×1,4 мм. Для обеспечения работы карты в устройствах, оснащённых обычным SD-слотом, используется адаптер.

MicroSD (Micro Secure Digital Card): являются на настоящий момент самыми компактными съёмными устройствами флеш-памяти (11×15×1 мм). Используются, в первую очередь, в мобильных телефонах, коммуникаторах, и т. п., так как, благодаря своей компактности, позволяют существенно расширить память устройства, не увеличивая при этом его размеры.

Memory Stick Duo: данный стандарт памяти разрабатывался и поддерживается компанией Sony. Корпус достаточно прочный. На данный момент - это самая дорогая память из всех представленных. Memory Stick Duo был разработан на базе широко распространённого стандарта Memory Stick от той же Sony, отличается малыми размерами (20×31×1,6 мм).

Memory Stick Micro (M2): Данный формат является конкурентом формата microSD (по аналогичному размеру), сохраняя преимущества карт памяти Sony.

xD-Picture Card: используются в цифровых фотоаппаратах фирм Olympus, Fujifilm и некоторых других.

8. ПОСТОЯННОЕ ЭНЕРГОНЕЗАВИСИМОЕ ЗАПОМИНАЮЩЕЕ УСТРОЙСТВО ROM

Постоянные запоминающие устройства (ПЗУ). Очень часто в различных применениях требуется хранение информации, которая не изменяется в процессе эксплуатации устройства. Это такая информация, как программы в микроконтроллерах, начальные загрузчики и BIOS в компьютерах, таблицы коэффициентов цифровых фильтров в сигнальных процессорах. Практически всегда эта информация не требуется одновременно, поэтому простейшие устройства для запоминания постоянной информации можно построить на мультиплексорах. Схема такого постоянного запоминающего устройства (ПЗУ) приведена на рис.1.

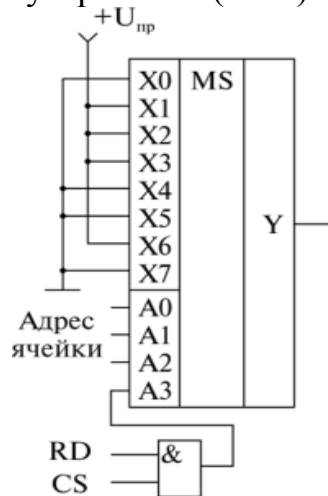


Рис. 1. Схема ПЗУ, построенная на мультиплексоре

В этой схеме построено постоянное запоминающее устройство на восемь одноразрядных ячеек. Запоминание конкретного бита в одноразрядную ячейку производится запайкой провода к источнику питания (запись единицы) или запайкой провода к корпусу (запись нуля). На принципиальных схемах такое устройство обозначается, как показано на рис. 2.

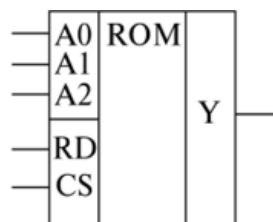


Рис. 2. Обозначение ПЗУ на принципиальных схемах

Для того чтобы увеличить разрядность ячейки памяти ПЗУ, эти микросхемы можно соединять параллельно (выходы и записанная информация, естественно, остаются независимыми). Схема параллельного соединения одноразрядных ПЗУ приведена на рис. 3.

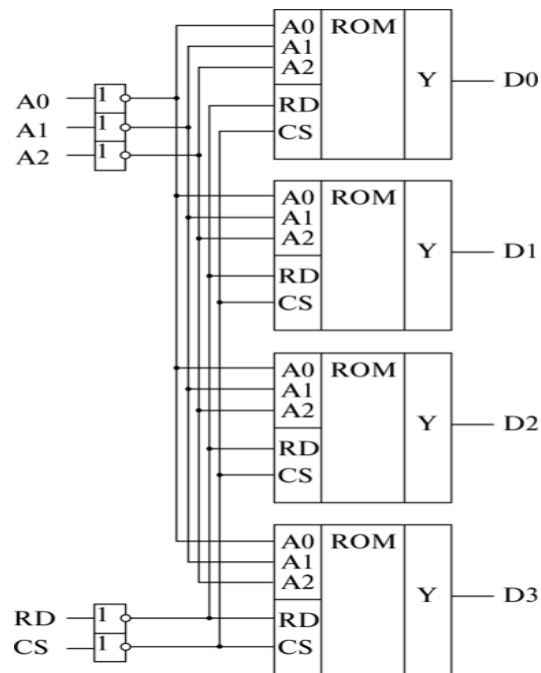


Рис. 3. Схема многоразрядного ПЗУ

В реальных ПЗУ запись информации производится при помощи последней операции производства микросхемы — металлизации. Металлизация производится при помощи маски, поэтому такие ПЗУ получили название масочных ПЗУ. Еще одно отличие реальных микросхем от упрощенной модели, приведенной выше, — это использование кроме мультиплексора еще и демultipлексора. Такое решение позволяет превратить одномерную запоминающую структуру в многомерную и тем самым существенно сократить объем схемы дешифратора, необходимого для работы схемы ПЗУ. Эта ситуация иллюстрируется рис. 4.

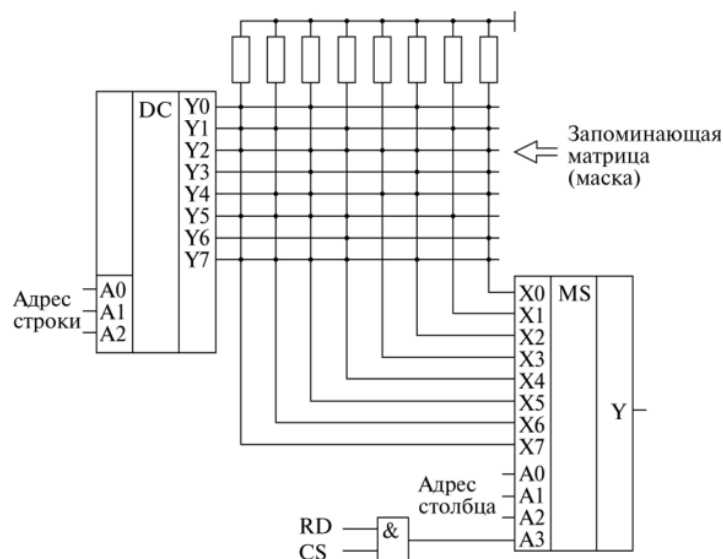


Рис. 4. Схема масочного ПЗУ

Масочные ПЗУ изображаются на принципиальных схемах, как показано на рис. 5. Адреса ячеек памяти в этой микросхеме подаются на выводы А0—А9. Микросхема выбирается сигналом CS. При помощи этого сигнала можно наращивать объем ПЗУ. Чтение микросхемы производится сигналом RD.

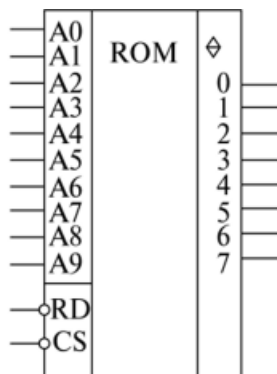


Рис. 5. Обозначение масочного ПЗУ на принципиальных схемах

Программирование масочного ПЗУ производится на заводе-изготовителе, что очень неудобно для мелких и средних серий производства, не говоря уже о стадии разработки устройства. Естественно, что для крупносерийного производства масочные ПЗУ являются самым дешевым видом ПЗУ и поэтому широко применяются в настоящее время. Для мелких и средних серий производства радиоаппаратуры были разработаны микросхемы, которые можно программировать в специальных устройствах — программаторах. В этих микросхемах постоянное соединение проводников в запоминающей матрице заменяется плавкими перемычками, изготовленными из поликристаллического кремния. При производстве микросхемы изготавливаются все перемычки, что эквивалентно записи во все ячейки памяти логических единиц. В процессе программирования на выводы питания и выходы микросхемы подается повышенное питание. При этом если на выход микросхемы подается напряжение питания (логическая единица), то через перемычку ток протекать не будет и перемычка останется неповрежденной. Если же на выход микросхемы подать низкий уровень напряжения (присоединить к корпусу), то через перемычку будет протекать ток, который испарит эту перемычку и при последующем считывании информации из этой ячейки будет считываться логический ноль.

Такие микросхемы называются программируемыми ПЗУ (ППЗУ) и изображаются на принципиальных схемах, как показано на рис. 6. В качестве примера можно назвать микросхемы 155РЕ 3, 556РТ 4, 556РТ 8 и др.

Программируемые ПЗУ оказались очень удобны при мелкосерийном и среднесерийном производстве. Однако при разработке радиоэлектронных устройств часто приходится менять записываемую в ПЗУ программу. ППЗУ при этом невозможно использовать повторно, поэтому раз записанное ПЗУ при ошибочной или промежуточной программе приходится выкидывать, что,

естественно, повышает стоимость разработки аппаратуры. Для устранения этого недостатка был разработан еще один вид ПЗУ, который может стираться и программироваться заново.

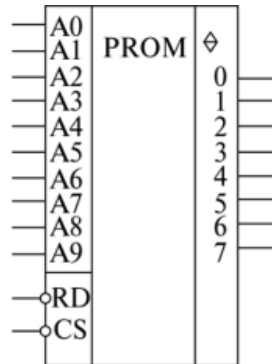


Рис. 6. Обозначение программируемого ПЗУ на принципиальных схемах

Структурная схема ПЗУ не отличается от описанного ранее масочного ПЗУ. В репрограммируемых ПЗУ стирание ранее записанной информации осуществляется ультрафиолетовым излучением. Для того чтобы этот свет мог беспрепятственно проходить к полупроводниковому кристаллу, в корпус микросхемы встраивается окошко из кварцевого стекла.

В качестве примера таких микросхем можно назвать микросхемы серии 573 российского производства, микросхемы серий 27сXXX зарубежного производства. В этих микросхемах чаще всего хранятся программы BIOS универсальных компьютеров. Репрограммируемые ПЗУ (РПЗУ) изображаются на принципиальных схемах, как показано на рис. 7.

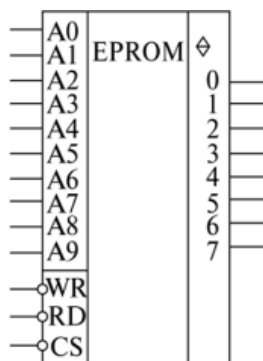


Рис. 7. Обозначение репрограммируемого ПЗУ на принципиальных схемах

Высокая стоимость корпусов с кварцевым окошком, а также малое количество циклов записи-стирания привели к поиску способов стирания информации из ППЗУ электрическим способом. На этом пути встретилось много трудностей, которые к настоящему времени практически решены. Сейчас достаточно широко распространены микросхемы с электрическим стиранием информации. В качестве запоминающей ячейки в них

используются такие же ячейки, как и в РПЗУ, но они стираются электрическим потенциалом, поэтому количество циклов записи-стирания для этих микросхем достигает 1 млн раз. Время стирания ячейки памяти в таких микросхемах уменьшается до 10 мс. Схема управления для таких микросхем получилась сложная, поэтому наметилось два направления развития этих микросхем:

- ЕСППЗУ;
- FLASH-ПЗУ.

Электрически стираемые ППЗУ (ЭСППЗУ) дороже и меньше по объему, но зато позволяют перезаписывать каждую ячейку памяти отдельно. В результате эти микросхемы обладают максимальным количеством циклов записи-стирания. Область применения электрически стираемых ПЗУ — хранение данных, которые не должны стираться при выключении питания. К таким микросхемам относятся отечественные микросхемы 573РРЗ, 558РР и зарубежные микросхемы серии 28сХХ. Электрически стираемые ПЗУ обозначаются на схемах, как показано на рис. 8.

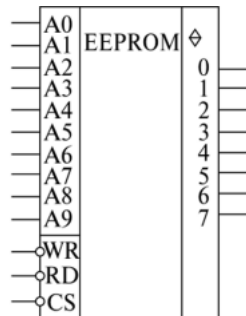


Рис. 8. Обозначение электрически стираемого ПЗУ на принципиальных схемах

В последнее время наметилась тенденция уменьшения габаритов ЭСППЗУ за счет уменьшения количества внешних ножек микросхем. Для этого адрес и данные передаются в микросхему и из микросхемы через последовательный порт. При этом используются два вида последовательных портов — SPI-порт и I2C-порт (микросхемы 93сХХ и 24сХХ серий соответственно). Зарубежной серии 24сХХ соответствует отечественная серия микросхем 558РРХ.

FLASH-ПЗУ отличаются от ЭСППЗУ тем, что стирание производится не каждой ячейки отдельно, а всей микросхемы в целом или блока запоминающей матрицы этой микросхемы, как это делалось в РПЗУ (рис. 9).

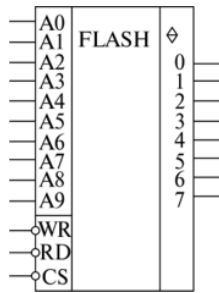


Рис. 9. Обозначение FLASH-памяти
на принципиальных схемах

При обращении к постоянному запоминающему устройству сначала необходимо выставить адрес ячейки памяти на шине адреса, а затем произвести операцию чтения из микросхемы.

Программируемые ПЗУ (ППЗУ)

Программируемая память, или память типа PROM (Programmable ROM), позволяет пользователю устранить или создать перемычки в исходной заготовке микросхемы памяти. Этот процесс называется *программированием* микросхемы памяти.

В микросхемах с *устраняемыми* плавкими перемычками в исходной заготовке имеются все перемычки. В процессе программирования часть из них расплавляется импульсами тока достаточно большой амплитуды и длительности. Плавкие перемычки изготавливаются из нихрома, поликремния или титаната вольфрама и обычно включаются в электроды диодов или транзисторов. Аналогичным образом осуществляется программирование биполярных транзисторов (в том числе и многоэмиттерных) с плавкими перемычками, включенными в эмиттерные цепи.

В микросхемах с *создаваемыми* перемычками элемент памяти в исходной заготовке представляет собой два встречно включенных диода или тонкие диэлектрические слои и имеет очень большое сопротивление. В процессе программирования на элемент памяти подается повышенное напряжение, в результате чего происходит пробой элемента с образованием короткого замыкания.

Так как микросхемы PROM программируются один раз, их часто называют микросхемами OTP (One Time Programmable). При изменении программы старая микросхема должна быть заменена новой.

Микросхемы PROM после изготовления содержат двоичные единицы (или нули). В процессе программирования, который часто называется прожигом и выполняется с помощью специального программирующего устройства, в нее записываются нули.

В зависимости от емкости памяти микросхемы и применяемого алгоритма процесс программирования PROM занимает от нескольких секунд до нескольких минут. Следует отметить, что для изменения BIOS в

современных компьютерах вместо PROM используются микросхемы Flash ROM.

Микросхемы PROM, как и масочные, практически нечувствительны к электромагнитным полям. Несанкционированное изменение их содержимого в устройстве исключено.

9. ВИДЫ НАКОПИТЕЛЕЙ ИНФОРМАЦИИ

Флэш-память – это особый вид энергонезависимой перезаписываемой полупроводниковой твердотельной памяти.

Впервые флэш-память была разработана компанией Toshiba в 1984 году. В 1988 году компания Intel разработала собственный вариант флэш-памяти. Полное историческое название флэш-памяти **Flash Erase Electronically Electrically Programmable ROM** – **электрически стираемое перепрограммируемое ПЗУ**. Считается, что название Flash было дано компанией Toshiba во время разработки первых микросхем флэш-памяти как характеристика скорости стирания информации в микросхеме («in a flash» - мгновенно).

Главной отличительной особенностью флэш является возможность перепрограммирования при подключении к стандартной системной шине микропроцессора. Число циклов репрограммирования флэш-памяти хотя и велико (от 10 000 до 1 000 000 раз), но ограничено. Это связано с тем, что перезапись идёт через стирание, которое приводит к износу микросхемы. Для увеличения долговечности флэш-памяти в её работе применяются специальные алгоритмы для «разравнивания» числа перезаписей по всем блокам микросхемы.

В отличие от жёстких дисков, CD- и DVD-ROM, во флэш-носителях нет движущихся частей, поэтому их и называют твердотельными. По оценкам производителей, информация на флэш может храниться от 20 до 100 лет. Благодаря компактным размерам, высокой степени надёжности и низкому энергопотреблению, флэш-память активно используется в современных вычислительных машинах в качестве съёмного носителя информации.

Одним из элементов структуры флэш-памяти является накопитель (матрица запоминающих элементов). По организации массива запоминающих элементов различают микросхемы флэш-памяти следующих типов:

1) *Bulk Erase* – стирание допустимо только для всего массива запоминающих элементов.

2) *Boot Block* – массив запоминающих элементов разделён на несколько блоков разного размера, содержимое которых может осуществляться независимо. Среди блоков есть так называемый загрузочный блок, содержимое которого аппаратно защищено от случайного стирания. В нём хранится программное обеспечение для правильной эксплуатации и инициализации микросхемы.

3) *Flash File* – массив запоминающих элементов разделён на несколько равноправных блоков одинакового размера, содержимое которых может стираться независимо. Файловая флэш-память ориентирована на замену жёстких дисков, поэтому её блоки являются аналогами секторов магнитных дисков.

Базовым элементом матрица является флэш-ячейка, которая состоит из транзистора особой архитектуры – полевого двухзатворного транзистора. Ячейки флэш-памяти можно соединить последовательно (в цепочку) или параллельно. В первом случае логическая организация памяти называется NAND (Not AND, НЕ-И), во втором – NOR (Not OR, НЕ-ИЛИ).

Процесс записи информации для ячеек NOR и NAND различный. В ячейках NOR запись осуществляется *методом инжекции* (когда электронам даётся дополнительная энергия для преодоления потенциального барьера перед изолированным затвором). В ячейках NAND запись производится *путём туннелирования* электронов (когда электроны переходят сквозь барьер). Стирание информации в ячейках обоих типов осуществляется механизмом туннельного перехода.

В чистом виде флэш-память NOR похожа на обычную оперативную память, а память NAND больше напоминает дисковый накопитель с блочным доступом. При существенно большей скорости чтения данных память NOR имеет значительно меньшую скорость стирания и несколько меньшую скорость записи по сравнению с памятью NAND. Однако память NOR позволяет исполнять записанный код, а программы из NAND перед исполнением всегда необходимо предварительно загружать в оперативную память. Ячейка NAND имеет значительно меньшие размеры в сравнении с ячейкой NOR. Хотя первоначально была более распространена память NOR в виде оперативной памяти для вычислительных машин и других программируемых устройств, то сегодня широкое применение получила память NAND в виде карт памяти и твердотельных носителей. Однако, для работы, требующей побайтового произвольного доступа (например, для хранения программного кода), память NOR предпочтительней. Следует отметить, что существуют гибридные решения, в одном корпусе объединяющие разные типы памяти.

Одна ячейка флэш-памяти содержит один транзистор, который в простейшем случае хранит один бит информации. Такие ячейки называются **одноуровневыми (SLC – Single Level Cell)**. Создание **многоуровневой** ячейки или ячейки с **многоуровневым кодированием (MLC – Multi Level Cell)** позволило хранить на одном транзисторе два бита информации. В качестве опытных образцов существуют 4-битовые ячейки. Компания Intel в 1997 году /4/ представила флэш-память с 2-битовыми ячейками, которая получила название Strata Flash.

Ячейки MLC применяются в памяти NOR, но наиболее популярны в памяти NAND. Память SLC NAND, в сравнении с MLC NAND, имеет более высокие скорости передачи данных, меньшее энергопотребление и повышенную надёжность. Однако, MLC NAND имеет большую ёмкость и меньшую цену.

Для согласования выходного интерфейса флэш-памяти с внешней шиной используется контроллер, выполненный в виде отдельной микросхемы либо встроенный в микросхему флэш-памяти.

У флэш-памяти перед другими накопителями (жесткие диски и оптические накопители) типа ПЗУ есть как свои преимущества, так и свои недостатки, с которыми вы можете познакомиться из таблицы расположенной ниже.

Тип ПЗУ	Преимущества	Недостатки
Жесткий диск	Большой объем хранимой информации. Высокая скорость работы. Дешевизна хранения данных (в расчете на 1 Мбайт).	Большие габариты. Чувствительность к вибрации. Тепловыделение. Шум.
Оптический диск	Удобство транспортировки. Дешевизна хранения информации. Возможность тиражирования.	Небольшой объем. Нужно считывающее устройство. Ограничения при операциях (чтение, запись). Невысокая скорость работы. Чувствительность к вибрации. Шум.
Флэш-память	Высокая скорость доступа к данным. Экономное энергопотребление. Устойчивость к вибрациям. Удобство подключения к компьютеру. Компактные размеры.	Ограниченное количество циклов записи.

Принцип работы флэш-памяти.

Элементарная ячейка хранения данных флэш-памяти представляет из себя транзистор с плавающим затвором. Особенность такого транзистора в том, что он умеет удерживать электроны (заряд). Вот на его основе и разработаны основные типы флэш-памяти NAND и NOR. Конкуренции между ними нет, потому что каждый из типов обладает своим преимуществом и недостатком. Кстати, на их основе строят гибридные версии такие как DiNOR и superAND.

Во флэш-памяти производители используют два типа ячеек памяти MLC и SLC. Флэш-память с MLC (Multi-level cell — многоуровневые ячейки памяти) ячейки более емкие и дешевые, но они с большим временем доступа и меньшим количеством циклов записи/стирания (около 10000). Флэш-память, которая содержит в себе SLC (Single-level cell — одноуровневые ячейки памяти) ячейки имеет максимальное количество циклов записи/стирания (100000) и обладают меньшим временем доступа. Изменение заряда (запись/стирание) выполняется приложением между затвором и истоком большого потенциала, чтобы напряженность электрического поля в тонком диэлектрике между каналом транзистора и карманом оказалась достаточна для возникновения туннельного эффекта. Для усиления эффекта тунеллирования электронов в карман при записи применяется небольшое ускорение электронов путем пропускания тока через канал полевого транзистора. Принцип работы флэш-памяти основан на изменении и регистрации электрического заряда в изолированной области («карман») полупроводниковой структуры. Чтение выполняется полевым транзистором,

для которого карман выполняет роль затвора. Потенциал плавающего затвора изменяет пороговые характеристики транзистора, что и регистрируется цепями чтения. Эта конструкция снабжается элементами, которые позволяют ей работать в большом массиве таких же ячеек.

Накопители на жестких магнитных дисках (НЖМД, жесткие диски, Hard Disk Drive — HDD) представляют собой устройства, предназначенные для длительного хранения информации. В качестве накопителей на жестких магнитных дисках широкое распространение в ПК получили накопители типа *винчестер*. Термин «винчестер» является жаргонным названием первой модели жесткого диска емкостью 16 Кбайт (IBM, 1973 год), имевшего 30 дорожек по 30 секторов, что случайно совпало с калибром 30/30 известного охотничьего ружья *eutwester*. В этих накопителях один или несколько жестких дисков, изготовленных из сплавов алюминия или из керамики и покрытых ферролаком, вместе с блоком магнитных головок считывания-записи помещены в герметически закрытый корпус. Под дисками расположен двигатель, обеспечивающий вращение дисков, а слева и справа — поворотный позиционер с коромыслом, управляющим движением магнитных головок по спиральной дуге для их установки на нужный цилиндр. Емкость винчестеров благодаря чрезвычайно плотной записи, выполняемой магниторезистивными головками в таких герметических конструкциях, достигает нескольких десятков гигабайтов; быстродействие их также весьма высокое: время доступа от 5 мс, трансфер до 6 Гбайт/с. Магниторезистивные технологии обеспечивают чрезвычайно высокую плотность записи, позволяющую размещать 2-3 Гбайт данных на одну пластину (диск). Появление же головок с гигантским магниторезистивным эффектом (GMR — Giant Magnetic Resistance) еще более увеличило плотность записи — возможная емкость одной пластины возросла до 6,4 Гбайт.

НЖМД весьма разнообразны. Диаметр дисков чаще всего 3,5 дюйма (89 мм). Наиболее распространенная высота корпуса дисководов: 25 мм — у настольных ПК, 41 мм — у машин-серверов, 12 мм — у портативных ПК, существуют и другие. Внешние дорожки диска длиннее внутренних. Поэтому в современных жестких дисках используется метод зонной записи. В этом случае все пространство диска делится на несколько зон, причем во внешних зонах секторов размещается больше данных, чем во внутренних. Это, в частности, позволило увеличить емкость жестких дисков примерно на 30 %.

Накопители на компакт-дисках CD-ROM, CD-R и CD-RW относятся к оптическим накопителям информации, чтение которой и запись (только для накопителей CD-R и CD-RW) производятся лучом лазера.

Накопитель на **CD-ROM** предназначен для хранения и чтения информации. Аббревиатура CD-ROM (CompactDiskRead-OnlyMemory) означает “компакт диск только для чтения”. Информация на диске представляется в виде последовательности углублений и выступов, расположенных на спиральной дорожке, выходящей из области вблизи оси диска. Углубления и выступы наносятся промышленным способом путем

штамповки заготовок дисков. Выступ означает значение двоичной цифры “1”, углубление - “0”. На CD-ROM размещается 780 Мбайт информации. Скорость считывания информации первых CD-ROM равнялась 150 Кб/с. Скорость считывания последующих моделей накопителей стала обозначаться и рассчитываться как xN , где N – множитель, на который следует умножить первоначальную скорость, чтобы получить искомую. Таким образом запись на накопителе “x52” означает скорость чтения в 52 раза большую, чем скорость считывания первого CD-ROM.

Типы.

CD-ROM — самый простой вид cd-привода, предназначенный только для чтения cd-дисков.

CD-RW — такой же, как и предыдущий, но способен записывать только на CD-R/RW-диски.

ЛИТЕРАТУРА

1. Цифровые устройства и микропроцессоры: учебное пособие / А.В. Микушин, А.М. Сажнев, В.И. Сединин. – СПб.: БХВ-Петербург, 2010. – 832 с.
2. Технические средства информатизации: учебник для студ. учреждений сред. проф. образования / Е. И. Гребенюк, Н.А.Гребенюк. – 9-е изд., стер. – М.: Издательский центр «Академия», 2014. – 352 с.
3. Арифметические и логические основы компьютера: учебно-методические указания / Н.М. Фатеева, О.А. Возилкина, Н.В. Тумбаева. Барнаул: Изд-во АГАУ, 2008. – 53 с.
4. Устройство персонального компьютера : учеб.-метод. пособие / А.Б. Крылов, М.А. Шеламова. – Мн.: БГМУ, 2006. – 62 с.

Учебное издание

**АППАРАТНЫЕ СРЕДСТВА
ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ
ДЛЯ ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Учебно-методическое пособие

Составитель: **Контылева** Елена Александровна

В авторской редакции

Изд. № 36/2022. Объем 4 п.л. Усл. печ. л. 3,72. Уч.-изд. л. 3,92.
РИИЦМ ФГАОУ ВО «Севастопольский государственный университет»