

## Лекция 1

**При классификации программ** принято деление на прикладные или проблемные пользовательские и программы обеспечивающие функционирование работы комплекса систем в автономном режиме.

**Прикладные программы** — наборы долговременных библиотек программ, используемых для решения задач из конкретной области применения техники.

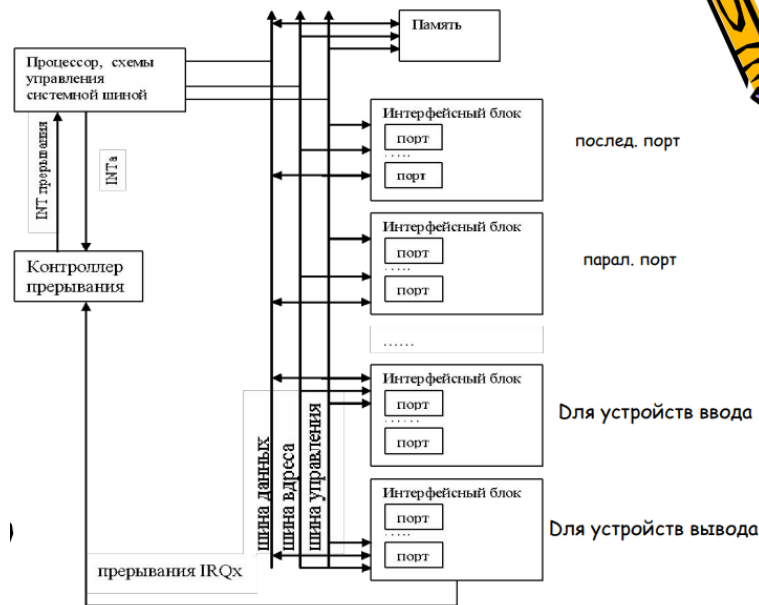
**Системные программы** используются для разработки новых программ, модификации уже существующих программ и выполнения программ автономным способом.

**Управляющие системные программы**, которые обеспечивают стабильность работы вычислительных систем, управляют процессами обработки, входят в ядро операционной системы, постоянно находятся в оперативной памяти, называются резидентными. А управляющие системные программы, которые загружаются в оперативную память перед их выполнением, называются транзитивными.

**Системные обрабатывающие программы** выполняются как специальное приложение и используются для разработки новых модификаций существующих программ.

**Архитектура ПК** включает в себя структурную организацию, то есть набор блоков и устройств, объединённых в вычислительную систему, и функциональную организацию, обеспечивающую работу этих блоков.

## Архитектура ПК



**Архитектура ПК** с точки зрения программиста — набор доступных блоков устройств.

**Современные ПК** имеют магистрально-модульный принцип построения, то есть к единой магистрали — системной шине подключены различные устройства.

**Шина** — набор линий, по которым информация передаётся от одного из источников к одному или нескольким приёмникам.

**Существует три типа шин:** адресная, данных и шина управления. По адресной шине информация передаётся от процессора, шина данных двунаправлена, то есть данные передаются от и к процессору, а шина управления включает в себя однонаправленные и двунаправленные каналы связи.

**Процессор** работает существенно быстрее внешних устройств, поэтому для организации параллельной работы процессора и внешних устройств в архитектуру ПК включены: канал прямого доступа к памяти и информационные блоки (устройство управления внешними устройствами).

**Чтобы синхронизировать работу внешних устройств и процессора** используется система прерывания. Если некоторому устройству требуется работа процессора, то это устройство посылает сигнал прерывания,

он проходит через контролер прерывания, если условия выполнены, то контроллер посылает процессору прерывание, процессор обрабатывает его и возвращает устройству выполнение внешним устройством.

**Существуют различные типы и классификации** прерываний, они бывают внешние и внутренние, маскируемые и немаскируемые.

**Процессор с точки зрения** программиста — набор программно доступных средств.

**Х86 процессор** при выключённом питании устанавливается в реальный режим работы оперативной памяти и процессора, но реальная система переводит его в защищённый режим, обеспечивающий многозадачность и ресурсы для этих задач. Начиная с 386 процессора доступны 16 основных регистров, 11 регистров для работы с мультимедиа и сопроцессором и некоторые управляющие регистры.

**Регистры общего назначения** могут использоваться для хранения адресов, данных и команд. При работе с 16-ти разрядными данными их имена: AX, BX, CX, DX.

**Для процессора** минимальной единицей информации является байт, он может работать с регистрами: AL, AH, BL, BH, DL, DH. Эти регистры имеют их собственные имена, отражающие их назначение.

**AX** — аккумулятор, в него записывается результат.

**BX** — базовый регистр, используется при адресации операндов по базе.

**CX** — счётчик, автоматически используется для организации циклов, работы со стеком.

**DX** — регистр данных.

## Регистры указателей и индексов

**Регистры индексов** используется для сложной адресации операндов, а регистры указателей SP, BP используются для работы со стеком.

**Сегментные регистры.** Рассматриваемый процессор может работать с оперативной памятью, как с 1 непрерывным массивом данных (flat), и памятью, разделённой на сегменты, в этом случае адрес байта состоит из 2-х частей: адрес начала сегмента и адрес внутри сегмента. И для получения адреса начала сегмента используются сегментные регистры DS, ES, FS, GS, CS, SS (16-ти разрядные).

**Операционная система** может размещать сегменты в любом месте оперативной памяти и даже временно на жёстком диске.

**Сегментных регистров 6**, но это не значит, что программа может использовать только 6 сегментов, программист может изменить содержимое сегментного регистра и попасть на другой адрес.

**Сегментный регистр называют** селектором, а с каждым селектором связан программно недоступный регистр — дескриптор и в защищённом режиме именно в дескрипторе находится адрес начала сегмента, его размер и дополнительная информация.

**В защищённом режиме** размер сегмента  $\leq 4\text{Гб}$ , а в реальном режиме размер сегмента фиксирован и равен 64Кб и в сегментном регистре находятся старшие цифры 16-тиричного адреса начала сегмента. Адрес сегмента всегда кратен 16 и поэтому младшие цифры равны 0.

**4 сегментных регистра** DS, ES, FS, GS используются для хранения сегмента данных. CS содержит адрес кодового сегмента, SS — стекового сегмента.

**Сегмент стека** реализуется особым образом, адрес начала сегмента стека определяется автоматически ОПС и записывается в SS, а при добавлении элемента в стек, указатель на вершину стека SP уменьшается.

**При работе с памятью** в режиме flat программы хранятся в младших адресах, а стек в старших.

**Стек используется** для работы с подпрограммами, в него записываются фактические параметры, а если программист хочет хранить локальные параметры, тогда после загрузки в стек фактических параметров, содержимое регистра Sp записывается в BP и тогда обращение к фактическим параметрам реализуется по формуле  $BP+k$ , а к локальным  $BP-n$ , где n и k вычисляет сам программист, исходя из количества параметров и их размера.

**IP** — счётчик команд указатель команд, в нём содержится смещение для следующей исполняемой команды.

**Регистр флагов FLAGS** (32-х разрядный), определяет состояние программы и процессора в каждый текущий момент времени.

31	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	AC	VM	RF		NF	IOPL	OF	DF	IF	TF	SF	ZF		AF		PF		CF		

- CF - перенос
- PF - четность
- AF - полуперенос
- ZF - флаг нуля
- SF - флаг знака
- TF - флаг трассировки
- IF - флаг прерывания
- DF - флаг направления
- OF - флаг переполнения

А в защищённом режиме добавляется ещё 5 флагов:

- AC - флаг выравнивания операндов
- VM - флаг виртуальных машин
- RF - флаг маскирования прерывания
- NT - флаг вложенной задачи
- IOPL - уровень привилегий ввода/вывода.

**Регистры** 1, 5, 15, 19-31 не используются.

**CF** — флаг переноса, устанавливается в 1, если в результате выполнения операций произошёл перенос из старшего разряда.

**PF** — флаг чётности, устанавливается в 1, если в младшем байте результата чётное число единиц.

**AF** — флаг полупереноса, устанавливается в 1, если при сложении произошёл перенос из третьего разряда в 4, а при вычитании из 4 в 3.

**ZF** — флаг нуля, устанавливается в 1, если результат равен 0.

**SF** — флаг знака, всегда равен знаку операнда ( $+$   $\rightarrow$  1, 0 или  $-$   $\rightarrow$  0).

**TF** — флаг трассировки, установленный в 1, переводит процессор в режим отладки.

**IF** — флаг прерывания, установленный в 1, может маскировать какое-то прерывание.

**DF** — флаг направления, определяет режим работы со строками, установленный в 1 приводит к обработке строк от старшего адреса к младшему,

автоматически уменьшая содержимое регистров индексов на размер операндов, при утановлении флага в 0, всё происходит наоборот.

**ОФ** — флаг переполнения, устанавливается в 1, если результат не уместился.

## Лекция 2

**Регистр** — набор из  $n$  устройств, способный хранить  $n$ -разрядное двоичное число.

**Оперативная память** состоит из байтов, байт состоит из 8 информационных битов-разрядов, разряды с 0 по 3 называются цифровой частью байта, а с 4 по 7 зонной частью байта.

**Оперативная память** 32-х разрядного процессора может достигать 4Гб с адресами от 0 до  $2^{32}-1$ , что в 16-ричной системе счисления записывается от 00000000 до FFFFFFFF.

**Байты** могут объединяться в поля фиксированной и переменной длины. Адресом поля является адрес младшего байта, входящего в поле. Длина поля — количество байтов, входящих в поле. Поля фиксированной длины имеют собственные имена. Слово состоит из 2-х байтов, двойное слово из 4-х байтов. Поля переменной длины могут начинаться с любого байта.

**Процессор** может работать с непрерывной и сегментированной памятью. Если память сегментированна, то физический адрес байта состоит из 2-х частей: <сегмент>:<смещение>. И получается он по формуле: адрес начала сегмента + исполняемый адрес.

**Смещение** — исполняемый адрес, который формируется в зависимости от способа адресации операндов. В защищённом режиме может быть определено до 16083 сегментов, размером до 4Гб, процессор может обработать 64Тб виртуальной памяти.

**В реальном режиме** старшие 4 цифры адреса начала сегмента хранятся в сегментном регистре, адрес сегмента кратен 16, поэтому физический адрес получается смещением содержимого сегментного регистра на 4 разряда (двоичных) влево и прибавлением к нему исполняемого адреса.

**Физический адрес** следующей исполняемой команды получается: содержимое регистра CS, смещённое на 4 разряда + IP. **Пример:**

$$\begin{aligned}\Phi A &= (CS) + (IP) \\ (CS) &= 7A15_{16} = 0111\ 1010\ 0001\ 0101\ 0000_2 \\ (IP) &= C7D9_{16} = 1100\ 0111\ 1101\ 1001_2 \\ \Phi A &= 86929_{16} = 1000\ 0110\ 1001\ 0010\ 1001_2\end{aligned}$$

## Форматы данных

**Рассматриваемый нами процессор** может обрабатывать целые числа без знака, целые числа со знаком, действительные числа с плавающей точкой, двоично-десятичные числа, символы, строки и указатели.

**Целое число без знака** может занимать байт, слово или двойное слово и изменяться от 0 до 255(байт), от 0 до 65535(слово) и от 0 до 4294967295(двойное слово).

**Целое число со знаком** может занимать байт, слово или двойное слово при этом старший разряд (7(байт), 15(слово) или 31(двойное слово)) отводится под знак числа (0 положительной, 1 отрицательное), остальные разряды под цифры числа.

**Цифры со знаком** хранятся в дополнительном коде, дополнительный код положительного числа равен числу, а дополнительный код отрицательного числа может быть вычислен по формуле:  $10^n - |x|$ .

**Например**, представим в слове отрицательное число -AC7 ( $10^4 - AC7 = F539$ ).

**Дополнительный код** двоичного числа можно получить инверсией разрядов и прибавлением 1 к младшему разряду.

**Например**, -12 (в байте) ( $12 = 11110100$ )

**Вычитание в машине:** дополнительный код уменьшаемого прибавляется к вычитаемому, чтобы получить  $65 - 42 = 23$

1)  $65 = 0100\ 0001$

2)  $-42 = 1101\ 0110$

3)  $65 + (-42) = 0100\ 0001 + 1101\ 0110$

**Число с плавающей точкой** может занимать 32 разряда, 64 разряда или 80 разрядов, и называется оно короткое вещественное, длинное вещественное и рабочее вещественное.

**Число с плавающей точкой** состоит из 3-х частей: знак (1 разряд), машинный порядок (8(если в общем число занимает 32 разряда) или 11(64 разряда), или 15(80 разрядов) разрядов), мантисса (23(32 разряда) или 52(64 разряда), или 64(80 разрядов) разряда).

**Машинный порядок** не явным образом содержит в себе знак порядка, он изменяется от всех 0 до всех 1, в поле, которое ему определено, а с истинным порядком машинный порядок связан формулой:

$$P_M = P_i + 127_{10} (1023_{10}, 16383_{10})$$

Пример,  $3060_{10}$  представить в виде числа с плавающей точкой, занимающего 4 байта.

$$1) 3060_{10} = BF4_{16}$$

1  
ОСНОВАНИЕ СИСТ. СЧИСЛЕНИЯ

2) нормализуем число  $0. BF4 \cdot 10^3_{16}$

3) получим машинный порядок  $Пм = 3_{16} + 7F_{16} = 82_{16}$

4) запишем в разрядную сетку в 2-ичной системе счисления:

0 1000 0010 011 1111 0100 0000 0000 0000<sub>2</sub>

Или в 16-ричном виде:  $413F4000_{16}$

0100 0001 0 011 1111 0100 0000 0000 0000<sub>2</sub>

- 1) переведём в 16-ричное
- 2) нормализуем число
- 3) получаем машинный порядок
- 4) записываем в разрядную сетку, но хитрость заключается в том, что для экономии памяти старшая цифра мантииссы нормализованного числа не записывается в разрядную сетку (т.к. она равна 1(вроде всегда))

**Двоично-десятичные числ** могут обрабатываться процессором как 8-ми разрядные в упакованном или неупакованном формате, а сопроцессором могут обрабатываться 80-ти разрядные в упакованном формате.

**Упакованный формат** предполагает хранение 2-х цифр в байте, а неупакованный только 1 цифры в цифровой части байта.

**Символьные данные** хранятся в ASCII коде, каждому символу отводится 1 байт памяти.

**Строковые данные** — это последовательности байтов, слов или двойных слов и указатели. Существует два типа указателей: длинный (48 разрядов селектор(16) + смещение(32)) и короткий (32 разряда).

## Форматы команд

**В машинном формате команда** — последовательность двоичных цифр, состоящая из двух частей, определяющих код операции и адресную часть, то есть где хранятся данные и куда можно записать результат.

**Рассматриваемый процессор может работать** с безадресными командами, с одноадресными командами, двухадресными и трёхадресными командами. В памяти команда может занимать от 1 до 15 байтов в зависимости от кода операции количество операндов и места их расположения. А располагаться операнды могут непосредственно в команде, в регистрах или в оперативной памяти.



**Наибольшее количество команд** двухадресных и тогда формат называют: R-R, M-M, R-M, M-R, R-D, M-D.

Существуют различные способы адресации операторов, а данные могут занимать байт, слово или двойное слово. И исполняемый адрес операнда зависит от способа адресации и может состоять из трёх частей (база, индекс и смещение). Например, [BX][SI]M

#### Способы адресации (в реальном режиме):

- 1) регистровая,
- 2) непосредственная,
- 3) прямая,
- 4) косвенно-регистровая,
- 5) по базе со смещением,
- 6) прямая с индексированием,
- 7) по базе с индексированием.

Машинный формат двухадресной команды, для которой один операнд находится всегда в регистре, а второй – в регистре или памяти можно представить следующим образом:

байты	1	2	3	4
биты	7 2 1 0	7 6 5 4 3 2 1 0	7 0	7 0
поля	код операции d w	MOD reg r/m	disp H	disp L

“disp H/disp L” – “старшая / младшая часть смещения.

Поля “код операции” и иногда “reg” определяют выполняемую операцию.

Поле “d” определяет место хранения первого операнда.

Поле “w” определяет с какими данными работают: с байтами, или словами.

Если w = 0, команда работает с байтами, w = 1 - со словами.

reg” - определяет один операнд, хранимый в регистре.

Поля “mod”, “disp H” и “disp L” определяют второй операнд, который может храниться в регистре или в памяти.

Если mod = 11, то второй операнд находится в регистре, он определяется полем “r/m”, а “disp H/disp L” – отсутствует, команда будет занимать 2 байта в памяти, если mod <> 11, то второй операнд находится в памяти.

Машинный формат двухадресной команды


Значение поля “mod” определяет как используется смещение:

mod  $\begin{cases} 0, \text{ disp – отсутствует} \\ 1, \text{ disp = disp L – с распространением знака до 16} \\ 10, \text{ смещение состоит из disp H и disp L.} \end{cases}$

Поля “reg” и “r/m” определяют регистры:

reg / r/m	000	001	010	011	100	101	110	111
w = 0	AL	CL	DL	BL	AH	CH	DH	BH
w = 1	AX	CX	DX	BX	SP	BP	SI	DI

Физический адрес определяется так:



r/m	ИА	ФА
000	(BX) + (SI) + disp	+ (DS)
001	(BX) + (DI) + disp	+ (DS)
010	(BP) + (SI) + disp	+ (SS)

Машинный формат двухадресной команды.

r/m	ИА	ФА
011	(BP) + (DI) + disp	+ (SS)
100	(SI) + disp	+ (DS)
101	(DI) + disp	+ (DS)
110	(BP) + disp	+ (SS)
111	(BX) + disp	+ (DS)

В ассемблере результат всегда посылается по адресу первого операнда.

**Адресация регистровая:**

MOV AX, BX ;(BX) → AX

Машинный формат: 1001 0011 1100 0011

“код операции” 100100

“d” = 1

“w” = 1

“mod” = 11

“reg” = 000

“r/m” = 011

**Непосредственная адресация:**

MOV AX,25 ; 25 → AX

В ассемблере как и в языках высокого уровня есть именованные константы, они определяются с помощью EQU

**Конструкция:** <имя> <EQU> <значение>

**Пример:** (CONST EQU 34h)

**Прямая адресация** (адрес операнда прямо в команде записывается):

**MOV AX, ES : 0001 ;**

ES – регистр сегмента данных, 0001 – смещение внутри сегмента.

Содержимое двух байтов, начиная с адреса (ES) + 0001 пересылаются в AX -  
(ES) + 0001 → AX.

Прямая адресация может быть записана с помощью символического имени, которому предварительно был присвоен некоторый адрес оперативной памяти, а присвоен может быть с помощью директивы.

например: DB – байт,

DW – слово,

DD – двойное слово.

Если в сегменте ES содержится директива Var\_p DW, тогда по команде

**MOV AX, ES : Var\_p ; ((ES) + Var\_p) → AX.**

Например, если команда имеет вид:



**MOV AX, Var\_p; ((DS) + Var\_p) → AX.**

**Косвенно-регистровая операция** (в регистре содержится адрес операнда), в записи косвенно-регистровая от регистровой отличается записью регистра в квадратных скобках.

**MOV AX, [SI] ;**

Могут использоваться регистры:

SI, DI, BX, BP, EAX, EBX, ECX, EDX, EBP, ESI, EDI.

Не могут использоваться: AX, CX, DX, SP, ESP.

**Адресация по базе со смещением:**

**MOV AX, [BX]+2** ; ((DS) + (BX) + 2) → AX.

≡ **MOV AX, [BX + 2]** ;

≡ **MOV AX, 2[BX]** ;

**MOV AX, [BP + 4]** ; ((SS) + (BP) + 4) → AX.

**BP** работает с сегментом стека.

**Прямая с индексированием адресация:**

**MOV AX, MAS[SI]** ; ((DS) + (SI) + MAS) → AX

**MAS** – адрес в области памяти.

С помощью этой адресации работают с одномерными массивами или с полями структур, символическое имя определяет адрес начала массива или структуры, а содержимое **SI** используется для перехода от одного элемента массива к другому или от одного поля структуры к другому.

С **двумерными массивами** используется адресация по базе с индексированием.

**MOV AX, Arr[BX][DI]** ; ((DS) + (BX) + (DI) + Arr) → AX.

Символическое имя определяет адрес начала массива, с помощью индексного регистра реализуется переход от одного элемента к другому (в строке), а с помощью базового регистра от одной строке к другой.

## Лекция 5

Различные формы адресации:

Команды изменяют значения флажков. (фото)

Умножение и деление:

Умножение для беззнаковых чисел (фото)

умножение знаковых чисел (фото)

в варианте 3-х адресной команды: **OP1** - всегда регистр, **OP2** - может быть данные, регистры или память, **OP3** - всегда данные, но не **BYTE**

1) При умножении результат может иметь удвоенный формат по отношению к сомножителю. Иногда мы точно знаем, что результат точно умещается в формат сомножителей и тогда мы его смело извлекаем ил аккумулятора **AL**, **AX** или **EAX**. Но если мы не знаем каким будет результат, нужно посмотреть на значения флажков **OF** и **CF**, если эти флажки равны 1, значит результат больше, чем сомножители, если **OF** и **CF** равны 0, то можно извлекать.

Примеры: (фото)

Деление беззнаковых чисел - **DIV OP2** (**OP2** - регистр или память)

Деление знаковых чисел - **IDIV OP2** (фото)

Содержимое аккумулятора AX или AX:DX или EAX:EDX делится на указанный операнд и результат записывается в AL или AX или EAX, в зависимости от типа результат. Остаток помещается в AH, DX или EDX.

Значение флагов при делении не меняются, но могут быть ошибки деления на 0 или переполнение.

Пример: (фото)

При выполнении команд умножения и деления необходимо следить за размером операндов и при необходимости за значениями флажков сдвига и переполнения.

Посмотрим фрагмент программы, в котором цифры целого беззнакового байтового числа N записывают в байты памяти, начиная с индекса D как символы. (фото)

Заголовок Директивы внешних ссылок

Директивы внешних ссылок позволяют организовать связь между различными модулями, расположенными на диске, и между различными файлами.

Пример: Public <имя>,[<имя>]

Эта директива определяет указанные имена как глобальные величины к которым можно обращаться из другого модуля.

Именем может быть метка или переменная.

Если некоторое имя определено в модуле А как глобальное, а к нему нужно обращаться из других модулей, например В и С, то в этих модулях В и С, должна быть директива EXTRN <имя>:<тип> (можно несколько)

Имя одно и тоже, что написано в директиве Public, а тип зависит от значения имени, если имя это имя переменной, то на месте слова тип может стоять одно из ключевых слов (BYTE, WORD, DWORD, FWORD, QWORD, TWORD), если имя это метка, то типом может быть NEAR или FAR.

Директива EXTRN говорит, что эти имена являются внешними для данного модуля.

Пример:(фото)

Директива INCLUDE позволяет подключить на этапе ассемблирования файлы, расположенные на диске, например: INCLUDE <имя файла> + (фото)

На этапе ассемблирования содержимое этого файла запишется на место этой директивы.

Заголовок Команды управления

Команды управления управляют кодом вычислительного процесса. К ним относятся команды условной передачи управления, безусловной передачи управления и команды организации управления.

Команды безусловной передачи управления (фото)

Имя - метка команды, которая будет выполняться следующей за JMP, команда, на которую передаём управление, может располагаться в том же кодовом сегменте, что и JMP, а может и в другом кодовом сегменте.

Пример: (фото)

Если метка содержится в другом кодовом сегменте, то в том сегменте, куда передаём управление, должна быть директива Public M1, а в сегменте

с JMP должна быть директива ETRN M1: FAR

Передачи бываю прямыми или косвенными, можно использовать прямую (JMP M1) и косвенную (JMP [BX]) адресацию.

Команда безусловной передачи управления на ближнюю метку занимает в памяти 3 байта, передача на дальнюю метку занимает 5 байтов памяти. Если мы знаем, что передаём управление не далее чем на -128 или 127 байтов, то можно использовать команду занимающую 1 байт памяти.

вид (фото)

За командой JMP должна следовать команда с меткой (обязательно, чтобы можно было вернуться к команде, следующей за JMP)

К командам безусловной передачи управления относятся команды обращения к подпрограммам и возврата из подпрограммы.

Процедура обязательно имеет тип NEAR или FAR, последний нужно указывать обязательно.

NEAR может быть вызвана только из того модуля в котором содержится. Основная или головная программа всегда имеет тип FAR, поскольку к ней обращается из отладчика. Если подпрограмм немного, то их размещают в том же сегменте, что и основная программа, а если их много, то для них выделяют отдельный кодовый сегмент.

Пример: (фото)

Команда CALL <имя>, которая может использовать как прямую адресацию, так и косвенную. При обращении к подпрограмме в стеке сохраняется адрес возврата, то есть адрес команды, следующей за командой CALL, но если мы обращаемся к подпрограмме ближнего типа, то в стеке сохраняется только смещение, а если к внешней процедуре, к подпрограмме, содержащейся в другом кодовом сегменте, то в стек записывается полный адрес (начало сегмента и смещение относительно него).

Команда возврата RET может использоваться в одном из 3-х видов (фото) Команда RET может реализовать выход из подпрограммы как NEAR, так и FAR

RETN - из подпрограммы ближнего типа вызова

RETF - из подпрограммы дальнего типа вызова

Параметр n необязательный, он говорит сколько надо байтов в стеке нужно очистить

Пример: (фото)

Заголовок Команды условной передачи управления

Команды условной передачи управления делят на 4 типа:

- 1) команды используемые после команд сравнения
- 2) команды используемые после команд отличных от команд сравнения
- 3) команды сравнения, но реагирующие на значения флагов
- 4) команды, реагирующие на значение регистра CX

Общий вид объявления Jx <метка> (J - всегда первая, а затем следует несколько букв), метка в этой команде имеет право отстоять не более чем на 127 байтов.

Например: (фото)

(фото)

Если нужно реализовать условную передачу управления больше чем на 127 байт, то можно изменить условие передачи управления (фото)

С помощью команд условной передачи и безусловной можно организовать циклы с предусловием и постусловием (фото)