

## 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.

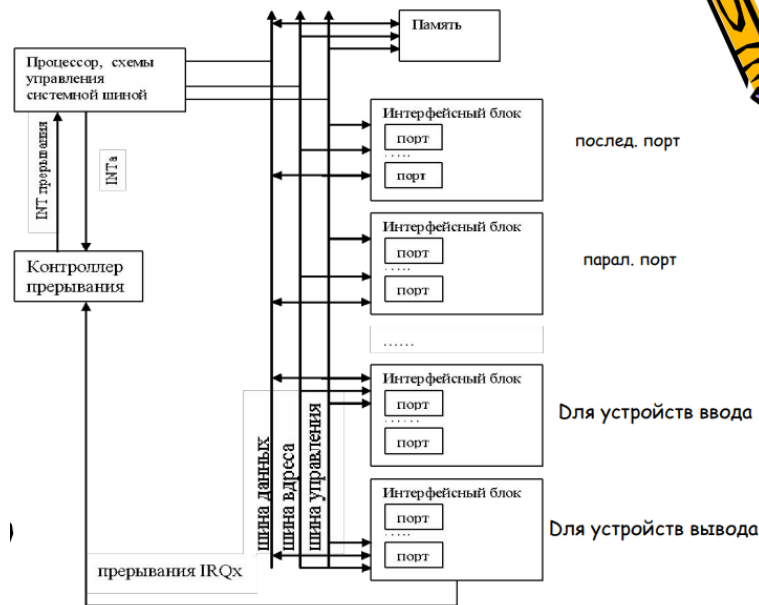
**Системные программы** используются для разработки новых программ, модификации уже существующих программ и выполнения программ автономным способом.

**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.

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

$\frac{1}{\text{ОСНОВАНИЕ СИСТ. СЧИСЛЕНИЯ}}$

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

### Сложение и вычитание в Ассемблере

Арифм-ие операции изменяют значение флажков OF, CF, SF, ZF, AF, PF.

В Ассемблере команда '+'

**ADD OP1, OP2** ; (OP1) + (OP2) → OP1

**ADC OP1, OP2** ; (OP1) + (OP2) + (CF) → OP1

**XADD OP1, OP2;** i486 и >

(OP1) ↔ (OP2) (меняет местами), (OP1) + (OP2) → OP1

**INC OP1** ; (OP1) + 1 → OP1

В Ассемблере команда '-'

**SUB OP1, OP2** ; (OP1) - (OP2) → OP1

**SBB OP1, OP2** ; (OP1) - (OP2) - (CF) → OP1

**DEC OP1** ; (OP1) - 1 → OP1.

Примеры:

X = 1234AB12h, Y = 5678CD34h, X + Y =

**MOV AX, 1234h**

**MOV BX, 0AB12h**

**MOV CX, 5678h**

**MOV DX, 0CD34h**

**ADD BX, DX**

**ADC AX, CX**



Умножение и деление:

Умножение беззнаковых чисел.  
**MUL OP2** ; (OP2)\*(AL)  $\vee$  (AX)  $\vee$  (EAX)  $\rightarrow$  AX  $\vee$  DX:AX  $\vee$  EDX:EAX  
 Умножение знаковых чисел.  
**IMUL OP2**; аналогично MUL  
**IMUL OP1, OP2** ; i386 и > **IMUL op1, op2, op3** ; i186 и >  
 OP1 всегда регистр, OP2 – непосредственный операнд, регистр или память.  
 При умножении результат имеет удвоенный формат по отношению к сомножителям. Иногда мы точно знаем, что результат может уместиться в формат сомножителей, тогда мы извлекаем его из AL, AX, EAX.  
 Размер результата можно выяснить с помощью флагов OF и CF.  
 Если OF = CF = 1, то результат занимает двойной формат, и OF = CF = 0, результат укладывается в формат сомножителей.  
 Остальные флаги не изменяются.

Деление беззнаковых чисел: Деление знаковых чисел.  
**DIV OP2** ; OP2 = r  $\vee$  m **IDIV OP2** ; OP2 = r  $\vee$  m  
 (AX)  $\vee$  (DX:AX)  $\vee$  (EDX:EAX) делится на указанный операнд и результат помещается в AL  $\vee$  AX  $\vee$  EAX,  
 остаток помещается в AH  $\vee$  DX  $\vee$  EDX.

(OP2 - регистр или память)

Содержимое ааккумулятора 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 меняется, но могут быть ошибки деления на 0 или переполнения.

**MOV AX, 600**  
**MOV BH, 2**  
**DIV BH** ; 600 div 2 = 300 - не уместается в AL.

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.

c = N mod 10  
 b = (N div 10) mod 10  
 a = (N div 10) div 10  
 Перевод в символы: код(i) = код ('0') + i

-----  
**D** N DB ?  
 D DB 3 Dup (?)

```

MOV BL, 10 ; делитель
MOV AL, N ; делимое
MOV AH, 0 ; расширяем делимое до слова
; или CBW AH конвертируем до слова
DIV BL ; AL = ab, AH = c
ADD AH, '0'
MOV D+2, AH
MOV AH, 0
DIV BL ; AL = a, AH = b
ADD AL, '0'
MOV D, AL
ADD AH, '0'
MOV D+1, AH

```



## 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.

В модуле А содержится:

**Public TOT**

-----/-----

**TOT DW 0 ;**

чтобы обратиться из В и С к имени TOT, в них должна быть директива  
**EXTRN TOT:WORD**

**Директива INCLUDE** позволяет подключить на этапе ассемблирования файлы, расположенные на диске, например: INCLUDE <имя файла>

**INCLUDE C:\WORK\Prim.ASM**

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

## 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 имеют вид:**

**JMP <имя>**

**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.

**JMP M1 ;** по умолчанию M1 имеет тип NEAR

**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 бывают 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.

**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.

## Процедуры Near и Far

```

1)  Cseg  segment....
      assume .....
      p1  proc far
      -----
          call p2
      m:  mov AX, BX
      -----
          ret
      p1  endp
      p2  proc near
          m1: mov CX, DX
          -----
              ret
      p2  endp
Cseg  ends

```



## Процедуры Near и Far

<pre> 2) extrn p2: far       cseg  segment.....           assume .....       p1  proc far       -----           call p2       -----           ret       p1  endp       cseg  ends </pre>	<pre>       public p2       cseg1 segment.....           assume .....       p2  proc far       -----           ret       p2  endp       cseg1 ends </pre>
--	---

**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,



кодирующей в другом кодовом сегменте, то в стек записывается полный адрес (начало сегмента и смещение относительно него).

Возврат из процедуры реализуется с помощью команды **RET**.

Она может иметь один из следующих видов:

**RET [n]** ; возврат из процедуры типа NEAR, и из процедуры типа FAR

**RETN [n]** ; возврат только из процедуры типа NEAR

**RETF [n]** ; возврат только из процедуры типа FAR

Параметр n является необязательным, он определяет какое количество байтов удаляется из стека после возврата из процедуры.



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

### Примеры прямого и косвенного перехода



1) -----

a dw L ; значением a является смещение для переменной L

jmp L ; прямой переход по адресу L

jmp a ; косвенный переход - goto (a) = goto L

-----

2) -----

mov DX, a ; значение a пересылается в DX

jmp DX ; косвенный переход - goto (DX) = goto L

-----

3) -----

jmp z ; ошибка

-----



Z DW L

3) jmp word ptr z

z DW L

### 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.

Примеры:

JE M1 ; передача управления на команду с меткой M1, если ZF = 1  
 JNE M2 ; передача управления на команду с меткой M2, если ZF = 0  
 JC M3 ; передача управления на команду с меткой M3, если CF = 1  
 JNC M4 ; передача управления на команду с меткой M4, если CF = 0

**ADD AX, BX**

**JC M**

если в результате сложения CF = 1, то управление передается на команду с меткой M, иначе – на команду, следующую за JC

**SUB AX, BX**

**JZ Met**

если результатом вычитания будет 0, то ZF = 1 и управление передается на команду с меткой Met.

Часто команды передачи управления используются после команд

сравнения **<метка> CMP OP1, OP2**

По этой команде выполняется (OP1) – (OP2) и результат всегда не посылается, формируются только флаги.



### Команды условной и безусловной передачи управления

условие	Для беззнаковых чисел	Для знаковых чисел
>	JA	JG
=	JE	JE
<	JB	JL
> =	JAЕ	JGE
< =	JBE	JLE
< >	JNE	JNE



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

**if AX = BX goto m** следует заменить на:

**if AX < > BX goto L**

**Goto m ; m – дальняя метка**

-----

**L: ----- ; L – близкая метка**


На Ассемблере это будет так:

cmp AX, BX

jne L

jmp m

мет: -----  
L: -----



С помощью команд jx и jmp можно реализовать цикл с предусловием:

1) while x > 0 do S;

beg: cmp x, byte ptr 0

jle fin

S

jmp beg

fin: -----

и с постусловием:

2) do S while x > 0;

beg:

S

cmp x, byte ptr 0

jg beg

fin: -----



## Лекция 6

Заголовок Команды для организации циклов  
(слайд с loop метками)

В форме 1 из содержимого CX вычитается единица, если окажется, что CX != 0, то управление передаётся на указанную метку (CX содержит количество итераций)

Во второй форме из CX вычитается 1, если CX != 0 и ZF == 1, то управление передаётся на указанную метку. А это значит, что цикл завершается, происходит выход из цикла (передаётся управление следующее за loop), или CX = 0, или ZF = 0, или это произойдёт одновременно.

В 3 варианте уменьшается содержимое CX если CX != 0 и одновременно ZF = 0, то управление передаётся на указанную метку, если условие нарушено, то происходит выход из цикла.

Примеры циклов (слайд с loop метками)

Если CX используется для других целей, тогда можно поступить следующим образом

mov SI, 0 (далее с того же слайда)

Дана матрица целых байтовых величин размером 4 на 5, нужно подсчитать количество 0 в каждой строке матрицы, заменить 0 на константы, например 0FF, будем решать задачу с помощью директив стандартной сегментации, выделив под стек 256 байтов, а кодовый сегмент оформим как 2 последовательные процедуры. Внешняя реализует связь с операционной системой и обращается к внутренней процедуре, решающей поставленную задачу

(пример с слайда) + дописать комментарии

```
title prim.asm
page , 132
Sseg segment para stack 'stack'
db 256 dup (?)
Sseg ends
Dseg segment para public 'data'
Dan db 0,2,5,0,91
db 4,0,0,15,47
db 24,15,0,9,55
db 1,7,12,0,4
Dseg ends
Cseg segment para public 'code'
Assume cs: cseg, ds:dseg, ss:sseg
start proc far
PUSH DS
PUSH AX
mov BX,Dseg
mov DS,BX
call main
ret
start endp
main proc near
mov BX, offset Dan
mov CX, 4
nz1: PUSH CX
mov DI, 0
mov SI, 0
```

```

mov CX, 5
nz2: PUSH CX
cmp byte ptr[BX+SI], 0
jne mz
mov byte ptr[BX+SI], 0FFh
inc DL
mz: inc SI
POP CX
kz2: loop nz2
add DL, 0
mov AH, 6
int 21h
add BX, 5
pop CX
kz:1 loop nz1
ret
main endp
Cseg ends
end start

```

Заголовок организация циклов в ассемблере

Массивы описываются, определяются с помощью директив определения данных и памяти, возможно с помощью конструкции повторения `dup`

Например:

`x DW 30 dup (?)` - выделила в памяти место под одномерный массив `x` (массив слов), состоящий из 30 элементов, но в этом описании неясно как мы будем нумеровать элементы массива, мы можем пронумеровать их от 0 до 29, может от 1 до 30, а может от `k` до `29+k`, в зависимости от постановки задачи, если это не обговорено, то удобнее нумеровать в ассемблере с 0, потому что адрес любого элемента массива будет записываться наиболее происходит

Можем записать

адрес  $(x[i]) = x + (\text{type } x) * i$

Для двумерного массива - `A[0..n-1, 0..m-1]`

адрес  $(i,j)$  можно вычислить так

адрес  $(A[i,j]) = A + m * (\text{type } A) * i + (\text{type } A) * j$

Например для нашего одномерного массива это было

$x + 2*i = x + \text{type}(x) * i$

Адрес состоит из двух частей. Из постоянной части `x` и переменной  $2 * i$ , поэтому логично использовать для адресации элементов одномерного массива прямую индексацию со смещением, т.е. `x` - смещение, а  $2*i$  - в регистре `SI` или `DI`

место под двумерный массив можно выделить следующим образом:

`A DD n DUP (m Dup (?))` - двумерный массив слов размером `n` на `m`

Если мы будем нумеровать от 0 элементы строк и столбцов, то адрес  $(A[i,j]) = A + m * 4 * i + 4 * j$

A - постоянная, переменные  $m * 4 * i$  и  $4 * j$ , то есть адресация по базе с индексированием.

Фрагмент программы, в которой в регистр AL записывается количество строк матрицы байтов размерность  $10 * 20$ , тип элементов - byte, имя массива - x. Посчитаем количество строк матрицы, в которых 1-ый элемент повторяется не менее 1 раза.

(Программа на слайде)

Заголовок Команды побитовой обработки данных

К ним относятся:

- 1) логические команды,
- 2) команды сдвига
- 3) Установки
- 4) сброса
- 5) инверсии битов

Логические (с слайда)

Второй операнд в этих командах называют маской, а основным назначением команды and - установка в 0 с помощью маски соответствующих разрядов первого операнда, потому что нулевые разряды маски обнуляют соответствующие разряды первого операнда, а единичные оставляют без изменения.

Маску можно задавать как константу в команде, можно хранить в регистре или в памяти. Соответственно можно использовать любой способ адресации

Пример (соответствующий слайд)

Команда `or OP1, OP2` - ложь только если оба разряда ложь, эта команда используется для установки в 1 некоторых разрядов первого операнда в соответствии с маской - OP2

Пример (соответствующий слайд)

В команде могут использоваться различные способы адресации:

пример (соответствующий слайд)

Команда `xor OP1, OP2`, если операнды одинаковые, то результат 0, если различные, то результат 1

Пример (соответствующий слайд)

Команда `not` выполняет инверсию операнда. Значение при этом не изменяется.

Команды `xor` обнуляет регистр AX быстрее, чем `mov` и `sub`

(слайд после этой строки)

Определить количество задолжников в группе из 20 студентов, информация содержится в массиве байтов X DB 20 DUP (?), причём (соответствующие слайды (2))

Команды сдвига

Арифметические логические команды сдвига : первая буква s, вторая определяет тип сдвига логический или арифметический, 3 определяет влево или вправо, причём первый оператор может быть регистром или памятью, а второй это константа или регистр CL, в котором используется 5 младших разрядов.

Пример (соответствующий слайд) + следующий слайд про сдвиги больше чем на 1

Циклические сдвиги (соответствующий слайд)

+ ещё следующий слайд

Циклические сдвиги с переносом содержимого флажка CF (соот)

для всех команд сдвига флажки ZF, SF, PF, устанавливаются в соответствии с результатом, AF тоже неопределён. OF - не определён при сдвигах на несколько разрядов, а при сдвигах на 1 разряд в зависимости от команды (слайд)

Для самостоятельного изучения (соответствующий слайд)

## Лекция 7

Заголовок структуры в ассемблере

Структуры - комбинированный тип, содержащий данные различного типа, занимающие последовательные поля памяти. (109 тип)

Чтобы использовать переменную структурного типа, нужно описать структуры (шаблон структуры), на основании которого место в памяти при ассемблировании не выделяется, а для транслятора только информация о формате структуры. Это описание структуры выглядит следующим образом:

```
<имя типа> struct  
описание полей  
<имя типа> ends
```

Для описания полей используется директивы определения данных и памяти (byte, word, DW), а имена указанные в этих директивах и будут именами полей.

Имена полей в директивах по стандарту считаются уникальными в рамках программы, и ещё по стандарту не допускаются вложенные структуры.

Например (слайд 110):

? - означает, что значения по умолчанию нет.

Имена полей - имена в директивах, а значения называются значениями, принятыми по умолчанию.

Расположение данных (слайд 110)

(слайд 111) Описание переменных:

уголки - не метасимволы, а реальные символы языка, внутри которых через запятую указываются начальные значения полей.

(слайд 111) значения полей + пример

Приоритетными значениями являются начальные значения. Если при описании переменной значением поля является ?, или какое-то другое значение, то значение полей по умолчанию игнорируется. Пример (слайд 112)

Если при описании переменной используется значение пусто, то в качестве начального значения принимается значение по умолчанию.

Значение по умолчанию устанавливается для тех полей, которые являются одинаковыми для нескольких переменных, например, для массива структур.

Если отсутствует начальное значение, нескольких полей при описании переменных и эти поля являются последними в описании, то запятые при описании можно не ставить.

пример (слайд 113)

Если нет совсем начальных значений у переменной, то нужно оставлять пустые угловые скобки

пример (слайд 113)

Можно писать за 1 раз несколько переменных, а можно писать массив структур, используя конструкцию DUP

пример (слайд 113)

Описан одномерный массив структур типа TData, в котором первый элемент массива имеет начальное значение 2000, 4, 1, а остальные элементы массива в качестве начальных получают значения, принятые по умолчанию.

Имя и адрес первой структуры dst, второй - dst+4, третьей dst+8,..., это начало первого элемента структуры.

Обращаться к полям можно также как и в языках высокого уровня:

пример + шаблон(слайд 114)

Ассемблер имени типа структуры и имени переменной структурного типа присваивает тип, определяющий размер структуры (количество байт, занимаемых структурой)

пример (слайд 114)

И тогда эту информацию можно использовать при программировании, то есть скопировать значение полей из одной структуры в другую

пример (слайд 114)

Из памяти в память пересылать нельзя.

пример (слайд 114)

Точка, при обращении к полю структуры, это оператор, который позволяет вычислить адрес поля по формуле

формула (слайд 115)

Тип полученного адреса, совпадает с типом поля, т.е.

(слайд 115)

Смещение поля в структуре - это имя поля, а адресное выражение может быть любой сложности

пример + замечания(слайд)

Если при описании типа структуры, при описании некоторого поля, используется несколько параметров или конструкция повторения DUP, то при описании переменной этого типа, у данного поля не должно быть начального значения, может быть только пустым, но есть одно исключение: если по умолчанию значением поля является строка, то у этого поля по этой переменной, то при описании переменной у этого поля может быть начальное значение, но размером не больше, чем строка по умолчанию, если окажется меньше, то справа это поле дополнится пробелами.

пример (слайд)



пример (используем прямое обращение к полям)(следующий слайд + следующий слайд)

пример (обращение к полям структуры в цикле)(слайд)

пример (обращение к полям структур цикл в цикле)(слайд + следующий слайд + следующий слайд)

Заголовок Записи в ассемблере

Записи в ассемблере это упакованные данные. Это данные, которые занимают нецелые байты или слова, а части байтов или слов, т.е. запись в ассемблере может занимать 1 байт или 2 байта, то есть слово, а поля записи занимают последовательные биты в байте или слове.

Поля должны быть прижаты к правой границе записи, прижаты к правой границе поля и между ними не должно быть неопределённых разрядов, размер записи может быть только байтом или словом, размер поля записи может быть любым, но так, чтобы в сумме размеры полей не превышали байта или слова. Если сумма размеров полей, меньше байта или слова, то старшие разряды этого байта или слова заполняются нулями, но никакого отношения к записи не имеют.

Поля, так же как и у структуры, имеют собственные имена, но обращаться к ним напрямую нельзя, так как это несколько разрядов, а наименьший адресуемый элемент для процессора это байт. Так же как и для структуры, должно быть описание типа записи (шаблон), на основании которого не выделяется место, это описание может располагаться в любом месте программы, но до первого описание переменной такого типа.

пример (слайд)

Поле по определению есть

(слайд)

Размер и выражение - это константные выражения. Размер определяет размер поля в битах (сколько разрядов занято полем), а выражение, если оно есть, определяет значение поля по умолчанию, но в отличие от структуры, знак вопроса не допускается

пример (слайд)

Используя идентификатора типа опишем переменные следующего типа

пример (слайд)

Угловые значения - это символы языка, внутри которых через запятую записываются начальные значения, а начальным значением может быть константное выражение, знак вопроса или пусто, в отличие от структуры знак вопроса определяет нулевое начальное значения, а начальное значение пусто приведёт к тому, что у поля будет значение, принятое по умолчанию

пример (слайд)

С запятыми можно поступить так же как и у структуры: если они последние, то можно их не писать, если значений нет, то можно тоже не писать.

пример (слайд)

массив записей (слайд)

Все 100 записей будут иметь значение, принятые по умолчанию.

пример (слайд)

Можно присвоить поля записи одной записи другой, тогда мы пользуемся конструкцией

пример (слайд)

Для работы с полями есть специальные операторы `width` и `mask`

(слайд)

оператор `width` определяет размер в битах указанного операнда, это будет размер поля или размер всей записи.

оператор `mask` определяет маску

(слайд)

результатом будет маска, в котором разряды оператора заполняются 1, а все остальные 0

пример (слайд)

пример (выявить родившихся первого числа)(слайд)