

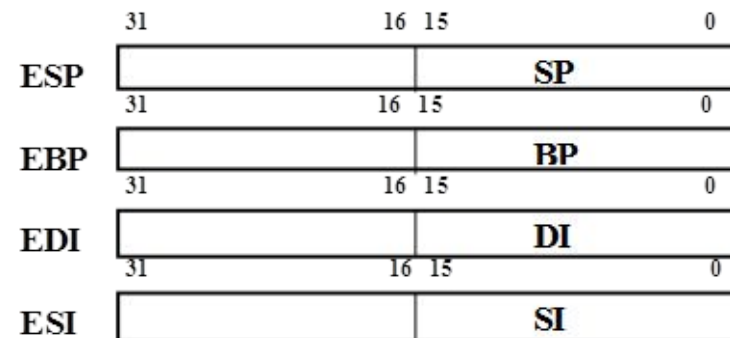
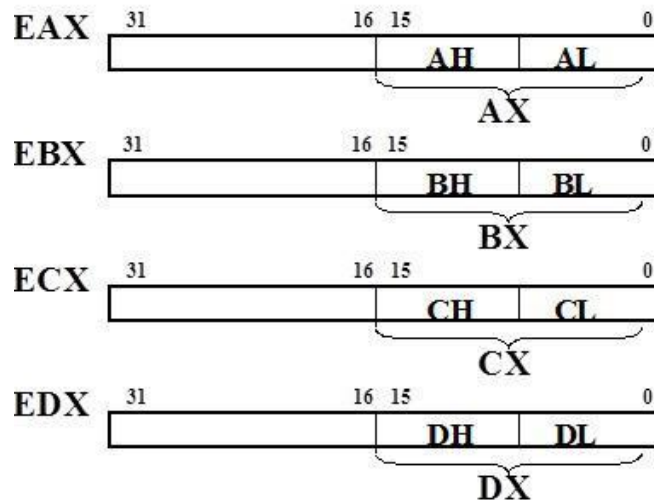
Лекция 3. Процессоры семейства x86. Регистры. Форматы данных

- Семейство процессоров Intel включает «линейку» 16-ти, 32-х и 64-разрядных процессоров:
8086, 8088, 80186, 80188, 80286
i386, i486, iPentium (i586), iPentium MMX, iPentium Pro, iPentium II, iPentium II Xeon, iCeleron, Pentium III, iPentium III Xeon, iPentium 4, iPentium D, iCore2, iPentium Dual Core, Core i7/i5/i3, iAtom и далее
- Родоначальник архитектуры x86 - 16-разрядный процессор 8086 (8088). Архитектура x86 реализована и в процессорах других фирм производителей
- Процессоры семейства x86 совместимы “снизу-вверх” по архитектуре и системе команд. Программный код для младшей модели процессора будет исполняться любым следующим.

Программно-доступные регистры 32-разрядного процессора x386

Регистры общего назначения

- 8-разрядные: AH, AL, BH, BL, CH, CL, DH, DL
- 16-разрядные: AX, BX, CX, DX, SP, BP, DI, SI
- 32-разрядные: EAX, EBX, ECX, EDX, ESP, EBP, EDI, ESI

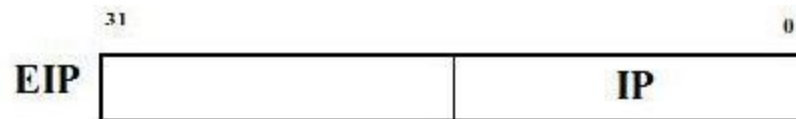


Регистры- указатели сегментов памяти

- ❑ 16- разрядные регистры: **CS**, DS, ES, SS, FS, GS
CS – указатель на сегмент с командами
остальные – указатели на сегменты с данными

Регистр- указатель команд

- ❑ 16-разрядный IP /32-разрядный EIP



Регистр флагов



Арифметические флаги: CF, AF, ZF, PF, SF и OF устанавливаются процессором в 0 или 1 после выполнения каждой арифметической команды.

- ☐ По состоянию арифметических флагов можно судить о свойствах полученного результата.
- ☐ Флаги программно доступны!

Арифметические флаги

CF (Carry Flag) - флаг переноса /заема

- CF=1 после сложения, если был перенос за формат результата
- CF=1 после вычитания, если был заем из-за предела формата данных («из воздуха»)

Примеры: после сложения /вычитания байтов

$$\begin{array}{r} F0 \\ + \underline{11} \\ 01 \end{array}$$

CF=1 (был перенос)

$$\begin{array}{r} 11 \\ - \underline{F0} \\ 21 \end{array}$$

CF=1 (был заем)

AF (Auxiliary Flag) - флаг вспомогательного переноса /заема

- AF=1 после сложения, если был перенос из младшей тетрады младшего байта результата,
- AF=1 после вычитания, если был заем из старшей тетрады младшего байта

Примеры:

$$\begin{array}{r} 1C \\ + \quad 2E \\ \hline 4A \end{array}$$

 AF=1

$$\begin{array}{r} 782A \\ - \quad 530B \\ \hline 251F \end{array}$$

AF=1

ZF (Zero Flag) - флаг нуля

- ZF=1 при получении нулевого результата

Примеры:

$$\begin{array}{r} F0 \\ + 11 \\ \hline 01 \end{array}$$

ZF=0

$$\begin{array}{r} 10 \\ + F0 \\ \hline 00 \end{array}$$

ZF=1

PF (Parity Flag) - флаг четности

- PF= 1, если младший байт результата содержит четное число двоичных единиц или все нули

Примеры:

$$\begin{array}{r} F0 \\ + \underline{11} \\ 01 \text{ (bin: } 00000000\textbf{1}) \\ \text{PF} = 0 \end{array}$$

$$\begin{array}{r} 11 \\ - \underline{F0} \\ 21 \text{ (bin: } 00\textbf{1}0000\textbf{1}) \\ \text{PF} = 1 \end{array}$$

SF (Sign Flag) - флаг знака

- SF повторяет значение старшего бита результата (знаковый разряд для знаковых чисел)

Примеры:

$$\begin{array}{r} 9C \\ + \underline{2E} \\ \hline CA \end{array} \quad \begin{array}{l} (\textcolor{red}{1}100\ 1010) \\ \textcolor{blue}{SF}=1 \end{array}$$

$$\begin{array}{r} 782A \\ - \underline{530B} \\ \hline 251F \end{array} \quad \begin{array}{l} (\textcolor{red}{0}010\ 0101\ 0001\ 1111) \\ \textcolor{blue}{SF}=0 \end{array}$$

OF (Overflow Flag) - флаг переполнения

- ❑ OF= 1 указывает на некорректное значение знакового бита результата после операции над знаковыми числами.
- ❑ Это происходит, когда результат **не поместился в используемый формат** знаковых данных. Следовательно, надо увеличить формат данных

Пример: сложение знаковых чисел

а) однобайтный формат

$$\begin{array}{rcl} 7F & (+127) \\ + 04 & (+ 4) \\ \hline 83 & (- 125) \end{array}$$

OF = 1

б) расширим до 2-байтных

$$\begin{array}{rcl} 007F & (+127) \\ + 0004 & (+ 4) \\ \hline 0083 & (+ 131) \end{array}$$

OF = 0

Управляющие флаги DF, IF и TF

Влияют на работу процессора. Программно доступны.


- **IF (Interrupt Flag)** - флаг внешних прерываний процессора: 0 – прерывания будут запрещены, 1 - разрешены

- **TF (Trace Flag)** - флаг трассировки. TF=1 переводит процессор в пошаговый режим исполнения команд.

- **DF (Direct Flag)** – флаг «направления» для исполнения строковых команд


Форматы целочисленных данных 32-разрядного процессора

Байт



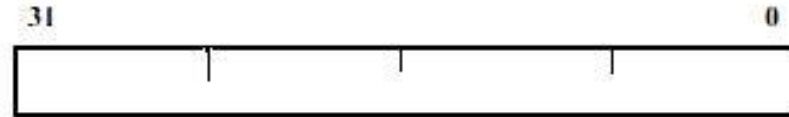
A horizontal rectangle representing a byte. Above the left end is the number 7, and above the right end is the number 0.

Слово



A horizontal rectangle representing a word, divided into two equal halves by a vertical line. Above the left end is the number 15, and above the right end is the number 0.

**Двойное
слово**



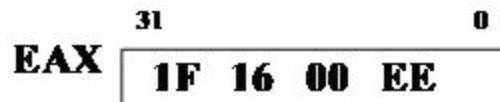
A horizontal rectangle representing a double word, divided into four equal quarters by three vertical lines. Above the left end is the number 31, and above the right end is the number 0.

Размещение многобайтных числовых данных в регистрах и памяти

□ Пример:

4-байтный код **1F 16 00 EE** размещен в регистре EAX и в памяти.

Обратите внимание, где «голова» (старший байт)



адрес байта
в сегменте памяти

| | |
|-------|-----|
| ... | ... |
| 0...7 | EE |
| 0...8 | 00 |
| 0...9 | 16 |
| 0...A | 1F |
| ... | .. |