Регистровая память
Регистры микропроцессора

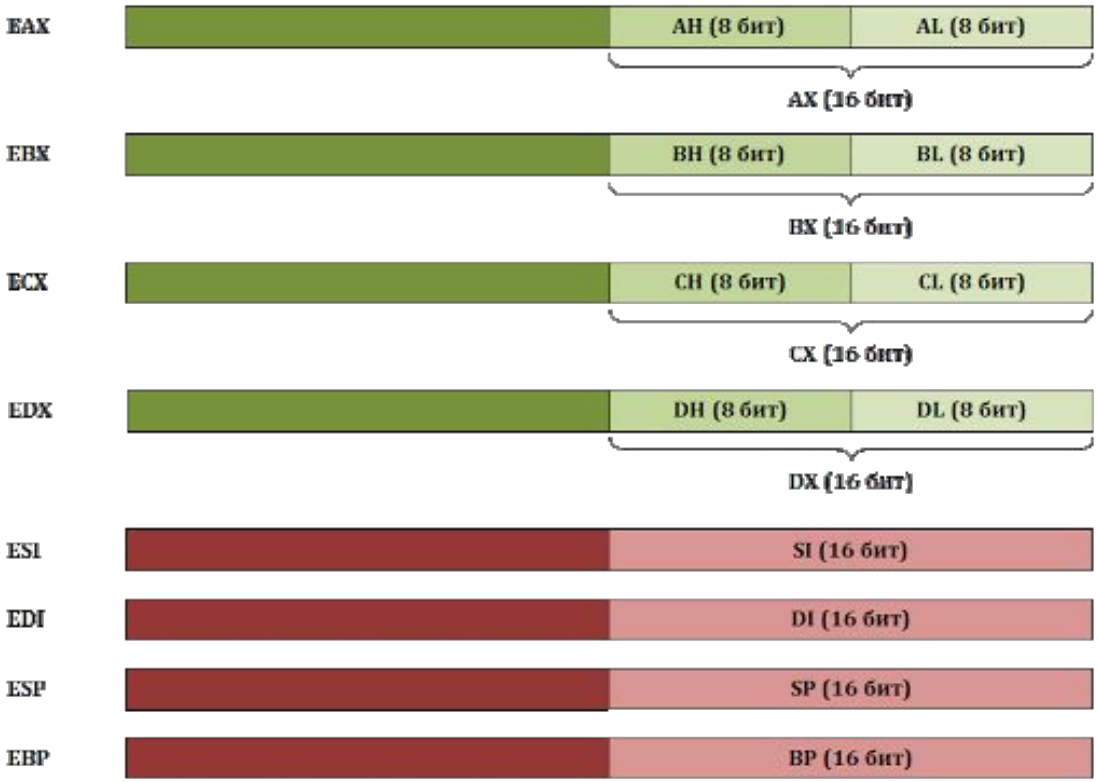
Лекция

Е.Н. Ливак

- Обычно регистры подразделяют на
  - Пользовательские
    - так называются потому, что программист может их использовать при разработке программ
  - Системные

Регистры общего назначения: 16 штук в IA-32 (x86-32)

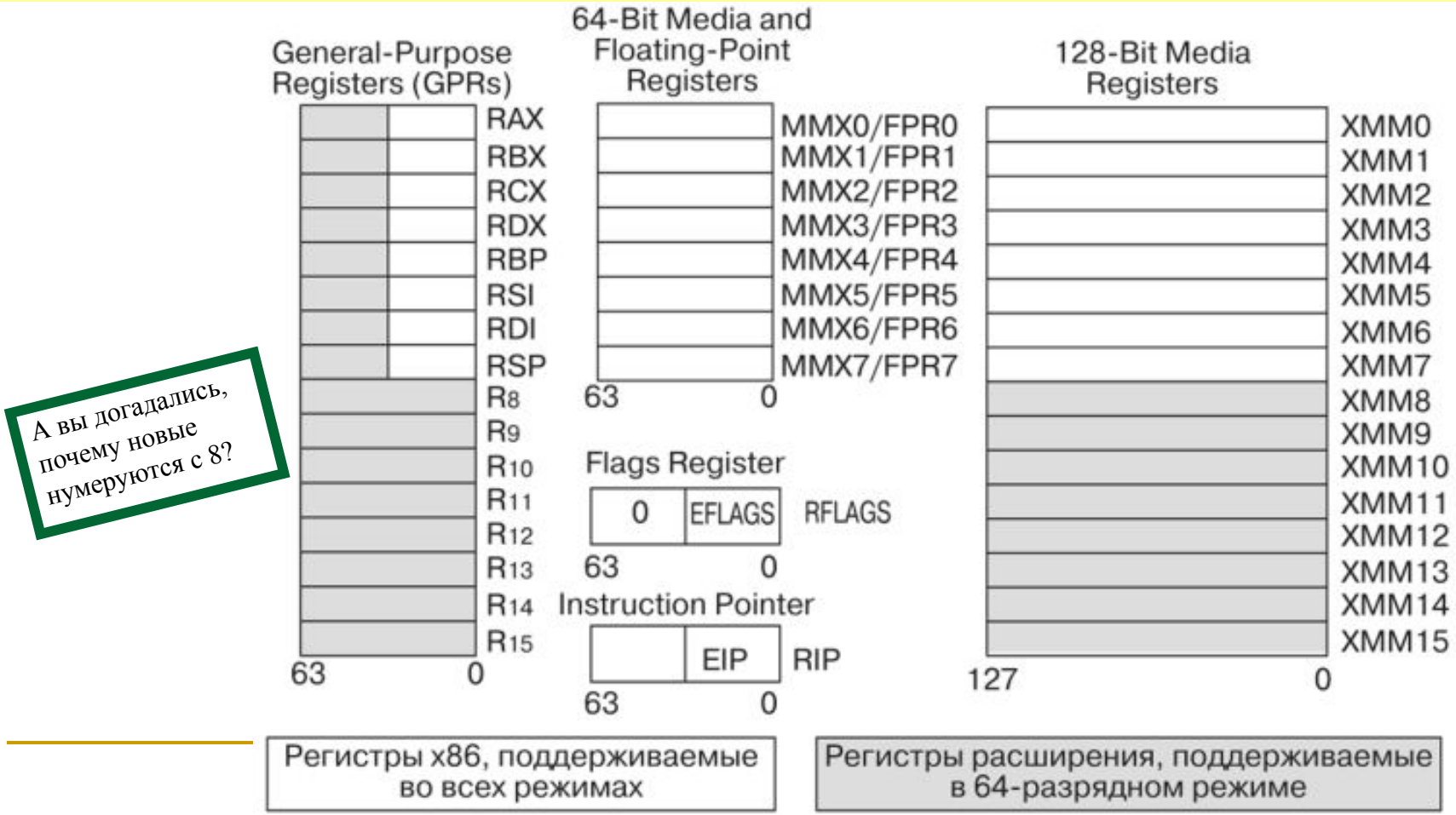
32-разрядные пользовательские регистры, непосредственно доступные программисту



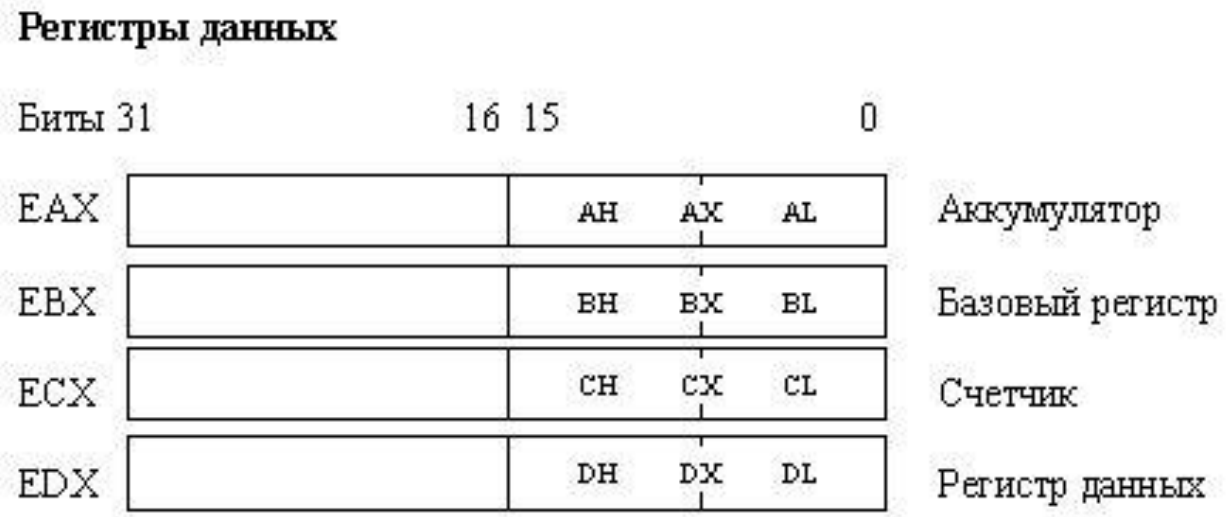
Регистры
с произвольным
доступом

Регистры AMD-процессоров (архитектура x86-64)

Прежние 32-разрядные регистры расширены до 64-бит
и получили имена с приставкой R.
К 8 прежним добавлены 8 новых. Новые регистры остались безымянными и просто пронумерованы от R8 до R15



Чаще всего программист использует регистры данных



eax (Accumulator register)
edx (Data register)
применяются для хранения промежуточных данных

ecx/cx (Count register)
Применяется в командах, производящих 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

ebx (Base register)
Применяется для хранения базового адреса некоторого объекта в памяти

6 сегментных регистров

Микропроцессор поддерживает следующие типы сегментов

- **Сегмент кода (содержит команды программы)**

  регистр **cs (code segment register)** - содержит адрес сегмента кода
- **Сегмент данных (обрабатываемые программой данные)**

  регистр **ds (data segment register)** - содержит адрес сегмента данных
- **Сегмент стека (область памяти, называемая стеком)**

  регистр **ss (stack segment register)** - содержит адрес сегмента стека
- **Дополнительные сегменты данных**
  - Если программе недостаточно одного сегмента данных, то она имеет возможность использовать еще три дополнительных сегмента данных.
  - Адреса дополнительных сегментов данных содержатся в регистрах

    es, gs, fs (extension data segment registers)

    es - сегментный регистр экстракодов (Extra Segment)

    fs,gs (следующие буквы в латинском алфавите после e)

Сегментные регистры ВСЕГДА 16-разрядные

Сегментные регистры

Биты 15 0

CS		Регистр сегмента команд
DS		Регистр сегмента данных
ES		Регистр дополнительного сегмента данных
FS		Регистр дополнительного сегмента данных
GS		Регистр дополнительного сегмента данных
SS		Регистр сегмента стека

Регистр управления

eip/ip (Instraction Pointer register)

регистр-указатель команд

Содержит смещение следующей подлежащей выполнению команды (относительно текущего сегмента кода) и связан с регистром сегмента кода CS

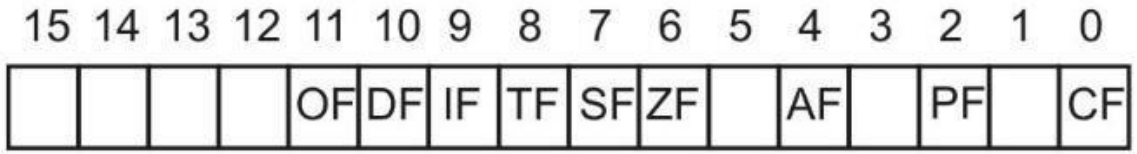
!!! Этот регистр непосредственно недоступен программисту.
При выполнении команды значение в регистре увеличивается автоматически (на длину команды),
Если команда относится к командам управления (переходы, циклы, вызовы подпрограмм и возвращения из подпрограмм, включая программные прерывания), то изменение его значения производится самими командами

Регистр состояния (микропроцессора) = **Регистр флагов**

eflags/flags

- содержит информацию о состоянии микропроцессора
- отдельные биты регистра имеют определенное функциональное назначение и называются флагами
- флаги имеют условные имена

Регистр состояния (FLAGS) процессора Intel 8086



- CF — флаг переноса при арифметических операциях,
- PF — флаг четности результата,
- AF — флаг дополнительного переноса,
- ZF — флаг нулевого результата,
- SF — флаг знака (старший бит результата),
- TF — флаг пошагового режима (для отладки),
- IF — флаг разрешения аппаратных прерываний,
- DF — флаг направления при строковых операциях,
- OF — флаг переполнения.

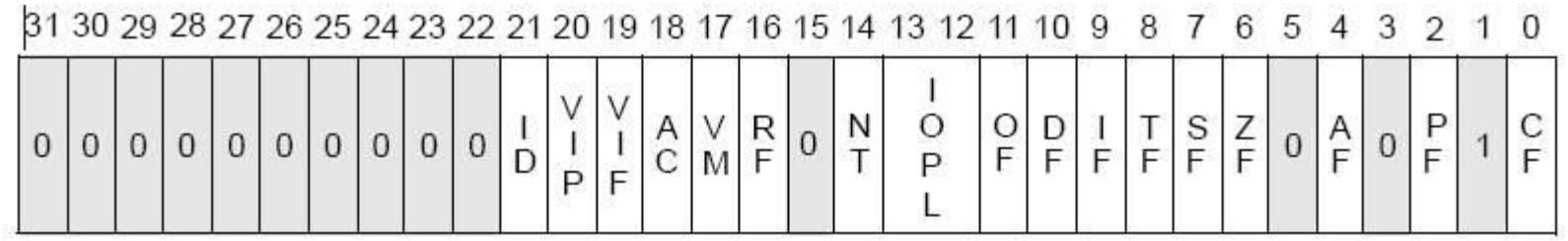
(Пока) необходимо понимать флаги:
CF
PF
ZF
SF
TF
IF
OF

Системный флаг if - Флаг прерывания (Interrupt enable Flag)
Предназначен для разрешения или запрещения (маскирования) аппаратных прерываний
(1 - аппаратные прерывания разрешены; 0 - запрещены)

! А что случится, если злоумышленник будет постоянно переводить флаг IF в 0?

Системный флаг tf - флаг трассировки (Trace Flag)
Предназначен для организации пошаговой работы микропроцессора (при отладке)

Регистр EFLAGS (32 бита)



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)

nt - флажок вложенности задачи (Nested Task)
Используется в защищенном режиме работы микропроцессора для фиксации того, что одна задача вложена в другую

Регистры IA-64

- 128 целочисленных регистров общего назначени
- 128 регистров для вычислений с плавающей точкой

они доступны программисту, являются регистрами с произвольным доступом

В процессорах x86 -
8 целочисленных регистров общего назначения

- 128 регистров специального назначения
- 8 регистров переходов
- 64 однобитных регистра предиката

Учить-запоминать
не надо
Только для сравнения!