Архитектура IA-32.

Два основных режима:

1. Real Address Mode (реальный режим);
2. Protected Virtual Address Mode (защищенный режим).

Новые возможности защищенного режима:

1. дополненный регистровый файл;
2. новые механизмы сегментации и страничной адресации;
3. режим виртуального процессора 8086 - Virtual 8086 Mode (V86);
4. добавления к системе команд.

Новый дополнительный режим - System Management Mode (режим системного управления)

Набор РОН включает в себя:

регистры 16-разрядных процессоров 8086/8088, но в 32 бита.

К обозначениям регистров добавлена приставка E (Extended - расширенный):

EAX, EBX, ECX, EDX, ESI, EDI, EBP, ESP.

Возможно обращение к младшим 16 разрядам – AX, BX,

а также отдельно к младшим и старшим байтам – AL, AH.

Регистр состояния процессора FLAGS расширен до 32 разрядов и обозначается – EFLAGS.

Флаги 16-разрядных процессоров с 0 по 11 разряд занимают такое же положение в EFLAGS.

Добавлены новые флаги:

- **ID Flag** (ID, 21 бит) – Если возможно программно устанавливать и сбрасывать этот флаг, процессор поддерживает команду CPUID.
- **Virtual Interrupt Pending** (VIP, 20 бит) – Указывает на то, что остались прерывания, ожидающие обработку. Устанавливается и сбрасывается программно, процессор только считывает его значение.
- **Virtual Interrupt Flag** (VIF, 19 бит) – Образ флага IF для режима V86.
- **Alignment Check** (AC, 18 бит) – Флаг контроля выравнивания. При установке этого флага во время обращении к невыровненному операнду возникает исключение.
- **Virtual-8086 Mode** (VM, 17 бит) – Включает/выключает режим V86 в защищенном режиме.
- **Resume Flag** (RF, 16 бит) – Флаг возобновления исполнения при отладке.
- **Nested Task** (NT, 14 бит) – Флаг вложенной задачи. Устанавливается, когда текущая задача связана с прерванной задачей, очищается, если такой связи нет.
- **I/O Privilege Level** (IOPL, 12-13 биты) – определяет уровень привилегий ввода/вывода для текущей задачи.

Сегментные регистры – CS, SS, DS, ES – 16 бит.

FS и GS – дополнительные сегментные регистры данных.

В **реальном режиме** сегментные регистры определяют 64Кб сегменты.

В **защищенном режиме** сегментные регистры содержат ***указатели*** (т.н. ***селекторы***) на описатели сегментов (64-разрядные ***дескрипторы***), находящиеся в памяти в виде таблиц.

Дескриптор содержит:

1. базовый адрес,
2. предельный размер сегмента,
3. атрибуты сегмента (права доступа).

Существуют две обязательные дескрипторные таблицы:

1. ***глобальная*** (GDT),
2. ***дескрипторная таблица прерывания*** (IDT),

а также множество (до 8192) ***локальных дескрипторных таблиц*** (LDT), из которых в один момент времени процессору доступна только одна.

Расположение дескрипторных таблиц определяется регистрами процессора:

1. **GDTR** (Global Descriptor Table Register),
2. **IDTR** (Interrupt Descriptor Table Register),
3. **LDTR** (Local Descriptor Table Register).

Регистры GDTR и IDTR - 6-байтные – содержат 32 бита линейного базового адреса дескрипторной таблицы и 16 бит предела таблицы.

Программно доступная часть регистра LDTR - 16 бит – *селектор LDT*.

***Дескрипторы LDT находятся в GDT*.**

Но, чтобы не обращаться каждый раз к GDT, в процессоре имеется ***теневая (программно недоступная) часть регистра LDTR***, в которую процессор помещает дескриптор LDT при каждой перегрузке селектора в регистре LDTR.

<u>Значение сегментного регистра (селектор) содержит:</u>

1. индекс дескриптора в дескрипторной таблице;
2. бит, определяющий, к какой дескрипторной таблице производится обращение (LDT или GDT);
3. запрашиваемые права доступа к сегменту.

селектор выбирает дескрипторную таблицу

↓

выбирает дескриптор из таблицы

↓

по дескриптору определяется положение сегмента в линейном пространстве памяти.

Обращение к дескрипторным таблицам происходит только при загрузке селектора в сегментный регистр

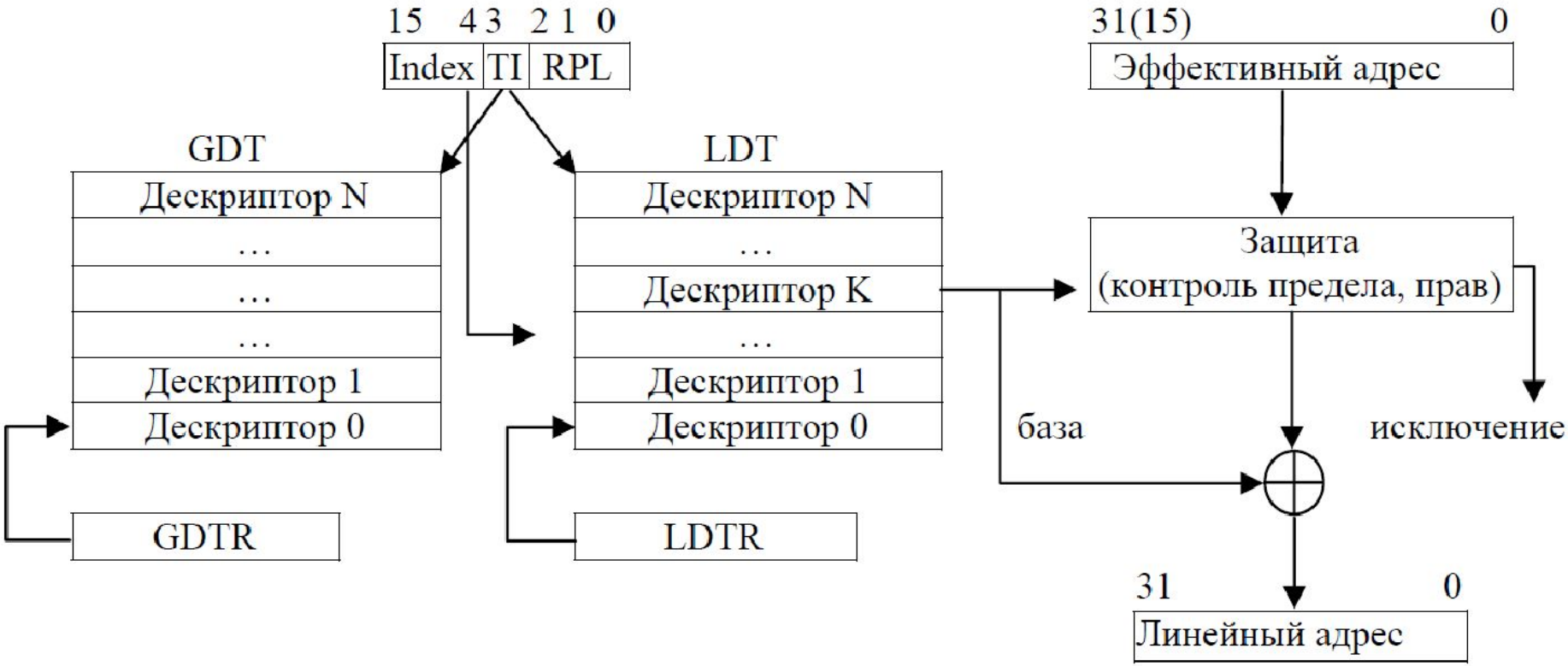
↓

процессор помещает дескриптор в теневую часть сегментного регистра.

При формировании линейного адреса дескриптор сегмента процессору уже известен.

Сегментная адресация в защищенном режиме

Сегментный регистр содержит селектор:



В используются также **защищенном режиме** 32-разрядные:

1. **регистры управления CR0-CR3**,
2. **регистры отладки DR0-DR7,**
3. **регистры проверки TR0-TR7**.

Страничное преобразование адресов:

базовый объект адресации – блок фиксированного размера (4Кбайт и/или 4 Мбайт) – **страница**.

В страничном преобразовании участвуют два типа структур:

1. каталоги таблиц,
2. таблицы страниц.

Их положение в памяти определяется физическим адресом, записанным в **регистр управления CR3**.

Для включения страничной переадресации устанавливают **31 бит (Paging) в регистре CR0**.

В **защищенном режиме** возможны **дополнительные методы адресации**.

Команды имеют длину от 1 до 15 байт.

Им могут предшествовать префиксные байты.

Кроме префиксов REP и SEG, введены **новые префиксы**:

1. размера операнда SIZ (operand SIZe), для переключения 16- и 32 –разрядных операндов;
2. размера адреса ADDRSIZ (ADDRess SIZe) - для переключения 16- и 32 –разрядных адресов.

Для новых методов адресации в формат команды добавлено поле **SIB** (Scale Index Base), которое определяет:

1. масштаб,
2. индексный регистр,
3. базовый регистр.

Эффективный адрес определяется как сумма значений базового регистра, смещения в команде и индексного регистра, умноженного на масштабный коэффициент (1, 2, 4, 8).

Примеры команд с новыми методами адресации приведены в следующей таблице:

Метод адресации	Пример команд
Индексный с масштабированием и смещением	mov eax, [2*esi + 100h]
Базовый индексный с масштабированием	mov eax, [ebp + 4*esi]
Базовый индексный с масштабированием и смещением	mov eax, [ebp + 8*esi + 10h]