Защищенный режим работы процессора.

Материалы по дисциплине «Микропроцессорные системы»
Специальность «Компьютерные системы и комплексы»
Составитель: Торгашин Р.Г

ГБПОУ ВО "Борисоглебский техникум промышленных и информационных технологий"

2016 год

Оглавление

Реальный режим (real mode)

После инициализации (системного сброса) центральный процессор находится в реальном режиме. В реальном режиме центральный процессор работает как очень быстрый i8086 с возможностью использования 32-битных расширений. Механизм адресации, размеры памяти и обработка прерываний (с их последовательными ограничениями) микропроцессор 8086 полностью совпадают с аналогичными функциями других микропроцессоров с 32-битной Intel архитектурой в реальном режиме.

В этом режиме в процессоре отключаются все функции защиты и поддержка страниц памяти, адресное пространство ограничивается 1 МБ физической памяти и используется адресация по сегментам и смещениям. Такой режим обеспечивает совместимость с процессорами i8086, i8088 и i80186, а также с реальным режимом процессора i80286.

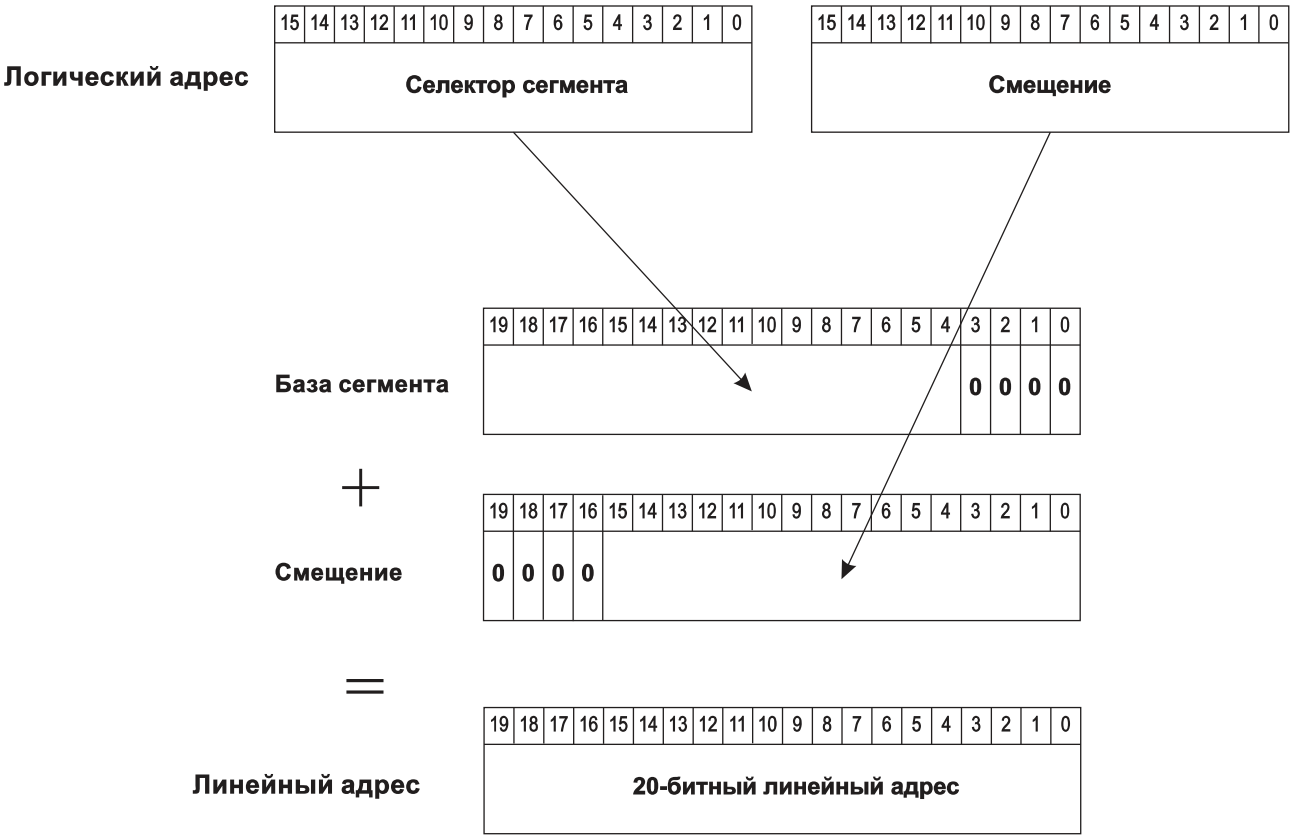

Рисунок 1: Формирование линейного адреса в реальном режиме работы процессора

Вообще говоря, режим реальных адресов в современных процессорах предназначен для запуска компьютера и подразумевается, что операционная система будет работать в защищённом режиме (поэтому оптимизация по производительности для процессоров IA-32 производится для защищённого режима).

В режиме реальных адресов не доступны основные достоинства процессора - виртуальная память, мультизадачность, уровни привилегий, работа с кэшами, буферами TLB, буфером ветвлений и некоторыми другими технологиями, обеспечивающими высокую производительность

Имеется две фиксированные области в памяти, которые резервируются в режиме реальной адресации:

- область инициализации системы
- область таблицы прерываний

Ячейки от 00000h до 003FFH резервируются для векторов прерываний. Каждое из 256 возможных прерываний имеет зарезервированный 4-байтовый адрес перехода. Ячейки от FFFFFFF0H до FFFFFFFFH резервируются для инициализации системы.

Защищенный режим (Protected Mode)

Основным режимом работы микропроцессора является защищенный режим. Ключевыми особенностями защищенного режима являются: виртуальное адресное пространство, защита и многозадачность.

В защищенном режиме программа оперирует адресами, которые могут относиться к физически отсутствующим ячейкам памяти, поэтому такое адресное пространство называется *виртуальным*. Размер виртуального адресного пространства программы может превышать емкость физической памяти и достигать 64Тбайт. Для адресации виртуального адресного пространства используется **сегментированная модель**, в которой адрес состоит из двух элементов: селектора сегмента и смещения внутри сегмента. С каждым сегментом связана особая структура, хранящая информацию о нем, - дескриптор. Кроме "виртуализации" памяти на уровне сегментов существует возможность "виртуализации" памяти при помощи страниц - **страничная трансляция.** Страничная трансляция предоставляет удобные средства для реализации в операционной системе функций подкачки, а кроме того в процессорах P6+ обеспечивает 36-битную физическую адресацию памяти (64Гбайт).

Работа механизма формирования линейного адреса в защищенном режиме работы процессора основана на двух специальных таблицах, размещаемых в памяти. Это **глобальная таблица дескрипторов (GDT) и локальная таблица дескрипторов (LDT)** (есть еще таблица дескрипторов прерываний, но она используется только при генерации прерываний и особых ситуаций ситуаций). Эти таблицы создаются и заполняются до переключения в защищенный режим, они содержат описания используемых программой сегментов памяти (базовый адрес, размер, тип, привилегии доступа и т.п.). Селектор сегмента, являющийся частью сформированного логического адреса в защищенном режиме содержит не базу физического адреса сегмента, а указатель на описание сегмента (дескриптор сегмента) в какой-либо таблице дескрипторов (LDT или GDT). Из выбранного таким образом дескриптора и смещения (вторая часть логического адреса) процессор автоматически вычисляет требуемый линейный адрес.

Положение таблиц дескрипторов в памяти задается следующим образом: для таблицы **GDT** — 32-разрядным значением ее линейного адреса в регистре GDTR, для таблицы **LDT** — специальным дескриптором в таблице **GDT**, ссылка на который (селектор) помещается в регистр LDTR.

Помимо дескрипторов сегментов кода и данных таблицы **LDT** и **GDT** могут содержать и ряд *специальных дескрипторов*, предназначенных для корректного переключения задач и обработки прерываний.

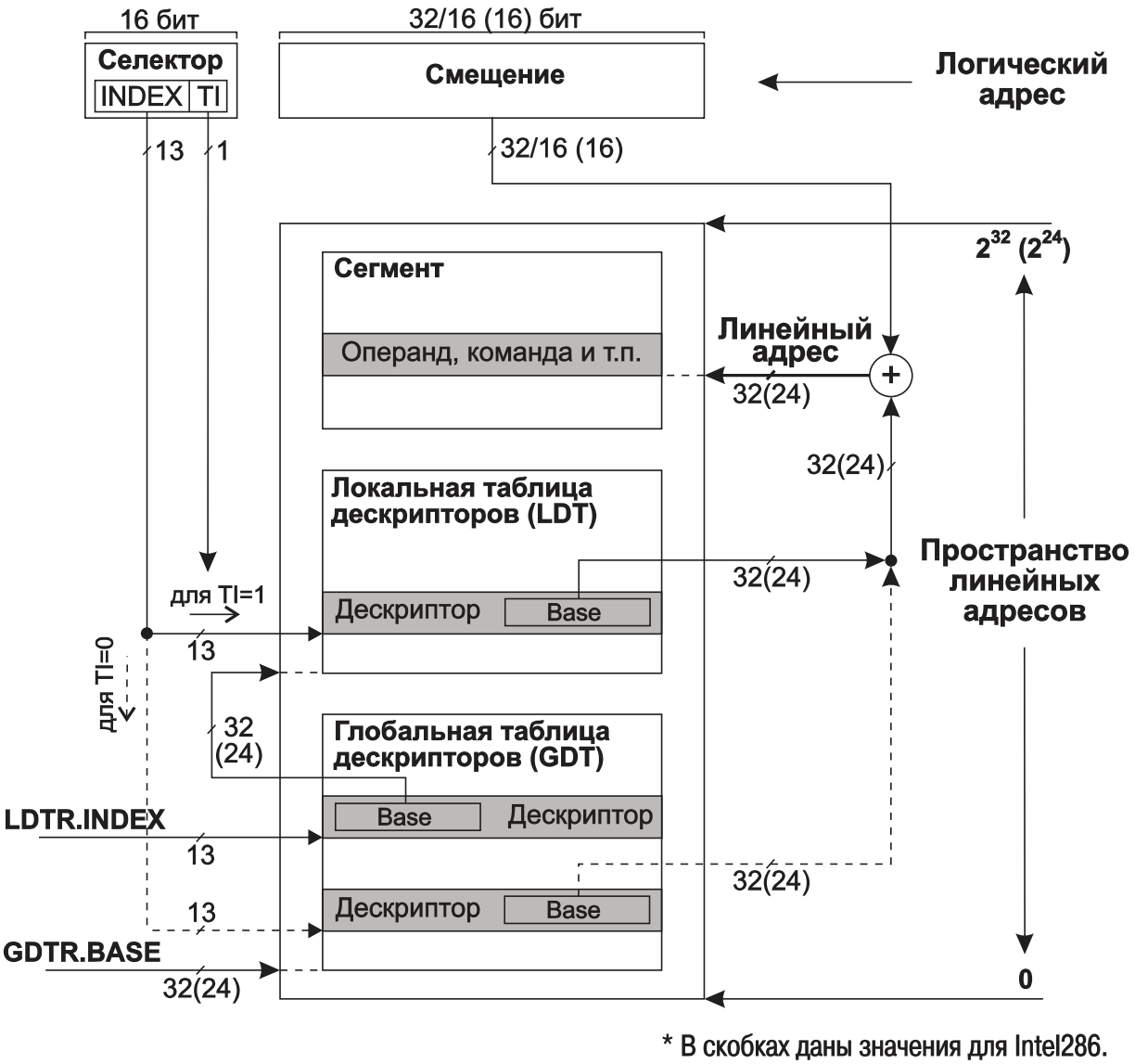

Рисунок 2: Процесс формирования линейного адреса в защищенном режиме работы процессора

Встроенные средства переключения задач обеспечивают ***многозадачность* в защищенном режиме.** Среда задачи состоит из содержимого регистров МП и всего кода с данными в пространстве памяти. Микропроцессор способен быстро переключаться из одной среды выполнения в другую, имитируя параллельную работу нескольких задач. Для некоторых задач может эмулироваться управление памятью как у процессора 8086. Такое состояние задачи называется *режимом виртуального 8086 (Virtual 8086 Mode)*. О пребывании задачи в таком состоянии сигнализирует бит VM в регистре флагов. При этом задачи виртуального МП 8086 изолированы и защищены, как от друг друга, так и от обычных задач защищенного режима.

Защита задач обеспечивается следующими средствами: контроль пределов сегментов, контроль типов сегментов, контроль привилегий, привилегированные инструкции и защита на уровне страниц. **Контроль пределов и типов сегментов** обеспечивает целостность сегментов кода и данных. Программа не имеет права обращаться к виртуальной памяти, выходящей за предел того или иного сегмента. Программа не имеет права обращаться к сегменту данных как к коду и наоборот. **Архитектура защиты микропроцессора обеспечивает 4 иерархических уровня привилегий**, что позволяет ограничить задаче доступ к отдельным сегментам в зависимости от ее текущих привилегий. Кроме того, текущий уровень привилегий задачи влияет на возможность выполнения тех или

иных специфических команд (привилегированных инструкций). Функции страничной трансляции, впервые появившиеся в МП Intel386, обеспечивают дополнительные механизмы защиты на уровне страниц.

Уровни привилегий. (Уровни защиты)

Для того, чтобы прикладная программа пользователя не смогла разрушить систему, каждая группа программ выполняется на своем уровне привилегий. При этом ошибки в программах, имеющих низкий уровень привилегий, никак не отражаются на работе программ, работающих на более высоком уровне привилегий.

Фирма Intel предложила в своем процессоре i80386 четырехуровневую систему привилегий на уровне сегмента.

Процессоры x86 поддерживают четыре уровня привилегий для сегментов программ и данных. Уровень 0 самый привилегированный, уровень 3 наименее привилегированный. Корпорация Intel рекомендует процессам занимать следующие уровни привилегий:
0 - ядро операционной системы;
1 - операционная система;
2 - системы программирования и базы данных;
3 - прикладные (пользовательские) программы.

На каждом уровне привилегий проверяется:

1. Может ли программа выполнить указанную подпрограмму?
2. К данным каких программ может обратиться та или иная программа?
3. Имеет ли программа право передавать управлению внешнему процессу и какому именно?

Рассмотрим накладываемые ограничения:

1. Привилегированные команды, управляющие сегментацией или влияющие на механизм защиты, могут работать только на нулевом уровне привилегий.

2. Программам не разрешается считывать/записывать элементы данных, которые имеют более высокий уровень привилегий. Однако программы могут использовать данные на своем и более низком уровне привилегий.

3. Передача управления внешним процедурам возможна, только если они имеют тот же уровень привилегий, что и исходный процесс.

Передача управления между уровнями привилегий.

Довольно часто встречается ситуация, когда необходимо передать управление между уровнями привилегий. Например, такая ситуация возникает при необходимости вызова стандартной подпрограммы операционной системы из прикладной программы. Или позволить прикладной программе прочитать данные из ядра операционной системы. Поскольку защита по привилегиям не разрешает такие действия напрямую, это осуществляется двумя косвенными методами: с использованием сегментов подчиненного кода и шлюзов вызова.

Режим системного управления (System Management Mode)

Режим системного управления предназначен для выполнения некоторых действий с возможностью их полной изоляции от прикладного программного обеспечения и даже операционной системы. Переход в этот режим возможен только аппаратно. Когда процессор находится в режиме SMM, он выставляет сигнал SMIACT#. Этот сигнал может служить для

включения выделенной области физической памяти (System Management RAM), так что память SMRAM можно сделать доступной только для этого режима.

Следует отметить, что в режиме SMM не предусмотрена работа с прерываниями и особыми случаями.

При возврате из SMM (по инструкции RSM) процессор восстанавливает свой контекст из SMRAM. Обработчик может программно внести изменения в образ контекста процессора, тогда процессор перейдет не в то состояние, в котором произошел переход в SMM.

Если переход произошел во время выполнения инструкции HLT, то дальнейшие действия при выходе из SMM определяются значением поля "Auto HALT Restart": процессор может снова вернуться к инструкции останова или перейти к выполнению следующей команды. Если SMI произошло при выполнении инструкции ввода-вывода, то в зависимости от значения поля "I/O Instruction Restart" возможен рестарт инструкции ввода вывода.

Эти особенности режима системного управления позволяют использовать его для реализации системы управления энергосбережением компьютера или функций безопасности и контроля доступа.

Переключение между режимами

После инициализации процессор находится в реальном режиме. Процессор может быть переведен в защищенный режим установкой бита 0 (Protect Enable) в регистре CR0.

Вернуться в режим реального адреса процессор может по сигналу RESET или (в отличие от 80286) сбросив бит PE.

Режим системного управления изолирован от других режимов. Процессор переходит в этот режим только аппаратно: по низкому уровню на контакте SMI# или по команде с шины APIC (Pentium+). Никакой программный способ не предусмотрен для перехода в этот режим. Процессор возвращается из режима системного управления в тот режим, при работе в котором был получен сигнал SMI#. Возврат происходит по команде RSM. Эта команда работает только в режиме системного управления и в других режимах не распознается, генерирую исключение #6 (недействительный код операции).

Характеристика	RM	PM, VM=0	PM, VM=1	SMM
Формирование линейного адреса	без дескрипторов	с дескрипторами	без дескрипторов	без дескрипторов
Предел сегментов	64K	определяется дескриптором	64K	4Г
Размер адреса/данных по умолчанию	16 бит	определяется дескриптором	16 бит	16 бит
Максимальный объем доступной памяти (виртуальной)	1M	64T	1M	4Г
Защита	Нет*	Да	Да	Нет
Страничное преобразование	Нет	Да	Да	Нет
Многозадачность	Нет	Да	Да	Нет
Обработка прерываний	таблица векторов	дескрипторная таблица	дескрипторная таблица	Нет**

* В реальном режиме контролируется предел сегментов.

** После определенных подготовительных действий возможна работа с прерываниями как в реальном режиме.

64-х разрядный расширенный режим IA-32 (AMD64, x86’’64, EM64T)

Этот режим процессора является расширением архитектуры IA-32, разработанным компанией AMD и в дальнейшем поддержанным Intel. Процессоры, поддерживающие 64-разрядные расширения, могут работать в реальном режиме (8086), режиме IA-32 или IA-32e. При использовании режима IA-32 процессор может работать в защищенном или виртуальном реальном режиме. Режим IA-32e позволяет работать в 64-разрядном режиме или в режиме совместимости, что подразумевает возможность одновременного выполнения 64- и 32-разрядных приложений. Режим IA-32e включает в себя два подрежима.

- 64-разрядный режим. Позволяет 64-разрядной операционной системе выполнять 64-разрядные приложения.
- Режим совместимости. Позволяет 64-разрядной операционной системе выполнять 32-разрядные приложения.

Первый подрежим активизируется после загрузки 64-разрядной операционной системы и используется 64-разрядными приложениями. В 64-разрядном подрежиме доступно несколько новых функций:

- 64-разрядная линейная адресация памяти;
- Поддержка физической памяти объемом более 4 Гбайт (определенные ограничения накладываются процессором);
- 8 новых регистров общего назначения GPR (General-Purpose Register);
- 8 новых регистров для поточных расширений SIMD (MMX, SSE, SSE2 и SSE3);
- 64-разрядные регистры GPR и указатели инструкций.

Режим совместимости IE-32e позволяет запускать 32- и 16-разрядные приложения под управлением 64-разрядной операционной системы. К сожалению, старые 16-разрядные программы, работающие в виртуальном реальном режиме (например, приложения DOS), не поддерживаются, а значит, их выполнение невозможно. Данное ограничение наверняка будет представлять наибольшую проблему для пользователей. Подобно 64-разрядному режиму, режим совместимости активизируется операционной системой для отдельных приложений, благодаря чему становится возможным одновременное выполнение 64- и 32-разрядных приложений.

Для того чтобы все эти приложения работали, необходима 64-разрядная операционная система и, что гораздо важнее, 64-разрядные драйверы для всех устройств, предназначенные именно для этой операционной системы.

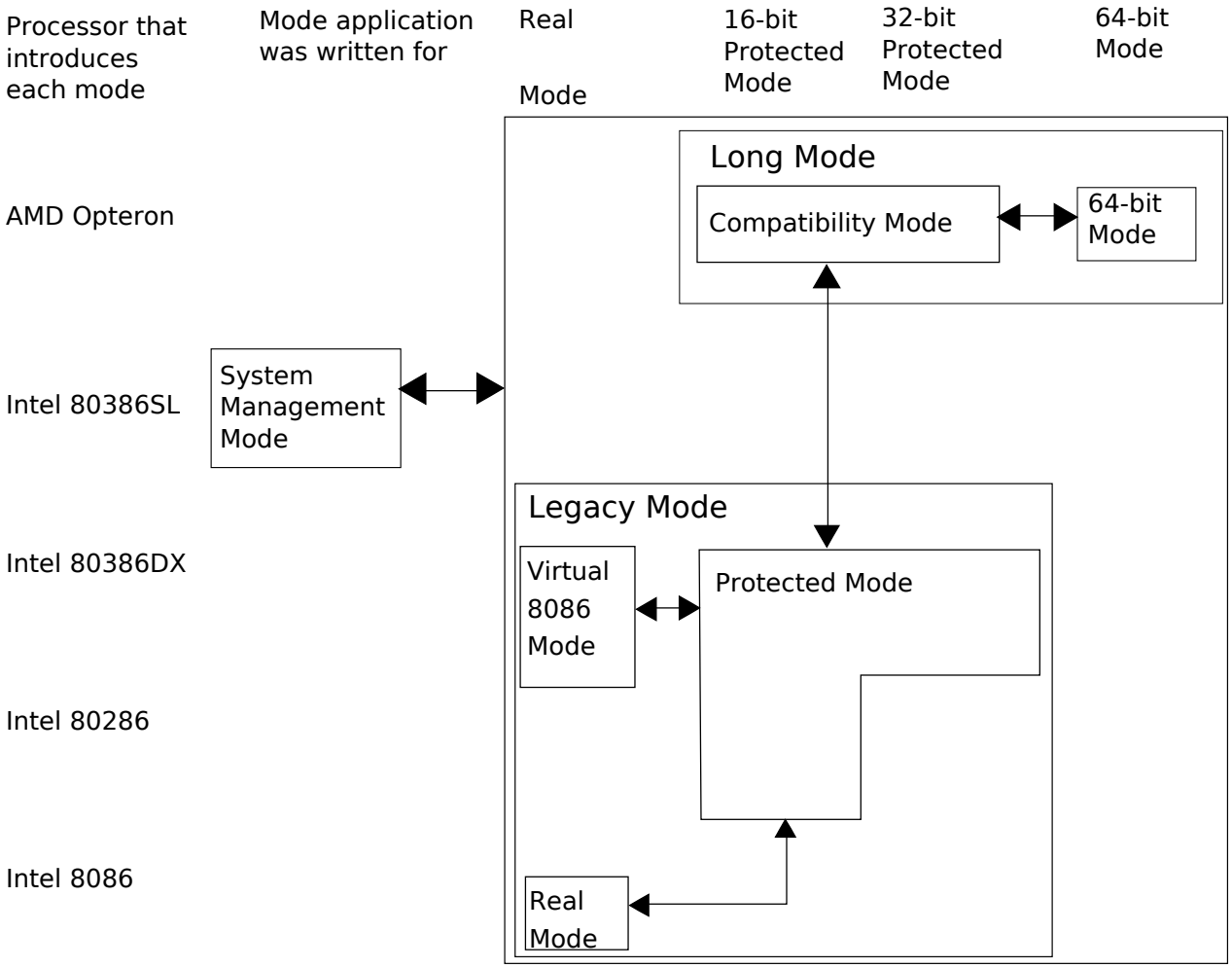

Рисунок 3: Автор: Jesse Viviano - собственная работа, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=9390252

Источники

Режимы работы микропроцессора http://dims.karelia.ru/x86/env_1.shtml
Адресация и многозадачность: Правила формирования линейного и физического адреса http://www.club155.ru/x86addr-lineaddress
Юрий А. Денисов Е.4. Уровни защиты.: http://citforum.ru/hardware/memory/mem_0505.shtml

Вопросы для контроля

1. Назовите основные особенности работы процессора в реальном режиме.
2. Для чего используется реальный режим в большинстве современных компьютеров?
3. Перечислите недостатки и ограничения реального режима.
4. Назовите основные особенности работы процессора в защищенном режиме.
5. Какие модели памяти используются для адресации виртуального адресного пространства?
6. Что такое глобальная таблица дескрипторов и для чего она предназначена?
7. Что такое локальная таблица дескрипторов и для чего она предназначена?
8. Из чего состоит среда задач?
9. Какие средства предназначены для защиты задач?
10. Назовите основные особенности работы процессора в режиме системного управления.
11. Для чего используется режим системного управления?
12. Как происходит переключение между режимами?
13. Как работает механизм иерархических уровней привилегий?
14. Для чего предназначен механизм иерархических уровней привилегий?
15. В каких режимах может работать процессор поддерживающий 64-х разрядный расширенный режим IA-32?
16. Какие новые функции доступны в 64-х разрядном расширенном режиме IA-32?
17. Какие приложения не поддерживаются в 64-х разрядном расширенном режиме?
18. Какие условия должны быть выполнены для использования возможностей 64-х разрядного режима?