Практическое задание 4

1. Ответить на вопросы

1. В каких режимах может работать IA-32?

   Реальный режим (Real Mode), Режим системного управления (System Management Mode), Защищенный режим (Protected Mode), режим супервизора, режим пользователя.

2. Как формируется физический адрес при сегментной адресации?

   Таким образом, для формирования физического адреса при сегментной адресации в 32-битных микропроцессорах семейства Intel IA-32 необходимо выполнить следующие шаги:

   Извлечь номер селектора сегмента из инструкции или данных программы.

   Получить из таблицы дескрипторов сегментов информацию о базовом адресе сегмента и его размере по индексу, соответствующему номеру селектора.

   Сложить смещение внутри сегмента с базовым адресом сегмента.

   Получить физический адрес, который будет использован для обращения к памяти.

3. Как формируется физический адрес при страничной адресации?

   физический адрес в 32-битных микропроцессорах семейства Intel IA-32 формируется путем комбинации индексов директории таблицы страниц, таблицы страниц и страницы, а также смещения, и преобразуется блоком страничного преобразования в физический адрес физической памяти, где расположены данные.

4. Что такое многозадачность? Какими средствами она поддерживается?

   Многозадачность - это возможность операционной системы обрабатывать несколько задач одновременно. Каждая задача получает часть времени процессора для выполнения своих вычислений.

   Процессор постоянно проверяет наличие прерываний, которые могут вызвать переключение контекста и передачу управления другой задаче. Контекст задачи содержит информацию о ее состоянии, включая значения регистров процессора, счетчика команд, таблицы страниц и другие параметры.

5. Какие правила на основе привилегий применяются для защиты сегментов кода, стека и данных?

   В IA-32 используются четыре уровня привилегий:

   Уровень 0 (Ring 0) - наивысший уровень привилегий, обычно используется для ядра операционной системы;

Уровень 1 (Ring 1) и уровень 2 (Ring 2) - используются для драйверов устройств и другого системного программного обеспечения;

Уровень 3 (Ring 3) - самый низкий уровень привилегий, используется для приложений.

Каждый сегмент имеет тип сегмента, который указывает на его назначение и определяет правила доступа к нему. Сегменты могут быть:

Кодовыми сегментами - содержащими исполняемый код;

Сегментами данных - содержащими данные;

Стековыми сегментами - содержащими стек операндов.

Правила на основе привилегий применяются следующим образом:

Во время выполнения инструкции процессор проверяет уровень привилегий текущего кодового сегмента и текущего стекового сегмента, а также уровень привилегий текущей инструкции.

Если уровень привилегий текущего кодового и стекового сегментов меньше или равен уровню привилегий текущей инструкции, то процессор разрешает выполнение инструкции. В противном случае происходит исключение привилегированности, и выполнение программы прерывается.

Если инструкция пытается обратиться к данным в сегменте данных или стековом сегменте, то процессор проверяет разрешение на чтение или запись данных в соответствующем сегменте. Если уровень привилегий текущего сегмента меньше или равен уровню привилегий текущей инструкции, и разрешение

2. Используя учебный материал составить терминологический словарь, состоящий по объему из 20 терминов и определений.

1. Реальный режим (Real Mode) - это один из режимов работы процессора в архитектуре IA-32, в котором процессор работает как быстрый 8086, используя механизм адресации и размеры памяти, аналогичные 8086, с возможностью использования 32-битных расширений.

2. Режим системного управления (System Management Mode) - это режим работы процессора в архитектуре IA-32, который используется для выполнения специальных функций с возможностью изоляции от прикладного программного обеспечения и операционной системы. Он позволяет реализовывать функции энергосбережения и переходит в этот режим только аппаратно.

3. System Management RAM (SMRAM) - это выделенная область физической памяти, которая может быть включена при работе в режиме системного управления (SMM) для обработки System Management Interrupt (SMI) и сохранения контекста процессора. Доступ к SMRAM может быть ограничен только для режима SMM.

4. Режим SMM (System Management Mode) - это специальный режим работы процессора, который предназначен для реализации функций управления энергосбережением компьютера или функций безопасности и контроля доступа. В этом режиме обработка прерываний замаскирована, и точки останова отключены. При возврате из режима SMM происходит восстановление контекста МП из SMRAM.

5. Защищенный режим (Protected Mode) - это режим работы процессора, в котором программа оперирует с виртуальными адресами, а не с физическими. В защищенном режиме предусмотрена защита памяти и многозадачность. Преобразование логического адреса в физический происходит в два этапа: трансляция адреса в соответствии с сегментированной моделью памяти и страничное преобразование.

6. IDT (Interrupt Descriptor Table) - это таблица дескрипторов прерываний, которая используется в защищенном режиме для обработки прерываний. Каждый дескриптор прерывания содержит информацию о типе прерывания, его адресе и правах доступа к обработчику прерывания. Инициализация IDT и разрешение прерываний необходимы для работы с прерываниями в режиме SMM.

7. Сегментированная модель адресации - это система адресации в компьютерных системах, в которой программа памяти представлена группой независимых адресных блоков, называемых сегментами, и для адресации байта памяти программа должна использовать логический адрес, состоящий из селектора сегмента и смещения.

8. Дескриптор - это 8-байтная единица описательной информации, распознаваемая устройством управления памятью в защищенном режиме, хранящаяся в дескрипторной таблице. Дескриптор сегмента содержит базовый адрес описываемого сегмента, предел сегмента и права доступа к сегменту.

9. Дескрипторная таблица - это массив памяти переменной длины, содержащий 8-байтные элементы: дескрипторы. Дескрипторная таблица может иметь длину от 8 байт до 64 Кбайт и содержит информацию о базовых адресах, пределах и правах доступа к сегментам памяти.

10. GDT - это дескрипторная таблица в операционной системе, содержащая дескрипторы сегментов и системные дескрипторы, которые доступны всем задачам в системе.

11. LDT - это дескрипторная таблица в операционной системе, связанная с конкретной задачей, которая содержит только дескрипторы сегментов, шлюзы вызовов и шлюзы задач, и обеспечивает изоляцию сегментов программы и данных исполняемой задачи от других задач.

12. IDT - это дескрипторная таблица в операционной системе, содержащая только шлюзы задач, шлюзы прерываний или шлюзы ловушек. IDT используется для обработки прерываний и исключений в процессоре.

13. Механизм сегментации - это способ организации виртуальной памяти, при котором адресное пространство процесса разбивается на логические сегменты, каждый из которых может иметь свои права доступа и храниться в разных областях физической памяти.

14. Страничное преобразование - это способ организации виртуальной памяти, при котором адресное пространство процесса разбивается на фиксированные блоки физической памяти - страницы, каждая из которых может быть размещена в любой области физической памяти и иметь свои права доступа.

15. Каталог таблиц страниц и таблицы страниц - это структуры данных, используемые в страничном преобразовании для хранения информации о соответствии виртуальных адресов страницам физической памяти. Каталог таблиц страниц содержит указатели на таблицы страниц, а таблицы страниц содержат записи о соответствии виртуальных адресов страницам физической памяти.

16. Страничная трансляция - процесс преобразования логических адресов, используемых программами, в физические адреса, которые используются для доступа к памяти компьютера. Это позволяет разделить физическую память на страницы определенного размера, что облегчает управление памятью и повышает безопасность системы.

17. Расширение физического адреса (Physical Address Extension - PAE) - технология, реализованная в процессорах Intel, которая позволяет увеличить адресное пространство физической памяти до 64 Гбайт. Это достигается путем расширения ширины адресной шины до 36 бит, что позволяет обрабатывать большее количество адресов.

18. Расширение размера страниц (Page Size Extension - PSE) - технология, реализованная в процессорах Intel, которая позволяет использовать страницы размером 4 Мбайт вместо стандартных страниц размером 4 Кбайт. Это уменьшает количество записей в таблице страниц и ускоряет процесс трансляции адресов.

19. Задача - это "единица измерения" заданий для процессора, которую процессор может выполнять, приостанавливать и осуществлять над ней диспетчеризацию. В качестве задачи может исполняться прикладная программа, сервис операционной системы, ядро операционной системы, обработчик прерывания или исключения и т.п.

20. Среда задачи состоит из содержимого регистров МП и всего кода с данными в пространстве памяти. МП способен быстро переключаться из одной среды выполнения в другую, имитируя параллельную работу нескольких задач. Для некоторых задач может эмулироваться управление памятью, как у МП 8086. Такое состояние задачи называется режимом виртуального 8086 (Virtual 8086 Mode).