**Практическое задание по лекции 4**

**Ответы на вопросы лекция 4**

**1. *В каких режимах может работать IA-32?***

IA-32 может работать в трёх режимах:

- реальный режим;

- защищённый режим;

- режим системного управления.

**2. *Как формируется физический адрес при сегментной адресации?***

Суть сегментной адресации заключается в следующем. Физический 20-разрядный адрес любой ячейки памяти вычисляется процессором путем сложения начального адреса сегмента памяти, в котором располагается эта ячейка, со смещением к ней (в байтах) от начала сегмента, которое иногда называют относительным адресом.

**3. *Как формируется физический адрес при страничной адресации?***

Преобразование логического адреса в физический происходит в два этапа: сначала блок управления сегментами выполняет трансляцию адреса в соответствии с сегментированной моделью памяти, получая 32-битный линейный адрес, а затем блок страничного преобразования выполняет разбиение на страницы, преобразуя 32-битный линейный адрес в 32-битный или 36-битный (P6) физический.

**4. *Что такое многозадачность? Какими средствами она поддерживается?***

Многозадачность - свойство операционной системы или среды выполнения обеспечивать возможность параллельной обработки нескольких задач.

Встроенные средства переключения задач обеспечивают многозадачность в защищенном режиме. В защищенном режиме архитектура IA-32 предоставляет механизм для сохранения состояния задачи и переключения с одной задачи на другую. Все команды процессора выполняются в контексте той или иной задачи. 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.

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

- Программа не должна обращаться за пределы сегмента, обозначенные лимитом;

- Программа не должна обращаться к сегменту данных как к коду и наоборот;

- Программа может обратиться к сегменту данных, который находится на том же или более низком уровне привилегий (с учетом RPL), т.е. доступ к данным разрешен, если max(CPL, RPL)<= DPL; в противном случае генерируется нарушение общей защиты;

- Контроль привилегий при доступе к стеку осуществляется при загрузке селектора в регистр SS. Программа должна использовать сегмент стека, находящийся на том же уровне привилегий, т.е. CPL = RPL = DPL.

- Для передачи управления на обычный сегмент кода его уровень привилегий должен совпадать с текущим уровнем привилегий. Значение RPL должно быть не больше CPL, чтобы не вызывать исключения, но вне зависимости от значения RPL уровень привилегий не изменится: CPL = DPL.

**Словарь лекция 4**

Реальный режим - это режим работы процессоров архитектуры x86, при котором используется сегментная адресация памяти. В реальном режиме МП работает как очень быстрый 8086 с возможностью использования 32-битных расширений.

Механизм адресации - это способ формирования исполнительного адреса операнда по адресному коду команды. Способ адресации существенно влияет на параметры процесса обработки информации.

Прерывание - одна из базовых концепций вычислительной техники, которая заключается в том, что при наступлении какого-либо события происходит передача управления специальной процедуре, называемой обработчиком прерываний.

Инициализация - создание, активация, подготовка к работе, определение параметров. Приведение программы или устройства в состояние готовности к использованию. Термин употребляется как для программных, так и для аппаратных средств.

Таблица прерываний - таблица векторов прерываний, которая используется в архитектуре x86 и служит для определения корректного ответа на прерывания и исключения. В первом слове элемента таблицы записана компонента смещения, а во втором - сегментная компонента адреса обработчика прерывания.

Режим системного управления - режим исполнения на процессорах x86/x86-64, при котором приостанавливается исполнение другого кода, и запускается специальная программа, хранящаяся в SMRAM в наиболее привилегированном режиме.

Архитектура процессора - количественная составляющая компонентов микроархитектуры вычислительной машины.

Обработчик прерываний (процедура обслуживания прерываний) - специальная процедура, вызываемая по прерыванию для выполнения его обработки. Обработчики прерываний могут выполнять множество функций, которые зависят от причины, которая вызвала прерывание.

Сегментные регистры – регистры, которые предназначены для того, чтобы указать на сегменты, к которым программа имеет доступ в конкретный момент времени. Фактически в этих регистрах содержатся адреса ячеек памяти, с которых начинаются соответствующие сегменты.

Защищённый режим - режим работы x86-совместимых процессоров. Частично был реализован уже в процессоре 80286, но там существенно отличался способ работы с памятью, так как процессоры ещё были 16-битными, и не была реализована страничная организация памяти.

Сегментная адресация памяти - схема логической адресации памяти компьютера в архитектуре x86. Линейный адрес конкретной ячейки памяти, который в некоторых режимах работы процессора будет совпадать с физическим адресом, делится на две части: сегмент и смещение.

Страничная адресация памяти - механизм управления памятью, позволяющий, с одной стороны, разрешить задачу повышения эффективности процессов обмена информацией между уровнями иерархической памяти.

Опциональный механизм - это механизм обработки ситуаций, при котором значение переменной может отсутствовать.

Дескрипторные таблицы - это массивы памяти переменной длины, содержащие 8-байтные элементы: дескрипторы. Она может иметь длину от 8 байт до 64 Кбайт и в каждой таблице может быть до 8192 дескрипторов.

Линейный адрес (база сегмента) – это адрес, который указывает на начало сегмента в адресном пространстве.

Физический адрес (MAC-адрес) - уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet.

Многозадачность - свойство операционной системы или среды выполнения обеспечивать возможность параллельной обработки нескольких задач.

Задача - это "единица измерения" заданий для процессора, которую процессор может выполнять, приостанавливать и осуществлять над ней диспетчеризацию.

Привилегии - это свойство (обычно устанавливаемое при проектировании системы), которое определяет, какие компьютерные операции разрешаются в любой момент времени и какие доступы к памяти законны.

CPL (текущий уровень привилегий) - это уровень привилегий, на котором в данный момент исполняется задача.

DPL (уровень привилегий дескриптора) - это наименее привилегированный уровень, на котором задача может получить доступ к сегменту или шлюзу, связанному с этим дескриптором.

RPL (запрашиваемый уровень привилегий) - это уровень привилегий, который используется для временного понижения своего уровня привилегий при обращении к памяти.