

Вторая лабораторная работа – перевод компьютера в защищенный режим:

Лабораторная работа 2

Защищенный режим

Задание:

Написать программу, переводящую компьютер в защищенный режим (32-разрядный режим работы компьютеров на базе процессоров Intel). Программа начинает работать в реальном режиме. Для перевода в защищенный режим выполняются необходимые действия. В защищенном режиме программа работает на нулевом уровне привилегий.

В защищенном режиме программа должна:

- определить объем доступной физической памяти;
- осуществить ввод с клавиатуры строки с выводом введенной строки на экран;
- получить информацию на экране от системного таймера или в виде мигающего курсора, или в виде количества тиков с момента запуска программы на выполнение, или в виде значения реального времени.

Затем программа корректно возвращается в реальный режим с соответствующими сообщениями.

Для реализации поставленной задачи необходимо:

- Создать две системные таблицы – глобальную таблицу дескрипторов (GDT) для описания сегментов физической памяти, с которыми будет работать запущенная программа и таблицу дескрипторов прерываний (IDT), в которой заполняются дескрипторы прерываний, которые необходимы для выполнения поставленной задачи.
- Заполнить дескрипторы в обеих таблицах необходимой информацией.
- Заполнить селекторы значениями смещения к соответствующим дескрипторам сегментов.
- Перевести компьютер из реального в защищенный режим, установив флаг ре в 1.
- В защищенном режиме определить объем доступной физической памяти следующим образом – первый мегабайт пропустить; начиная со второго мегабайта сохранить байт или слово памяти, записать в этот байт или слово сигнатуру, прочитать сигнатуру и сравнить с сигнатурой в программе, если сигнатуры совпали, то это – память. Вывести на экран полученной количество байтов доступной памяти.
- Для ввода строки с клавиатуры необходимо написать обработчик прерывания от клавиатуры. Доступ к обработчику осуществляется через предварительно заполненный дескриптор прерывания от клавиатуры в IDT.
- Для получения информации от системного таймера необходимо написать обработчик прерывания от системного таймера. Доступ к обработчику осуществляется через предварительно заполненный необходимой информацией дескриптор прерывания от таймера в IDT.
- Если в таблице дескрипторов прерываний были пропущены первые 32 дескриптора (так сделано фирмой Microsoft), то необходимо перепрограммировать контроллер прерывания на новый базовый вектор.
- При переходе в защищенный режим необходимо открыть линию A20.
- Возвращение в реальный режим должно выполняться корректно с использованием 32-разрядных операндов.
- При переходе из режима в режим выдавать соответствующие сообщения.
- В защищенном режиме информация для вывода на экран записывается непосредственно в видеобuffer.
- Для возвращения в реальный режим выполнить необходимые действия.

Литература

1. Рудаков П.И., Финогенов К.Г. Программирование на **ASSEMBLER**. – М.: Диалог МИФИ, 2001, с.640
2. Зубков С. В. Программирование Assembler. - М.: Мир, 2004, с.685