# Первое занятие ОС

## Первая лабораторная работа

1) Состоит из двух частей, обе части офрмляем в виде отчёта в бумажном виде

Обе части связаны с системным таймером

в Операционной системе есть системный такймер - это единственное ... прерывание ()

1.1 первая часть древняя связана с DOS'ом (16 разрядная Intel 80/86)

DOS последняя версия 6.22

Дизасемблирование кода операционной системы windows xp в режиме эмуляции и получение листинга кода 8ого прерывания,

для этого используется когда специально написанная программа source'с (src.exe)

1.2 вторая часть Отдельный отчёт (сдаём почти в конце семестра) - это функция обработчика прерываний (?в системах разделения о времени?)

## Книги

Существует две книги (Вахалия unix изнутри И Марк Руссинович (wind) "главное - мастер класс")

Три семейства операционных систем:

1) Винды

2) Юникс

3) Линуксы (интересует нас)

Читаем книжки и по ним состовляем отчёты

## Вторая лаба

вторая лабораторная - Перевод компьютера из реального режима в защищённый

Реальный - 80/86

Защищённый - 32-разрядный режим

Все компьютеры запускаются в реальном режиме а потом програмно переводятся в защищённый

В защищённом режиме надо ... (клава...)

И вернуть компьютер в реальный режим (мы НЕ переводим компьютер в режим long (64-разоядный))

?Нулевого уровня привелегий?

Для этого нужно иметь вирутальную машину (например: DOSbox)

## Еще книги

Рудаков Финогенов (язык ассемблера глава - защищённый режим или Зубков, такая же глава)

Разбираем на ассемблере

Курс ассемблера является входным для дисциплины Операционных систем

## 3-4 Лабы

3, 4, 5 лабы выполняем под Линукс (напоминаем Линукс это unix-подобная операцинная система)

Фактически это лабораторные по Unix, поскольку мы затрагиваем в ней основные команды unix

### Первая (3)

Первая лабораторная (3я) это командная строка (в терминале), но нас интересует две команды:

PS - о процессах

LS - информация о файлах

...

И создаём линги (Хард и софт?)

### Вторая (4)

Вторая лаба (4ая)- 5 основных системных вызовов

### Третья (5)

Третья лаба (5ая)- взаимодействие параллельных процессов (наши системы многопроцессные)

Взаимодействовать процессы могут только на уровне данных

В этой лабе опишим две программы для двух классических ...(процессов?)

задача Производства Потребления и Читатели-Писатели

## Последняя лаба (6)

Последняя 6ая лаба - Читатель-писатель под винды(Windows)

Пишим эту задачу на потоках thread'ах (event'ы - события)

## Сдача лаб

Все лаборатные мы сдаём запуская программы

* и демонстрируя что мы можем их запустить (минимум)
* как максимум (понимаем что там происходит)
* и экстра класс (понимаем почему)

## 2ой семестр

2ой семестр выполняем под линукс (открытая операционная система)

Операционная система - это тоже программа

Линукс написан на C

Изучаем файловую подсистему

Всё это связанно с ядрой, со структурами ядра и прерываниями

## 8ое прерывание

int 8h

Выполнить дизасемблирование кода операционной системы windows xp в режиме эмуляции (w86) и получить листинга кода 8ого прерывания.

### Вложенный if (см. тетрадь)

Таблица векторов прерываний в DOS’е начинается с нулевого адреса и содержит адреса обработчиков прерываний

Любой адрес в DOS’е – 4 байта

По номеру прерывания мы получаем смещение в таблице векторов прерываний

?Используя дебаг мы указываем это смещение…?

*Нам надо получить адрес восьмого прерывания*

*Его можно получить с помощью 35ой функции*

Мы умеем получить вектор прерывания 😊

Получим 4 столбца

1. 1ый столбец – адреса типа смещения
2. Машинные команды
3. Эти же команды на ASM
4. Комментарии

Поскольку это эмуляция, там есть куски кода не связанные с 8ым прерыванием

# 2ое занятие

Еще раз: Вектор прерывания это адрес обработчика прерывание (2 байта сегмент 2 байта смещение)

Что такое тик? (см. Тетрадь)

Мы сейчас рассмотрим:

## Концептуальная трёх шинная структура

(PIC?)

В нашем компе передаются сигналы трёх типов

1. Данные (собственно данные и команды)
2. Адреса
3. Сигналы управления

Следовательно, концептуально существует три шины (данных, адреса и управления)

Сам компьютер — это процессор, остальное – внешние устройства

На контроллер прерываний приходят аппаратные прерываний

Система прерываний

1. Системные вызовы
2. Исключения
3. Аппаратные прерывания (Interrupt)

Пропущена важная информация 😊 IRQ12 – клавиатура?

?ПС пополам? (PS/2 — компьютерный порт, применяемый для подключения клавиатуры и мыши, использующий 6-контактный разъём mini-DIN.)

Контроллер формирует сигнал int который по шину управление поступает …

На контроллер прерываний приходят маскируемые прерывания

Маска запрещает прерывания

Маску, контроллер, получает по шине данных

В конце сброс контроллера прерываний?

В нашей системы два адресного пространства

* Оперативной памяти
* И портов ввода вывода

(MSI?)

В DOS’е три функции счётчика (INT 8H):

1. Инкремент счётчика таймера по известному адресу (область данных BIOS)  
   То есть кол-во тиков в этом счётчике можно перевести в реальное время  
   В составе наших компьютеров есть CMOS микросхема (энергонезависимая, которая питается от аккумулятора (наз. таблетка)) – поэтому мы видим на компьютере дату (Год, месяц, день недели и тд…)  
   Про CMOS читаем в интернете (будут спрашивать)  
   BIOS (**BASE** **input**/**output** **system**) (тоже читать в интернете?)
2. Вызов пользовательского прерывания int 1cH (вызывается 18,2 раз в секунда)  
   (как int1cH и как косвенный вызов)
3. Декремент счётчика таймера до выключения моторчика (дисковода)…?

(Почитать про винчестер – жёсткий диск?)

Файлы нужны для долговременного хранения информации

Файлы хранятся во вторичной памяти (энергонезависимой)

Непроизводительные временные затраты (тратим время на дурацкую работу, Пример: раскрутка дискеты?) => предложили выключать моторчик дисковода, только если к дисководу не было обращения в течении двух секунд. То-есть храним значение примерно = 2 секундам и каждый тик декрементируем, если = 0 дискета перестаёт крутиться – это называется отложенное действие

Смысл 3ей функции 8ого прерывания – это отложенное действие – выключение моторчика дисковода

Не может ПО отключить моторчик дисковода

Всё через порт?

Установление флага (для остальных прерываний) и установления в порт команды – классическое отложенное действие

Сброс контроллера прерывания (прочитаем у Фролова/Рудакова Финагенова) (для чего его сбрасывать)

Обработчик прерываний заканчивается iret’ом

Код до Iret’а мы игнорируем – не знаем что он делает

В отчёте будет:

1. Листинг 8ого прерывания
2. Листинг субратины (subroutine - подпрограмма) (алгоритм 8ого прерывания)
3. Этот алгоритм нарисовать схему (подумать: для чего вызывать ?…?)

Титульник берём в электронном университете с логотипом и правильными названиями (Министерство науки и образования)

8ое прерывание только на Windows XP