Прерывание int 8h

Это прерывание DOS;

Контролер прерываний

Прерывание от системного таймера;

Любая современная ОС работает под управлением прерываний;

Прерывания - двигок ОС;

Система прерываний

3 типа прерываний:

1) Системные вызовы (system call) - буквально вызов системы;

   Часто наз. программными прерываниями;

   API (Application Function Interface); предоставляет набор сист. вызовов;

   Большая часть сист. вызовов UNIX/Linux сертифицированы POSIX;

2) Исключения (исключительные ситуации);

3) Аппаратные прерывания (прерывания, поступающие от аппаратуры);

Interrupt („голое слово") - аппаратное (подразумевается) прерывание;

3 группы аппаратных прерываний:

1) Прерывание таймера (<u>одно единственное</u>)

Единственное периодическое прерывание в системе, которое возникает 18,2... раз/сек. (столько именно в DOS, а в других ОС это другие периоды);

> В совр. ОС при частоте процессоров ~ нескольких ГГц квант не может выполняться так редко

2) Прерывания от внешних устройств
Самая большая группа;

> Компьютер по фон Нейману - процессор и оперативная память;
> У процессора нет памяти;
> Регистры - не память
> (без них невозможно выполнение команд);

Информируют процессор о завершении операции ввода - вывода;

> Монитор и видеокарта - внеш. устр-ва

2 способа взаимодействия с внеш. устр-вами в Intel и Intel-подобных системах:

- memory mapping (отображение) (используются команды работы с памятью (mov));
- input/output mapping (работа процессора с внешними устройствами через порты ввода-вывода – команды in и out)

Порт – адрес;

(условное название)

Мин. адресуемый порт – 1 байт;

Итого: 2 адр. пр-ва в системе:
- адр. пр-во оперативной памяти;
- адр. пр-во портов ввода-вывода;

{Сокеты имеют порт}

В коде int 8h происходит обращение к портам дисковода и контролера прерываний (им посылаются команды out);

3) Прерывания от действий оператора

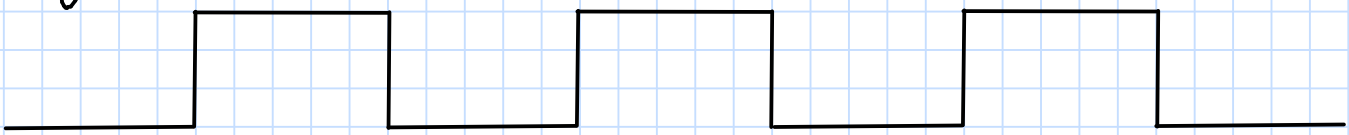
При ctrl+alt+del вызывается task manager;
В DOS нажатие ctrl+c вызывает завершение процесса;

int 8h – таймер;

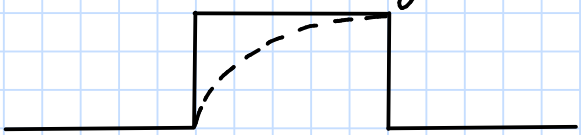
Время – способ измерения длительности событий;
А в компьютерах это доп. информация;

В любом процессоре есть тактовый генератор, генерирующий меандр — сигнал, у которого длительность „0" равна длительности „1";

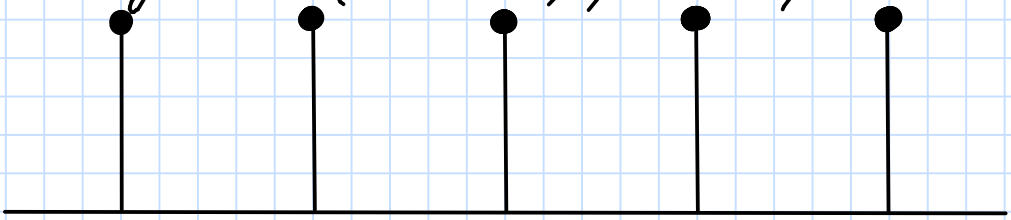
Идеально:



На самом деле:



Из этой частоты с помощью делителя (микросхемы) и линии задержки выделяются импульсы (тики), повторяемые 18,2... раз/сек; (только в DOS)



Импульс приходит на контроллер прерываний (не прийти он не может), формируется вектор прерывания, использующийся ОС для получения адреса обработчика прерывания;

В DOS по таблице векторов прерываний (начиная с нулевого адреса и занимает 256 байт);

В других (реальных?) ОС это IDT (Interrupt Descriptor Table) (уже другая таблица);

Вектор прерывания - адрес обработчика прерывания;
(4б = 2б + 2б — Far — адрес)
сегм. смещ.

Прерывание таймера вызывается по тику;

Тик приводит к переходу системы по известному адресу на выполнение обработчика прерывания;

Windows XP написана для 32-разр. систем;
Только там есть режим эмуляции DOS (выполнение 16-разр. приложений);

восемнадцать целых и две десятых раз в секунду

Программа sourcer: (листинг)
sr.exe достанет нам код прерывания int 8h;

Intel 8086

Именно в DOS появилось понятие резидентной программы;

Мы будем дизассемблировать режим V86 – virtual
– режим эмуляции DOS;

В sourcer надо указать нач. и конец. адреса, написать g (go), и у нас будет листинг:

адрес типа сегм:смещ	машинные команды в 16-ричном формате	эквивалентная команда на ассемблере	комментарии (порт... команда...)

По номеру прерывания мы получаем смещение адреса обработчика прерывания в таблице векторов прерываний;

Конец. адрес = начало + сколько занимает обработчик (примерно)

Подбираем

Конец прерывания – команда iret;

Вопрос к л/р 1: чем iret отличается от ret?

В коде int 8h есть jump, который приведёт нас к iret;

В листинге нужно указать адрес iret;

Функции обработчика 8 прерывания:

1) Инкремент счётчика реального времени;

Реальное время – (реальное) физ. время, на которое настроен компьютер;

Т.е. счётчик инкрементирует реальное время;

Счётчик находится в об-ти данных BIOS, т.е. по известному адресу в оперативной памяти;

Это возможно благодаря наличию энергонезависимой CMOS-микросхемы (питается от аккумуляторной батареи, называемой „таблетка")

→ (Читать Википедию)

Содержимое счётчика хотрется в об-ть данных BIOS;

2) Декремент счётчика времени до отключения мотора дисковода;

Дискета - гибкий диск, вставляющийся в дисковод;

В первых компьютерах на 8086 не было винчестеров, всё писалось/считалось с „флопиков" (FDD - Floppy Disk Drive);

Для чтения/записи дискету нужно было раскрутить;

Раскручиваем, пишем

Непроизводительные затраты времени, а не „долго" и „быстро"

Ф-ция отключения моторчика дисковода (отложенное действие) возложено на обработчик прерывания от системного таймера;

Отлож. действия можно вешать только на прерывание от сист. таймера (таймер, если коротко);

Такие счётчики называют d/a+m'ами;

Если дисковод простаивает 2 с. (к нему не было обращения), то его моторчик отключается;

После каждой операции ввода-вывода в счётчик записывается число, примерно равное 2 секундам;

Команда посылается на контроллер дисковода;

3) Вызов пользовательского прерывания 1Ch;

(чтобы программисты не грузили int 8h)

Объём памяти в реальном режиме – 1 Мб

Однозадачная ОС – в ОЗУ только одна исполняемая программа, потребляющая все ресурсы;

...

Приходится писать резидентные программы

...

Питер Нортон – писал программы (и называл их своим именем) и фантастические романы;

Norton Commander – программа для DOS;

Far – „воспоминание о Norton";

Получив листинг, строим схему алгоритма;

„В алгоритмах нет блоков, в них есть только элементы";

В самом начале есть sub (subroutine), её код тоже надо получить;

Итого 2 листинга:
– дизассемблер int 8h;
– дизассемблер subroutine (запрещает прерывания, то-ли есть ветвление);

+2 схемы алгоритма;

В алгоритме показать каждую команду;

Смотреть по смыслу, максимально подробно;

В алгоритме будет префиксная команда lock, которая делает следующую за ней команду неделимой (нельзя прервать);

Ещё вопросы по лабе:
Перед какой командой стоит lock?
Почему именно перед ней?