Государственное образовательное учреждение высшего профессионального образования
“Московский государственный технический университет имени Н.Э.Баумана”

Отчет
По лабораторной работе №1 (Часть 1)
По курсу "Операционные системы"
Тема: "Дизассемблирование INT 8h"

Студент: Степанов А.О.
Группа: ИУ7-53
Преподаватель: Рязанова Н.Ю.

Москва, 2019 г.

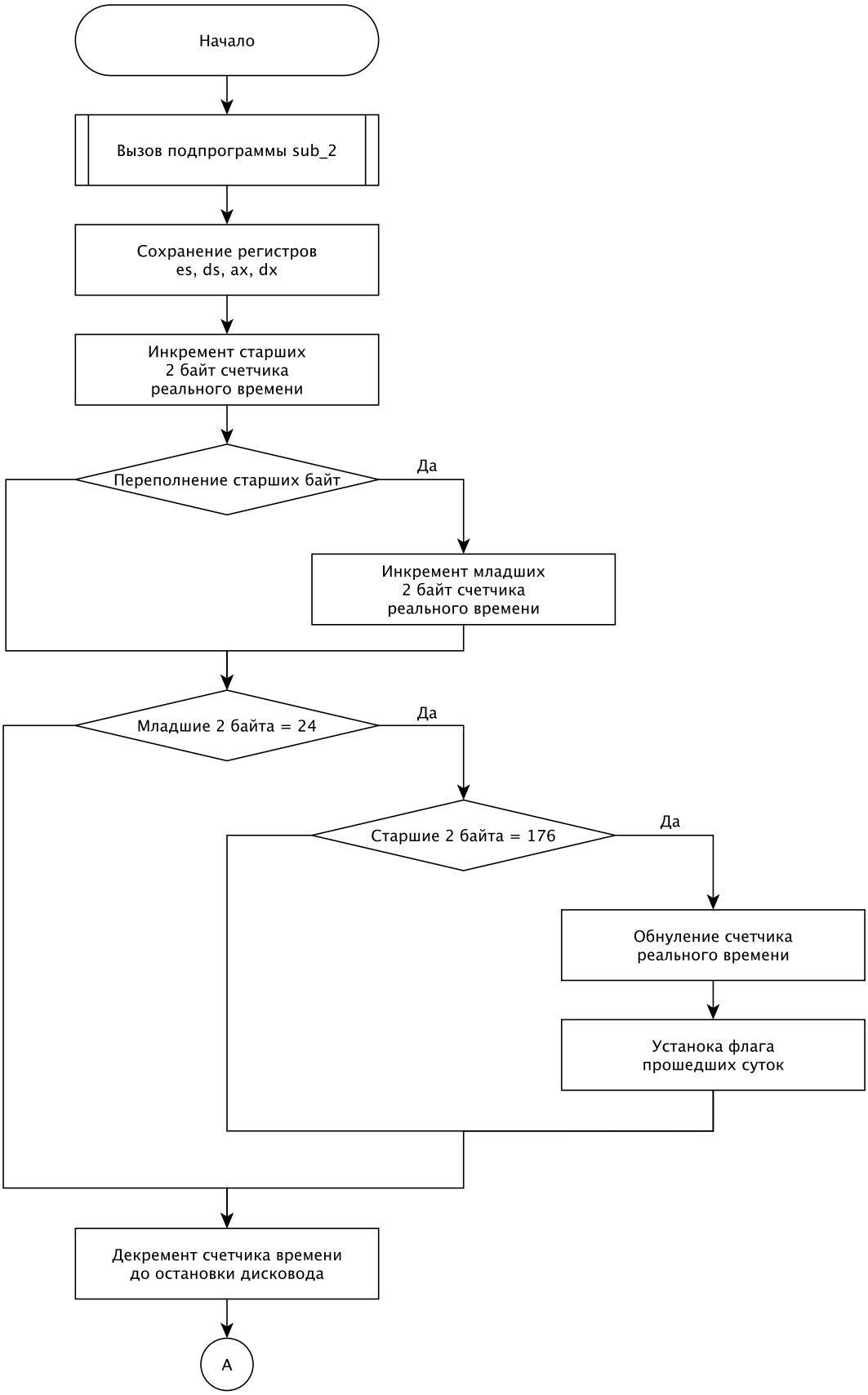
Листинг прерывания INT 8H

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Вход в прерывание, вызов подпрограммы, сохранение регистров
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:0746  E8 0070              call    sub_2           ; (07B9)
020C:0749  06                   push    es
020C:074A  1E                   push    ds
020C:074B  50                   push    ax
020C:074C  52                   push    dx
020C:074D  B8 0040              mov ax,40h
020C:0750  8E D8                mov ds,ax
020C:0752  33 C0                xor ax,ax           ; Zero register
020C:0754  8E C0                mov es,ax

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Инкремент счетчика суточного времени
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:0756  FF 06 006C               inc word ptr ds:[6Ch]   ; (0040:006C=1610h)
020C:075A  75 04                jnz loc_16          ; Jump if not zero
020C:075C  FF 06 006E               inc word ptr ds:[6Eh]   ; (0040:006E=17h)

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Сброс счетчика, если наступили новые сутки
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:0760            loc_16:                        ;  xref 020C:075A
020C:0760  83 3E 006E 18            cmp word ptr ds:[6Eh],18h   ; (0040:006E=17h)
020C:0765  75 15                jne loc_17          ; Jump if not equal
020C:0767  81 3E 006C 00B0          cmp word ptr ds:[6Ch],0B0h  ; (0040:006C=1610h)
020C:076D  75 0D                jne loc_17          ; Jump if not equal
020C:076F  A3 006E              mov word ptr ds:[6Eh],ax    ; (0040:006E=17h)
020C:0772  A3 006C              mov word ptr ds:[6Ch],ax    ; (0040:006C=1610h)
020C:0775  C6 06 0070 01            mov byte ptr ds:[70h],1 ; (0040:0070=0)
020C:077A  0C 08                or  al,8

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Декремент счетчика времени до отключения моторчика дисковода
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:077C            loc_17:                        ;  xref 020C:0765, 076D
020C:077C  50                   push    ax
020C:077D  FE 0E 0040               dec byte ptr ds:[40h]   ; (0040:0040=72h)
020C:0781  75 0B                jnz loc_18          ; Jump if not zero

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Посылка в порт дисковода команды на отключение моторчика
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:0783  80 26 003F F0            and byte ptr ds:[3Fh],0F0h  ; (0040:003F=0)
020C:0788  B0 0C                mov al,0Ch
020C:078A  BA 03F2              mov dx,3F2h
020C:078D  EE                   out dx,al           ; port 3F2h, dsk0 contrl output
020C:078E            loc_18:                        ;  xref 020C:0781
020C:078E  58                   pop ax

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Проверка на возможность вызова прерываний
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:078F  F7 06 0314 0004          test    word ptr ds:[314h],4    ; (0040:0314=3200h)
020C:0795  75 0C                jnz loc_19          ; Jump if not zero
020C:0797  9F                   lahf                ; Load ah from flags
020C:0798  86 E0                xchg    ah,al
020C:079A  50                   push    ax
020C:079B  26: FF 1E 0070           call    dword ptr es:[70h]  ; (0000:0070=6ADh)
020C:07A0  EB 03                jmp short loc_20        ; (07A5)
020C:07A2  90                   nop

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Вызов пользовательского прерывания
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:07A3            loc_19:                        ;  xref 020C:0795
020C:07A3  CD 1C                int 1Ch         ; Timer break (call each 18.2ms)
020C:07A5            loc_20:                        ;  xref 020C:07A0
020C:07A5  E8 0011              call    sub_2           ; (07B9)

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Отправка сигнала end of interrupt контроллеру прерываний
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:07A8  B0 20                mov al,20h          ; ' '
020C:07AA  E6 20                out 20h,al          ; port 20h, 8259-1 int command
                                        ;  al = 20h, end of interrupt
020C:07AC  5A                   pop dx
020C:07AD  58                   pop ax
020C:07AE  1F                   pop ds
020C:07AF  07                   pop es

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Переход по метке в сторону завершения работы прерывания
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:07B0  E9 FE99              jmp $-164h          ; (064C)


020C:06AC  CF                   iret                ; Interrupt return
```

Листинг подпрограммы sub_2

```
               sub_2       proc    near
020C:07B9  1E                  push    ds
020C:07BA  50                  push    ax
020C:07BB  B8 0040             mov ax,40h
020C:07BE  8E D8               mov ds,ax
020C:07C0  9F                  lahf                ; Load ah from flags

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Проверка на возможность вызова прерывания
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:07C1  F7 06 0314 2400         test    word ptr ds:[314h],2400h    ; (0040:0314=3200h)
020C:07C7  75 0C               jnz loc_22          ; Jump if not zero

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Запрет маскируемых прерываний (сброс if)
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:07C9  F0> 81 26 0314 FDFF             lock and word ptr ds:[314h],0FDFFh   ; (0040:0314=3200h)
020C:07D0           loc_21:                     ;  xref 020C:07D6
020:07D0  9E                   sahf                ; Store ah into flags
020C:07D1  58                  pop ax
020C:07D2  1F                  pop ds
020C:07D3  EB 03               jmp short loc_ret_23    ; (07D8)

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Запрет маскируемых прерываний
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
020C:07D5           loc_22:                     ;  xref 020C:07C7
020C:07D5  FA                  cli             ; Disable interrupts
020C:07D6  EB F8               jmp short loc_21        ; (07D0)

020C:07D8           loc_ret_23:                 ;  xref 020C:07D3
020C:07D8  C3                  retn
               sub_2       endp
```

Схема алгоритма работы обработчика прерываний 08h



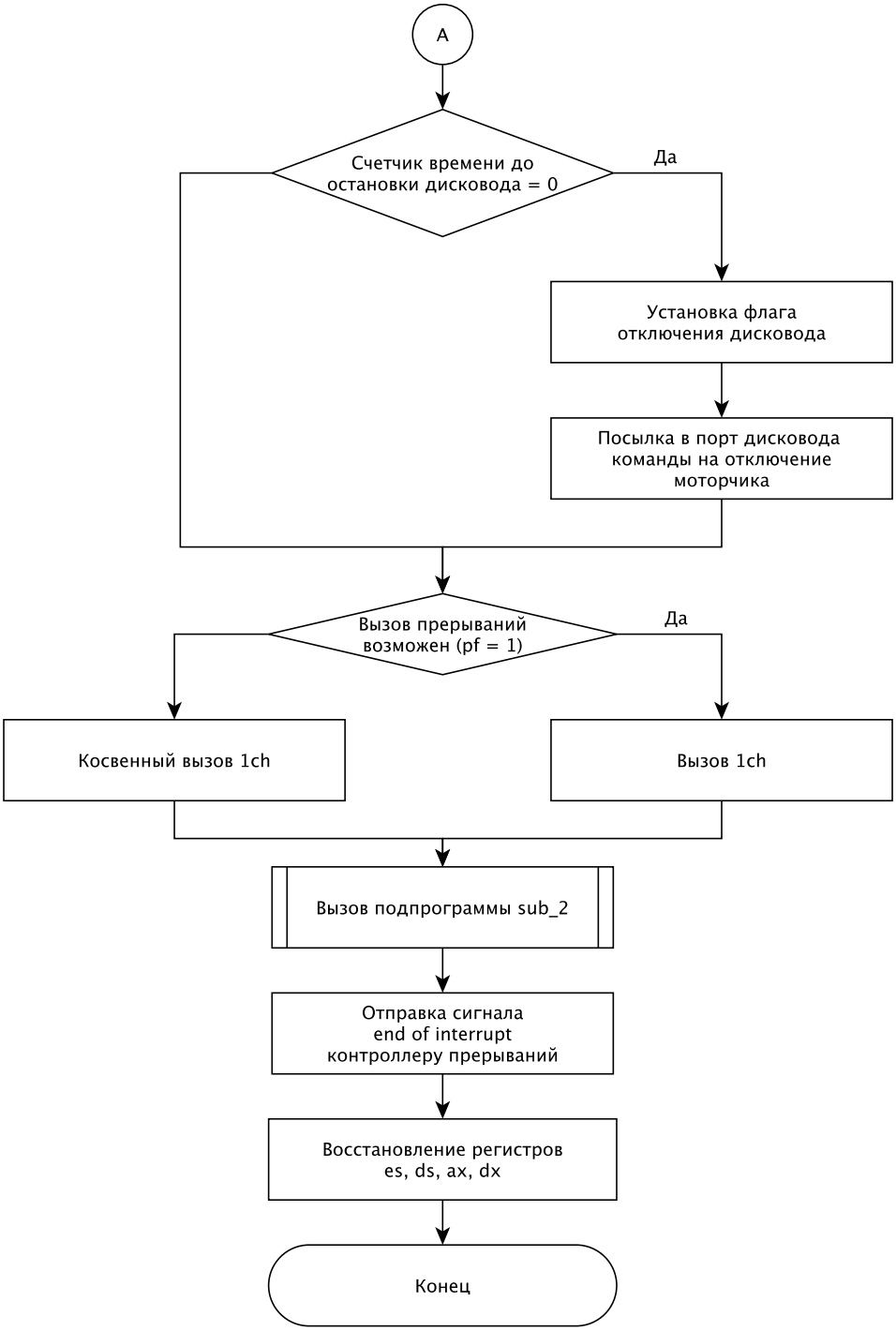

A
Счетчик времени до остановки дисковода = 0
Да
Установка флага отключения дисковода
Посылка в порт дисковода команды на отключение моторчика
Вызов прерываний возможен (pf = 1)
Да
Косвенный вызов 1ch
Вызов 1ch
Вызов подпрограммы sub_2
Отправка сигнала end of interrupt контроллеру прерываний
Восстановление регистров es, ds, ax, dx
Конец

Схема алгоритма работы подпрограммы sub_2