

Министерство науки и высшего образования Российской Федерации Федеральное государственное бюджетное образовательное учреждение высшего образования

«Московский государственный технический университет имени Н.Э. Баумана

(национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

Отчет

к лабораторной работе №1 (1 часть) по курсу «Операционные системы» по теме «Дизассемблирование INT 8h»

студентки ИУ7-55Б Оберган Татьяны

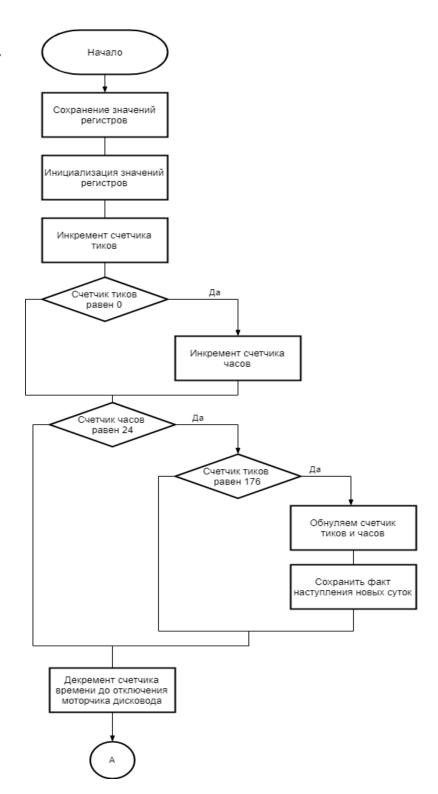
Преподаватель: Рязанова Н. Ю.

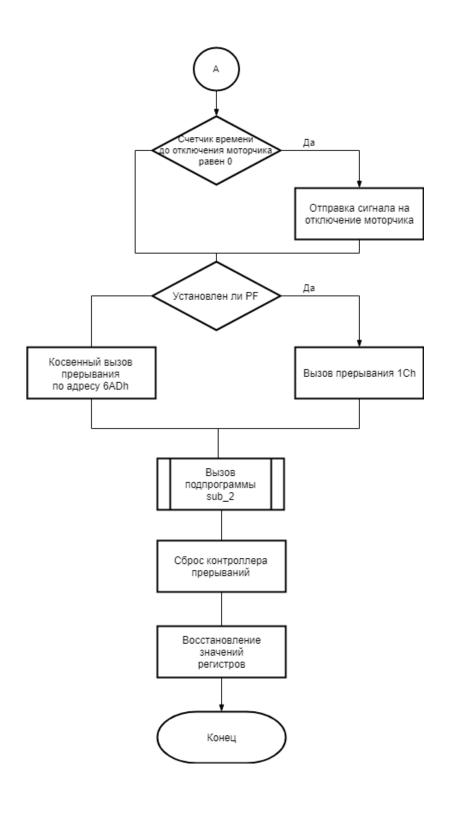
Листинг прерывания int 8h:

```
Temp.lst
                               Sourcer v5.10 15-Sep-19
                                                         8:55 pm
; вызов подпрограммы sub 2
                               ; *
020A:0746 E8 0070
                                      call
                                              sub 2
                                                                      ; (07B9)
020A:0746 E8 70 00
                               db
                                      0E8h, 70h, 00h
; сохранение значения регистров
020A:0749 06
                               push
020A:074A 1E
                                      ds
                               push
020A:074B 50
                               push
                                      ax
020A:074C 52
                               push
; инициализация значений регистров
020A:074D B8 0040
                                      ax, 40h
                               mov
020A:0750 8E D8
                               mov
                                      ds,ax
020A:0752
          33 C0
                               xor
                                      ax,ax
                                                             ; Zero register
020A:0754 8E CO
                               mov
                                      es,ax
; инкремент счетчиков времени
                                      word ptr ds:[6Ch] ; (0040:006C=0EDB8h)
020A:0756 FF 06 006C
                               inc
020A:075A
          75 04
                                      loc 1
                                                     ; Jump if not zero
                               jnz
020A:075C FF 06 006E
                                      word ptr ds:[6Eh]
                                                             ; (0040:006E=14h)
                               inc
; сброс счетчиков времени, при наступлении нового дня
020A:0760
                       loc 1:
020A:0760 83 3E 006E 18
                                      word ptr ds:[6Eh],18h ; (0040:006E=14h)
                               cmp
020A:0765
          75 15
                                      loc 2 ; Jump if not equal
                               jne
020A:0767 81 3E 006C 00B0
                                      word ptr ds:[6Ch],0B0h
                               cmp
                                       ; (0040:006C=0EDB8h)
020A:076D 75 0D
                               jne
                                      loc 2 ; Jump if not equal
020A:076F A3 006E
                               mov
                                      word ptr ds:[6Eh],ax
(0040:006E=14h)
020A:0772 A3 006C
                               mov
                                      word ptr ds:[6Ch],ax
(0040:006C=0EDB8h)
020A:0775 C6 06 0070 01
                                      byte ptr ds:[70h],1 ; (0040:0070=0)
                               mov
020A:077A OC 08
                               or
                                      al,8
; отправка сигнала отключения моторчика
020A:077C
                       loc 2:
020A:077C
          50
                               push
                                      ax
020A:077D
          FE 0E 0040
                                      byte ptr ds:[40h] ; (0040:0040=0E5h)
                               dec
020A:0781
           75 OB
                                      loc 3
                               jnz
                                                      ; Jump if not zero
           80 26 003F F0
                                      byte ptr ds:[3Fh],0F0h; (0040:003F=0)
020A:0783
                               and
          B0 0C
020A:0788
                               mov
                                      al,0Ch
          BA 03F2
020A:078A
                               mov
                                      dx,3F2h;floppy controller control port
020A:078D EE
                               out
                                      dx,al ; port 3F2h, dsk0 contrl output
; проверка возможности вызова маскируемых прерываний
020A:078E
                       loc 3:
020A:078E
          58
                               pop
                                      aх
020A:078F F7 06 0314 0004
                                      word ptr ds:[314h],4;(0040:0314=3200h)
                               test
020A:0795
          75 OC
                                      loc 4
                                                      ; Jump if not zero
                               jnz
020A:0797
          9 F
                               lahf
                                                      ; Load ah from flags
          86 E0
020A:0798
                               xchg
                                      ah,al
020A:079A
          50
                               push
                                      ax
020A:079B
          26: FF 1E 0070
                               call
                                      dword ptr es:[70h] ; (0000:0070=6ADh)
020A:07A0
          EB 03
                               jmp
                                      short loc 5
                                                      ; (07A5)
020A:07A2
          90
                               nop
                                       ;no operation
; вывоз прерывания по таймеру
020A:07A3
                       loc_4:
020A:07A3 CD 1C
                               int
                                      1Ch; Timer break (call each 18.2ms)
020A:07A5
                       loc 5:
020A:07A5 E8 0011
                               call
                                      sub 2
                                                      ; (07B9)
; сброс контроллера прерываний
                                                      , 1 1
020A:07A8
          B0 20
                               mov
                                      al,20h
020A:07AA
          E6 20
                               out
                                      20h, al
                                       ; port 20h, 8259-1 int command
                                         al = 20h, end of interrupt
```

```
; восстановление значений регистров
020A:07AC 5A
                                      dx
                              pop
020A:07AD
          58
                                      ax
                              pop
020A:07AE 1F
                                      ds
                              pop
020A:07AF
          07
                                      es
                              pop
; выход из программы
020A:07B0 E9 FE99
                                      $-164h
                              jmp
020A:07B3 C4
                              db
                                      0C4h
;* No entry point to code
020A:07B4 C4 0E 93E9
                                      cx,dword ptr ds:[93E9h]
                              les
(0000:93E9=6EEh) Load 32 bit ptr
020A:07B8 FE
                                      0FEh
```

Схема алгоритма обработки прерывания от системного таймера:



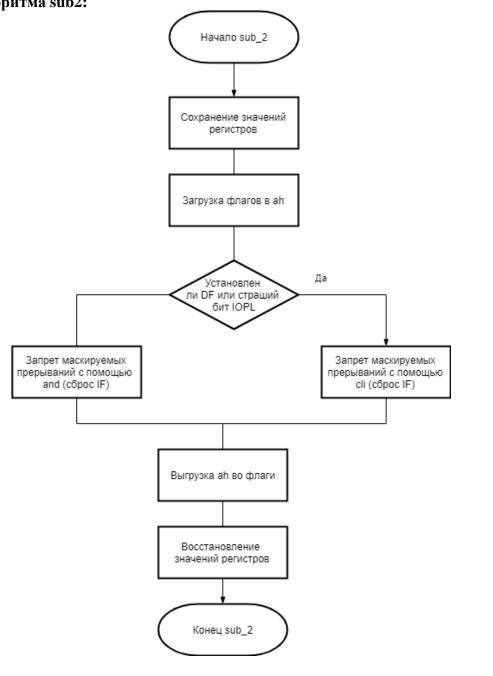


Листинг подпрограммы sub2:

```
Temp.lst
                               Sourcer v5.10 15-Sep-19
                                                         8:55 pm
                                                                     Page 2
                               proc near
                       sub 2
; сохранение значений регистров, восстановление значений флагов
020A:07B9 1E
020A:07BA 50
                               push ds
                               push
                                      ax
020A:07BB B8 0040
                                      ax,40h
                               mov
020A:07BE 8E D8
                              mov
                                      ds,ax
020A:07C0 9F
                               lahf
                                                      ; Load ah from flags
; проверка разрешены ли маскируемые прерывания
```

```
020A:07C1 F7 06 0314 2400
                            test word ptr ds:[314h],2400h
                              ; (0040:0314=3200h) 0010 0100 0000 0000
020A:07C7 75 0C jnz loc_7 ; Jump if not zero 020A:07C9 F0> 81 26 0314 FDFF lock and word ptr ds:[314h],0FDFFh
(0040:0314=3200h) ;1111 1101 1111 1111
; сохраняем значения флагов, восстанавливаем значение регистров
020A:07D0
                      loc 6:
020A:07D0 9E
                               sahf
                                                     ; Store ah into flags
020A:07D1 58
                              pop
                                      ax
020A:07D2 1F
                                     ds
                              pop
020A:07D3 EB 03
                              jmp
                                     short loc 8
                                                             ; (07D8)
; сбрасываем IF в eflags, процессор игнорирует все прерывания, кроме NMI
020A:07D5
                     loc 7:
020A:07D5 FA
                               cli
020A:07D6 EB F8
                               jmp
                                      short loc 6
                                                     ; (07D0)
020A:07D8
                       loc_8:
020A:07D8 C3
                              retn
                       sub 2
                              endp
```

Схема алгоритма sub2:



Функции обработчика прерывания 08h:

- Инкремент значения счетчика тиков.
- Контроль переполнения счетчика тиков (наступление нового дня).
- Декремент времени, оставшегося до выключения моторчика дисковода.
- Выключение моторчика дисковода, по истечению таймера.
- Вызов пользовательского прерывания 1Ch (IRET). С помощью которого можно совершать периодические действия.

Вывод:

В данной лабораторной работе я научилась получать адрес начала прерывания и листинг прерывания с помощью дизассемблера. Изучила алгоритм работы прерывания int 8h. Это прерывание отвечает за изменение счётчика системного времени, управление контроллером дисковода с целью минимизировать время работы моторчика дисковода, а также является способом периодического вызова пользовательского прерывания.