



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 (ИУ7)

**О Т Ч Е Т**

по лабораторной работе № 1

Название: Дизассемблирование INT 8h

Дисциплина: Операционные системы

Студент

ИУ7-54Б

(Группа)

\_\_\_\_\_  
(Подпись, дата)

Тартыков Л.Е.

(И.О. Фамилия)

Преподаватель

\_\_\_\_\_  
(Подпись, дата)

Рязанова Н.Ю.

(И.О. Фамилия)

Москва, 2021

# Листинг 1. Код прерывания INT8h

```
Temp.lst      Sourcer Listing v3.07      6-Sep-21  11:20 pm  Page 1
;вызов подпрограммы sub_2
020A:0746  E8 0070                      call  sub_2                      ; (07B9)

;сохранение в стеке регистров es, ds, ax, dx
020A:0749  06                          push  es
020A:074A  1E                          push  ds
020A:074B  50                          push  ax
020A:074C  52                          push  dx

;загрузка в ds адреса области данных BIOS
020A:074D  B8 0040                      mov   ax,40h
020A:0750  8E D8                      mov   ds,ax

;загрузка в es адреса начала таблицы векторов прерывания
020A:0752  33 C0                      xor   ax,ax                      ; Zero register
020A:0754  8E C0                      mov   es,ax

;инкремент младшей части счетчика системного таймера по адресу 0040:006C
020A:0756  FF 06 006C                  inc   word ptr ds:[6Ch]; (0040:006C=5899h)

020A:075A  75 04                      jnz   loc_16                    ; Jump if not zero
;инкремент старшей части счетчика, если прошел час
020A:075C  FF 06 006E                  inc   word ptr ds:[6Eh] ; (0040:006E=17h)

020A:0760                      loc_16:
;прошли ли сутки
020A:0760  83 3E 006E 18              cmp   word ptr ds:[6Eh],18h    ; (0040:006E=17h)
020A:0765  75 15                      jne   loc_17                    ; Jump if not equal

;сравнение значения счетчика с 0B0h = 176
020A:0767  81 3E 006C 00B0          cmp   word ptr ds:[6Ch],0B0h   ; (0040:006C=5899h)
020A:076D  75 0D                      jne   loc_17                    ; Jump if not equal

;обнуление счетчика времени при наступлении новых суток
020A:076F  A3 006E                      mov   word ptr ds:[6Eh],ax     ; (0040:006E=17h)
020A:0772  A3 006C                      mov   word ptr ds:[6Ch],ax     ; (0040:006C=5899h)

;запись значения 1 в ячейку с адресом 0000:0470h при наступлении новых суток
020A:0775  C6 06 0070 01              mov   byte ptr ds:[70h],1     ; (0040:0070=0)

;установка значения флага 1000 (3 бит) для порта 3F2h
020A:077A  0C 08                      or     al,8

020A:077C                      loc_17:
020A:077C  50                          push  ax

;декремент счетчика времени, оставшегося до выключения моторчика
020A:077D  FE 0E 0040                  dec   byte ptr ds:[40h] ;
(0040:0040=5Dh)
020A:0781  75 0B                      jnz   loc_18                    ; Jump if not zero

;поднятие флага отключения моторчика дисковод
020A:0783  80 26 003F F0              and   byte ptr ds:[3Fh],0F0h   ; (0040:003F=0)
;посылка команды отключения моторчика 0Ch в порт дисковод 3F2h
020A:0788  B0 0C                      mov   al,0Ch
020A:078A  BA 03F2                      mov   dx,3F2h
020A:078D  EE                      out   dx,al                    ; port 3F2h, dsk0 contrl output

020A:078E                      loc_18:
020A:078E  58                          pop   ax
```

```

;поднят ли флаг PF по адресу 0040:0314
020A:078F F7 06 0314 0004 test word ptr ds:[314h],4 ; (0040:0314=3200h)
020A:0795 75 0C jnz loc_19 ; Jump if not zero

;сохранение флагов в стеке
020A:0797 9F lahf ; Load ah from flags
020A:0798 86 E0 xchg ah,al
020A:079A 50 push ax

;косвенный вызов прерывания int 1Ch
020A:079B 26 FF 1E 0070 call dword ptr es:[70h] ; (0000:0070=6ADh)
020A:07A0 EB 03 jmp short loc_20 ; (07A5)
020A:07A2 90 nop

020A:07A3 loc_19:
;вызов прерывания 1Ch
020A:07A3 CD 1C int 1Ch ; Timer break (call each
18.2ms)
020A:07A5 loc_20:
020A:07A5 E8 0011 call sub_2 ; (07B9)

;сброс контроллера прерываний с записью 20h в порт 20h
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 регистров dx, ax, ds, es

020A:07AC 5A pop dx
020A:07AD 58 pop ax
020A:07AE 1F pop ds
020A:07AF 07 pop es

020A:07B0 E9 FE99 jmp loc_1 ; (064C)

020A:064C loc_1:
;сохранение регистров в стеке
020A:064C 1E push ds
020A:064D 50 push ax
;.....
;восстановление регистров из стека
020A:06AA loc_9:
020A:06AA 58 pop ax
020A:06AB 1F pop ds
020A:06AC CF iret ; Interrupt return

```

## Листинг 2. Код подпрограммы sub\_2

```
sub_2 proc near
;сохранение в стеке регистров ds, ax
020A:07B9 1E push ds
020A:07BA 50 push ax

;загрузка в ds адреса области данных BIOS
020A:07BB B8 0040 mov ax,40h
020A:07BE 8E D8 mov ds,ax

020A:07C0 9F lahf ; Load ah from flags

;поднят ли флаг DF или IOPL
020A:07C1 F7 06 0314 2400 test word ptr ds:[314h],2400h ; (0040:0314=3200h)

020A:07C7 75 0C jnz loc_22 Jump if not zero

;сброс флага IF при помощи зануления 9-ого бита
020A:07C9 F0> 81 26 0314 FDFF lock and word ptr ds:[314h],0FDFFh
; (0040:0314=3200h)

020A:07D0 loc_21:
020A:07D0 9E sahf ; Store ah into flags

;восстановление регистров ax, ds
020A:07D1 58 pop ax
020A:07D2 1F pop ds
020A:07D3 EB 03 jmp short loc_23 ; (07D8)

020A:07D5 loc_22:
;сброс флага прерывания IF командой cli
020A:07D5 FA cli ; Disable interrupts
020A:07D6 EB F8 jmp short loc_21 ; (07D0)
020A:07D8 loc_23:
020A:07D8 C3 retn
sub_2 endp
```

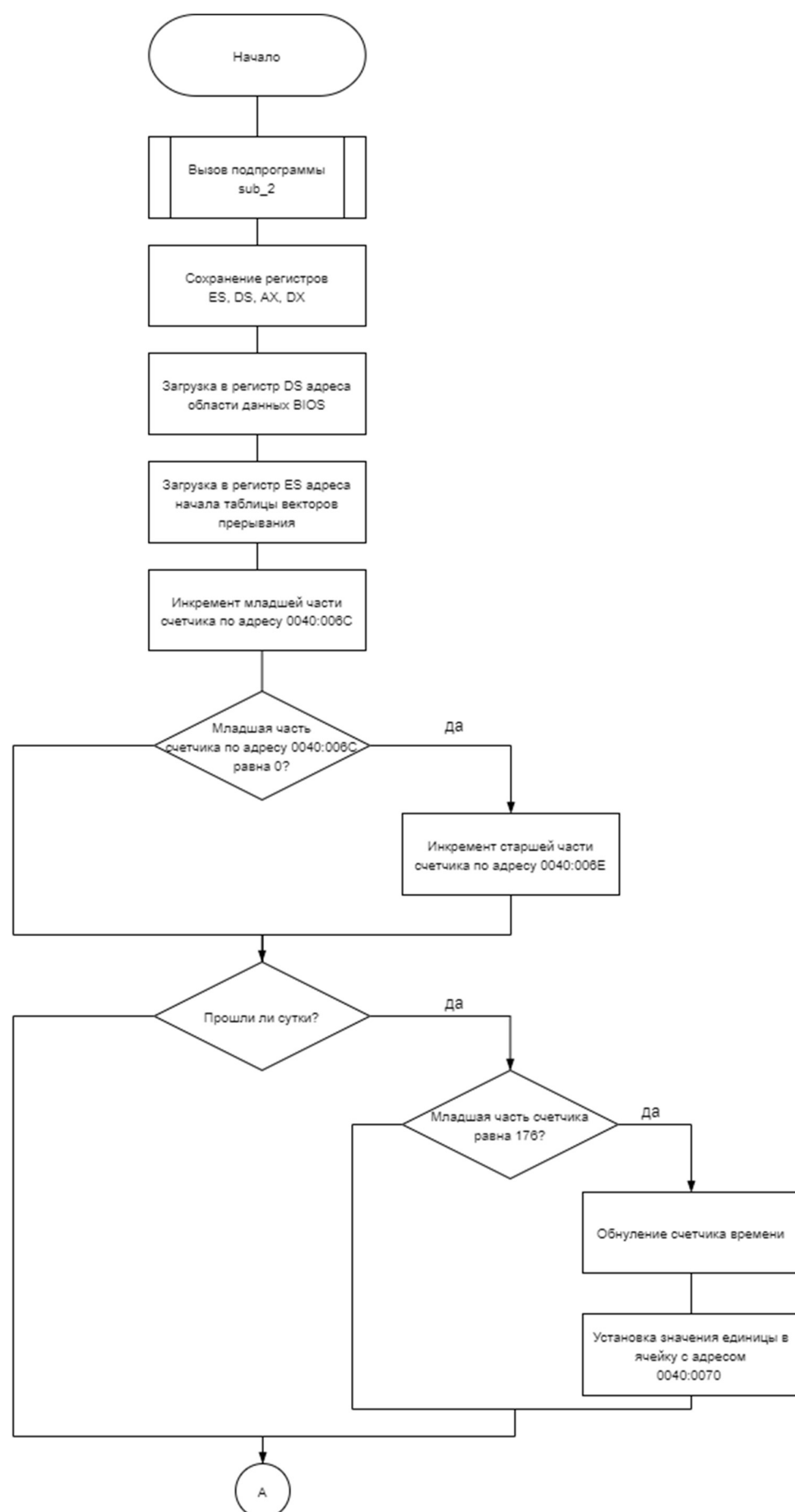


Рисунок 1 – Схема алгоритма int 8h

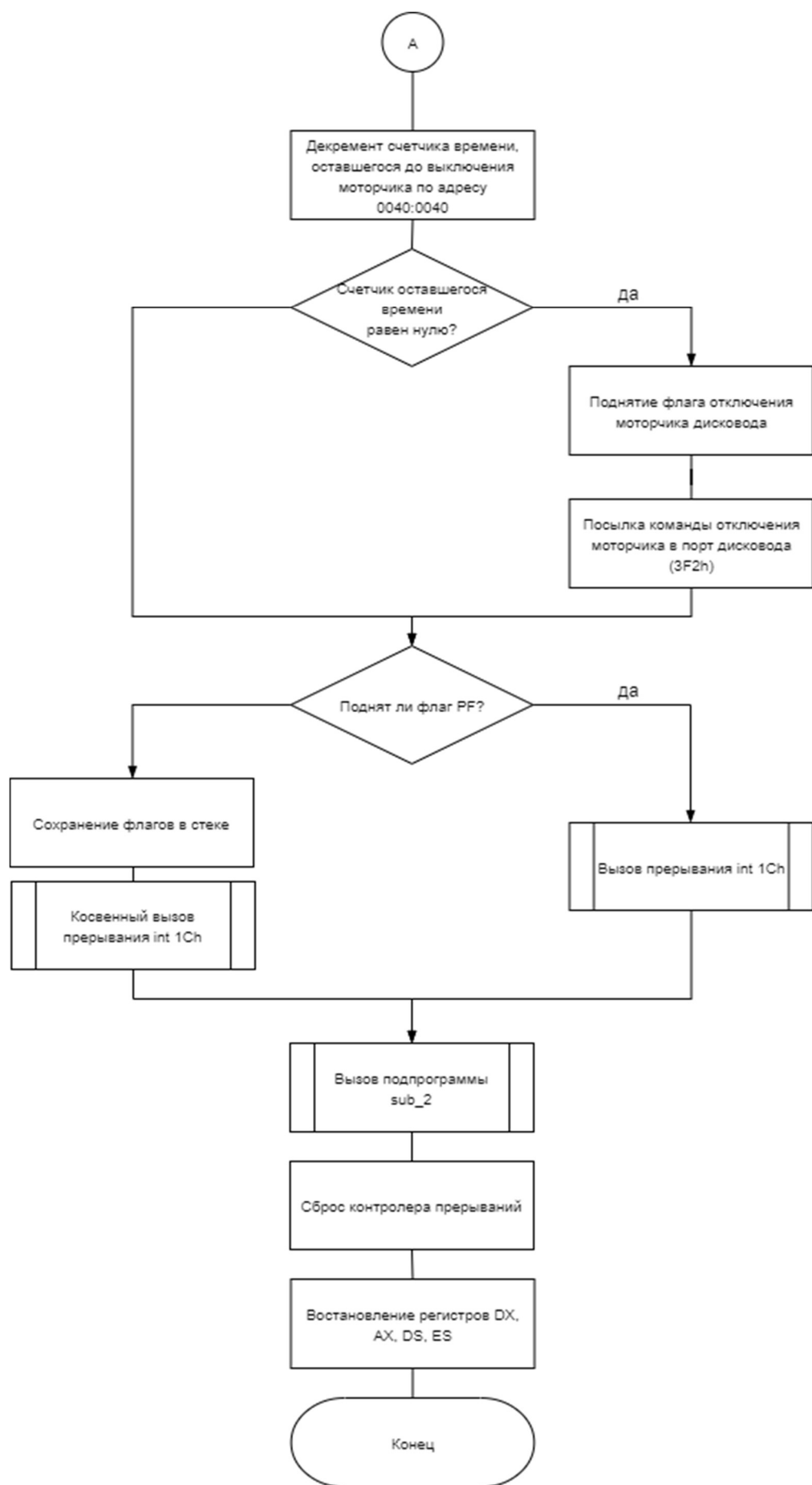


Рисунок 2 – Схема алгоритма int 8h (продолжение)

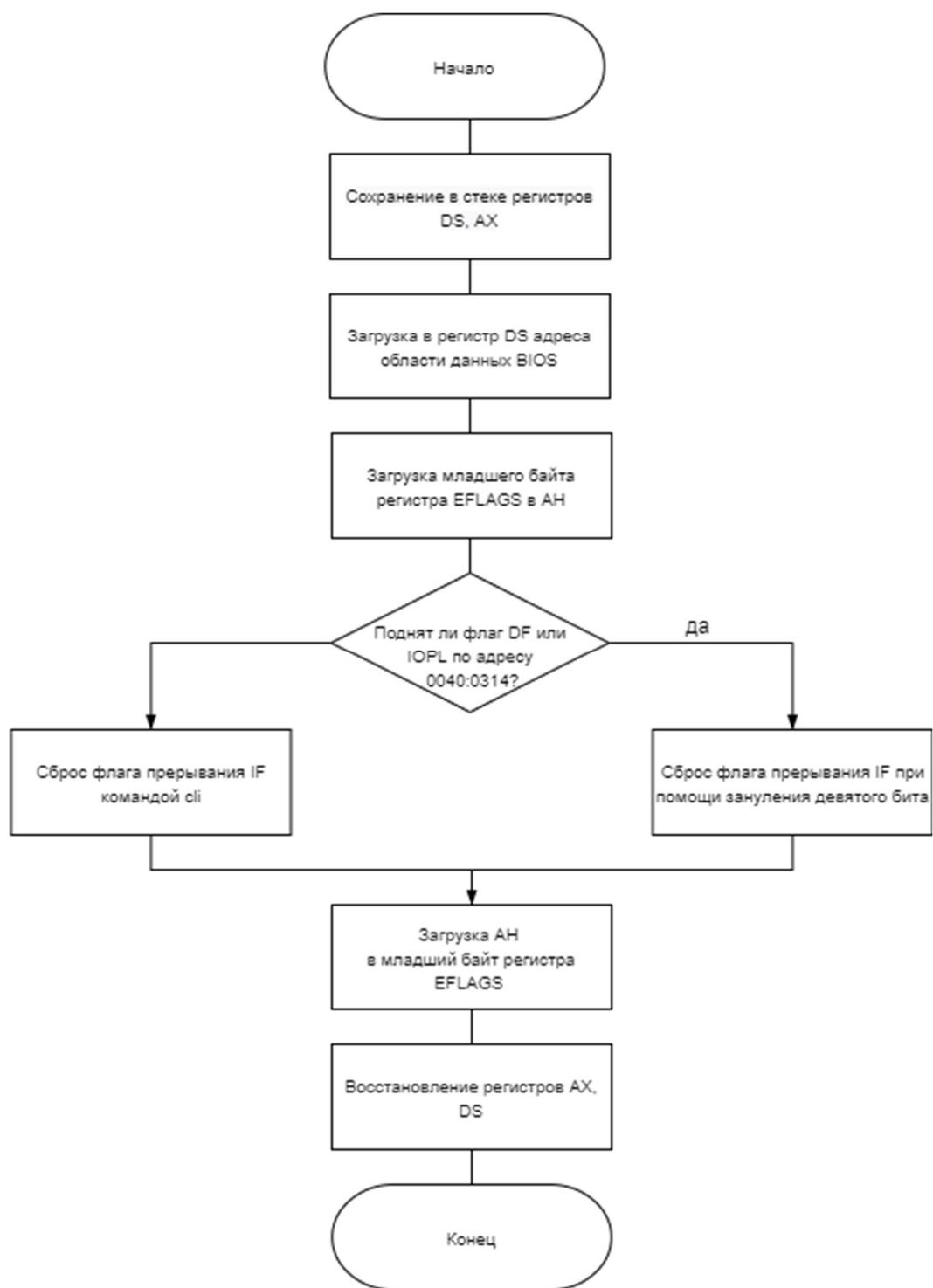


Рисунок 2 – Схема алгоритма sub\_2