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

по лабораторной работе №1

по курсу «Операционные системы»

на тему: «Дизассемблирование INT 8h»

Студент ИУ7-53Б _____ Лагутин Д. В.

(Группа) (Подпись, дата) (Фамилия И. О.)

Преподаватель _____ Рязанова Н. Ю.

(Подпись, дата) (Фамилия И. О.)

Москва, 2022 г.

1. Полученный дизассемблированный код

1.1. Код прерывания int 8h

```
; Вызов подпрограммы sub_2
020A:0746  E8 0070                 call    sub_2                   ; (07B9)

; Запись в стек 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

; Запись адреса сегмента данных bios в регистр ds
020A:074D  B8 0040                 mov     ax,40h
020A:0750  8E D8                   mov     ds,ax

; Запись адреса сегмента таблицы векторов прерываний в регистр es
020A:0752  33 C0                   xor     ax,ax                   ; Zero register
020A:0754  8E C0                   mov     es,ax

; Инкремент счетчика реального времени (внутри часа)
020A:0756  FF 06 006C              inc     word ptr ds:[6Ch]       ; (0040:006C=107Eh)
; Инкремент счетчика реального времени (часы)
020A:075A  75 04                   jnz     loc_16                  ; Jump if not zero
020A:075C  FF 06 006E              inc     word ptr ds:[6Eh]       ; (0040:006E=0Fh)

; Проверка переполнения счетчика реального времени
020A:0760                  loc_16:
020A:0760  83 3E 006E 18           cmp     word ptr ds:[6Eh],18h   ; (0040:006E=0Fh)
020A:0765  75 15                   jne     loc_17                  ; Jump if not equal
020A:0767  81 3E 006C 00B0         cmp     word ptr ds:[6Ch],0B0h  ; (0040:006C=107Eh)
020A:076D  75 0D                   jne     loc_17                  ; Jump if not equal

; Сброс счетчика реального времени после переполнения
020A:076F  A3 006E                 mov     word ptr ds:[6Eh],ax    ; (0040:006E=0Fh)
020A:0772  A3 006C                 mov     word ptr ds:[6Ch],ax    ; (0040:006C=107Eh)

; Установка флага переполнения счетчика реального времени
020A:0775  C6 06 0070 01           mov     byte ptr ds:[70h],1     ; (0040:0070=0)
; Установка 3 бита в регистре ax
020A:077A  0C 08                   or      al,8
020A:077C                  loc_17:
020A:077C  50                      push    ax

; Декремент счетчика выключения мотора дисковода
020A:077D  FE 0E 0040              dec     byte ptr ds:[40h]       ; (0040:0040=0C3h)
020A:0781  75 0B                   jnz     loc_18                  ; Jump if not zero

; Сброс 4 младших бит в байте по адресу 43Fh
```

```
020A:0783  80 26 003F F0           and     byte ptr ds:[3Fh],0F0h  ; (0040:003F=0)

; Запись 0Ch в порт 3F2h контроллера дисковода
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

; Проверка: установлен ли 2 бит в слове по адресу 714h
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

; Косвенный вызов int 1Ch
020A:0797  9F                      lahf                            ; Load ah from flags
020A:0798  86 E0                   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_20            ; (07A5)
020A:07A2  90                      nop
020A:07A3                  loc_19:

; Вызов прерывнания 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
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:
020A:064C  1E                      push    ds
020A:064D  50                      push    ax
; ---------------------------------------------------------------------------
020A:06AA  58                      pop     ax
020A:06AB  1F                      pop     ds

; Возврат из прерывания
020A:06AC  CF                      iret                            ; Interrupt return
```

1.2. Код процедуры sub_2

```
1  ;###########################################################################################
2  ;                                        SUBROUTINE
3  ;###########################################################################################
4
5                                  sub_2         proc  near
6  ; Запись в стек регистров ds, ax
7  020A:07B9  1E                                 push  ds
8  020A:07BA  50                                 push  ax
9
10
11 ; Запись адреса сегмента данных bios в регистр ds
12 020A:07BB  B8 0040                            mov   ax,40h
13 020A:07BE  8E D8                              mov   ds,ax
14
15 ; Загрузка флагов состояния в ah
16 020A:07C0  9F                                 lahf                    ; Load ah from flags
17
18 ; Уствновлены ли бит 10 или бит 13
19 020A:07C1  F7 06 0314 2400                    test  word ptr ds:[314h],2400h
20                                                                       ; (0040:0314=3200h)
21                                                                       ; 0010 0100 0000 0000
22 020A:07C7  75 0C                              jnz   loc_22            ; Jump if not zero
23
24 ; Сброс 9 бита в слове по адресу 714h
25 020A:07C9  F0> 81 26 0314 FDFF          lock and   word ptr ds:[314h],0FDFFh
26                                                                       ; (0040:0314=3200h)
27                                                                       ; 1111 1101 1111 1111
28
29 ; Загрузка флагов состояния из регистра ah
30 020A:07D0                       loc_21:
31 020A:07D0  9E                                 sahf                    ; Store ah into flags
32
33 ; Извлечение из стека регистров ax, ds
34 020A:07D1  58                                 pop   ax
35 020A:07D2  1F                                 pop   ds
36 020A:07D3  EB 03                              jmp   short loc_23
37                                                                       ; (07D8)
38
39 ; Сброс флага IF
40 020A:07D5                       loc_22:
41 020A:07D5  FA                                 cli                     ; Disable interrupts
42 020A:07D6  EB F8                              jmp   short loc_21
43                                                                       ; (07D0)
44 020A:07D8                       loc_23:
45 020A:07D8  C3                                 retn
46                                  sub_2        endp
```

2. Схемы алгоритмов

2.1. Схема алгоритма обработчика прерывания int 8h

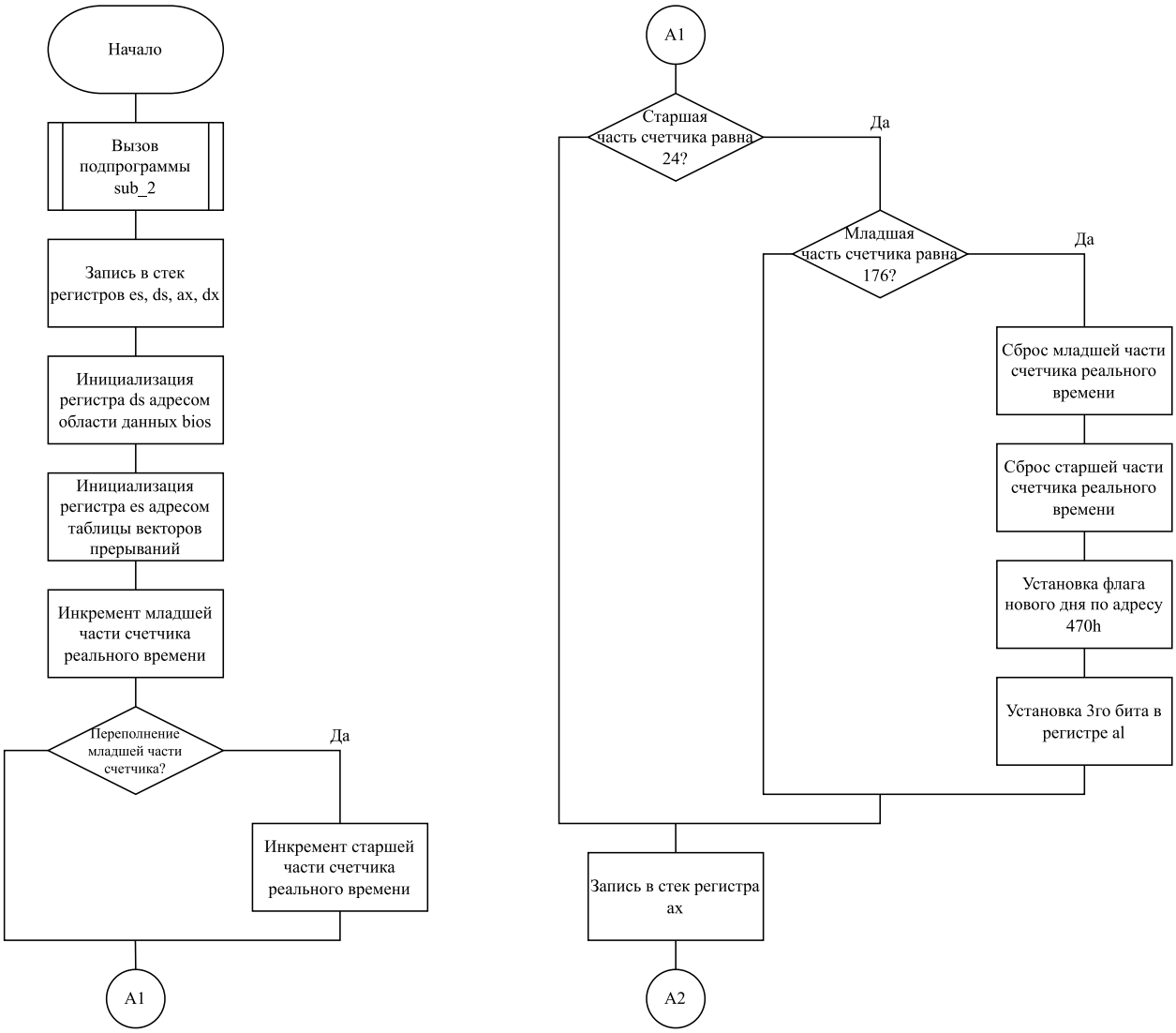

Рисунок 2.1 – Схема обработчика прерывания int 8h(1)

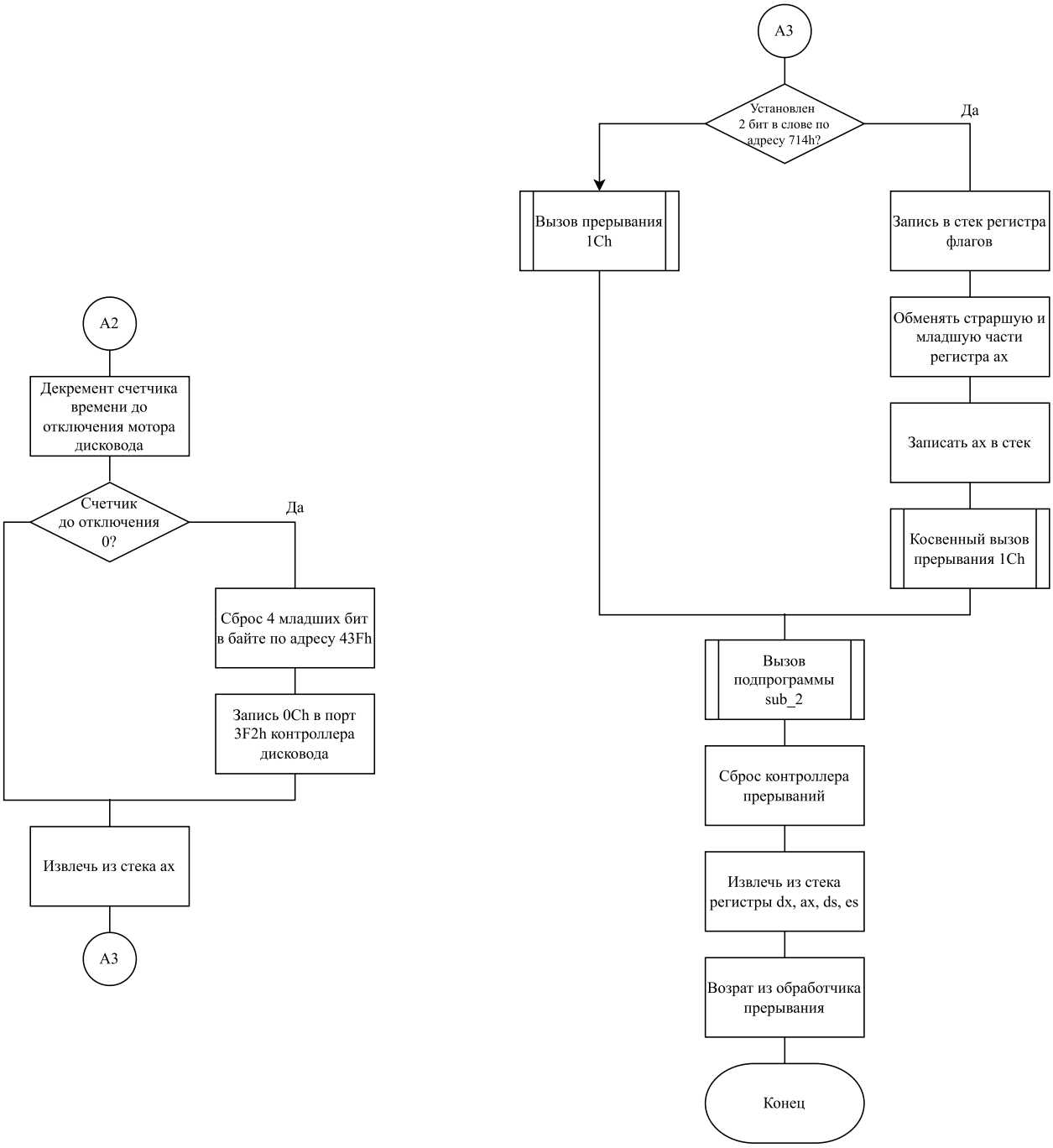

Рисунок 2.2 – Схема обработчика прерывания int 8h(2)

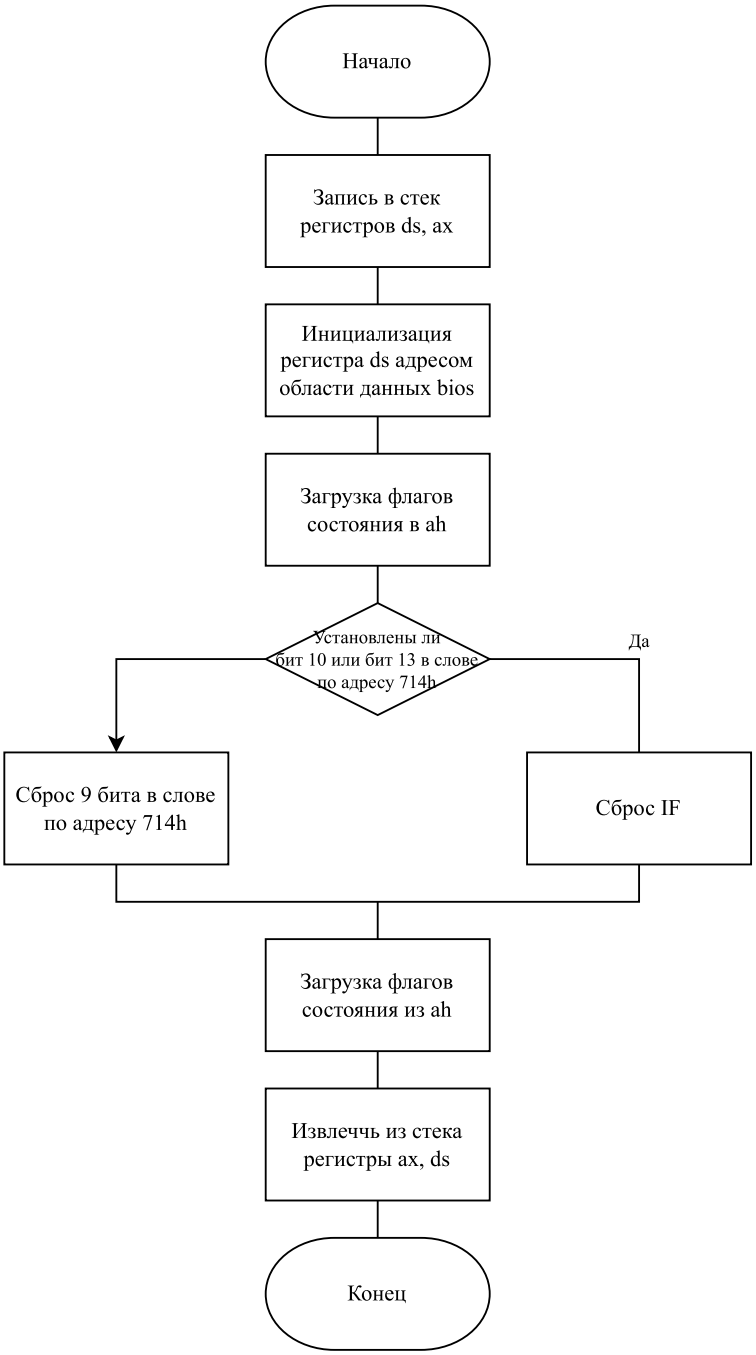

Рисунок 2.3 – Схема попрограммы sub_2