



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»

## Лабораторная работа №1 по дисциплине "Операционные системы"

Тема Дизассемблирование INT 8h

Студент Тузов Даниил Александрович

Группа ИУ7-52Б

Преподаватель Рязанова Наталья Юрьевна

Москва, 2024 г.

# 1 Дизассемблированные коды

## 1.1 Дизассемблированный код обработчика прерывания int8h

```
1      Temp.lst                      Sourcer v5.10    18-Sep-24  12:41 am    Page 1
2
3      ; Вызов сабрутины
4      020C:0746  E8 0070              call     sub_1                ; (07B9)
5      020C:0746  E8 70 00              db      0E8h, 70h, 00h
6      ; Сохранение регистров
7      020C:0749  06                    push     es
8      020C:074A  1E                    push     ds
9      020C:074B  50                    push     ax
10     020C:074C  52                    push     dx
11     ; Записать в DS - 40h
12     020C:074D  B8 0040              mov     ax,40h
13     020C:0750  8E D8              mov     ds,ax
14     ; Записать в ES - 00h
15     020C:0752  33 C0              xor     ax,ax                ; Zero register
16     020C:0754  8E C0              mov     es,ax
17     ; Инкремент младшего слова счетчика тиков
18     020C:0756  FF 06 006C          inc     word ptr ds:[6Ch]    ; (0040:006C=0B1F0h)
19     020C:075A  75 04              jnz     loc_1                ; Jump if not zero
20     ; Инкремент старшего слова тиков, если обнулилось младшее
21     020C:075C  FF 06 006E          inc     word ptr ds:[6Eh]    ; (0040:006E=0)
22     020C:0760              loc_1:
23     ; Если старшее слово равно 24 и младшее равно 176, значит прошел день и надо сбросить счетчики
24     020C:0760  83 3E 006E 18      cmp     word ptr ds:[6Eh],18h ; (0040:006E=0)
25     020C:0765  75 15              jne     loc_2                ; Jump if not equal
26     020C:0767  81 3E 006C 00B0    cmp     word ptr ds:[6Ch],0B0h ; (0040:006C=0B1F0h)
27     020C:076D  75 0D              jne     loc_2                ; Jump if not equal
28     ; Сброс младшего слова
29     020C:076F  A3 006E              mov     word ptr ds:[6Eh],ax ; (0040:006E=0)
30     ; Сброс старшего слова
31     020C:0772  A3 006C              mov     word ptr ds:[6Ch],ax ; (0040:006C=0B1F0h)
32     ; Занесение значения 1 в ds:[70h]
33     020C:0775  C6 06 0070 01      mov     byte ptr ds:[70h],1 ; (0040:0070=0)
34     ; Установка 3-его бита в al
35     020C:077A  0C 08              or      al,8
36     020C:077C              loc_2:
37     020C:077C  50                    push     ax
38     ;Декремент счетчика времени до отключения моторчика дисковода
39     020C:077D  FE 0E 0040          dec     byte ptr ds:[40h]    ; (0040:0040=94h)
40     020C:0781  75 0B              jnz     loc_3                ; Jump if not zero
41     ; Если счетчик обнулится, сбрасывается флаг работы моторчика
42     020C:0783  80 26 003F F0      and     byte ptr ds:[3Fh],0F0h ; (0040:003F=0)
43     ;Отправка команды 0Ch отключения моторчика дисковода на порт 3F2h
44     020C:0788  B0 0C              mov     al,0Ch
45     020C:078A  BA 03F2            mov     dx,3F2h
46     020C:078D  EE                    out     dx,al                ; port 3F2h, dsk0 contrl output
47     020C:078E              loc_3:
48     020C:078E  58                    pop      ax
49     ; Проверка флага четности
50     020C:078F  F7 06 0314 0004    test     word ptr ds:[314h],4 ; (0040:0314=3200h)
51     020C:0795  75 0C              jnz     loc_4                ; Jump if not zero
52     ; Загрузка младшего байта регистра флагов в ah
53     020C:0797  9F                    lahf                     ; Load ah from flags
54     020C:0798  86 E0              xchg     ah,al
55     020C:079A  50                    push     ax
56     ; Косвенный вызов прерывания 1Ch
57     020C:079B  26: FF 1E 0070      call     dword ptr es:[70h]  ; (0000:0070=6ADh)
58     020C:07A0  EB 03              jmp     short loc_5          ; (07A5)
59     020C:07A2  90                    nop
60     020C:07A3              loc_4:
61     ; Вызов прерывания 1Ch
62     020C:07A3  CD 1C              int     1Ch                ; Timer break (call each 18.2ms)
63     020C:07A5              loc_5:
64     ; Вызов сабрутины
65     020C:07A5  E8 0011              call     sub_1                ; (07B9)
66     ; Сброс контроллера прерываний (разрешаются прерывания с более низким приоритетом)
```

```

67 020C:07A8 B0 20      mov al,20h      ; ' '
68 020C:07AA E6 20      out 20h,al      ; port 20h, 8259-1 int command
69                               ; al = 20h, end of interrupt
70 ; Восстановление регистров
71 020C:07AC 5A          pop dx
72 020C:07AD 58          pop ax
73 020C:07AE 1F          pop ds
74 020C:07AF 07          pop es
75 020C:07B0 E9 FE99     jmp $-164h
76 ; ...
77 020C:06AC CF          itret      ; Возврат из прерывания

```

## 1.2 Дизассемблированный код subrouting

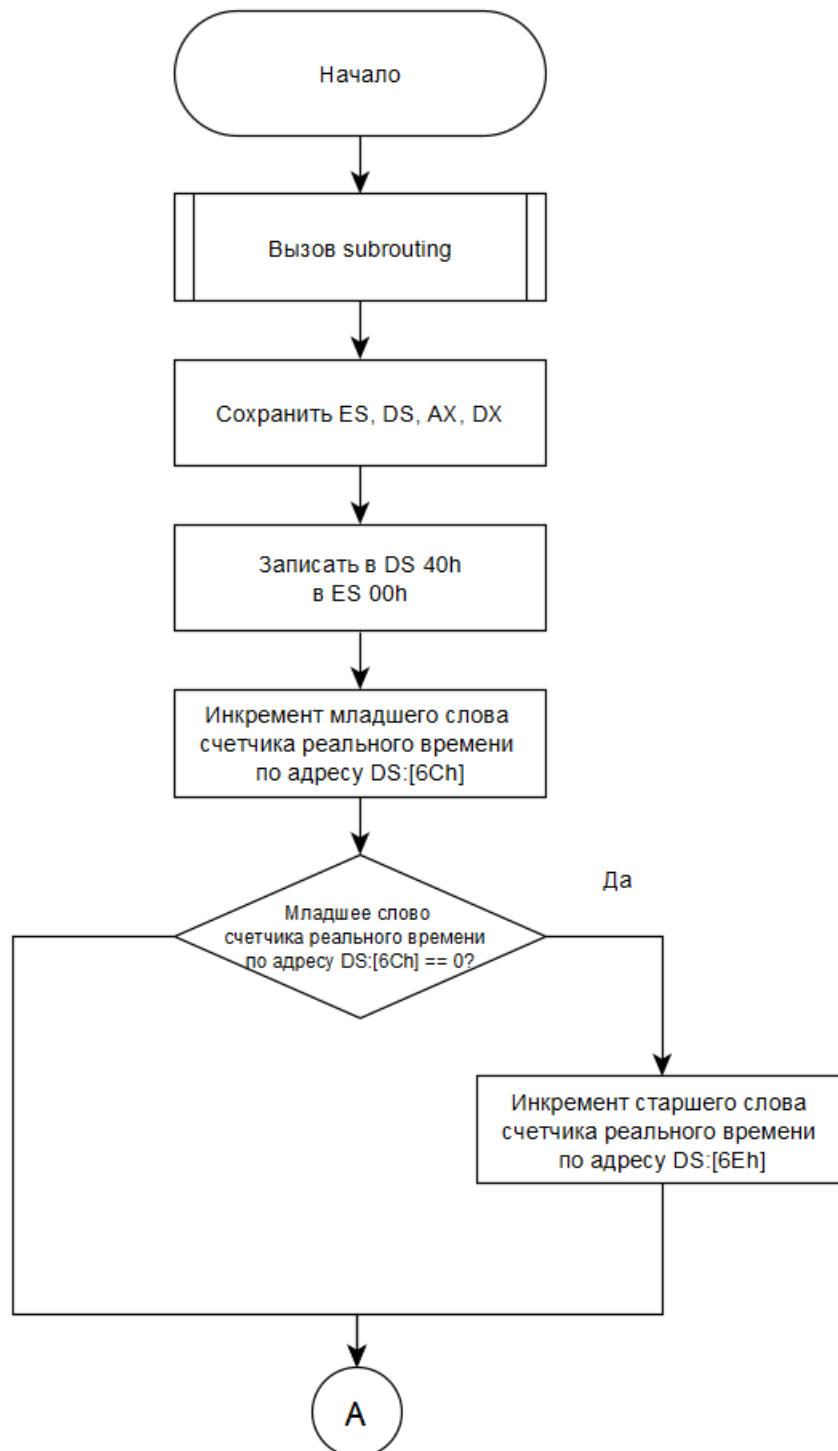
```

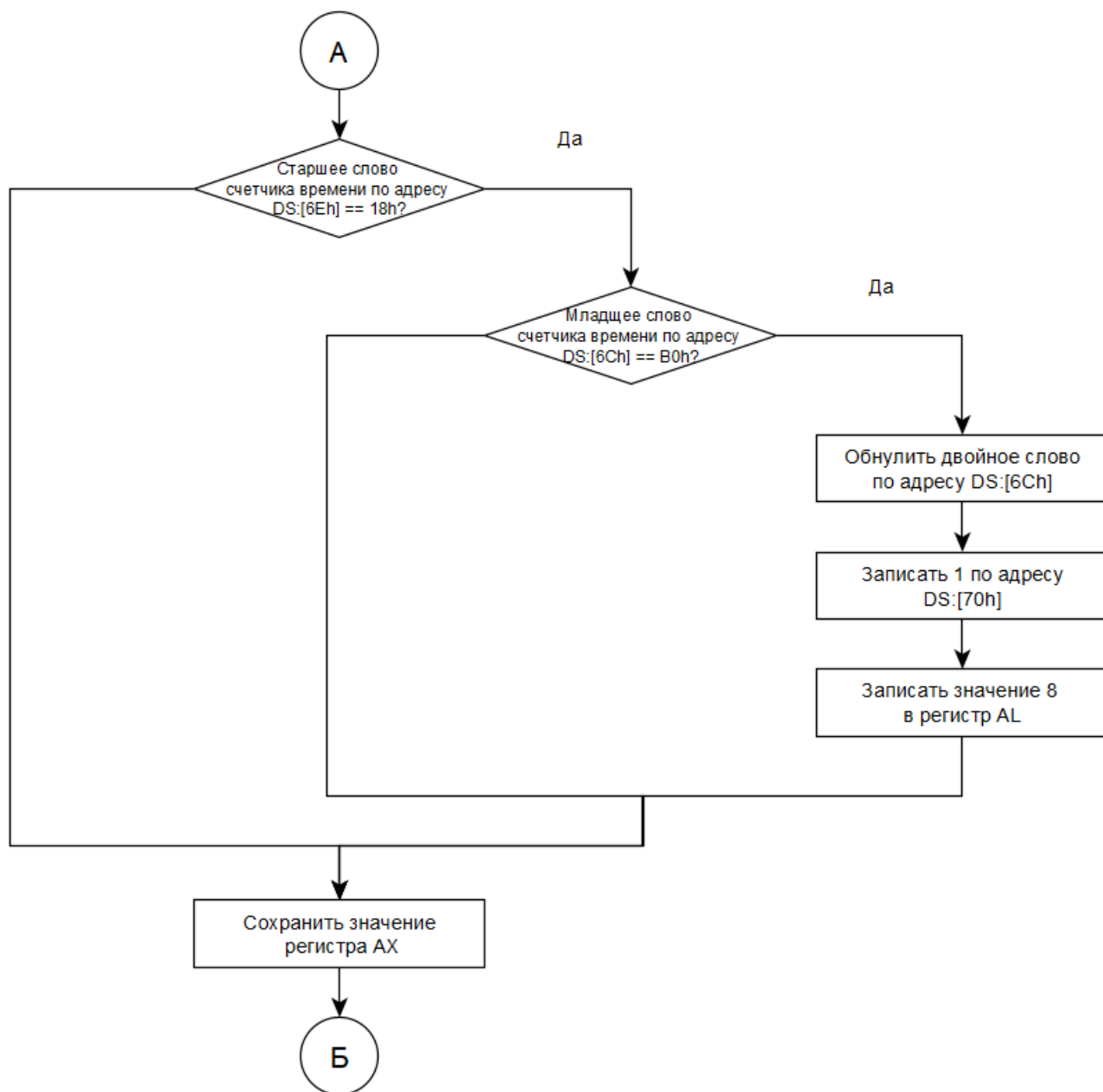
1      sub_1      proc      near
2      ; Сохранение значений регистров
3      020C:07B9 1E          push     ds
4      020C:07BA 50          push     ax
5      ; Записать в DS - 40h
6      020C:07BB B8 0040     mov ax,40h
7      020C:07BE 8E D8       mov ds,ax
8      ; Загрузка младшего байта регистра флагов в ah
9      020C:07C0 9F          lahf             ; Load ah from flags
10     ; Проверка флага DF и старшего бита флага IOPL
11     020C:07C1 F7 06 0314 2400 test word ptr ds:[314h],2400h ; (0040:0314=3200h)
12     020C:07C7 75 0C       jnz loc_7      ; Jump if not zero
13     ; Сброс флага прерываний IF
14     020C:07C9 F0> 81 26 0314 FDFF lock and word ptr ds:[314h],0FDFFh ;
      (0040:0314=3200h)
15     020C:07D0             loc_6:
16     ; Загрузка из ah младшего байта регистра флагов
17     020C:07D0 9E          sahf             ; Store ah into flags
18     ; Восстановление регистров
19     020C:07D1 58          pop ax
20     020C:07D2 1F          pop ds
21     020C:07D3 EB 03       jmp short loc_8      ; (07D8)
22     020C:07D5             loc_7:
23     ; Сброс флага прерываний IF
24     020C:07D5 FA          cli             ; Disable interrupts
25     020C:07D6 EB F8       jmp short loc_6      ; (07D0)
26     020C:07D8             loc_8:
27     020C:07D8 C3          retn
28     sub_1      endp

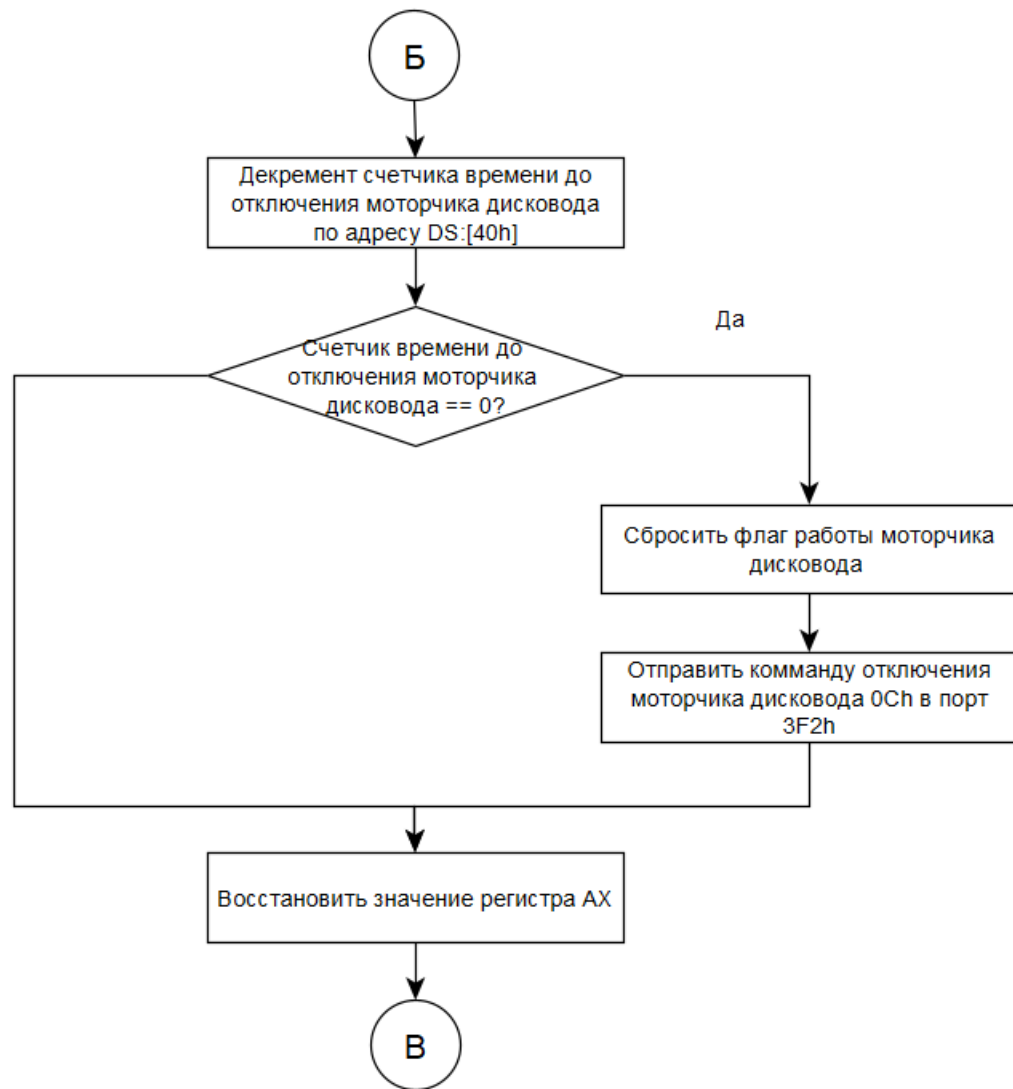
```

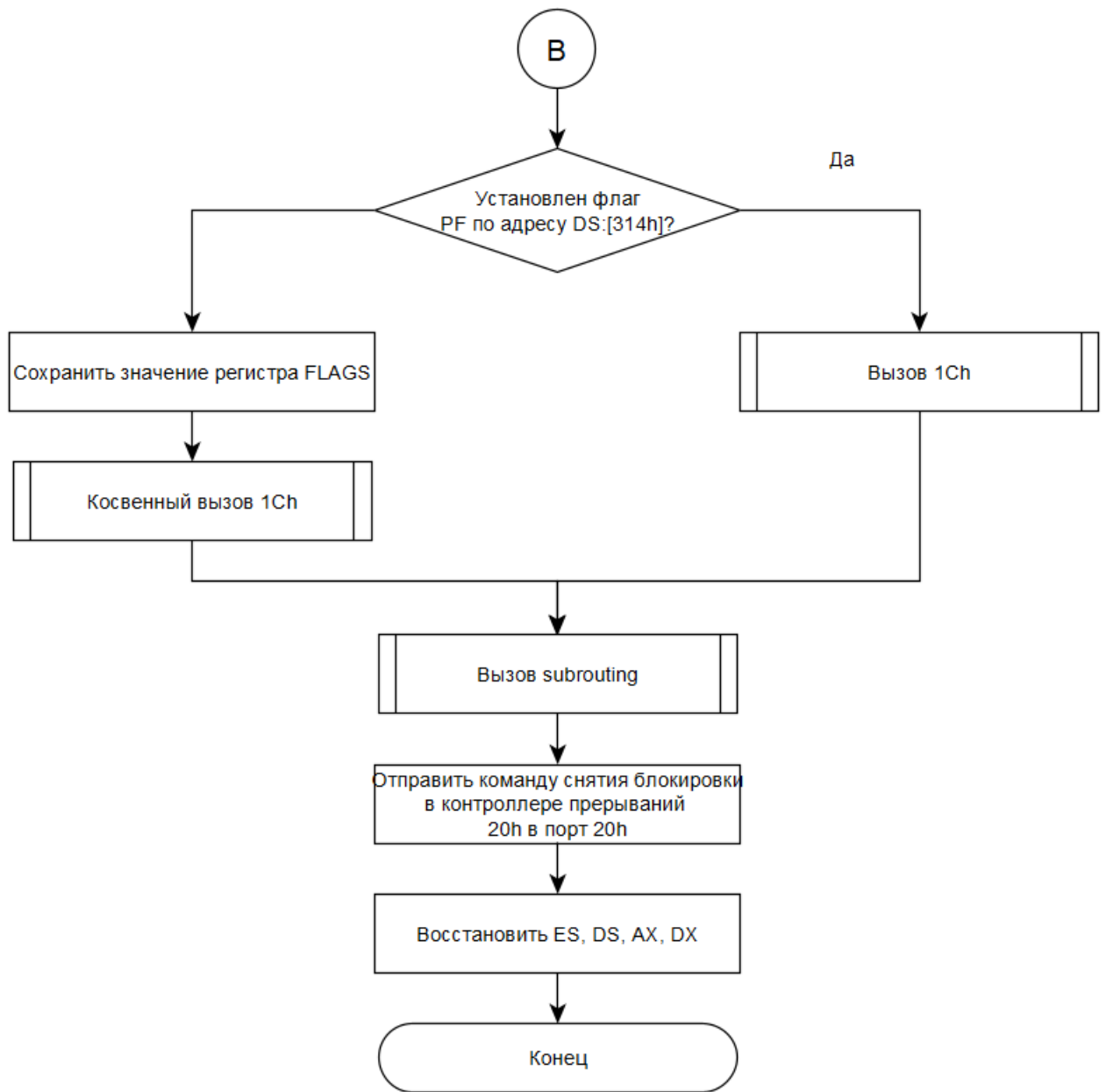
## 2 Схемы алгоритмов

### 2.1 Схема алгоритма обработчика прерывания int8h









## 2.2 Схема алгоритма subrouting

