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"

Тема Дизассемблирование прерывания int8h

Студент Городский Ю.Н.

Группа ИУ7-52Б

Оценка (баллы)

Преподаватель Рязанова Н.Ю.

Москва — 2024 г.

Содержание

1 Листинги кода

```
; Сохранение регистров DS, AX
020A:07B9  1E                    push    ds
020A:07BA  50                    push    ax

; Установка значения сегментного регистра DS - 0040h
; 40H - адресное пространство BIOS
020A:07BB  B8 0040               mov ax,40h
020A:07BE  8E D8                 mov ds,ax

; Загрузка младшего байта регистра флагов в ah
020A:07C0  9F                    lahf                ; Load ah from flags

; Флаг DF или старший бит IOPL установлены в ds:314h?
020A:07C1  F7 06 0314 2400          test    word ptr ds:[314h],2400h    ;
    (0040:0314=3200h)


020A:07C7  75 0C                 jnz loc_7           ; Jump if not zero

; Сброс флага IF по адресу ds:314h
020A:07C9  F0> 81 26 0314 FDFF                               lock and word
    ptr ds:[314h],0FDFFh    ; (0040:0314=3200h)

020A:07D0           loc_6:

; Загрузка AH в регистр флагов
020A:07D0  9E                    sahf                ; Store ah into flags

; Восстановление значений регистров AX, DS
020A:07D1  58                    pop ax
020A:07D2  1F                    pop ds
020A:07D3  EB 03                 jmp short loc_8     ; (07D8)

020A:07D5           loc_7:

; Запрет маскируемых прерываний с помощью cli
020A:07D5  FA                    cli             ; Disable interrupts
020A:07D6  EB F8                 jmp short loc_6     ; (07D0)


020A:07D8           loc_8:
020A:07D8  C3                    retn
```

Листинг 1.1 – sub_1

```
; Вызов sub_1
020A:0746  E8 0070              call    sub_1           ; (07B9)

; Сохранение регистров es,ds,ax,dx
020A:0746  E8 70 00             db  0E8h, 70h, 00h
020A:0749  06                   push    es
020A:074A  1E                   push    ds
020A:074B  50                   push    ax
020A:074C  52                   push    dx

; Установка значений сегментных регистров DS, ES
020A:074D  B8 0040              mov ax,40h
020A:0750  8E D8                mov ds,ax
020A:0752  33 C0                xor ax,ax           ; Zero register
020A:0754  8E C0                mov es,ax

; Инкремент младшего слова счетчика тиков по адресу ds:6Ch
020A:0756  FF 06 006C               inc word ptr ds:[6Ch]   ;
    (0040:006C=8F66h)

; Младшее слово счетчика тиков = 0?
020A:075A  75 04                jnz loc_1           ; Jump if not zero

; Инкремент старшего слова счетчика тиков по адресу ds:6Eh
020A:075C  FF 06 006E               inc word ptr ds:[6Eh]   ; (0040:006E=3)

; Старшее слово счетчика тиков = 24?
020A:0760           loc_1:
020A:0760  83 3E 006E 18            cmp word ptr ds:[6Eh],18h   ;
    (0040:006E=3)
020A:0765  75 15                jne loc_2           ; Jump if not equal

; Младшее слово счетчика тиков = 0B0h?
020A:0767  81 3E 006C 00B0          cmp word ptr ds:[6Ch],0B0h  ;
    (0040:006C=8F66h)
020A:076D  75 0D                jne loc_2           ; Jump if not equal

; Сброс счетчика тиков
020A:076F  A3 006E              mov word ptr ds:[6Eh],ax    ; (0040:006E=3)
020A:0772  A3 006C              mov word ptr ds:[6Ch],ax    ;
    (0040:006C=8F66h)

; Установка 1 по адресу ds:70h
020A:0775  C6 06 0070 01            mov byte ptr ds:[70h],1 ; (0040:0070=0)

; Установка 3 бита регистра AL
020A:077A  0C 08                or  al,8

```

```
020A:077C           loc_2:

; Сохранение регистра AX
020A:077C  50                   push    ax

; Декремент счетчика времени отключения моторчика дисковода по адресу ds:40h
020A:077D  FE 0E 0040               dec byte ptr ds:[40h]   ;
    (0040:0040=19h)

; Счетчик времени отключения моторчика дисковода = 0?
020A:0781  75 0B                jnz loc_3           ; Jump if not zero

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

; Отправка в порт 3F2h команды отключения моторчика 0Ch
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_3:

; Восстановление регистра AX
020A:078E  58                   pop ax

; Флаг PF установлен в ds:[314h]?
020A:078F  F7 06 0314 0004          test    word ptr ds:[314h],4    ;
    (0040:0314=3200h)
020A:0795  75 0C                jnz loc_4           ; Jump if not zero

; Загрузка младшего байта регистра флагов в AH
020A:0797  9F                   lahf                ; Load ah from flags
020A:0798  86 E0                xchg    ah,al
020A:079A  50                   push    ax

; Косвенный вызов прерывания 1Ch
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

; Вызов прерывания 1Ch
020A:07A3           loc_4:
020A:07A3  CD 1C                int 1Ch         ; Timer break (call each
    18.2ms)

```

```
87  020A:07A5           loc_5:
88
89  ; Вызов sub_1
90  020A:07A5  E8 0011              call    sub_1           ; (07B9)
91
92  ; Сброс контроллера прерываний
93  020A:07A8  B0 20                mov al,20h          ; ' '
94  020A:07AA  E6 20                out 20h,al          ; port 20h, 8259-1 int
        command
95                                          ;  al = 20h, end of interrupt
96
97  ; Восстановление значения регистров dx, ax, ds, es
98  020A:07AC  5A                   pop dx
99  020A:07AD  58                   pop ax
100 020A:07AE  1F                   pop ds
101 020A:07AF  07                   pop es
102
103 ; Переход по адресу 020A:064Ch
104 020A:07B0  E9 FE99              jmp $-164h
```

Листинг 1.2 – Прерывание int 8h

2 Схемы алгоритмов

2.1 Схема sub_1

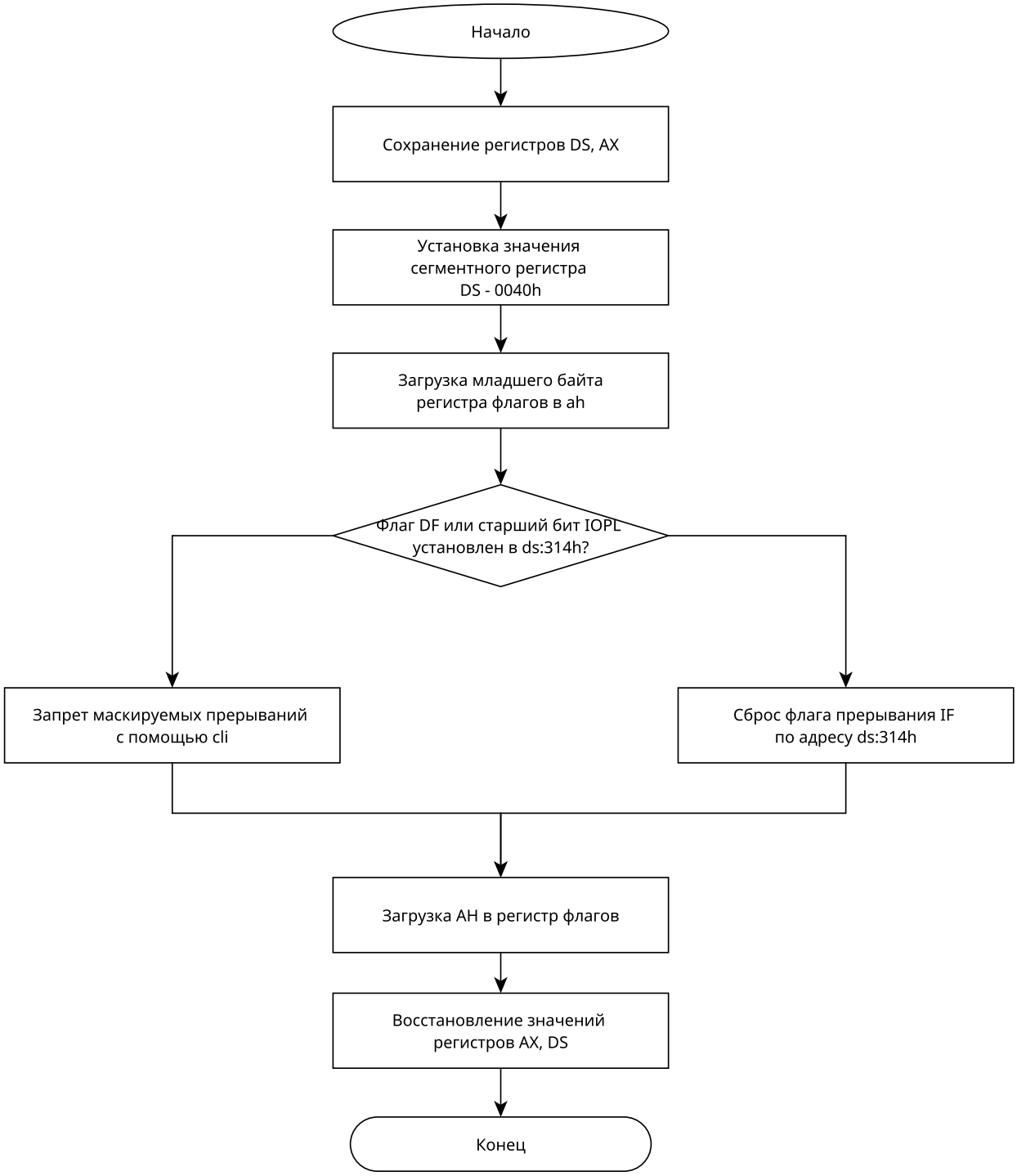

Рисунок 2.1 – Схема sub_1

2.2 Схема int8h

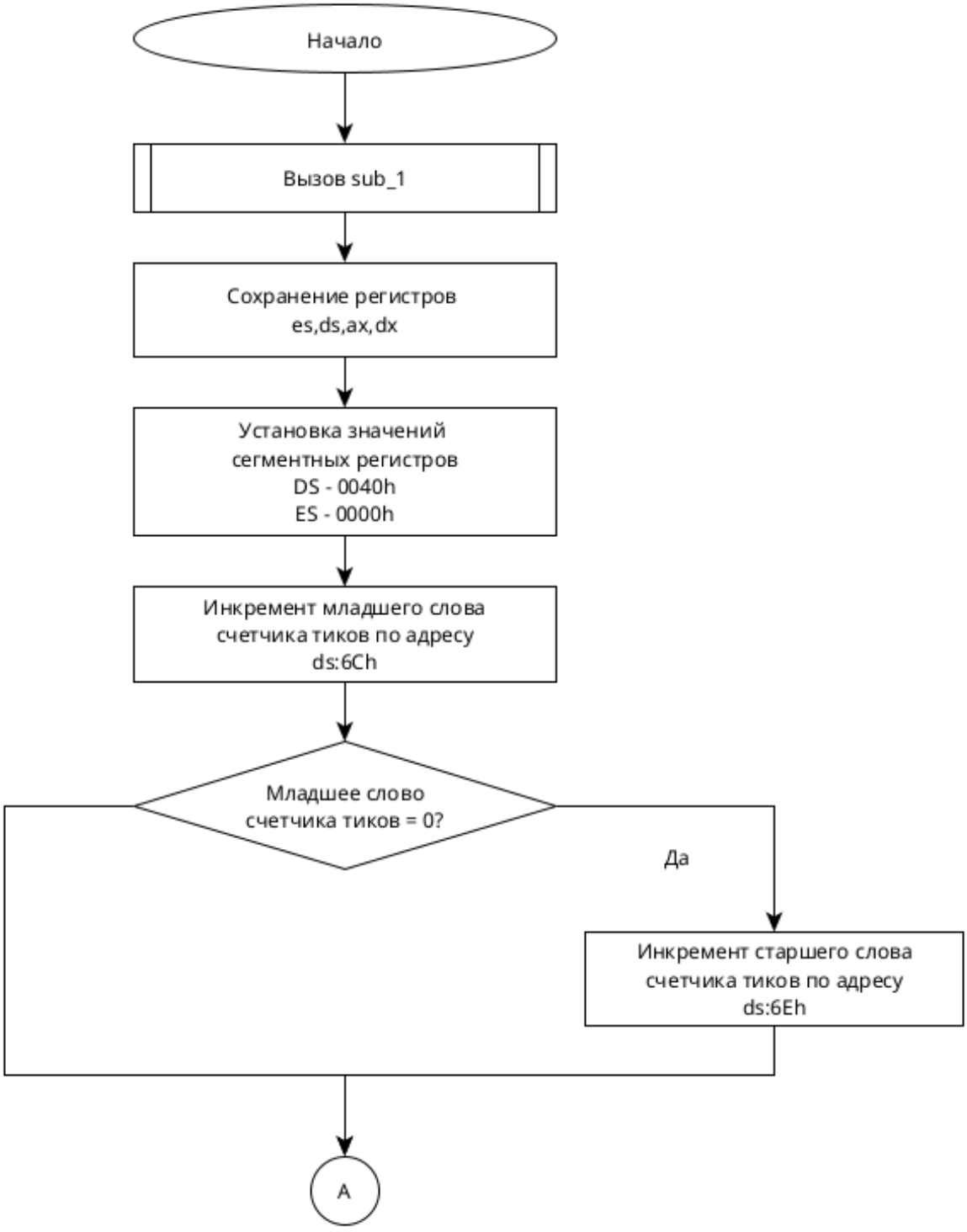

Рисунок 2.2 – Схема int8h - 1

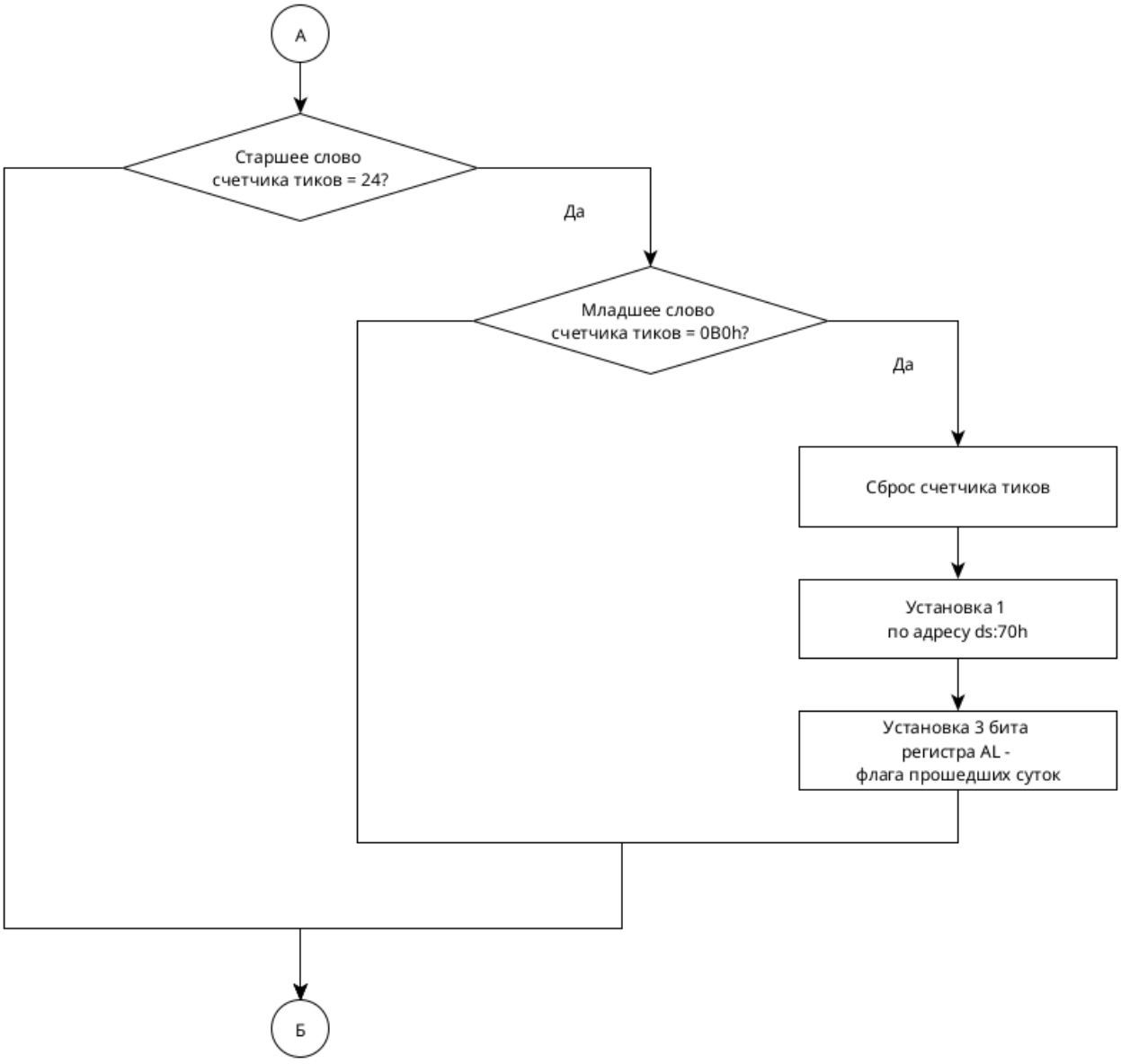

Рисунок 2.3 – Схема int8h - 2

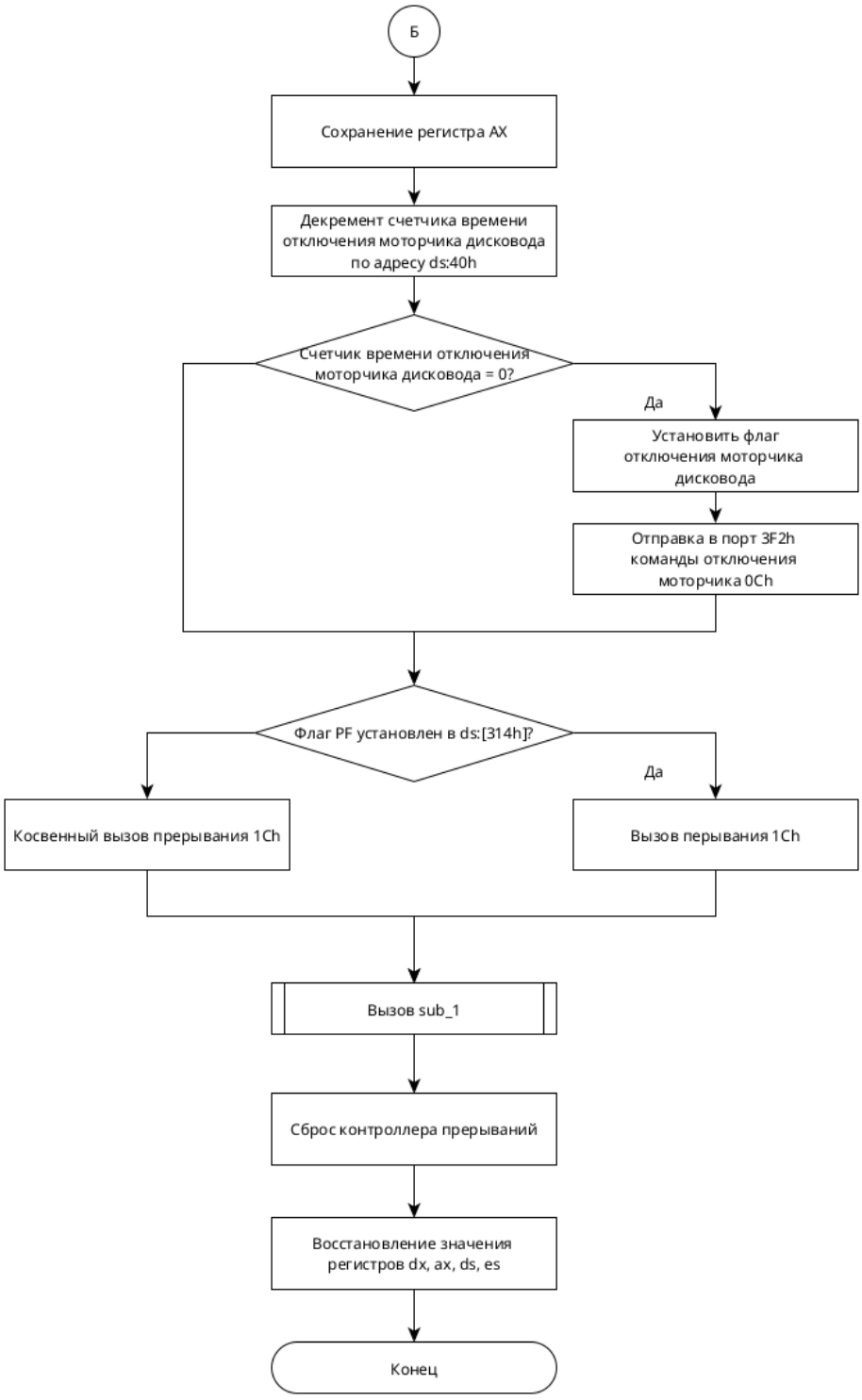

Рисунок 2.4 – Схема int8h - 3