



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 (часть 1) по курсу "Операционные системы"

Тема Исследование прерывания INT 8h

Студент Щербина М. А.

Группа ИУ7-52Б

Преподаватель Рязанова Н.Ю.

Москва — 2022 г.

Листинг кода

Далее будут представлены листинги прерывания int 8h и процедуры sub_2

Листинг INT8h

```
1 ;; Вызов процедуры sub_2 (запрет прерываний)
2 020A:0746 E8 0070      call    sub_2          ; (07B9)
3
4 ;; Сохранение содержимого регистров ES, DS, AX, DX
5 020A:0749 06          push    es
6 020A:074A 1E          push    ds
7 020A:074B 50          push    ax
8 020A:074C 52          push    dx
9
10 ;; В регистр DS загружается адрес 0040:0000
11 ; начало области данных BIOS (через буфер AX)
12 020A:074D B8 0040      mov     ax,40h
13 020A:0750 8E D8      mov     ds,ax
14
15 ;; В регистр ES загружается адрес 0000:0000
16 ; адрес начала таблицы векторов прерывания (через буфер AX)
17 020A:0752 33 C0      xor     ax,ax          ; Zero register
18 020A:0754 8E C0      mov     es,ax
19
20 ;; Инкремент счетчика таймера
21 ;; Инкремент младшей части счётчика таймера
22 020A:0756 FF 06 006C    inc     word ptr ds:[6Ch] ; (0040:006C=0A808h)
23
24 ;; Если младшая часть счетчика CB == 0,
25 ; то инкремент двух старших байтов CB
26 ; иначе переходим на loc_16
27 020A:075A 75 04      jnz     loc_16      ; Jump if not zero
28
29 ;; Инкремент старшей части счётчика CB
30 020A:075C FF 06 006E    inc     word ptr ds:[6Eh] ; (0040:006E=8)
31
32 ;; Сброс счётчика CB и выставление флага окончания суток
33
34 ;; Если два старших байта счетчика CB == 24
35 ; то сравниваем два младших байта счетчика CB
```

```

36 ; иначе декемент счетчика СВ до отключения моторчика дисковод
37 020A:0760          loc_16:
38 020A:0760  83 3E 006E 18      cmp word ptr ds:[6Eh],18h
39 020A:0765  75 15              jne loc_17          ; Jump if not equal
40
41 ;; Если два младших байта счетчика СВ == 176
42 ; то обнуление счетчика СВ и установка флага прошедших суток
43 ; иначе декемент счетчика СВ до отключения моторчика дисковод
44 020A:0767  81 3E 006C 00B0    cmp word ptr ds:[6Ch],0B0h
45
46 ; Обнуляем счетчик ( если прошел день )
47 020A:076D  75 0D              jne loc_17      ; Jump if not equal
48 020A:076F  A3 006E            mov word ptr ds:[6Eh],ax
49 ; (0040:006E=8) обнуляем счётчик (старшая часть)
50 020A:0772  A3 006C            mov word ptr ds:[6Ch],ax
51 ; (0040:006C=0A808h) (младшая часть)
52
53 ;; В ячейку 0040:0070 записываем единицу
54 ; (Для фиксации о том , что новый день наступил )
55
56 020A:0775  C6 06 0070 01      mov byte ptr ds:[70h],1 ; (0040:0070=0)
57 020A:077A  0C 08              or  al,8
58
59 ;; Декремент счетчика до отключения моторчика дисковод
60 020A:077C          loc_17:
61 020A:077C  50                  push  ax
62 020A:077D  FE 0E 0040          dec byte ptr ds:[40h]    ; (0040:0040=8Dh)
63
64 ;; Если значени этого счетчика == 0
65 ; то установка флага отключения моторчика и посылка команды в порт на откл
    ючения моторчика
66 020A:0781  75 0B              jnz loc_18      ; Jump if not zero
67
68 020A:0783  80 26 003F F0      and byte ptr ds:[3Fh],0F0h ; (0040:003F=0)
69 020A:0788  B0 0C              mov  al,0Ch
70 020A:078A  BA 03F2            mov  dx,3F2h
71 020A:078D  EE                  out  dx,al        ; port 3F2h, dsk0 contrl
    output
72
73 ;; Проверка, установлен ли PF(parity flag), т.е. разрешен ли ответ на маск
    ируемые прерывания
74 020A:078E          loc_18:
75 020A:078E  58                  pop  ax
76
77 ;; Проверяем флаг PF по адресу 0040:0314
78 ; (0100, поднят 2 бит, отвечает за флаг PF, флаг четности)
79 020A:078F  F7 06 0314 0004    test word ptr ds:[314h],4 ;
    (0040:0314=3200h)

```

```

80 ;; если вызов маскируемых прерываний разрешен, переход к вызову int 1Ch
    (в loc_19)
81 020A:0795 75 0C          jnz loc_19    ; Jump if not zero
82
83 020A:0797 9F            lahf          ; Load ah from flags
84 020A:0798 86 E0          xchg         ah,al ; Обмен
85
86 ;; иначе, косвенный вызов 1Ch - как процедуры командой call и переход к
    loc_20
87 ; (1C * 4 = 70h )
88 020A:079B 26: FF 1E 0070 call     dword ptr es:[70h] ; (0000:0070=6ADh)
89 020A:07A0 EB 03          jmp short loc_20      ; (07A5)
90 020A:07A2 90            nop
91
92 ;; вызов пользовательского прерывания по таймеру
93 020A:07A3          loc_19:
94 020A:07A3 CD 1C          int 1Ch          ; Timer break (call each
    18.2ms)
95 ;; после инициализации системы вектор INT 1Ch указывает на команду IRET
96
97 ; сброс контроллера прерываний
98 020A:07A5          loc_20:
99 020A:07A5 E8 0011        call     sub_2          ; (07B9)
100
101 020A:07A8 B0 20          mov     al,20h          ; ' '
102 020A:07AA E6 20          out     20h,al        ; port 20h, 8259-1 int
    command
103 ; al = 20h, end of interrupt
104
105 ;; восстановление значений регистров
106 020A:07AC 5A            pop     dx
107 020A:07AD 58            pop     ax
108 020A:07AE 1F            pop     ds
109 020A:07AF 07            pop     es
110 ;; прыжок в адрес 020A:064C
111 020A:07B0 E9 FE99        jmp     loc_1          ; (064C)
112 ; ---
113 020A:064C 1E            push    ds
114 020A:064D 50            push    ax
115 ; ---
116 020A:06AA 58            pop     ax
117 020A:06AB 1F            pop     ds
118
119 020A:06AC CF            iret          ; Interrupt return

```

Листинг sub_2

```
1      sub_2      proc      near
2  ;; Сохранение содержимого регистров DS, AX
3  020A:07B9  1E      push    ds
4  020A:07BA  50      push    ax
5
6  ;; В регистр DS загружается адрес 0040:0000 начало области данных BIOS
7  020A:07BB  B8 0040      mov    ax,40h
8  020A:07BE  8E D8      mov    ds,ax
9
10 ;; Загрузка младшего байта регистра EFLAGS в A
11 020A:07C0  9F      lahf          ; Load ah from flags
12
13 ;; Если флаг DF == 0 и старший бит IOPL == 0
14 ; то сброс флага разрешения прерывания IF в 0040:0314
15 ; иначе запрет маскируемых прерываний инструкцией CLI
16 020A:07C1  F7 06 0314 2400  test    word ptr ds:[314h],2400h      ;
    (0040:0314=3200h)
17
18 020A:07C7  75 0C      jnz    loc_22      ; Jump if not zero
19
20 ;; Сброс флага IF
21 020A:07C9  F0> 81 26 0314 FDFF  lock and word ptr ds:[314h],0FDFFh      ;
    (0040:0314=3200h)
22
23 ;; Восстановление значений флагов
24 020A:07D0      loc_21:
25 020A:07D0  9E      sahf          ; Store ah into flags
26
27 ;; Восстановление значений регистров
28 020A:07D1  58      pop    ax
29 020A:07D2  1F      pop    ds
30 020A:07D3  EB 03      jmp short loc_23      ; (07D8)
31
32 ;; Сброс IF, т. е. запрет прерываний с помощью команды cli
33 020A:07D5      loc_22:
34 020A:07D5  FA      cli          ; Disable interrupts
35 020A:07D6  EB F8      jmp short loc_21      ; (07D0)
36
37 ;; Выход из программы
38 020A:07D8      loc_23:
39 020A:07D8  C3      retn
40 sub_2      endp
```

Схема алгоритма

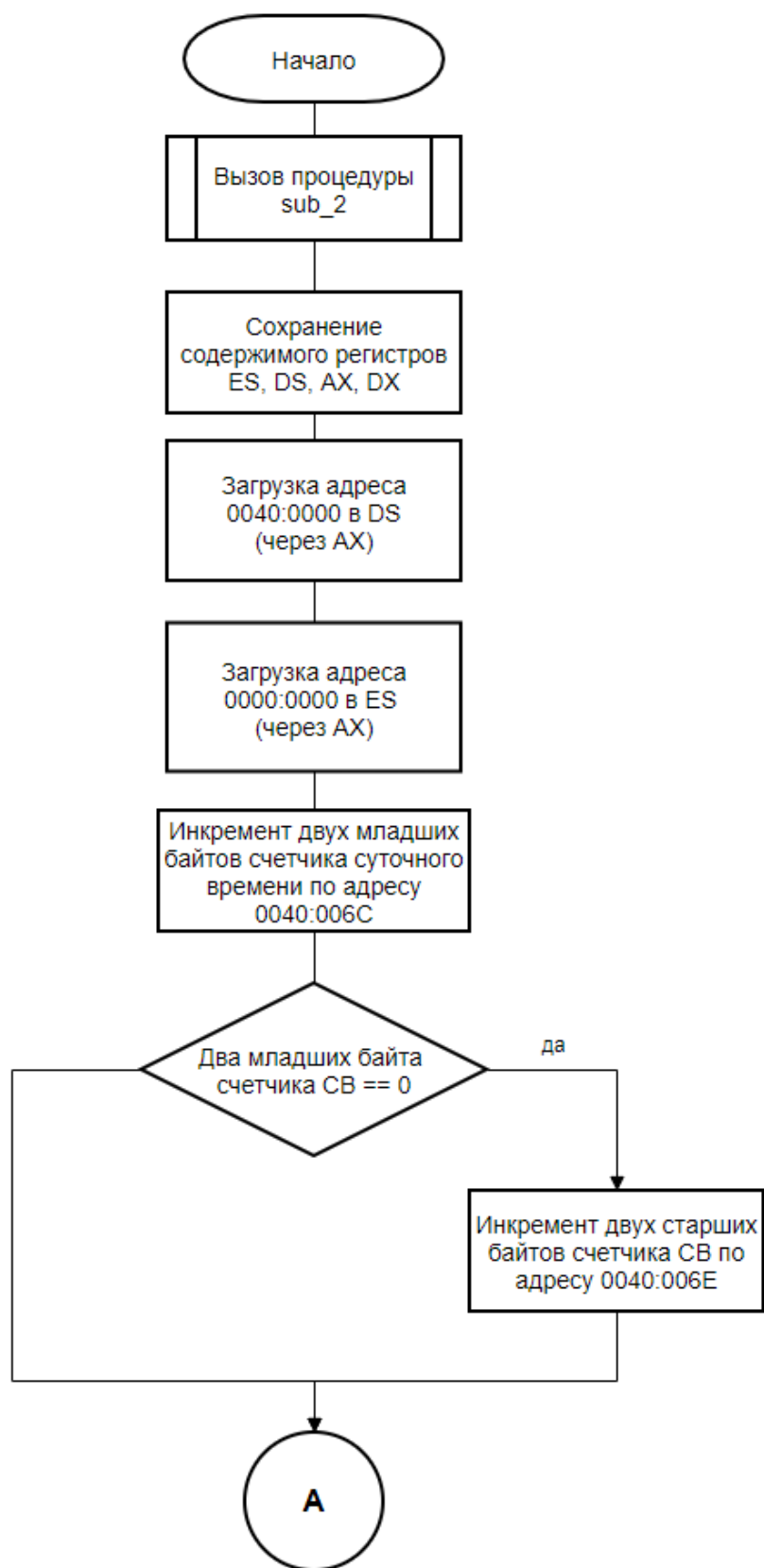


Рисунок 1 – Схема обработчика прерываний INT 8h

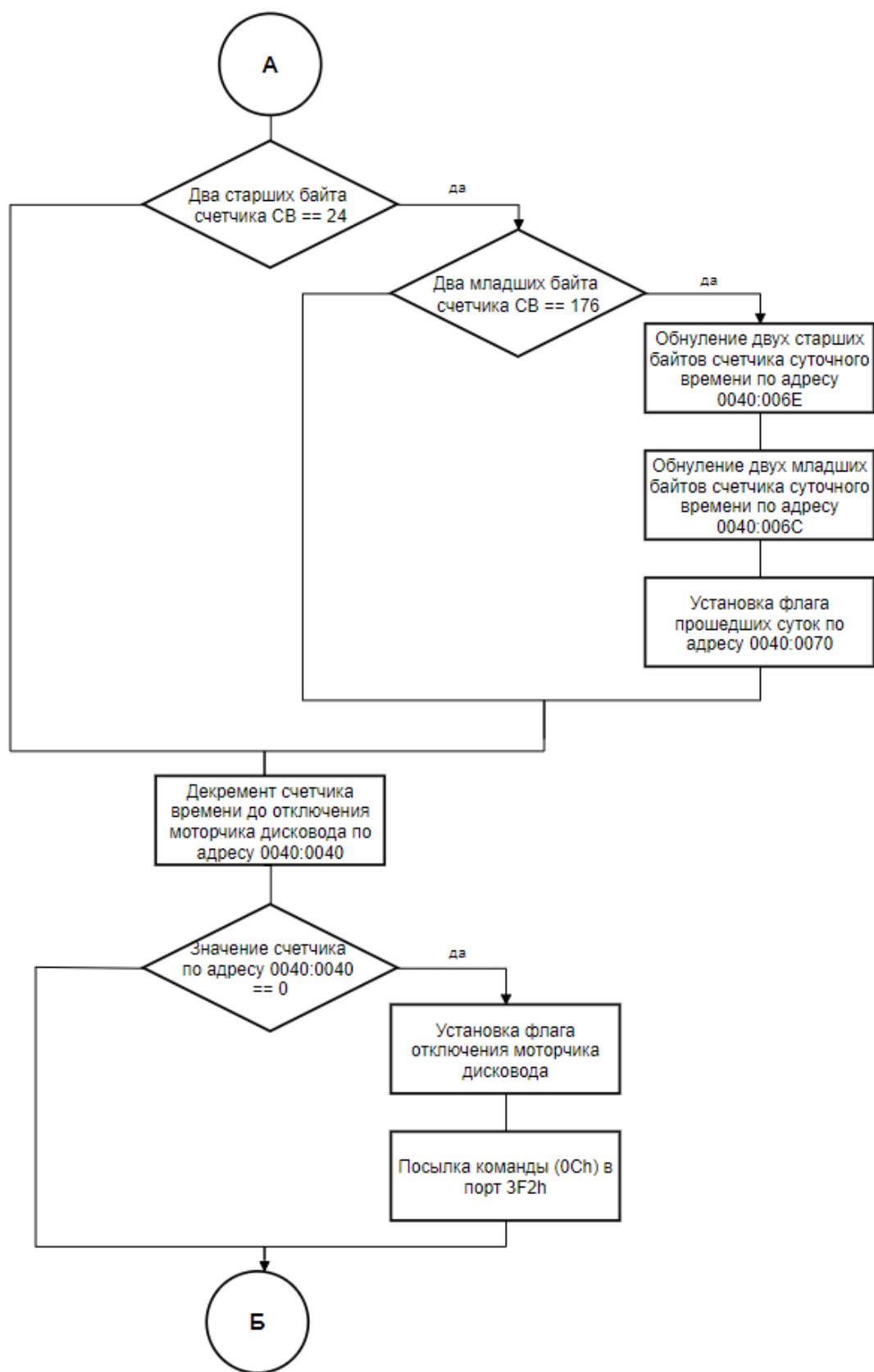


Рисунок 2 – Схема обработчика прерываний INT 8h

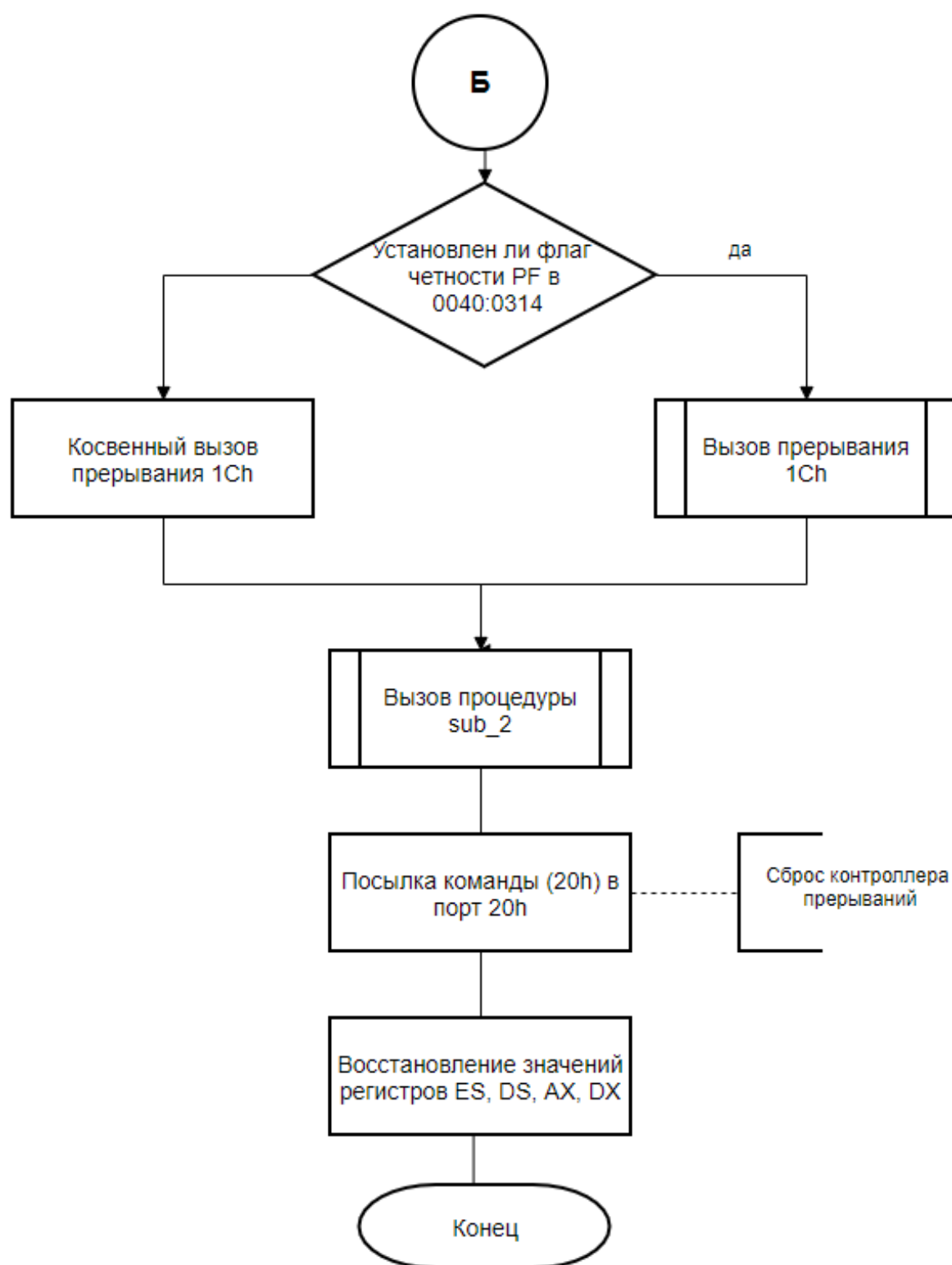


Рисунок 3 – Схема обработчика прерываний INT 8h

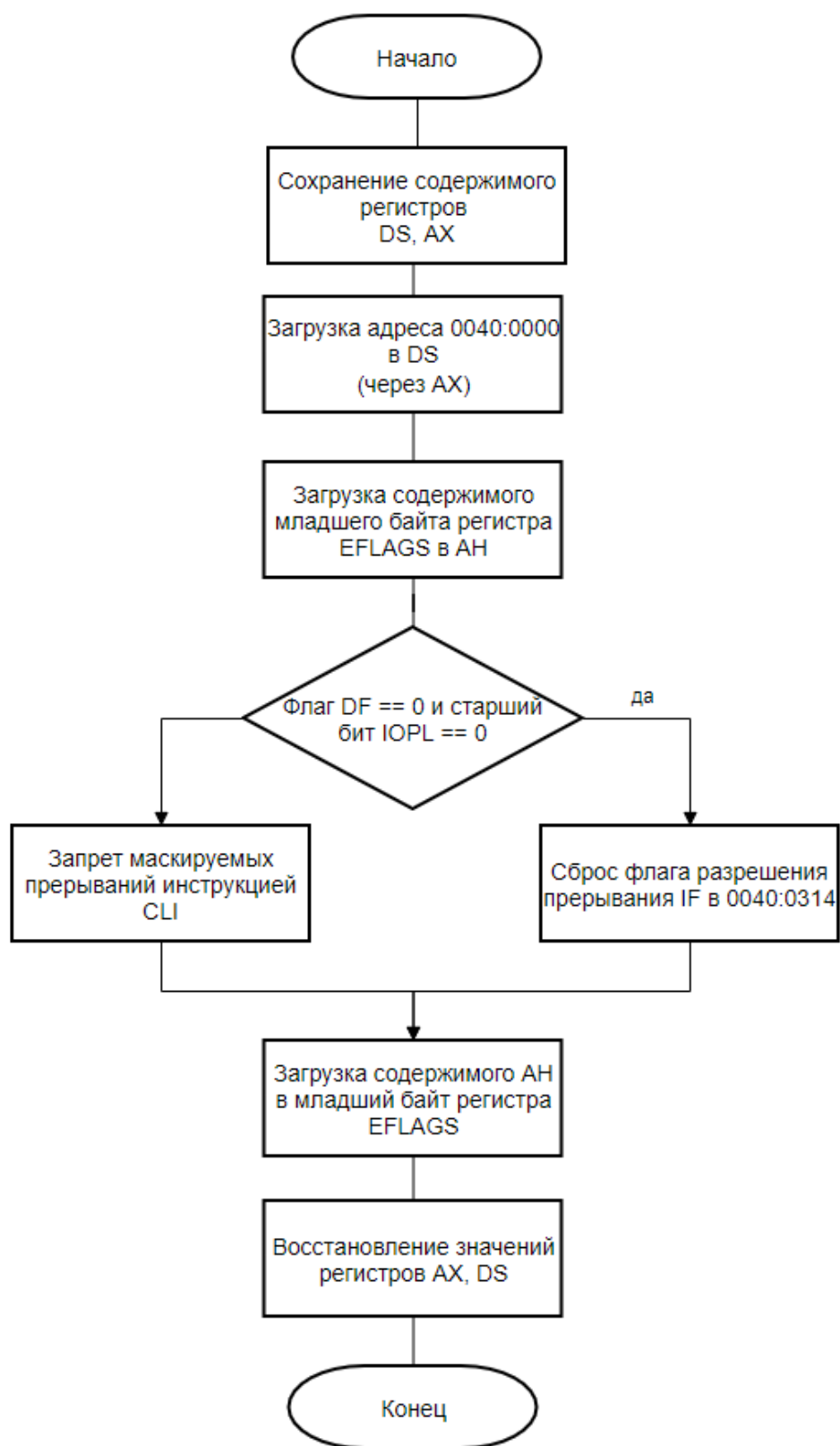


Рисунок 4 – Схема процедуры sub_2