



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 Исследование прерывания INT 8h

Студент Морозов Д.В.

Группа ИУ7-52Б

Преподаватель Рязанова Н.Ю.

Москва — 2022 г.

Листинг кода

Листинги прерывания int 8h и процедуры sub_1

Листинг INT8h

```
1 ; Вызов процедуры sub_1 (запрет прерываний)
2 020A:0746 E8 0070          call     sub_1          ; (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 записывается адрес 40h
11 ; адрес области данных BIOS
12 020A:074D B8 0040          mov     ax,40h
13 020A:0750 8E D8           mov     ds,ax
14
15 ; В регистр ES записывается адрес 0h
16 ; (адрес таблицы векторов прерываний)
17 020A:0752 33 C0           xor     ax,ax          ; Zero register
18 020A:0754 8E C0           mov     es,ax
19
20 ; Инкремент младшей части счётчика CB
21 020A:0756 FF 06 006C      inc     word ptr ds:timer_low ;
    (0040:006C=817h)
22
23 ; Если младшая часть счетчика CB == 0,
24 ; то инкремент двух старших байтов CB
25 ; иначе переходим на loc_1
26 020A:075A 75 04          jnz     loc_1          ; Jump if not zero
27
28 ; Инкремент старшей части счётчика CB
29 020A:075C FF 06 006E      inc     word ptr ds:timer_hi ;
    (0040:006E=11h)
30
31 ; Если два старших байта счетчика CB == 24
32 ; то сравниваем два младших байта счетчика CB
33 ; иначе декемент счетчика CB до отключения моторчика дисковод
34 020A:0760          loc_1:          ; xref 020A:075A
```

```

35 020A:0760 83 3E 006E 18          cmp word ptr ds:timer_hi,18h      ;
    (0040:006E=11h)
36 020A:0765 75 15                  jne loc_2                        ; Jump if not equal
37
38 ; Если два младших байта счетчика СВ == 176
39 ; то обнуление счетчика СВ и установка флага прошедших суток
40 ; иначе декремент счетчика времени до отключения моторчика дисковод
41 020A:0767 81 3E 006C 00B0        cmp word ptr ds:timer_low,0B0h    ;
    (0040:006C=817h)
42 020A:076D 75 0D                  jne loc_2                        ; Jump if not equal
43
44 ; Обнуляем счетчик ( если прошел день )
45 020A:076F A3 006E                mov ds:timer_hi,ax              ; (0040:006E=11h)
46 020A:0772 A3 006C                mov ds:timer_low,ax            ; (0040:006C=817h)
47
48 ; В ячейку 0040:0070 записываем единицу
49 ; (Для фиксации о том , что новый день наступил )
50 020A:0775 C6 06 0070 01          mov byte ptr ds:timer_rolled,1  ;
    (0040:0070=0)
51 020A:077A 0C 08                  or al,8
52
53 ; Декремент счетчика времени до отключения моторчика дисковод
54 020A:077C          loc_2:                ; xref 020A:0765, 076D
55 020A:077C 50                    push ax
56 020A:077D FE 0E 0040            dec byte ptr ds:dsk_motor_tmr    ;
    (0040:0040=0CAh)
57
58 ; Если значени этого счетчика == 0
59 ; то установка флага отключения моторчика и посылка команды в порт на откл
    ючения моторчика
60 020A:0781 75 0B                  jnz loc_3                        ; Jump if not zero
61 020A:0783 80 26 003F F0          and byte ptr ds:dsk_motor_stat,0F0h ;
    (0040:003F=0)
62 020A:0788 B0 0C                mov al,0Ch
63 020A:078A BA 03F2                mov dx,3F2h
64 020A:078D EE                    out dx,al                        ; port 3F2h, dsk0
    contrl output
65
66
67 020A:078E          loc_3:                ; xref 020A:0781
68 020A:078E 58                    pop ax
69
70 ; Проверка, установлен ли PF(parity flag) по адресу 0040:0314,
71 ; т.е. разрешен ли ответ на маскируемые прерывания
72 ; (0100, установлен 2 бит, отвечает за флаг PF, флаг четности)
73 020A:078F F7 06 0314 0004        test word ptr ds:data_12e,4      ;
    (0040:0314=3200h)
74

```

```

75 ; Если вызов маскируемых прерываний разрешен, переход к вызову int 1Ch (в
    loc_4)
76 020A:0795  75 0C                jnz loc_4                ; Jump if not zero
77 020A:0797  9F                    lahf                     ; Load ah from flags
78 020A:0798  86 E0                xchg    ah,al
79 020A:079A  50                    push    ax
80
81 ; иначе, косвенный вызов 1Ch - как процедуры командой call и переход к
    loc_5
82 ; (1C * 4 = 70h )
83 020A:079B  26: FF 1E 0070          call     dword ptr es:data_4e ;
    (0000:0070=6ADh)
84 020A:07A0  EB 03                jmp short loc_5          ; (07A5)
85
86 ; вызов пользовательского прерывания по таймеру
87 020A:07A3          loc_4:                ; xref 020A:0795
88 020A:07A3  CD 1C                int 1Ch                  ; Timer break (call each
    18.2ms)
89 ; после инициализации системы вектор INT 1Ch указывает на команду IRET
90
91 ; сброс контроллера прерываний
92 020A:07A5          loc_5:                ; xref 020A:07A0
93 020A:07A5  E8 0011          call     sub_1            ; (07B9)
94 020A:07A8  B0 20                mov al,20h              ; ' '
95 020A:07AA  E6 20                out 20h,al              ; port 20h, 8259-1
    int command
96 ; al = 20h, end of interrupt
97
98 ; восстановление значений регистров
99 020A:07AC  5A                    pop dx
100 020A:07AD  58                    pop ax
101 020A:07AE  1F                    pop ds
102 020A:07AF  07                    pop es
103
104 ; прыжок в адрес 020A:064C
105 020A:07B0  E9 FE99          jmp $-164h
106
107 ; ---
108 020A:06AC  CF                    iret                    ; Interrupt return

```

Листинг sub_1

```
1          sub_1          proc      near
2
3 ; Сохранение содержимого регистров DS, AX
4 020A:07B9  1E                      push    ds
5 020A:07BA  50                      push    ax
6
7 ; В регистр DS загружается адрес 0040:0000 начало области данных BIOS
8 020A:07BB  B8 0040                  mov     ax,40h
9 020A:07BE  8E D8                    mov     ds,ax
10
11 ; Загрузка AH
12 020A:07C0  9F                      lahf                    ; Load ah from flags
13
14 ; Если флаг DF == 0 и старший бит IOPL == 0
15 ; то сброс флага разрешения прерывания IF в 0040:0314
16 ; иначе запрет маскируемых прерываний инструкцией CLI
17 020A:07C1  F7 06 0314 2400          test     word ptr ds:data_12e,2400h ;
    (0040:0314=3200h)
18 020A:07C7  75 0C                    jnz     loc_7           ; Jump if not zero
19
20 ; Сброс флага IF
21 020A:07C9  F0> 81 26 0314 FDFF          lock and word
    ptr ds:data_12e,0FDFFh ; (0040:0314=3200h)
22 020A:07D0                    loc_6:                    ; xref 020A:07D6
23
24 ; Восстановление значений флагов
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_ret_8 ; (07D8)
31
32 ; Сброс IF, т. е. запрет прерываний с помощью команды cli
33 020A:07D5                    loc_7:                    ; xref 020A:07C7
34 020A:07D5  FA                      cli                    ; Disable interrupts
35 020A:07D6  EB F8                    jmp     short loc_6      ; (07D0)
36
37 020A:07D8                    loc_ret_8:                ; xref 020A:07D3
38
39 ; Выход из программы
40 020A:07D8  C3                      retn
41          sub_1          endp
```

Схема алгоритма

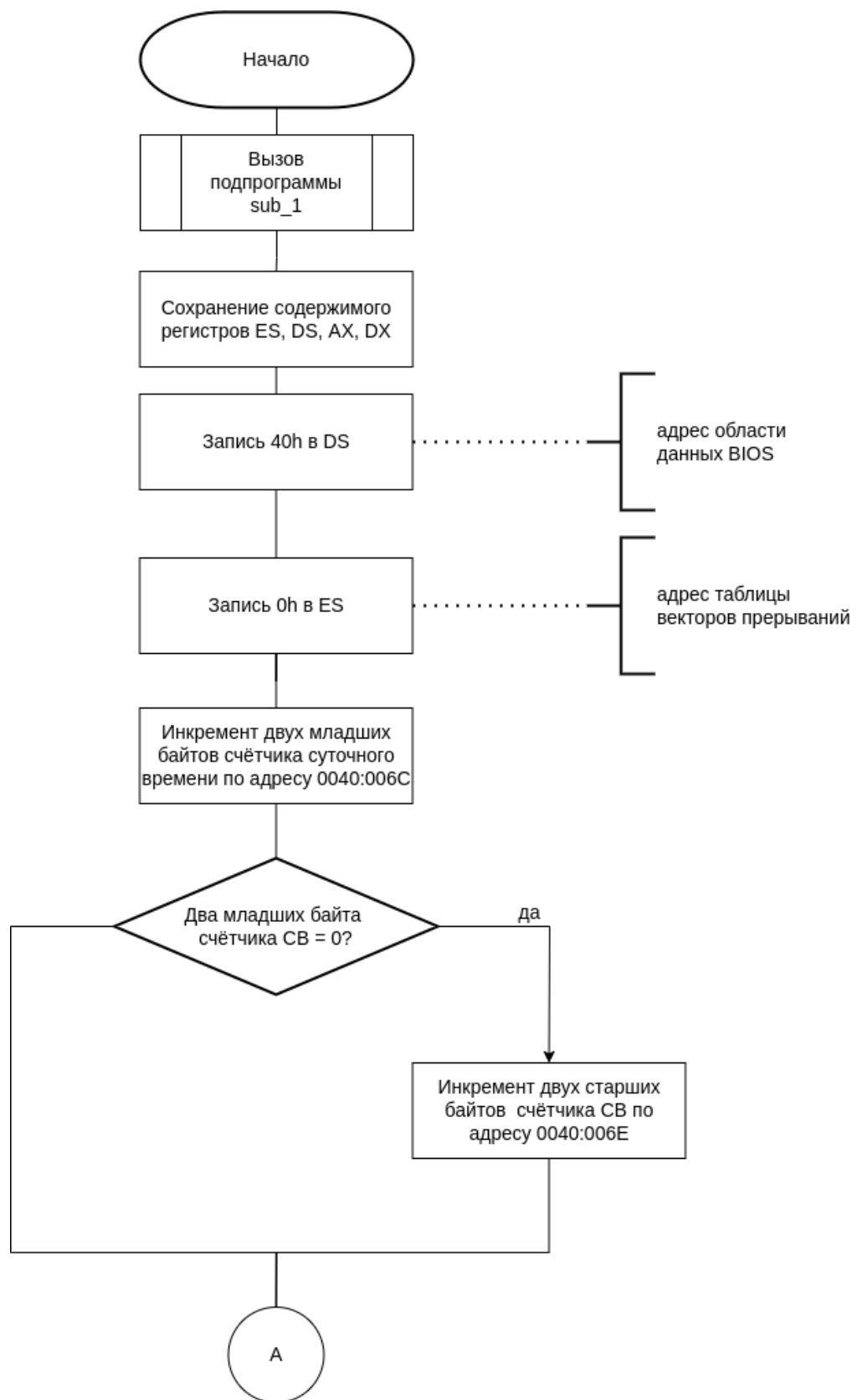


Рисунок 1 – Схема обработчика прерываний INT 8h

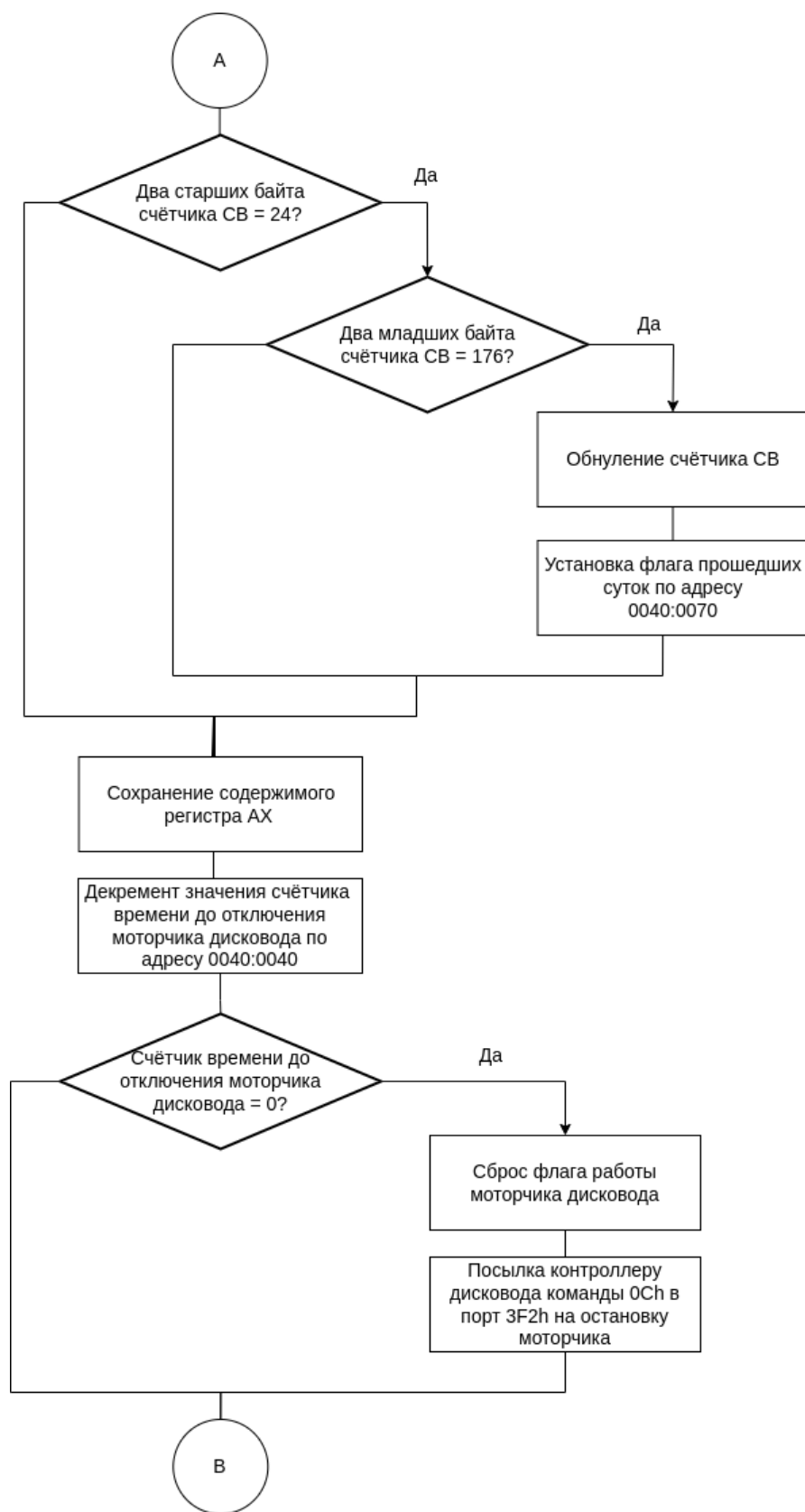


Рисунок 2 – Схема обработчика прерываний INT 8h

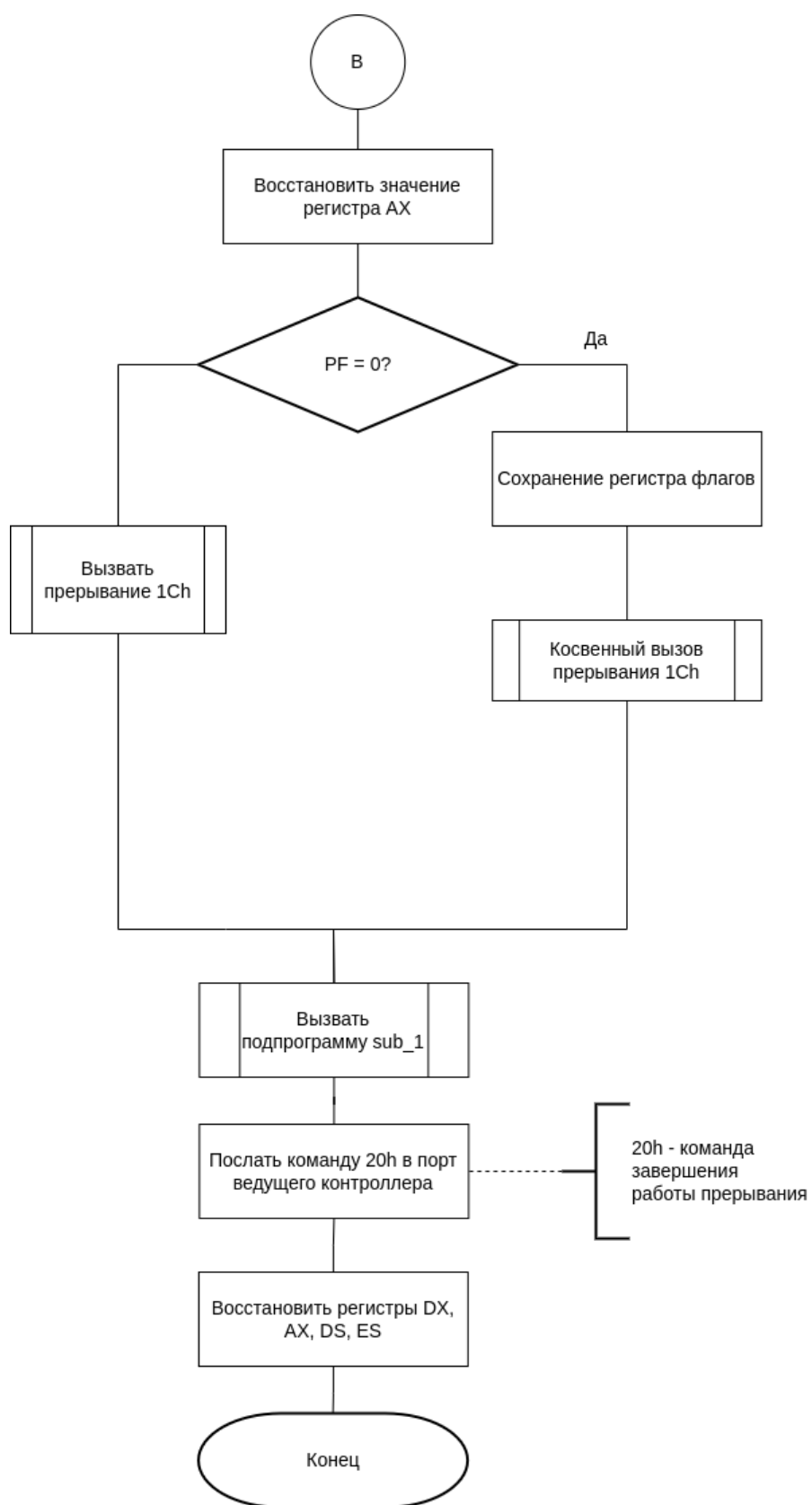


Рисунок 3 – Схема обработчика прерываний INT 8h

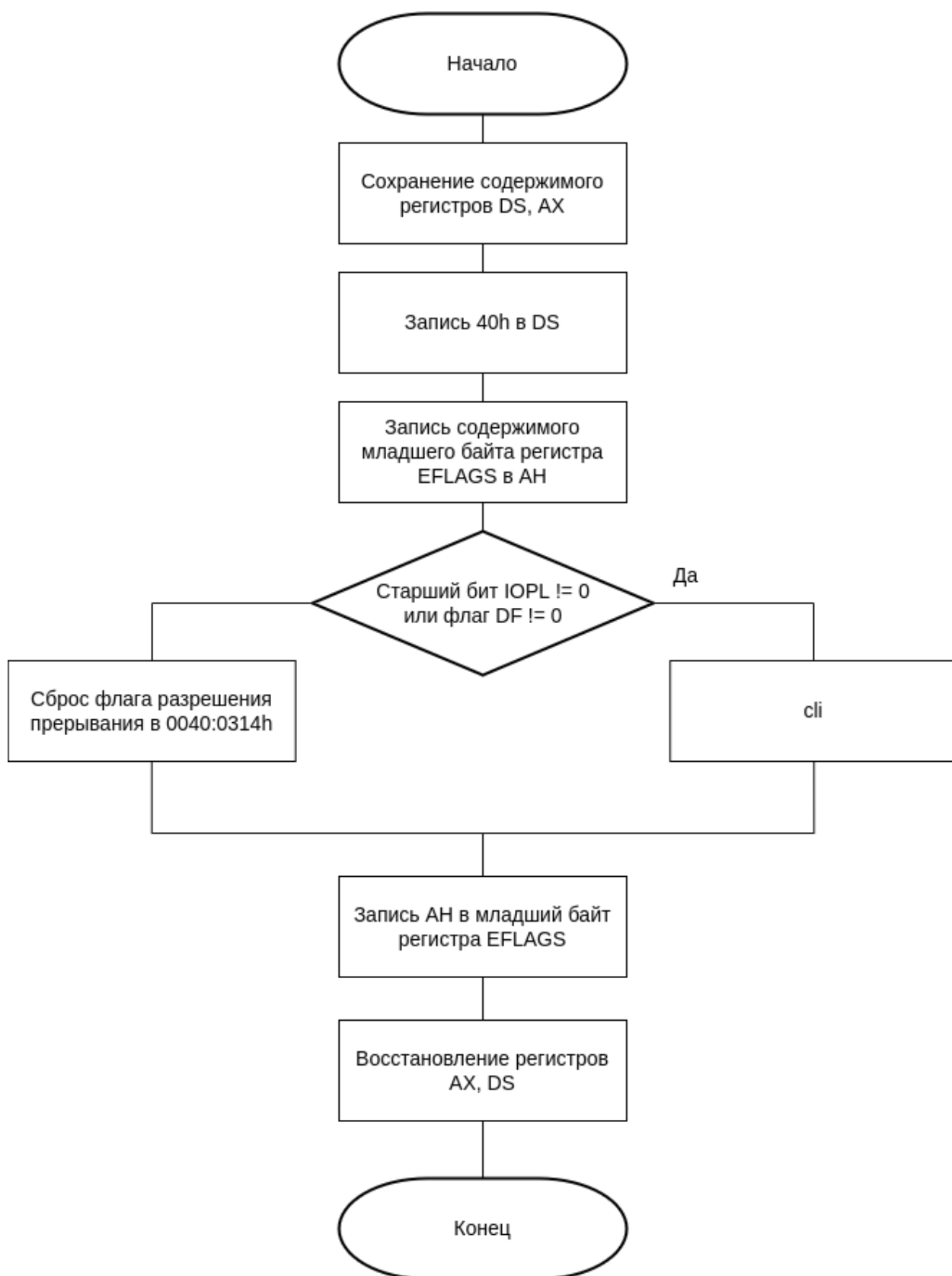


Рисунок 4 – Схема процедуры sub_1