



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 Хамзина Р.Р.

Группа ИУ7-53Б

Преподаватель Рязанова Н.Ю.

Москва — 2021 г.

Листинг кода

Цель

Знакомство со средством дизассемблирования – sourcer и с получением дизассемблерного кода ядра операционной системы Windows на примере обработчика прерывания INT 8h в virtual mode – специальном режиме защищенного режима, который эмулирует реальный режим работы вычислительной системы на базе процессоров Intel.

Листинг INT 8h

```
1 ; Вызов подпрограммы sub_1.
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 ; Загрузка в регистр DS 40h.
11 020A:074D B8 0040          mov     ax,40h
12 020A:0750 8E D8          mov     ds,ax
13
14 ; Загрузка в регистр ES 00h.
15 020A:0752 33 C0          xor     ax,ax          ; Zero register
16 020A:0754 8E C0          mov     es,ax
17
18 ; Инкремент счетчика таймера.
19 020A:0756 FF 06 006C      inc     word ptr ds:[6Ch] ;
    (0040:006C=4FBAh)
20 ; Проверка счетчика таймера == 0.
21 020A:075A 75 04          jnz     loc_1          ; Jump if not zero
22
23 ; Инкремент старшей части счетчика таймера.
24 020A:075C FF 06 006E      inc     word ptr ds:[6Eh] ;
    (0040:006E=11h)
25
```

```

26 020A:0760          loc_1:                      ; xref 020A:075A
27 ; Сравнение старшей части счетчика таймера с 24.
28 020A:0760  83 3E 006E 18          cmp word ptr ds:[6Eh],18h      ;
      (0040:006E=11h)
29 020A:0765  75 15                  jne loc_2              ; Jump if not equal
30
31 ; Сравнение младшей части счетчика таймера с 176.
32 020A:0767  81 3E 006C 00B0        cmp word ptr ds:[6Ch],0B0h    ;
      (0040:006C=4FBAh)
33 020A:076D  75 0D                  jne loc_2              ; Jump if not equal
34
35 ; Обнуление счетчика таймера.
36 020A:076F  A3 006E                mov word ptr ds:[6Eh],ax      ;
      (0040:006E=11h)
37 020A:0772  A3 006C                mov word ptr ds:[6Ch],ax      ;
      (0040:006C=4FBAh)
38
39 ; Загрузка 1 по адресу 0000:0470h,
40 ; если прошло более 24 часов с момента запуска таймера.
41 020A:0775  C6 06 0070 01          mov byte ptr ds:[70h],1      ;
      (0040:0070=0)
42 020A:077A  0C 08                  or al,8
43
44 020A:077C          loc_2:                      ; xref 020A:0765, 076D
45 ; Сохранение регистра AX.
46 020A:077C  50                    push ax
47 ; Декремент времени, оставшегося до отключения моторчика дисковод.
48 020A:077D  FE 0E 0040            dec byte ptr ds:[40h]        ;
      (0040:0040=44h)
49 ; Проверка счетчика таймера == 0.
50 020A:0781  75 0B                  jnz loc_3              ; Jump if not zero
51 ; Установка флага, необходимого для отключения моторчика дисковод.
52 020A:0783  80 26 003F F0          and byte ptr ds:[3Fh],0F0h    ;
      (0040:003F=0)
53 ; В порт - команду отключения моторчика дисковод.
54 020A:0788  B0 0C                  mov al,0Ch
55 020A:078A  BA 03F2                mov dx,3F2h
56 020A:078D  EE                    out dx,al                ; port 3F2h, disk
      contrl output
57
58 020A:078E          loc_3:                      ; xref 020A:0781
59 ; Восстановление регистра AX.
60 020A:078E  58                    pop ax
61 ; Проверка флага PF.
62 020A:078F  F7 06 0314 0004        test word ptr ds:[314h],4      ;
      (0040:0314=3200h)
63 020A:0795  75 0C                  jnz loc_4              ; Jump if not zero
64 ; Сохранение младшего байта регистра FLAGS в AH.

```

```

65 020A:0797  9F          lahf                ; Load ah from flags
66 020A:0798  86 E0      xchg         ah,al
67 ; Сохранение регистра AX.
68 020A:079A  50          push         ax
69 ; Косвенный вызов 1Ch.
70 020A:079B  26: FF 1E 0070      call         dword ptr es:[70h] ;
    (0000:0070=6ADh)
71 020A:07A0  EB 03      jmp short loc_5      ; (07A5)
72 020A:07A2  90          nop
73
74 020A:07A3          loc_4:                ; xref 020A:0795
75 ; Вызов прерывания 1Ch.
76 020A:07A3  CD 1C      int 1Ch            ; Timer break (call each
    18.2ms)
77
78 020A:07A5          loc_5:                ; xref 020A:07A0
79 ; Вызов подпрограммы sub_1.
80 020A:07A5  E8 0011      call         sub_1            ; (07B9)
81 ; Сброс контроллера прерываний.
82 020A:07A8  B0 20      mov al,20h          ; ' '
83 020A:07AA  E6 20      out 20h,al         ; port 20h, 8259-1
    int command
84
85
86 ; Восстановление регистров DX, AX, DS, ES.
87 020A:07AC  5A          pop dx
88 020A:07AD  58          pop ax
89 020A:07AE  1F          pop ds
90 020A:07AF  07          pop es
91
92 ; Переход в адрес 020A:064C.
93 020A:07B0  E9 FE99      jmp $-164h
94 ; ...
95 020A:06AC  CF          iret                ; Interrupt return

```

Листинг sub_1

```
1      sub_1      proc      near
2  ; Сохранение содержимого регистров DS, AX.
3  020A:07B9      1E                                push      ds
4  020A:07BA      50                                push      ax
5
6  ; Загрузка в регистр DS 40h.
7  020A:07BB      B8 0040                          mov ax,40h
8  020A:07BE      8E D8                          mov ds,ax
9
10 ; Сохранение младшего байта регистра FLAGS в AH.
11 020A:07C0      9F                                lahf                                ; Load ah from flags
12
13 ; Проверка флага DF == 0. Проверка старшего бита IOPL == 0.
14 020A:07C1      F7 06 0314 2400                  test      word ptr ds:[314h],2400h ;
    (0040:0314=3200h)
15 020A:07C7      75 0C                          jnz loc_2                          ; Jump if not zero
16
17 ; IF = 0 в 0040:0314h.
18 020A:07C9      F0> 81 26 0314 FDFD             lock and word ptr
    ds:[314h],0FDFFh ; (0040:0314=3200h)
19
20 020A:07D0                                loc_1:                                ; xref 020A:07D6
21 ; Загрузка содержимого AH в младший байт регистра FLAGS.
22 020A:07D0      9E                                sahf                                ; Store ah into flags
23
24 ; Восстановление регистров AX, DS.
25 020A:07D1      58                                pop ax
26 020A:07D2      1F                                pop ds
27 020A:07D3      EB 03                          jmp short loc_ret_3                ; (07D8)
28
29 020A:07D5                                loc_2:                                ; xref 020A:07C7
30 ; IF = 0. Запрет прерываний от внешних устройств.
31 020A:07D5      FA                                cli                                ; Disable interrupts
32 020A:07D6      EB F8                          jmp short loc_1                    ; (07D0)
33
34 020A:07D8                                loc_ret_3:                            ; xref 020A:07D3
35 ; Возврат из подпрограммы.
36 020A:07D8      C3                                retn
37 sub_1      endp
```

Схемы алгоритмов



Рисунок 1 – Схема обработчика прерываний INT 8h

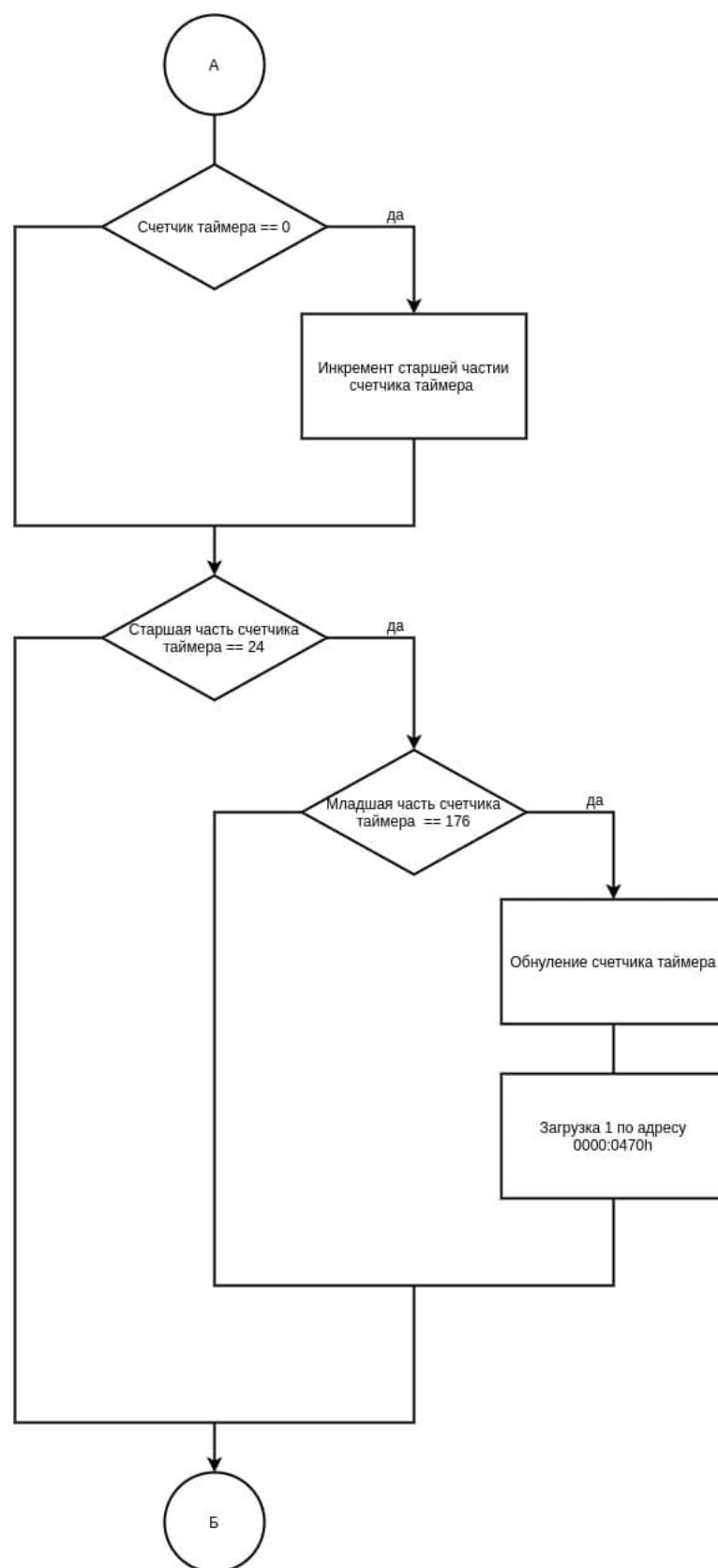


Рисунок 2 – Схема обработчика прерываний INT 8h



Рисунок 3 – Схема обработчика прерываний INT 8h

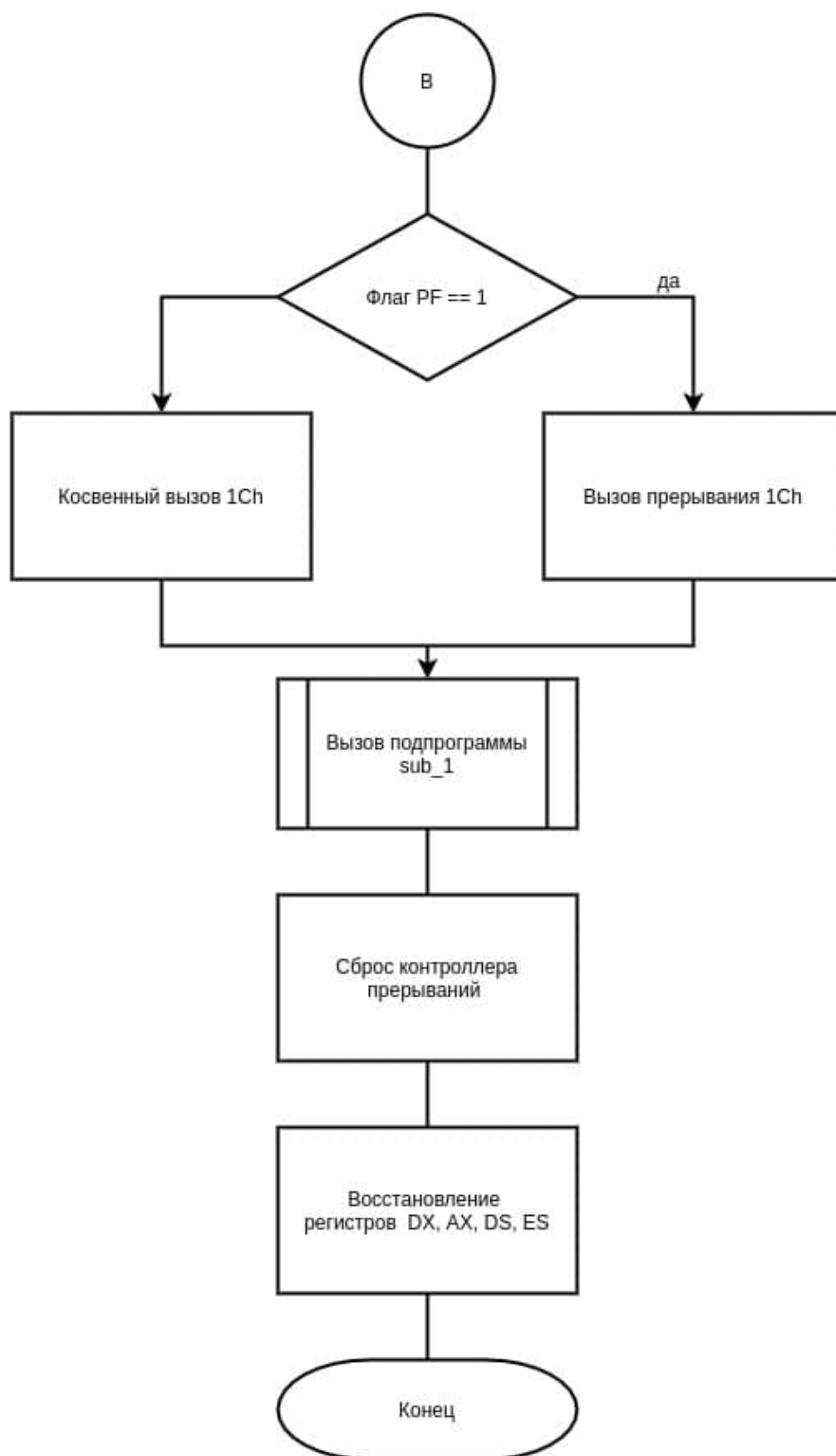


Рисунок 4 – Схема обработчика прерываний INT 8h

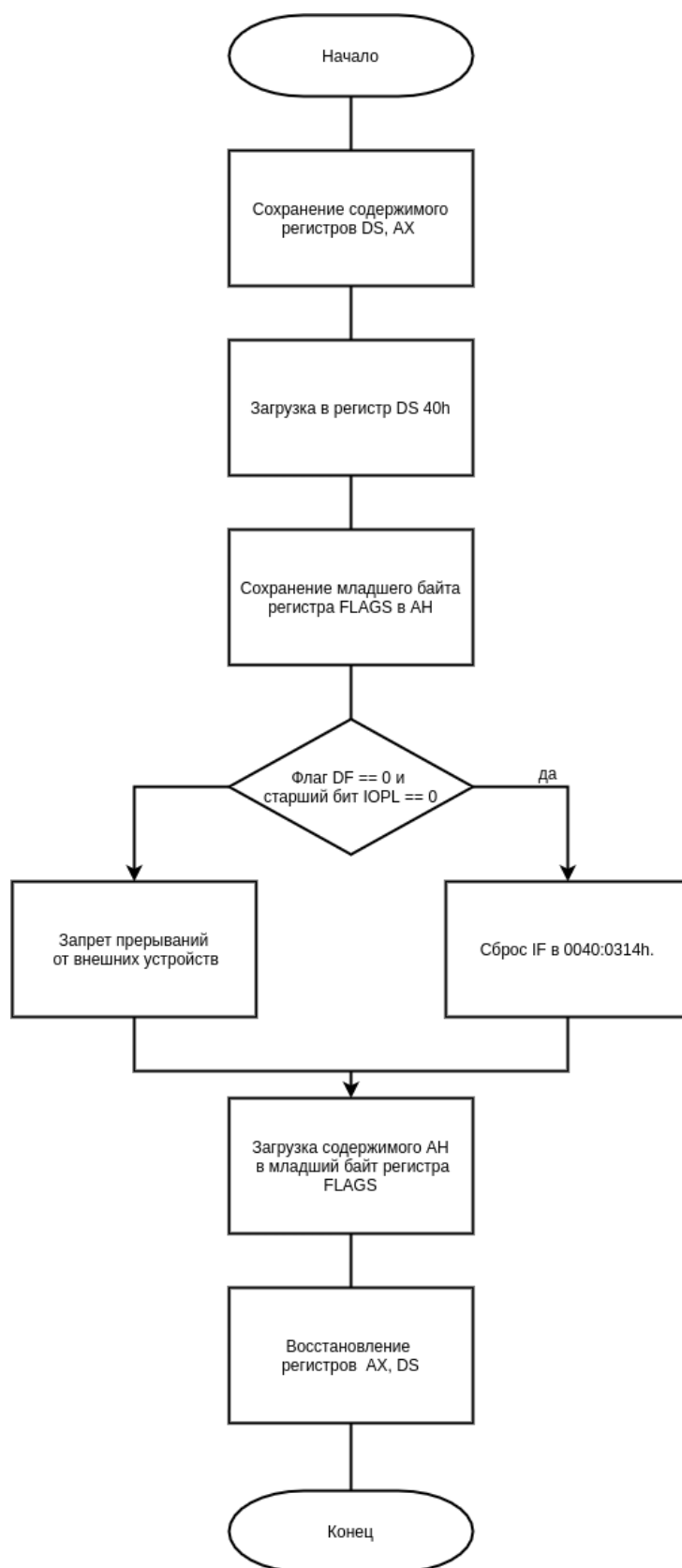


Рисунок 5 – Схема подпрограммы sub_1