



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

Тема Прерывание INT 8h

Студент Кононенко С.С.

Группа ИУ7-53Б

Оценка (баллы) _____

Преподаватели Рязанова Н.Ю.

Москва — 2020 г.

Цель работы

Знакомство со средством дизассемблирования Sourcer, получение дизассемблированного кода ядра операционной системы Windows на примере обработчика прерывания INT 8h в virtual mode – специальном режиме защищенного режима (32-разрядный режим работы), который эмулирует реальный режим работы вычислительной системы на базе процессоров Intel.

Задание

Используя Sourcer получить дизассемблированный код обработчика аппаратного прерывания от системного таймера INT 8h.

На основе полученного кода составить алгоритм работы обработчика INT 8h.

Листинг кода

```
1 ;; Вызов процедуры sub_1
2 020A:0746 E8 0070          call sub_1      ; (07B9)
3 ;; Сохранение регистров ES, DS, AX, DX
4 020A:0749 06              push es
5 020A:074A 1E              push ds
6 020A:074B 50              push ax
7 020A:074C 52              push dx
8 020A:074D B8 0040          mov ax,40h
9 020A:0750 8E D8            mov ds,ax
10 020A:0752 33 C0           xor ax,ax      ; Zero register
11 020A:0754 8E C0           mov es,ax
12 ;; 0040:006Ch - адрес счетчика таймера
13 020A:0756 FF 06 006C         inc word ptr ds:[6Ch] ; (0040:006C=5060h)
14 020A:075A 75 04           jnz loc_1      ; Jump if not zero
15 ;; 0040:006Eh - старшие 2 байта счетчика таймера
16 020A:075C FF 06 006E         inc word ptr ds:[6Eh] ; (0040:006E=0Fh)
17 020A:0760 loc_1:
18 ;; Проверка: 0040:006Eh == 18h (24) И 0040:006Ch == B0h (176)
```

```

19 ;; Это проаерка на то, прошли ли сутки
20 020A:0760 83 3E 006E 18      cmp word ptr ds:[6Eh],18h ; (0040:006E=0Fh)
21 020A:0765 75 15              jne loc_2      ; Jump if not equal
22 020A:0767 81 3E 006C 00B0    cmp word ptr ds:[6Ch],0B0h ; (0040:006C=5061h)
23 020A:076D 75 0D              jne loc_2      ; Jump if not equal
24 ;; Зануление счетчика
25 020A:076F A3 006E              mov word ptr ds:[6Eh],ax ; (0040:006E=0Fh)
26 020A:0772 A3 006C              mov word ptr ds:[6Ch],ax ; (0040:006C=5061h)
27 ;; Прошло более 24 часов, занесение значения 1 в 0040:0070
28 020A:0775 C6 06 0070 01      mov byte ptr ds:[70h],1 ; (0040:0070=0)
29 020A:077A 0C 08              or al,8
30 020A:077C      loc_2:
31 020A:077C 50                  push ax
32 ;; Декремент счетчика отключения моторчика дисковод
33 020A:077D FE 0E 0040          dec byte ptr ds:[40h] ; (0040:0040=0F6h)
34 020A:0781 75 0B              jnz loc_3      ; Jump if not zero
35 ;; Установка флага отключения дисковод
36 020A:0783 80 26 003F F0      and byte ptr ds:[3Fh],0F0h ; (0040:003F=0)
37 ;; Посылка дисководу команды на отключение
38 020A:0788 B0 0C              mov al,0Ch
39 020A:078A BA 03F2            mov dx,3F2h
40 020A:078D EE              out dx,al      ; port 3F2h, dsk0 contrl output
41 020A:078E      loc_3:
42 020A:078E 58                  pop ax
43 ;; Проверка 2 бита PF
44 020A:078F F7 06 0314 0004      test word ptr ds:[314h],4 ; (0040:0314=3300h)
45 020A:0795 75 0C              jnz loc_4      ; Jump if not zero
46 ;; Младший байт FLAGS в AH
47 020A:0797 9F              lahf          ; Load ah from flags
48 020A:0798 86 E0              xchg ah,al
49 020A:079A 50                  push ax
50 020A:079B 26: FF 1E 0070      call dword ptr es:[70h] ; (0000:0070=6ADh)
51 020A:07A0 EB 03              jmp short loc_5 ; (07A5)
52 020A:07A2 90                  nop
53 020A:07A3      loc_4:
54 ;; Вызов прерывания
55 020A:07A3 CD 1C              int 1Ch      ; Timer break (call each 18.2ms)
56 020A:07A5      loc_5:
57 020A:07A5 E8 0011            call sub_1    ; (07B9)
58 ;; Сброс контроллера прерываний
59 020A:07A8 B0 20              mov al,20h   ; ' '
60 020A:07AA E6 20              out 20h,al   ; port 20h, 8259-1 int command
61 ; al = 20h, end of interrupt
62 ;; Восстановление регистров
63 020A:07AC 5A                  pop dx
64 020A:07AD 58                  pop ax
65 020A:07AE 1F                  pop ds
66 020A:07AF 07                  pop es

```

```

67 ; (020A:07B0h - 164h = 020A:064Ch)
68 020A:07B0 E9 FE99          jmp $-164h
69 ;; ... -164h
70 020A:064C 1E              push ds
71 020A:064D 50              push ax
72 ;; ...
73 020A:06AA 58              pop ax
74 020A:06AB 1F              pop ds
75 020A:06AC CF              iret ; Interrupt return

```

Листинг 1: Обработчик INT 8h

```

1 sub_1 proc near
2 ;; Сохранение регистров
3 020A:07B9 1E              push ds
4 020A:07BA 50              push ax
5 020A:07BB B8 0040          mov ax,40h
6 020A:07BE 8E D8           mov ds,ax
7 ;; Младший байт FLAGS в AH
8 020A:07C0 9F              lahf      ; Load ah from flags
9 ;; Проверка старшего бита IOPL или DF?
10 020A:07C1 F7 06 0314 2400 test word ptr ds:[314h],2400h ;
    (0040:0314=3300h)
11 020A:07C7 75 0C           jnz loc_7   ; Jump if not zero
12 ;; Сброс IF в 0040:0314h
13 020A:07C9 F0> 81 26 0314 FDFF lock and word ptr ds:[314h],0FDFFh ;
    (0040:0314=3300h)
14 020A:07D0 loc_6:
15 ;; AH в младший байт FLAGS
16 020A:07D0 9E              sahf      ; Store ah into flags
17 020A:07D1 58              pop ax
18 020A:07D2 1F              pop ds
19 020A:07D3 EB 03           jmp short loc_8 ; (07D8)
20 020A:07D5 loc_7:
21 ;; Сброс IF
22 020A:07D5 FA              cli      ; Disable interrupts
23 020A:07D6 EB F8           jmp short loc_6 ; (07D0)
24 020A:07D8 loc_8:
25 020A:07D8 C3              retn
26 sub_1 endp

```

Листинг 2: Процедура sub_1

Схема алгоритма

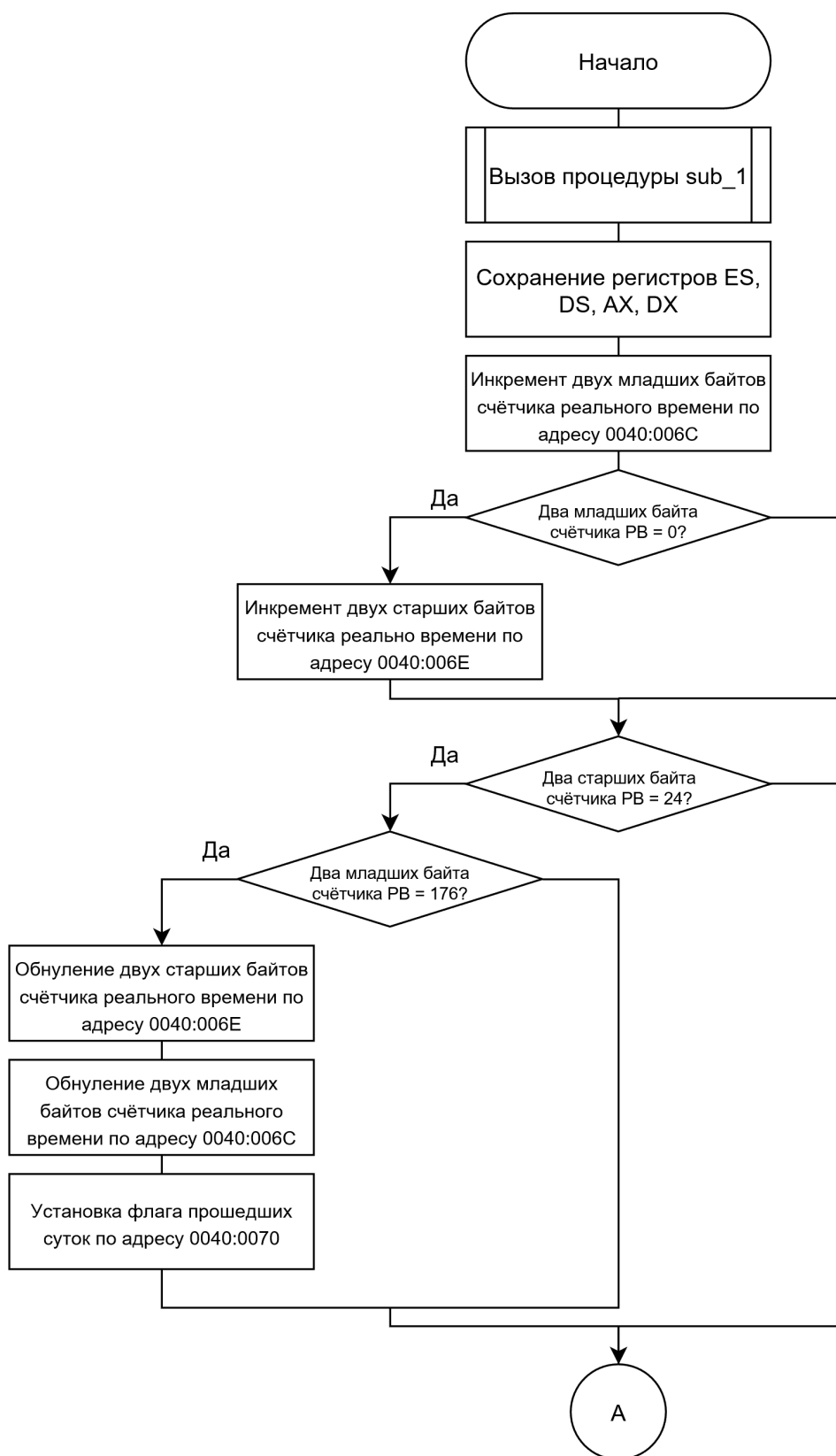


Рисунок 1: Схема обработчика прерываний INT 8h

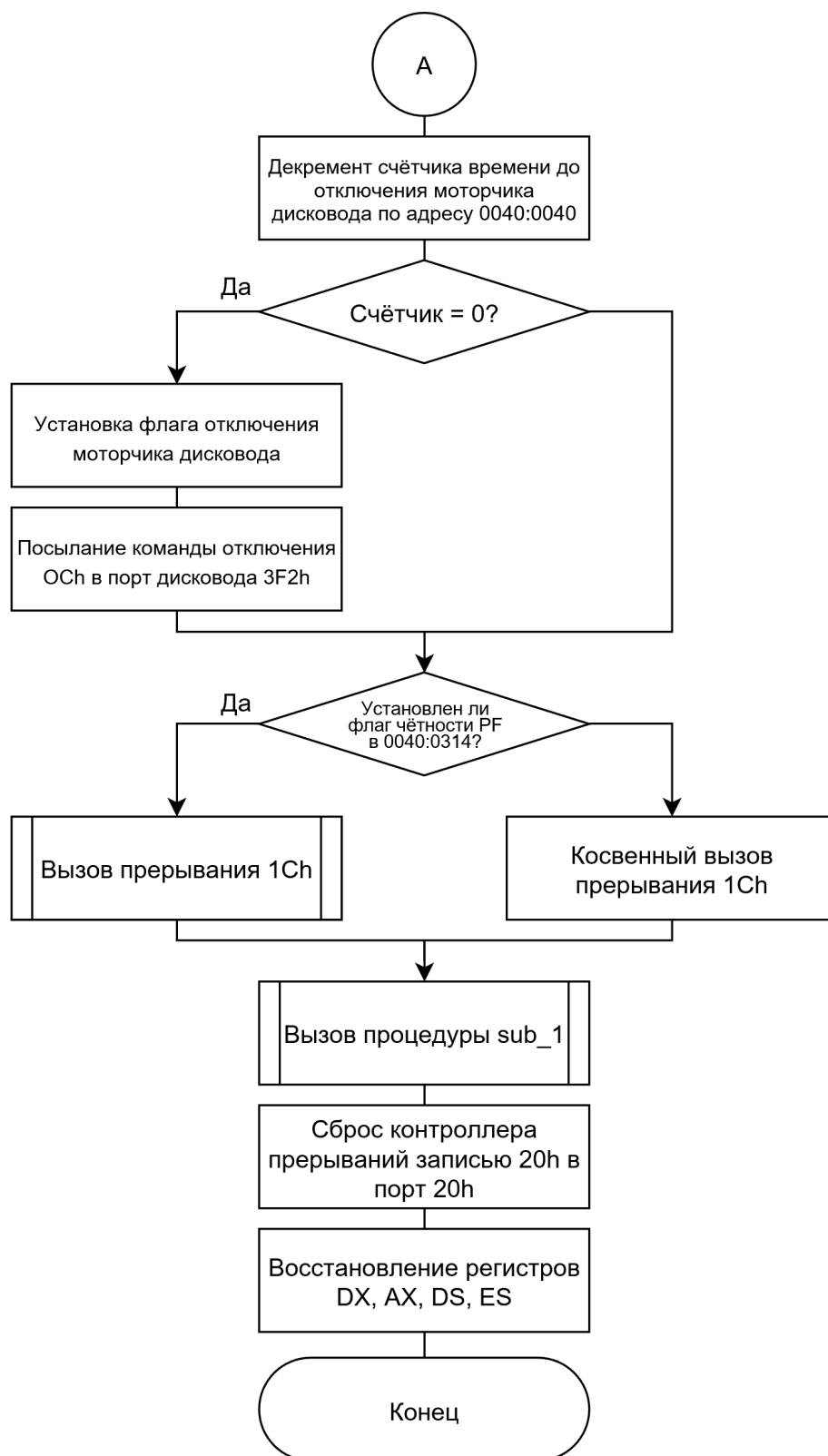


Рисунок 2: Схема обработчика прерываний INT 8h



Рисунок 3: Схема процедуры sub_1

Вывод

Функции обработчика прерывания INT 8h в DOS:

- Увеличивает текущее значение четырехбайтовой переменной, располагающейся в области данных BIOS по адресу 0000:046Ch. По этому адресу располагается счетчик тиков таймера. Если этот счетчик переполняется (после 24 часов с момента запуска таймера), в ячейку 0000:0470h заносится 1.
- Контроль за работой двигателей моторчика дисководов. Если после последнего обращения к НГМД прошло более 2 секунд, обработчик прерывания выключает двигатель. Ячейка с адресом 0000:0440h содержит время, оставшееся до выключения двигателя. Это время постоянно уменьшается обработчиком прерывания таймера. Когда оно становится равно 0, двигатель НГМД отключается.
- Вызов пользовательского прерывания 1Ch. Его стандартный обработчик состоит из одной команды IRET. Во время выполнения прерывания INT 1Ch все аппаратные прерывания запрещены.

Заключение

Прерывание INT 8h отвечает за изменение счётчика системного времени и управление контроллером дисководов с целью минимизации времени работы дисководов, а также отвечает за периодический вызов пользовательского прерывания.