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

к лабораторной работе №1 (часть 1) по курсу «Операционные системы» по теме «Дизассемблирование INT 8h»

студента ИУ7-53Б

Саркисов Артём

Преподаватель: Рязанова Н. Ю.

2020 г.

Листинг 1: прерывание int 8h

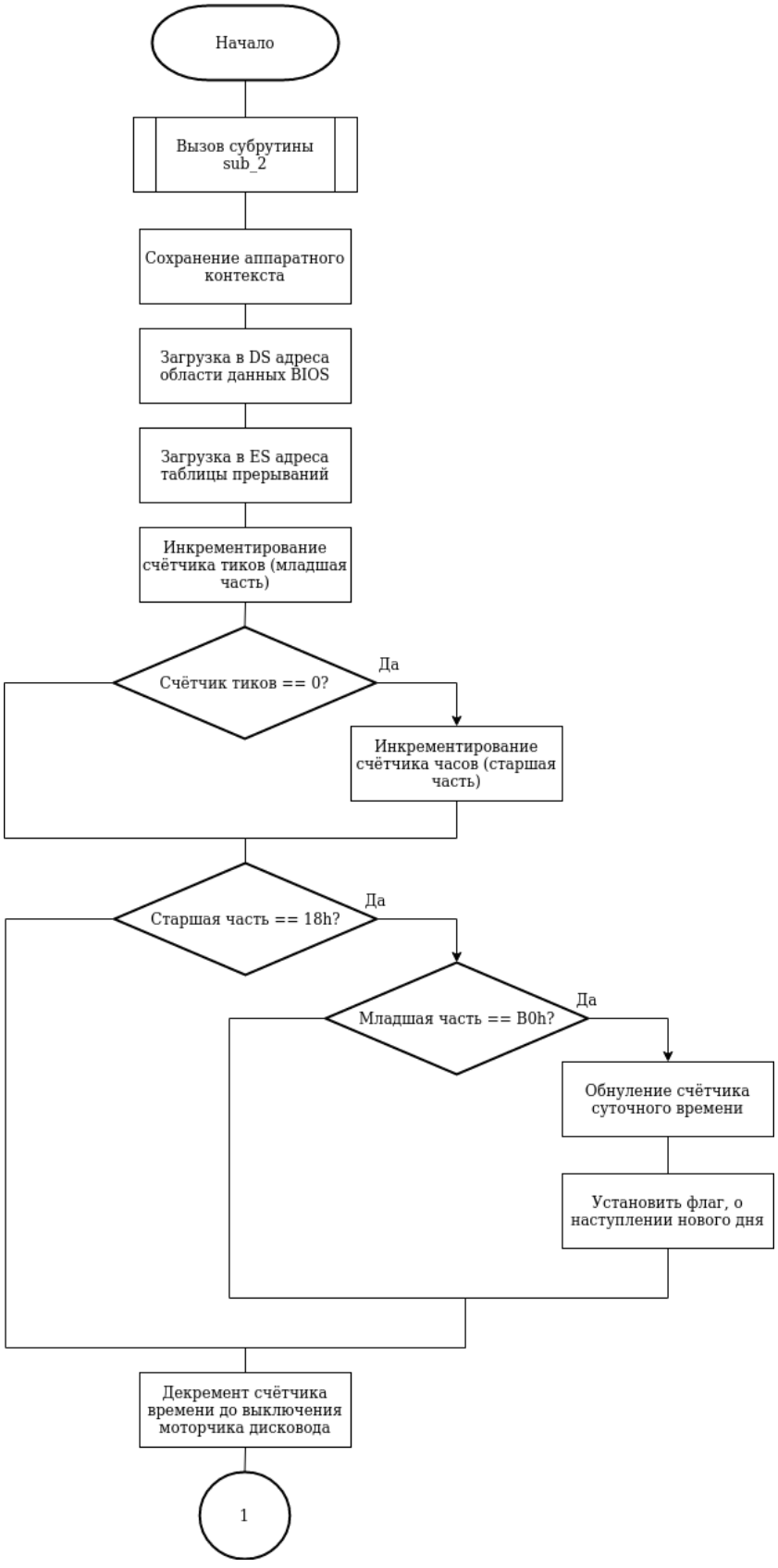
```
; Вызов подпрограммы sub_2
020C:0746  E8 0070         call   sub_2     ; (07B9)

; Сохранение аппаратного контекста
020C:0749  06          push   es
020C:074A  1E          push   ds
020C:074B  50          push   ax
020C:074C  52          push   dx

; Сегмент данных BIOS
020C:074D  B8 0040         mov ax,40h
020C:0750  8E D8           mov ds,ax

; Адрес начала таблицы прерываний
020C:0752  33 C0           xor ax,ax        ; Zero register
020C:0754  8E C0           mov es,ax

; Инкремент счетчиков времени
020C:0756  FF 06 006C         inc word ptr ds:[6Ch]   ;(0040:006C=4FF2h)
020C:075A  75 04           jnz loc_1        ; Jump if not zero
020C:075C  FF 06 006E         inc word ptr ds:[6Eh]   ; (0040:006E=16h)

; Сброс счетчиков времени при наступлении нового дня
020C:0760       loc_1:
020C:0760  83 3E 006E 18         cmp word ptr ds:[6Eh],18h  ; 020C:0765  75
15             jne loc_2  ; Jump if not equal
020C:0767  81 3E 006C 00B0       cmp word ptr ds:[6Ch],0B0h ;
020C:076D  75 0D              jne loc_2  ; Jump if not equal
020C:076F  A3 006E            mov word ptr ds:[6Eh],ax   ;
020C:0772  A3 006C            mov word ptr ds:[6Ch],ax   ;
020C:0775  C6 06 0070 01                mov byte ptr ds:[70h],1 ;
020C:077A  0C 08              or  al,8

; Отправка сигнала отключения моторчика
020C:077C       loc_2:
020C:077C  50              push   ax
020C:077D  FE 0E 0040            dec byte ptr ds:[40h]   ;
020C:0781  75 0B              jnz loc_3  ; Jump if not zero
020C:0783  80 26 003F F0         and byte ptr ds:[3Fh],0F0h ;
020C:0788  B0 0C              mov al,0Ch
020C:078A  BA 03F2            mov dx,3F2h
020C:078D  EE              out dx,al        ; port 3F2h, dsk0 contrl output

; Проверка возможности вызова маск. прерываний
020C:078E       loc_3:
020C:078E  58              pop ax
020C:078F  F7 06 0314 0004       test   word ptr ds:[314h],4   ;
020C:0795  75 0C              jnz loc_4  ; Jump if not zero
020C:0797  9F              lahf   ; Load ah from flags
020C:0798  86 E0              xchg   ah,al
020C:079A  50              push   ax
020C:079B  26: FF 1E 0070        call   dword ptr es:[70h]  ;
020C:07A0  EB 03              jmp short loc_5  ; (07A5)
020C:07A2  90              nop

; Вызов прерывания по таймеру
020C:07A3       loc_4:
020C:07A3  CD 1C              int 1Ch; Timer break (call each 18.2ms)
020C:07A5       loc_5:
020C:07A5  E8 0011            call   sub_2  ; (07B9)
```

```
; Сброс контроллера прерываний
020C:07A8  B0 20              mov al,20h; ' '
020C:07AA  E6 20              out 20h,al; port 20h, 8259-1 int
                      ;  al = 20h, end of interrupt


; Восстановление аппаратного контекста
020C:07AC  5A              pop dx
020C:07AD  58              pop ax
020C:07AE  1F              pop ds
020C:07AF  07              pop es

; Переход по метке, чтобы выйти из прерывания
020C:07B0  E9 FE99            jmp $-164h
020C:07B3  C4              db  0C4h

; Выход из прерывания
020C:06AA 58               pop ax
020C:06AB 1F               pop ds
020C:06AC CF               iret; Interrupt return
```

Листинг 2: подпрограмма sub_2:

```
             sub_2     proc   near
; Сохранение значений регистров, восстановление значений флагов
020C:07B9  1E              push   ds
020C:07BA  50              push   ax

; Сегмент данных BIOS
020C:07BB  B8 0040            mov ax,40h
020C:07BE  8E D8              mov ds,ax

020C:07C0  9F              lahf; Load ah from flags

; Проверка: разрешены ли маскируемые прерывания?
020C:07C1  F7 06 0314 2400       test   word ptr ds:[314h],2400h;
020C:07C7  75 0C              jnz loc_7; Jump if not zero
020C:07C9  F0> 81 26 0314 FDFF         lock   and word ptr ds:[314h],0FDFFh
   ; (0040:0314=3200h)

; Сохраняем значения флагов, восстанавливаем значения регистров
020C:07D0        loc_6:
020C:07D0  9E              sahf; Store ah into flags
020C:07D1  58              pop ax
020C:07D2  1F              pop ds
020C:07D3  EB 03              jmp short loc_8   ; (07D8)

; Сбрасываем IF в eflags, процессор игнорирует все прерывания кроме NMI
(Non-maskable interrupt)
020C:07D5        loc_7:
020C:07D5  FA              cli; Disable interrupts
020C:07D6  EB F8              jmp short loc_6      ; (07D0)
020C:07D8        loc_8:
020C:07D8  C3              retn
             sub_2         endp
```

Схема алгоритма обработки прерывания от системного таймера:



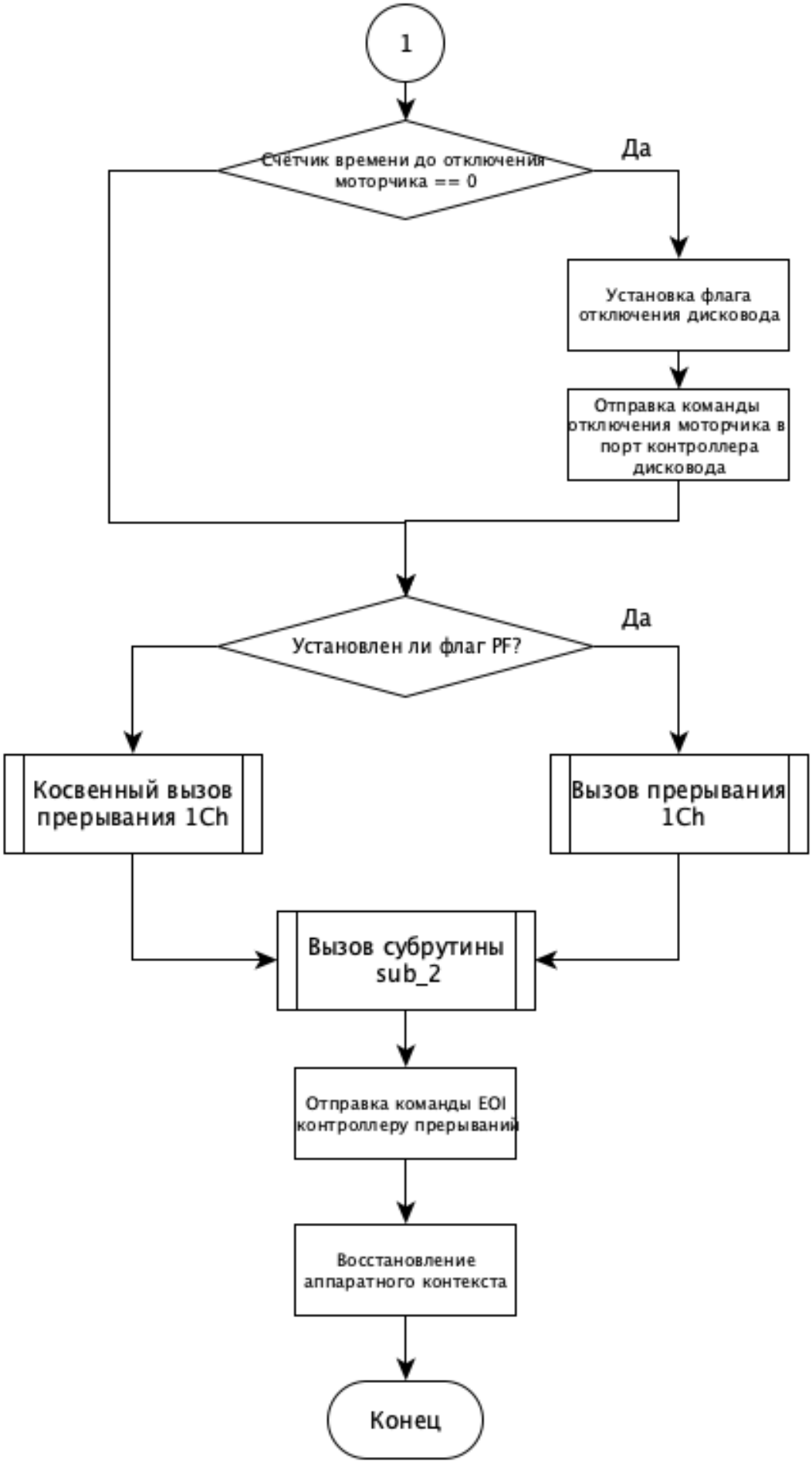
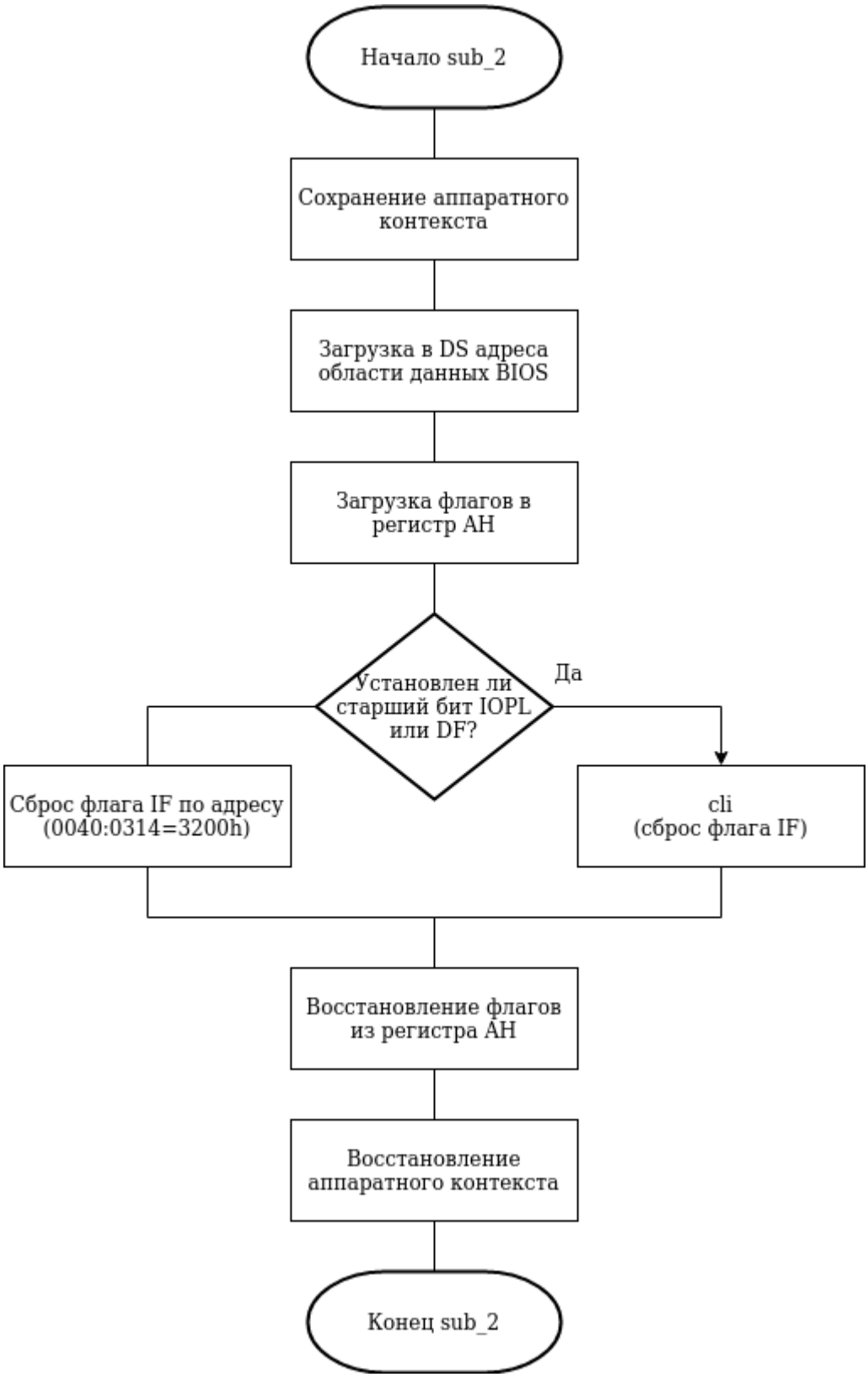

1
Счётчик времени до отключения моторчика == 0
Да
Установка флага отключения дисковода
Отправка команды отключения моторчика в порт контроллера дисковода
Установлен ли флаг PF?
Да
Косвенный вызов прерывания 1Ch
Вызов прерывания 1Ch
Вызов субрутины sub_2
Отправка команды EOI контроллеру прерываний
Восстановление аппаратного контекста
Конец

Схема алгоритма субрутины sub_2:



ы

Функции обработчика прерывания 08h:

- Инкремент значения счетчика тиков.
- Контроль переполнения счетчика тиков (наступление нового дня).
- Вызов пользовательского прерывания 1Ch (iret), с помощью которого
- можно совершать периодические действия.
- Декремент времени, оставшегося до выключения моторчика дисковода.
- Выключение моторчика дисковода, по истечению таймера.

Вывод:

В данной лабораторной работе я:

1. научился получать адрес начала прерывания и листинг прерывания с помощью дизассемблирования;
2. изучил алгоритм работы прерывания int 8h. Это прерывание отвечает за изменение счётчика системного времени, управление контроллером дисковода с целью минимизировать время работы моторчика дисковода, а также является способом периодического вызова пользовательского прерывания.