Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательно

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”

Лабораторная работа № 1

по дисциплине “Операционные системы”

Студент: Федин А.А.

Группа: ИУ7-54Б

Тема: Дизассемблирование INT 8h

Студент	_____	**Федин А.А.**
	Подпись, дата	**Фамилия, И.О.**
Преподаватель:	_____	**Рязанова Н.Ю.**
	Подпись, дата	**Фамилия, И.О.**

Москва, 2025 год

1 Листинги дизассемблированного кода

1.1 Листинг обработчика прерывания INT 8

```
1            Temp.lst                 Sourcer v5.10   10-Sep-25
                 6:58 pm   Page 1
2
3                                                     ;* No entry
                                                          point to
                                                          code
4   ;; -- Вызов подпрограммы sub_1
5   020A:0746  E8 0070      ;*      call    sub_1           ;*
6   020A:0746  E8 70 00             db  0E8h, 70h, 00h
7   ;; -- Сохранение регистров es,dx,ax,dx
8   020A:0749  06                   push    es
9   020A:074A  1E                   push    ds
10  020A:074B  50                   push    ax
11  020A:074C  52                   push    dx
12  ;; -- Загрузка в ds 0040h
13  020A:074D  B8 0040              mov ax,40h
14  020A:0750  8E D8                mov ds,ax
15  020A:0752  33 C0                xor ax,ax           ; Zero register
16  020A:0754  8E C0                mov es,ax
17  ;; -- Инкремент счетчика реального времени по адресу DS:06CH
18  020A:0756  FF 06 006C               inc word ptr ds:[6Ch]   ;
        (0040:006C=0F9B1h)
19  020A:075A  75 04                jnz loc_1           ; Jump if not
        zero
20  ;; -- Инкремент 2 старших байтов счетчика реального времени по адре
        су DS:06CH
21  020A:075C  FF 06 006E               inc word ptr ds:[6Eh]   ;
        (0040:006E=12h)
22  ;; -- Сброс счетчика времени при наступлении нового дня:
23  ;;  0040:006E = 18h (24), 0040:006C =0B0h (176)
24  ;;  18h << 16 + B0H = 24 * 60 * 60 * c
25  ;;  c = 1573040 / 86400 = 18.2... - количество срабатываний таймера
         в секунду
26  ;;  Таким образом из выполнения условия следует, что прошли сутки
27  020A:0760           loc_1:
28  020A:0760  83 3E 006E 18            cmp word ptr ds:[6Eh],18h   ;
        (0040:006E=12h)
29  020A:0765  75 15                jne loc_2           ; Jump if not
        equal
30  020A:0767  81 3E 006C 00B0          cmp word ptr ds:[6Ch],0B0h  ;
        (0040:006C=0F9B1h)
31  020A:076D  75 0D                jne loc_2           ; Jump if not
        equal
32  ;; -- Обнуление счетчика реального времени
33  020A:076F  A3 006E              mov word ptr ds:[6Eh],ax    ;
        (0040:006E=12h)
34  020A:0772  A3 006C              mov word ptr ds:[6Ch],ax    ;
        (0040:006C=0F9B1h)
35  ;; -- Установка в DS:0070 так как прошло более 24 часов
36  020A:0775  C6 06 0070 01            mov byte ptr ds:[70h],1 ;
        (0040:0070=0)
37  ;; -- Установка 3-й бит в al
38  020A:077A  0C 08                or  al,8
```

```
020A:077C           loc_2:
;; -- Сохранение значения регистра ax
020A:077C  50                   push    ax
;; -- Декремент счетчика времени до отключения моторчика дисковода
020A:077D  FE 0E 0040               dec byte ptr ds:[40h]   ;
    (0040:0040=0D3h)
020A:0781  75 0B                jnz loc_3           ; Jump if not
    zero
;; -- Сброс флагов, отвечающих за работу моторчика дисковода
020A:0783  80 26 003F F0            and byte ptr ds:[3Fh],0F0h  ;
    (0040:003F=0)
;; -- Отправка команды на отключение моторчика дисковода
020A:0788  B0 0C                mov al,0Ch
020A:078A  BA 03F2              mov dx,3F2h
020A:078D  EE                   out dx,al           ; port 3F2h,
    dsk0 contrl output
020A:078E           loc_3:
;; -- Восстановление регистра ax
020-- A:078E  58                   pop ax
;; Проверка второго бита флага PF(Parity Flag - флаг четности)
;; DS:0314 -  адрес области данных BIOS, содержащей копию флагов
020A:078F  F7 06 0314 0004          test    word ptr ds:[314h],4
        ; (0040:0314=3200h)
020A:0795  75 0C                jnz loc_4           ; Jump if not
    zero
;; -- Сохранение младшего байта регистра FLAGS в  ah
020A:0797  9F                   lahf                ; Load ah from
    flags
;; -- Обмен значений регистров AH и AL
;; Таким образом младший байт регистра FLAGS находится в младшем ба
    йте регистра ax
020A:0798  86 E0                xchg    ah,al
;;  -- Сохранение регистра ax
020A:079A  50                   push    ax
;;  -- Косвенный вызов прерывания 1Ch
;;  В этом случае не произойдет push регистра FLAGS в стек, на его
    месте будет ax,
;;  который по выходу из 1ch будет установлен в FLAGS через iret
020A:079B  26: FF 1E 0070           call    dword ptr es:[70h]  ;
    (0000:0070=6ADh)
020A:07A0  EB 03                jmp short loc_5
                                                    ; now data
                                                       because:
                                                       after jmp/
                                                       ret
020A:07A2  90                   db  90h
;;  -- Вызов пользовательского прерывания через 1Ch
020A:07A3           loc_4:
020A:07A3  CD 1C                int 1Ch         ; Timer break (call
     each 18.2ms)
020A:07A5           loc_5:
020A:07A5  E8 0011      ;*      call    sub_1           ;*
020A:07A5  E8 11 00             db  0E8h, 11h, 00h
;;  -- Сброс контроллера прерываний
020A:07A8  B0 20                mov al,20h          ; ' '
020A:07AA  E6 20                out 20h,al          ; port 20h,
    8259-1 int command
```

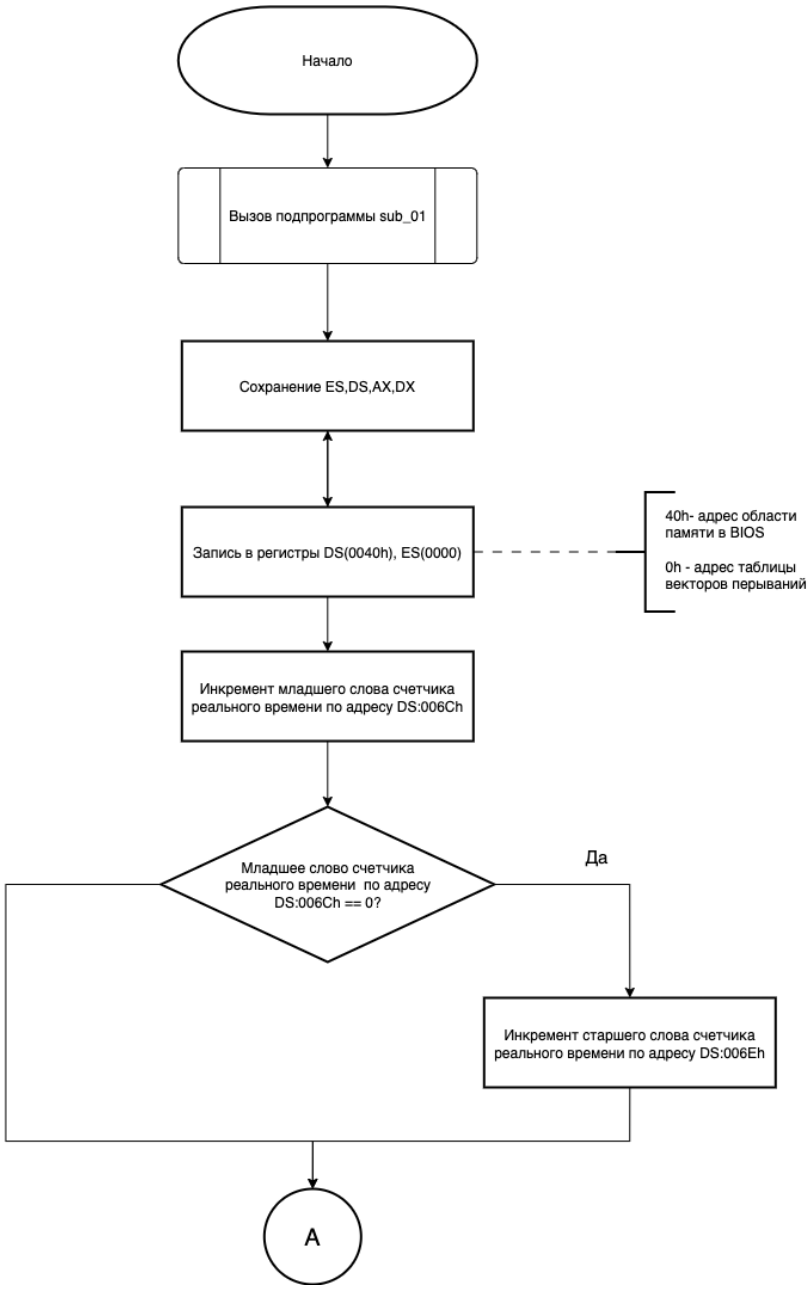
```
                                        ;  al = 20h, end of
                                         interrupt
;; -- Возврат значений регистров es,dx,ax,dx
020A:07AC  5A                   pop dx
020A:07AD  58                   pop ax
020A:07AE  1F                   pop ds
020A:07AF  07                   pop es
020A:07B0  E9 FE99              jmp $-164h
;; ...
020A:064C  1E                   push    ds
020A:064D  50                   push    ax
;; ...
020A:06AA  58                   pop ax
020A:06AB  1F                   pop ds
;; -- Возврат из прерывания
020A:06AC  CF                   iret                ; Interrupt
    return
```

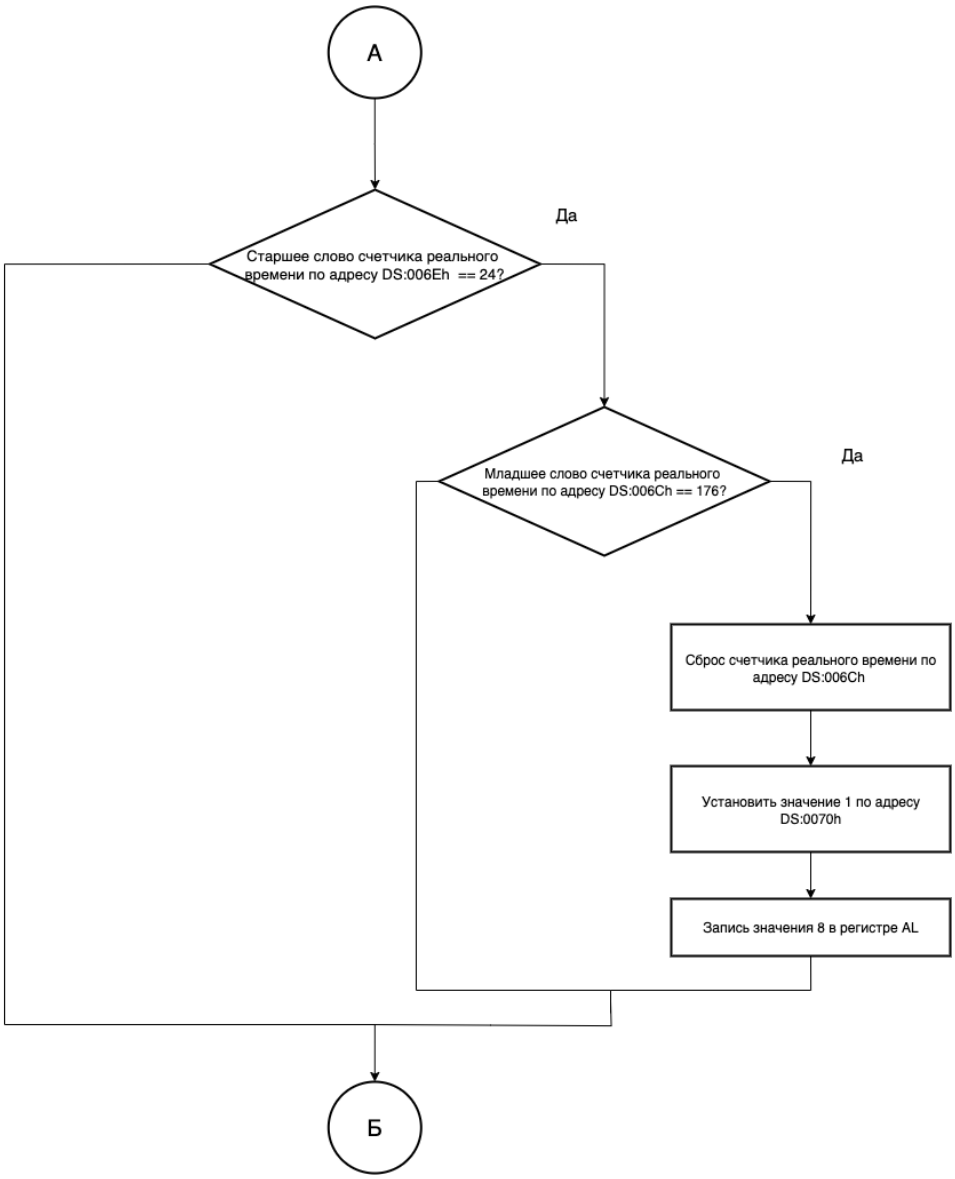
1.2 Листинг процедуры sub_1

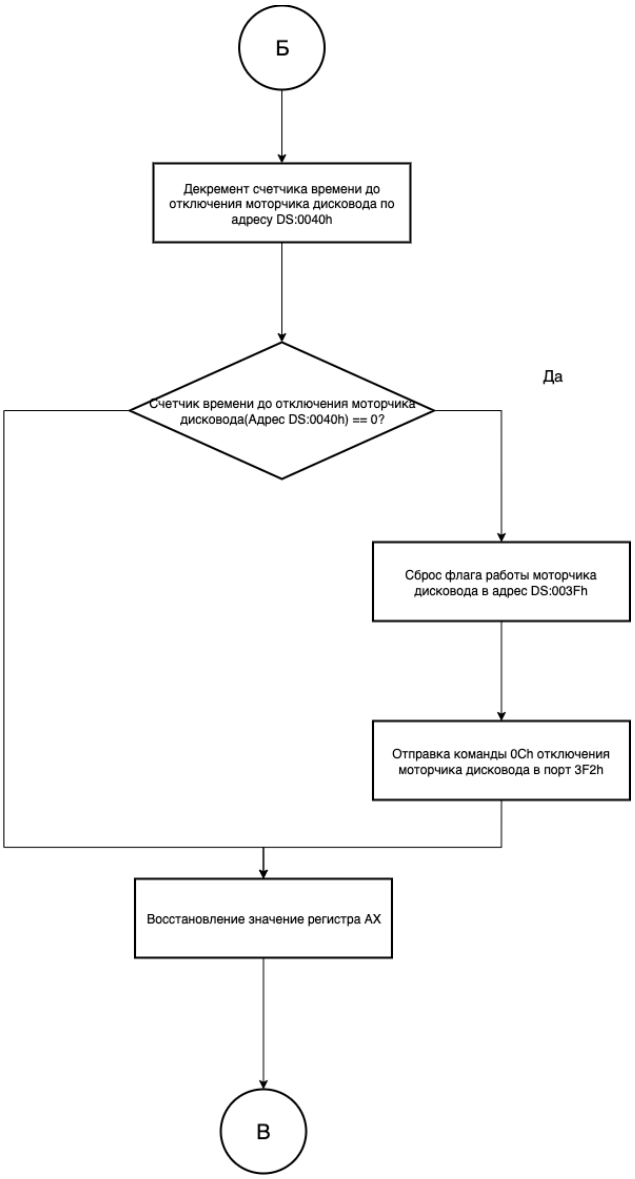
```
1  Temp.lst                Sourcer v5.10   10-Sep-25
       7:22 pm   Page 1
2
3  ;; -- Сохранение регистров ds, ax
4  020A:07B9  1E                   push    ds
5  020A:07BA  50                   push    ax
6  ;; -- Загрузка сегментного регистра dx
7  020A:07BB  B8 0040              mov ax,40h
8  020A:07BE  8E D8                mov ds,ax
9  ;; -- Сохранение младшего байта регистра FLAGS в  ah
10 020A:07C0  9F                a  lahf                ; Load ah from
       flags
11 ;; -- Проверка флага DF и старшего бита IORL по адресу DS:0314h
12 020A:07C1  F7 06 0314 2400          test    word ptr ds:[314h],2400
       h    ; (0040:0314=3200h)
13 020A:07C7  75 0C                jnz loc_2           ; Jump if not
       zero
14 ;; -- Сброс флага прерываний IF в BIOS
15 ;;    lock для того, чтобы команда была неделимой
16 020A:07C9  F0> 81 26 0314 FDFF                                lock and
        word ptr ds:[314h],0FDFFh   ; (0040:0314=3200h)
17 020A:07D0            loc_1:
18 ;; -- Загрузка ah в младший байт FLAGS
19 020A:07D0  9E                   sahf                ; Store ah into
       flags
20 ;; -- Восстановление регистров
21 020A:07D1  58                   pop ax
22 020A:07D2  1F                   pop ds
23 020A:07D3  EB 03                jmp short loc_3     ; (07D8)
24 020A:07D5            loc_2:
25 ;; -- Сброс флага прерываний IF
26 020A:07D5  FA                   cli             ; Disable
       interrupts
27 020A:07D6  EB F8                jmp short loc_1     ; (07D0)
28 020A:07D8            loc_3:
29 ;; -- Возврат из подпрограммы
30 020A:07D8  C3                   retn
```

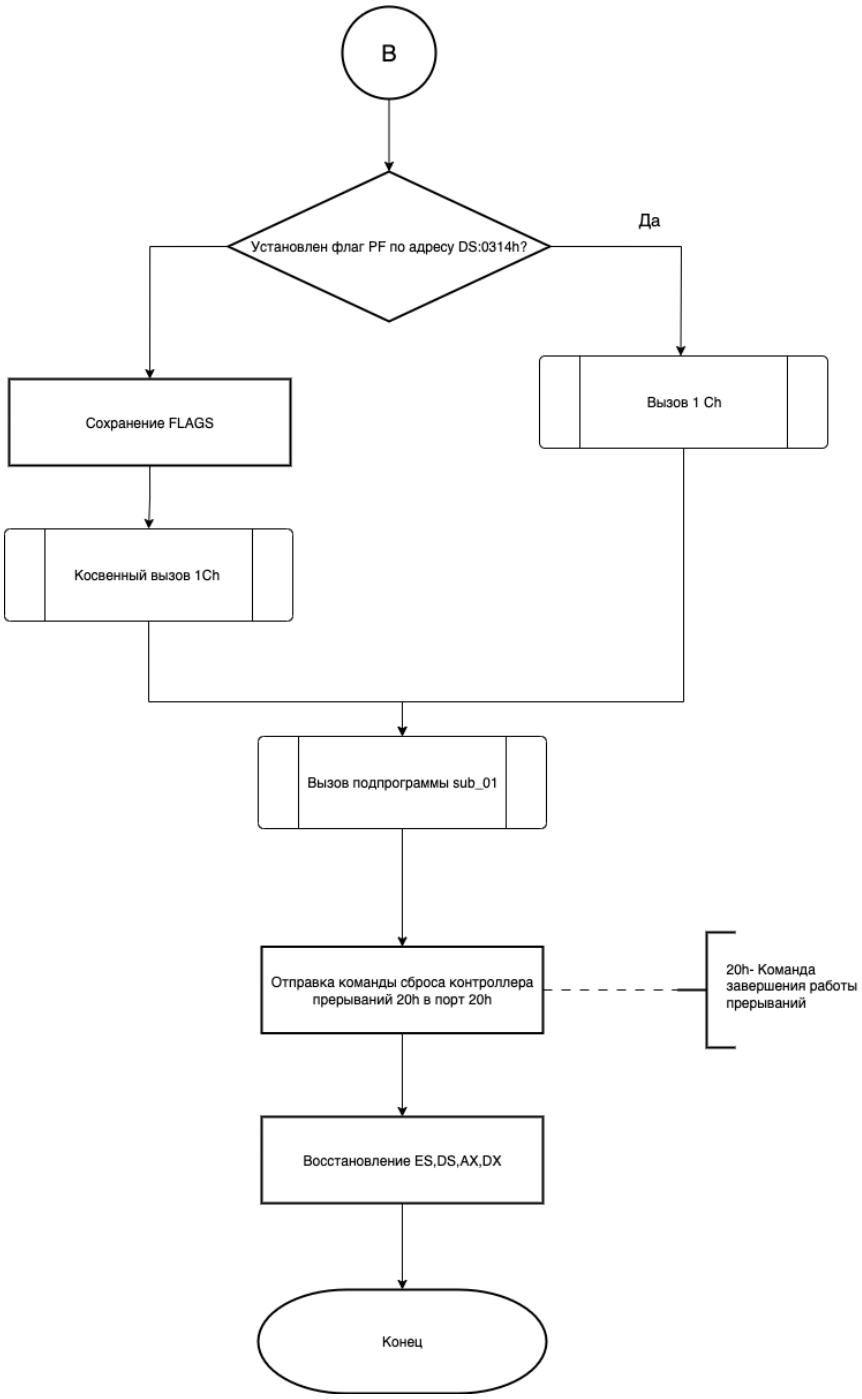
2 Схема алгоритмов

2.1 Схема алгоритма обработчика INT8h




А
Старшее слово счетчика реального времени по адресу DS:006Eh == 24?
Да
Младшее слово счетчика реального времени по адресу DS:006Ch == 176?
Да
Сброс счетчика реального времени по адресу DS:006Ch
Установить значение 1 по адресу DS:0070h
Запись значения 8 в регистре AL
Б


Б
Декремент счетчика времени до отключения моторчика дисковода по адресу DS:0040h
Счетчик времени до отключения моторчика дисковода(Адрес DS:0040h) == 0?
Да
Сброс флага работы моторчика дисковода в адрес DS:003Fh
Отправка команды 0Ch отключения моторчика дисковода в порт 3F2h
Восстановление значение регистра AX
В


B
Установлен флаг PF по адресу DS:0314h?
Да
Сохранение FLAGS
Вызов 1 Ch
Косвенный вызов 1Ch
Вызов подпрограммы sub_01
Отправка команды сброса контроллера прерываний 20h в порт 20h
20h- Команда завершения работы прерываний
Восстановление ES,DS,AX,DX
Конец

2.2 Схема алгоритма процедуры sub_1