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»

Лабораторная работа №1
по дисциплине "Операционные системы"

Тема Дизассемблирование INT 8h

Студент Тузов Даниил Александрович

Группа ИУ7-52Б

Преподаватель Рязанова Наталья Юрьевна

Москва, 2024 г.

1 Дизассемблированные коды

1.1 Дизассемблированный код обработчика прерывания int8h

```
            Temp.lst                Sourcer v5.10   18-Sep-24  12:41 am   Page 1

; Вызов сабрутины
020C:0746  E8 0070              call    sub_1           ; (07B9)
020C:0746  E8 70 00             db  0E8h, 70h, 00h
; Сохранение регистров
020C:0749  06                   push    es
020C:074A  1E                   push    ds
020C:074B  50                   push    ax
020C:074C  52                   push    dx
; Записать в DS - 40h
020C:074D  B8 0040              mov ax,40h
020C:0750  8E D8                mov ds,ax
; Записать в ES - 00h
020C:0752  33 C0                xor ax,ax           ; Zero register
020C:0754  8E C0                mov es,ax
; Инкремент младшего слова счетчика тиков
020C:0756  FF 06 006C               inc word ptr ds:[6Ch]   ; (0040:006C=0B1F0h)
020C:075A  75 04                jnz loc_1           ; Jump if not zero
; Инкремент старшего слова тиков, если обнулилось младшее
020C:075C  FF 06 006E               inc word ptr ds:[6Eh]   ; (0040:006E=0)
020C:0760           loc_1:
; Если старшее слово равно 24 и младшее равно 176, значит прошел день и надо сбросить счетчики
020C:0760  83 3E 006E 18            cmp word ptr ds:[6Eh],18h   ; (0040:006E=0)
020C:0765  75 15                jne loc_2           ; Jump if not equal
020C:0767  81 3E 006C 00B0          cmp word ptr ds:[6Ch],0B0h  ; (0040:006C=0B1F0h)
020C:076D  75 0D                jne loc_2           ; Jump if not equal
; Сброс младшего слова
020C:076F  A3 006E              mov word ptr ds:[6Eh],ax    ; (0040:006E=0)
; Сброс старшего слова
020C:0772  A3 006C              mov word ptr ds:[6Ch],ax    ; (0040:006C=0B1F0h)
; Занесение значения 1 в ds:[70h]
020C:0775  C6 06 0070 01            mov byte ptr ds:[70h],1 ; (0040:0070=0)
; Установка 3-его бита в al
020C:077A  0C 08                or  al,8
020C:077C           loc_2:
020C:077C  50                   push    ax
;Декремент счетчика времени до отключения моторчика дисковода
020C:077D  FE 0E 0040               dec byte ptr ds:[40h]   ; (0040:0040=94h)
020C:0781  75 0B                jnz loc_3           ; Jump if not zero
; Если счетчик обнулился, сбрасывается флаг работы моторчика
020C:0783  80 26 003F F0            and byte ptr ds:[3Fh],0F0h  ; (0040:003F=0)
;Отправка команды 0Ch отключения моторчика дисковода на порт 3F2h
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
020C:078E           loc_3:
020C:078E  58                   pop ax
; Проверка флага четности
020C:078F  F7 06 0314 0004          test    word ptr ds:[314h],4    ; (0040:0314=3200h)
020C:0795  75 0C                jnz loc_4           ; Jump if not zero
; Загрузка младшего байта регистра флагов в ah
020C:0797  9F                   lahf                ; Load ah from flags
020C:0798  86 E0                xchg    ah,al
020C:079A  50                   push    ax
; Косвенный вызов прерывания 1Ch
020C:079B  26: FF 1E 0070           call    dword ptr es:[70h]  ; (0000:0070=6ADh)
020C:07A0  EB 03                jmp short loc_5     ; (07A5)
020C:07A2  90                   nop
020C:07A3           loc_4:
; Вызов прерывания 1Ch
020C:07A3  CD 1C                int 1Ch         ; Timer break (call each 18.2ms)
020C:07A5           loc_5:
; Вызов сабрутины
020C:07A5  E8 0011              call    sub_1           ; (07B9)
; Сброс контроллера прерываний (разрешаются прерывания с более низким приоритетом)
```

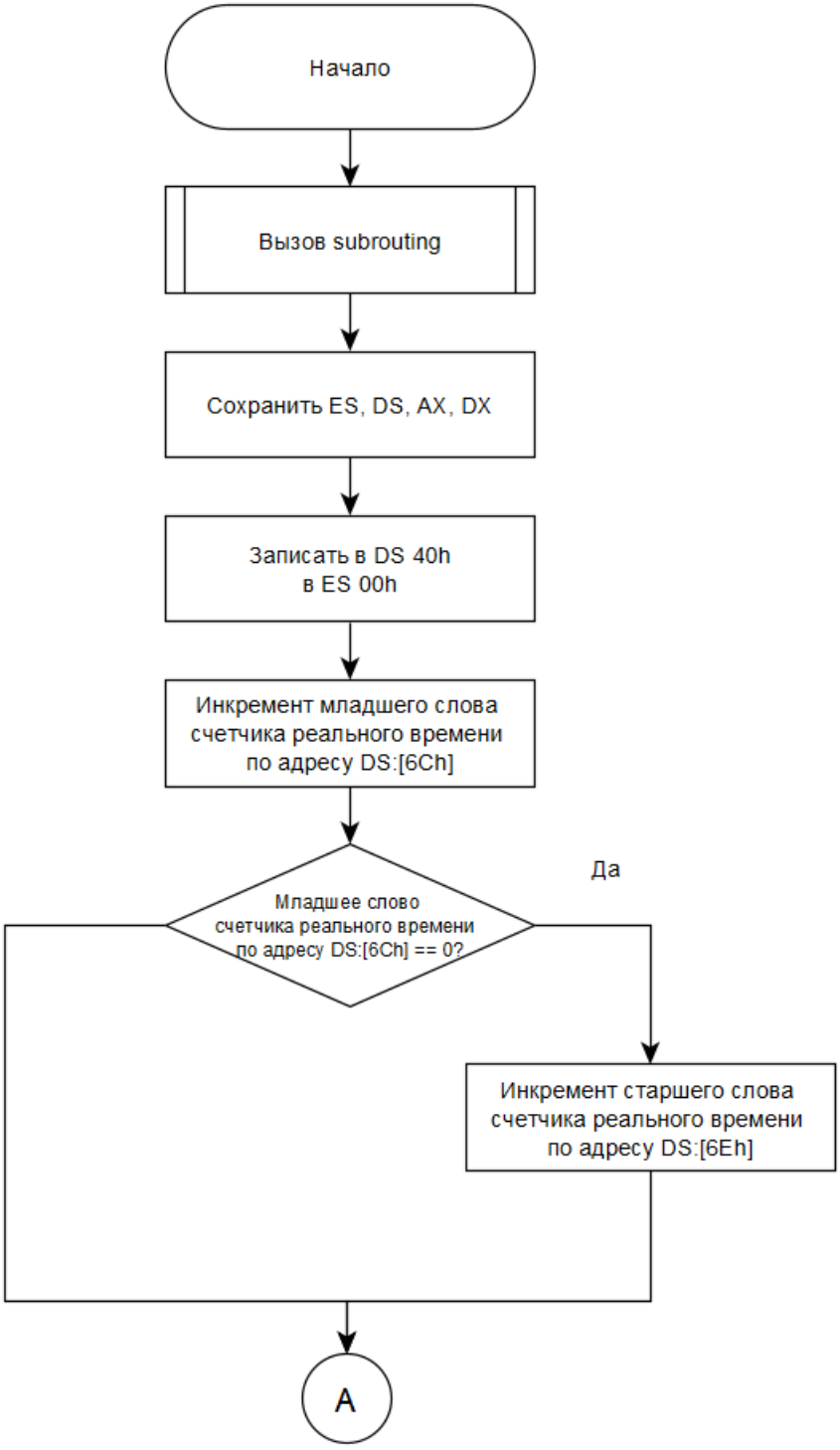
```
020C:07A8  B0 20                mov al,20h          ; ' '
020C:07AA  E6 20                out 20h,al          ; port 20h, 8259-1 int command
                                        ;  al = 20h, end of interrupt
; Восстановление регистров
020C:07AC  5A                   pop dx
020C:07AD  58                   pop ax
020C:07AE  1F                   pop ds
020C:07AF  07                   pop es
020C:07B0  E9 FE99              jmp $-164h
; ...
020C:06AC CF                    itret           ; Возврат из прерывания
```

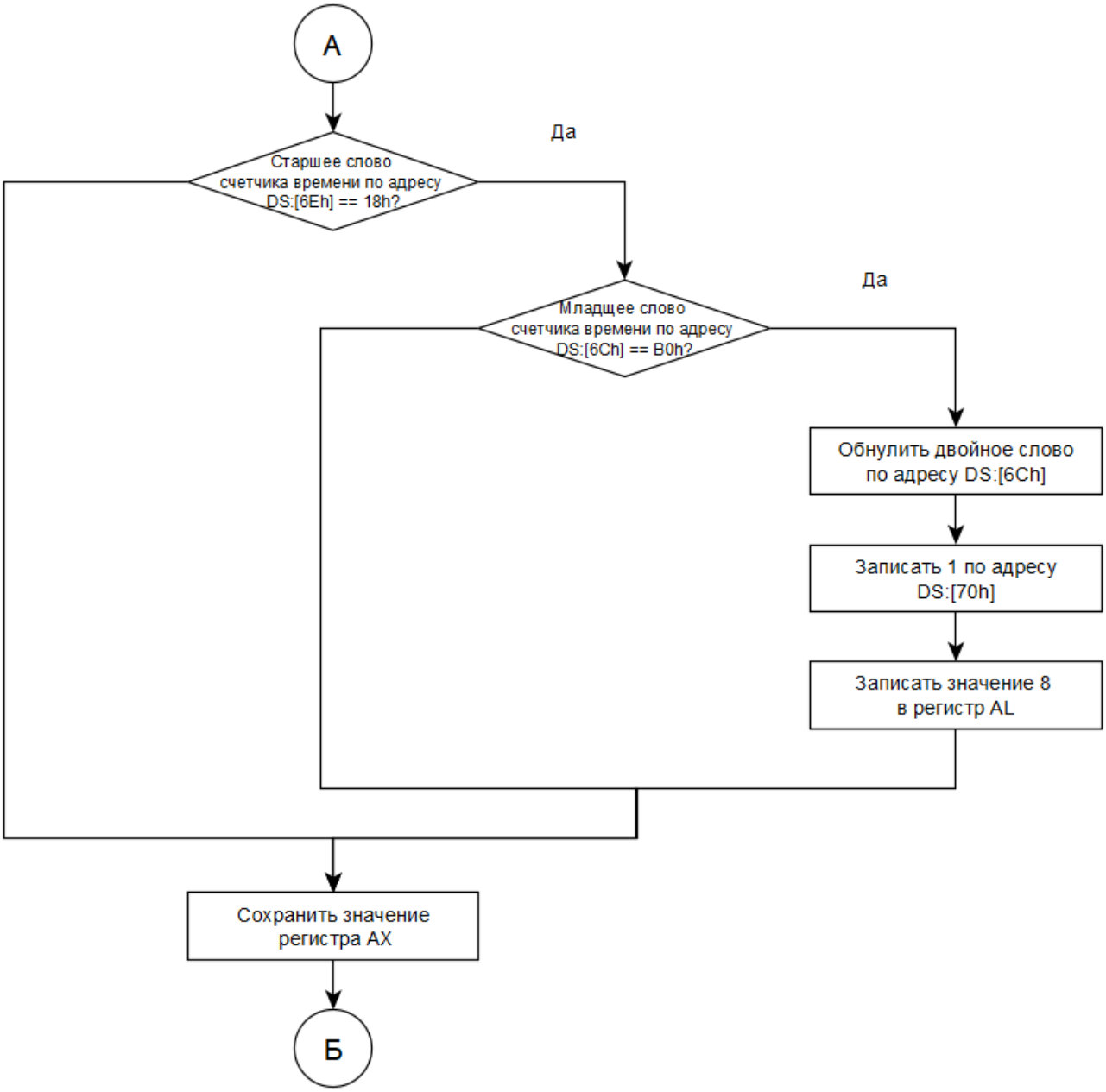
1.2 Дизассемблированный код subrouting

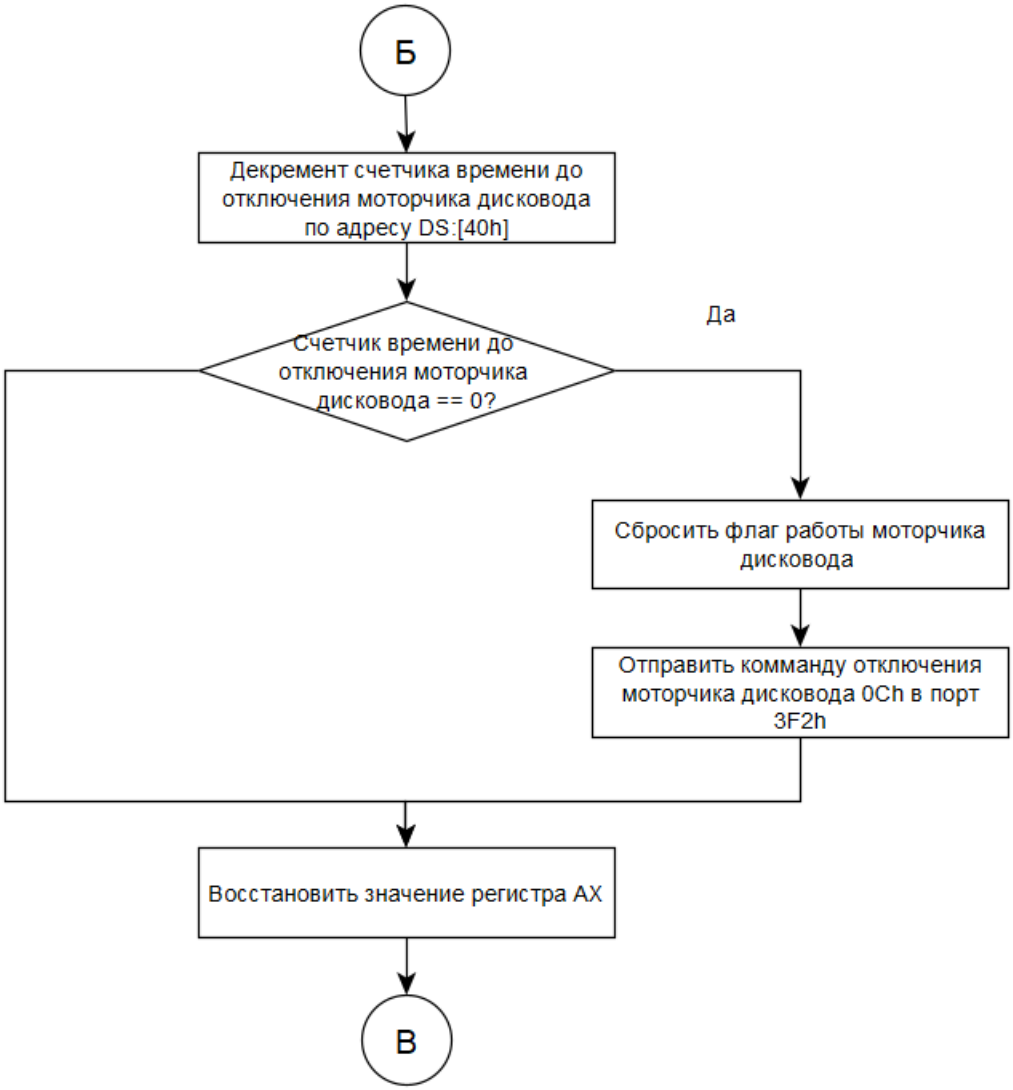
```
                sub_1       proc    near
; Сохранение значений регистров
020C:07B9  1E                   push    ds
020C:07BA  50                   push    ax
; Записать в DS - 40h
020C:07BB  B8 0040              mov ax,40h
020C:07BE  8E D8                mov ds,ax
; Загрузка младшего байта регистра флагов в ah
020C:07C0  9F                   lahf                ; Load ah from flags
; Проверка флага DF и старшего бита флага IOPL
020C:07C1  F7 06 0314 2400          test    word ptr ds:[314h],2400h    ; (0040:0314=3200h)
020C:07C7  75 0C                jnz loc_7           ; Jump if not zero
; Сброс флага прерываний IF
020C:07C9  F0> 81 26 0314 FDFF                              lock and word ptr ds:[314h],0FDFFh   ;
    (0040:0314=3200h)
020C:07D0           loc_6:
; Загрузка из ah младшего байта регистра флагов
020C:07D0  9E                   sahf                ; Store ah into flags
; Восстановление регистров
020C:07D1  58                   pop ax
020C:07D2  1F                   pop ds
020C:07D3  EB 03                jmp short loc_8     ; (07D8)
020C:07D5           loc_7:
; Сброс флага прерываний IF
020C:07D5  FA                   cli             ; Disable interrupts
020C:07D6  EB F8                jmp short loc_6     ; (07D0)
020C:07D8           loc_8:
020C:07D8  C3                   retn
                sub_1       endp
```

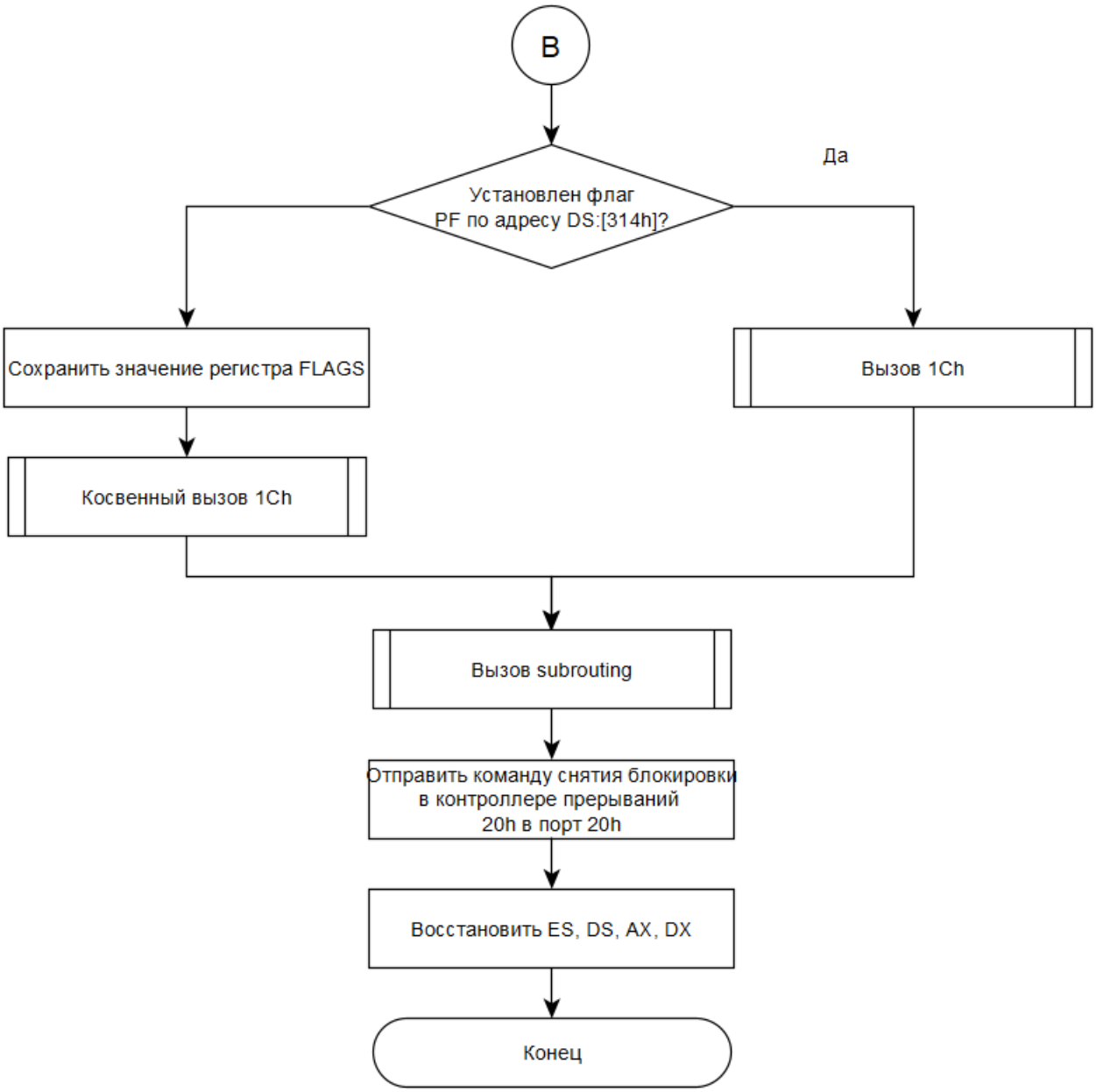
2 Схемы алгоритмов

2.1 Схема алгоритма обработчика прерывания int8h




А
Старшее слово
счетчика времени по адресу
DS:[6Eh] == 18h?
Да
Младщее слово
счетчика времени по адресу
DS:[6Ch] == B0h?
Да
Обнулить двойное слово
по адресу DS:[6Ch]
Записать 1 по адресу
DS:[70h]
Записать значение 8
в регистр AL
Сохранить значение
регистра AX
Б


Б
Декремент счетчика времени до отключения моторчика дисковода по адресу DS:[40h]
Счетчик времени до отключения моторчика дисковода == 0?
Да
Сбросить флаг работы моторчика дисковода
Отправить комманду отключения моторчика дисковода 0Ch в порт 3F2h
Восстановить значение регистра AX
В


B
Установлен флаг
PF по адресу DS:[314h]?
Да
Сохранить значение регистра FLAGS
Вызов 1Ch
Косвенный вызов 1Ch
Вызов subrouting
Отправить команду снятия блокировки
в контроллере прерываний
20h в порт 20h
Восстановить ES, DS, AX, DX
Конец

2.2 Схема алгоритма subrouting