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 Артемьев И. О.

Группа ИУ7-53Б

Преподаватель Рязанова Н. Ю.

Москва

2021 г.

1 Полученный дизассемблированный код

1.1 Листинг INT8h

```
    020A:0746     ;*        call     sub_1              ; (07B9)
020A:0746               db   0E8h, 70h, 00h

; сохранение регистров
020A:0749               push     es
020A:074A               push     ds
020A:074B               push     ax
020A:074C               push     dx
020A:074D               mov ax,40h
020A:0750               mov ds,ax
020A:0752               xor  ax,ax             ; Zero register
020A:0754               mov es,ax

; инкремент счетчика таймера реального времени
020A:0756               inc word ptr ds:[6Ch]
; (0040:006C=2E56h), по этому адресу располагается счетчик реального времени
020A:075A               jnz  loc_1             ; Jump if not zero
;если значение  в 0040:006C равно нулю, то инкрементируются старшие 2 байта
020A:075C               inc word ptr ds:[6Eh]    ; (0040:006E=2)

; сброс счетчика таймера реального времени, если наступили новые сутки
020A:0760     loc_1:
020A:0760               cmp word ptr ds:[6Eh],18h    ; (0040:006E=2)
020A:0765               jne  loc_2             ; Jump if not equal
020A:0767               cmp word ptr ds:[6Ch],0B0h   ; (0040:006C=2E56h)
020A:076D               jne  loc_2             ; Jump if not equal
; прошло более 24 часов с момента запуска таймера, обнуление счетчика
020A:076F               mov word ptr ds:[6Eh],ax     ; (0040:006E=2)
020A:0772               mov word ptr ds:[6Ch],ax     ; (0040:006C=2E56h)
020A:0775               mov byte ptr ds:[70h],1 ; (0040:0070=0)
; в 0040:0070 хранится переполнения таймера (переход через 24 часа)
020A:077A               or   al,8



; декремент значения времени до выключения моторчика дисковода
020A:077C     loc_2:
020A:077C               push     ax
020A:077D               dec byte ptr ds:[40h]    ; (0040:0040=5Bh)
; ячейка с адресом 0040:0040 содержит время, оставшееся до выключения двигателя
020A:0781               jnz  loc_3             ; Jump if not zero
;  посыл команды на отключение моторчика дисковода
020A:0783               and byte ptr ds:[3Fh],0F0h   ; (0040:003F=0)
; в 0040:003F хранится состояние моторчика дисковода
020A:0788               mov al,0Ch
020A:078A               mov dx,3F2h
020A:078D               out  dx,al             ; port 3F2h, dsko contrl output

;  проверка на возможность вызова маскируемых прерываний
020A:078E     loc_3:
020A:078E               pop ax
020A:078F               test     word ptr ds:[314h],4     ; (0040:0314=3200h)
; ячейка с адресом 0040:0314 содержит информацию о значениях флагов (Проверка parity  flag)
020A:0795               jnz  loc_4             ; Jump if not zero
020A:0797               lahf                   ; Load ah from flags
; загрузка младшего байта регистра флагов в AH
; обмен ah и al
020A:0798               xchg     ah,al
020A:079A               push     ax
; косвенный вызов пользовательского прерывания
; Вызов 1Ch с помощью адреса в таблице векторов прерывания
; При вызове через int произойдет сохранения регистра флагов в стек,
; а в случае вызова через call на его месте будет лежать сохраненный до ax
; который по выходе из 1Ch будет установлен в флаги через iret
020A:079B               call     dword ptr es:[70h]   ; (0000:0070=6ADh)
020A:07A0               jmp short loc_5       ; (07A5)
020A:07A2               nop

;  вызов пользовательского прерывания
020A:07A3     loc_4:
020A:07A3               int  1Ch          ; Timer break (call each 18.2ms)

```

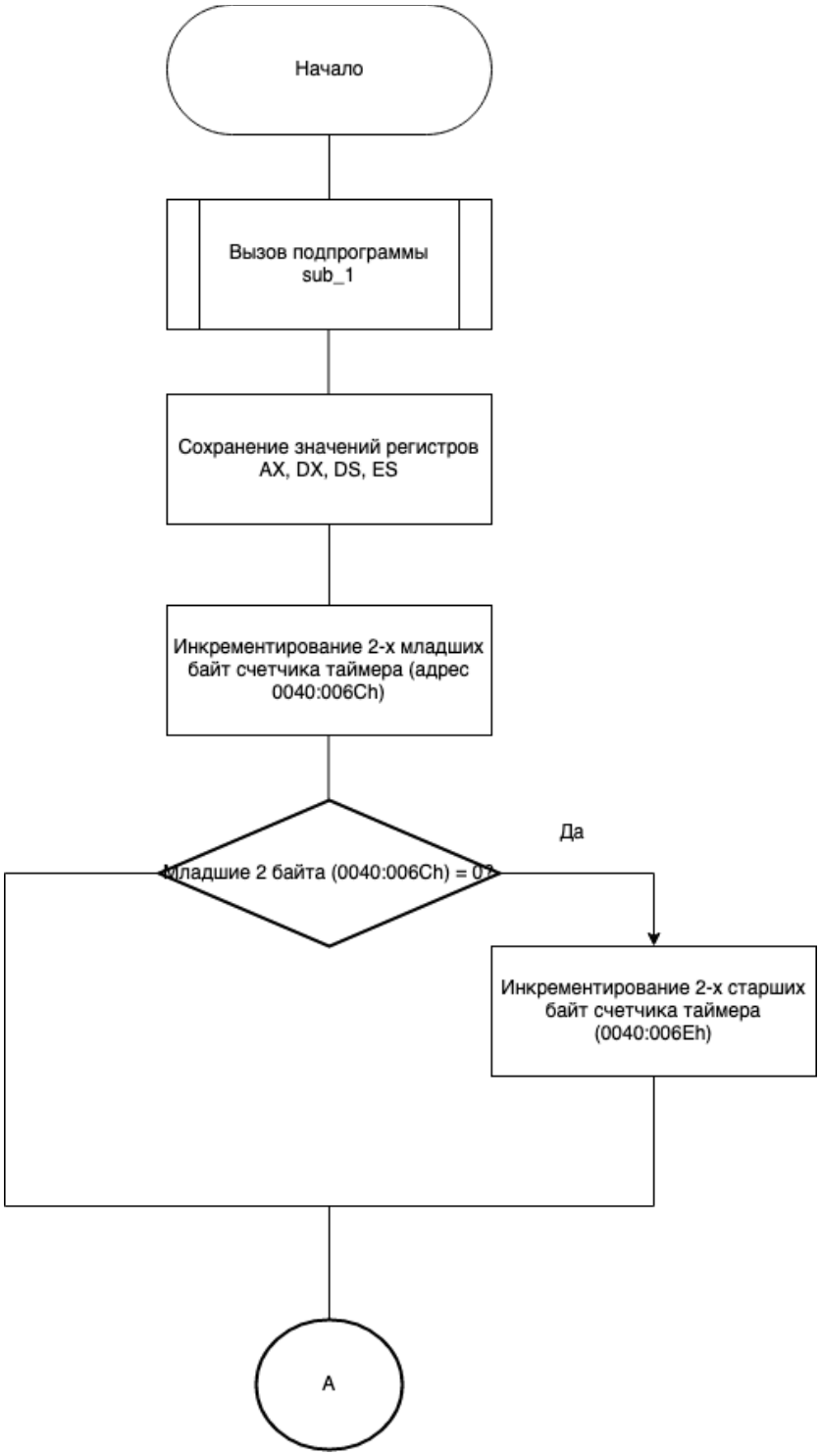
```
73 ; сброс контроллера прерываний
74 020A:07A5      loc_5:
75 020A:07A5                call      sub_1               ; (07B9)
76 020A:07A8                mov al,20h                    ; ' '
77 020A:07AA                out 20h,al                    ; port 20h, 8259-1 int command
78                                                        ;   al = 20h, end of interrupt
79 ; восстановление регистров
80 020A:07AC                pop   dx
81 020A:07AD                pop   ax
82 020A:07AE                pop   ds
83 020A:07AF                pop   es
84 ; переход по метке для завершения работы прерывания
85 020A:07B0                jmp $-164h
86 020A:07B3                db    0C4h
87                                                        ;* No entry point to code
88 020A:07B4                les cx,dword ptr ds:[93E9h] ; (0000:93E9=5A14h) Load 32 bit ptr
89 020A:07B8                db    0FEh
```

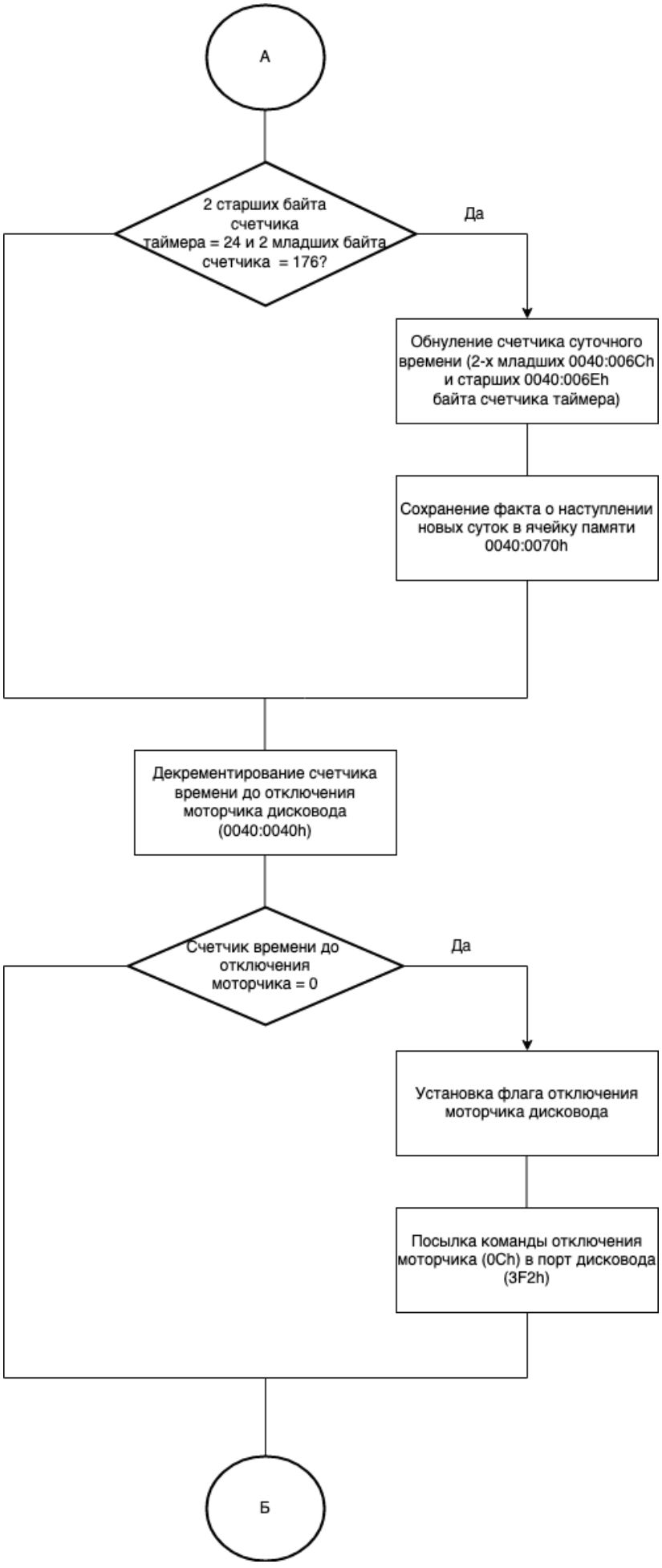
1.2 Листинг процедуры sub_1

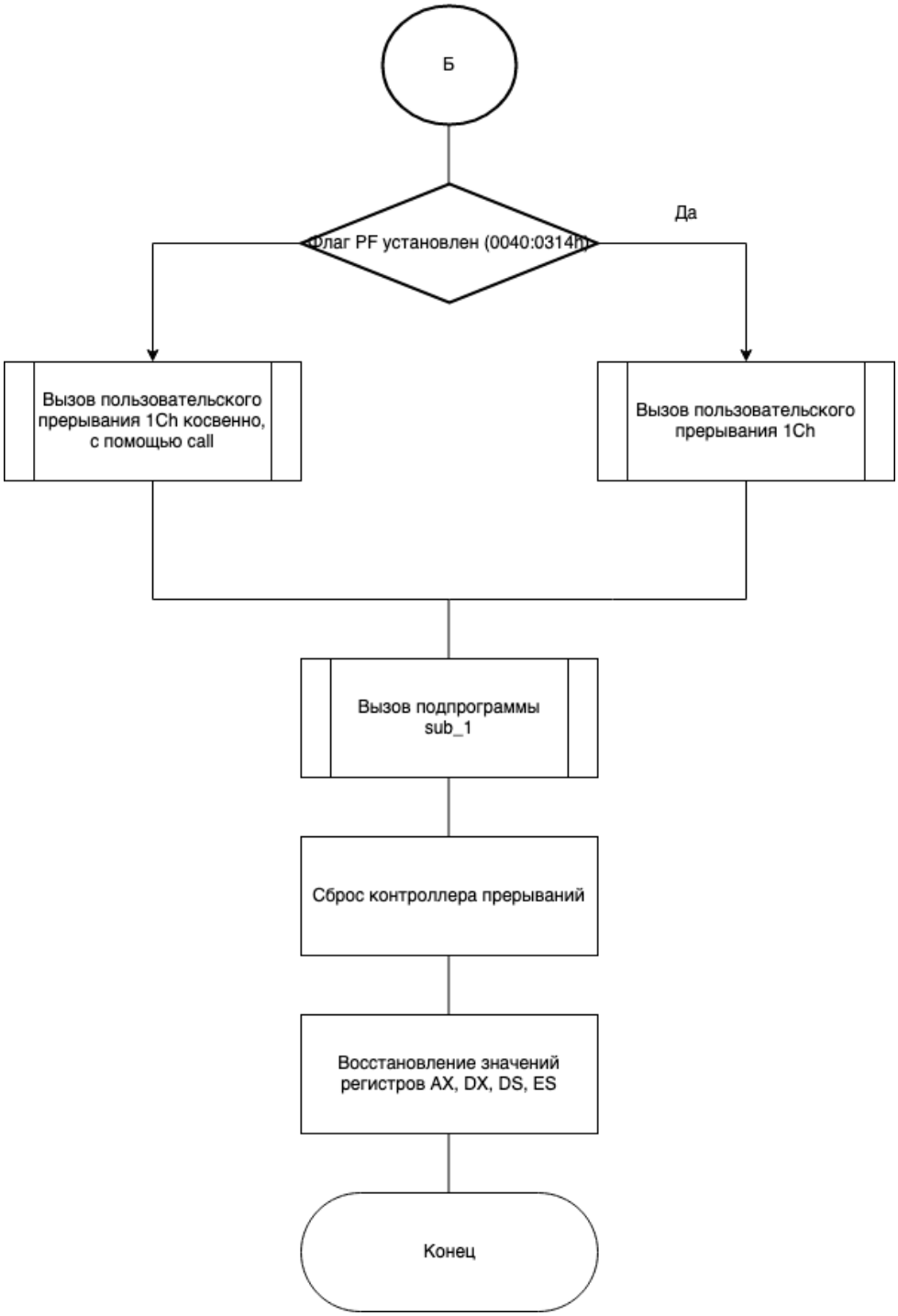
```
1   sub_1       proc    near
2   ; сохранение регистров и загрузка регистра флагов
3   020A:07B9           push    ds
4   020A:07BA           push    ax
5   020A:07BB           mov ax,40h
6   020A:07BE           mov ds, ax
7   020A:07C0           lahf                    ; Load ah from flags
8
9   ; проверка на возможность вызова маскируемых прерываний
10  020A:07C1           test    word ptr ds:[314h],2400h;(0040:0314=3200h)
11  020A:07C7           jnz loc_7               ;Jump if not zero
12  ; Сброс IEF (9 бит) lock для того, чтобы команда была неделимой
13  020A:07C9                       lock and word ptr ds:[314h],0FDFFh; (0040:0314=3200h)
14  ; установка флага IF в ноль
15
16  ;сохранение флагов и восстановление регистров
17  020A:07D0   loc_6:
18  020A:07D0           sahf                    ; Store ah into flags
19  020A:07D1           pop ax
20  020A:07D2           pop ds
21  020A:07D3           jmp short loc_8         ; (07D8)
22
23
24  ;запрет на вызов маскируемых прерываний
25  020A:07D5   loc_7:
26  020A:07D5           cli             ; Disable interrupts
27  ; сбрасывает interrupt flag (IF). Когда этот флаг сброшен процессор игнорирует все
28  ; прерывания (кроме NMI) от внешних устройств.
29  020A:07D6           jmp short loc_6         ;(07D0)
30
31  ;завершение процедуры
32  020A:07D8   loc_8:
33  020A:07D8           retn
34          sub_1       endp
```

2 Схема алгоритмов

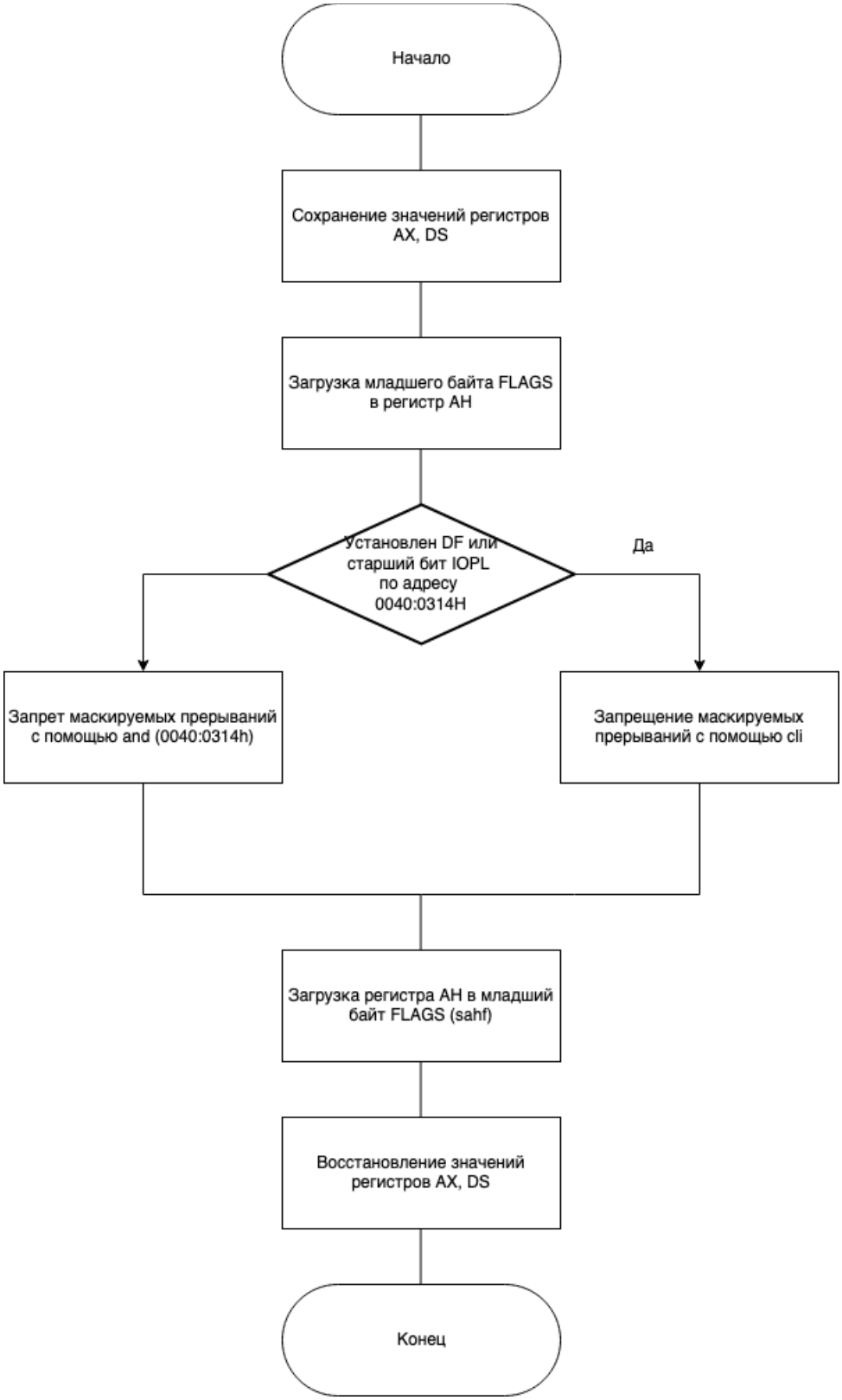
2.1 Схема алгоритма обработчика INT8h




A
2 старших байта счетчика таймера = 24 и 2 младших байта счетчика = 176?
Да
Обнуление счетчика суточного времени (2-х младших 0040:006Ch и старших 0040:006Eh байта счетчика таймера)
Сохранение факта о наступлении новых суток в ячейку памяти 0040:0070h
Декрементирование счетчика времени до отключения моторчика дисковода (0040:0040h)
Счетчик времени до отключения моторчика = 0
Да
Установка флага отключения моторчика дисковода
Посылка команды отключения моторчика (0Ch) в порт дисковода (3F2h)
Б


Б
Флаг PF установлен (0040:0314h)
Да
Вызов пользовательского прерывания 1Ch косвенно, с помощью call
Вызов пользовательского прерывания 1Ch
Вызов подпрограммы sub_1
Сброс контроллера прерываний
Восстановление значений регистров AX, DX, DS, ES
Конец

2.2 Схема алгоритма процедуры sub_1



Вывод

1) Увеличивает значение четырехбайтной переменной в области данных BIOS по адресу 0000:046Ch. По этому адресу располагается счетчик тиков таймера. При переполнении счетчика, в ячейку 0000:0470h заносится 1 (прошло 24 часа с момента запуска таймера).

2) Контролирует работу двигателя моторчика дисковода. Если после последнего обращения к дисководу прошло более 2 секунд обработчик прерывания выключает двигатель. В ячейке по адресу 0000:0440h содержится оставшееся до выключения двигателя время. Это время постоянно уменьшается обработчиком прерывания таймера. Когда оно становится равным 0, двигатель моторчика дисковода отключается.

3) Вызывает пользовательское прерывание 1Ch. Его обработчик состоит только из команды IRET. Во время выполнения INT 1Ch все аппаратные прерывания запрещены.