|  |  |
| --- | --- |
|  | **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 (часть 1)**

**По курсу «Операционные Системы»**

**Тема** \_\_Дизассемблирование INT 8h\_\_

**Студент** \_\_\_Малышев И. А.\_\_\_

**Группа** \_\_\_ИУ7-51Б\_\_\_

**Оценка (баллы)** \_\_\_\_\_\_\_\_\_\_\_

**Преподаватель** \_\_Рязанова Н. Ю.\_\_

*2021 г.*

1. **Полученный ассемблерный код прерывания int 8h с адресами команд и комментариями**

; Вход в прерывание, вызов подпрограммы sub\_1

020A:0746 E8 0070 call sub\_1 ; (07B9)

; Сохранение аппаратного контекста (регистров **ES**, **DS**, **AX**, **DX**)

020A:0749 06 push es

020A:074A 1E push ds

020A:074B 50 push ax

020A:074C 52 push dx

; Установка сегментных регистров **DS**, **ES**

020A:074D B8 0040 mov ax,40h

020A:0750 8E D8 mov ds,ax

020A:0752 33 C0 xor ax,ax ; Zero register

020A:0754 8E C0 mov es,ax

; Инкремент счётчика суточного времени. Инкремент счётчика тиков (2 младших байт счётчика суточного времени)

020A:0756 FF 06 006C inc word ptr ds:[6Ch] ;(0040:006C=0E83Dh)

020A:075A 75 04 jnz loc\_1 ; Jump if not zero

; Если счётчик тиков равен нулю, тогда инкремент счётчика часов (2 старших байт счётчика суточного времени)

020A:075C FF 06 006E inc word ptr ds:[6Eh] ; (0040:006E=0Dh)

; Проверка прохождения 24 часов: 0040:006Eh = 18h и 0040:6Ch = B0h

020A:0760 loc\_1:

020A:0760 83 3E 006E 18 cmp word ptr ds:[6Eh],18h ;(0040:006E=0Dh)

020A:0765 75 15 jne loc\_2 ; Jump if not equal

020A:0767 81 3E 006C 00B0 cmp word ptr ds:[6Ch],0B0h ;(0040:006C=0E83Dh)

020A:076D 75 0D jne loc\_2 ; Jump if not equal

; Сброс счётчика суточного времени, если прошло 24 часа

020A:076F A3 006E mov word ptr ds:[6Eh],ax ; (0040:006E=0Dh)

020A:0772 A3 006C mov word ptr ds:[6Ch],ax ; (0040:006C=0E83Dh)

; По прошествии 24 часов установка единицы в 0040:0070h

020A:0775 C6 06 0070 01 mov byte ptr ds:[70h],1 ; (0040:0070=0)

; Установка третьего бита регистра **AX**

020A:077A 0C 08 or al,8

; Сохранение регистра **AX**

020A:077C loc\_2:

020A:077C 50 push ax

; Декремент счётчика времени до отключения двигателей НГМД

020A:077D FE 0E 0040 dec byte ptr ds:[40h] ; (0040:0040=0E5h)

020A:0781 75 0B jnz loc\_3 ; Jump if not zero

; По истечении времени отключение всех двигателей НГМД

020A:0783 80 26 003F F0 and byte ptr ds:[3Fh],0F0h ; (0040:003F=0)

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

; Восстановление регистра **AX**

020A:078E loc\_3:

020A:078E 58 pop ax

; Проверка флага **PF**

020A:078F F7 06 0314 0004 test word ptr ds:[314h],4;(0040:0314=3200h)

; Если **PF** = 1, то вызов прерывание 1Ch через команду **INT**, иначе – вызов по адресу в таблице векторов

020A:0795 75 0C jnz loc\_4 ; Jump if not zero

020A:0797 9F lahf ; Load ah from flags

020A:0798 86 E0 xchg ah,al

020A:079A 50 push ax

020A:079B 26: FF 1E 0070 call dword ptr es:[70h]; (0000:0070=6ADh)

020A:07A0 EB 03 jmp short loc\_5 ; (07A5)

020A:07A2 90 nop

020A:07A3 loc\_4:

020A:07A3 CD 1C int 1Ch ; Timer break (call each 18.2ms)

; Вызов подпрограммы sub\_1 и сброс контроллера прерываний НГМД

020A:07A5 loc\_5:

020A:07A5 E8 0011 call sub\_1 ; (07B9)

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

; Восстановление аппаратного контекста (регистров **ES**, **DS**, **AX**, **DX**)

020A:07AC 5A pop dx

020A:07AD 58 pop ax

020A:07AE 1F pop ds

020A:07AF 07 pop es

; Переход к команде **IRET**

020A:07B0 E9 FE99 jmp $-164h ; 07B0h - 164h = 064Ch

; ...

020A:064C 1E push ds

020A:064D 50 push ax

020A:064E B8 0040 mov ax,40h

020A:0651 8E D8 mov ds,ax

020A:0653 F7 06 0314 2400 test word ptr ds:[314h],2400h; (0040:0314=3200h)

020A:0659 75 4F jnz loc\_9 ; Jump if not zero

...

020A:06AA loc\_9:

020A:06AA 58 pop ax

020A:06AB 1F pop ds

; Выход из прерывания

020A:06AC CF iret ; Interrupt return

1. **Полученный ассемблерный код подпрограммы sub\_1 с адресами команд и комментариями**

; Вход в подпрограмму. Сохранение регистров **DS**, **AX**

sub\_1 proc near

020A:07B9 1E push ds

020A:07BA 50 push ax

; Настройка сегментного регистра: **DS** = 0040h

020A:07BB B8 0040 mov ax,40h

020A:07BE 8E D8 mov ds,ax

; Загрузка младшего байта регистра флагов в регистр **AH**

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

; Проверка флага **DF** и старшего бита **IOPL**

020A:07C1 F7 06 0314 2400 test word ptr ds:[314h],2400h ; (0040:0314=3200h)

; Если оба флага не установлены, то блокировка системной шины и сброс флага **IF**

020A:07C7 75 0C jnz loc\_7 ; Jump if not zero

020A:07C9 F0> 81 26 0314 FDFF lock and word ptr ds:[314h],0FDFFh ; (0040:0314=3200h)

; Восстановление младшего байта регистра флагов из **AH**

020A:07D0 loc\_6:

020A:07D0 9E sahf ; Store ah into flags

; Восстановление регистров **AX**, **DS**

020A:07D1 58 pop ax

020A:07D2 1F pop ds

020A:07D3 EB 03 jmp short loc\_8 ; (07D8)

; Запрет маскируемых прерываний

020A:07D5 loc\_7:

020A:07D5 FA cli ; Disable interrupts

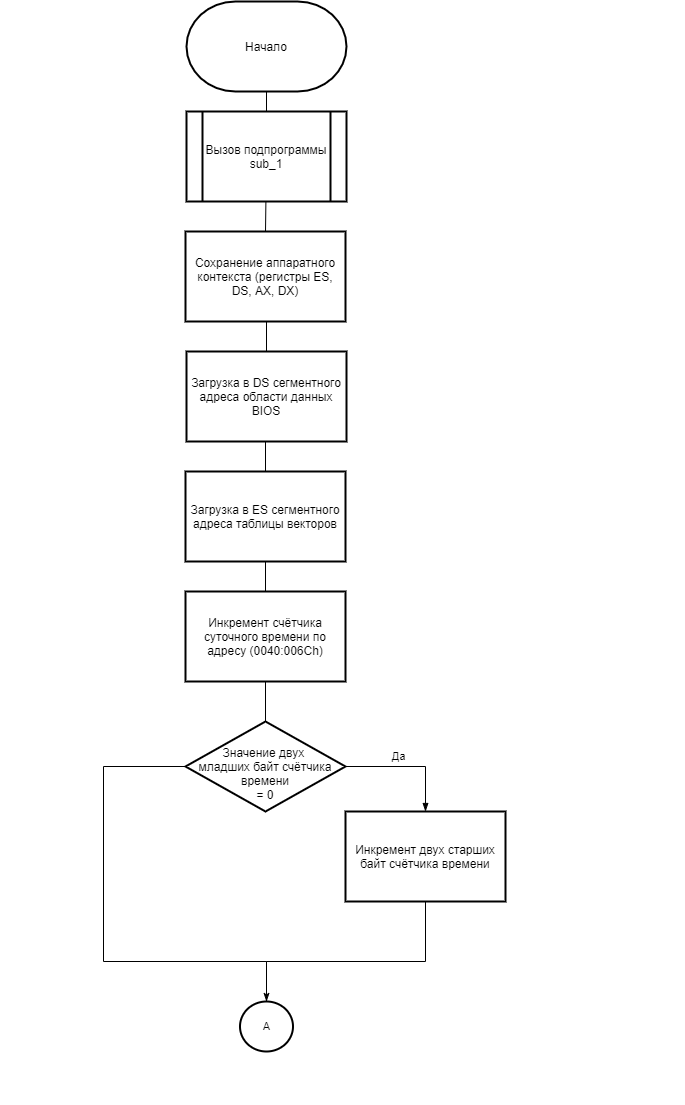
020A:07D6 EB F8 jmp short loc\_6 ; (07D0)

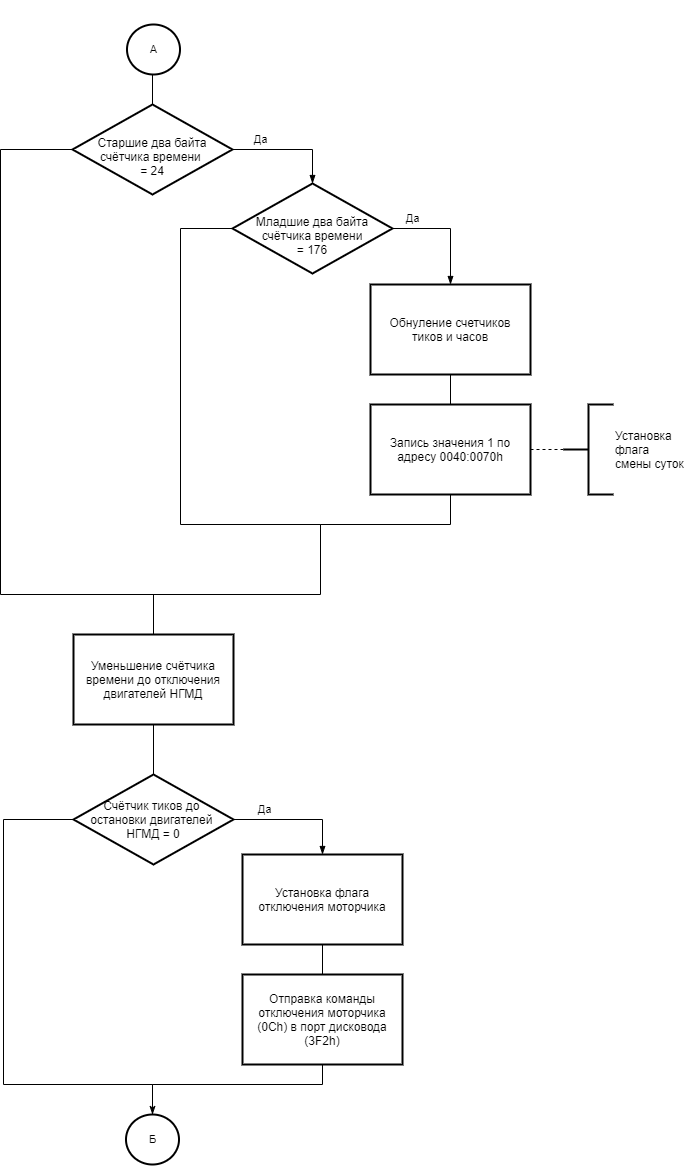
; Выход из подпрограммы

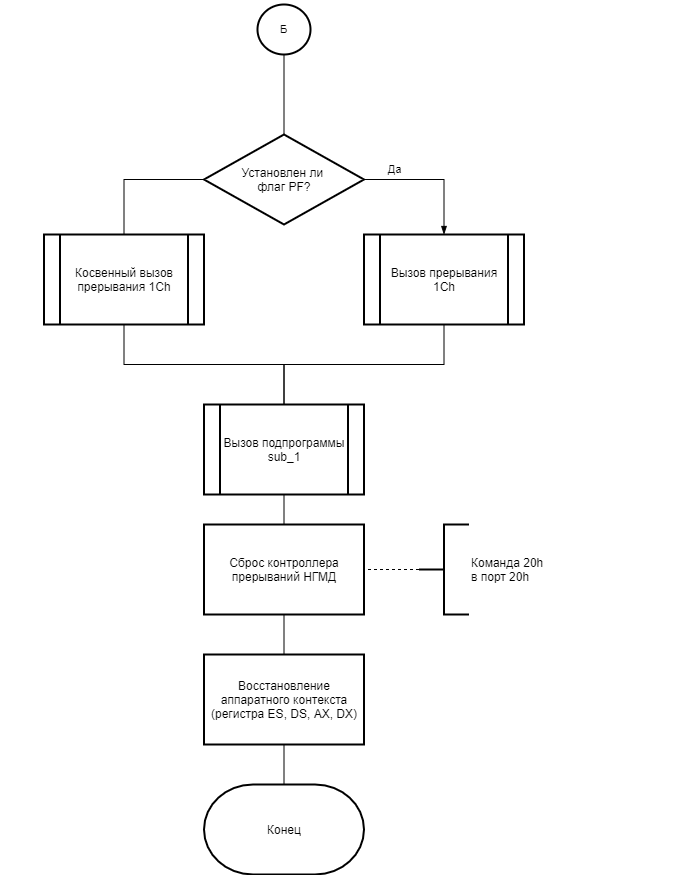
020A:07D8 loc\_8:

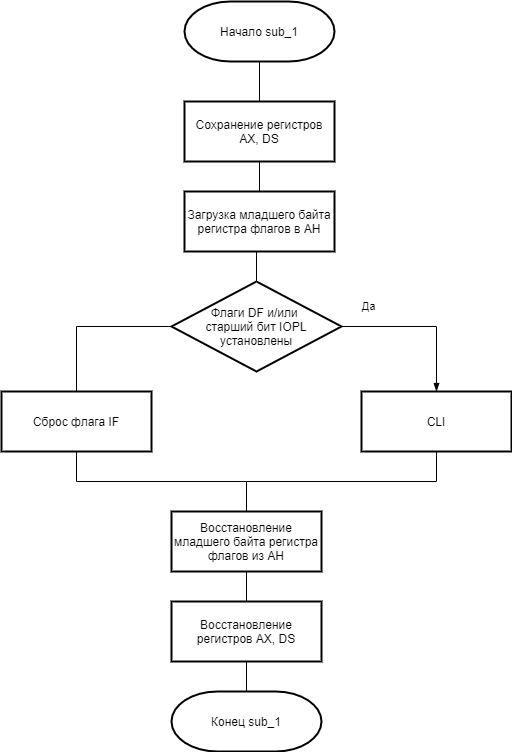
020A:07D8 C3 retn

sub\_1 endp

1. **Схема алгоритма прерывания int 8h**





1. **Схема алгоритма подпрограммы**