**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 (ИУ7)

НАПРАВЛЕНИЕ ПОДГОТОВКИ **09.03.01 Информатика и вычислительная техника**

О т ч е т

# по лабораторной работе № 1 (часть 1)

**Название: Дизассемблирование int 8h**

# Дисциплина: Операционные системы

Студент гр. ИУ7-55Б О.Н.Талышева

(Подпись, дата) (И.О. Фамилия)

Преподаватель Н.Ю. Рязанова

(Подпись, дата) (И.О. Фамилия)

**Листинг прерывания int 8h:**

Temp.lst Sourcer v7.00 13-Sep-24 10:59 pm Page 1

; вызов sub\_1 (эта SUBROUTINE запрещает маскируемые прерывания)

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

; значения регистров es, ds, ax, dx сохраняются

020C:0749 06 **push** es

020C:074A 1E **push** ds

020C:074B 50 **push** ax

020C:074C 52 **push** dx

; ds = 40h (область данных биос), es = 0h (адрес таблицы векторов прерываний)

020C:074D B8 0040 **mov** ax,40h

020C:0750 8E D8 **mov** ds,ax

020C:0752 33 C0 **xor** ax,ax ; Zero register

020C:0754 8E C0 **mov** es,ax

; инкремент младшего слова счётчика реального времени по адресу DS:006Ch

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

; младшее слово счётчика реального времени равно 0?

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

; ДА -> инкремент старшего слова счётчика реального времени по адресу DS:006Eh

020C:075C FF 06 006E **inc** **word** **ptr** ds:[6Eh] ; (0040:006E=17h)

020C:0760 loc\_1:

; старшее слово счётчика реального времени равно 24? (18h - это 24 часа)

020C:0760 83 3E 006E 18 **cmp** **word** **ptr** ds:[6Eh],18h ; (0040:006E=17h)

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

; ДА -> младшее слово счётчика реального времени равно 176?

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

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

; ДА -> ДА -> сброс счётчика реального времени

020C:076F A3 006E **mov** **word** **ptr** ds:[6Eh],ax ; (0040:006E=17h)

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

; ДА -> ДА -> установка 1 по адресу DS:0070h

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

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

020C:077C loc\_2:

020C:077C 50 **push** ax

; декремент счётчика времени до отключения моторчика дисковода по адресу DS:0040h

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

; счётчик времени до отключения моторчика дисковода равен 0?

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

; ДА -> сброс флага отключения моторчика дисковода по адресу DS:003Fh

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

; ДА -> команда 0Ch в порт 3F2h - отключение моторчика дисковода

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

; установлен флаг PF?

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

; ДА -> сохранение FLAGS

020C:0797 9F **lahf** ; Load ah from flags

020C:0798 86 E0 **xchg** ah,al

020C:079A 50 **push** ax

; ДА -> косвенный вызов пользовательского прерывания 1Ch с помощью команды call

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**

; НЕТ -> вызов пользовательского прерывания int 1Ch

020C:07A3 loc\_4:

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

020C:07A5 loc\_5:

; второй вызов sub\_1

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

; сброс контроллера прерываний

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

; значения регистров es, ds, ax, dx восстанавливаются

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

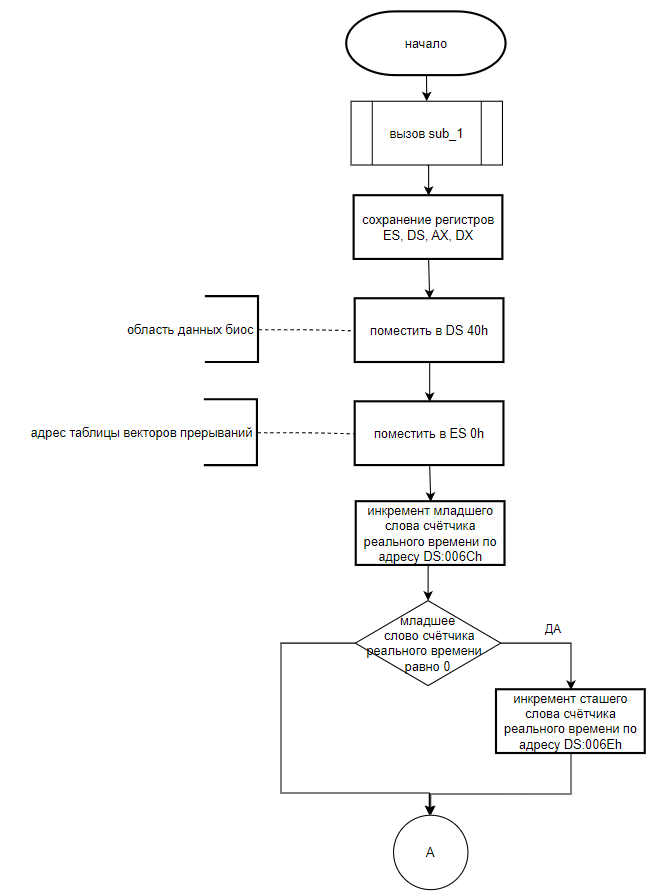
; 020C:07B0h - 164h = 020C:064Сh

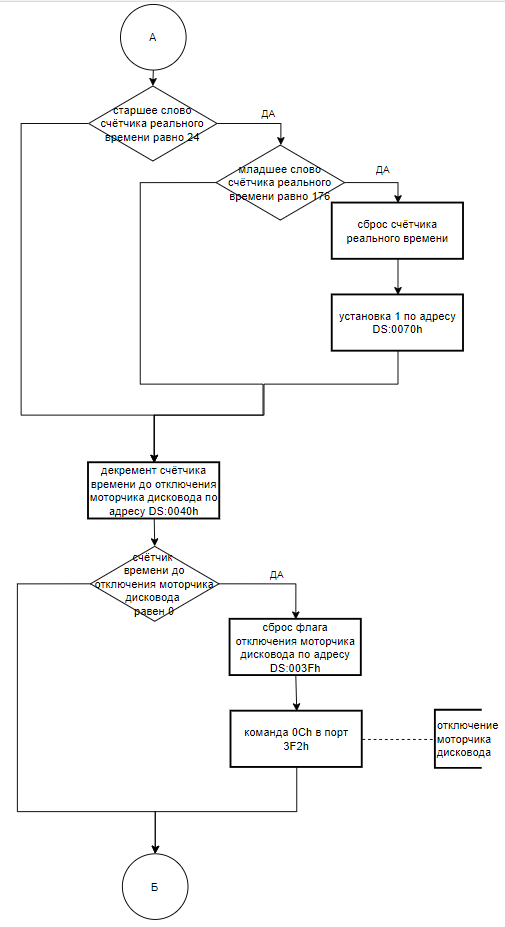
; ...

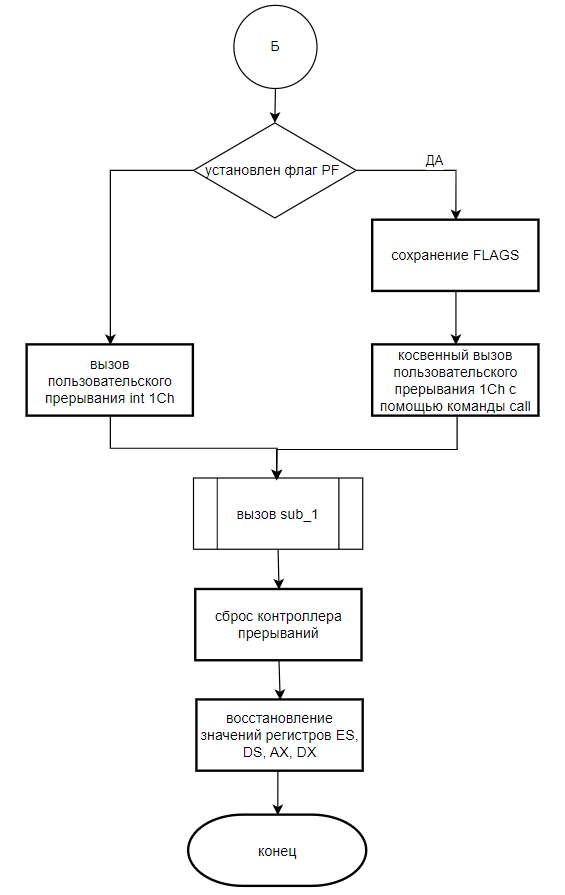
; Возврат из прерывания

020C:06AC CF **iret** ; Interrupt return

**Схема алгоритма прерывания int 8h:**







**Листинг подпрограммы sub\_1:**

;ЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯЯ

Temp.lst Sourcer v7.00 13-Sep-24 10:59 pm Page 2

; SUBROUTINE

;ЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬЬ

; запрет маскируемых прерываний (зануление IF)

020C:07B9 sub\_1 proc **near**

; значения регистров ds, ax сохраняются

020C:07B9 1E **push** ds

020C:07BA 50 **push** ax

; ds = 40h (область данных биос)

020C:07BB B8 0040 **mov** ax,40h

020C:07BE 8E D8 **mov** ds,ax

; загрузка AH из младшего слова FLAGS

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

; установлен старший бит IOPL или флаг DF?

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

; ДА -> сброс IF по адресу DS:0314h

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

020C:07D0 loc\_6:

; загрузка AH в младшее слово FLAGS

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

; восстановление регистров AX, DS

020C:07D1 58 **pop** ax

020C:07D2 1F **pop** ds

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

020C:07D5 loc\_7:

; НЕТ -> сброс IF командой cli

020C:07D5 FA **cli** ; Disable interrupts

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

; возврат из sub\_1

020C:07D8 loc\_8:

020C:07D8 C3 **retn**

sub\_1 endp

**Схема алгоритма подпрограммы sub\_1:**

