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 “ИУ, Информатика и системы управления”

КАФЕДРА “ИУ7, Программное обеспечение ЭВМ и информационные технологии”

Лабораторная работа №1

по дисциплине

“Операционные системы”

Тема: Дизассемблирование INT 8h

Студент: Андреев А.А.

Группа: ИУ7-54Б

Преподаватель: Рязанова н7Ю.

Москва - 2021 г.

1. Полученный дизассемблированный код

1.1. Листинг INT 8h

```
call    sub_4               ; (07B9)
                push  es
                push  ds
                push  ax
                push  dx
                mov   ax,40h
                mov   ds,ax
                xor   ax,ax             ; Zero register
                mov   es,ax
                inc   word ptr ds:[6Ch] ; (0040:006C=22A7h)
                jnz   loc_3             ; Jump if not zero
                inc   word ptr ds:[6Eh] ; (0040:006E=16h)
loc_3:
                cmp   word ptr ds:[6Eh],18h     ; (0040:006E=16h)
                jne   loc_4             ; Jump if not equal
                cmp   word ptr ds:[6Ch],0B0h    ; (0040:006C=22A7h)
                jne   loc_4             ; Jump if not equal
                mov   word ptr ds:[6Eh],ax      ; (0040:006E=16h)
                mov   word ptr ds:[6Ch],ax      ; (0040:006C=22A7h)
                mov   byte ptr ds:[70h],1 ; (0040:0070=0)
                or    al,8
loc_4:
                push  ax
                dec   byte ptr ds:[40h]   ; (0040:0040=35h)
                jnz   loc_5             ; Jump if not zero
                and   byte ptr ds:[3Fh],0F0h    ; (0040:003F=0)
                mov   al,0Ch
                mov   dx,3F2h
                out   dx,al             ; port 3F2h, dsk0 contrl output
loc_5:
                pop   ax
                test  word ptr ds:[314h],4      ; (0040:0314=3200h)
                jnz   loc_6             ; Jump if not zero
                lahf                    ; Load ah from flags
                xchg  ah,al
                push  ax
                call  dword ptr es:[70h] ; (0000:0070=6ADh)
                jmp   short loc_7       ; (07A5)
                nop
```

```
loc_6:
                int     1Ch             ; Timer break (call each 18.2ms)
loc_7:
                call    sub_4           ; (07B9)
                mov     al,20h          ; ' '
                out     20h,al          ; port 20h, 8259-1 int command
                                        ;  al = 20h, end of interrupt
                pop     dx
                pop     ax
                pop     ds
                pop     es
                jmp     $-164h
                db      0C4h
                les     cx,dword ptr ds:[93E9h]  ; (0000:93E9=0E181h) Load 32
bit ptr
                db      0FEh
```

2. Схема алгоритмов