

**МИНОБРНАУКИ РОССИИ**  
**САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ**  
**ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**  
**«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)**  
**Кафедра МО ЭВМ**

**ОТЧЕТ**  
**по лабораторной работе №1**  
**по дисциплине «Операционные системы»**  
**Тема: Исследование структур загрузочных модулей.**

Студент гр. 8383

Кормщикова А. О.

Преподаватель

Ефремов М. А.

Санкт-Петербург

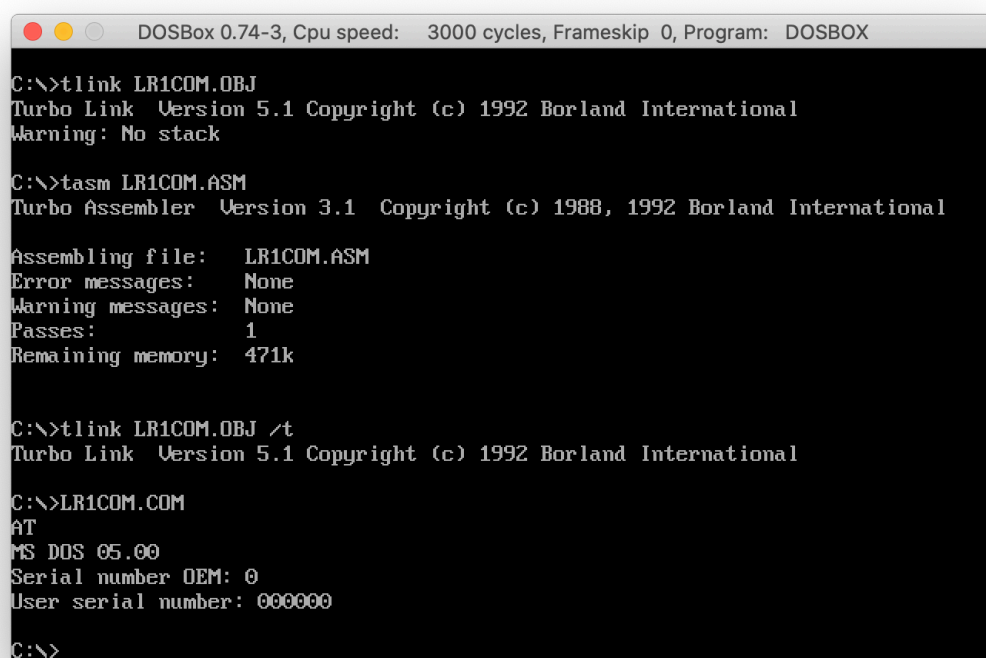
2020

### Цель работы.

Исследование различий в структурах исходных текстов модулей типов **.COM** и **.EXE**, структур файлов загрузочных модулей и способов их загрузки в основную память.

### Ход выполнения.

Был написан код исходного **.COM** модуля (LR1COM.ASM представлен в приложении А), который определяет тип PC и версию системы. Ассемблерная программа читает содержимое предпоследнего байта ROM BIOS, по коду определяет тип PC и выводит строку с названием модели. Из данного кода были собраны "хороший" **.COM** модуль и "плохой" **.EXE** модуль. Во время линковки "плохого" модуля было выведено предупреждение об отсутствии стека. Результаты выполнения **.COM** модуля представлены на рис. 1, **.EXE** модуля на рис. 2.



```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX

C:\>tlink LR1COM.OBJ
Turbo Link Version 5.1 Copyright (c) 1992 Borland International
Warning: No stack

C:\>tasm LR1COM.ASM
Turbo Assembler Version 3.1 Copyright (c) 1988, 1992 Borland International

Assembling file: LR1COM.ASM
Error messages: None
Warning messages: None
Passes: 1
Remaining memory: 471k

C:\>tlink LR1COM.OBJ /t
Turbo Link Version 5.1 Copyright (c) 1992 Borland International

C:\>LR1COM.COM
AT
MS DOS 05.00
Serial number OEM: 0
User serial number: 000000

C:\>
```

Рисунок 1 - Результат выполнения **.COM** модуля



## Отличия исходных текстов COM и EXE программ

### 1. Сколько сегментов должна содержать COM-программа?

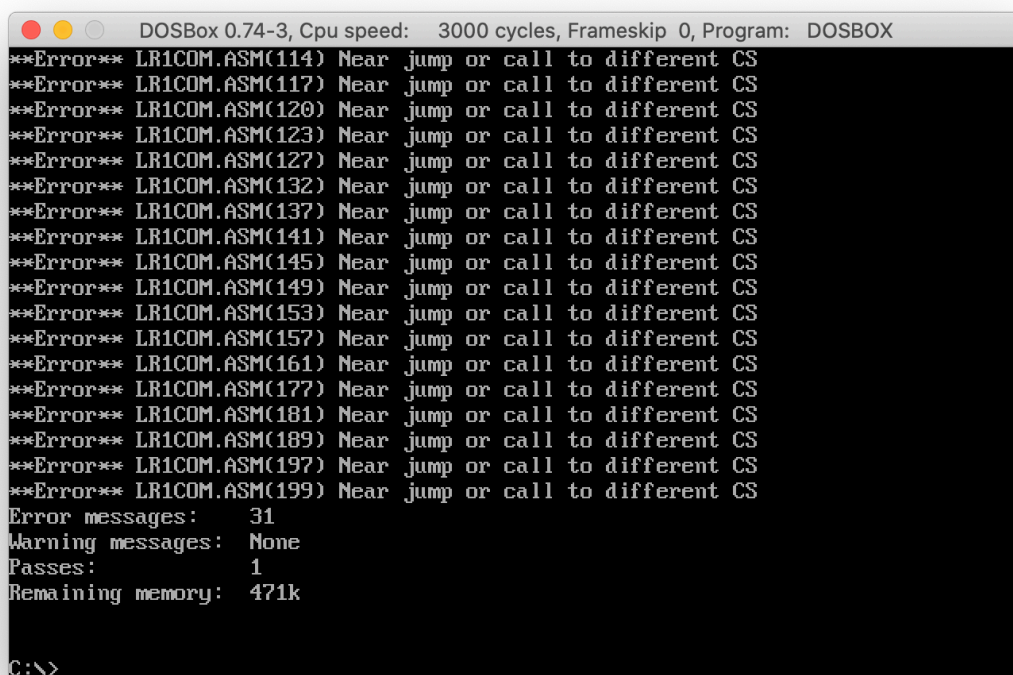
COM-программа содержит ровно один сегмент

### 2. EXE-программа?

EXE-программа должна содержать не менее одного сегмента

### 3. Какие директивы должны обязательно быть в тексте COM -программы?

Должна присутствовать директива `assume` в которой инициализируются регистры, `CS` и `DS` указывают на общий сегмент, при попытке компиляции программы без директивы `assume` выдается ошибка см рис 1.1. `ORG 100h`, которая резервирует первые 256 байт под PSP, директива говорит, что вся адресация внутри кода смещена на эти байты.



```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
***Error** LR1COM.ASM(114) Near jump or call to different CS
***Error** LR1COM.ASM(117) Near jump or call to different CS
***Error** LR1COM.ASM(120) Near jump or call to different CS
***Error** LR1COM.ASM(123) Near jump or call to different CS
***Error** LR1COM.ASM(127) Near jump or call to different CS
***Error** LR1COM.ASM(132) Near jump or call to different CS
***Error** LR1COM.ASM(137) Near jump or call to different CS
***Error** LR1COM.ASM(141) Near jump or call to different CS
***Error** LR1COM.ASM(145) Near jump or call to different CS
***Error** LR1COM.ASM(149) Near jump or call to different CS
***Error** LR1COM.ASM(153) Near jump or call to different CS
***Error** LR1COM.ASM(157) Near jump or call to different CS
***Error** LR1COM.ASM(161) Near jump or call to different CS
***Error** LR1COM.ASM(177) Near jump or call to different CS
***Error** LR1COM.ASM(181) Near jump or call to different CS
***Error** LR1COM.ASM(189) Near jump or call to different CS
***Error** LR1COM.ASM(197) Near jump or call to different CS
***Error** LR1COM.ASM(199) Near jump or call to different CS
Error messages: 31
Warning messages: None
Passes: 1
Remaining memory: 471k
C:\>
```

Рисунок 1.1 - Компиляции com -модуля без директивы `assume`

#### 4. Все ли форматы команд можно использовать в COM-программе?

Модуль такого типа не содержит таблицы настроек, поэтому некорректно указание адреса сегмента.

При помощи программы FAR были открыты загрузочные модули. Вид модулей в шестнадцатеричном виде представлен на рис. 4-6.

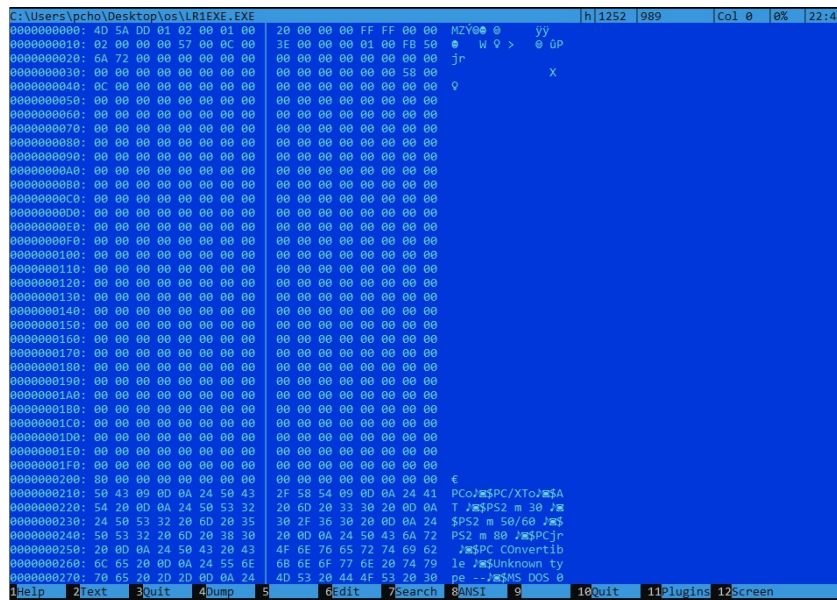


Рисунок 4 - Содержимое файла "хорошего" .EXE модуля

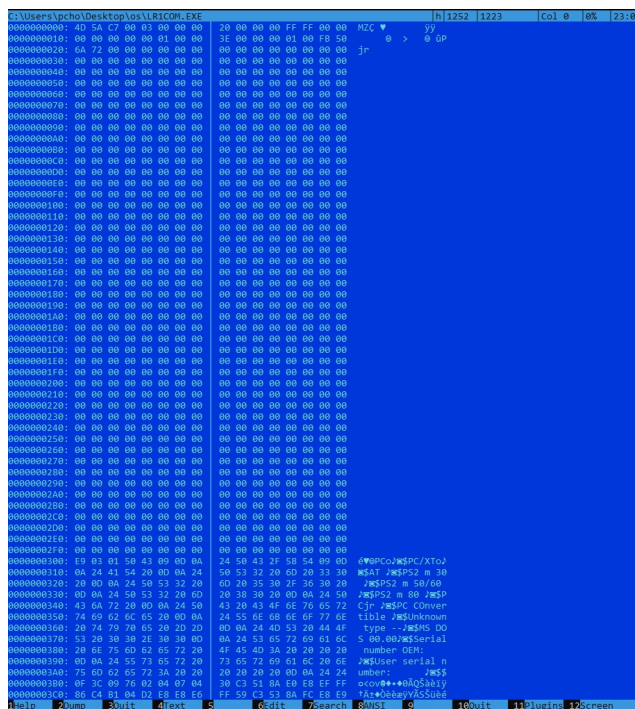


Рисунок 5 - Содержимое модуля .COM





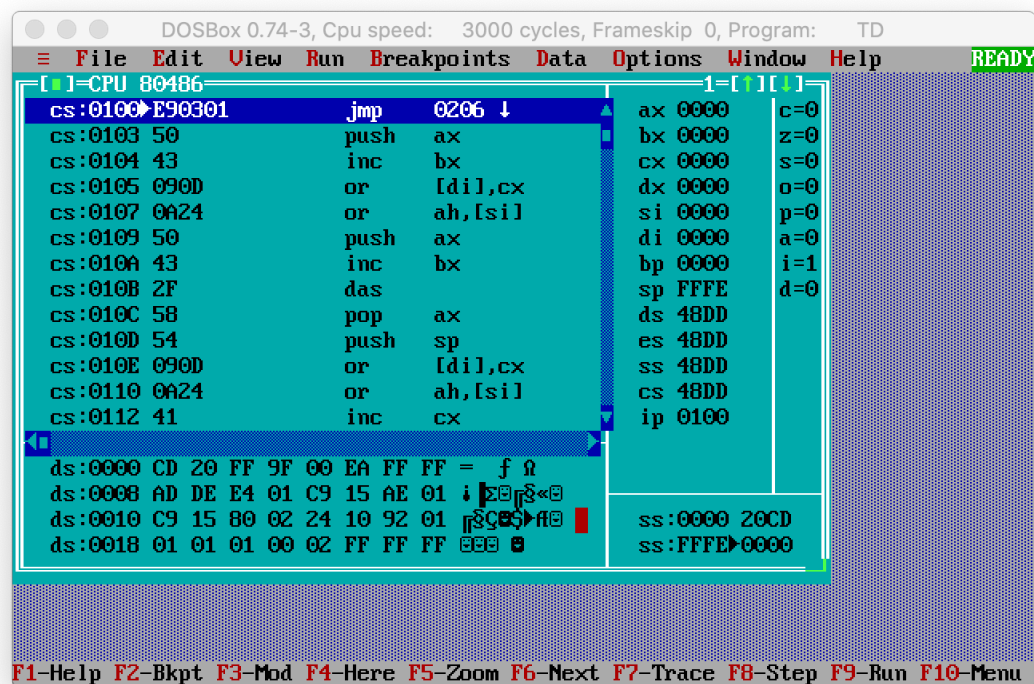


Рисунок 7 - модуль COM в отладчике TD

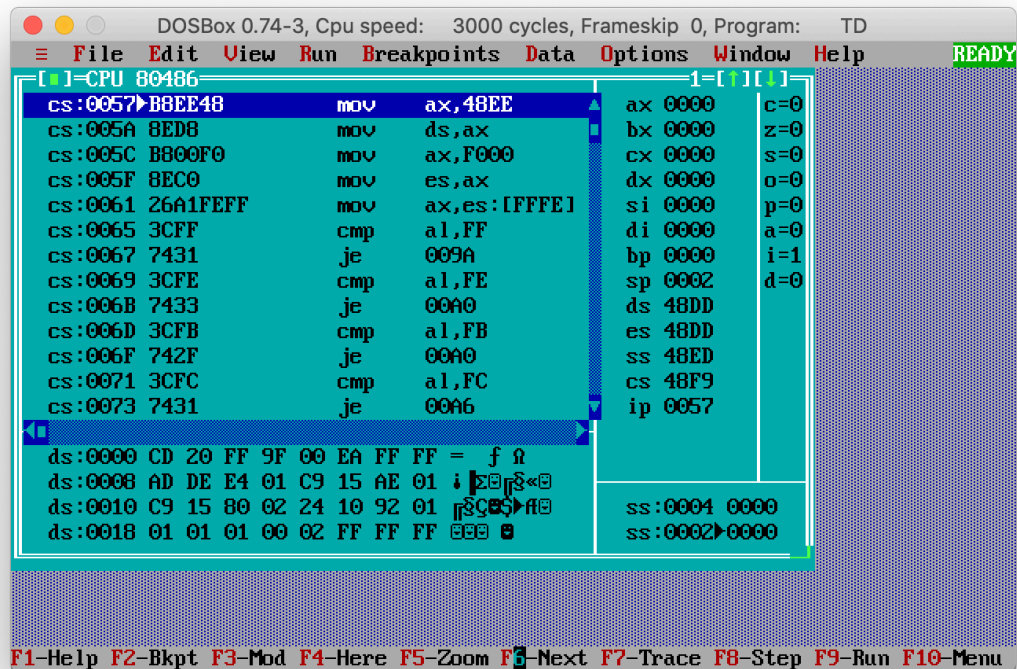


Рисунок 8 - модуль EXE в отладчике TD

### **Загрузка COM модуля в основную память**

1. Какой формат загрузки модуля COM? С какого адреса располагается код?

COM файл загружается со смещением 100h, код и данные располагаются в памяти с этого адреса.

2. Что располагается с адреса 0?

С адреса 0h при загрузке ОС располагает PSP

3. Какие значения имеют сегментные регистры? На какие области памяти они указывают?

Все сегментные регистры имеют одинаковое значение и указывают на PSP.

4. Как определяется стек? Какую область памяти он занимает? Какие адреса?

Стек занимает всю доступную память после кода. При загрузке SP устанавливается в FFFEh.

### **Загрузка «хорошего» EXE модуля в основную память**

1. Как загружается «хороший» .EXE? Какие значения имеют сегментные регистры?

При загрузке сегментные регистры CS и SS устанавливаются в начало соответствующего сегмента, DS и ES устанавливаются на начало PSP. В IP загружается смещение точки входа в программу.

2. На что указывают регистры DS и ES?

DS и ES устанавливаются на начало PSP

3. Как определяется стек?

Стек определяется с помощью директивы `assume SS:SSTACK`. Где SSTACK - сегмент, отведенный под стек.

4. Как определяется точка входа?



Если точка входа не указана явно, то ей является начало сегмента кода. В программе точка входа указывается при помощи директивы END <метка>, где метка - точка входа в программу.

### **Выводы.**

В ходе выполнения лабораторной работы были исследованы различия в структурах исходных текстов модулей **.COM** и **.EXE**, а также структур файлов загрузочных модулей и способы их загрузки в основную память.

## ПРИЛОЖЕНИЕ

### Содержимое файла "хорошего" EXE модуля:

```
SSTACK SEGMENT STACK
        DW 128
SSTACK  ENDS

DATA SEGMENT

        pcff db 'PC ', 0DH, 0AH, '$'
        pcxt db 'PC/XT ', 0DH, 0AH, '$'
        atfc db 'AT ', 0DH, 0AH, '$'
        ps30 db 'PS2 m 30 ', 0DH, 0AH, '$'
        ps50 db 'PS2 m 50/60 ', 0DH, 0AH, '$'
        ps80 db 'PS2 m 80 ', 0DH, 0AH, '$'
        pcjr db 'PCjr ', 0DH, 0AH, '$'
        pccm db 'PC CONvertible ', 0DH, 0AH, '$'
        unkt db 'Unknown type --', 0DH, 0AH, '$'
        ver  db 'MS DOS 00.00', 0DH, 0AH, '$'
        oem  db 'Serial number OEM: ', 0DH, 0AH, '$'
        usn  db 'User serial number: ', 0DH, 0AH, '$'

DATA ENDS

CODE SEGMENT

ASSUME CS:CODE, DS:DATA, SS:SSTACK

;-----
TETR_TO_HEX  PROC  near
                and     AL,0Fh
                cmp     AL,09
                jbe     NEXT
                add     AL,07
NEXT:         add     AL,30h
                ret
TETR_TO_HEX  ENDP

;-----
BYTE_TO_HEX  PROC  near
; байт в AL переводится в два символа в шестн. числа в AX
                push    CX
                mov     AH,AL
                call    TETR_TO_HEX
                xchg     AL,AH
                mov     CL,4
                shr     AL,CL
                call    TETR_TO_HEX ;в AL старшая цифра
                pop     CX           ;в AH младшая
                ret
BYTE_TO_HEX  ENDP

;-----
WRD_TO_HEX  PROC  near
;перевод в 16 с/с 16-ти разрядного числа
; в AX - число, DI - адрес последнего символа
                push    BX
                mov     BH,AH
                call    BYTE_TO_HEX
                mov     [DI],AH
                dec     DI
```

```

        mov [DI],AL
        dec DI
        mov AL,BH
        call BYTE_TO_HEX
        mov [DI],AH
        dec DI
        mov [DI],AL
        pop BX
        ret
WRD_TO_HEX ENDP ;-----

BYTE_TO_DEC PROC near
; перевод в 10 с/с, SI - адрес поля младшей цифры
        push CX
        push DX
        xor AH,AH
        xor DX,DX
        mov CX,10
loop_bd: div CX
        or DL,30h
        mov [SI],DL
        dec SI
        xor DX,DX
        cmp AX,10
        jae loop_bd
        cmp AL,00h
        je end_1
        or AL,30h
        mov [SI],AL
end_1:   pop DX
        pop CX
        ret
BYTE_TO_DEC ENDP

MAIN PROC FAR

        mov ax, DATA
        mov ds, ax
;type
        mov ax,0F000h
        mov es, ax
        mov ax, es:[0FFFEh]

        cmp al, 0FFh
        je PC

        cmp al, 0FEh
        je XT

        cmp al, 0FBh
        je XT

        cmp al, 0FCh
        je AT

        cmp al, 0FAh
        je PS230

        cmp al, 0FCh
        je PS250

        cmp al, 0F8h
        je PS280

```

```

        cmp al, 0FDh
        je PCJ

        cmp al, 0F9h
        je PCC

;UNKNOWN TYPE

        call BYTE_TO_HEX
        mov bx, offset unkt
        mov [bx+14], al
        mov [bx+15], ah
        mov dx, bx
        jmp res

PC:
        mov dx, offset pcff
        jmp res

XT:
        mov dx, offset pcxt
        jmp res

AT:
        mov dx, offset atfc
        jmp res

PS230:
        mov dx, offset ps30
        jmp res

PS250:
        mov dx, offset ps50
        jmp res

PS280:
        mov dx, offset ps80
        jmp res

PCJ:
        mov dx, offset pcjr
        jmp res

PCC:
        mov dx, offset pccm

RES:
        mov ah, 09h
        int 21h

;os ver
        mov ah, 30h
        int 21h

        push ax
        mov si, offset ver
        add si, 8
        call BYTE_TO_DEC
        pop ax
        mov al, ah
        add si, 3
        call BYTE_TO_DEC
        mov dx, offset ver

```

```

mov ah, 09h
int 21h

mov si, offset oem
add si, 19
mov al, bh
call BYTE_TO_DEC
mov dx, offset oem
mov ah, 09h
int 21h

mov di, offset usn
add di, 25
mov ax, cx
call WRD_TO_HEX
mov al, bl
call BYTE_TO_HEX
sub di, 2
mov [di], ax
mov dx, offset usn
mov ah, 09h
int 21h

;exit to dos

xor AL,AL
mov AH,4Ch
int 21H

MAIN      ENDP
CODE ENDS
END MAIN

```

## Содержимое .COM модуля:

```

TESTPC SEGMENT
        ASSUME  CS:TESTPC, DS:TESTPC, ES:NOTHING, SS:NOTHING
        ORG     100H
START:   JMP     BEGIN

;DATA

pcff db 'PC ', 0DH, 0AH, '$'
pcxt db 'PC/XT ', 0DH, 0AH, '$'
atfc db 'AT ', 0DH, 0AH, '$'
ps30 db 'PS2 m 30 ', 0DH, 0AH, '$'
ps50 db 'PS2 m 50/60 ', 0DH, 0AH, '$'
ps80 db 'PS2 m 80 ', 0DH, 0AH, '$'
pcjr db 'PCjr ', 0DH, 0AH, '$'
pccm db 'PC COnvertible ', 0DH, 0AH, '$'
unkt db 'Unknown type --', 0DH, 0AH, '$'
ver db 'MS DOS 00.00', 0DH, 0AH, '$'
oem db 'Serial number OEM: ', 0DH, 0AH, '$'
usn db 'User serial number: ', 0DH, 0AH, '$'

;-----
TETR_TO_HEX PROC near
        and     AL,0Fh
        cmp     AL,09
        jbe     NEXT
        add     AL,07
NEXT:

```

```

NEXT:      add      AL,30h
           ret
TETR_TO_HEX ENDP

;-----
BYTE_TO_HEX PROC near
; байт в AL переводится в два символа в шестн. числа в AX
           push     CX
           mov      AH,AL
           call     TETR_TO_HEX
           xchg     AL,AH
           mov      CL,4
           shr      AL,CL
           call     TETR_TO_HEX ;в AL старшая цифра
           pop      CX          ;в AH младшая
           ret
BYTE_TO_HEX ENDP
;-----

WRD_TO_HEX PROC near
;перевод в 16 с/с 16-ти разрядного числа
; в AX - число, DI - адрес последнего символа
           push     BX
           mov      BH,AH
           call     BYTE_TO_HEX
           mov      [DI],AH
           dec      DI
           mov      [DI],AL
           dec      DI
           mov      AL,BH
           call     BYTE_TO_HEX
           mov      [DI],AH
           dec      DI
           mov      [DI],AL
           pop      BX
           ret
WRD_TO_HEX ENDP ;-----

BYTE_TO_DEC PROC near
; перевод в 10 с/с, SI - адрес поля младшей цифры
           push     CX
           push     DX
           xor      AH,AH
           xor      DX,DX
           mov      CX,10
loop_bd:   div      CX
           or       DL,30h
           mov      [SI],DL
           dec      SI
           xor      DX,DX
           cmp      AX,10
           jae      loop_bd
           cmp      AL,00h
           je       end_1
           or       AL,30h
           mov      [SI],AL
end_1:     pop      DX
           pop      CX
           ret

```



```
BYTE_TO_DEC      ENDP
```

```
BEGIN:
```

```
;type
```

```
    mov ax,0F000h
    mov es, ax
    mov ax, es:[0FFFEh]
```

```
    cmp al, 0FFh
    je PC
```

```
    cmp al, 0FEh
    je XT
```

```
    cmp al, 0FBh
    je XT
```

```
    cmp al, 0FCh
    je AT
```

```
    cmp al, 0FAh
    je PS230
```

```
    cmp al, 0FCh
    je PS250
```

```
    cmp al, 0F8h
    je PS280
```

```
    cmp al, 0FDh
    je PCJ
```

```
    cmp al, 0F9h
    je PCC
```

```
;UNKNOWN TYPE
```

```
    call BYTE_TO_HEX
    mov bx, offset unkt
    mov [bx+14], al
    mov [bx+15], ah
    mov dx, bx
    jmp res
```

```
PC:
```

```
    mov dx, offset pcff
    jmp res
```

```
XT:
```

```
    mov dx, offset pcxt
    jmp res
```

```
AT:
```

```
    mov dx, offset atfc
    jmp res
```

```

PS230:
    mov dx, offset ps30
    jmp res

PS250:
    mov dx, offset ps50
    jmp res

PS280:
    mov dx, offset ps80
    jmp res

PCJ:
    mov dx, offset pcjr
    jmp res

PCC:
    mov dx, offset pccm

RES:
    mov ah, 09h
    int 21h

;os ver
    mov ah, 30h
    int 21h

    push ax
    mov si, offset ver
    add si, 8
    call BYTE_TO_DEC
    pop ax
    mov al, ah
    add si, 3
    call BYTE_TO_DEC
    mov dx, offset ver
    mov ah, 09h
    int 21h

    mov si, offset oem
    add si, 19
    mov al, bh
    call BYTE_TO_DEC
    mov dx, offset oem
    mov ah, 09h
    int 21h

    mov di, offset usn
    add di, 25
    mov ax, cx
    call WRD_TO_HEX
    mov al, bl
    call BYTE_TO_HEX
    sub di, 2
    mov [di], ax
    mov dx, offset usn
    mov ah, 09h
    int 21h

;exit to dos

```

```
        xor AL,AL
        mov AH,4Ch
        int 21H

TESTPC      ENDS
END START
```