

МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
“ЛЭТИ” ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра математического обеспечения и применения ЭВМ

Отчет
По лабораторной работе №1
По дисциплине “Операционные системы”
Тема: Исследование структур загрузочных модулей

Студент гр. 8382

Никитин А.Е.

Преподаватель

Ефремов М.А.

Санкт-Петербург

2020

Цель работы.

Исследование различий структур исходных модулей типов .com и .exe, структур файлов загрузочных модулей и способов загрузки в основную память.

Необходимые сведения.

Тип IBM PC хранится в байте по адресу 0F000:0FFFEh, в предпоследнем байте ROM BIOS. Соответствие кода и типа в таблице:

PC	FF
PC/XT	FE, FB
AT	FC
PS2 модель 30	FA
PS2 модель 50 или 60	FC
PS2 модель 80	F8
PCjr	FD
PC Convertible	F9

Для определения версии MS DOS следует воспользоваться функцией 30h прерывания 21h. Входным параметром является номер функции в AH:

mov ah, 30h

int 21h

Выходными параметрами являются:

AL - номер основной версии. Если 0, то <2.0

AH - номер модификации

BH - серийный номер OEM (Original Equipment Manufacturer)

BL:CH – 24-битовый серийный номер пользователя.

Постановка задачи.

Требуется реализовать текст исходного .com модуля, который определяет тип PC и версию системы. Ассемблерная программа должна читать содержимое предпоследнего байта ROM BIOS, по таблице, сравнивая коды, определять тип PC и выводить строку с названием модели. Если код не совпадает ни с одним значением, то двоичный код переводиться в символьную строку, содержащую запись шестнадцатеричного числа и выводиться на экран в виде соответствующего сообщения. Затем определяется версия системы. Ассемблерная программа должна по значениям регистров al и ah формировать текстовую строку в формате xx.yy, где xx - номер основной версии, а yy - номер модификации в десятичной системе счисления, формировать строки с серийным номером OEM и серийным номером пользователя. Полученные строки выводятся на экран.

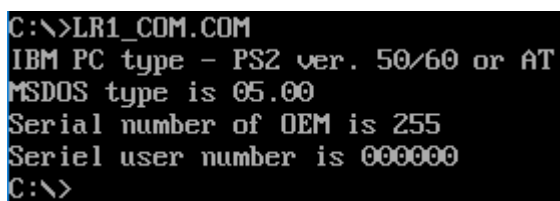
Далее необходимо отладить полученный исходный модуль и получить “хороший” .com модуль, а также необходимо построить “плохой” .exe, полученный из исходного текста для .com модуля.

Затем нужно написать текст “хорошего” .exe модуля, который выполняет те же функции, что и модуль .com, далее его построить, отладить и сравнить исходные тексты для .com и .exe модулей.

Выполнение работы.

Для определения типа PC и версии были написаны тексты .com и .exe модулей. Для определения версии MS DOS была использована функция 30h прерывания 21h. После ее вызова версия системы определяется значением регистров al, ah. В регистре bh - серийный номер OEM, в bl:cx – 24-битовый серийный номер пользователя.

Результат выполнения .com модуля виден на рис. 1. Результат выполнения “плохого” .exe модуля, полученного из исходного текста для .com модуля, виден на рис. 2. Результат выполнения “хорошего” .exe модуля - на рис. 3.



```
C:\>LR1_COM.COM
IBM PC type - PS2 ver. 50/60 or AT
MSDOS type is 05.00
Serial number of OEM is 255
Serial user number is 000000
C:\>
```

Рисунок 1 - Результат работы LR1_COM.COM

```

C:\>LR1_COM.EXE

        00000000 IBM PC type -

        00000000 IBM PC type -

        00000000 IBM PC type - 5 0

PC type -

        00000000 IBM PC type - 255

        00000000 IBM PC type - 000000
C:\>

```

Рисунок 2 - Результат LR1_COM.EXE

```

C:\>LR1_EXE.EXE
IBM PC type - PS2 ver. 50/60 or AT
MSDOS type is 05.00
Serial number of OEM is 255
Serial user number is 000000
C:\>

```

Рисунок 3 - Результат работы LR1_EXE.EXE

Представление исходных файлов в шестнадцатеричном виде
представление исходных файлов в шестнадцатеричном виде:

```

C:\Users\User\Desktop\TASM\LR1_COM.COM
00000000: E9 0C 01 49 42 4D 20 50 43 20 74 79 70 65 20 2D  é900IBM PC type -
00000001: 20 24 50 43 0A 0D 24 50 43 2F 58 54 0A 0D 24 50  $PC$PC/XT$P
00000002: 53 32 20 76 65 72 2E 20 33 30 0A 0D 24 50 53 32  S2 ver. 30$P$P$2
00000003: 20 76 65 72 2E 20 35 30 2F 36 30 20 6F 72 20 41  ver. 50/60 or A
00000004: 54 0A 0D 24 50 53 32 20 76 65 72 2E 20 38 30 0A  T$P$P$2 ver. 80$
00000005: 0D 24 50 43 6A 72 0A 0D 24 50 43 20 43 6F 6E 76  $PCjr$PC Conv
00000006: 65 72 74 69 62 6C 65 0A 0D 24 4D 53 44 4F 53 20  ertible$MSDOS
00000007: 74 79 70 65 20 69 73 20 24 3C 32 2E 30 0A 0D 24  type is $<2.0$
00000008: 30 78 2E 30 79 0A 0D 24 53 65 72 69 61 6C 20 6E  0x.0y$Serial n
00000009: 75 6D 62 65 72 20 6F 66 20 4F 45 4D 20 69 73 20  umber of OEM is
0000000A: 24 0A 0D 53 65 72 69 65 6C 20 75 73 65 72 20 6E  $Serial user n
0000000B: 75 6D 62 65 72 20 69 73 20 24 51 52 E8 1C 00 8A  umber is $QRèL 5
0000000C: EC 8A D0 B4 02 CD 21 8A D5 B4 02 CD 21 5A 59 C3  i50'0i!50'0i!ZYA
0000000D: 24 0F 3C 09 76 02 04 07 04 30 C3 51 8A E0 E8 EF  $o<ov0+0AQ5aèi
0000000E: FF 86 C4 B1 04 D2 E8 E8 E6 FF 59 C3 51 52 32 E4  y†A±0èèayYQR2a
0000000F: 33 D2 B9 0A 00 F7 F1 80 CA 30 88 14 4E 33 D2 3D  30'è +hèÈ0'jN30=
00000010: 0A 00 73 F1 3C 00 74 04 0C 30 88 04 5A 59 C3 B8  sñ< t+90+ZYA,
00000011: 00 F0 8E C0 26 A0 FE FF BA 03 01 B4 09 CD 21 BA  òŽ& pye'0'oi!è
00000012: 12 01 3C FF 74 31 BA 17 01 3C FE 74 2A 3C FB 74  $0<y†1èi0<pt*<ùt
00000013: 26 BA 2D 01 3C FC 74 1F BA 1F 01 3C FA 74 18 BA  &è-0<ùt'è'0<ùt†è
00000014: 44 01 3C F8 74 11 BA 52 01 3C FD 74 0A BA 59 01  D0<0t<èR0<y†èèY0
00000015: 3C F9 75 00 E8 63 FF B4 09 CD 21 BA 6A 01 B4 09  <ùu ècy'oi!èj0'o
00000016: CD 21 B4 30 CD 21 3C 00 75 07 BA 79 01 B4 09 CD  I! '0i!< u+èy0'oi
00000017: 21 BE 80 01 83 C6 01 E8 72 FF 83 C6 04 8A C4 E8  !%è0fA0èryfA+5Aè
00000018: 6A FF BA 80 01 B4 09 CD 21 B4 30 CD 21 BA 88 01  jyeè0'oi! '0i!è'0
00000019: B4 09 CD 21 8A C7 E8 53 FF 8A 14 B4 02 CD 21 8A  'oi!5çesysg'oi!5
0000001A: 54 01 CD 21 8A 54 02 CD 21 B4 30 CD 21 BA A1 01  T0i!5T0i! '0i!è;0
0000001B: B4 09 CD 21 8A C3 E8 01 FF 8A C5 E8 FC FE 8A C1  'oi!5Aèy5Aèup5A
0000001C: E8 F7 FE 32 C0 B4 4C CD 21 21 21 21 21 21 21 21  è+p2A'Lf!

```

Рисунок 4 – LR1_COM.COM в шестнадцатеричном виде.


```

C:\Users\User\Desktop\TASM\LR1_EXE.EXE
00000000: 4D 5A D4 01 03 00 01 00 20 00 00 00 FF FF 00 00 MZ0e  U , >  yy
00000010: 00 02 00 00 55 00 2C 00 3E 00 00 00 01 00 FB 50  U , >  U P
00000020: 6A 72 00 00 00 00 00 00 00 00 00 00 00 00 00 jr
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 56 00
00000040: 2C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 , v
00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000200: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000210: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000220: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000230: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000240: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

```

000000270: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000280: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000290: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000002F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000310: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000320: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000330: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000340: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000370: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000390: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000003A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000003B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000003C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000003D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000003E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000003F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000400: 49 42 4D 20 50 43 20 74 79 70 65 20 2D 20 24 50 IBM PC type - $P
000000410: 43 0A 0D 24 50 43 2F 58 54 0A 0D 24 50 53 32 20 C0)$PC/XT)$PS2
000000420: 76 65 72 2E 20 33 30 0A 0D 24 50 53 32 20 76 65 ver. 30)$PS2 ve
000000430: 72 2E 20 35 30 2F 36 30 20 6F 72 20 41 54 0A 0D r. 50/60 or AT)$
000000440: 24 50 53 32 20 76 65 72 2E 20 38 30 0A 0D 24 50 $PS2 ver. 80)$P
000000450: 43 6A 72 0A 0D 24 50 43 20 43 6F 6E 76 65 72 74 Cjr)$PC Convert
000000460: 69 62 6C 65 0A 0D 24 4D 53 44 4F 53 20 74 79 70 ible)$MSDOS typ
000000470: 65 20 69 73 20 24 3C 32 2E 30 0A 0D 24 30 78 2E e is $<2.0)$0x.
000000480: 30 79 0A 0D 24 53 65 72 69 61 6C 20 6E 75 6D 62 0y)$Serial numb
000000490: 65 72 20 6F 66 20 4F 45 4D 20 69 73 20 24 0A 0D er of OEM is $0)
0000004A0: 53 65 72 69 65 6C 20 75 73 65 72 20 6E 75 6D 62 Serial user numb
0000004B0: 65 72 20 69 73 20 24 00 00 00 00 00 00 00 00 er is $
0000004C0: 51 52 E8 1C 00 8A EC 8A D0 B4 02 CD 21 8A D5 B4 QR0L $i5p'0i150'
0000004D0: 02 CD 21 5A 59 C3 24 0F 3C 09 76 02 04 07 04 30 0i1ZYA$ocov000$
0000004E0: C3 51 8A E0 E8 FF 86 C4 B1 04 D2 E8 E8 E6 FF AQ$00iY+A+0000y
0000004F0: 59 C3 51 52 32 E4 33 D2 B9 0A 00 F7 F1 80 CA 30 YAQ$2000$ +0000
000000500: 88 14 4E 33 D2 3D 0A 00 73 F1 3C 00 74 04 0C 30 *JN30= s0< t000
000000510: 88 04 5A 59 C3 B8 20 00 8E D8 B8 00 F0 8E C0 26 *ZYA, 00 0000
000000520: A0 FE FF BA 00 00 B4 09 CD 21 BA 0F 00 3C FF 74 py0 '0i100 <y
000000530: 31 BA 14 00 3C FE 74 2A 3C FB 74 26 BA 2A 00 3C 100 <pt*00t000 <
000000540: FC 74 1F BA 1C 00 3C FA 74 18 BA 41 00 3C F8 74 000000550: 11 BA 4F 00 3C FD 74 0A BA 56 00 3C F9 75 00 E8 000000560: 5E FF B4 09 CD 21 BA 67 00 B4 09 CD 21 B4 30 CD 000000570: 21 3C 00 75 07 BA 76 00 B4 09 CD 21 BE 7D 00 83 000000580: C6 01 E8 6D FF 83 C6 04 8A C4 E8 65 FF BA 7D 00 000000590: B4 09 CD 21 B4 30 CD 21 BA 85 00 B4 09 CD 21 BA 0000005A0: C7 E8 4E FF BA 14 B4 02 CD 21 BA 54 01 CD 21 BA 0000005B0: 54 02 CD 21 B4 30 CD 21 BA 9E 00 B4 09 CD 21 BA 0000005C0: C3 E8 FC FE 8A C5 E8 F7 FE 8A C1 E8 F2 FE 32 C0 0000005D0: B4 4C CD 21 0000005E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

Рисунок 6 – LR1_EXE.EXE в шестнадцатеричном виде.