

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

Гордиенко А.М.

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.

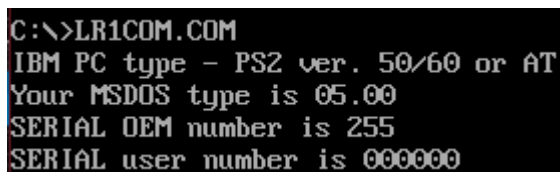
Далее необходимо отладить полученный исходный модуль и получить “хороший” .com модуль, а также необходимо построить “плохой” .exe, полученный из исходного текста для .com модуля.

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:\>LR1COM.COM
IBM PC type - PS2 ver. 50/60 or AT
Your MSDOS type is 05.00
SERIAL OEM number is 255
SERIAL user number is 000000
```

Рисунок 1 - Результат работы lr1com.com

```

C:\>LR1COM.EXE

        00000000 IBM PC type -

        00000000 IBM PC type -

        00000000 IBM PC type - 5 0

        00000000 IBM PC type - 255

        00000000 IBM PC type - 000000

```

Рисунок 2 - Результат lr1com.exe

```

C:\>LR1EXE.EXE
IBM PC type - PS2 ver. 50/60 or AT
Your MSDOS type is 05.00
SERIAL OEM number is 255
SERIAL user number is 000000

```

Рисунок 3 - Результат работы lr1exe.exe

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

0000000000: E9 0E 01 49 42 4D 20 50	43 20 74 79 70 65 20 2D	0000000000: IBM PC type -
0000000010: 20 24 50 43 0A 0D 24 50	43 2F 58 54 0A 0D 24 50	0000000010: PC/XT/PS2
0000000020: 53 32 20 76 65 72 2E 20	33 30 0A 0D 24 50 53 32	0000000020: S2 ver. 30/PS2
0000000030: 20 76 65 72 2E 20 35 30	2F 36 30 20 6F 72 20 41	0000000030: ver. 50/60 or A
0000000040: 54 0A 0D 24 50 53 32 20	76 65 72 2E 20 38 30 0A	0000000040: T/PS2 ver. 80/
0000000050: 0D 24 50 43 6A 72 0A 0D	24 50 43 20 43 6F 6E 76	0000000050: PCjr/PC Conv
0000000060: 65 72 74 69 62 6C 65 0A	0D 24 59 6F 75 72 20 4D	0000000060: ertible/Your M
0000000070: 53 44 4F 53 20 74 79 70	65 20 69 73 20 24 3C 32	0000000070: SDOS type is \$<2
0000000080: 2E 30 0A 0D 24 30 78 2E	30 79 0A 0D 24 53 45 52	0000000080: .00/\$0x.0y/\$SER
0000000090: 49 41 4C 20 4F 45 4D 20	6E 75 6D 62 65 72 20 69	0000000090: IAL OEM number i
00000000A0: 73 20 24 0A 0D 53 45 52	49 41 4C 20 75 73 65 72	00000000A0: s \$/SERIAL user
00000000B0: 20 6E 75 6D 62 65 72 20	69 73 20 24 51 52 E8 1C	00000000B0: number is \$QRèL
00000000C0: 00 8A EC 8A D0 B4 02 CD	21 8A D5 B4 02 CD 21 5A	00000000C0: ŠiŠD'ŃiŠD'ŃiZ
00000000D0: 59 C3 24 0F 3C 09 76 02	04 07 04 30 C3 51 8A E0	00000000D0: YÁ\$<ov0♦♦0AQŠā
00000000E0: E8 EF FF 86 C4 B1 04 D2	E8 E8 E6 FF 59 C3 51 52	00000000E0: èiÿrÄ±♦0èèÿYÄQR
00000000F0: 32 E4 33 D2 B9 0A 00 F7	F1 80 CA 30 88 14 4E 33	00000000F0: 2ā3D¹ ÷ñ€E0`JN3
0000000100: D2 3D 0A 00 73 F1 3C 00	74 04 0C 30 88 04 5A 59	0000000100: 0= sñ< t♦90♦ZY
0000000110: C3 B8 00 F0 8E C0 26 A0	FE FF BA 03 01 B4 09 CD	0000000110: Ā, ðŽÀ& þÿ♥°'oÍ
0000000120: 21 BA 12 01 3C FF 74 31	BA 17 01 3C FE 74 2A 3C	0000000120: !°†0<ÿt1°±0<pt* <
0000000130: FB 74 26 BA 2D 01 3C FC	74 1F BA 1F 01 3C FA 74	0000000130: út&°-0<üt°°<út
0000000140: 18 BA 44 01 3C F8 74 11	BA 52 01 3C FD 74 0A BA	0000000140: †°D0<øt°°R0<ýt°°
0000000150: 59 01 3C F9 75 00 E8 63	FF B4 09 CD 21 BA 6A 01	0000000150: Y0<uu ècÿ'°Í!°j0
0000000160: B4 09 CD 21 B4 30 CD 21	3C 00 75 07 BA 7E 01 B4	0000000160: '°Í! '°Í!< u°°~°
0000000170: 09 CD 21 BE 85 01 83 C6	01 E8 72 FF 83 C6 04 8A	0000000170: oÍ!X..0fA0èrÿfA♦Š
0000000180: C4 E8 6A FF BA 85 01 B4	09 CD 21 B4 30 CD 21 BA	0000000180: Åèjÿ°..0'°Í! '°Í!°
0000000190: 8D 01 B4 09 CD 21 8A C7	E8 53 FF 8A 14 B4 02 CD	0000000190: 00'°Í!ŠÇèÿŠÿ'°Í
00000001A0: 21 8A 54 01 CD 21 8A 54	02 CD 21 B4 30 CD 21 BA	00000001A0: !ŠT0Í!ŠT0Í! '°Í!°
00000001B0: A3 01 B4 09 CD 21 8A C3	E8 01 FF 8A C5 E8 FC FE	00000001B0: f0'°Í!ŠÀèÿŠÀèÿb
00000001C0: 8A C1 E8 F7 FE 32 C0 B4	4C CD 21	00000001C0: ŠÀè±þ2A`LÍ!

Рисунок 4 – lr1com.com в шестнадцатеричном виде.

0000000000: 4D 5A CB 06 03 00 00 00 00	20 00 00 00 FF FF 00 00	MZE ♥	yy
0000000010: 00 00 A4 0F 00 01 00 00 00	1E 00 00 00 01 00 00 00	Re @ ▲	0
0000000020: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000030: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000040: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000050: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000060: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000070: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000080: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000090: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000000A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000000B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000000C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000000D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000000E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000000F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000100: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000110: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000120: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000130: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000140: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000150: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000160: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000170: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000180: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000190: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000001A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000001B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000001C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000001D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000001E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000001F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000200: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000210: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000220: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000230: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000240: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000250: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000260: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000270: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000280: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000290: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000002A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000002B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000002C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000002D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00000002F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000000300: E9 0E 01 49 42 4D 20 50	43 20 74 79 70 65 20 2D	éIBM PC type -	
0000000310: 20 24 50 43 0A 0D 24 50	43 2F 58 54 0A 0D 24 50	\$PC\$PC/XT\$P	
0000000320: 53 32 20 76 65 72 2E 20	33 30 0A 0D 24 50 53 32	S2 ver. 30\$PS2	
0000000330: 20 76 65 72 2E 20 35 30	2F 36 30 20 6F 72 20 41	ver. 50/60 or A	
0000000340: 54 0A 0D 24 50 53 32 20	76 65 72 2E 20 38 30 0A	T\$PS2 ver. 80\$	
0000000350: 0D 24 50 43 6A 72 0A 0D	24 50 43 20 43 6F 6E 76	\$PCjr\$PC Conv	
0000000360: 65 72 74 69 62 6C 65 0A	0D 24 59 6F 75 72 20 4D	ertible\$Your M	
0000000370: 53 44 4F 53 20 74 79 70	65 20 69 73 20 24 3C 32	SDOS type is \$<	
0000000380: 2E 30 0A 0D 24 30 78 2E	30 79 0A 0D 24 53 45 52	.0\$0x.0y\$SER	
0000000390: 49 41 4C 20 4F 45 4D 20	6E 75 6D 62 65 72 20 69	IAL OEM number i	
00000003A0: 73 20 24 0A 0D 53 45 52	49 41 4C 20 75 73 65 72	s \$SERIAL user	
00000003B0: 20 6E 75 6D 62 65 72 20	69 73 20 24 51 52 E8 1C	number is \$QR&	
00000003C0: 09 8A EC 8A 0D B4 02 CD	21 8A D5 B4 02 CD 21 5A	ŠiŠD oŠiŠD oŠiZ	
00000003D0: 59 C3 24 0F 3C 09 76 02	0A 07 0A 30 C3 51 8A E0	YĂ\$<ov0\$+0AQŠ	
00000003E0: E8 EF FF 86 C4 B1 04 D2	E8 E8 E6 FF 59 C3 51 52	ëÿtA+0ëëëYVAQR	
00000003F0: 32 E4 33 D2 B9 0A 00 F7	F1 80 CA 30 88 14 4E 33	2ă30Š :nëE0ŠN3	
0000000400: D2 3D 0A 00 73 F1 3C 00	74 04 0C 30 88 04 5A 59	0= sŋ< t00ŠZy	
0000000410: C3 B8 00 F0 8E C0 26 A0	FE FF BA 03 01 B4 09 CD	Â, đŽ&Šÿ\$0Šof	
0000000420: 21 BA 12 01 3C FF 74 31	BA 17 01 3C FE 74 2A 3C	!00Šyt100Špt*<	
0000000430: FB 74 26 B4 2D 01 3C FC	74 1F BA 1F 01 3C FA 74	ŭt0Š<0ŭtŷ0Šŭt	
0000000440: 18 BA 44 01 3C F8 74 11	BA 52 01 3C FD 74 0A BA	ŭtD0Št0ŠR0Šyt0Š	
0000000450: 59 01 3C F9 75 00 E8 63	FF B4 09 CD 21 BA 6A 01	Y0ŠŭŠŠŠŠŠŠŠŠŠŠŠ	
0000000460: B4 09 CD 21 B4 30 CD 21	3C 00 75 07 BA 7E 01 B4	ŠofŠŠŠŠŠŠŠŠŠŠŠ	
0000000470: 09 CD 21 BE 85 01 83 C6	01 E8 72 FF 83 C6 04 8A	oŠŠŠŠŠŠŠŠŠŠŠŠŠ	
0000000480: CA E8 6A FF BA 85 01 B4	09 CD 21 B4 30 CD 21 BA	ŠëÿŷŠŠŠŠŠŠŠŠŠŠ	
0000000490: 8D 01 B4 09 CD 21 8A C7	E8 53 FF 8A 14 B4 02 CD	0ŠŠŠŠŠŠŠŠŠŠŠŠŠ	
00000004A0: 21 8A 54 01 CD 21 8A 54	02 CD 21 B4 30 CD 21 BA	ŠŠŠŠŠŠŠŠŠŠŠŠŠ	
00000004B0: A3 01 B4 09 CD 21 8A C3	E8 01 FF 8A C5 E8 FC FE	ŠŠŠŠŠŠŠŠŠŠŠŠŠ	
00000004C0: 8A C1 E8 F7 FE 32 C0 B4	4C CD 21	ŠŠŠŠŠŠŠŠŠŠŠŠŠ	

Рисунок 5 – lr1com.exe в шестнадцатеричном виде.

0000000000: 4D 5A D4 01 03 00 01 00	20 00 00 00 FF FF 00 00	MZ00 00 00 00 00 00 00 00
0000000010: 00 02 DC D6 55 00 2C 00	1E 00 00 00 01 00 56 00	0000 00 00 00 00 00 00 00
0000000020: 2C 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000030: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000040: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000050: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000060: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000070: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000080: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000090: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000100: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000110: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000120: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000130: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000140: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000150: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000160: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000170: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000180: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000190: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000200: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000210: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000220: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000230: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000240: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000250: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000260: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000270: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000280: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000290: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000300: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000310: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000320: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000330: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000340: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000350: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000360: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000370: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000380: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000390: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000400: 49 42 4D 20 50 43 20 74	79 70 65 20 2D 20 24 50	IBM PC type - \$P
0000000410: 43 0A 0D 24 50 43 2F 58	54 0A 0D 24 50 53 32 20	CM \$PC/XT \$PS2
0000000420: 76 65 72 2E 20 33 30 0A	0D 24 50 53 32 20 76 65	ver. 30 \$PS2 ve
0000000430: 72 2E 20 35 30 2F 36 30	20 6F 72 20 41 54 0A 0D	r. 50/60 or AT
0000000440: 24 50 53 32 20 76 65 72	2E 20 38 30 0A 0D 24 50	\$PS2 ver. 80 \$P
0000000450: 43 6A 72 0A 0D 24 50 43	20 43 6F 6E 76 65 72 74	Cjr \$PC Convert
0000000460: 69 62 6C 65 0A 0D 24 59	6F 75 72 20 4D 53 44 4F	ible \$Your MSDO
0000000470: 53 20 74 79 70 65 20 69	73 20 24 3C 32 2E 30 0A	S type is \$<2.0
0000000480: 0D 24 30 78 2E 30 79 0A	0D 24 53 45 52 49 41 4C	\$0x.0y \$SERIAL
0000000490: 20 4F 45 4D 20 6E 75 6D	62 65 72 20 69 73 20 24	OEM number is \$
00000004A0: 0A 0D 53 45 52 49 41 4C	20 75 73 65 72 20 6E 75	\$SERIAL user nu
00000004B0: 6D 62 65 72 20 69 73 20	24 00 00 00 00 00 00 00	mber is \$
00000004C0: 51 52 E8 1C 00 8A EC 8A	D0 B4 02 CD 21 8A D5 B4	QReL SiSD 0iIS0
00000004D0: 02 CD 21 5A 59 C3 24 0F	3C 09 76 02 04 07 04 30	0iIZYA0<ov000
00000004E0: C3 51 8A E0 E8 EF FF 86	C4 B1 04 D2 E8 E8 E6 FF	AQSa0iYtA00000
00000004F0: 59 C3 51 52 32 E4 33 D2	B9 0A 00 F7 F1 80 CA 30	YAQR2030000
0000000500: 88 14 4E 33 D2 3D 0A 00	73 F1 3C 00 74 04 0C 30	00N30000 s0< t000
0000000510: 88 04 5A 59 C3 B8 20 00	8E D8 B8 00 F0 8E C0 26	00ZYA 00 00 00 00 00 00
0000000520: A0 FE FF BA 00 00 B4 09	CD 21 BA 0F 00 3C FF 74	0000 00 00 00 00 00 00 00
0000000530: 31 BA 14 00 3C FE 74 2A	3C FB 74 26 BA 2A 00 3C	1000 <pt*<ut&0* <
0000000540: FC 74 1F BA 1C 00 3C FA	74 18 BA 41 00 3C F8 74	ut00L <ut0A <0t
0000000550: 11 BA 4F 00 3C FD 74 0A	BA 56 00 3C F9 75 00 E8	000 <y00V <uu 0
0000000560: 5E FF B4 09 CD 21 BA 67	00 B4 09 CD 21 B4 30 CD	0000 00 00 00 00 00 00 00
0000000570: 21 3C 00 75 07 BA 7B 00	B4 09 CD 21 BE 82 00 83	0000 00 00 00 00 00 00 00
0000000580: C6 01 E8 6D FF 83 C6 04	8A C4 E8 65 FF BA 82 00	0000 00 00 00 00 00 00 00
0000000590: B4 09 CD 21 B4 30 CD 21	BA 8A 00 B4 09 CD 21 8A	0000 00 00 00 00 00 00 00
00000005A0: C7 E8 4E FF 8A 14 B4 02	CD 21 8A 54 01 CD 21 8A	0000 00 00 00 00 00 00 00
00000005B0: 54 02 CD 21 B4 30 CD 21	BA A0 00 B4 09 CD 21 8A	0000 00 00 00 00 00 00 00
00000005C0: C3 E8 FC FE 8A C5 E8 F7	FE 8A C1 E8 F2 FE 32 C0	0000 00 00 00 00 00 00 00
00000005D0: B4 4C CD 21		0000 00 00 00 00 00 00 00

Рисунок 6 – lr1ex.exe в шестнадцатеричном виде.

Рассмотреть файлы модулей .com и .exe можно в отладчике.

[CPU 80486]				1=[↑][↓]	
cs:0100	E90E01	jmp	0211 ↓	ax	0000 c=0
cs:0103	49	dec	cx	bx	0000 z=0
cs:0104	42	inc	dx	cx	0000 s=0
cs:0105	4D	dec	bp	dx	0000 o=0
cs:0106	205043	and	[bx+si+43],dl	si	0000 p=0
cs:0109	207479	and	[si+79],dh	di	0000 a=0
cs:010C	7065	jo	0173	bp	0000 i=1
cs:010E	202D	and	[dil,ch	sp	FFFE d=0
cs:0110	2024	and	[sil,ah	ds	489D
cs:0112	50	push	ax	es	489D
cs:0113	43	inc	bx	ss	489D
cs:0114	0A0D	or	cl,[dil	cs	489D
cs:0116	2450	and	al,50	ip	0100
ds:0000 CD 20 FF 9F 00 EA FF FF = f Ω				ss:0000 20CD	
ds:0008 AD DE E0 01 C5 15 AA 01 i xΩ S-Ω				ss:FFFE 0000	
ds:0010 C5 15 89 02 20 10 92 01 +SeΩ >ffΩ					
ds:0018 01 01 01 00 02 FF FF FF ΩΩΩ Ω					

Рисунок 7 – lrlcom.com в td.exe отладчике.

[CPU 80486]				1=[↑][↓]	
cs:0055	B8CD48	mov	ax,48CD	ax	0000 c=0
cs:0058	8ED8	mov	ds,ax	bx	0000 z=0
cs:005A	B800F0	mov	ax,F000	cx	0000 s=0
cs:005D	8EC0	mov	es,ax	dx	0000 o=0
cs:005F	26A0FEFF	mov	al,es:[FFFE]	si	0000 p=0
cs:0063	BA0000	mov	dx,0000	di	0000 a=0
cs:0066	B409	mov	ah,09	bp	0000 i=1
cs:0068	CD21	int	21	sp	0200 d=0
cs:006A	BA0F00	mov	dx,000F	ds	489D
cs:006D	3CFF	cmp	al,FF	es	489D
cs:006F	7431	je	00A2	ss	48AD
cs:0071	BA1400	mov	dx,0014	cs	48D9
cs:0074	3CFE	cmp	al,FE	ip	0055
ds:0000 CD 20 FF 9F 00 EA FF FF = f Ω				ss:0202 204D	
ds:0008 AD DE E0 01 C5 15 AA 01 i xΩ S-Ω				ss:0200 4249	
ds:0010 C5 15 89 02 20 10 92 01 +SeΩ >ffΩ					
ds:0018 01 01 01 00 02 FF FF FF ΩΩΩ Ω					

Рисунок 8 – lrl.exe в td.exe отладчике.

Контрольные вопросы.

Отличие исходных текстов com и exe программ:

1. Сколько сегментов должна содержать com-программа?

Представляет собой один сегмент и его размер не превышает 64кб памяти, ровно как размер одного сегмента.

2. ... exe-программа

Сама exe-программа на уровень сложнее com-программы ввиду того, что может содержать несколько сегментов: сегмент кода, сегмент стека, и несколько сегментов данных.

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

Assume для установления соответствующих сегментных регистров. Org 100h для установки смещения в psp, то есть резервирует память под psp.

4. Все ли форматы команд можно использовать в com-программе.

Нельзя использовать сегментные регистры. И ограничение по памяти: код и данные меньше 64кб должны занимать.

Отличие форматов файлов com и exe модулей:

1. Какова структура файла com? С какого адреса располагается код?

Располагается по адресу 0h и состоит из одного сегмента.

2. Какова структура файла “плохого” exe? С какого адреса располагается код? Что располагается с адреса 0?

Плохой exe состоит из одного сегмента и начинается с настроек, затем psp, затем уже код. Расположение кода можно посмотреть в бинарном представлении программы. Видно, что начало кода расположено по адресу 0300h. А с адреса 0h расположена таблица настроек, с адреса 0200h расположен psp размера 100h, по адресу 300h опять же - код.

3. Какова структура файла “хорошего” exe? Чем он отличается от файла “плохого” exe?

“Хороший” exe теперь имеет три сегмента. Код смещен на величину 100h, то есть на размер сегмента стека, и теперь расположен по адресу 0400h.

Загрузка com модуля в основную память:

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

Код расположен с адреса 100h, так как перед ним расположен psp такого размера.

2. Что располагается с адреса 0h?

Psp, так как мы в начале программы выделяем под него память.

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

Значение регистров можно посмотреть в TD отладчике. Регистры указывают на адреса 489Dh.

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

Стек расположен в конце основного сегмента. SP указывает на FFFEh, а в самом стеке лежит адрес возврата(0000h).

Загрузка “хорошего” exe модуля в основную память:

1. Как загружается “хороший” exe? Какие значения имеют сегментные регистры?

SS - начало стека, DS - начало psp, CS - сегмент кода соответственно. SS = 0200h, DS = 489Dh, CS = 48D9h, ES = 489Dh.

2. На что указывают регистры DS и ES?

Оба имеют значение 489Dh и указывают на psp.

3. Как определяется стек?

При использовании директивы assume значению ss присваивается значение начала сегмента стека.

4. Как определяется точка входа?

Exe-программа может содержать несколько функций, и ,чтобы определить, с какой должна начать выполняться работа, применяется директива END func, где func - метка, с которой программа должна начинать работу.

Выводы.

В ходе работы были получены навыки по созданию и работе с com и exe файлами. Были реализованы программы, определяющие тип РС, а также версию системы.