

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. 9384

Прашутинский К.И.

Преподаватель

Ефремов М.А.

Санкт-Петербург

2021

Постановка задачи.

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

Название процедуры	Предназначение процедуры
TETR_TO_HEX	Переводит значение тетрады (4-ех младших битов регистра AL) в цифру 16-ичной СС и представляет ее в виде символа, который далее записывается в регистр AL.
BYTE_TO_HEX	Переводит значение байта (регистра AL) в число 16ичной СС и представляет его в виде двух символов, которые далее записываются в регистры AL и AH.
WRD_TO_HEX	Переводит значение слова (регистра AX) в число 16ичной СС и представляет его в виде четырех символов, которые далее записываются по адресу, на который указывает DI.
BYTE_TO_DEC	Переводит значение байта (регистра AL) в число 10ичной СС и представляет его в виде символов, которые далее записываются по адресу, на который указывает SI.
PRINT	Вызывает функцию вывода строки на экран (функция 09h прерывания 21h).
PC_TYPE	Печатает на экран тип ПК. Если версия ПК не идентифицирована, выводится байт в 16-ичной СС, который содержит информацию о типе ПК.
PC_VERSION	Печатает на экран версию ОС, серийные номера OEM и пользователя.

Последовательность действий программы.

1)Вызывается процедура PC_TYPE, которая выводит на экран тип ПК. Информация о типе ПК получается из предпоследнего байта ROM BIOS по адресу 0F000:0FFFFh. В зависимости от значения байта определяется тип:

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

В случае, если значение не совпадает со значениями, приведенными выше, то в качестве типа ПК выводится значения предпоследнего байта ROM BIOS.

2)Вызывается процедура PC_VERSION, которая выводит на экран версию ОС, серийные номера OEM и пользователя. Информация получается при помощи вызова функции 30h прерывания 21h.

3)Завершение работы программы.

Ход работы.

1. Для начала был написан текст исходного .COM модуля lab1_com.asm. Далее при помощи транслятора TASM.EXE и компоновщика TLINK.EXE был скомпилирован «хороший» .COM и «плохой» .EXE модуль lab1_com.exe.
2. Отладил «плохой» .EXE модуль и по нему построил «хороший» .EXE модуль
3. Сравнил исходные тексты lab1_com.asm и lab1_exe.asm.
4. После при помощи программы FAR были открыты файлы загрузочных модулей lb1_COM.com, lb1_EXE.exe и lb1_COM.exe в шестнадцатеричном виде, далее было выполнено сравнение.
5. Далее был исследован загрузочный модуль .COM при помощи отладчика TD.EXE.

6. Далее был исследован «хороший» загрузочный модуль .EXE при помощи отладчика TD.EXE.

Результаты исследования проблем.

План загрузки модуля .COM в основную память.

1. Определяется сегментный адрес свободного участка основной памяти для загрузки программы.
2. Для программы формируется блок PSP и загружается в начало.
3. После блока PSP по адресу PSP:0100h загружается COM модуль.

После загрузки COM-программы в основную память CS, DS, ES и SS указывают на PSP, SP указывает на конец сегмента PSP, слово 00h помещено на стек, IP имеет значение 100h.

Контрольные вопросы.

Отличия исходных текстов COM и EXE программ.

1. Сколько сегментов должна содержать COM-программа?

Только один сегмент

2. Сколько сегментов должна содержать EXE-программа?

Один или более сегментов.

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

Директива ORG. В начальной части COM-программы размещается специальный блок PSP (префикс программного сегмента), в начале которого размещена команда вызова обработчика прерывания для завершения программы и возврата в DOS. Так как после загрузки все сегментные регистры, включая CS, указывают на начало PSP, а IP = 0, то программа не может исполняться, начиная с этого адреса. Поэтому требуется директива ORG 100h, которая установит CS:IP на конец PSP (размер PSP равен 256 байт, значит сдвиг нужно делать на $256 = 100h$ байт).

Директива ASSUME. Указывает ассемблеру, с каким сегментом или группой сегментов связан тот или иной сегментный регистр. Она не

изменяет значений сегментных регистров, а только позволяет ассемблеру проверять допустимость ссылок и самостоятельно вставлять при необходимости префиксы переопределения сегментов. Без этой директивы программа не скомпилируется, так как ассемблер не будет понимать, относительно чего вычислять смещения меток.

Директива END. Этой директивой завершается любая программа на ассемблере.

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

Нет. Поскольку в COM-программе отсутствует таблица настройки, использование таких форматов команд не доступно: `seg NAME`, где NAME – название сегмента.

Отличия форматов файлов COM и EXE модулей.

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

В COM-файле код, данные и стек располагаются в одном сегменте. Код (как и данные) начинается с адреса 0h. Файл в 16-ичном представлении расположен снизу.

0000000000: E9 FC 01 50 43 20 74 79	70 65 3A 20 24 50 43 0D	éü@PC type: \$PC
0000000010: 0A 24 50 43 2F 58 54 0D	0A 24 41 54 0D 0A 24 50	\$PC/XT\$AT\$P
0000000020: 53 32 20 6D 6F 64 65 6C	20 33 30 0D 0A 24 50 53	S2 model 30\$PS
0000000030: 32 20 6D 6F 64 65 6C 20	35 30 20 6F 72 20 36 30	2 model 50 or 60
0000000040: 0D 0A 24 50 53 32 20 6D	6F 64 65 6C 20 38 30 0D	\$PS2 model 80
0000000050: 0A 24 50 43 6A 72 0D 0A	24 50 43 20 43 6F 6E 76	\$PCjr\$PC Conv
0000000060: 65 72 74 69 62 6C 65 0D	0A 24 20 20 0D 0A 24 4F	ertible\$ \$0
0000000070: 53 20 76 65 72 73 69 6F	6E 3A 20 24 20 20 2E 20	S version: \$.
0000000080: 20 0D 0A 24 4F 45 4D 20	73 65 72 69 61 6C 20 6E	\$OEM serial n
0000000090: 75 6D 62 65 72 3A 20 24	20 20 0D 0A 24 55 73 65	umber: \$ \$Use
00000000A0: 72 20 73 65 72 69 61 6C	20 6E 75 6D 62 65 72 3A	r serial number:
00000000B0: 20 24 20 20 20 20 20 20	0D 0A 24 24 0F 3C 09 76	\$ \$<ov
00000000C0: 02 04 07 04 30 C3 51 8A	E0 E8 EF FF 86 C4 B1 04	♦♦♦0ÄQŠaëiÿ†Ä±♦
00000000D0: D2 E8 E8 E6 FF 59 C3 53	8A FC E8 E9 FF 88 25 4F	ðèæÿYÄSŠüèéÿ`%0
00000000E0: 88 05 4F 8A C7 E8 DE FF	88 25 4F 88 05 5B C3 51	^+0ŠCèbÿ`%0^+[\ÄQ
00000000F0: 52 32 E4 33 D2 B9 0A 00	F7 F1 80 CA 30 88 14 4E	R2ä30¹ ÷ñ€Ê0`JN
0000000100: 33 D2 3D 0A 00 73 F1 3C	00 74 04 0C 30 88 04 5A	3ð= sñ< t♦90♦Z
0000000110: 59 C3 50 B4 09 CD 21 58	C3 50 53 52 06 B8 00 F0	YÄP´oÍ!XÄPSR♦. ð
0000000120: 8E C0 26 A0 FE FF BA 03	01 E8 E6 FF 3C FF 74 23	ŽÀ& þÿ°▼0èæÿ<ÿt#
0000000130: 3C FE 74 25 3C FD 74 21	3C FC 74 23 3C FA 74 25	<þt%<ÿt!<üt#<út%
0000000140: 3C FC 74 27 3C F8 74 29	3C FD 74 2B 3C F9 74 2D	<üt'<øt)<ÿt+<üt-
0000000150: EB 31 90 BA 0D 01 EB 38	90 BA 12 01 EB 32 90 BA	ë1000è800†0ë200
0000000160: 1A 01 EB 2C 90 BA 1F 01	EB 26 90 BA 2E 01 EB 20	→0ë,00▼0ë&00.0ë
0000000170: 90 BA 43 01 EB 1A 90 BA	52 01 EB 14 90 BA 59 01	00C0ë→00R0ëJ00Y0
0000000180: EB 0E 90 E8 40 FF BB 6A	01 88 07 88 67 01 8B D3	ë00è0ÿ»j0~•^g0<Ó
0000000190: E8 7F FF 07 5A 5B 58 C3	50 53 51 52 56 57 B4 30	è0ÿ•Z[XÄPSQRVW´0
00000001A0: CD 21 BE 7D 01 8A D4 E8	45 FF 8A C2 83 C6 03 E8	Í!%}0Š0èEÿŠÄfA♥è
00000001B0: 3D FF BA 6F 01 E8 5A FF	BA 7C 01 E8 54 FF 8A C7	=ÿ°00èZÿ° 0èTÿŠC
00000001C0: E8 03 FF BF 98 01 88 05	88 65 01 BA 84 01 E8 41	è♥ÿ¿~0^+^e00,,0èA
00000001D0: FF BA 98 01 E8 3B FF 8A	C3 E8 EA FE BF B2 01 88	ÿ°~0è;ÿŠÄèèþ¿²0^
00000001E0: 05 88 65 01 8B C1 83 C7	05 E8 EB FE BA 9D 01 E8	♦^e0<ÄfÇ♦èèþ000è
00000001F0: 20 FF BA B2 01 E8 1A FF	5F 5E 5A 59 5B 58 C3 E8	ÿ°²0è→ÿ_^ZY[XÄè
0000000200: 17 FF E8 93 FF 32 C0 B4	4C CD 21	‡ÿè“ÿ2Ä`LÍ!

2. Какова структура файла «плохого» EXE? С какого адреса располагается код? Что располагается с адреса 0?

В плохом EXE-файле код, данные и стек располагаются в одном сегменте. Код (как и данные) начинается с адреса 300h. С адреса 0h располагается управляющая информация для загрузчика, которая содержит заголовок и таблицу настройки адресов. Файл в 16-ичном представлении расположен снизу.

[illegible]

00000000300:	E9 FC 01 50 43 20 74 79	70 65 3A 20 24 50 43 0D	éüPC type: \$PC
00000000310:	0A 24 50 43 2F 58 54 0D	0A 24 41 54 0D 0A 24 50	\$PC/XT.\$AT.\$P
00000000320:	53 32 20 6D 6F 64 65 6C	20 33 30 0D 0A 24 50 53	S2 model 30.\$PS
00000000330:	32 20 6D 6F 64 65 6C 20	35 30 20 6F 72 20 36 30	2 model 50 or 60
00000000340:	0D 0A 24 50 53 32 20 6D	6F 64 65 6C 20 38 30 0D	.\$PS2 model 80
00000000350:	0A 24 50 43 6A 72 0D 0A	24 50 43 20 43 6F 6E 76	\$PCjr.\$PC Conv
00000000360:	65 72 74 69 62 6C 65 0D	0A 24 20 20 0D 0A 24 4F	ertible.\$ \$0
00000000370:	53 20 76 65 72 73 69 6F	6E 3A 20 24 20 20 2E 20	S version: \$.
00000000380:	20 0D 0A 24 4F 45 4D 20	73 65 72 69 61 6C 20 6E	.\$OEM serial n
00000000390:	75 6D 62 65 72 3A 20 24	20 20 0D 0A 24 55 73 65	umber: \$.\$Use
000000003A0:	72 20 73 65 72 69 61 6C	20 6E 75 6D 62 65 72 3A	r serial number:
000000003B0:	20 24 20 20 20 20 20 20	0D 0A 24 24 0F 3C 09 76	\$.\$\$<ov
000000003C0:	02 04 07 04 30 C3 51 8A	E0 E8 EF FF 86 C4 B1 04	0♦♦0ÄQ\$æëÿtÄ+♦
000000003D0:	D2 E8 E8 E6 FF 59 C3 53	8A FC E8 E9 FF 88 25 4F	0ëæÿYÄS\$üëéÿ"%0
000000003E0:	88 05 4F 8A C7 E8 DE FF	88 25 4F 88 05 5B C3 51	^+0\$Càþÿ"%0+^[ÄQ
000000003F0:	52 32 E4 33 D2 B9 0A 00	F7 F1 80 CA 30 88 14 4E	R2ä30¹ ÷ñëÊ0`JN
00000000400:	33 D2 3D 0A 00 73 F1 3C	00 74 04 0C 30 88 04 5A	30= sñ< t♦00`Z
00000000410:	59 C3 50 B4 09 CD 21 58	C3 50 53 52 06 B8 00 F0	YÄP´oÍ!XÄPSR^, ð
00000000420:	8E C0 26 A0 FE FF BA 03	01 E8 E6 FF 3C FF 74 23	Ž& þÿ♥0æÿ<ÿt#
00000000430:	3C FE 74 25 3C FD 74 21	3C FC 74 23 3C FA 74 25	<þt%<ÿt!<üt#<üt%
00000000440:	3C FC 74 27 3C F8 74 29	3C FD 74 2B 3C F9 74 2D	<üt'<øt)<ÿt+<üt-
00000000450:	EB 31 90 BA 0D 01 EB 38	90 BA 12 01 EB 32 90 BA	ë100.00ë8000\$0ë200
00000000460:	1A 01 EB 2C 90 BA 1F 01	EB 26 90 BA 2E 01 EB 20	→0ë,00▼0ë&00.0ë
00000000470:	90 BA 43 01 EB 1A 90 BA	52 01 EB 14 90 BA 59 01	00C0ë→00R0ëJ00Y0
00000000480:	EB 0E 90 E8 40 FF BB 6A	01 88 07 88 67 01 8B D3	ëJ0ë0ÿj0`~`g0<Ó
00000000490:	E8 7F FF 07 5A 5B 58 C3	50 53 51 52 56 57 B4 30	è0ÿ•Z[XÄPSQRVW`0
000000004A0:	CD 21 BE 7D 01 8A D4 E8	45 FF 8A C2 83 C6 03 E8	Í!%}0\$0ëEÿ\$ÄfA♥è
000000004B0:	3D FF BA 6F 01 E8 5A FF	BA 7C 01 E8 54 FF 8A C7	=ÿ000èZÿ0 0èTÿ\$C
000000004C0:	E8 03 FF BF 98 01 88 05	88 65 01 BA 84 01 E8 41	èÿÿ~0`+`e00,,0èA
000000004D0:	FF BA 98 01 E8 3B FF 8A	C3 E8 EA FE BF B2 01 88	ÿ0`0è;ÿ\$Äèþÿ²0`
000000004E0:	05 88 65 01 8B C1 83 C7	05 E8 EB FE BA 9D 01 E8	+`e0<ÄfC+èëþ000è
000000004F0:	20 FF BA B2 01 E8 1A FF	5F 5E 5A 59 5B 58 C3 E8	ÿ0²0è→ÿ`^ZY[XÄè
00000000500:	17 FF E8 93 FF 32 C0 B4	4C CD 21	±ÿè“ÿ2Ä´LÍ!

```

70 65 3A 20 24 50 43 0D 00 PC type: $PC
0A 24 41 54 0D 0A 24 50 00 PC/XT $AT $P
20 33 30 0D 0A 24 50 53 S2 model 30 $PS
35 30 20 6F 72 20 36 30 2 model 50 or 60
6F 64 65 6C 20 38 30 0D $PS2 model 80
24 50 43 20 43 6F 6E 76 $PCjr $PC Conv
0A 24 20 20 0D 0A 24 4F ertible $ $0
6E 3A 20 24 20 20 2E 20 S version: $
73 65 72 69 61 6C 20 6E $OEM serial n
20 20 0D 0A 24 55 73 65 umber: $ $Use
20 6E 75 6D 62 65 72 3A r serial number:
0D 0A 24 24 0F 3C 09 76 $ $ $ <ov
E0 E8 EF FF 86 C4 B1 04 00 00 00 00 00 00 00 00 00
8A FC E8 E9 FF 88 25 4F 00 00 00 00 00 00 00 00
88 25 4F 88 05 5B C3 51 00 00 00 00 00 00 00 00
F7 F1 80 CA 30 88 14 4E 00 00 00 00 00 00 00 00
00 74 04 0C 30 88 04 5A 30 00 00 00 00 00 00
C3 50 53 52 06 B8 00 F0 YÄP 'oÍ!XÄPSRÄ. ð
01 E8 E6 FF 3C FF 74 23 ŽÄ& þÿ♥œäÿ<ÿt#
3C FC 74 23 3C FA 74 25 <þt%<ÿt!<üt#<út%
3C FD 74 2B 3C F9 74 2D <üt'<øt)<ÿt+<üt-
90 BA 12 01 EB 32 90 BA ë1 00 00 00 00 00 00 00
EB 26 90 BA 2E 01 EB 20 →0ë, 00♥0ë&00. 0ë
52 01 EB 14 90 BA 59 01 00C0ë→00R0ë 00Y0
01 88 07 88 67 01 8B D3 ë 00ë0ÿ»j0^•g0<0
50 53 51 52 56 57 B4 30 è0ÿ•Z[XÄPSQRVW'0
45 FF 8A C2 83 C6 03 E8 Í!%}0Š0ëEÿŠÄfA♥è
BA 7C 01 E8 54 FF 8A C7 =ÿ000ëZÿ|0ëTÿŠC
88 65 01 BA 84 01 E8 41 è♥ÿ;~0^+~e0,,0ëA
C3 E8 EA FE BF B2 01 88 ÿ~0ë;ÿŠÄëþ;20^
05 E8 EB FE BA 9D 01 E8 +^e0<ÄfC+ëëþ000ë
5F 5E 5A 59 5B 58 C3 E8 ÿ020ë→ÿ^ZY[XÄë
4C CD 21 ‡vë"v2Ä'ÍÍ!

```

3. Какова структура «хорошего» EXE? Чем он отличается от файла «плохого» EXE?

В хорошем EXE-файле код, данные и стек находятся в различных сегментах, а в плохом – в одном и том же сегменте. По мимо этого, изменен порядок расположения сегментов в памяти, и стек имеет другой размер – 256 байт (100h). Файл в 16-ичном представлении расположен снизу.

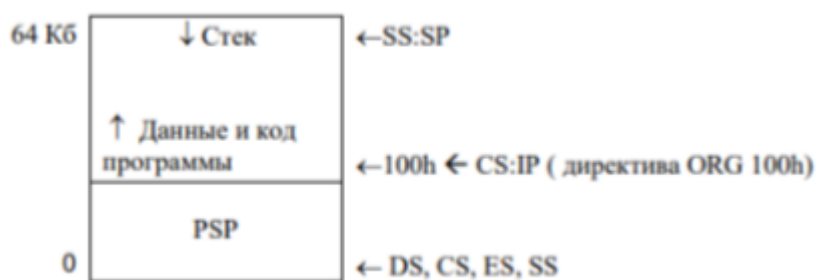
0000000000: 4D 5A 28 00 03 00 01 00	20 00 11 00 FF FF 23 00	MZ(♥ ☹ ◀ яя#
0000000010: 00 01 00 00 10 00 00 00	3E 00 00 00 01 00 FB 30	☹ ▶ > ☹ ы☹
0000000020: 6A 72 00 00 00 00 00 00	00 00 00 00 00 00 00 00	jr
0000000030: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 58 01	X☹
0000000040: 00 00 00 00 00 00 00 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: E9 44 01 24 0F 3C 09 76	02 04 07 04 30 C3 51 8A	йD@ \$о<ov☹♦♦♦0ГQ/ь
0000000220: E0 E8 EF FF 86 C4 B1 04	D2 E8 E8 E6 FF 59 C3 53	аипя†Д±♦ТиижяYGS
0000000230: 8A FC E8 E9 FF 88 25 4F	88 05 4F 8A C7 E8 DE FF	льийя€%O€+O/ь3и0я
0000000240: 88 25 4F 88 05 5B C3 51	52 32 E4 33 D2 B9 0A 00	€%O€+ [ГQR2д3TN☹
0000000250: F7 F1 80 CA 30 88 14 4E	33 D2 3D 0A 00 73 F1 3C	чсѣK0€ЎN3T=☹ sc<
0000000260: 00 74 04 0C 30 88 04 5A	59 C3 50 B4 09 CD 21 58	t♦90€♦ZYГроH!X
0000000270: C3 50 53 52 06 B8 00 F0	8E C0 26 A0 FE FF BA 00	ГPSR♦ё рѣA& юяе
0000000280: 00 E8 E6 FF 3C FF 74 23	3C FE 74 25 3C FD 74 21	иижя<ят#<ют%<эт!
0000000290: 3C FC 74 23 3C FA 74 25	3C FC 74 27 3C F8 74 29	<ьт#<ьт%<ьт'<шт)
00000002A0: 3C FD 74 2B 3C F9 74 2D	EB 31 90 BA 0A 00 EB 38	<эт+<шт-л1ђє☹ л8
00000002B0: 90 BA 0F 00 EB 32 90 BA	17 00 EB 2C 90 BA 1C 00	ђє♦ л2ђє\$ л,ђєL
00000002C0: EB 26 90 BA 2B 00 EB 20	90 BA 40 00 EB 1A 90 BA	л&ђє+ л ђє@ л→ђє
00000002D0: 4F 00 EB 14 90 BA 56 00	EB 0E 90 E8 40 FF BB 67	O лђђєV лђђи@я»g
00000002E0: 00 88 07 88 67 01 8B D3	E8 7F FF 07 5A 5B 58 C3	€•€g@<Уидя•Z[XГ
00000002F0: 50 53 51 52 56 57 B4 30	CD 21 BE 7A 00 8A D4 E8	PSQRVWr0H!sz /ьФи

0000000300:	45 FF 8A C2 83 C6 03 E8	3D FF BA 6C 00 E8 5A FF	ЕяЬВГЖЖи=яеl иЗя
0000000310:	BA 79 00 E8 54 FF 8A C7	E8 03 FF BF 95 00 88 05	еу иТяЬЗи♥яї• €♣
0000000320:	88 65 01 BA 81 00 E8 41	FF BA 95 00 E8 3B FF 8A	€е0€Г иАяе• и;яЬ
0000000330:	C3 E8 EA FE BF AF 00 88	05 88 65 01 8B C1 83 C7	Гикюїї €♣€е0<БГЗ
0000000340:	05 E8 EB FE BA 9A 00 E8	20 FF BA AF 00 E8 1A FF	♣илуеь и яеї и→я
0000000350:	5F 5E 5A 59 5B 58 C3 B8	17 00 8E D8 E8 12 FF E8	_ ^ZY[XГё± Ѓши±яи
0000000360:	8E FF 32 C0 B4 4C CD 21	00 00 00 00 00 00 00 00	Ѓя2ArLH!
0000000370:	50 43 20 74 79 70 65 3A	20 24 50 43 0D 0A 24 50	PC type: \$PCЉ\$P
0000000380:	43 2F 58 54 0D 0A 24 41	54 0D 0A 24 50 53 32 20	C/XTЉ\$ATЉ\$PS2
0000000390:	6D 6F 64 65 6C 20 33 30	0D 0A 24 50 53 32 20 6D	model 30Љ\$PS2 m
00000003A0:	6F 64 65 6C 20 35 30 20	6F 72 20 36 30 0D 0A 24	odel 50 or 60Љ\$
00000003B0:	50 53 32 20 6D 6F 64 65	6C 20 38 30 0D 0A 24 50	PS2 model 80Љ\$P
00000003C0:	43 6A 72 0D 0A 24 50 43	20 43 6F 6E 76 65 72 74	CjrЉ\$PC Convert
00000003D0:	69 62 6C 65 0D 0A 24 20	20 0D 0A 24 4F 53 20 76	ibleЉ\$ Љ\$OS v
00000003E0:	65 72 73 69 6F 6E 3A 20	24 20 20 2E 20 20 0D 0A	ersion: \$. Љ
00000003F0:	24 4F 45 4D 20 73 65 72	69 61 6C 20 6E 75 6D 62	\$OEM serial numb
0000000400:	65 72 3A 20 24 20 20 0D	0A 24 55 73 65 72 20 73	er: \$ Љ\$User s
0000000410:	65 72 69 61 6C 20 6E 75	6D 62 65 72 3A 20 24 20	erial number: \$
0000000420:	20 20 20 20 20 0D 0A 24		Љ\$

Загрузка COM модуля в основную память.

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

COM-модуль имеет следующую структуру:



Код располагается с адреса 100h, поскольку с адреса 0h располагается блок PSP размером 256 байт.

AX 0000	SI 0000	CS 119C	IP 0100
BX 0000	DI 0000	DS 119C	
CX 020B	BP 0000	ES 119C	HS 119C
DX 0000	SP FFF5	SS 119C	FS 119C

2. Что располагается с адреса 0?

Специальный блок PSP (префикс программного сегмента).

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

Регистры DS, ES, CS, SS указывают на начало блока PSP.

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

Регистр SS указывает на начало блока PSP (0h), а SP указывает на конец модуля (FFFFh). То есть стек расположен между адресами SS:0000h и SS:FFFFh и заполняется с конца модуля в сторону уменьшения адресов.

Загрузка «хорошего» EXE модуля в основную память.

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

Регистры DS и ES указывают на начало блока PSP, регистр CS указывает на начало сегмента кода, а регистр SS – на начало сегмента стека.

Структура выглядит следующим образом:



AX	0000	SI	0000	CS	11AC	IP	0010
BX	0000	DI	0000	DS	119C		
CX	0228	BP	0000	ES	119C	HS	119C
DX	0000	SP	0100	SS	11CF	FS	119C

2. На что указывают регистры DS и ES?

Регистры DS и ES указывают на начало блока PSP.

3. Как определяется стек?

Регистр SS указывает на начало сегмента стека, а SS:SP – на конец сегмента стека.

4. Как определяется точка входа?

Точка входа определяется параметром после директивы END, в качестве которого нужно передать метку, с которой программа начнет выполнение команд.

Выводы.

Были изучены различия в структурах исходных текстов модулей типов .COM и .EXE, структур файлов загрузочных модулей и способов их загрузки в основную память.