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. 9382	 Савельев И.С
Преподаватель	Ефремов М.А

Санкт-Петербург

Цель работы.

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

Задание.

Шаг 1. Напишите текст исходного .СОМ модуля, который определяет тип РС версию системы. Это довольно простая задача и для тех, кто уже имеет опыт программирования на ассемблере, это будет небольшой разминкой. Для тех, кто раньше не сталкивался с программированием на ассемблере, это неплохая задача для первого опыта. За основу возьмите шаблон, приведенный в разделе «Основные сведения». Необходимые сведения о том, как извлечь требуемую информацию, представлены в следующем разделе. Ассемблерная программа должна читать содержимое предпоследнего байта ROM BIOS, по таблице, сравнивая коды, определять тип РС 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 сообщения.Затем соответствующего определяется версия системы. Ассемблерная программа должна по значениям регистров AL и AH формировать текстовую строку в формате хх.уу, где хх - номер основной версии, а уу - номер модификации в десятичной системе счисления, формировать строки с серийным номером ОЕМ и серийным номером пользователя.Полученные строки выводятся на экран.Отладьте полученный исходный модуль.Результатом выполнения этого шага будет «хороший» .COM модуль, а такженеобходимо построить «плохой» .EXE, полученный из исходного текста для .САМ модуля.

Шаг 2. Напишите текст исходного .EXE модуля, который выполняет те же функции, что и модуль в Шаге 1 и постройте и отладьте его. Таким образом, будет получен «хороший» .EXE.

Шаг 3. Сравните исходные тексты для .СОМ и .ЕХЕ модулей. Ответьте

на контрольные вопросы «Отличия исходных текстов СОМ и EXE

программ».

Шаг 4. Запустите FAR и откройте (F3/F4) файл загрузочного модуля

.COM и файл«плохого» .EXE в шестнадцатеричном виде. Затем откройте

(F3/F4) файл загрузочного модуля «хорошего» .EXE и сравните его с

предыдущими файлами. Ответьте на контрольные вопросы «Отличия

форматов файлов СОМ и EXE модулей».

Шаг 5. Откройте отладчик TD.EXE и загрузите .COM. Ответьте на

контрольные вопросы «Загрузка СОМ модуля в основную память».

Представьте в отчете план загрузки модуля .СОМ в основную память.

Шаг 6. Откройте отладчик TD.EXE и загрузите «хороший» .EXE.

Ответьте на контрольные вопросы «Загрузка «хорошего» ЕХЕ модуля в

основную память».

Шаг 7. Оформление отчета в соответствии с требованиями. В отчете

необходимо привести скриншоты. Для файлов их вид в шестнадцатеричном

виде, для загрузочных модулей – в отладчике

Ход работы.

В обоих программах в начале были объявлены константные строки для

вывода информации о ПК и версии MS DOS. Также были написаны

собственные функции MYPRINT - для вывода строк, DEFINE PC TYP - для

определения типа ПК и DEFINE OS VER - для определения версии MS

DOS.

Запуск хорошего .com модуля

Type: AT

MS-DOS version: 5.0

Serial OEM: 0

User Serial: 000000H

Запуск плохого .exe модуля



Запуск хорошего .exe модуля

Type: AT MS-DOS version: 5.0 Serial OEM: 0 User Serial: 000000H

Вывод.

В результате выполнения лабораторной работы были написаны программы для определения версии РС и MS DOS. Исследованы различия в структурах исходных текстовых модулей типов .COM и .EXE, структурах файлов загрузочных модулей и способов их загрузки в основную память.

Ответы на контрольные вопросы.

Отличия исходных текстов СОМ и ЕХЕ программ

- Сколько сегментов должна содержать СОМ-программа?
 У СОМ-программы 1 сегмент.
- 2) Сколько сегментов должна содержать ЕХЕ-программа?
- У ЕХЕ-программы может быть больше одного сегмента, отдельные сегменты для данных, кода и стека.
 - 3) Какие директивы должны обязательно быть в тексте СОМ программы?

В тексте COM-программы обязательно должна быть директива ORG 100h, так как в первых 256(100h) байтах находится PSP, а код программы располагается после него. Также обязательно должна присутствовать директива ASSUME, которая сообщает о том, какой сегмент к какому сегментному регистру привязан.

4) Все ли форматы команд можно использовать в СОМ-программе?

Нет, не все. Например в СОМ-программе нельзя использовать команды вида mov register, segment и команды, содержащие дальнюю(far) адресацию, так как для нормальной работы этим командам нужна relocation table, которой нет в СОМ-программах.

Отличия форматов файлов СОМ и ЕХЕ модулей

1) Какова структура файла СОМ? С какого адреса располагается код?

Структура состоит из одного сегмента размером не больше 64КБ. В файле код располагается с нулевого адреса, но при загрузке модуля смещается на 100h.

```
E9 CF 01 54 79 70 65 3A 20 50 43 0D 0A 24 54 79
                                                       0 L. Type: PC..$Ty
00000000
00000010
         70 65 3A 20 50 43 2F 58 54 0D 0A 24 54 79 70 65
                                                       pe: PC/XT..$Type
00000020 3A 20 41 54 0D 0A 24 54 79 70 65 3A 20 50 53 32 : AT...$Type: PS2
000000030 20 6D 6F 64 65 6C 20 33 30 0D 0A 24 54 79 70 65
                                                       model 30..$Type
000000040 3A 20 50 53 32 20 6D 6F 64 65 6C 20 35 30 20 6F
                                                       : PS2 model 50 o
00000050 72 20 36 30 0D 0A 24 54 79 70 65 3A 20 50 53 32 r 60..$Type: PS2
000000060 20 6D 6F 64 65 6C 20 38 30 0D 0A 24 54 79 70 65
                                                       model 80..$Type
                                                        : Plíjr..$Type:
00000070 3A 20 50 D0 A1 6A 72 0D 0A 24 54 79 70 65 3A 20
00000080 50 43 20 43 6F 6E 76 65 72 74 69 62 6C 65 0D 0A
                                                       PC Convertible..
000000090 24 4D 53 2D 44 4F 53 20 76 65 72 73 69 6F 6E 3A
                                                      $MS-DOS version:
000000A0
        20 20 2E 20 20 0D 0A 24 53 65 72 69 61 6C 20 4F
                                                         . ..$Serial 0
000000B0 45 4D 3A 20 20 0D 0A 24 55 73 65 72 20 53 65 72
                                                       EM: ..$User Ser
000000000 69 61 6C 3A 20 20 20 20 20 20 48 0D 0A 24 24
                                                       ial:
                                                                 H..$$
.<.v...0 -0èαΦ∩
000000E0 86 C4 B1 04 D2 E8 E8 E6 FF 59 C3 53 8A FC E8 E9
                                                       å-. тФФµ Y-SènФО
000000F0 FF 88 25 4F 88 05 4F 8A C7 E8 DE FF 88 25 4F 88
                                                       ê%0ê.0è Φ  ê%0ê
                                                       .[-QR2Σ3--..≈±Ç-
00000100 05 5B C3 51 52 32 E4 33 D2 B9 0A 00 F7 F1 80 CA
00000110 30 88 14 4E 33 D2 3D 0A 00 73 F1 3C 00 74 04 0C
                                                       0ê.N3π=..s±<.t..
                                                       0ê.ZY H .=! |q.≡Ä L
00000120 30 88 04 5A 59 C3 B4 09 CD 21 C3 B8 00 F0 8E C0
00000130 26 A0 FE FF 3C FF 74 1C 3C FE 74 1E 3C FB 74 1A
                                                       &á• < t.<•t.<√t.
00000140 3C FC 74 1C 3C FA 74 1E 3C F8 74 26 3C FD 74 28
                                                       <nt.<.t.<°t&<2t(
00000150 3C F9 74 2A BA 03 01 EB 2B 90 BA 0E 01 EB 25 90
                                                       <·t*|..δ+É|..δ%É
                                                        |..δ.έ||'.δ.έ||<.δ
00000160 BA 1C 01 EB 1F 90 BA 27 01 EB 19 90 BA 3C 01 EB
                                                       .έ|W.δ.έ|l.δ.έ|z
00000170 13 90 BA 57 01 EB 0D 90 BA 6C 01 EB 07 90 BA 7A
                                                       .δ.ÉΦf H 0=!P∃æ.
â =.Φm Xè—â =.Φd
00000190 83 C6 10 E8 6D FF 58 8A C4 83 C6 03 E8 64 FF BA
                                                       æ.Φü = ¿.â = .è | ΦS
000001A0 91 01 E8 81 FF BE A8 01 83 C6 0C 8A C7 E8 53 FF
000001B0 BA A8 01 E8 70 FF BF B8 01 83 C7 12 8B C1 E8 2A
                                                       è p. ân.ë. ₹.ΦU
000001C0
         FF 8A C3 E8 14 FF 83 EF 02 89 05 BA B8 01 E8 55
                                                        ΦV Φ\ 2 4 L=!
000001D0 FF C3 E8 56 FF E8 B0 FF 32 C0 B4 4C CD 21 +
```

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

В «плохом» EXE файле данные и код содержатся в одном сегменте. Код располагается с адреса 300h. С адреса 0h располагается Relocation Table

00000000	4D	5A	DE	00	03	00	00	00	20	00	00	00	FF	FF	00	00	MZ
00000010	00	00	04	89	00	01	00	00	1E	00	00	00	01	00	00	00	ë
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	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	00	
00000070	00	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	00	
00000090	00	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	00	
000000B0	00	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	00	
000000D0	00	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	00	
000000F0	00	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	00	
00000110	00	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	00	
00000130	00	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	00	
00000150	00	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	00	
00000170	00	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	00	
00000190	00	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	00	
000001B0	00	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	00	
000001D0	00	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	00	
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

```
000002E0
          000002F0
          . . . . . . . . . . . . . . . .
                                                          θ<sup>⊥</sup>.Type: PC..$Ty
         E9 CF 01 54 79 70 65 3A 20 50 43 0D 0A 24 54 79
00000300
00000310
         70 65 3A 20 50 43 2F 58 54 0D 0A 24 54 79 70 65
                                                          pe: PC/XT..$Type
         3A 20 41 54 0D 0A 24 54 79 70 65 3A 20 50 53 32
                                                          : AT.. $Type: PS2
00000320
00000330 20 6D 6F 64 65 6C 20 33 30 0D 0A 24 54 79 70 65
                                                          model 30..$Type
         3A 20 50 53 32 20 6D 6F 64 65 6C 20 35 30 20 6F
00000340
                                                          : PS2 model 50 o
         72 20 36 30 0D 0A 24 54 79 70 65 3A 20 50 53 32
00000350
                                                          r 60..$Type: PS2
         20 6D 6F 64 65 6C 20 38 30 0D 0A 24 54 79 70 65
00000360
                                                          model 80..$Type
          3A 20 50 D0 A1 6A 72 0D 0A 24 54 79 70 65 3A 20
                                                          : Plíjr..$Type:
00000370
                                                          PC Convertible..
00000380
         50 43 20 43 6F 6E 76 65 72 74 69 62 6C 65 0D 0A
00000390 24 4D 53 2D 44 4F 53 20 76 65 72 73 69 6F 6E 3A
                                                          $MS-DOS version:
          20 20 2E 20 20 0D 0A 24 53 65 72 69 61 6C 20 4F
000003A0
                                                          . ..$Serial 0
000003B0
         45 4D 3A 20 20 0D 0A 24 55 73 65 72 20 53 65 72
                                                          EM: ..$User Ser
000003C0 69 61 6C 3A 20 20 20 20 20 20 48 0D 0A 24 24
                                                                    H..$$
                                                          .<.v...0 -QèαΦn
          OF 3C 09 76 02 04 07 04 30 C3 51 8A E0 E8 EF FF
000003D0
000003E0 86 C4 B1 04 D2 E8 E8 E6 FF 59 C3 53 8A FC E8 E9
                                                          å-. тФФµ Y-SènФО
000003F0 FF 88 25 4F 88 05 4F 8A C7 E8 DE FF 88 25 4F 88
                                                          ê%0ê.0è Φ  ê%0ê
                                                          .[-QR2Σ3-..≈±Ç-
00000400
          05 5B C3 51 52 32 E4 33 D2 B9 0A 00 F7 F1 80 CA
00000410
         30 88 14 4E 33 D2 3D 0A 00 73 F1 3C 00 74 04 0C
                                                          0ê.N3π=..s±<.t..
                                                          0ê.ZYH .=! |q.≡ÄL
00000420 30 88 04 5A 59 C3 B4 09 CD 21 C3 B8 00 F0 8E C0
00000430
          26 A0 FE FF 3C FF 74 1C 3C FE 74 1E 3C FB 74 1A
                                                          &á• < t.<•t.<√t.
00000440 3C FC 74 1C 3C FA 74 1E 3C F8 74 26 3C FD 74 28
                                                          <nt.<.t.<°t&<2t(
00000450 3C F9 74 2A BA 03 01 EB 2B 90 BA 0E 01 EB 25 90
                                                          <·t*|..δ+É|..δ%É
00000460
          BA 1C 01 EB 1F 90 BA 27 01 EB 19 90 BA 3C 01 EB
                                                          |..δ.έ|'.δ.έ|<.δ
00000470 13 90 BA 57 01 EB 0D 90 BA 6C 01 EB 07 90 BA 7A
                                                          .É|W.δ.É|l.δ.É|z
          01 EB 01 90 E8 9F FF C3 B4 30 CD 21 50 BE 91 01
                                                          .δ.ÉΦf H 0=!P-læ.
00000480
         83 C6 10 E8 6D FF 58 8A C4 83 C6 03 E8 64 FF BA
                                                          â =.Φm Xè—â =.Φd
00000490
          91 01 E8 81 FF BE A8 01 83 C6 OC 8A C7 E8 53 FF
                                                          æ.Φü ᆗ;.â⊨.è ΦS
000004A0
          BA A8 01 E8 70 FF BF B8 01 83 C7 12 8B C1 E8 2A
                                                          | ¿.Φp ¬¬.â|.ï⊥Φ*
000004B0
000004C0
         FF 8A C3 E8 14 FF 83 EF 02 89 05 BA B8 01 E8 55
                                                           è ф. ân.ë. ╕.ФU
                                                           ΦV Φ\\ 2 \ L=!
000004D0
          FF C3 E8 56 FF E8 B0 FF 32 C0 B4 4C CD 21 +
```

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

В «хорошем» ЕХЕ, код, стек и данные выделены в отдельные сегменты в отличии от «плохого». В файле «плохого» ЕХЕ смещение 300h(100h изначальное смещение и 200h размер модуля PSP). У «хорошего» ЕХЕ память под стек выделяется между PSP и кодом.

00000000	4D	5A	E7	00	03	00	01	00	20	00	00	00	FF	FF	00	00	MΖτ
00000010	00	01	2F	99	03	01	1D	00	1E	00	00	00	01	00	07	01	/Ö
00000020	1D	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	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	00	
00000070	00	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	00	
00000090	00	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	00	
000000B0	00	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	00	
000000D0	00	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	00	
000000F0	00	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	00	
00000110	00	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	00	
00000130	00	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	00	
00000150	00	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	00	
00000170	00	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	00	
00000190	00	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	00	
000001B0	00	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	00	
000001D0	00	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	00	
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

```
000002F0
          . . . . . . . . . . . . . . . .
00000300
          54 79 70 65 3A 20 50 43 0D 0A 24 54 79 70 65 3A
                                                             Type: PC..$Type:
          20 50 43 2F 58 54 0D 0A 24 54 79 70 65 3A 20 41
                                                              PC/XT..$Type: A
00000310
          54 0D 0A 24 54 79 70 65 3A 20 50 53 32 20 6D 6F
                                                             T..$Type: PS2 mo
00000320
          64 65 6C 20 33 30 0D 0A 24 54 79 70 65 3A 20 50
                                                             del 30..$Type: P
00000330
          53 32 20 6D 6F 64 65 6C 20 35 30 20 6F 72 20 36
                                                             S2 model 50 or 6
00000340
          30 0D 0A 24 54 79 70 65 3A 20 50 53 32 20 6D 6F
                                                             0..$Type: PS2 mo
00000350
                                                             del 80..$Type: P
00000360
          64 65 6C 20 38 30 0D 0A 24 54 79 70 65 3A 20 50
                                                             √ijr..$Type: PC
00000370
          DO A1 6A 72 OD OA 24 54 79 70
                                         65 3A 20 50 43 20
          43 6F 6E 76 65 72 74 69 62 6C 65 0D 0A 24 4D 53
                                                             Convertible..$MS
00000380
00000390
          2D 44 4F 53 20 76 65 72 73 69 6F 6E 3A 20 20 2E
                                                             -DOS version: .
000003A0
          20 20 0D 0A 24 53 65 72 69 61 6C 20 4F 45 4D 3A
                                                               .. $Serial OEM:
000003B0
          20 20 0D 0A 24 55 73 65 72 20 53 65 72 69 61 6C
                                                               ..$User Serial
          3A 20 20 20 20 20 20 20 48 0D 0A 24 00 00 00 00
000003C0
                                                                     H..$...
          24 OF 3C 09 76 02 04 07 04 30 C3 51 8A E0 E8 EF
                                                             $.<.v...0 -QèαΦ∩
000003D0
                                                              å-. пФФµ Y-SènФ
          FF 86 C4 B1 04 D2 E8 E8 E6 FF 59 C3 53 8A FC E8
000003E0
          E9 FF 88 25 4F 88 05 4F 8A C7 E8 DE FF 88 25 4F
                                                             Θ ê%0ê.0è Φ  ê%0
000003F0
                                                             ê.[ -QR2Σ3π ..≈±Ç
00000400
          88 05 5B C3 51 52 32 E4 33 D2 B9 0A 00 F7 F1 80
          CA 30 88 14 4E 33 D2 3D 0A 00 73 F1 3C 00 74 04
                                                             <u>4</u>0ê.N3<sub>π</sub>=..s±<.t.
00000410
                                                              .0ê.ZYĤ.=!├q.≡Ä
00000420
          OC 30 88 04 5A 59 C3 B4 09 CD 21 C3 B8 00 F0 8E
00000430
          CO 26 AO FE FF 3C FF 74 1C 3C FE 74 1E 3C FB 74
                                                             L&á• < t.<•t.<√t
                                                             .<nt.<.t.<°t&<2t
00000440
          1A 3C FC 74 1C 3C FA 74 1E 3C F8 74 26 3C FD 74
                                                             (<·t*||..δ+É||..δ%
00000450
          28 3C F9 74 2A BA 00 00 EB 2B 90 BA 0B 00 EB 25
          90 BA 19 00 EB 1F 90 BA 24 00 EB 19 90 BA 39 00
                                                             É ..δ.É $.δ.É 9.
00000460
                                                             δ.έ T.δ.έ i.δ.έ
00000470
          EB 13 90 BA 54 00 EB 0D 90 BA 69 00 EB 07 90 BA
          77 00 EB 01 90 E8 9F FF C3 B4 30 CD 21 50 BE 8E
                                                             w.δ.ÉΦf | 0=!P- Ä
00000480
00000490
          00 83 C6 10 E8 6D FF 58 8A C4 83 C6 03 E8 64 FF
                                                             .â ⊨.Φm Xè—â ⊨.Φd
          BA 8E 00 E8 81 FF BE A5 00 83 C6 0C 8A C7 E8 53
                                                             Ä.Фü ╛Ñ.â⊨.è ФS
000004A0
          FF BA A5 00 E8 70 FF BF B5 00 83 C7 12 8B C1 E8
                                                              |N.Φp ¬= .â|-.ï⊥Φ
000004B0
000004C0
          2A FF 8A C3 E8 14 FF 83 EF 02 89 05 BA B5 00 E8
                                                             * è Φ. â∩.ë. ╡.Φ
000004D0
          55 FF C3 2B C0 50 B8 10 00 8E D8 E8 4E FF E8 A8
                                                             U
                                                               + LP= .. Ä=ΦN Φ;
                                                              24L=!
          FF 32 CO B4 4C CD 21
000004E0
```

Загрузка СОМ модуля в основную память.

DOS	DO	SB	ох	0.7	4-3	, c	pu	spe	ed:		esk	ip	0,	Pro	gr	am	:	AFI	OPF	10	-	0.713	×
AX 0000	SI	000	00	CS	3 19	F5		IP 01	100		Sta	ack	+0	000	90	Fla	ıgs	72	92				
BX 0000		000			3 19								-	200									
CX 01DE		000	3.5		3 19			IS 19						9FI				IF	SF		ΑF		CF
DX 0000	SP	FFI	E	S3	3 19	9F5]	FS 19	9F5				+6	EAG	90	Θ	0	1	0	0	Θ	Θ	0
CMD >												П	1			0	1	2	3	4	5	6	7
														:000	90	CD	20	FF	9F	00	EA	FO	FE
												- 1		:000		AD	DE	1B	05	C5	06	00	00
0100 E9CF	01			JI	P		92D2	2					DS	:00:	LO	18	01	10	01	18	01	92	01
0103 54				Pl	JSH		SP					_	DS	:00:	18	01	01	01	00	FF	00	01	FF
0104 7970				JI	48	(9176	5				- 1	DS	:002	20	FF	FF	FF	FF	FF	FF	FF	FF
0106 65				DI	В	6	55					- 1	DS	:000	28	FF	FF	FF	FF	EB	19	CO	11
0107 3A20				C	P	f	AH, I	BX+S	311			- 1	DS	:003	30	AZ	01	14	00	18	$\Theta\Theta$	F5	19
0109 50				Pl	JSH	f	XF					- 1	DS	:003	38	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	00	00	00	00
010A 43				11	AC.]	BX					- 1	DS	:004	10	05	∞	00	∞	00	∞	00	00
010B 0D0A	24			01	R	f	AX,2	240A					DS	:004	18	00	00	00	99	00	00	00	00
2	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	Т						
DS:0000	CD	20	FF	9F	00	EA	FO	FE	AD	DE	1B	05	C5	06	00	00	:	= }	f.Ω≡		11	+	
DS:0010	18	01	10	01	18	01	92	01	01	01	01	00	FF	00	01	FF	- 1		f				
DS:0020	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	EB	19	CO	11						δ	. L.
DS:0030	A2	01	14	00	18	00	F5	19	FF	FF	FF	FF	00	00	00	00	i	ó		١.			
DS:0040	05	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00							
1 Step	200			- 0.7	-	-		Hely	ON	- 2	2721					7	=	8		_			

1) Какой формат загрузки СОМ модуля? С какого адреса располагается кол?

В начале определяется адрес сегмента оперативной памяти, в котором хватит места для загрузки программы, после чего система отводит первые 256 байт для PSP, а СОМ файл помещается в память со смещение 100h. Затем инициализируются сегментные регистры, которые все указывают на начало PSP. SP при этом будет указывать на конец PSP, IP станет равным 100h, в стек будет помещено 0000h. Код будет располагаться со смещением в 100h.

- 2) Что располагается с 0 адреса? Сегмент PSP.
- 3) Какие значения имеют сегментные регистры? На какие области памяти они указывают?

Сегментные регистры будут иметь одинаковые значения. И будут указывать на начало PSP.

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

Стек определяется автоматически. Регистр SS указывает на начало сегмента, а SP=FFFEh – на его конец.

Загрузка «хорошего» EXE модуля в основную память

AX 0000		000			16]	IP 01	03		Sta	ack		795		Flā	ags	720	92				
BX 0000 CX 02E7		000			19 19		H	IS 19	F5					651 203		OF	DF	IF	SF	ZF	ΑF	PF	CF
DX 0000		010			16		I	'S 19	F5					435		0	0	1	0	0	0	0	0
CMD >												Т	1			0	1	2	3	4	5	6	7
- TO-TO- TO												4		000	90	CD	20	FF	9F	00	EA	FΘ	FE
													DS	:000	98	AD	DE	1B	05	C5	06	00	00
0103 ZBC0				SL			λX,	λX						:00:		18	01	10		18			01
0105 50					JSH		ìΧ							:00:		01	01	01	00	FF	90	01	FF
0106 B815:	1A			MC				LA15						:002		FF	FF	FF	FF	FF		FF	FF
0109 8ED8				MC			08,6							:002		FF	FF	FF	FF	EB		CO	11
010B E84E					LL		0050							:003		AZ	01	14	00	18			19
010E E8A81					LL		90B9							:00:		FF	FF	FF	FF	00	00	00	∞
0111 32C0				X			AL, f							:004		05 00	00	00	00	00 00			∞
0113 B44C				MC	IV.	'	ΉΗ, <u>«</u>	rt.					סמ	:004	10	00	00	00	00	00	00	00	00
2	0	1	Z	3	4	5	6	7	8	9	A	В	С	D	E	F							
DS:0000	CD	20	$\mathbf{F}\mathbf{F}$	9F	00	EA	FO	FE	AD	DE	1B	05	C5	06	00	00	-	= ;	f.Ω≡		Ĭ.	+.	٠.,
DS:0010	18	01	10	01	18	01	92	01	01	01	01	00	FF	00	01	FF			f	Ŧ.			
DS:0020	FF	FF	FF	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	FF	FF	EB	19	-	11		,				δ.	۲.
DS:0030	A2		14				F5		FF	FF	FF	FF				00	į (ó					•••
DS:0040	05	00	00	00	90	00	00	00	00	00	00	00	00	00	90	00						•••	•••
1 Step	2Pr	rocS	Step	3	leti	rie	ле 4	Help	ON	5	BRK	Men	nu 6	5		7	t	8	ı	9	(= [0 =	→

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

Сначала считывается информация с заголовка EXE. Затем инициализируются сегментные регистры. SS будет указывать на начало сегмента стека, PS на конец сегмента стека, CS на начало сегмента кода. В IP запишется точка входа в программу.

- 2) На что указывают регистры DS и ES? ES и DS будут указывать на начало PSP.
- Как определяется стек?
 В программе с помощью специальной директивы .STACK с указанием размера.

4) Как определяется точка входа?
Точка входа в программу определяется с помощью директивы END.