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

ОТЧЕТ

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

Студент гр. 8383 _____ Мирсков А.А.

Преподаватель _____ Губкин А.Ф.

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.

Выполнение работы.

Был написан текст исходного .COM модуля, который определяет тип PC и версию системы. Из него были построены .COM модуль и «плохой» .EXE модуль. Далее был написан текст исходного .EXE модуля. Из которого был построен «хороший» .EXE модуль. Процесс создания модулей и их вывод представлены на скриншотах ниже.

Рисунок 1 – Создание и выполнение **.COM** модуля

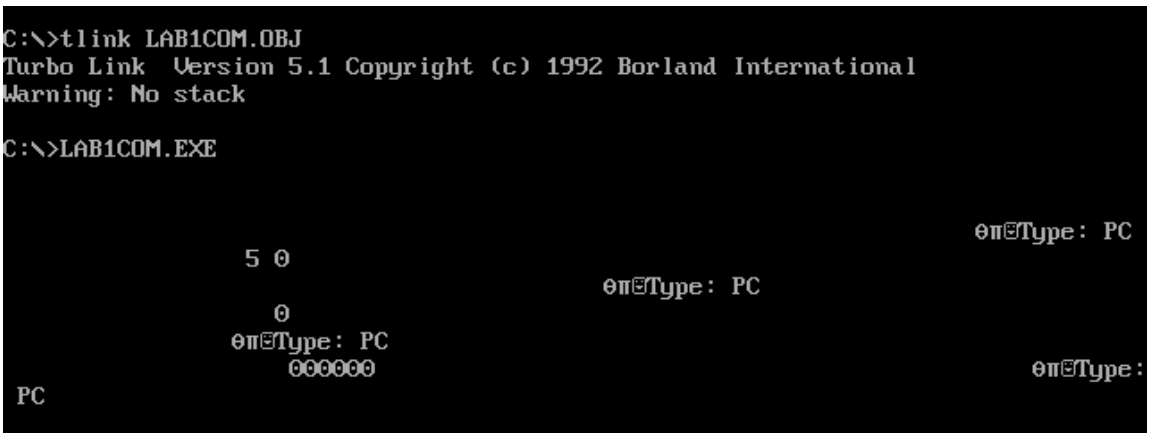


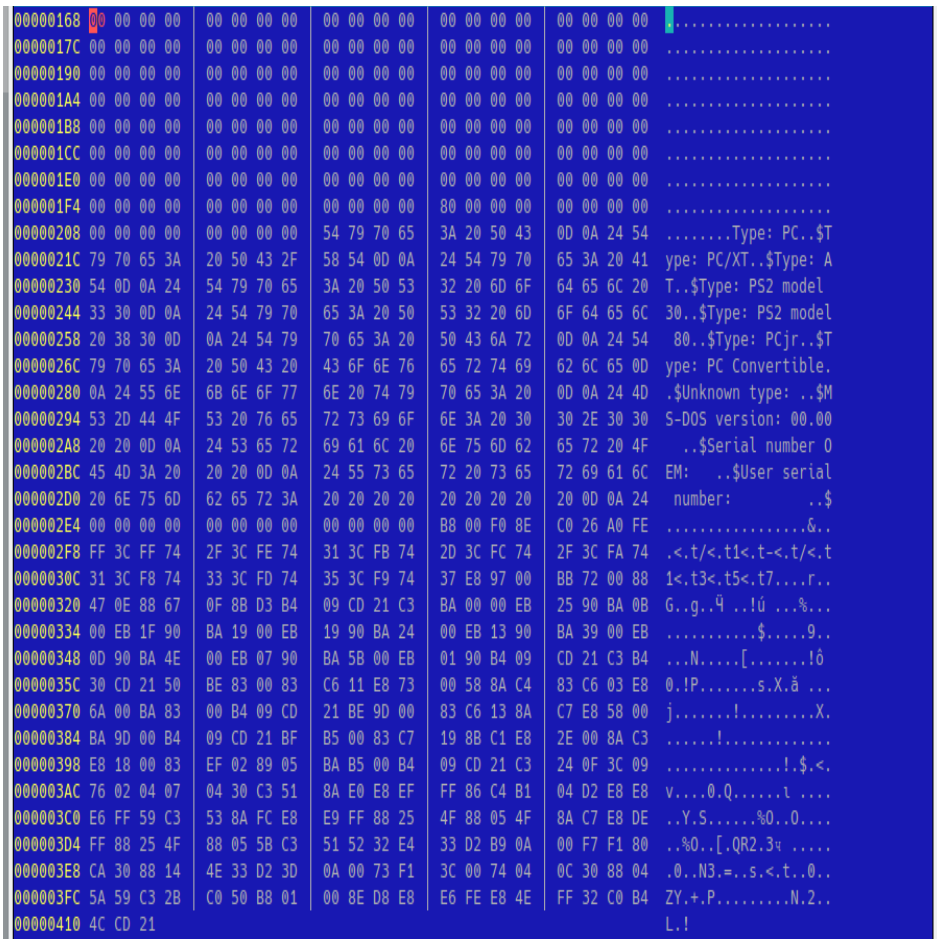
Рисунок 2 – Создание и выполнение «плохого» **.EXE** модуля

Рисунок 3 – Создание и выполнение «хорошего» **.EXE** модуля

Отличия исходных текстов COM и EXE программ

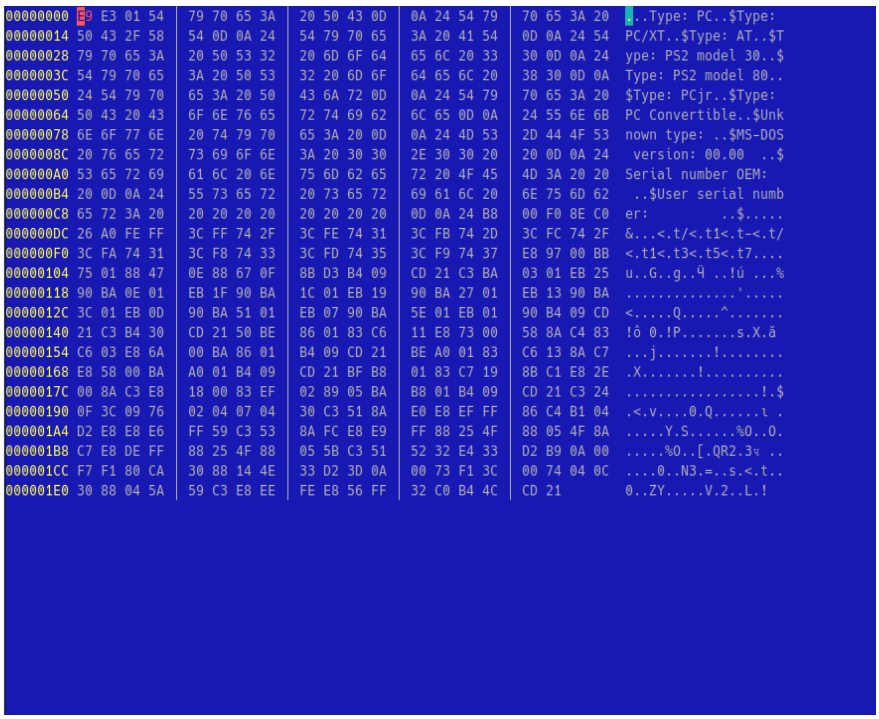
1) COM-программа содержит один сегмент.
2) EXE-программа содержит не менее одного сегмента.
3) COM-программа, в отличии от EXE-программы должна начинаться с ORG 100h, потому что адресация имеет смещение в 256 байт. Также необходима директива ASSUME, в которой сегмент кода и сегмент данных должны указывать на общий сегмент.
4) В COM-программах нельзя использовать команды вида mov <регистр>, <сегмент>.

В приложении Midnight Commander были открыты загрузочные модули в шестнадцатеричном виде. Скриншоты представлены ниже.



```
00000168 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0000017C 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  ................
000001A4 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001B8 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
000001CC 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  ................
000001F4 00 00 00 00  00 00 00 00  00 00 00 00  80 00 00 00  ................
00000208 00 00 00 00  00 00 00 00  54 79 70 65  3A 20 50 43  ........Type: PC
0000021C 79 70 65 3A  20 50 43 2F  58 54 0D 0A  24 54 79 70  ype: PC/XT..$Typ
00000230 54 0D 0A 24  54 79 70 65  3A 20 50 53  32 20 6D 6F  T..$Type: PS2 mo
00000244 33 30 0D 0A  24 54 79 70  65 3A 20 50  53 32 20 6D  30..$Type: PS2 m
00000258 20 38 30 0D  0A 24 54 79  70 65 3A 20  50 43 6A 72  80..$Type: PCjr
0000026C 79 70 65 3A  20 50 43 20  43 6F 6E 76  65 72 74 69  ype: PC Convertib
00000280 0A 24 55 6E  6B 6E 6F 77  6E 20 74 79  70 65 3A 20  .$Unknown type:
00000294 53 2D 44 4F  53 20 76 65  72 73 69 6F  6E 3A 20 30  S-DOS version: 0
000002A8 20 20 0D 0A  24 53 65 72  69 61 6C 20  6E 75 6D 62  ....$Serial numb
000002BC 45 4D 3A 20  20 20 0D 0A  24 55 73 65  72 20 73 65  EM:   ..$User se
000002D0 20 6E 75 6D  62 65 72 3A  20 20 20 20  20 20 20 20  rial number:
000002E4 00 00 00 00  00 00 00 00  00 00 00 00  B8 00 F0 8E  ............
000002F8 FF 3C FF 74  2F 3C FE 74  31 3C FB 74  2D 3C FC 74  .<.t/<.t1<.t-<.t
0000030C 31 3C F8 74  33 3C FD 74  35 3C F9 74  37 E8 97 00  1<.t3<.t5<.t7....
00000320 47 0E 88 67  0F 8B D3 B4  09 CD 21 C3  BA 00 00 EB  G..g..Ч ..!ú ...
00000334 00 EB 1F 90  BA 19 00 EB  19 90 BA 24  00 EB 13 90  ...........$....
00000348 0D 90 BA 4E  00 EB 07 90  BA 5B 00 EB  01 90 B4 09  ...N.....[.....
0000035C 30 CD 21 50  BE 83 00 83  C6 11 E8 73  00 58 8A C4  0.!P.......s.X.
00000370 6A 00 BA 83  00 B4 09 CD  21 BE 9D 00  83 C6 13 8A  j.......!.....
00000384 BA 9D 00 B4  09 CD 21 BF  B5 00 83 C7  19 8B C1 E8  ......!.....
00000398 E8 18 00 83  EF 02 89 05  BA B5 00 B4  09 CD 21 C3  ..............
000003AC 76 02 04 07  04 30 C3 51  8A E0 E8 EF  FF 86 C4 B1  v....0.Q....
000003C0 E6 FF 59 C3  53 8A FC E8  E9 FF 88 25  4F 88 05 4F  ..Y.S.....%O..O
000003D4 FF 88 25 4F  88 05 5B C3  51 52 32 E4  33 D2 B9 0A  ..%O..[.QR2.3
000003E8 CA 30 88 14  4E 33 D2 3D  0A 00 73 F1  3C 00 74 04  .0..N3.=..s.<.t.
000003FC 5A 59 C3 2B  C0 50 B8 01  00 8E D8 E8  E6 FE E8 4E  ZY.+.P.........N
00000410 4C CD 21                                           L.!
```

Рисунок 6 – Содержимое «хорошего» EXE модуля



```
00000000 E9 E3 01 54  79 70 65 3A  20 50 43 0D  0A 24 54 79  ...Type: PC..$Ty
00000014 50 43 2F 58  54 0D 0A 24  54 79 70 65  3A 20 41 54  PC/XT..$Type: AT
00000028 79 70 65 3A  20 50 53 32  20 6D 6F 64  65 6C 20 33  ype: PS2 model 3
0000003C 54 79 70 65  3A 20 50 53  32 20 6D 6F  64 65 6C 20  Type: PS2 model
00000050 24 54 79 70  65 3A 20 50  43 6A 72 0D  0A 24 54 79  $Type: PCjr..$Ty
00000064 50 43 20 43  6F 6E 76 65  72 74 69 62  6C 65 0D 0A  PC Convertible..
00000078 6E 6F 77 6E  20 74 79 70  65 3A 20 0D  0A 24 4D 53  nown type: ..$MS
0000008C 20 76 65 72  73 69 6F 6E  3A 20 30 30  2E 30 30 20  version: 00.00
000000A0 53 65 72 69  61 6C 20 6E  75 6D 62 65  72 20 4F 45  Serial number OE
000000B4 20 0D 0A 24  55 73 65 72  20 73 65 72  69 61 6C 20  ...$User serial
000000C8 65 72 3A 20  20 20 20 20  20 20 20 20  0D 0A 24 B8  er:          ..$.
000000DC 26 A0 FE FF  3C FF 74 2F  3C FE 74 31  3C FB 74 2D  &...<.t/<.t1<.t-
000000F0 3C FA 74 31  3C F8 74 33  3C FD 74 35  3C F9 74 37  <.t1<.t3<.t5<.t7
00000104 75 01 88 47  0E 88 67 0F  8B D3 B4 09  CD 21 C3 BA  u..G..g..Ч ..!ú
00000118 90 BA 0E 01  EB 1F 90 BA  1C 01 EB 19  90 BA 27 01  ..............'.
0000012C 3C 01 EB 0D  90 BA 51 01  EB 07 90 BA  5E 01 EB 01  <.....Q.....^...
00000140 21 C3 B4 30  CD 21 50 BE  86 01 83 C6  11 E8 73 00  !ô 0.!P.......s.
00000154 C6 03 E8 6A  00 BA 86 01  B4 09 CD 21  BE A0 01 83  ...j.......!....
00000168 E8 58 00 BA  A0 01 B4 09  CD 21 BF B8  01 83 C7 19  .X.......!......
0000017C 00 8A C3 E8  18 00 83 EF  02 89 05 BA  B8 01 B4 09  ..............!.
00000190 0F 3C 09 76  02 04 07 04  30 C3 51 8A  E0 E8 EF FF  .<.v....0.Q.....
000001A4 D2 E8 E8 E6  FF 59 C3 53  8A FC E8 E9  FF 88 25 4F  .....Y.S......%O
000001B8 C7 E8 DE FF  88 25 4F 88  05 5B C3 51  52 32 E4 33  .....%O..[.QR2.3
000001CC F7 F1 80 CA  30 88 14 4E  33 D2 3D 0A  00 73 F1 3C  ....0..N3.=..s.<
000001E0 30 88 04 5A  59 C3 E8 EE  FE E8 56 FF  32 C0 B4 4C  0..ZY.....V.2..L
000001F4 CD 21                                              .!
```

Рисунок 4 – Содержимое COM модуля

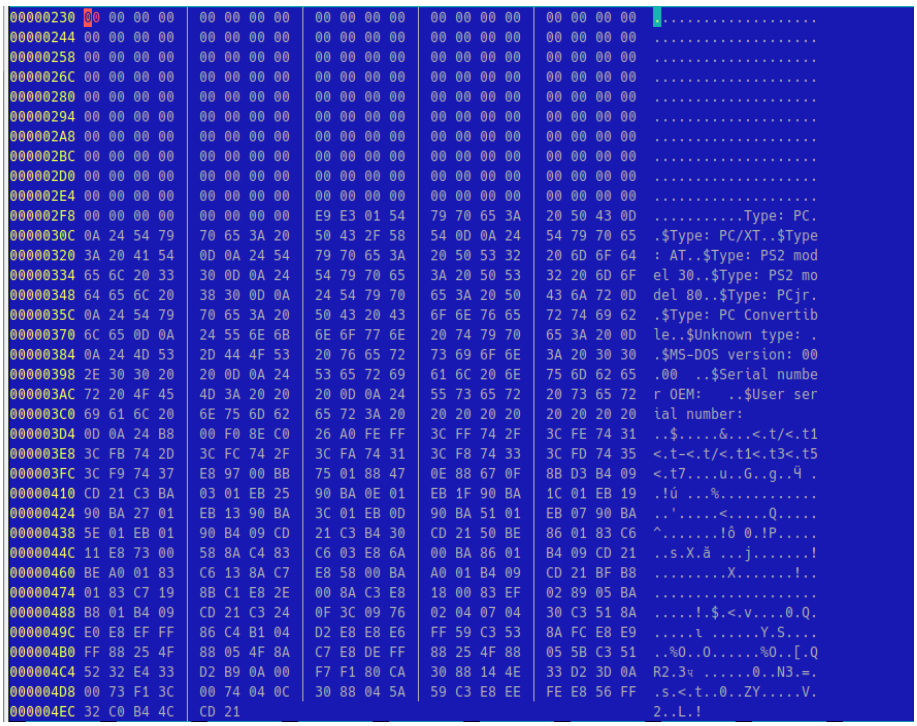


Рисунок 5 – Содержимое «плохого» EXE модуля

Отличие форматов файлов COM и EXE модулей

1) COM файл содержит только машинный код и данные программы. Код начинается с адреса 0h, но при загрузке устанавливается смещение на 100h.
2) В «плохом» EXE модуле код и данные располагаются в одном сегменте. С адреса 0h идет таблица настроек. Код начинается со смещения 300h.
3) В «хорошем» EXE модуле данные, стэк и машинный код в разных сегментах. От «плохого» EXE он так же отличается наличием стека.

При помощи отладчика TD COM и EXE файлы были загружены в основную память. Скриншоты представлены ниже.

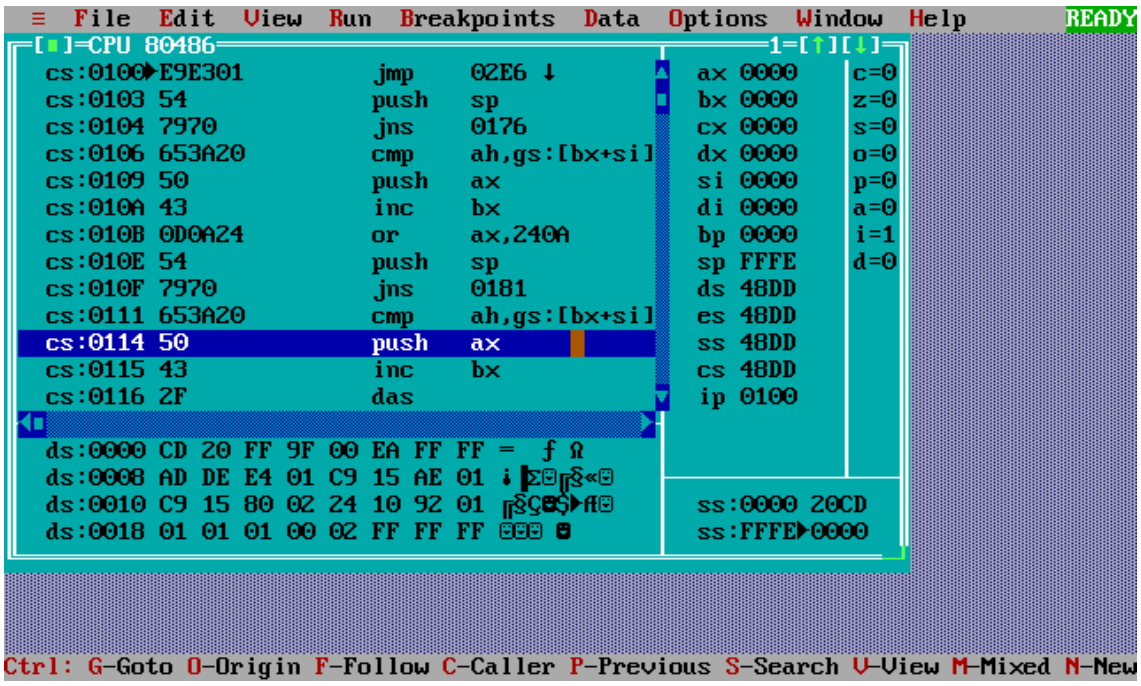


Рисунок 7 – Результат загрузки COM файла в память

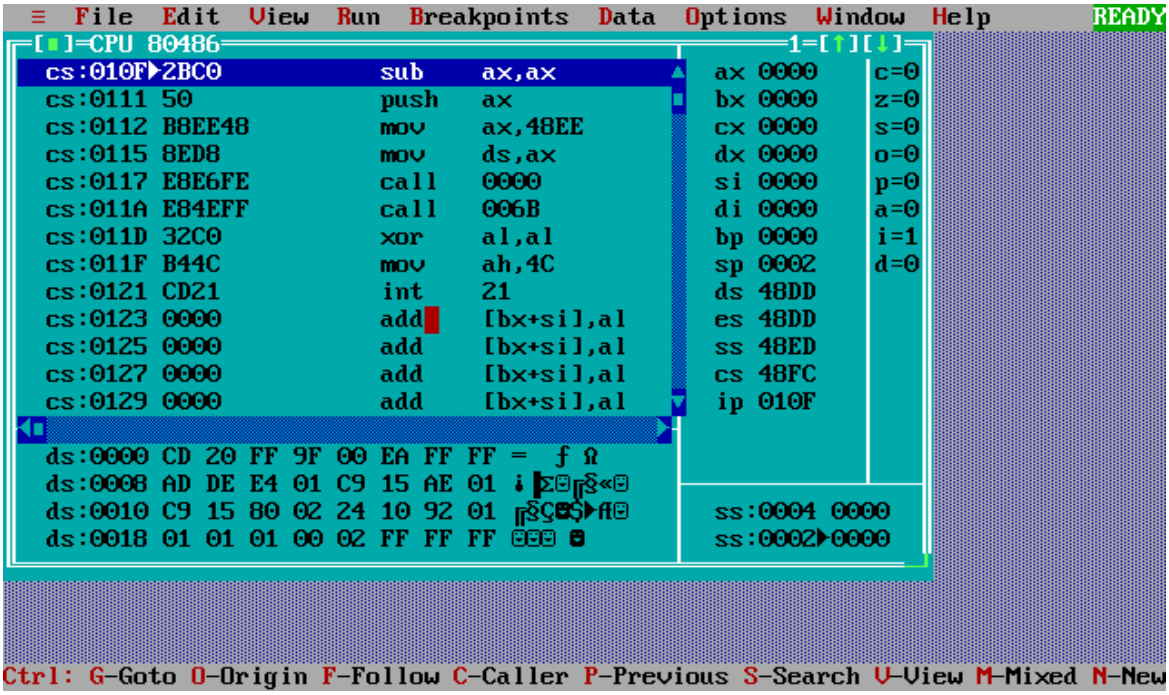


Рисунок 8 – Результат загрузки EXE файла в память

Загрузка COM модуля в основную память

1) Определяется сегментный адрес участка ОП, у которого достаточно места для загрузки программы, образ COM-файла считывается с диска

и помещается в память, начиная с PSP:100h. Код начинается с адреса 100h.

2) Сегмент PSP, размером 256 байт.
3) Ссегментные регистры CS, DS, ES и SS указывают на PSP и имеют значения 48DD.
4) Стек занимает все доступное пространство после кода. Регистр SP иимеет значение FFFEh.

Загрузка «хорошего» EXE модуля в основную память

1) Определяется адрес свободного участка ОП, в который можно загрузить программу. Создается блок памяти для PSP и программы. В IP загружается смещение точки входа в программу, которая берётся из метки после директивы END. Начиная с адреса PSP:0100h загружается код. DS и ES устанавливаются на начало сегмента PSP, SS — на начало стека. CS — на начало сегмента команд.
2) Регистры ES и DS указывают на начало PSP.
3) Стек определяется с помощью директивы ASSUME
4) Точка входа определяется при помощи директивы END

Выводы.

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