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

# ОТЧЕТ

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

Студент гр. 7383 _____ Александров Р.А.

Преподаватель _____ Ефремов М.А.

Санкт-Петербург
2018

**Цель работы.**

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

**Постановка задачи.**

Таблица 1 – Сведения о функциях программы

| Функции программы | Описание функций |
|---|---|
| PRINT | Вывод строки в консоль |
| OSVER | Получение информации о номере основной версии системы, номере её модификации, серийном номере OEM и серийном номере пользователя |
| PCVER | Получение информации о типе PC |
| TETR_TO_HEX | Перевод числа из 2 с/с в 16 с/с |
| BYTE_TO_HEX | Перевод байта из 2 с/с в 16 с/с |
| WRD_TO_HEX | Перевод слова из 2 с/с в 16 с/с |
| BYTE_TO_DEC | Перевод байта из 2 с/с в 10 с/с |
| BEGIN | Начало работы программы |

Таблица 2 – Сведения о структурах данных программы

| Название | Тип | Назначение |
|---|---|---|
| PC_TYPE | db | Type PC |
| ifPC | db | PC |
| ifPC_XT | db | PC/XT |
| ifPC_AT | db | AT |
| ifPS2_30 | db | PS2 модель 30 |
| ifPS2_50_60 | db | PS2 модель 50 или 60 |
| ifPS2_80 | db | PS2 модель 80 |
| ifPC_jr | db | PCjr |

Окончание таблицы 2

| | | |
|---|---|---|
| ifPC_Conv | db | PC Convertible |
| isVer | db | Версия ОС |
| isOem | db | Серийный номер OEM |
| isSerial | db | Серийный номер пользователя |

Таблица 3 – Последовательность действий, выполняемых утилитой

| Номер действия | Что делает |
|---|---|
| 1 | Выводит версию системы в формате xx.yy, где xx – номер основной версии, yy – номер модификации |
| 2 | Выводит серийный номер OEM |
| 3 | Выводит серийный номер пользователя |
| 4 | Выводит тип PC |

Результат работы .com модуля представлен на рис. 1.

Результат работы «хорошего» exe представлен на рис. 2, «плохого» exe – на рис. 3.

Файлы .com, «плохой» exe и «хороший» exe в шестнадцатеричном виде в FAR представлены на рис. 4, 5 и 6 соответственно.

Загрузка .com модуля в основную память представлена на рис. 7, «хорошего» exe – на рис. 8.

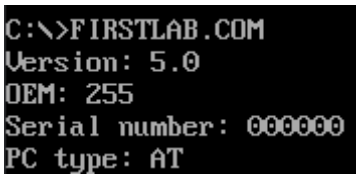



Рисунок 1 – Результат работы .COM

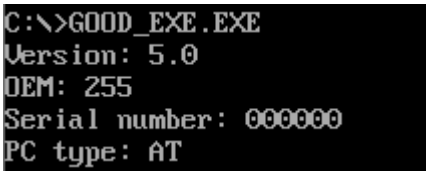



Рисунок 2 – Результат работы «хорошего» .EXE файла

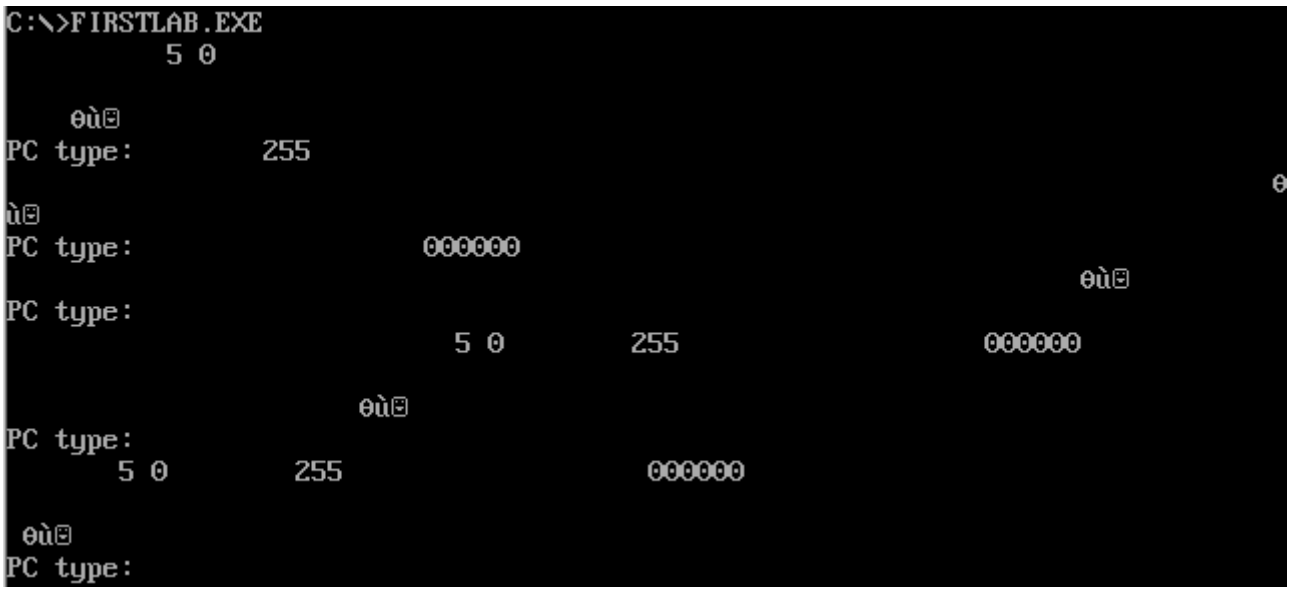
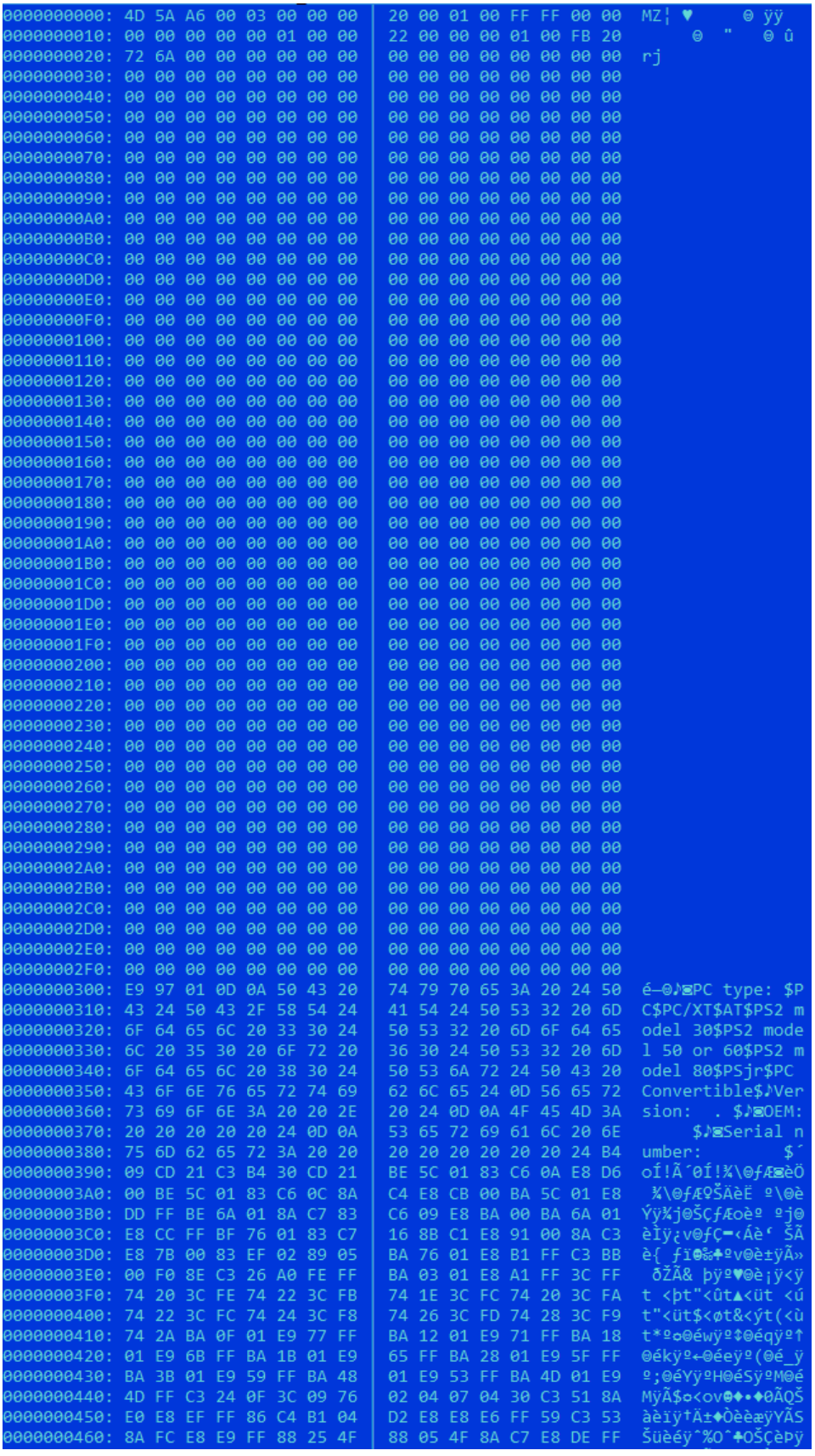



Рисунок 3 – Результат работы «плохого» .EXE файла


Рисунок 4 – Файл .COM в шестнадцатеричном виде



```
0000000000: 4D 5A A6 00 03 00 00 00  20 00 01 00 FF FF 00 00  MZ¦ ♥     ☺ ÿÿ
0000000010: 00 00 00 00 00 01 00 00  22 00 00 00 01 00 FB 20        ☺  "    ☺ û
0000000020: 72 6A 00 00 00 00 00 00  00 00 00 00 00 00 00 00  rj
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
00000002E0: 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 97 01 0D 0A 50 43 20  74 79 70 65 3A 20 24 50  é–@♪◙PC type: $P
0000000310: 43 24 50 43 2F 58 54 24  41 54 24 50 53 32 20 6D  C$PC/XT$AT$PS2 m
0000000320: 6F 64 65 6C 20 33 30 24  50 53 32 20 6D 6F 64 65  odel 30$PS2 mode
0000000330: 6C 20 35 30 20 6F 72 20  36 30 24 50 53 32 20 6D  l 50 or 60$PS2 m
0000000340: 6F 64 65 6C 20 38 30 24  50 53 6A 72 24 50 43 20  odel 80$PSjr$PC
0000000350: 43 6F 6E 76 65 72 74 69  62 6C 65 24 0D 56 65 72  Convertible$♪Ver
0000000360: 73 69 6F 6E 3A 20 20 2E  20 24 0D 0A 4F 45 4D 3A  sion:  . $♪◙OEM:
0000000370: 20 20 20 20 20 24 0D 0A  53 65 72 69 61 6C 20 6E       $♪◙Serial n
0000000380: 75 6D 62 65 72 3A 20 20  20 20 20 20 20 24 B4  umber:        $´
0000000390: 09 CD 21 C3 B4 30 CD 21  BE 5C 01 83 C6 0A E8 D6  oÍ!Ã´0Í!¾\0ƒÆ◙èÖ
00000003A0: 00 BE 5C 01 83 C6 0C 8A  C4 E8 CB 00 BA 5C 01 E8   ¾\0ƒÆ♀ŠÄèË º\0è
00000003B0: DD FF BE 6A 01 8A C7 83  C6 09 E8 BA 00 BA 6A 01  Ýÿ¾j0ŠÇƒÆ○èº ºj0
00000003C0: E8 CC FF BF 76 01 83 C7  16 8B C1 E8 91 00 8A C3  èÌÿ¿v0ƒÇ▬‹Áè‘ ŠÃ
00000003D0: E8 7B 00 83 EF 02 89 05  BA 76 01 E8 B1 FF C3 BB  è{ ƒï0‰♦ºv0è±ÿÃ»
00000003E0: 00 F0 8E C3 26 A0 FE FF  BA 03 01 E8 A1 FF 3C FF   ðŽÃ& þÿº♥0è¡ÿ<ÿ
00000003F0: 74 20 3C FE 74 22 3C FB  74 1E 3C FC 74 20 3C FA  t <þt"<ût▲<üt <ú
0000000400: 74 22 3C FC 74 24 3C F8  74 26 3C FD 74 28 3C F9  t"<üt$<øt&<ýt(<ù
0000000410: 74 2A BA 0F 01 E9 77 FF  BA 12 01 E9 71 FF BA 18  t*º☼0éwÿº↕0éqÿº↑
0000000420: 01 E9 6B FF BA 1B 01 E9  65 FF BA 28 01 E9 5F FF  ☺ékÿº←☺éeÿº(☺é_ÿ
0000000430: BA 3B 01 E9 59 FF BA 48  01 E9 53 FF BA 4D 01 E9  º;☺éYÿºH☺éSÿºM☺é
0000000440: 4D FF C3 24 0F 3C 09 76  02 04 07 04 30 C3 51 8A  MÿÃ$☼<○v☻♦•♦0ÃQŠ
0000000450: E0 E8 EF FF 86 C4 B1 04  D2 E8 E8 E6 FF 59 C3 53  àèïÿ†Ä±♦ÒèèæÿYÃS
0000000460: 8A FC E8 E9 FF 88 25 4F  88 05 4F 8A C7 E8 DE FF  Šüèéÿˆ%O^♣OŠÇèÞÿ
```

Рисунок 5 – «Плохой» .EXE в шестнадцатеричном виде

```
0000000000: 4D 5A DA 01 02 00 01 00  20 00 01 00 FF FF 00 00  MZÚ☺☻ ☺   ☺ ÿÿ
0000000010: 18 00 00 00 05 00 0B 00  22 00 00 00 01 00 FB 20  ↑   ♣ ♂ "   ☺ û
0000000020: 72 6A 0A 00 0B 00 00 00  00 00 00 00 00 00 00 00  rj◙ ♂
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: 0D 0A 50 43 20 74 79 70  65 3A 20 24 50 43 24 50  ♪◙PC type: $PC$P
0000000230: 43 2F 58 54 24 41 54 24  50 53 32 20 6D 6F 64 65  C/XT$AT$PS2 mode
0000000240: 6C 20 33 30 24 50 53 32  20 6D 6F 64 65 6C 20 35  l 30$PS2 model 5
0000000250: 30 20 6F 72 20 36 30 24  50 53 32 20 6D 6F 64 65  0 or 60$PS2 mode
0000000260: 6C 20 38 30 24 50 53 6A  72 24 50 43 20 43 6F 6E  l 80$PSjr$PC Con
0000000270: 76 65 72 74 69 62 6C 65  24 0D 56 65 72 73 69 6F  vertible$♪Versio
0000000280: 6E 3A 20 20 2E 20 24 0D  0A 4F 45 4D 3A 20 20 20  n:  . $♪◙OEM:
0000000290: 20 20 24 0D 0A 53 65 72  69 61 6C 20 6E 75 6D 62    $♪◙Serial numb
00000002A0: 65 72 3A 20 20 20 20 20  20 20 20 24 00 00 00 00  er:        $
00000002B0: B4 09 CD 21 C3 1E 2B C0  50 B8 02 00 8E D8 E8 0F  ´oÍ!Ã▲+ÀP¸☻ ŽØè☼
00000002C0: 00 E8 5B 00 32 C0 B4 4C  CD 21 CB B4 09 CD 21 C3   è[ 2À´LÍ!Ë´oÍ!Ã
00000002D0: 50 33 C0 B4 30 CD 21 BE  59 00 83 C6 0A E8 D7 00  P3À´0Í!¾Y ƒÆ◙è×
00000002E0: BE 59 00 83 C6 0C 8A C4  E8 CC 00 BA 59 00 E8 DA  ¾Y ƒÆ♀ŠÄèÌ ºY èÚ
00000002F0: FF BE 67 00 8A C7 83 C6  09 E8 BB 00 BA 67 00 E8  ÿ¾g ŠÇƒÆ○è» ºg è
0000000300: AE FF BF 73 00 83 C7 16  8B C1 E8 92 00 8A C3 E8  ®ÿ¿s ƒÇ▬‹Áè' ŠÃè
0000000310: 7C 00 83 EF 02 89 05 BA  73 00 E8 AE FF 58 C3 BB  | ƒï☻‰♣ºs è®ÿXÃ»
0000000320: 00 F0 8E C3 26 A0 FE FF  BA 00 00 E8 9D FF 3C FF   ðŽÃ& þÿº  è¤ÿ<ÿ
0000000330: 74 20 3C FE 74 22 3C FB  74 1E 3C FC 74 20 3C FA  t <þt"<ût▲<üt <ú
0000000340: 74 22 3C FC 74 24 3C F8  74 26 3C FD 74 28 3C F9  t"<üt$<øt&<ýt(<ù
0000000350: 74 2A BA 0C 00 E9 73 FF  BA 0F 00 E9 6D FF BA 15  t*º♀ ésÿº☼ émÿº§
0000000360: 00 E9 67 FF BA 18 00 E9  61 FF BA 25 00 E9 5B FF   égÿº↑ éaÿº% é[ÿ
0000000370: BA 38 00 E9 55 FF BA 45  00 E9 4F FF BA 4A 00 E9  º8 éUÿºE éOÿºJ é
0000000380: 49 FF C3 24 0F 3C 09 76  02 04 07 04 30 C3 51 8A  IÿÃ$☼<○v☻♦•♦0ÃQŠ
0000000390: E0 E8 EF FF 86 C4 B1 04  D2 E8 E8 E6 FF 59 C3 53  àèïÿ†Ä±♦ÒèèæÿYÃS
00000003A0: 8A FC E8 E9 FF 88 25 4F  88 05 4F 8A C7 E8 DE FF  Šüèéÿˆ%Oˆ♣OŠÇèÞÿ
00000003B0: 88 25 4F 88 05 5B C3 51  52 32 E4 33 D2 B9 0A 00  ˆ%Oˆ♣[ÃQR2ä3Ò¹◙
00000003C0: F7 F1 80 CA 30 88 14 4E  33 D2 3D 0A 00 73 F1 3C  ÷ñ€Ê0ˆ¶N3Ò=◙ sñ<
```

Рисунок 6 – «Хороший» .EXE в шестнадцатеричном виде

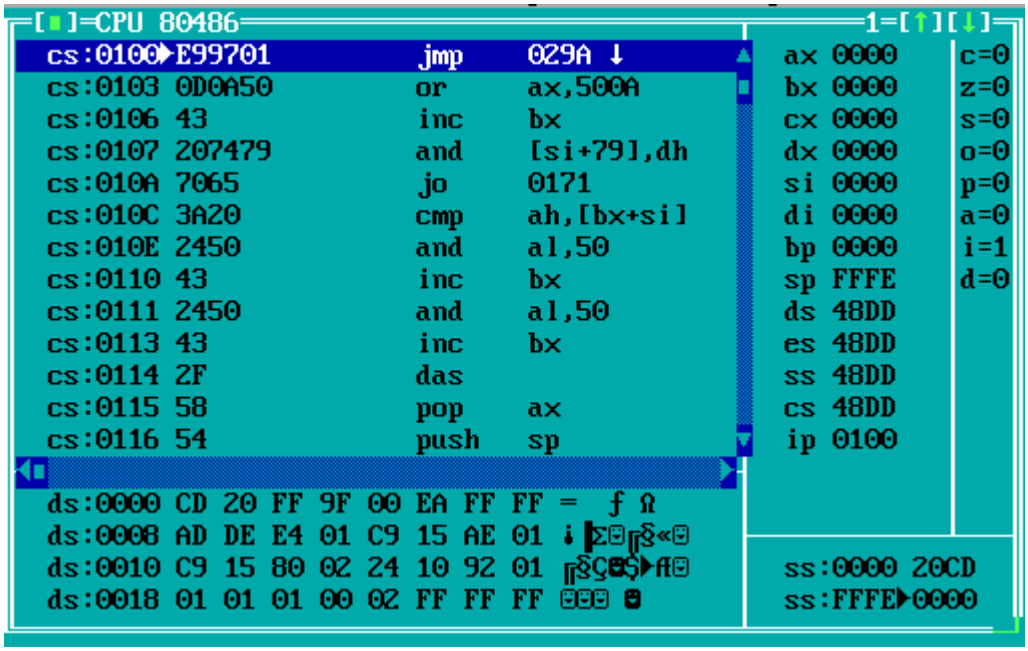



Рисунок 7 – Загрузка .COM модуля в основную память

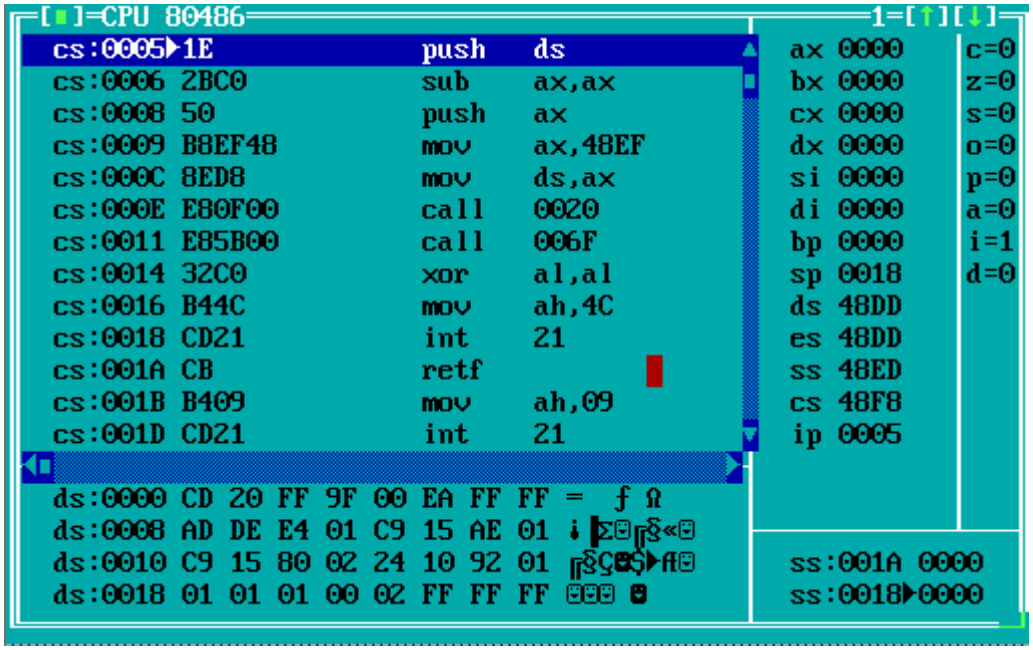



Рисунок 8 – Загрузка «хорошего» .EXE модуля в основную память

Ответы на контрольные вопросы представлены в приложении А.

**Выводы.**

В лабораторной работы были исследованы различия в структурах исходных текстов загрузочный модулей типов .COM и .EXE, структур файлов этих модулей и способах их загрузки в основную память.

# ПРИЛОЖЕНИЕ А
# ОТВЕТЫ НА КОНТРОЛЬНЫЕ ВОПРОСЫ

**Отличия исходный текстов COM и EXE программ**:

1. Сколько сегментов должна содержать COM-программа?

COM-программа должна содержать 1 сегмент.

2. EXE-программа?

EXE-программа должна содержать не менее 1 сегмента.

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

Обязательно должна быть директива org 100h (org 256), так как операционная система при загрузке программы размещает в ее первые 100h байт префикс программного сегмента.

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

Нельзя использовать команды вида mov <регистр>, seg <имя сегмента> и команды, которые используют дальнюю адресацию, так как отсутствует таблица настроек. Таблица (присутствующая в «хорошем» EXE-файле) состоит из элементов, число которых записано в байтах 06-07. Элемент таблицы настройки состоит из двух полей: 2-байтного смещения и 2-байтного сегмента, и указывает слова в загрузочном модуле, содержащее адрес, который должен быть настроен на место памяти, в которое загружается задача.

**Отличия форматов файлов COM и EXE модулей**:

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

COM-файл содержит данные и машинные команды. Код начинается с адреса 0h, но при загрузке модуля устанавливается смещение в 100h.

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

В «плохом» EXE данные и код содержатся в одном сегменте. С адреса 0h идёт таблица настроек. Код располагается с адреса 300h

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

В «хорошем» EXE данные, стек и код разделены по сегментам. Код располагается с адреса 220h.

Как видно на рис. 5 и рис. 6 в «хорошем» и «плохом» EXE с адреса 0 располагается заголовок с таблицей настроек, в COM-модуле код начинается с адреса 0h, но при загрузке модуля устанавливается смещение в 100h.

При комментировании директивы Assume программа не компилируется. Эта директива показывает, в значение какого сегмента установлен данный сегментный регистр, компилятору необходимо знать о сегменте кода для того, чтобы установить выполняемую программу.

**Загрузка COM модуля в основную память**:

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

Во время загрузки COM- программы выделяется первый свободный сегмент памяти и в его начале размещается PSP. Регистр SP (указатель стека) устанавливается на конец сегмента программы. Сегмент кода располагается с адреса 48DDh.

2. Что располагается с адреса 0?

Сегмент PSP

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

При загрузке программы они указывают на начало PSP.

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

Регистр SP указывает на конец стека (FFFEh), SS – на начало (0h). Адреса стека находятся в диапазоне 0h – FFFEh.

**Загрузка «хорошего» EXE модуля в основную память**:

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

Выделяется сегмент для PSP. Значение этого сегмента записывается в регистры ES (дополнительный сегмент) и DS. SS указывает на начало сегмента стека 48EDh, CS – на начало сегмента команд 48F8h.

2. На что указывают регистры DS и ES?

Регистры DS и ES указывают на начало сегмента PSP.

3. Как определяется стек?

Стек определяется с помощью директивы SEGMENT STACK.

4. Как определяется точка входа?

Точка входа определяется директивой END. После этой директивы указывается метка (адрес), куда переходит программа при запуске.