

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. 7383

Власов Р.А.

Преподаватель

Ефремов М.А.

Санкт-Петербург
2019

Цель работы: исследование различий в структурах исходных текстов модулей .COM и .EXE, структур файлов загрузочных модулей и способов их загрузки в основную память.

Ход работы.

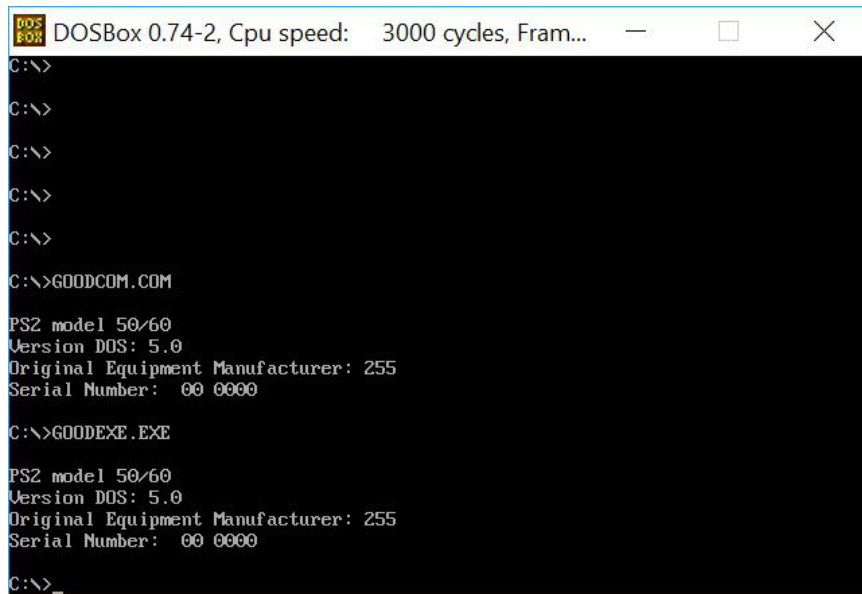
Функции и структуры данных управляющей программы:

Название	Назначение
PRINT_STRING	Вывод сообщения на экран
ENDL	Перевод каретки на новую строку
TETR_TO_HEX	Перевод числа из 2-ой в 16-ую с/с (1/2 байта)
BYTE_TO_HEX	Перевод числа из 2-ой в 16-ую с/с (1 байт)
WRD_TO_HEX	Перевод числа из 2-ой в 16-ую с/с (2 байта)
BYTE_TO_DEC	Перевод числа из 2-ой в 10-ую с/с (1 байт)
GET_PC_TYPE	Определяет тип IBM PC
GET_SYS_VER	Определяет версию системы
GET_OEM_NUM	Определяет OEM
GET_SERIAL_NUM	Определяет серийный номер пользователя

Структуры данных управляющей программы:

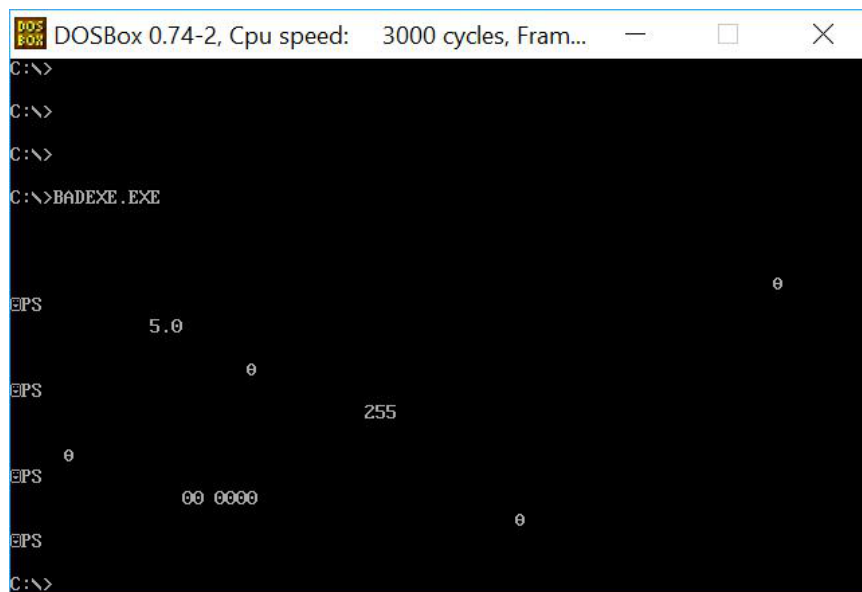
Наименование	Назначение
PC_TYPE	Хранит тип IBM PC
SYSTEM_VERSION	Хранит версию системы
OEM_NUMBER	Хранит номер OEM
SERIAL_NUMBER	Хранит серийный номер пользователя

Программа определяет и выводит на экран тип IBM PC, версию ОС, серийный номер OEM и серийный номер пользователя. Результаты работы программы приведены на рисунках 1 и 2.



```
DOS FOR DOSBox 0.74-2, Cpu speed: 3000 cycles, Fram...
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>GOODCOM.COM
PS2 model 50/60
Version DOS: 5.0
Original Equipment Manufacturer: 255
Serial Number: 00 0000
C:\>GOODEXE.EXE
PS2 model 50/60
Version DOS: 5.0
Original Equipment Manufacturer: 255
Serial Number: 00 0000
C:\>_
```

Рисунок 1 – Результат работы программ GOODCOM.COM и GOODEXE.EXE



```
DOS FOR DOSBox 0.74-2, Cpu speed: 3000 cycles, Fram...
C:\>
C:\>
C:\>
C:\>BADEXE.EXE
EPS
5.0
0
EPS
255
0
EPS
00 0000
EPS
0
C:\>
```

Рисунок 2 – Результат работы программы BADEXE.EXE

Ответы на контрольные вопросы:

Отличия исходных текстов COM и EXE программ

1. Сколько сегментов должна содержать COM-программа?

COM-программа должна содержать один сегмент.

2. Сколько сегментов должна содержать EXE-программа?

EXE-программа может содержать один или более сегментов.

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

Обязательная должна быть директива `ORG 100h`. Она нужна по той причине, что при загрузке модуля в ОП в начале COM-программы определяется 256-байтовый (`100h`) префикс программного сегмента, так что адресация имеет смещение в 256 байт от нулевого адреса. Это смещение мы и задаём директивой `ORG 100h` (в отличие от EXE-программы, где PSP расположен вне кодового сегмента и, следовательно, явно определять смещение там не нужно). Также обязательна директива `ASSUME`. С ее помощью ассемблеру сообщается информация о соответствии между сегментными регистрами, и программными сегментами. При ее отсутствии MASM укажет ошибку: “missing or unreachable CS”.

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

Нельзя использовать команды с дальней адресацией, поскольку в COM-программе отсутствует таблица настроек, которая указывает, какие абсолютные адреса при загрузке должны быть изменены, так как до загрузки неизвестно, куда будет загружена программа.

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`). Структура файла показана на рисунке 3.

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

Структура «плохого» EXE-файла менее компактна, чем у COM-файла. Код располагается с адреса 300h, с нулевого адреса располагается таблица настроек, при помощи которых строится данный EXE-файл. Структура файла показана на рисунке 4.

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

Структура «хорошего» EXE-файла несколько компактнее, чем структура «плохого» файла, так как в этом файле отсутствует директива ORG 100h, резервирующая пространство для заголовка. Именно поэтому код располагается с адреса 200h, а не с 300h, как в «плохом» EXE-файле. Структура файла показана на рисунке 5.

E:\OS\lab1\GOODCOM.COM															
00000000:	0AE9	5001	2453	5350	582F	2454	5350	2032	00000000	'					
000000010:	6F6D	6564	206C	3033	5024	3253	6D20	646F	00000001						
000000020:	6C65	3520	2F30	3036	5024	3253	6D20	646F	00000002						
000000030:	6C65	3820	2430	4350	726A	5024	2043	6F43	00000003	-0					
000000040:	766E	7265	6974	6C62	2465	6556	7372	6F69	00000004						
000000050:	206E	4F44	3A53	2020	2020	4F24	6972	6967	00000005	+					
000000060:	616E	206C	7145	6975	6D70	6E65	2074	614D	00000006	0					
000000070:	756E	6166	7463	7275	7265	203A	2020	2020	00000007	+					
000000080:	5324	7265	6169	206C	754E	626D	7265	203A	00000008	>					
000000090:	2020	2020	2020	2020	2020	2020	2020	2420	00000009	+					
0000000A0:	B450	CD09	5821	50C3	B452	B202	CD0A	B221	0000000A						
0000000B0:	CD0D	5A21	C358	5251	E432	D233	0AB9	F700	0000000B						
0000000C0:	80F1	30CA	1488	334E	3DD2	000A	F173	003C	0000000C	<					
0000000D0:	0474	300C	0488	595A	53C3	FC8A	12E8	8800	0000000D	V					
0000000E0:	4F25	0588	8A4F	E8C7	0007	2588	884F	5B05	0000000E	.					
0000000F0:	51C3	E08A	0BE8	8600	B1C4	D204	E8E8	0002	0000000F						
000000100:	C359	0F24	093C	0276	0704	3004	1EC3	96E8	00000010	c					
000000110:	B8FF	F000	D88E	FEBB	8AFF	1F07	FF3C	0775	00000011						
000000120:	168D	0103	48EB	3C90	75FE	8D07	0616	EB01	00000012						
000000130:	9040	FB3C	0675	06BA	EB01	9036	FA3C	0775	00000013						
000000140:	168D	010C	2BEB	3C90	75FC	8D07	1916	EB01	00000014						
000000150:	9020	F83C	0775	168D	0129	15EB	3C90	75FD	00000015						
000000160:	8D07	3616	EB01	900A	F93C	168D	013B	01EB	00000016	q					
000000170:	E890	FF2C	30E8	B4FF	CD30	8D21	4A36	5601	00000017						
000000180:	8350	0FC6	C48A	2DE8	B0FF	882E	4E04	5A58	00000018						
000000190:	23E8	E8FF	FF0A	0EE8	8DFF	5B36	5601	C683	00000019						
0000001A0:	8A23	E8C7	FF10	E85A	FEF6	FAE8	8DFE	813E	0000001A						
0000001B0:	5701	C783	8A10	E8C3	FF37	86AA	AAC4	C783	0000001B						
0000001C0:	8B04	E8C1	FF13	E85A	FED6	DAE8	B8FE	4C00	0000001C						
0000001D0:	21CD								0000001D						

Рисунок 3 – Структура COM файла

E:\OS\lab1\BADEXE.EXE		E:\OS\lab1\BADEXE.EXE	
00000000: 4D 5A D2 00 03 00 00 00	20 00 00 00 FF FF 00 00	000000270: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000010: 00 00 59 48 00 01 00 00	1E 00 00 00 01 00 00 00	000000280: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000020: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000290: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000030: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000002A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000040: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000002B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000050: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000002C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000060: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000002D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000070: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000002E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000080: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000002F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000090: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000300: E9 0A 01 50 53 24 50 53	2F 58 54 24 50 53 32 20
0000000A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000310: 6D 6F 64 65 6C 20 33 30	24 50 53 32 20 6D 6F 64
0000000B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000320: 65 6C 20 35 30 2F 36 30	24 50 53 32 20 6D 6F 64
0000000C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000330: 65 6C 20 38 30 24 50 43	6A 72 24 50 43 20 43 6F
0000000D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000340: 6E 76 65 72 74 69 62 6C	65 24 56 65 72 73 69 6F
0000000E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000350: 6E 20 44 4F 53 3A 20 20	20 20 24 4F 72 69 67 69
0000000F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000360: 6E 61 6C 20 45 71 75 69	70 6D 65 6E 74 20 4D 61
000000100: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000370: 6E 75 66 61 63 74 75 72	65 72 3A 20 20 20 20 20
000000110: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000380: 24 53 65 72 69 61 6C 20	4E 75 6D 62 65 72 3A 20
000000120: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000390: 20 20 20 20 20 20 20 20	20 20 20 20 20 20 20 20
000000130: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003A0: 58 04 09 CD 21 58 C3 52	52 84 02 B2 0A CD 21 B2
000000140: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003B0: 0D CD 21 5A 58 C3 51 52	32 E4 33 D2 B9 0A 00 F7
000000150: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003C0: F1 80 CA 30 88 14 4E 33	D2 3D 0A 00 73 F1 3C 00
000000160: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003D0: 74 64 0C 30 88 04 5A 59	C3 53 8A FC E8 12 00 88
000000170: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003E0: 25 4F 88 05 4F 8A C7 E8	07 00 88 25 4F 88 05 58
000000180: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003F0: C3 51 8A E0 E8 00 00 86	C4 B1 04 D2 E8 E8 02 00
000000190: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000400: 59 C3 24 0F 3C 09 76 02	04 07 04 30 C3 1E E8 07
0000001A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000410: FF B8 00 F0 8E D8 BB FE	FF 8A 07 1F 3C FF 76 02
0000001B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000420: 8D 16 03 01 EB 48 90 3C	FE 75 07 8D 16 06 01 EB
0000001C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000430: 40 9C 3C F8 75 06 BA 06	01 EB 36 90 3C FA 75 07
0000001D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000440: 8D 16 0C 01 EB 28 90 3C	FC 75 07 8D 16 19 01 EB
0000001E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000450: 20 9C 3C F8 75 07 8D 16	29 01 EB 15 90 3C FD 75
0000001F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000460: 07 8D 16 36 01 EB 0A 90	3C F9 8D 16 3B 01 EB 01
000000200: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000470: 9E 08 2C FF E8 30 FF 84	38 CD 21 8D 36 4A 01 56
000000210: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000480: 50 83 C6 0F 8A CA E8 2D	FF 80 2E 88 04 4E 58 5A
000000220: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000490: E2 23 FF E8 0A FF E8 0E	FF 8D 36 58 01 56 83 C6
000000230: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000004A0: 28 BA C7 E8 10 FF 5A E8	F6 FE E8 FA FE 8D 3E 81
000000240: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000004B0: 01 57 83 C7 10 BA C3 E8	37 FF AA 86 CA AA 83 C7
000000250: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000004C0: 04 88 C1 E8 13 FF 5A E8	D6 FE E8 DA FE B8 00 4C
000000260: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000004D0: CD 21	II

Рисунок 4 – Структура «плохого» EXE файла

E:\OS\lab1\GOODEXE.EXE			
00000000: 4D 5A D2 00 03 00 00 00	20 00 00 00 FF FF 00 00	000000270: 38 30 24 50 43 6A 72 24	50 43 20 43 6F 6E 76 65
000000010: 00 00 5B 0E 6D 00 0E 00	1E 00 00 00 01 00 0E 00	000000280: 72 74 69 62 6C 65 24 56	65 72 73 69 6F 6E 20 44
000000020: 0E 00 78 0E 0E 00 E0 00	0E 00 04 01 0E 00 1A 01	000000290: 4F 53 3A 20 20 20 20 24	4F 72 69 67 69 6E 61 6C
000000030: 0E 00 3C 01 0E 00 00 00	00 00 00 00 00 00 00 00	0000002A0: 20 45 71 75 69 70 6D 65	6E 74 20 4D 61 6E 75 66
000000040: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000002B0: 61 63 74 75 72 65 72 3A	20 20 20 20 20 24 53 65
000000050: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000002C0: 72 69 61 6C 20 4E 75 6D	62 65 72 3A 20 20 20 20
000000060: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000002D0: 20 20 20 20 20 20 20 20	20 20 20 20 24 00 00 00
000000070: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000002E0: 50 84 09 CD 21 58 C3 52	52 84 02 B2 0A CD 21 B2
000000080: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000002F0: 0D CD 21 5A 58 CB 51 52	32 E4 33 D2 B9 0A 00 F7
000000090: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000300: F1 80 CA 30 88 14 4E 33	D2 3D 0A 00 73 F1 3C 00
0000000A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000310: 74 04 0C 30 88 04 5A 59	C3 24 0F 3C 09 76 02 04
0000000B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000320: 07 04 30 C3 51 8A E0 E8	EF FF 86 C4 B1 04 D2 E8
0000000C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000330: E8 E6 FF 59 C3 53 8A FC	E8 E9 FF 88 25 4F 88 05
0000000D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000340: 4F 8A C7 E8 DE FF 88 25	4F 88 05 5B C3 88 04 00
0000000E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000350: 8E D8 8E C0 1E 9A 07 00	0E 00 88 00 F0 8E D8 BB
0000000F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000360: FE FF 8A 07 1F 3C FF 75	07 8D 16 00 00 EB 48 90
000000100: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000370: 3C FE 75 07 8D 16 03 00	EB 40 90 3C F8 75 06 BA
000000110: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000380: 03 00 EB 36 90 3C FA 75	07 8D 16 09 00 EB 28 90
000000120: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000390: 3C FC 75 07 8D 16 16 00	EB 20 90 3C F8 75 07 8D
000000130: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003A0: 16 26 00 EB 15 90 3C FD	75 07 8D 16 33 00 EB 0A
000000140: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003B0: 90 3C F9 8D 16 38 00 EB	01 90 E8 23 FF 9A 07 00
000000150: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003C0: 0E 00 B4 30 CD 21 8D 36	47 00 56 50 83 C6 0F 8A
000000160: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003D0: C4 E8 22 FF B0 2E 88 04	4E 58 5A E8 18 FF E8 FF
000000170: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003E0: FE 9A 07 00 0E 00 8D 36	58 00 56 83 C6 23 8A C7
000000180: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000003F0: E8 03 FF 5A E8 E9 FE 9A	07 00 0E 00 8D 3E 7E 00
000000190: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000400: 57 83 C7 10 8A C3 E8 1B	FF AA 86 CA AA 83 C7 04
0000001A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000410: 8B C1 E8 20 FF 5A E8 C7	FE 9A 07 00 0E 00 B8 00
0000001B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	000000420: 4C CD 21	LI
0000001C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000001D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000001E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
0000001F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
000000200: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
000000210: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
000000220: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
000000230: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
000000240: 50 53 24 50 53 2F 58 54	24 50 53 32 20 6D 6F 64	PS\$PS/XT\$PS2 mod	
000000250: 65 6C 20 33 30 24 50 53	32 20 6D 6F 64 65 6C 20	e1 30\$PS2 model	
000000260: 35 30 2F 36 30 24 50 53	32 20 6D 6F 64 65 6C 20	50/60\$PS2 model	

Рисунок 5 – Структура «хорошего» EXE файла

Загрузка COM-модулей в основную память

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

Порядок загрузки модуля COM: PSP, данные и код, стек. Код начинается с адреса 100h.

2. Что располагается с адреса 0?

С нулевого адреса располагается PSP.

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

Все сегментные регистры имеют значение «48DD» и указывают на начало PSP.

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

Стек занимает всё свободное пространство до конца файла (размер .COM файла не может превышать 64 кб), оставшееся после загрузки данных и кода. В данном случае значение регистра SP=FFFE.

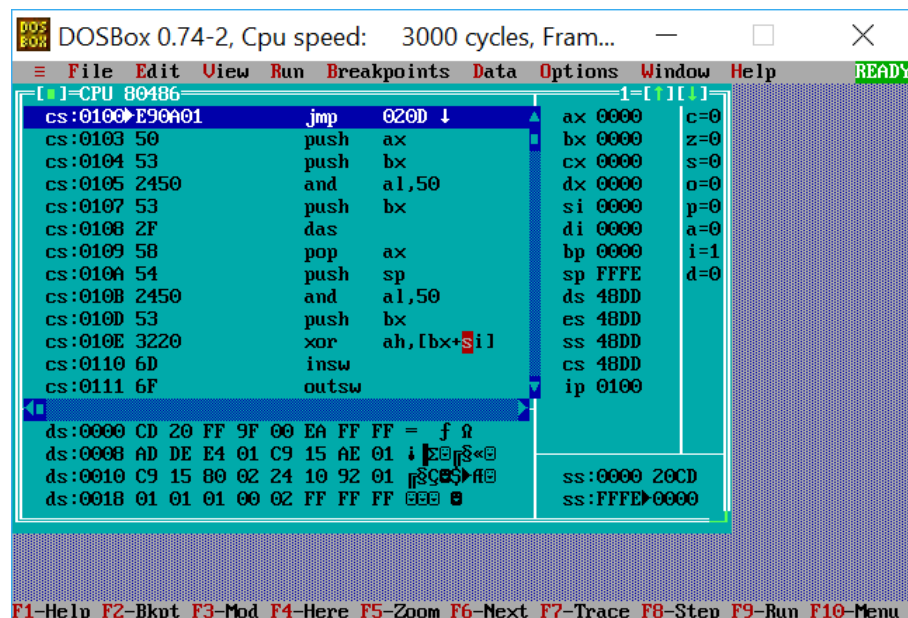


Рисунок 6 – COM модуль в отладчике TD.EXE

Загрузка «хорошего» EXE-модуля в основную память

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

Порядок загрузки EXE-модуля: PSP, сегмент кода, сегмент данных, сегмент стека. Сегментные регистры на момент загрузки программы имеют значения: ES=48DD, CS=48FB, DS=48DD, SS=48ED. На начальном этапе ES=DS, так как не были выполнены команды “mov ax, data; mov ds, ax”, т.е. в регистр данных не был помещён адрес сегмента данных.

2. На что указывают регистры DS и ES?

ES указывает на начало PSP, DS указывает на начало данных. После выполнения команд (см. предыдущий вопрос), значение DS= 48F1.

3. Как определяется стек?

Для стека в программе выделяется отдельный сегмент с параметром STACK. SS указывает на начало стека, а SP – на верхушку стека.

4. Как определяется точка входа?

Точка входа определяется с помощью директивы END <точка_входа>. Точкой входа можно указать как процедуру, так и метку.

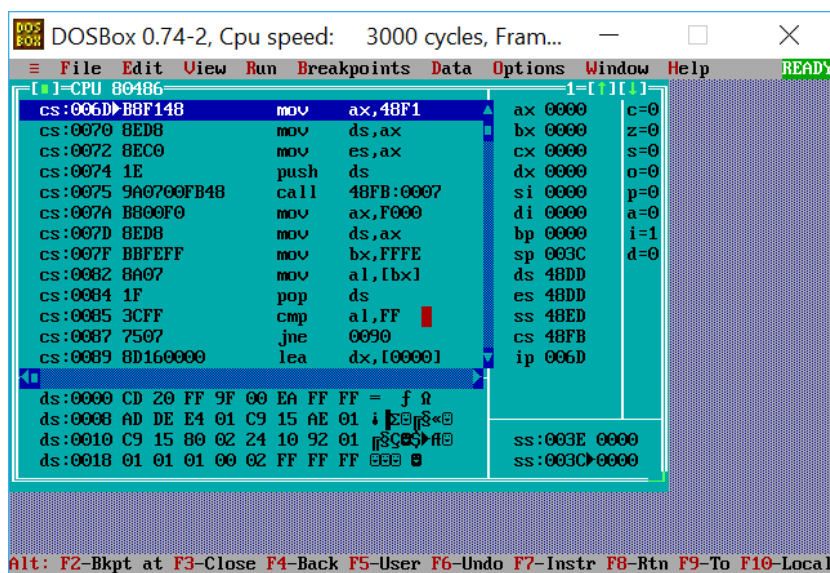


Рисунок 7 – EXE модуль в отладчике TD.EXE

Выводы:

В ходе данной лабораторной работы было проведено сравнение структуры COM и EXE файлов, исследованы различия в исходных текстах модулей COM и EXE, а также были сравнены способы их загрузки в память.