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. 8381 _____ Сосновский Д.Н.

Преподаватель _____ Ефремов М.А.

Санкт-Петербург

2020

Цель работы.

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

Основные теоретические положения.

Тип IBM PC хранится в байте по адресу 0F000:0FFFEh, в предпоследнем байте ROM BIOS. Соответствие кода и типа представлены в табл.1.

Таблица 1 – Соответствие кода и типа PC

Тип IBM PC	Код
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

Для определения версии MS DOS следует воспользоваться функцией 30H прерывания 21H. Входным параметром является номер функции в AH.

Выходными параметрами являются:

- AL - номер основной версии. Если 0, то < 2.0

- AH - номер модификации
- BH - серийный номер OEM (Original Equipment Manufacturer)
- BL:CX - 24-битовый серийный номер пользователя.

Ход работы.

Мною был написан исходный код на языке ассемблер .COM модуля, определяющего тип PC, версию системы MS DOS и серийный номер пользователя. Полученный модуль был скомпонован, в результате чего был получен «плохой» .EXE модуль. Далее с помощью программы EXE2BIN был сгенерирован «хороший» .COM модуль. Изображения работы приведены на рисунках 1-3.

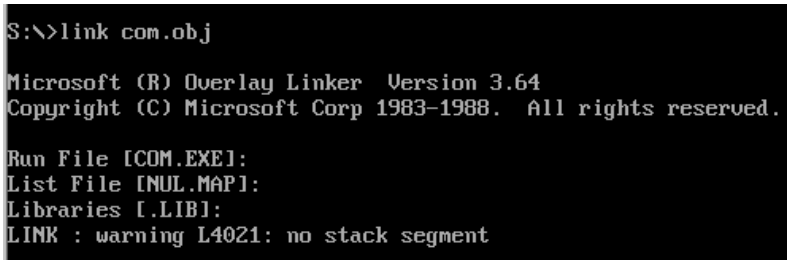

Рисунок 1 – предупреждение об отсутствии сегмента стека

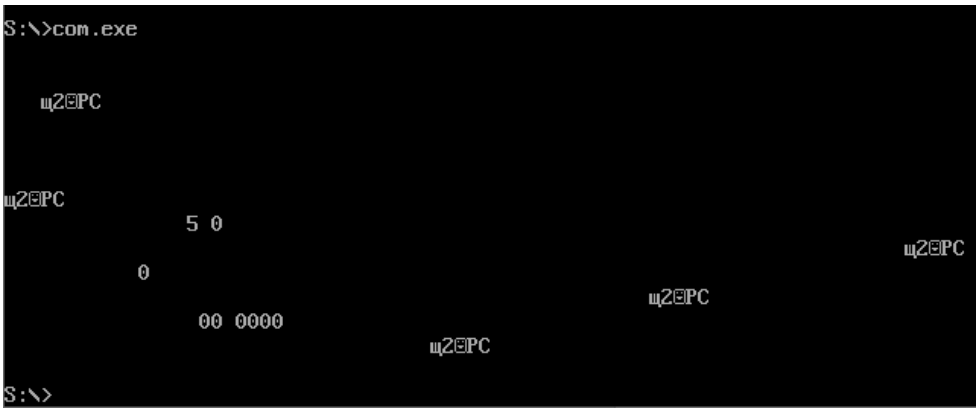

Рисунок 2 - результат выполнения "плохого" .EXE модуля

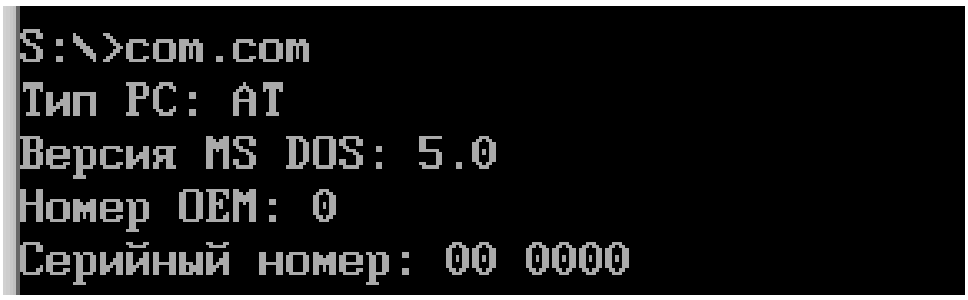

Рисунок 3 - результат выполнения "Хорошего" .COM модуля

Следующим шагом была разработка текста исходного .EXE модуля. Результат работы приведён на рисунке 4.

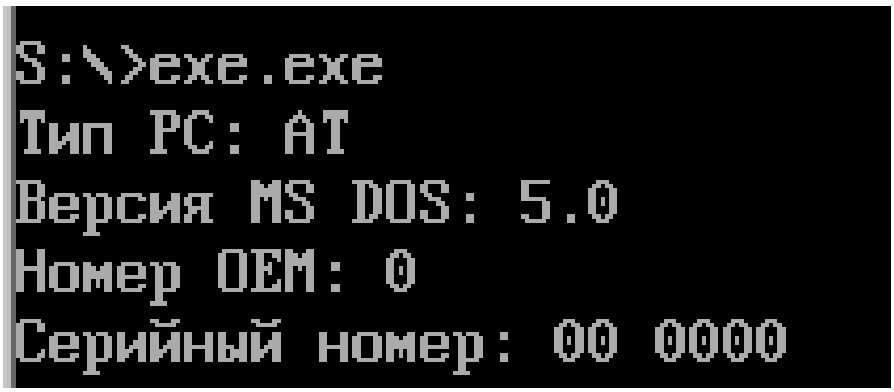

Рисунок 4 - результат работы «хорошего» EXE модуля

Ответы на контрольные вопросы

Отличия исходных текстов COM и EXE программ

1) Сколько сегментов должна содержать COM-программа?

COM – программа содержит один сегмент.

2) EXE-программа?

EXE – программа может содержать несколько сегментов: сегмент кода, сегмент данных и сегмент стека. Их возможное количество зависит от модели памяти.

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

Обязательно присутствие директивы ORG 100h, которая выделяет место под PSP и устанавливает адрес начала выполнения кода после PSP. Так же обязательно присутствие директивы ASSUME, которая ставит адрес сегмента кода и данных в регистры cs и ds.

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

Нельзя использовать команды, которые работают с адресами сегментов, потому что в COM-программе нет таблицы настроек с местоположением адресов в коде, а значит адреса сегментов не известны, пока программа не будет запущена.

Отличия форматов файлов COM и EXE модулей

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

Вид COM-файла в шестнадцатеричном формате представлен на рисунке 5.

Рисунок 5 - COM файл в 16-ричном формате

Видно, что этот файл состоит из одного сегмента. Код начинается на 130h с 3-го байта.

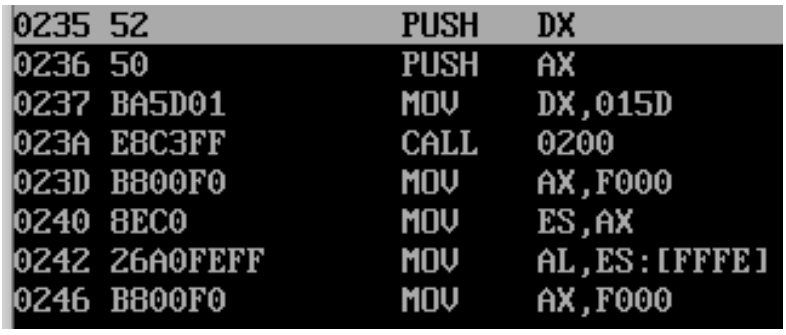

Рисунок 6 - адрес начала кода

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

«Плохой» EXE в 16-ричном виде представлен на рисунке 7.

Рисунок 7 - "плохой" EXE модуль

Код располагается с адреса 430h. С адреса 0 располагается таблица настроек.

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

Структура «хорошего» EXE приведена на рисунке 8.

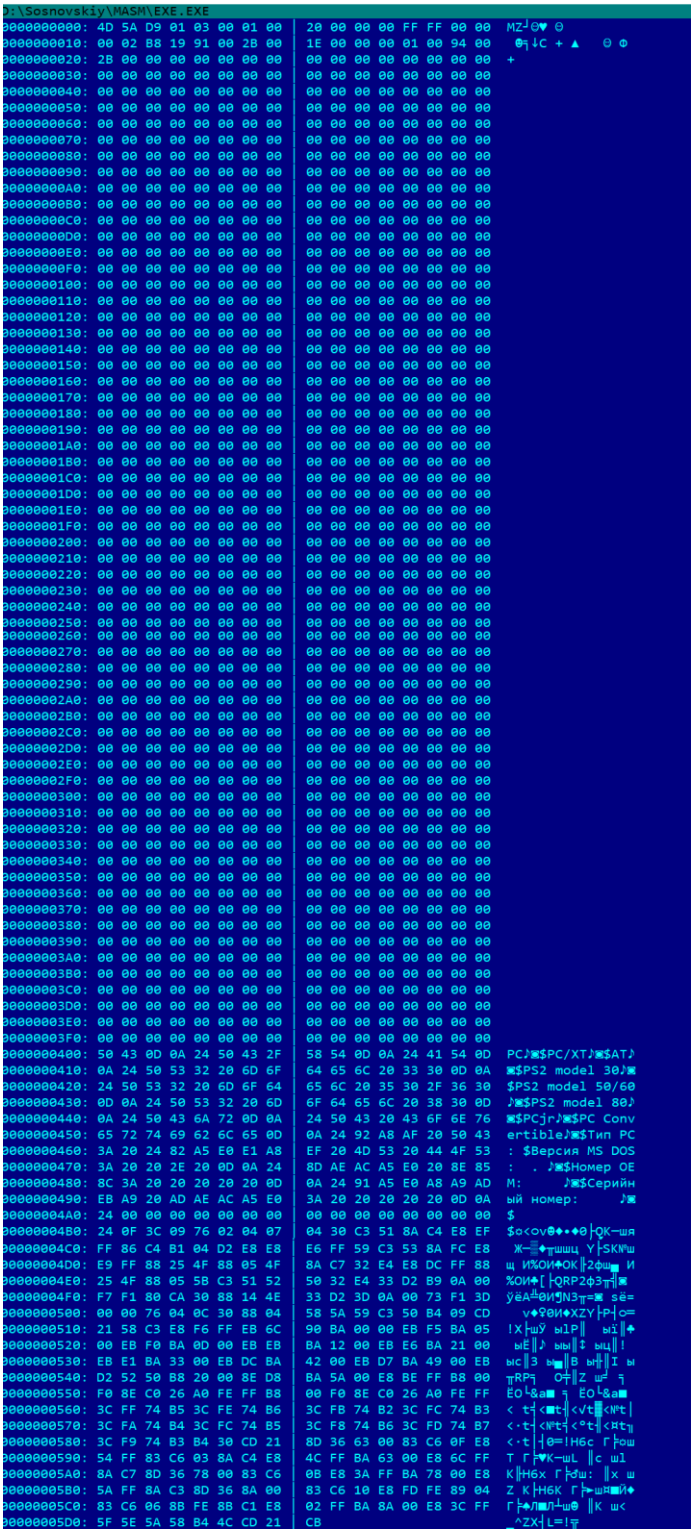

Рисунок 8 - "хороший" EXE модуль

В «хорошем» EXE модуле сначала располагается таблица настроек. Далее перед кодом располагается сегмент стека. Отличие «хорошего» EXE от

«плохого» заключается в том, что в нём не резервируются 100h для PSP, что, в свою очередь, происходит в «плохом».

Загрузка COM модуля в основную память

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

Загрузка COM модуля в отладчик TD.exe представлена на рисунке 9.

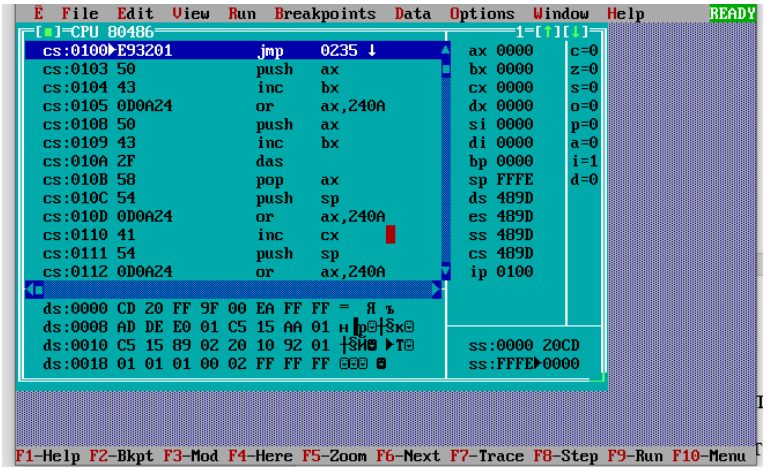

Рисунок 9 - COM модуль в TD.exe

Когда COM модуль загружен в основную память, сегментные регистры указывают на начало PSP. Код располагается с адреса 100h (директива ORG 100h). IP следующей команды также имеет адрес 100h.

2) Что располагается с адреса 0?

С адреса 0 располагается PSP.

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

Сегментные регистры имеют значения 489Dh и указывают на начало сегмента PSP.

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

В COM модуле стек создаётся автоматически. SP хранит адрес конца сегмента, на рисунке 9 это FFFEh. Адреса стека изменяются от FFFEh до 0h.

Загрузка «хорошего» EXE модуля в основную память

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

Загрузка «хорошего» EXE в TD.exe представлена на рисунке 10.

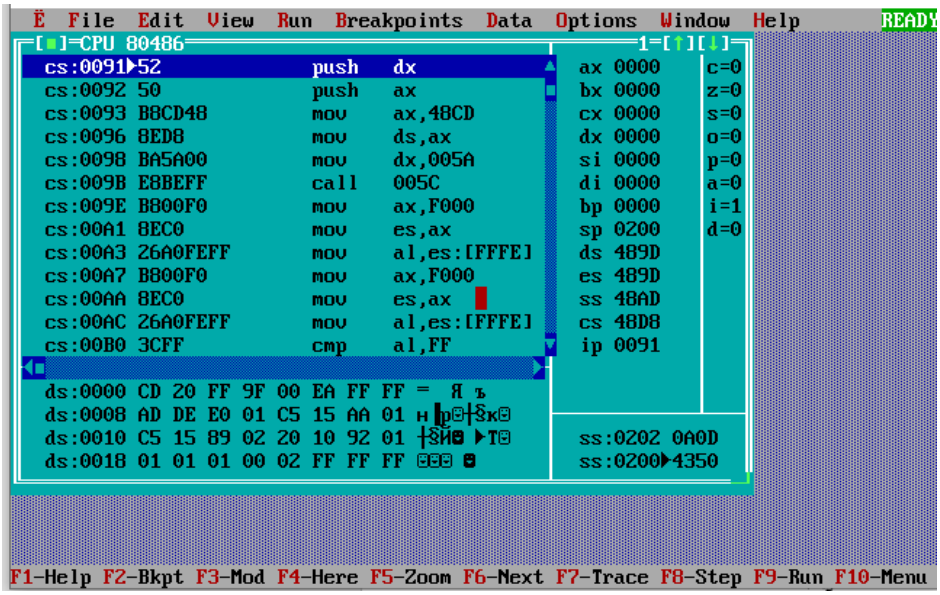

Рисунок 10 - "хороший" EXE в td.exe

Вначале для PSP выделяется блок памяти. Значения регистров: DS = 489Dh, ES = 489Dh, CS = 48D8h, SS = 48AD.

2) На что указывают регистры DS и ES?

Регистры DS и ES указывают на начало PSP в начале работы программы.

3) Как определяется стек?

Стек определяется в исходном коде при помощи директивы ASSUME, которая устанавливает SS на начало сегмента стека.

4) Как определяется точка входа?

Смещение точки входа загружается в указатель IP и определяется меткой директивы END. Эта метка является точкой входа.

Вывод.

В ходе работы были разработаны модули .COM и .EXE и для их сравнения были исследованы их структуры кода, загрузочные модули и способ загрузки в основную память.