**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. 6383 |  | Яковлев Е.А. |
| Преподаватель |  | Губкин А.Ф. |

Санкт-Петербург

2018

**Цель работы:** Исследование различий в структурах исходных текстов модулей типов .СОМ и .ЕХЕ, структур файлов загрузочных модулей и способов их загрузки в основную память.

**Необходимые сведения для составления программы:** Тип IBM PC хранится в байте по адресу 0F000:0FFFEh, в предпоследнем байте ROM BIOS. Соответствие кода и типа в таблице:

**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 ЗОН прерывания 21Н. Входным параметром является номер функции в АН:

**MOV AH,30h**

**INT 2Ih**

Выходными параметрами являются:

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

**АН -** номер модификации

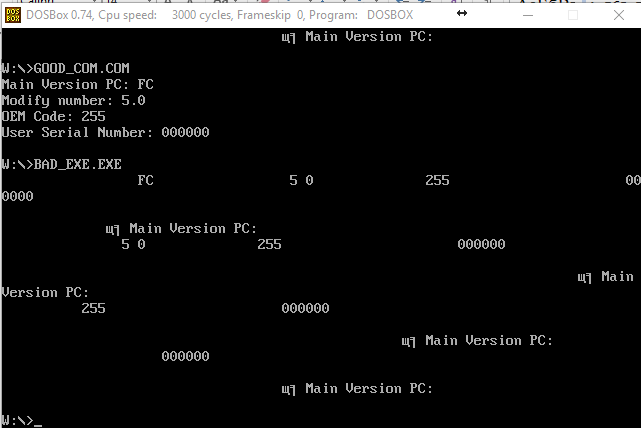
**ВН** - серийный номер OEM (Original Equipment Manufacturer)

**BL:CX** - 24-битовый серийный номер пользователя.

**Ход выполнения работы:**

**Шаг 1:**

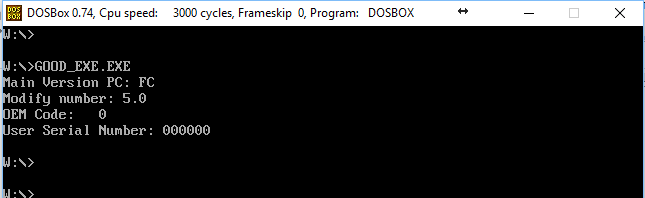
Запуск хорошего \*.СOM и плохого \*.EXE:



*Рис. 1. Результат выполнения программ GOOD\_COM.COM и BAD\_EXE.EXE*

**Шаг 2:**

Запуск хорошего \*.EXE:



*Рис.2. Результат выполнения программы GOOD\_EXE.EXE*

**Шаг 3:**

*Ответы на контрольные вопросы “отличия исходный текстов COM и EXE программ”:*

1. **Сколько сегментов должна содержать COM-программа?**

СOM-программа может содержать один и только один сегмент.

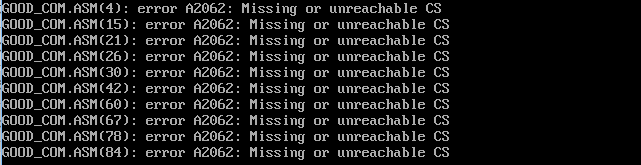
1. **EXE-программа?**

EXE-программа может содержать любое число сегментов, при условии, что существует хотя бы один сегмент.

1. **Какие директивы должны обязательно быть в тексте COM-программе?**

Так как адресация начинается со смещения 100h от начала PSP, то в программе используется директива ORG 100h. Этой директивой мы задаем смещение в 256 байт от нулевого адреса, так как при загрузке модуля в ОП в начале .COM – программы определяется 256 байтный префикс программного сегмента.

Закомментируем директиву ASSUME(В данной программе она указывает, что CS и DS установлены в сегмент TESTPC).



*При компиляции возникает ошибка error A2062: Missing or unreachable, так как теперь сегментный регистр не указывает на текущий кодовый сегмент*

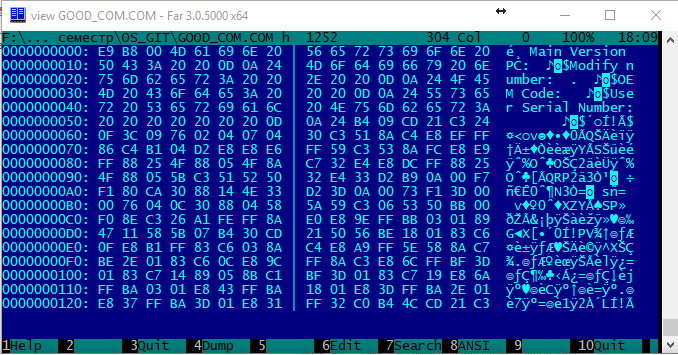
*(программа не может найти начало сегмента кода).*

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

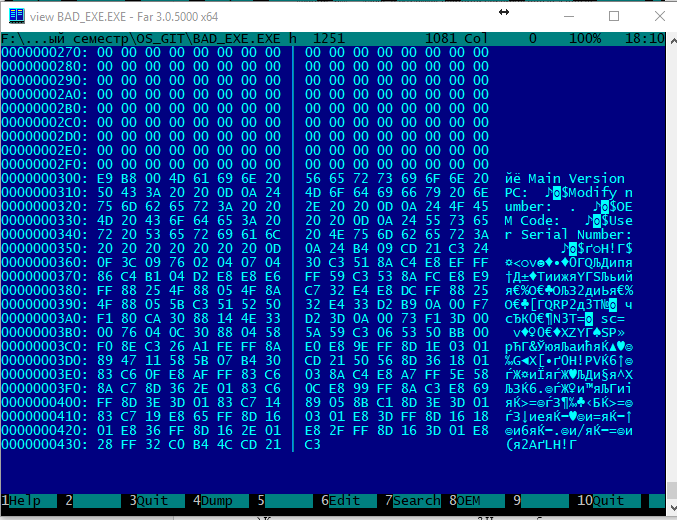
Нельзя использовать команды, связанные с адресом сегмента, потому что адрес сегмента до загрузки неизвестен. В итоге загрузчик не сможет его определить. Также нельзя использовать оператор FAR - переход на метку возможен только в результате межсегментной передачи управления, а так как в .com-файле только один сегмент, то никаких межсегментных переходов быть не может. В данных командах используется таблица разметки (relocation table), в которых содержатся адреса сегментов. Данная таблица есть только в .EXE файлах.

**Шаг 4:**

Откроем файлы загрузочного модуля \*.COM и “плохого” загрузочного модуля \*.EXE:

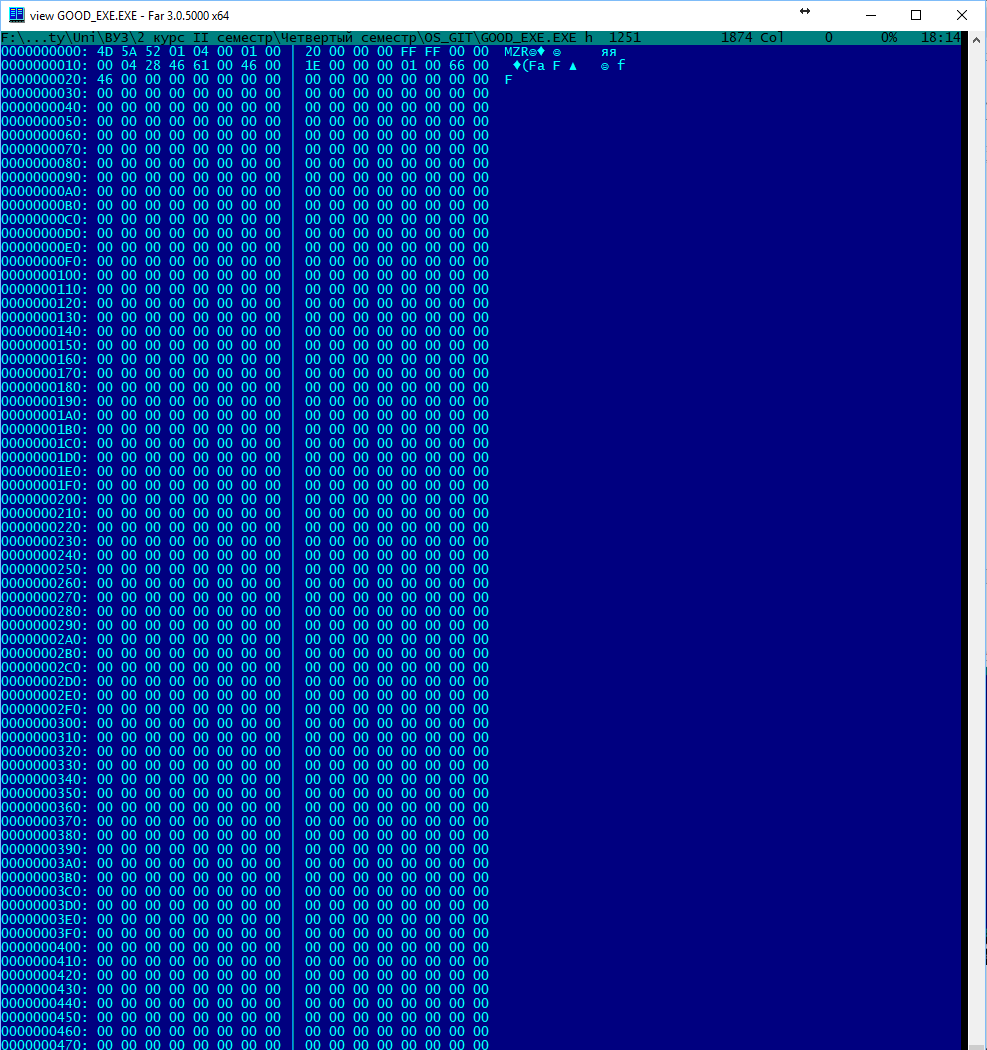
**

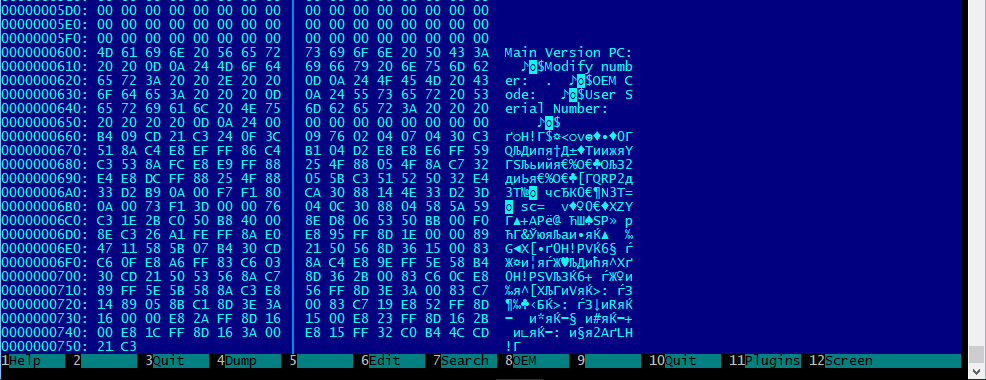
*Рис. 3. HEX представление файла GOOG\_COM.СОМ.*



*Рис. 4. HEX представление файла BAD\_EXE.EXE.*

Откроем файл “хорошего” загрузочного модуля \*.EXE:





*Рис. 5 HEX представление файла GOOD\_EXE.EXE.*

*Ответы на контрольные вопросы “Отличие форматов файлов COM и EXE модулей”****:***

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

COM-программа состоит из одного сегмента и содержит как данные, так и машинные команды. Код располагается с адреса 0h (но при загрузке модуля устанавливается смещение 100h). Стек COM-программа генерирует автоматически.

1. Какова структура “плохого файла” EXE? Что располагается с адреса 0?

В «плохом» EXE данные и код содержатся в одном сегменте.

С адреса 0h идёт таблица настроек (Relocation table -управляющая информация для загрузчика). Код располагается с адреса 300h. 200h байт идет на заголовок, еще 100h за счет сдвига директивой ORG 100h. С 0 располагается заголовок, как сказано ранее.

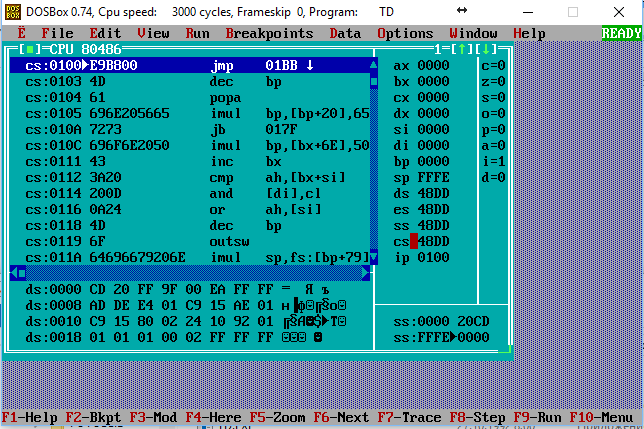
1. Какова структура “хорошего файла” EXE? Чем он отличается от “плохого файла” EXE?

EXE-файл состоит из информации для загрузчика, сегмента стека, сегмент данных и сегмент кода. Отличается количеством сегментов (в «плохом» .EXE – 1 сегмент, в хорошем - 3), а также набором разрешённых команд.

Не требуется директива ORF 100h, так как загрузчик автоматически положит программу после PSP.

**Шаг 5:**

Откроем файл загрузочного модуля \*.COM с использованием отладчика td.exe:



*Рис. 6. Запуск GOOD\_COM.COM с помощью отладчика TD*

**Шаг 6:**

*Ответы на контрольные вопросы “Загрузка COM модуля в основную память”:*

1. **Какой формат загрузки модуля COM? С какого адреса располагается код?**
2. Создаётся блок памяти для PSP и программы
3. Загружается COM-файл с адреса 100h
4. Сегментные регистры CS,DS,ES,SS устанавливаются на начало PSP(0h)
5. Регистр SP устанавливается на конец PSP (FFh)
6. В стек записывается значении 0000
7. В регистр IP записывается значение 100h

Код располагается с адреса 100h.

1. **Что располагается с адреса 0?**

С адреса 0 располагается PSP.

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

Все сегментные регистры имеют значения 119С. Они указывают на PSP.

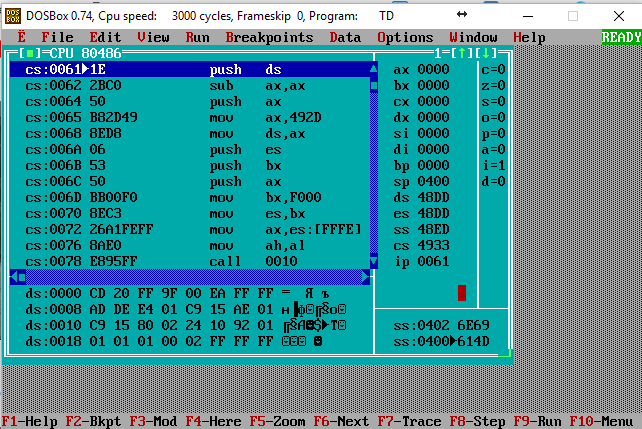


1. **Как определяется стек? Какую область памяти он занимает? Какие адреса?**

Адрес верхнего элемента стека хранится в регистре SP (указателе на стек). В регистре SS хранится сегментный адрес стека. Cтек создается автоматически, указатель стека в конце сегмента. Из этого следует, что он занимает оставшуюся память и адреса изменяются от больших к меньшим, то есть от FFFEh к 0000h.

**Шаг 6:**

Откроем “хороший” \*.EXE с использованием отладчика td.exe:



*Рис. 7 Запуск GOOD\_EXE.EXEс помощью отладчика TD*

*Ответы на контрольные вопросы “Загрузка COM модуля в основную память”:*

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

DS и ES устанавливаются на начало сегмента

PSP, SS– на начало сегмента стека,

CS– на начало сегмента команд.

Сегментный адрес PSP заносится в регистр DS в момент исполнения программы

1. **На что указывают регистры DS и ES?**

Регистры DS и ES указывают на начало сегмента PSP

1. **Как определяется стек?**

Стек определяется при помощи команды STACK

1. **Как определяется точка входа?**

Смещение точки входа в программу загружается в указатель команд IP . IP, а именно адрес, с которого начинается выполнение программы, определяется операндом директивы END, который называется точкой входа.

**Вывод.**

В результате выполнения лабораторной работы были исследованы различия в структурах исходных текстов модулей типов .СОМ и .ЕХЕ, структур файлов загрузочных модулей и способов их загрузки в основную память.