МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Вятский государственный университет»
(ФГБОУ ВО «ВятГУ»)
Институт математики и информационных систем
Факультет автоматики и вычислительной техники
Кафедра электронных вычислительных машин

Отчёт
Лабораторная работа №7 по дисциплине
"Системное программное обеспечение"

Выполнил студент группы ИВТб-3301-04-00_____/Бикметов И.Р.
Проверил доцент кафедры ЭВМ_____/Караваева О.В.

Киров 2024

1 Цель работы

Целью данной лабораторной работы является изучение форматов PE и COFF-файлов, а также процессов компановки и загрузки исполняемых модулей в системах Win32.

2 Задание

1. написать программу на языке ассемблера для API-функции GetShortPathNameA с использованием функций MessageBox и ExitProcess;
2. открыть объектный файл программы в PELinker;
3. сформировать заголовок PE-файла;
4. создать секции PE-файла;
5. произвести разрешение статических и внешних ссылок.

3 Ход работы

В ходе лабораторной работы была написана программа на языке ассемблера для функции GetShortPathNameA.

Результат компиляции программы, то есть объектный код является входом для программной модели PELinker.

Работа в программной модели PELinker начинается с создания заголовка PE-файла, далее создаются секции и производится разрешение статических и внешних ссылок с помощью информации, хранящейся в структуре COFF-файла в таблице Relocation и секции SYMBOLTABLE.Сначала определяется адрес вызова функции или адрес переменной в таблице Relocation; далее, по адресу в поле SymIndex определяется индекс в секции SYMBOLTABLE, где хранится информация о типе ссылки(EXTERNAL или STATIC), имя и, в случае STATIC, значение ссылки. На основании полученных сведений заполняется секция .text.

4 Экранные формы

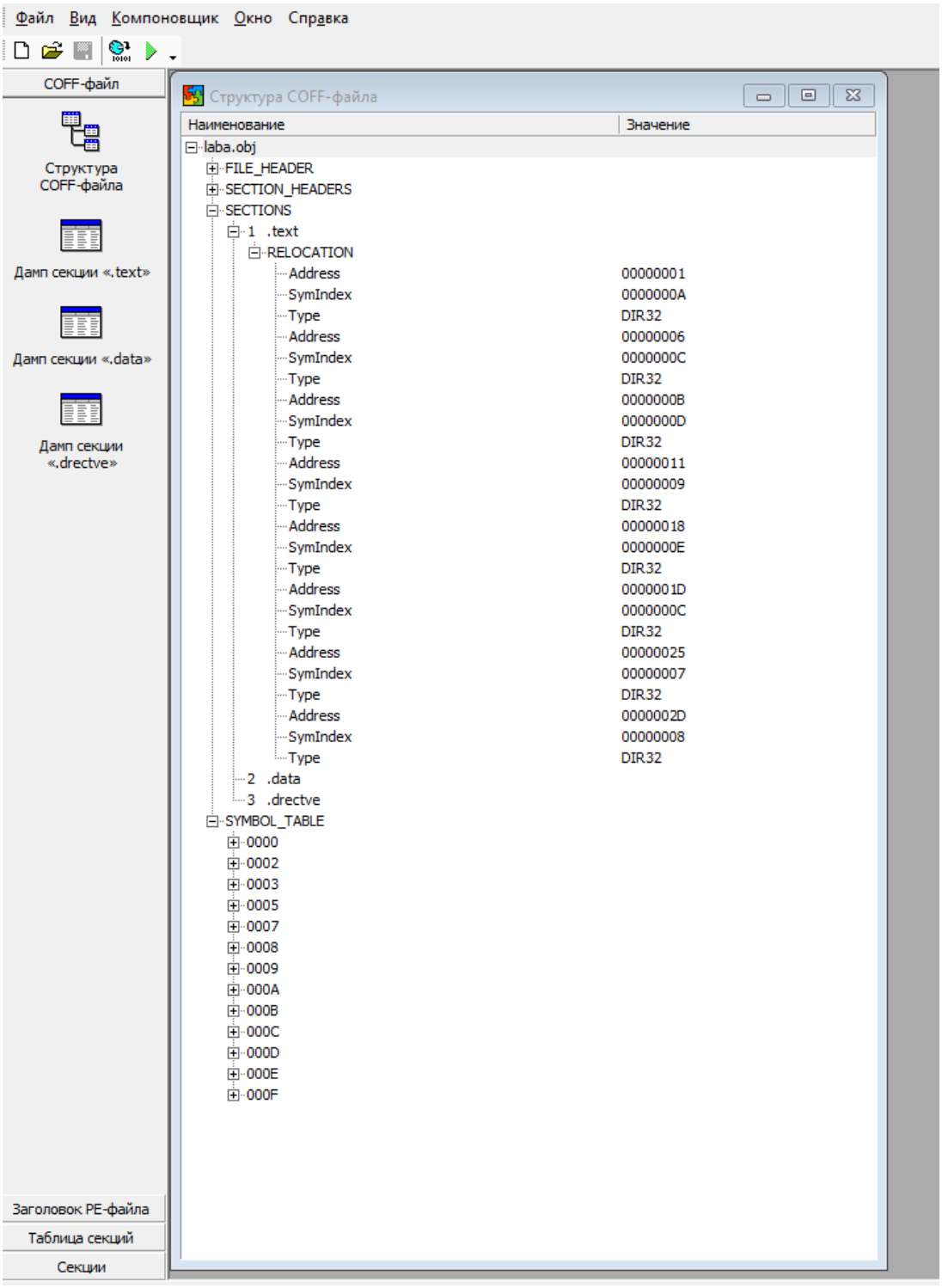

Рисунок 1 – Структура COFF-файла

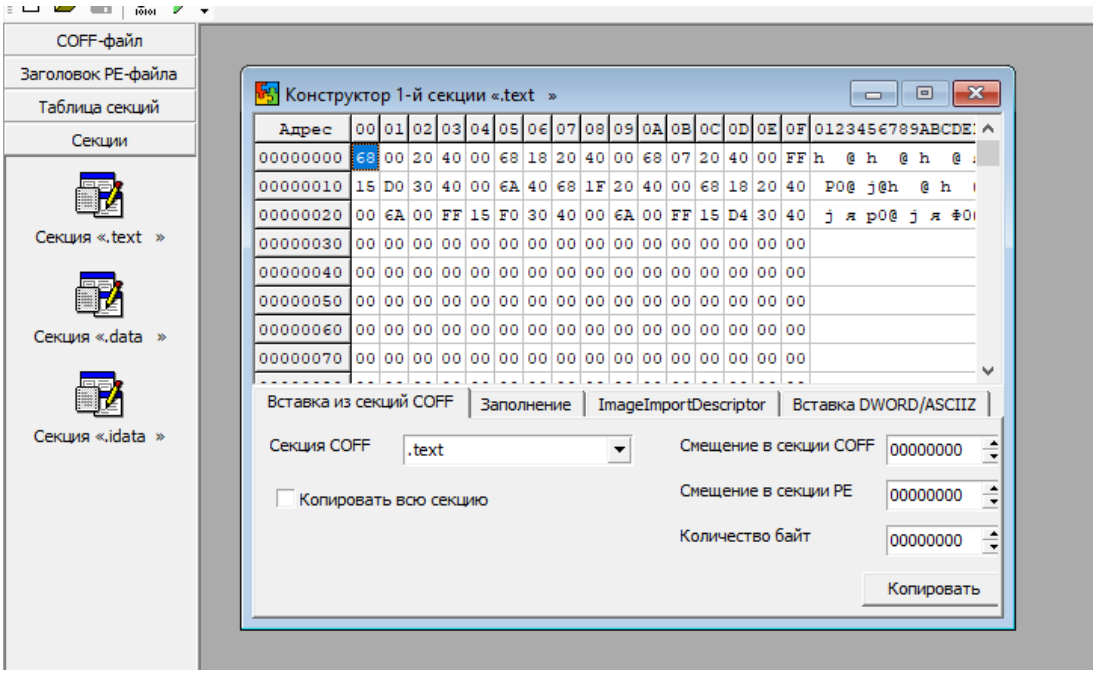

Рисунок 2 – Секция .text с разрешенными ссылками

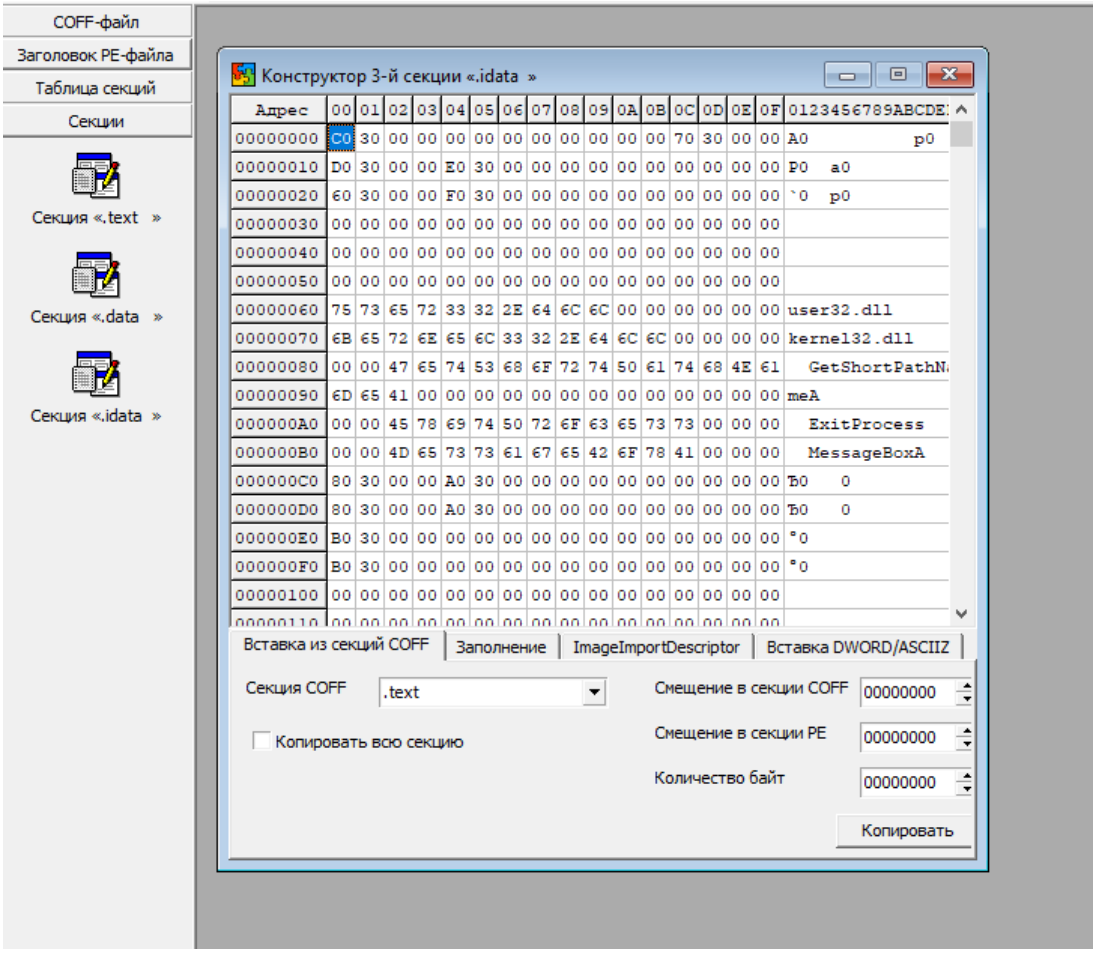

Рисунок 3 – Секция импорта .idata

5 Исходный код

```
.386
.model flat
 extrn MessageBoxA: dword
 extrn ExitProcess: dword
 extrn GetShortPathNameA: dword
.code
_start:
 push offset cchBuffer
 push offset lpszShortPath
 push offset lpszLongPath
 call GetShortPathNameA
 push 40h
 push offset msg
 push offset lpszShortPath
 push 00h
 call MessageBoxA
 push 00h
 call ExitProcess
.data
 cchBuffer db 6 dup(0),0
 lpszLongPath db 'D:\Lab7\lab7.txt',0
 lpszShortPath db 6 dup(0),0
 msg db 'ShortName',0
end _start
```

6 Вывод

В результате лабораторной работы были изучены форматы PE и COFF-файлов, а также выполнены все поставленные задания на лабораторную работу. В частности, была написана программа на языке ассемблера для функции GetShortPathNameA и создан PE-файл для этой программы.