# Лабораторная работа №1

**Тема**: Создание собственного загрузочного сектора.

**Задание**: Создать собственный загрузочный сектор на USB-флеш устройстве и записать в него свою небольшую программу, демонстрирующую особенность вашей USB-флеш. При этом USB-флеш должна нормально восприниматься операционной системой, в подтверждение чего отчет о работе с исходными текстами программ записать на эту же USB-флеш.

**Состав отчета**: Титульный лист; постановка задачи; алгоритм программы (схема программы); текст программы; результаты работы с описанием и экранными копиями.

# Методические указания к выполнению ЛР №1

Загрузка операционной системы (ОС) начинается с того, что с загрузочного диска в оперативную память (ОП) по адресу 0000h:7C00h копируется содержимое самого первого сектора диска — 512 байт и, затем, после успешной проверки наличия сигнатуры загрузочного сектора, управление передается на загрузочную программу по адресу 0000h:7C00h.

Структура загрузочного сектора представлена в таблице.

|  |  |  |
| --- | --- | --- |
| **Смещение** | **Размер, байт** | **Описание** |
| 00h | 3 | Инструкция безусловного перехода JMP NN |
| 03h | 8 | OEM ID — идентификатор |
| 0Bh | 25 | BPB — блок параметров BIOS |
| 24h | 48 | Расширение BPB |
| 54h | 362 | Код программы-загрузчика |
| 1BEh | 16 | Раздел 1 диска |
| 1CEh | 16 | Раздел 2 диска |
| 1DEh | 16 | Раздел 3 диска |
| 1EEh | 16 | Раздел 4 диска |
| 1FEh | 2 | Сигнатура загрузочного сектора (55AAh) |

В лабораторной работе не требуется писать программу загрузки ОС для загрузочного сектора. Вместо загрузочной программы нужно написать свою несложную программу и поместить ее в загрузочный сектор. Здесь важно вписаться в ограниченный диапазон (54h–1BDh) и не задеть ничего лишнего.

В некоторых загрузчиках код программы может начинаться со смещения, отличного от 54h. Смещение конкретно вашей программы-загрузчика вы можете увидеть в самой первой инструкции. Команда JMP будет вас отсылать на данное смещение.

Определимся с таким понятием, как «образ». Образом называют двоичную информацию, точную копию (клон, слепок) объекта. Как правило, образы хранят в файлах на диске.

Диск, на котором будет меняться загрузочный сектор, назовем «подопытным». Таковым может являться дискета 3.5” или USB Flash накопитель.

Для достижения результата рекомендуется следующий порядок действий:

1. Чтение загрузочного сектора с «подопытного» диска и запись двоичного образа в файл «source.bin» на «рабочий» диск.
2. Загрузка файла «source.bin» в ОП.
3. Модификация образа загрузочного сектора (замена программы загрузчика на свою собственную) в ОП с сохранением блока параметров BIOS и таблицы разделов диска.
4. Сохранение модифицированного в ОП образа загрузочного сектора в файл «dest.bin» на «рабочем» диске, «рядом» с файла «source.bin».
5. Запись файла «dest.bin» с новым, модифицированным образом загрузочного сектора в загрузочный сектор «подопытного» диска.

После проделанных операций необходимо убедиться, что «подопытный» диск остался работоспособен, а файлы хранящиеся на нем не пострадали.

Для организации чтения/записи загрузочного сектора в/из ОП рекомендуется бесплатная программа — дисковый редактор DMDE. Полная инструкция и скачивание редактора на сайте <http://dmde.ru/> .

DMDE поддерживает файловые системы FAT12/16, FAT32, NTFS/NTFS5 и работает в Windows 98/.../XP/Vista/7/8, имеет графический GUI и консольный интерфейсы.

Программу для загрузочного сектора, взамен существующей загрузочной программы, можно написать с использованием системной утилиты «debug.exe», или с помощью отладчика «td.exe», входящего в пакет программ Borland Pascal, или Borland C++.

При разработке собственной программы для загрузочного сектора нужно помнить, что на момент ее выполнения в ОП нет никакой DOS. Следовательно, будет невозможно пользоваться прерывания ДОС и файлами. Единственная помощь вам — службы ROM BIOS.

Что должно произойти после того, как ваша программа завершится? Здесь два варианта: либо ваша программа никогда не завершается, либо ваша программа завершается вызовом прерывания BIOS — INT 19h — «теплая перезагрузка». Термин «теплая перезагрузка» (warm start) — перезапуск системы без выполнения ряда процедур начального тестирования и инициализации некоторых интерфейсных СБИС.