***Билет 17***

Существует множество форматов исполняемых файлов для разных операционных систем, например, COM, EXE (Windows, DOS), COFF, ELF (Unix). Обычно данные, хранящиеся в исполняемом файле, состоят из нескольких частей:

· заголовки (предполагаемые исполнители инструкций, настройки исполнителя инструкций и окружения, формат инструкций). Исполнители инструкций — это аппаратно-программный комплекс, способный исполнить инструкцию (процессоры, микроконтроллеры, интерпретаторы, виртуальные машины);

· инструкции (собственно код программы). Представлены либо машинными инструкциями, либо исходным кодом (для интерпретируемого языка), либо байт-кодом для виртуальной машины;

· дополнение (данные, используемые для отладки, список библиотек и используемых функций, иконки для ярлыков, тексты, изображения, звуки, видео и др.)

Структура COM - файла проста. В файлах данного типа содержатся только машинный код и данные программы. Размер COM - файла ограничен 64 кб, т. е. размером одного сегмента памяти. В основном COM файлы пишут на языке Ассемблера, но это не обязательно. Написать файл можно на любом языке, который можно потом компилировать.

EXE файлы могут из нескольких сегментов, следовательно, их размер не ограничен 64 кб. По структуре EXE файл сложнее, кроме кода программы в файле также содержатся: заголовок файла, таблица настройки адресов, данные и т. п. Примерная структура EXE файла:

• Заголовок EXE файла - содержит данные необходимые для загрузки программы.

• Тело программы - основная часть программы, выполняющая какие-либо действия.

• Конец программы - завершающая часть программы, которая сохраняет нужные и удаляет ненужные данные из оперативной памяти, закрывает все открытые данной программой файлы и т. п.

Префикс программного сегмента всегда создается при загрузке программы в память и имеет следующий формат:

Программы могут получить из PSP такую информацию, как параметры командной строки при запуске, размер доступной памяти. Зная адрес PSP, легко найти сегмент области переменных среды и получить другую полезную информацию.

**Формат PSP**

Формат блока PSP и описание назначения всех его полей приведены ниже:

|  |  |  |  |
| --- | --- | --- | --- |
| **Смещение, байт** | **Размер, байт** | **Имя поля** | **Описание** |
| 0 | 2 | int20h | Двоичный код команды INT 20h (программы могут использовать эту команду для завершения своей работы) |
| 2 | 2 | mem\_top | Нижняя граница доступной памяти в системе в параграфах |
| 4 | 1 | reserv1 | Зарезервировано |
| 5 | 5 | call\_dsp | Команда CALL межсегментного вызова диспетчера MS-DOS |
| 10 | 4 | term\_adr | Адрес завершения (Terminate Address) |
| 14 | 4 | cbrk\_adr | Адрес обработчика прерывания, который получает управление, если пользователь нажал комбинацию клавиш <Ctrl+Break> |
| 18 | 4 | crit\_err | Адрес обработчика критической ошибки |
| 22 | 2 | parn\_psp | Сегмент PSP программы, запустившей данную программу (программы-родителя) |
| 24 | 20 | file\_tab | Таблица открытых файлов; если в этом поле находятся байты 0FFH, то таблица не используется |
| 44 | 2 | env\_seg | Сегмент блока памяти, содержащего переменные среды |
| 46 | 4 | ss\_sp | Адрес стека программы SS:SP |
| 50 | 2 | max\_open | Максимальное количество открытых файлов |
| 52 | 4 | file\_tba | Адрес таблицы открытых файлов |
| 56 | 24 | reserv2 | Зарезервировано |
| 80 | 3 | disp | Диспетчер функций MS-DOS |
| 83 | 9 | reserv3 | Зарезервировано |
| 92 | 16 | fcb1 | Если первый аргумент командной строки содержит правильное имя файла, поле форматируется как стандартный блок FCB |
| 108 | 20 | fcb2 | Заполняется для второго аргумента командной строки аналогично fcb1 |
| 128 | 1 | p\_size | Количество значащих символов в неформатированной области параметров, либо буфер обмена с диском DTA , назначенный по умолчанию |
| 129 | 127 | parm | Неформатированная область параметров, заполняется при запуске программы из командной строки |

**Определение адреса PSP**

Как программе определить адрес своего PSP?

Очень просто сделать это в программах, составленных на языке ассемблера: при запуске программы адрес PSP передается ей через регистры DS и ES. То есть этот адрес равен DS:0000 или ES:0000 (для com-программ на PSP указывают также регистры CS и SS).