Машинно-зависимые языки программирования

Лабораторная работа №6

“Перехват прерываний. Резидентные программы”

Справочная информация

Заголовок EXE-файла

Насчитывается порядка 5 форматов EXE-файлов:

- MZ — 16-битный формат, основной формат файлов .EXE в DOS.

EXE-файлы для Windows и OS/2 используют другие форматы для основной части программы, но всё равно начинаются с заглушки в формате MZ, которая, как правило, при попытке запустить файл в DOS выводит сообщение This program cannot be run in DOS mode. («Эту программу невозможно запустить в режиме DOS») и завершает выполнение, хотя теоретически может запускать некий произвольный код, работоспособный в DOS.

- NE — 16-битный формат, использовался в Windows 3.x[2], OS/2 и MS-DOS.
- LE — смешанный 16- и 32-битный формат, ранее использовался в OS/2 и Windows (VxD).
- LX — 32-битный формат, используется в OS/2.
- PE — 32- и 64-битный формат, используется в современных версиях Windows, начиная с Windows NT и Windows 95.

(ц) Википедия

Заголовок начинается с двухбайтной сигнатуры (аббревиатура MZ), далее идут поля размера образа задачи (т.е. части файла, которая будет загружена в память и станет выполняемой программой), размера заголовка, начальные значения SP и IP и т.д. Также заголовок содержит **таблицу настройки адресов**, с помощью которой DOS при загрузке программы в память подставляет в нужные места сегмента кода реальные сегментные адреса, например, сегмента данных.

Префикс программного сегмента

Префикс программного сегмента (PSP - Program Segment Prefix) - структура данных, которая используется в DOS для сохранения состояния программы.
Содержит:

- ссылки на области памяти, связанные с **вызвавшей** программой (чаще всего - командного интерпретатора или оболочки командной строки);
- указатель на область памяти с переменными среды;
- двойное слово для сохранения SS и SP программы обработчиком 21-го прерывания;
- параметры командной строки;
- и т. д.

Располагается PSP перед прочими сегментами программы. Размер PSP - 256 байт, отсюда в COM-программах начальное смещение при запуске 100h, т.е. размер PSP.
При запуске программы номер параграфа начала PSP заносится в DS.
Также он может быть позже определён через использование функции 62h прерывания 21h.

Резидентная (TSR) программа

Резидентная программа (TSR - Terminate and Stay Resident) - в операционной системе MS-DOS программа, вернувшая управление операционной системе, но оставшаяся в оперативной памяти компьютера. Резидентная программа активизируется каждый раз при возникновении прерывания, вектор которого эта программа изменила на адрес одной из своих процедур.
При работе с MS-DOS резидентные программы широко использовались для достижения различных целей (например, русификаторы клавиатуры, программы доступа к локальной сети, менеджеры отложенной печати).
В многозадачных ОС резидентными иногда называют программы, загруженные постоянно и работающие в фоновом режиме, но такое применение этого термина некорректно.

Завершение программы с оставлением в памяти

Для завершения программы с сохранением в памяти в DOS предусмотрено 2 способа:

1. int 27h - для com-программ, размером до 64 Кб. В DX должно находиться количество байтов, которые следует оставить от начала PSP. Другими словами, в DX требуется загрузить смещение команды, начиная с которой фрагмент программы может быть удалён из памяти.
   CS должен указывать на PSP программы (как при работе com-программы).
2. Функция 31h прерывания INT 21h. AL - код завершения, DX - количество параграфов, которые нужно оставить в памяти. Ограничения на размер программы из п.1 нет.

Структура резидентной программы

Сначала в памяти располагаются данные и подпрограммы обработчиков прерываний, затем секция инициализации (которая имеет точку входа INIT и именно в эту точку передается управление при запуске программы). Основная задача секции инициализации — установить резидент в памяти (она нужна лишь при установке программы, потом её из памяти удаляют). Эту секцию располагают в старших адресах (так как «обрезать» мы можем только старшие адреса).

Установка обработчика прерывания

Для замены вектора прерывания на свой адрес можно либо переопределить его напрямую в памяти таблицы векторов, либо использовать функции 25h и 35h.

Практическое задание

Написать резидентную программу под DOS, которая будет реализовывать некий простейший функционал: показывать текущее время в правом верхнем углу, моргать индикаторами на клавиатуре раз в секунду, или выполнять какое-либо подобное действие, демонстрирующее корректную работу программы в фоновом режиме.