Машинно-зависимые языки программирования

Лабораторная работа №6

“Перехват прерываний. Резидентные программы. Ввод-вывод через порты”

Справочная информация

Префикс программного сегмента DOS

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).

Обработка прерываний, перехват прерываний

Вектором прерывания называется полный адрес его обработчика. Таблица векторов прерываний в реальном режиме работы процессора занимает первый килобайт оперативной памяти, таким образом, всего доступно 256 прерываний (размер таблицы - 1024 байта делится на 4 байта - размер одного адреса). При срабатывании прерывания процессор немедленно сохраняет в стек содержимое регистра флагов и адрес возврата из прерывания (всего 6 байт). В конце любой обработчик прерывания завершает свою работу командой IRET, которая восстанавливает из стека 3 сохранённых регистра (IP, CS, FLAGS), что аналогично работе двух команд RETF и POPF.

Для замены вектора прерывания на свой адрес можно либо переопределить его напрямую в памяти таблицы векторов, либо использовать функции 25h и 35h прерывания 21h.

DOS - однозадачная операционная система, поэтому при необходимости выполнения каких-либо действий в фоновом режиме (отображение времени в углу экрана, переключение раскладки, реализация всплывающего псевдографического окна калькулятора и т. д.) резидентной программе требуется “перехватить” наиболее подходящее прерывание, по срабатыванию которого выполнять свою функцию. **При этом необходимо вызывать и код ранее установленного обработчика, чтобы не нарушить функционирование системы.**

Ввод-вывод через порты

Для взаимодействия с внешними устройствами в архитектуре x86 предусмотрен так называемый механизм ввода-вывода через порты, для которого предназначены команды процессора IN и OUT.
В частности, для работы с клавиатурой задействованы порты 61h и 60h. Порт 60h доступен для записи и обычно принимает пары байтов последовательно: первый - код команды, второй - данные. В частности, команда F3h отвечает за параметры режима автоповтора нажатой клавиши. Её байт данных имеет следующее значение:
7 бит (старший) - всегда 0
5,6 биты - пауза перед началом автоповтора (250, 500, 750 или 1000 мс)
4-0 биты - скорость автоповтора (от 0000b (30 символов в секунду) до 11111b - 2 символа в секунду).

Практическое задание

Написать резидентную программу под DOS, которая будет каждую секунду менять скорость автоповтора ввода символов в циклическом режиме, от самой медленной до самой быстрой. *По желанию можно реализовать другой способ взаимодействия с устройствами через порты ввода-вывода, но такой, который можно будет наглядно продемонстрировать на сдаче лаб. работы.*
Варианты вызова предшествующего обработчика прерывания:

1. Командой дальнего вызова подпрограммы CALL в начале обработчика прерывания с предварительным сохранением регистра флагов в стеке.
2. Командой дальнего безусловного перехода JMP в конце обработчика прерывания, сохранив адрес перехода в переменной.
0. Через машинный код EA команды far JMP, сохранив адрес перехода напрямую в непосредственный операнд команды.

Индивидуальный вариант определяется как остаток от деления своего номера в журнале на 3.