ВЛАДИСЛАВ ПИРОГОВ

bhv®

АССЕМБЛЕР для WINDOWS

4-е ИЗДАНИЕ

СРЕДСТВА ПРОГРАММИРОВАНИЯ В WINDOWS

ОТЛАДКА, ИССЛЕДОВАНИЕ КОДА ПРОГРАММ, ДРАЙВЕРЫ

СОЗДАНИЕ ДИНАМИЧЕСКИХ БИБЛИОТЕК

МНОГОЗАДАЧНОЕ И СЕТЕВОЕ ПРОГРАММИРОВАНИЕ

ГРАФИЧЕСКОЕ ПРОГРАММИРОВАНИЕ (GDI+, OpenGL, DirectX)

ПРИМЕРЫ, ПРОВЕРЕННЫЕ НА РАБОТОСПОСОБНОСТЬ В ОС WINDOWS VISTA

PRO
ПРОФЕССИОНАЛЬНОЕ ПРОГРАММИРОВАНИЕ

+CD

Владислав Пирогов

АССЕМБЛЕР для WINDOWS

4-е ИЗДАНИЕ

Санкт-Петербург

«БХВ-Петербург»

2007

УДК 681.3.068+800.92Assembler
ББК 32.973.26-018.1
П33

Пирогов В. Ю.

П33 Ассемблер для Windows. Изд. 4-е перераб. и доп. — СПб.: БХВ-Петербург, 2007. — 896 с.: ил. + CD-ROM — (Профессиональное программирование)

ISBN 978-5-9775-0084-5

Рассмотрены необходимые сведения для программирования Windows-приложений на ассемблерах MASM и TASM: разработка оконных и консольных приложений; создание динамических библиотек; многозадачное программирование; программирование в локальной сети, в том числе и с использованием сокетов; создание драйверов, работающих в режиме ядра; простые методы исследования программ и др. В 4-м издании материал существенно переработан в соответствии с новыми возможностями ОС. Значительно шире рассмотрены вопросы управления файлами и API-программирования в Windows. Добавлен материал по программированию в ОС семейства Windows NT: Windows 2000/ XP/ Server 2003/Vista. На компакт-диске приведены многочисленные примеры, сопровождающие текст и проверенные на работоспособность в операционной системе Windows Vista.

Для программистов

УДК 681.3.068+800.92Assembler
ББК 32.973.26-018.1

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Игорь Шишигин*
Зав. редакцией	*Григорий Добин*
Редактор	*Анна Кузьмина*
Компьютерная верстка	*Натальи Караваевой*
Корректор	*Виктория Пиотровская*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.08.07.
Формат $70\times100^1/_{16}$. Печать офсетная. Усл. печ. л. 72,24.
Тираж 3000 экз. Заказ №
"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.02.953.Д.006421.11.04 от 11.11.2004 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0084-5

Оглавление

Введение

Вот уже и до четвертого издания добрались. Путь был нелегкий. Когда я писал первый вариант книги, я не был уверен в ее успехе. Ассемблер в Windows казался экзотической затеей. Но вот появилась книга, и стало приходить большое количество положительных откликов. Я даже не ожидал, что книга будет пользоваться таким успехом. Ко мне приходит большое количество отзывов, на которые, к моему глубокому сожалению, я не всегда, по причине занятости, могу вовремя ответить.

Признаюсь, что иногда я брожу по Интернету и ищу отрицательные отзывы на свои книги. Таких набирается довольно много. К моему глубокому удовлетворению, по книге "Ассемблер для Windows" (см. [22]) я не нашел ни одного отклика, который бы указывал мне на серьезную ошибку в программе или изложении. Встречаются ошибки и погрешности, связанные с моей невнимательностью во время редакторской работы — книга все-таки довольно объемна. В данном издании я постараюсь их исправить. Есть претензии к моему стилю программирования, но я сразу оговорился, что это *мой стиль*, и от него я отступать не намерен. Кроме того, этот стиль продиктован и педагогическими соображениями — учащийся должен видеть все детали, которые часто скрывают при использовании макросредств.

Вы держите в руках новое издание. Чем же продиктовано его появление? Во-первых, мне хотелось избавиться от некоторых устаревших материалов. В первую очередь это касается ассемблера TASM и программирования под Windows 3.1. Во-вторых, я посчитал необходимым расширить рамки книги за счет добавления нового материала по программированию под Windows. И я надеюсь, что читатель здесь не будет разочарован. Наконец, в данной книге я ориентируюсь на операционные системы версии не ниже Windows XP. Кроме Windows XP программы, представленные в книге, были проверены на Windows Server 2003 и Windows Vista. И последнее, к книге на сей раз будет приложен компакт-диск со всеми примерами.

Интернет-поддержку моей книги осуществляет мой сайт **http://asm.shadrinsk.net**. Рад буду встрече там с моими читателями.

Что нового?

Пять лет назад вышло первое издание данной книги. За это время она нашла своих читателей. Некоторые купили все издания данной книги. Ориентируясь как раз на таких поклонников ассемблера, я решил представить некоторый анализ того, что сделано в данном издании по сравнению с предыдущим. Ниже представлена табл. В1, в которой дана сжатая информация о том, как изменились главы предыдущего издания книги в данном издании. В таблице три столбца: крайний левый содержит старое название главы, средний столбец — новое название, крайний правый столбец — краткую информацию того, что произошло с данной главой.

Таблица В1

Старое название главы	**Новое название главы**	**Изменения**
Глава 1.1. Средства программирования в Windows	Глава 1.1. Средства программирования в Windows	Добавлен новый материал
Глава 1.2. Основы программирования в операционной системе Windows	Глава 1.2. Основы программирования в операционной системе Windows	Добавлен новый материал
Глава 1.3. Примеры простых программ на ассемблере	Глава 1.3. Примеры простых программ на ассемблере	Незначительные изменения
Глава 1.4. Экскурс в 16-битное программирование		Глава изъята
Глава 1.5. Ассемблеры MASM и TASM	Глава 1.4. Ассемблер MASM	Значительно переработана
Глава 1.6. О кодировании текстовой информации в операционной системе Windows	Глава 1.5. О кодировании текстовой информации в операционной системе Windows	Незначительные изменения
Глава 2.1. Примеры простейших программ	Глава 2.1. Вывод графики и текста в окно. Библиотека GDI	Незначительные изменения
	Глава 2.2. Графика: GDI+, DirectX, OpenGL	Новая глава

Таблица В1 *(продолжение)*

Старое название главы	Новое название главы	Изменения
Глава 2.2. Консольные приложения	Глава 2.3. Консольные приложения	Незначительные изменения
Глава 2.3. Понятие ресурса. Редакторы и трансляторы ресурсов	Глава 2.4. Понятие ресурса. Редакторы и трансляторы ресурсов	Незначительные изменения
Глава 2.4. Примеры программ, использующих ресурсы	Глава 2.5. Примеры программ, использующих ресурсы	Незначительные изменения
Глава 2.5. Управление файлами: начало	Глава 2.6. Управление файлами: начало	Незначительные изменения
Глава 2.6. Директивы и макросредства ассемблера	Глава 2.7. Директивы и макросредства ассемблера	Незначительные изменения
Глава 2.7. Еще об управлении файлами (функция *CreateFile* и др.)	Глава 2.8. Еще об управлении файлами (*CreateFile* и другие функции)	Добавлен новый материал
Глава 3.1. Примеры программ, использующих таймер	Глава 3.1. Таймер в оконных приложениях	Незначительные изменения
Глава 3.2. Многозадачное программирование	Глава 3.2. Многозадачное программирование	Значительно переработана
Глава 3.3. Создание динамических библиотек	Глава 3.3. Создание динамических библиотек	Незначительные изменения
Глава 3.4. Программирование в сети	Глава 3.4. Сетевое программирование	Незначительные изменения
Глава 3.5. Разрешение некоторых проблем программирования в Windows	Глава 3.5. Разрешение некоторых проблем программирования в Windows	Значительно переработана. Добавлен новый материал
Глава 3.6. Некоторые вопросы системного программирования в Windows	Глава 3.6. Некоторые вопросы системного программирования в Windows	Добавлен новый материал
Глава 3.7. Использование ассемблера с языками высокого уровня	Глава 3.7. Совместное использование ассемблера с языками высокого уровня	Добавлен новый материал
Глава 3.8. Программирование сервисов	Глава 3.8. Программирование сервисов	Незначительные изменения

Таблица В1 *(окончание)*

Старое название главы	**Новое название главы**	**Изменения**
Глава 4.1. Обзор отладчиков и дизассемблеров	Глава 4.1. Обзор инструментов для отладки и дизассемблирования	Значительно переработана
Глава 4.2. Введение в турбоассемблер		Глава изъята
	Глава 4.2. Отладчик OllyDbg	Новая глава
Глава 4.3. Описание работы с дизассемблером W32Dasm и отладчиком ICE	Глава 4.3. Описание работы с дизассемблером W32Dasm и отладчиком SoftICE	Добавлен новый материал
Глава 4.4. Основы анализа кода программ	Глава 4.4. Основы анализа кода программ	Незначительные изменения
Глава 4.5. Исправление исполняемых модулей	Глава 4.5. Исправление исполняемых модулей	Значительно переработана. Добавлен новый материал
Глава 4.6. Структура и написание драйверов	Глава 4.6. Структура и написание драйверов	Удален устаревший материал
Приложения	Приложения	Содержимое значительно переработано. Добавлено приложение с развернутым примером консольной обработки событий

Соглашения

Синонимами в данной книге являются такие термины, как: ассемблер и язык ассемблера; процедура, функция[1], подпрограмма. Под операционной системой Windows в данной книге будут пониматься операционные системы семейства NT — Windows XP, Windows Server 2003, Windows Vista. В более ранних версиях Windows приводимые программы мною не апробировались, хотя большинство из них, скорее всего, будут корректно работать и в других версиях Windows.

[1] Согласитесь, что различия между понятиями "процедура", "функция" и "подпрограмма" могут существовать лишь в языках высокого уровня.

О Windows Vista

Все примеры, которые приведены к книге и размещены, соответственно, на компакт-диске, проверялись в первую очередь на работоспособность в операционной системе Windows Vista, которая, несомненно, довольно скоро станет основной настольной системой от Microsoft. Кроме этого, все скриншоты (за незначительным исключением) окон приложений, представленных в книге, взяты именно из этой операционной системы.

Структура изложения

- *Часть I. Основы программирования в Windows.*
  - *Глава 1.1. Средства программирования в Windows.*

    Первая программа на языке ассемблера и ее трансляция. Объектные модули. Директива `INVOKE`. Данные в объектном модуле. Упрощенный режим сегментации. Пакет MASM32 — обзор утилит, возможностей и библиотек. Дается краткое описание средств программирования на ассемблере: трансляторов, компоновщиков, отладчиков и т. п.

  - *Глава 1.2. Основы программирования в операционной системе Windows.*

    Вызов функций API. Структура программы. Примеры простых программ для Windows. Передача параметров через стек. Описываются основные структуры на языке ассемблера.

  - *Глава 1.3. Примеры простых программ на ассемблере.*

    Принципы построения оконных приложений. Приводятся примеры программ для Windows с их подробными комментариями. Окно с кнопкой. Окно с полем редактирования. Окно со списком. Дочерние и собственные окна.

  - *Глава 1.4. Ассемблер MASM.*

    Командные строки LINK.EXE и ML.EXE. Получение консольных и GUI-приложений. Автоматическая компоновка. Использование пакетных файлов. "Самотранслирующаяся" программа.

  - *Глава 1.5. О кодировании текстовой информации в операционной системе Windows.*

    О кодировании текстовой информации. OEM и ANSI. Кодировка Unicode. API-функции, полезные при работе с текстовой информацией. Примеры перекодировок.

- *Часть II. Простые программы, консольные приложения, обработка файлов.*
  - *Глава 2.1. Вывод графики и текста в окно. Библиотека GDI.*

    Приводятся примеры простейших 32-битных программ с выводом в окно и с подробными пояснениями. Вывод текста в окне. Выбор шрифта. Графические образы. Библиотека GDI.
  - *Глава 2.2. Графика: GDI+, DirectX, OpenGL.*

    Обзор графических библиотек Windows: GDI+, DirectX, OpenGL с подробными примерами.
  - *Глава 2.3. Консольные приложения.*

    Понятие консольного приложения. Создание консоли. Обработка событий от мыши и клавиатуры. Таймер в консольном приложении. Общая событийная модель консольного приложения.
  - *Глава 2.4. Понятие ресурса. Редакторы и трансляторы ресурсов.*

    Язык описания ресурсов. Редакторы ресурсов. Трансляторы ресурсов. Немодальные диалоговые окна как элементы ресурсов.
  - *Глава 2.5. Примеры программ, использующих ресурсы.*

    Продолжение работы с ресурсами. Динамическое меню. Горячие клавиши. Управление списками. Программирование в стиле Windows XP.
  - *Глава 2.6. Управление файлами: начало.*

    Излагаются основы файловых систем Windows FAT32 и NTFS. Характеристики файлов. Файловая система FAT32. Файловая система NTFS. Поиск файлов. Приемы работы с двоичными файлами. Пример получения временных характеристик файла. Дается описание основных API-функций работы с файлами, приводятся примеры программ с файловой обработкой, пример рекурсивного поиска файлов по дереву каталогов.
  - *Глава 2.7. Директивы и макросредства ассемблера.*

    Макровозможности MASM32. Метки. Структуры. Объединения. Удобный прием работы со структурами. Условное ассемблирование. Вызов процедур. Макроповторения. Макроопределения. Некоторые другие директивы транслятора ассемблера. Конструкции времени исполнения программы. Принцип разработки программ, транслируемых различными ассемблерами.
  - *Глава 2.8. Еще об управлении файлами (CreateFile и другие функции).*

    Более углубленное изучение файлов. Полное описание функции `CreateFile` для работы с файлами. Другие возможности функции

`CreateFile`. Обзор некоторых других функций API, используемых для управления файлами. Асинхронный ввод/вывод. Запись в поток файла.

- *Часть III. Сложные примеры программирования в Windows.*

  - *Глава 3.1. Таймер в оконных приложениях.*

    Таймеры. Простейший пример использования таймера. Взаимодействие таймеров. Теория всплывающих подсказок.

  - *Глава 3.2. Многозадачное программирование.*

    Многозадачность. Процессы и потоки. Создание процесса. Потоки. Взаимодействие потоков. Семафоры. События. Критические секции. Взаимоисключения. Примеры создания и управления потоками.

  - *Глава 3.3. Создание динамических библиотек.*

    Общие понятия. Динамические библиотеки, их структура. Создание динамических библиотек. Неявное связывание. Использование общего адресного пространства. Совместное использование памяти разными процессами.

  - *Глава 3.4. Сетевое программирование.*

    Элементы сетевого программирования. Сетевые устройства. Поиск сетевых устройств и подключение к ним. О сетевых протоколах TCP/IP. Управление сокетами. Примеры простейшего клиента и сервера.

  - *Глава 3.5. Разрешение некоторых проблем программирования в Windows.*

    Примеры интересных задач. Значок на системной панели инструментов. Средства файловой обработки. Контроль данных в окне ввода. Обмен данными между приложениями. Предотвращение многократного запуска приложения. Операции над группами файлов или каталогов. Использование списка задач и списка окон.

  - *Глава 3.6. Некоторые вопросы системного программирования в Windows.*

    О защищенном режиме. О страничной и сегментной адресации. Адресное пространство процесса. Управление памятью: динамическая и виртуальная память. Управление памятью. Файлы, проецируемые в память. Фильтры (Hooks). Перехват функций API.

  - *Глава 3.7. Использование ассемблера с языками высокого уровня.*

    Ассемблер и языки высокого уровня (ЯВУ). Согласование вызовов. Согласование имен. Согласование параметров. Простой пример использования ассемблера с языками высокого уровня. Передача параметров через регистры. Вызовы API и ресурсы в ассемблерных модулях. Развернутый пример совместного использования языков ассемблера и C. Использование языка C и библиотек языка C из языка ассемблера. Встроенный ассемблер. Пример использования динамической библиотеки на языке высокого уровня.

- *Глава 3.8. Программирование сервисов.*

  Сервисы. Понятие сервиса. Основные понятия и функции управления. Структура сервисов. Пример программирования сервиса.

- *Часть IV. Отладка, анализ кода программ, драйверы.*

  - *Глава 4.1. Обзор инструментов для отладки и дизассемблирования.*

    Утилиты, используемые при отладке и дизассемблировании исполняемого кода: dumpbin.exe, hiew.exe и др.

  - *Глава 4.2. Отладчик OllyDbg.*

    Отладчик OllyDbg. Окна отладчика. Выполнение под отладчиком. Точки останова. Исправление исполняемого кода и др.

  - *Глава 4.3. Описание работы с дизассемблером W32Dasm и отладчиком SoftICE.*

    Дизассемблер и отладчик W32Dasm. Интерфейс и настройка программы. Работа с дизассемблируемым кодом. Отладка программ. Отладчик уровня ядра SoftICE. Инсталляция, загрузка, особенности отладки. Справочник команд отладчика SoftICE.

  - *Глава 4.4. Основы анализа кода программ.*

    Некоторые парадигмы исследования исполняемого кода. Переменные и константы. Управляющие структуры языка C. Локальные переменные. Функции и процедуры. Оптимизация кода. Объектное программирование.

  - *Глава 4.5. Исправление исполняемых модулей.*

    Примеры исследования и исправления исполняемых модулей.

  - *Глава 4.6. Структура и написание драйверов.*

    Драйверы, работающие в режиме ядра. Основные понятия. Пример простейшего драйвера, работающего в режиме ядра. Драйверы режима ядра и устройства.

- *Приложения.*

  - *Приложение 1. Справочник API-функций и сообщений Windows.*

    Приложение содержит краткое описание API-функций и сообщений Windows, которые упоминаются в книге.

- *Приложение 2. Справочник по командам и архитектуре микропроцессора Pentium.*

  Дан полный справочник команд микропроцессора Pentium, кратко описана его архитектура.
- *Приложение 3. Защищенный режим микропроцессора Pentium.*

  Дано описание защищенного режима микропроцессора Intel Pentium.
- *Приложение 4. Структура исполняемых модулей.*

  Дано описание структуры исполняемых модулей операционной системы Windows.
- *Приложение 5. Файл kern.inc, используемый в главе 4.6.*

  В приложении содержится файл kern.inc, используемый в *главе 4.6* при написании драйверов режима ядра.
- *Приложение 6. Пример консольного приложения с полной обработкой событий.*

  Представлен полный пример консольного приложения, обрабатывающего все события от клавиатуры и мыши.
- *Приложение 7. Описание компакт-диска.*

  Дано описание компакт-диска, прилагаемого к книге.

Введение ко второму изданию книги "Ассемблер для Windows"

Если Вы, дорогой читатель, знакомы с книгой "Assembler: учебный курс" Вашего покорного слуги, то, наверное, обратили внимание, что программированию в операционной системе Windows было посвящено всего две главы. Это немного и может служить лишь введением в данную область. Пришло время заняться этим серьезно.

Прежде всего, как и полагается во введении, отвечу на возможное замечание: зачем нужен ассемблер в Windows, если есть, например, Си и другие языки? Зачем нужен ассемблер, я уже писал в упомянутой выше книге. Позволю себе процитировать ее: "Зачем нужен язык ассемблера? — спросят меня. Самой простой и убедительный ответ на поставленный вопрос такой — затем, что это язык процессора и, следовательно, он будет нужен до тех пор, пока будут существовать процессоры. Более пространный ответ на данный вопрос содержал бы в себе рассуждение о том, что ассемблер может понадобиться для оптимизации кода программ, написания драйверов, трансляторов, программирования некоторых внешних устройств и т. д. Для себя я, однако, имею и другой ответ: программирование на ассемблере дает ощущение власти над компьютером, а жажда власти — один из сильнейших инстинктов человека".

Что касается операционной системы Windows[1], то здесь, как ни странно это прозвучит для уха некоторых программистов, программировать на ассемблере гораздо легче, чем в операционной системе MS-DOS. В данной книге я берусь доказать, что программировать на ассемблере в Windows ничуть не сложнее, чем на Си, и при этом получается компактный, эффективный и быстрый код. Работая с языками высокого уровня, мы теряем определенные

---

[1] Под термином "операционная система Windows" в данной книге я подразумеваю сразу несколько по сути разных операционных систем: Windows 95/98, Windows NT, Windows 2000 *(см. далее)*. При необходимости мы будем оговаривать, какую ОС имеем в виду.

алгоритмические навыки. И процесс заходит все дальше. Честное слово, только ради повышения своего профессионального уровня стоит заниматься программированием на ассемблере.

Как и предыдущая, эта книга будет содержать только работающие программы с подробным разбором и комментарием.

В настоящее время наиболее часто используются два ассемблера: MASM (Microsoft Assembler) и TASM (Turbo Assembler). Именно на них мы сконцентрируем наше внимание в книге.

И еще, в книгу вошел материал, который можно назвать "хакерским". Мы рассмотрим способы и средства анализа и исправления кода программ. Для тех, кто начнет говорить о безнравственности исправления чужих программ, замечу, что хакеры все равно существуют, а раз так, то почему бы и не познакомиться с тем, как они работают. Это будет полезно многим программистам.

Надо сказать, что в литературе по программированию для Windows 9*x* образовалась некоторая брешь — авторы очень быстро перешли от чистого API-программирования[2] к описанию визуальных компонентов тех или иных языков. Автору известна лишь одна, да и то переводная, книга по "чистому" программированию для Windows — Герберт Шилдт "Программирование на C и C++ для Windows 95" (см. [4]). В своей книге я пытаюсь прикрыть эту брешь, рассматривая некоторые мало освещенные в литературе вопросы: программирование в локальной сети, использование многозадачности, написание V*x*D-драйверов, обработка файлов и др.

Обычно книги по программированию тяготеют к одной из двух крайностей: описание языка программирования, описание возможностей операционной системы. Мне хотелось удержаться посередине. Данная книга — не руководство по языку ассемблера и не руководство по программированию в Windows. Это нечто среднее, можно сказать — симбиоз языка ассемблера и операционной системы Windows. Как я справился с данной задачей — судить Вам, дорогой читатель.

Изложу некоторые принципы, на которые я опирался, когда писал данную книгу.

- Детальное изложение рассматриваемых вопросов. Я не очень жалую макросредства[3] и считаю, что начинающим программистам их не стоит использовать. Однако цель, которую я преследую в книге: сблизить позиции

---

[2] Под API-программированием мы понимаем программирование с использованием одних API-функций.

[3] См. книгу автора "Assembler: учебный курс" — [1].

MASM и TASM — потребует от нас знания и макросредств. Итак, макросредства будут играть в моей книге достаточно узкую подчиненную роль. Впрочем, в книге имеется глава, где подробно разбираются директивы и макросредства ассемблера.

- Чтобы сделать изложение максимально полезным, все программы будут излагаться либо в двух вариантах — для MASM и для TASM, либо с подробным объяснением того, как перейти к другому ассемблеру. За основу взят пакет MASM версии 7.0 и TASM (TASM32.EXE версии 5.0, TLINK32.EXE версии 1.6.71). Читателям рекомендую пользоваться версиями не ниже указанных.
- Книга содержит в себе изложение материала, начиная с простых программ и заканчивая элементами системного программирования. Поэтому книгу можно считать специальным учебным курсом по программированию в операционной системе Windows. Желательно (хотя не обязательно) знакомство читателя с языком Си и весьма желательно наличие начальных знаний по языку ассемблера. В качестве учебников по языку ассемблера можно рекомендовать книги [1, 13].
- Книга содержит обширный справочный материал для того, чтобы читатель не отвлекался на поиски его в других книгах и в Интернете. В *приложении 2* имеется справочник по командам микропроцессора с пояснениями. Более подробное объяснение команд можно найти в книгах [1, 3, 13].
- Хорошее знание ассемблера помогает легко разбираться в коде программ. Взломщики чужих программ всегда хорошо владеют ассемблером. Вопросы анализа кода программ не часто рассматривают в компьютерной литературе. Знание этого не только не помешает любому программисту, но и поможет ему защищать свои программы более эффективно.

Введение к третьему изданию книги "Ассемблер для Windows"

Некоторое время назад вышла моя книга "Ассемблер для Windows". Неожиданно для меня она имела довольно высокий рейтинг продаж. По отзывам, которые я получаю, оказалось, что такую книгу ждали. Дело в том, что долгое время писать на ассемблере означало писать под DOS. Выход на арену операционной системы Windows 95 нанес чувствительный удар по программированию на ассемблере. В определенном смысле ассемблер не оправился от этого удара до сих пор. А ведь уже во всю работают операционные системы Windows XP и Windows Server 2003. Своей работой мне хотелось бы вернуть ассемблеру его несколько пошатнувшиеся позиции.

Данная книга строится на основе уже упомянутой мною книги "Ассемблер для Windows". Значительная часть материала взята именно оттуда. Однако, во-первых, этот материал подвергся определенной переработке и уточнению. Уточнения относятся как к самому языку ассемблера, так и к новым возможностям операционных систем. Во-вторых, в книгу добавлен новый материал, касающийся возможностей операционных систем семейства Windows NT, к коим я отношу Windows 2000[1], Windows XP и Windows Server 2003. Например, появилась глава, посвященная сервисам, рассматривается создание драйверов, работающих в режиме ядра и др. Мною добавлен материал и по вопросам, которые были изложены в предыдущей книге. Например, более чем в два раза увеличился объем страниц, посвященных управлению файлами. Вообще значительно расширен материал, посвященный вопросам API-программирования в Windows.

Отмечу также, что все примеры, приведенные в книге, в том числе и перешедшие из книги "Ассемблер для Windows" и, возможно, несколько переработанные, проверялись мною на этот раз именно в операционных системах семейства NT, и, следовательно, я не могу гарантировать их корректную работу в операционных системах семейства Windows 9*x*/Windows ME. То же я

[1] Windows 2000 имеет и другое название: Windows NT 5.0.

могу сказать и о процессоре: все примеры проверялись на процессорах Pentium III и Pentium 4.

Как и в предыдущей книге, я использую два ассемблера — MASM и TASM. Не так давно TASM был продан фирмой Borland компании Paradigm и развивается теперь под другим названием (PASM). Поскольку, однако, среди программистов, пишущих на ассемблере, TASM остается довольно популярным средством, я по-прежнему строю свое изложение, опираясь (там, где это возможно) на оба компилятора.

Данная книга в значительной степени отражает пристрастия автора в области программирования и преподавания. В первую очередь, это коснулось макросредств ассемблера. Мне кажется, они (макросредства) в значительной степени скрывают от нас красоту и возможности ассемблера. Я полагаю, что, говоря о программировании как о технологии и в этой связи о стиле программирования, мы забываем, что для многих программирование — это еще и средство самовыражения. Эти две стороны программирования часто входят в противоречие друг с другом, но это уже особый, я бы сказал, философский разговор, и в данной книге мы заниматься этим не будем.

Несколько слов скажу о нумерации глав в данной книге. Книга разбита на части, а те, в свою очередь, на главы. В каждой части своя нумерация глав. Полный номер главы состоит из номера части и номера главы в ней. Таким образом, *глава 2.3* означает главу 3 из части II. Номер рисунка содержит в себе номер части, номер главы и номер рисунка в главе. Программы и фрагменты программ называются листингами, и принцип их нумерации такой же, как у рисунков.

Часть I

ОСНОВЫ ПРОГРАММИРОВАНИЯ В WINDOWS