

**Зубков С.В.**

Assembler. Для DOS, Windows и Unix. – М.: ДМК Пресс, 2017. – 638 с., ил.

**ISBN 978-5-97060-535-6**

В книге описываются все аспекты современного программирования на ассемблере для DOS, Windows и Unix (Solaris, Linux и FreeBSD), включая создание резидентных программ и драйверов, прямое программирование периферийных устройств, управление защищенным режимом и многое другое. Подробно рассмотрена архитектура процессоров Intel вплоть до Pentium II. Все главы иллюстрированы подробными примерами работоспособных программ.

Книга ориентирована как на профессионалов, так и на начинающих без опыта программирования.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность наличия технических и просто человеческих ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

© Зубков С. В.

**ISBN 978-5-97060-535-6**

© Оформление, издание, ДМК Пресс, 2017

# СОДЕРЖАНИЕ

<b>ВВЕДЕНИЕ</b> .....	12
<b>1. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ</b> .....	15
1.1. Что потребуется для работы с ассемблером .....	15
1.2. Представление данных в компьютерах .....	16
1.2.1. Двоичная система счисления .....	17
1.2.2. Биты, байты и слова .....	17
1.2.3. Шестнадцатеричная система счисления .....	19
1.2.4. Числа со знаком .....	19
1.2.5. Логические операции .....	20
1.2.6. Коды символов .....	21
1.2.7. Организация памяти .....	21
<b>2. ПРОЦЕССОРЫ INTEL В РЕАЛЬНОМ РЕЖИМЕ</b> .....	23
2.1. Регистры процессора .....	23
2.1.1. Регистры общего назначения .....	23
2.1.2. Сегментные регистры .....	25
2.1.3. Стек .....	26
2.1.4. Регистр флагов .....	27
2.2. Способы адресации .....	28
2.2.1. Регистровая адресация .....	28
2.2.2. Непосредственная адресация .....	28
2.2.3. Прямая адресация .....	29
2.2.4. Косвенная адресация .....	29
2.2.5. Адресация по базе со сдвигом .....	30
2.2.6. Косвенная адресация с масштабированием .....	30
2.2.7. Адресация по базе с индексированием .....	31
2.2.8. Адресация по базе с индексированием и масштабированием .....	31
2.3. Основные непривileгированные команды .....	32
2.3.1. Пересылка данных .....	32
2.3.2. Двоичная арифметика .....	40

2.3.3. Десятичная арифметика .....	45
2.3.4. Логические операции .....	48
2.3.5. Сдвиговые операции .....	50
2.3.6. Операции над битами и байтами .....	53
2.3.7. Команды передачи управления .....	55
2.3.8. Строковые операции .....	63
2.3.9. Управление флагами .....	69
2.3.10. Загрузка сегментных регистров .....	72
2.3.11. Другие команды .....	72
2.4. Числа с плавающей запятой .....	77
2.4.1. Типы данных FPU .....	77
2.4.2. Регистры FPU .....	79
2.4.3. Исключения FPU .....	82
2.4.4. Команды пересылки данных FPU .....	83
2.4.5. Базовая арифметика FPU .....	85
2.4.6. Команды сравнения FPU .....	90
2.4.7. Трансцендентные операции FPU .....	92
2.4.8. Константы FPU .....	95
2.4.9. Команды управления FPU .....	95
2.5. Расширение IA MMX .....	100
2.5.1. Регистры MMX .....	100
2.5.2. Типы данных MMX .....	101
2.5.3. Команды пересылки данных MMX .....	101
2.5.4. Команды преобразования типов MMX .....	102
2.5.5. Арифметические операции MMX .....	104
2.5.6. Команды сравнения MMX .....	106
2.5.7. Логические операции MMX .....	107
2.5.8. Сдвиговые операции MMX .....	108
2.5.9. Команды управления состоянием MMX .....	109
2.5.10. Расширение AMD 3D .....	109
<b>3. ДИРЕКТИВЫ И ОПЕРАТОРЫ АССЕМБЛЕРА .....</b>	<b>112</b>
3.1. Структура программы .....	112
3.2. Директивы распределения памяти .....	114
3.2.1. Псевдокоманды определения переменных .....	114
3.2.2. Структуры .....	115

3.3. Организация программы .....	116
3.3.1. Сегменты .....	116
3.3.2. Модели памяти и упрощенные директивы определения сегментов .....	119
3.3.3. Порядок загрузки сегментов .....	121
3.3.4. Процедуры .....	122
3.3.5. Конец программы .....	123
3.3.6. Директивы задания набора допустимых команд .....	123
3.3.7. Директивы управления программным счетчиком .....	124
3.3.8. Глобальные объявления .....	125
3.3.9. Условное ассемблирование .....	126
3.4. Выражения .....	128
3.5. Макроопределения .....	130
3.5.1. Блоки повторений .....	131
3.5.2. Макрооператоры .....	133
3.5.3. Другие директивы, используемые в макроопределениях .....	134
3.6. Другие директивы .....	134
3.6.1. Управление файлами .....	134
3.6.2. Управление листингом .....	134
3.6.3. Комментарии .....	135
<b>4. Основы программирования для MS-DOS .....</b>	<b>136</b>
4.1. Программа типа COM .....	137
4.2. Программа типа EXE .....	139
4.3. Вывод на экран в текстовом режиме .....	141
4.3.1. Средства DOS .....	141
4.3.2. Средства BIOS .....	144
4.3.3. Прямая работа с видеопамью .....	149
4.4. Ввод с клавиатуры .....	151
4.4.1. Средства DOS .....	151
4.4.2. Средства BIOS .....	159
4.5. Графические видеорежимы .....	162
4.5.1. Работа с VGA-режимами .....	162
4.5.2. Работа с SVGA-режимами .....	167

4.6. Работа с мышью .....	179
4.7. Другие устройства .....	185
4.7.1. Системный таймер .....	185
4.7.2. Последовательный порт .....	192
4.7.3. Параллельный порт .....	196
4.8. Работа с файлами .....	198
4.8.1. Создание и открытие файлов .....	198
4.8.2. Чтение и запись в файл .....	201
4.8.3. Заккрытие и удаление файла .....	203
4.8.4. Поиск файлов .....	204
4.8.5. Управление файловой системой .....	208
4.9. Управление памятью .....	211
4.9.1. Обычная память .....	211
4.9.2. Область памяти UMB .....	212
4.9.3. Область памяти HMA .....	213
4.9.4. Интерфейс EMS .....	214
4.9.5. Интерфейс XMS .....	215
4.10. Загрузка и выполнение программ .....	220
4.11. Командные параметры и переменные среды .....	227
<b>5. БОЛЕЕ СЛОЖНЫЕ ПРИЕМЫ ПРОГРАММИРОВАНИЯ .....</b>	<b>232</b>
5.1. Управляющие структуры .....	232
5.1.1. Структуры IF.. THEN... ELSE .....	232
5.1.2. Структуры CASE .....	233
5.1.3. Конечные автоматы .....	234
5.1.4. Циклы .....	235
5.2. Процедуры и функции .....	236
5.2.1. Передача параметров .....	236
5.2.2. Локальные переменные .....	242
5.3. Вложенные процедуры .....	243
5.3.1. Вложенные процедуры со статическими ссылками .....	243
5.3.2. Вложенные процедуры с дисплеями .....	245

<b>5.4. Целочисленная арифметика</b>	
повышенной точности .....	246
5.4.1. Сложение и вычитание .....	246
5.4.2. Сравнение .....	247
5.4.3. Умножение .....	248
5.4.4. Деление .....	249
<b>5.5. Вычисления с фиксированной запятой</b> .....	250
5.5.1. Сложение и вычитание .....	250
5.5.2. Умножение .....	251
5.5.3. Деление .....	251
5.5.4. Трансцендентные функции .....	251
<b>5.6. Вычисления с плавающей запятой</b> .....	256
<b>5.7. Популярные алгоритмы</b> .....	261
5.7.1. Генераторы случайных чисел .....	261
5.7.2. Сортировки .....	265
<b>5.8. Перехват прерываний</b> .....	269
5.8.1. Обработчики прерываний .....	270
5.8.2. Прерывания от внешних устройств .....	274
5.8.3. Повторная входимость .....	278
<b>5.9. Резидентные программы</b> .....	281
5.9.1. Пассивная резидентная программа .....	282
5.9.2. Мультиплексорное прерывание .....	288
5.9.3. Выгрузка резидентной программы из памяти .....	304
5.9.4. Полурезидентные программы .....	321
5.9.5. Взаимодействие между процессами .....	326
<b>5.10. Программирование на уровне</b>	
портов ввода-вывода .....	335
5.10.1. Клавиатура .....	335
5.10.2. Последовательный порт .....	339
5.10.3. Параллельный порт .....	345
5.10.4. Видеоадаптеры VGA .....	347
5.10.5. Таймер .....	363
5.10.6. Динамик .....	368
5.10.7. Часы реального времени и CMOS-память .....	369

5.10.8. Звуковые платы .....	373
5.10.9. Контроллер DMA .....	381
5.10.10. Контроллер прерываний .....	389
5.10.11. Джойстик .....	395
5.11. Драйверы устройств в DOS .....	397
5.11.1. Символьные устройства .....	400
5.11.2. Блочные устройства .....	409
<b>6. ПРОГРАММИРОВАНИЕ В ЗАЩИЩЕННОМ РЕЖИМЕ .....</b>	<b>414</b>
6.1. Адресация в защищенном режиме .....	414
6.2. Интерфейс VCPI .....	418
6.3. Интерфейс DPMI .....	420
6.3.1. Переключение в защищенный режим .....	421
6.3.2. Функции DPMI управления дескрипторами .....	422
6.3.3. Передача управления между режимами в DPMI .....	424
6.3.4. Обработчики прерываний .....	426
6.3.5. Пример программы .....	428
6.4. Расширители DOS .....	431
6.4.1. Способы объединения программы с расширителем ...	432
6.4.2. Управление памятью в DPMI .....	433
6.4.3. Вывод на экран через линейный кадровый буфер .....	435
<b>7. ПРОГРАММИРОВАНИЕ ДЛЯ WINDOWS 95 и WINDOWS NT .....</b>	<b>442</b>
7.1. Первая программа .....	442
7.2. Консольные приложения .....	446
7.3. Графические приложения .....	451
7.3.1. Окно типа MessageBox .....	451
7.3.2. Окна .....	452
7.3.3. Меню .....	457
7.3.4. Диалоги .....	462
7.3.5. Полноценное приложение .....	467
7.4. Динамические библиотеки .....	483
7.5. Драйверы устройств .....	489

<b>8. Ассемблер и языки высокого уровня .....</b>	<b>492</b>
8.1. Передача параметров .....	492
8.1.1. Конвенция <i>Pascal</i> .....	492
8.1.2. Конвенция <i>C</i> .....	493
8.1.3. Смешанные конвенции .....	495
8.2. Искажение имен .....	495
8.3. Встроенный ассемблер .....	496
8.3.1. Встроенный ассемблер в <i>Pascal</i> .....	496
8.3.2. Встроенный ассемблер в <i>C</i> .....	496
<b>9. Оптимизация .....</b>	<b>498</b>
9.1. Высокоуровневая оптимизация .....	498
9.2. Оптимизация на среднем уровне .....	498
9.2.1. Оптимизация циклов .....	499
9.3. Низкоуровневая оптимизация .....	501
9.3.1. Общие принципы низкоуровневой оптимизации .....	501
9.3.2. Особенности архитектуры процессоров Pentium и Pentium MMX .....	505
9.3.3. Особенности архитектуры процессоров Pentium Pro и Pentium II .....	507
<b>10. Процессоры Intel в защищенном режиме .....</b>	<b>511</b>
10.1. Регистры .....	511
10.1.1. Системные флаги .....	511
10.1.2. Регистры управления памятью .....	513
10.1.3. Регистры управления процессором .....	513
10.1.4. Отладочные регистры .....	515
10.1.5. Машинно-специфичные регистры .....	517
10.2. Системные и привилегированные команды .....	517
10.3. Вход и выход из защищенного режима .....	525
10.4. Сегментная адресация .....	527
10.4.1. Модель памяти в защищенном режиме .....	527
10.4.2. Селектор .....	528



10.4.3. Дескрипторы .....	528
10.4.4. Пример программы .....	530
10.4.5. Нереальный режим .....	535
10.5. Обработка прерываний и исключений .....	537
10.6. Страничная адресация .....	548
10.7. Механизм защиты .....	555
10.7.1. Проверка лимитов .....	556
10.7.2. Проверка типа сегмента .....	557
10.7.3. Проверка привилегий .....	557
10.7.4. Выполнение привилегированных команд .....	558
10.7.5. Защита на уровне страниц .....	559
10.8. Управление задачами .....	559
10.8.1. Сегмент состояния задачи .....	560
10.8.2. Переключение задач .....	561
10.9. Режим виртуального 8086 .....	568
10.9.1. Прерывания в V86 .....	568
10.9.2. Ввод-вывод в V86 .....	569

## **11. ПРОГРАММИРОВАНИЕ НА АССЕМБЛЕРЕ В СРЕДЕ UNIX**

11.1. Синтаксис AT&T .....	570
11.1.1. Основные правила .....	571
11.1.2. Запись команд .....	572
11.1.3. Адресация .....	574
11.2. Операторы ассемблера .....	574
11.2.1. Префиксные, или унарные операторы .....	575
11.2.2. Инфиксные, или бинарные операторы .....	575
11.3. Директивы ассемблера .....	575
11.3.1. Директивы определения данных .....	575
11.3.2. Директивы управления символами .....	576
11.3.3. Директивы определения секций .....	577
11.3.4. Директивы управления разрядностью .....	578
11.3.5. Директивы управления программным указателем .....	578
11.3.6. Директивы управления листингом .....	579

11.3.7. Директивы управления ассемблированием .....	579
11.3.8. Блоки повторения .....	579
11.3.9. Макроопределения .....	580
11.4. Программирование с использованием <i>libc</i> .....	581
11.5. Программирование без использования <i>libc</i> .....	583

<b>12.ЗАКЛЮЧЕНИЕ .....</b>	<b>587</b>
----------------------------	------------

<b>ПРИЛОЖЕНИЕ 1. ТАБЛИЦЫ СИМВОЛОВ .....</b>	<b>588</b>
1. Символы ASCII .....	588
2. Управляющие символы ASCII .....	589
3. Кодировки второй половины ASCII .....	590
4. Коды символов расширенного ASCII .....	593

<b>ПРИЛОЖЕНИЕ 2. Команды Intel 80x86 .....</b>	<b>596</b>
1. Общая информация о кодах команд .....	596
1.1. Общий формат команды процессора Intel .....	596
1.2. Значения полей кода команды .....	596
1.3. Значения поля ModRM .....	598
1.4. Значения поля SIB .....	599
2. Общая информация о скоростях выполнения .....	599
3. Префиксы .....	601
4. Команды процессоров Intel 8088 – Pentium II .....	602

<b>СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ .....</b>	<b>624</b>
---	------------

<b>ГЛОССАРИЙ .....</b>	<b>627</b>
------------------------	------------

<b>АЛФАВИТНЫЙ УКАЗАТЕЛЬ .....</b>	<b>630</b>
-----------------------------------	------------