

# Ассемблер и программная модель процессоров x86/64

Ассемблеры a86/a386

Netwide Assembler (nasm)

Система команд i80x86/64

32-битный защищенный режим

64-битные режимы



Андрей Жуков



Материалы  
на [www.bhv.ru](http://www.bhv.ru)

# Оглавление

Предисловие .....	9
Примечания.....	11
<b>ЧАСТЬ I. РЕАЛЬНЫЙ РЕЖИМ.....</b>	<b>13</b>
<b>Глава 1. Установка программ .....</b>	<b>15</b>
Установка и настройка <i>Bochs</i> .....	15
Формирование образа диска.....	16
Настройка отладочного варианта <i>Bochs</i> .....	18
Примечания.....	18
<b>Глава 2. Программирование данных .....</b>	<b>21</b>
Вызов <i>a86</i> .....	21
Программирование последовательностей .....	22
Программирование <i>bin</i> -файла.....	26
Примечания.....	29
<b>Глава 3. Данные, имена и типы.....</b>	<b>31</b>
Структура программы .....	31
Директивы определения данных .....	32
Обозначение чисел .....	37
Символические обозначения чисел, выражения.....	38
Переменные и метки.....	40
Типы имен.....	41
Типы и выражения.....	43
Алгоритм трансляции.....	46
Повторное определение имен.....	50
Локальные имена .....	51
Предопределенные имена .....	52
Имя <i>end</i> .....	52
Примечания.....	54
<b>Глава 4. Способы адресации .....</b>	<b>57</b>
Данные процессора.....	57
Обозначения операндов машинных команд.....	59

Способы адресации операндов .....	60
Регистровая и непосредственная адресация .....	60
Адресация данных в памяти .....	61
Прямая адресация .....	61
Косвенная адресация .....	63
Ограничение на адресацию операндов в памяти .....	67
Примечания .....	68
<b>Глава 5. Система команд i8086 .....</b>	<b>69</b>
Способы адресации операндов .....	69
Регистровая, непосредственная и прямая адресация .....	70
Косвенная адресация .....	71
Косвенная адресация по значению одного регистра .....	71
Косвенная адресация по сумме значений двух регистров .....	71
Обзор системы команд .....	71
Команды пересылки .....	72
Арифметические команды .....	73
Логические команды .....	74
Команды сдвигов и вращений .....	74
Команды передачи управления .....	75
Адресация в командах передачи управления .....	76
Команды условных переходов .....	77
Воздействие команд на флаги .....	79
Строковые команды .....	82
Примечания .....	83
<b>Глава 6. Программирование циклов .....</b>	<b>85</b>
Поиск в массиве байтов .....	85
Поиск в массиве слов .....	87
Поиск байта со значением больше заданного .....	88
Подсчет байтов в заданном диапазоне значений .....	89
Алгоритмическое решение .....	89
Табличное решение .....	90
Примечания .....	92
<b>Глава 7. Примеры программ .....</b>	<b>93</b>
Обработка данных на уровне битов .....	93
Программирование ввода-вывода .....	95
Опережающие ссылки .....	98
Упаковка четырехбитовых кодов .....	100
Задания на составление программ .....	102
Задания первого уровня сложности .....	102
Варианты заданий .....	102
Задания второго уровня сложности .....	104
Примечания .....	108
<b>Глава 8. Математический сопроцессор .....</b>	<b>111</b>
Окно FPU в d86 .....	111
Загрузка и выгрузка данных .....	112

Порядок двуместных операций .....	114
Организация ветвлений .....	117
Признаки в слове состояния .....	118
Настройки FPU .....	120
Форматы действительных чисел .....	121
Внутренний формат данных FPU .....	122
Стандартные форматы вещественных чисел .....	124
Операции FPU .....	125
Пересылки .....	126
Загрузка данных .....	126
Команды выгрузки .....	128
Команда обмена .....	130
Арифметические операции .....	130
Основные арифметические операции .....	131
Операции над знаковым битом .....	132
Округление до целого .....	133
Получение остатка от деления .....	134
Извлечение корня .....	135
Масштабирование .....	135
Операции сравнения и тестирования .....	135
Тригонометрические операции .....	137
Возведение в степень .....	137
Возведение числа 2 в целую степень .....	138
Возведение числа 2 в дробную степень .....	138
Вычисление целой и дробной частей значения степени .....	139
Возведение числа 2 в произвольную степень .....	139
Вычисление логарифмов .....	139
Команды управления .....	141
Сохранение и восстановление состояния .....	142
Задачи .....	143
Примечания .....	145
<b>Глава 9. Сегменты.....</b>	<b>149</b>
Эффективный адрес.....	150
Базовый адрес и сегментные регистры .....	151
Перепрограммирование сегментных регистров.....	154
Регистр <i>es</i> .....	154
Регистр <i>ss</i> .....	156
Регистр <i>cs</i> .....	157
Регистр <i>ds</i> .....	159
Повторный запуск резидентной программы .....	160
Программные секции.....	162
Префикс переназначения сегмента .....	167
Задачи .....	172
Примечания .....	173
<b>Глава 10. Исключения.....</b>	<b>177</b>
Таблица векторов.....	177
Векторные вызовы.....	178

Исключения и прерывания .....	185
Ассемблер <i>nasm</i> .....	189
Отладочные исключения .....	193
Примечания .....	196
<b>Глава 11. Внешние прерывания .....</b>	<b>197</b>
Системный таймер .....	197
Клавиатура .....	201
Часы реального времени .....	203
Примечания .....	203
<b>Глава 12. 32-битовые данные и адреса .....</b>	<b>205</b>
Префиксы размерности операнда и адреса .....	205
Косвенная адресация через 32-битовые регистры .....	211
Новые команды .....	213
Примечания .....	215
<b>ЧАСТЬ II. ЗАЩИЩЕННЫЙ РЕЖИМ .....</b>	<b>217</b>
<b>Глава 13. Код в защищенном режиме .....</b>	<b>219</b>
Опыты с дескрипторами и защитой памяти .....	225
Первые опыты с привилегиями .....	226
Переключение сегментов кода и вентили вызова .....	227
Обратное переключение режима .....	231
Примечания .....	232
<b>Глава 14. Данные и стек .....</b>	<b>235</b>
Дескрипторы данных .....	235
Дескриптор стека .....	238
Режим <i>unreal</i> .....	241
Адресная линия A20 .....	242
Привилегии сегментов данных .....	244
Примечания .....	250
<b>Глава 15. Исключения и прерывания .....</b>	<b>253</b>
Дескрипторы прерываний и исключений .....	253
Коды ошибок для исключений .....	258
Внешние прерывания .....	259
Поле <i>IOPL</i> в регистре флагов .....	266
Примечания .....	267
<b>Глава 16. LDT и TSS .....</b>	<b>269</b>
Дескрипторы LDT .....	269
Программное переключение контекста .....	272
Дескрипторы TSS .....	276
Примечания .....	285
<b>Глава 17. Преобразование адресов .....</b>	<b>287</b>
Первый вариант трансляции адресов .....	288
Вариант <i>PSE</i> .....	292
Вариант <i>PAE</i> .....	295

Плоская модель памяти.....	301
Примечания.....	305
<b>Глава 18. Привилегии .....</b>	<b>307</b>
Изменение уровня привилегий.....	307
Вызов привилегированной процедуры.....	311
Обращение к портам ввода-вывода.....	317
Привилегии при страничном отображении.....	318
Примечания.....	320
<b>ЧАСТЬ III. 64-БИТОВЫЕ РЕЖИМЫ .....</b>	<b>321</b>
<b>Глава 19. Переход в режим совместимости.....</b>	<b>323</b>
Переход в режимы <i>long</i> .....	323
Особенности режима совместимости.....	328
Примечания.....	330
<b>Глава 20. Переход в 64-битовый режим.....</b>	<b>331</b>
Загрузчик <i>ld0</i> .....	331
Применимость 64-битовых данных.....	339
Примечания.....	339
<b>Глава 21. Особенности 64-битового режима .....</b>	<b>341</b>
64-битовые операнды.....	342
Относительная адресация и перемещаемость.....	345
Селекторы <i>fs</i> и <i>gs</i> .....	349
Системные вызовы.....	352
Сегмент задачи в 64-битовом режиме.....	357
Обработка прерываний в 64-битовом режиме.....	359
Примечания.....	370
<b>Послесловие.....</b>	<b>373</b>
<b>ПРИЛОЖЕНИЯ .....</b>	<b>375</b>
<b>Приложение 1. Компиляция Vochs .....</b>	<b>377</b>
Подготовка к компиляции для Windows и Linux.....	377
Компиляция для Windows.....	378
Компиляция для Linux.....	379
Примечания.....	380
<b>Приложение 2. Инструментальные программы FreeDOS.....</b>	<b>381</b>
Файловый менеджер.....	381
Текстовый редактор <i>edit</i> .....	382
Редактор памяти <i>e32</i> .....	382
Форматы отображения данных в <i>d86</i> .....	383
<b>Приложение 3. Дополнительные опыты с FPU.....</b>	<b>384</b>
Команда <i>fistp</i> .....	384
Формат <i>VCD</i> .....	385

---

Прерывания от i80x87 .....	385
Синхронизация процессора и сопроцессора .....	388
Расширение MMX .....	389
Примечания .....	392
<b>Приложение 4. Ошибки в a86/a386 .....</b>	<b>393</b>
Ошибки в a86 .....	393
Ошибки в a386 .....	394
<b>Приложение 5. Описание электронного архива.....</b>	<b>395</b>
<b>Список источников.....</b>	<b>397</b>
<b>Предметный указатель .....</b>	<b>398</b>