
*Студентам и преподавателям курса 15-213
университета Карнеги–Меллона, вдохновившим
нас на переработку и уточнение этого издания*

Оглавление

Предисловие от издательства	17
Вступление	18
Об авторах	34
Глава 1. Экскурс в компьютерные системы	36
1.1. Информация – это биты + контекст.....	38
1.2. Программы, которые переводятся другими программами в различные формы	39
1.3. Как происходит компиляция	41
1.4. Процессоры читают и интерпретируют инструкции, хранящиеся в памяти	42
1.4.1. Аппаратная организация системы.....	42
1.4.2. Выполнение программы hello	44
1.5. Различные виды кеш-памяти	46
1.6. Устройства памяти образуют иерархию.....	47
1.7. Операционная система управляет работой аппаратных средств.....	48
1.7.1. Процессы	49
1.7.2. Потоки.....	50
1.7.3. Виртуальная память.....	51
1.7.4. Файлы.....	53
1.8. Обмен данными в сетях.....	53
1.9. Важные темы	55
1.9.1. Закон Амдала	56
1.9.2. Конкуренция и параллелизм	57
1.9.3. Важность абстракций в компьютерных системах.....	60
1.10. Итоги.....	61
Библиографические заметки.....	61
Решения упражнений	61
Часть I	
Структура программы и ее выполнение	63
Глава 2. Представление информации и работа с ней	64
2.1. Хранение информации.....	68
2.1.1. Шестнадцатеричная система счисления.....	68
2.1.2. Размеры данных	71
2.1.3. Адресация и порядок следования байтов	74
2.1.4. Представление строк	80
2.1.5. Представление программного кода	81
2.1.6. Введение в булеву алгебру	82
2.1.7. Битовые операции в С	85
2.1.8. Логические операции в С.....	87

2.1.9. Операции сдвига в С.....	88
2.2. Целочисленные представления	90
2.2.1. Целочисленные типы	91
2.2.2. Представление целых без знака	92
2.2.3. Представление в дополнительном коде.....	94
2.2.4. Преобразования между числами со знаком и без знака.....	99
2.2.5. Числа со знаком и без знака в С.....	104
2.2.6. Расширение битового представления числа	106
2.2.7. Усечение чисел	109
2.2.8. Советы по приемам работы с числами со знаком и без знака	111
2.3. Целочисленная арифметика	113
2.3.1. Сложение целых без знака	113
2.3.2. Сложение целых в дополнительном коде	118
2.3.3. Отрицание целых в дополнительном коде	123
2.3.4. Умножение целых без знака	124
2.3.5. Умножение целых в дополнительном коде	124
2.3.6. Умножение на константу.....	128
2.3.7. Деление на степень двойки	130
2.3.8. Заключительные размышления о целочисленной арифметике	134
2.4. Числа с плавающей точкой.....	135
2.4.1. Дробные двоичные числа.....	136
2.4.2. Представление значений с плавающей точкой в стандарте IEEE	139
2.4.3. Примеры чисел	141
2.4.4. Округление	146
2.4.5. Операции с плавающей точкой	148
2.4.6. Значения с плавающей точкой в С	150
2.5. Итоги.....	151
Библиографические заметки.....	152
Домашние задания.....	153
Правила представления целых чисел на битовом уровне	154
Правила представления чисел с плавающей точкой на битовом уровне	165
Решения упражнений	167
Глава 3. Представление программ на машинном уровне	184
3.1. Историческая перспектива	187
3.2. Программный код.....	190
3.2.1. Машинный код.....	190
3.2.2. Примеры кода	192
3.2.3. Замечание по форматированию.....	195
3.3. Форматы данных.....	197
3.4. Доступ к информации	198
3.4.1. Спецификаторы операндов	200
3.4.2. Инструкции перемещения данных	201
3.4.3. Примеры перемещения данных	205
3.4.4. Вталкивание данных в стек и выталкивание из стека	208
3.5. Арифметические и логические операции.....	209

3.5.1. Загрузка эффективного адреса	210
3.5.2. Унарные и бинарные операции	212
3.5.3. Операции сдвига	212
3.5.4. Обсуждение	213
3.5.5. Специальные арифметические операции	215
3.6. Управление	218
3.6.1. Флаги условий	218
3.6.2. Доступ к флагам	219
3.6.3. Инструкции перехода	222
3.6.4. Кодирование инструкций перехода	223
3.6.5. Реализация условного ветвления потока управления	225
3.6.6. Реализация условного ветвления потока данных	229
3.6.7. Циклы	235
3.6.8. Оператор switch	245
3.7. Процедуры	250
3.7.1. Стек времени выполнения	251
3.7.2. Передача управления	252
3.7.3. Передача данных	256
3.7.4. Локальные переменные на стеке	258
3.7.5. Локальные переменные в регистрах	260
3.7.6. Рекурсивные процедуры	262
3.8. Распределение памяти под массивы и доступ к массивам	264
3.8.1. Базовые принципы	264
3.8.2. Арифметика указателей	266
3.8.3. Вложенные массивы	267
3.8.4. Массивы фиксированных размеров	268
3.8.5. Массивы переменных размеров	271
3.9. Структуры разнородных данных	273
3.9.1. Структуры	273
3.9.2. Объединения	276
3.9.3. Выравнивание	279
3.10. Комбинирование инструкций управления потоком выполнения и передачи данных в машинном коде	282
3.10.1. Указатели	283
3.10.2. Жизнь в реальном мире: использование отладчика GDB	284
3.10.3. Ссылки на ячейки за границами выделенной памяти и переполнение буфера	286
3.10.4. Предотвращение атак методом переполнения буфера	290
3.10.5. Поддержка кадров стека переменного размера	295
3.11. Вычисления с плавающей точкой	298
3.11.1. Операции перемещения и преобразования данных	300
3.11.2. Операции с плавающей точкой в процедурах	305
3.11.3. Арифметические операции с плавающей точкой	305
3.11.4. Определение и использование констант с плавающей точкой	307
3.11.5. Поразрядные логические операции с числами с плавающей точкой	308
3.11.6. Операции сравнения значений с плавающей точкой	309

3.11.7. Заключительные замечания об операциях с плавающей точкой.....	312
3.12. Итоги.....	312
Библиографические заметки.....	313
Домашние задания.....	314
Решения упражнений.....	325
Глава 4. Архитектура процессора.....	349
4.1. Архитектура системы команд Y86-64.....	352
4.1.1. Состояние, видимое программисту.....	352
4.1.2. Инструкции Y86-64.....	353
4.1.3. Кодирование инструкций.....	355
4.1.4. Исключения в архитектуре Y86-64.....	360
4.1.5. Программы из инструкций Y86-64.....	361
4.1.6. Дополнительные сведения об инструкциях Y86-64.....	366
4.2. Логическое проектирование и язык HCL.....	368
4.2.1. Логические вентили.....	368
4.2.2. Комбинационные цепи и булевы выражения в HCL.....	369
4.2.3. Комбинационные цепи для слов и целочисленные выражения в HCL.....	371
4.2.4. Принадлежность множеству.....	375
4.2.5. Память и синхронизация.....	375
4.3. Последовательные реализации Y86-64 (SEQ).....	378
4.3.1. Организация обработки в несколько этапов.....	378
4.3.2. Аппаратная реализация последовательной архитектуры SEQ.....	387
4.3.3. Синхронизация в последовательной реализации SEQ.....	391
4.3.4. Реализация этапов в последовательной версии SEQ.....	394
4.4. Общие принципы конвейерной обработки.....	402
4.4.1. Вычислительные конвейеры.....	402
4.4.2. Подробное описание работы конвейера.....	404
4.4.3. Ограничения конвейерной обработки.....	406
4.4.4. Конвейерная обработка с обратной связью.....	408
4.5. Конвейерные реализации Y86-64.....	409
4.5.1. SEQ+: переупорядочение этапов обработки.....	409
4.5.2. Добавление конвейерных регистров.....	411
4.5.3. Переупорядочение сигналов и изменение их маркировки.....	415
4.5.4. Прогнозирование следующего значения PC.....	416
4.5.5. Риски конвейерной обработки.....	418
4.5.6. Обработка исключений.....	431
4.5.7. Реализация этапов в PIPE.....	434
4.5.8. Управляющая логика конвейера.....	441
4.5.9. Анализ производительности.....	451
4.5.10. Незаконченная работа.....	454
4.6. Итоги.....	457
4.6.1. Имитаторы Y86-64.....	458
Библиографические заметки.....	458
Домашние задания.....	459
Решения упражнений.....	465

Глава 5. Оптимизация производительности программ	478
5.1. Возможности и ограничения оптимизирующих компиляторов.....	481
5.2. Выражение производительности программы	484
5.3. Пример программы	486
5.4. Устранение неэффективностей в циклах	490
5.5. Сокращение вызовов процедур	493
5.6. Устранение избыточных ссылок на память	495
5.7. Общее описание современных процессоров	498
5.7.1. Общие принципы функционирования.....	498
5.7.2. Производительность функционального блока	502
5.7.3. Абстрактная модель работы процессора	504
5.8. Развертывание циклов	510
5.9. Увеличение степени параллелизма	514
5.9.1. Несколько аккумуляторов.....	515
5.9.2. Переупорядочение операций.....	520
5.10. Обобщение результатов оптимизации комбинирующего кода	524
5.11. Некоторые ограничивающие факторы.....	525
5.11.1. Вытеснение регистров.....	525
5.11.2. Прогнозирование ветвлений и штрафы за ошибки предсказания.....	526
5.12. Понятие производительности памяти	530
5.12.1. Производительность операций загрузки.....	530
5.12.2. Производительность операций сохранения.....	531
5.13. Жизнь в реальном мире: методы повышения производительности.....	537
5.14. Выявление и устранение узких мест производительности	538
5.14.1. Профилирование программ.....	538
5.14.2. Использование профилировщика при выборе кода для оптимизации.....	540
5.15. Итоги.....	544
Библиографические заметки.....	545
Домашние задания.....	545
Решения упражнений	548
Глава 6. Иерархия памяти	553
6.1. Технологии хранения информации.....	554
6.1.1. Память с произвольным доступом.....	554
6.1.2. Диски	562
6.1.3. Твердотельные диски	572
6.1.4 Тенденции развития технологий хранения.....	574
6.2. Локальность.....	577
6.2.1. Локальность обращений к данным программы	577
6.2.2. Локальность выборки инструкций	579
6.2.3. В заключение о локальности.....	579
6.3. Иерархия памяти	581
6.3.1. Кеширование в иерархии памяти.....	582
6.3.2. В заключение об иерархии памяти	585
6.4. Кеш-память	586

6.4.1. Обобщенная организация кеш-памяти	586
6.4.2. Кеш с прямым отображением.....	588
6.4.3. Ассоциативные кеши.....	595
6.4.4. Полностью ассоциативные кеши.....	597
6.4.5. Проблемы с операциями записи	600
6.4.6. Устройство реальной иерархии кешей.....	601
6.4.7. Влияние параметров кеша на производительность	602
6.5. Разработка программ, эффективно использующих кеш	603
6.6. Все вместе: влияние кеша на производительность программ	608
6.6.1. Гора памяти.....	608
6.6.2. Переупорядочение циклов для улучшения пространственной локальности	612
6.6.3. Использование локальности в программах.....	615
6.7. Итоги	616
Библиографические заметки.....	616
Домашние задания.....	617
Решения упражнений	627
Часть II	
Выполнение программ в системе	633
Глава 7. Связывание	634
7.1. Драйверы компиляторов	636
7.2. Статическое связывание.....	637
7.3. Объектные файлы	638
7.4. Перемещаемые объектные файлы.....	638
7.5. Идентификаторы и таблицы имен.....	640
7.6. Разрешение ссылок	643
7.6.1. Как компоновщик разрешает ссылки на повторяющиеся имена	644
7.6.2. Связывание со статическими библиотеками.....	648
7.6.3. Как компоновщики разрешают ссылки на статические библиотеки.....	651
7.7. Перемещение	652
7.7.1. Записи перемещения	653
7.7.2. Перемещение ссылок.....	654
7.8. Выполняемые объектные файлы	657
7.9. Загрузка выполняемых объектных файлов.....	659
7.10. Динамическое связывание с разделяемыми библиотеками.....	660
7.11. Загрузка и связывание с разделяемыми библиотеками из приложений	662
7.12. Перемещаемый программный код	665
7.13. Подмена библиотечных функций	668
7.13.1. Подмена во время компиляции	669
7.13.2. Подмена во время компоновки.....	670
7.13.3. Подмена во время выполнения.....	671
7.14. Инструменты управления объектными файлами.....	673
7.15. Итоги	673

Библиографические заметки.....	674
Домашние задания.....	674
Решения упражнений.....	677
Глава 8. Управление исключениями	680
8.1. Исключения.....	682
8.1.1. Обработка исключений.....	683
8.1.2. Классы исключений.....	685
8.1.3. Исключения в системах Linux/x86-64	687
8.2. Процессы	690
8.2.1. Логический поток управления	691
8.2.2. Конкурентные потоки управления.....	692
8.2.3. Изолированное адресное пространство	693
8.2.4. Пользовательский и привилегированный режимы	693
8.2.5. Переключение контекста	694
8.3. Системные вызовы и обработка ошибок	695
8.4. Управление процессами	696
8.4.1. Получение идентификатора процесса	697
8.4.2. Создание и завершение процессов	697
8.4.3. Утилизация дочерних процессов.....	701
8.4.4. Приостановка процессов.....	706
8.4.5. Загрузка и запуск программ	707
8.4.6. Запуск программ с помощью функций fork и execve	709
8.5. Сигналы	712
8.5.1. Терминология сигналов	714
8.5.2. Посылка сигналов	715
8.5.3. Получение сигналов	717
8.5.4. Блокировка и разблокировка сигналов.....	720
8.5.5. Обработка сигналов.....	721
8.5.6. Синхронизация потоков во избежание неприятных ошибок конкурентного выполнения	730
8.5.7. Явное ожидание сигналов	732
8.6. Нелокальные переходы	735
8.7. Инструменты управления процессами.....	739
8.8. Итоги.....	739
Библиографические заметки.....	740
Домашние задания.....	740
Решения упражнений	747
Глава 9. Виртуальная память	750
9.1. Физическая и виртуальная адресация	752
9.2. Пространства адресов.....	753
9.3. Виртуальная память как средство кеширования.....	754
9.3.1. Организация кеша DRAM.....	754
9.3.2. Таблицы страниц	755
9.3.3. Попадание в кеш DRAM	756
9.3.4. Промах кеша DRAM	757

9.3.5. Размещение страниц.....	758
9.3.6. И снова о локальности.....	759
9.4. Виртуальная память как средство управления памятью.....	759
9.5. Виртуальная память как средство защиты памяти.....	761
9.6. Преобразование адресов.....	762
9.6.1. Интегрирование кешей и виртуальной памяти.....	765
9.6.2. Ускорение трансляции адресов с помощью TLB.....	766
9.6.3. Многоуровневые таблицы страниц.....	767
9.6.4. Все вместе: сквозное преобразование адресов.....	769
9.7. Практический пример: система памяти Intel Core i7/Linux.....	773
9.7.1. Преобразование адресов в Core i7.....	774
9.7.2. Система виртуальной памяти Linux.....	776
9.8. Отображение в память.....	780
9.8.1. И снова о разделяемых объектах.....	781
9.8.2. И снова о функции fork.....	783
9.8.3. И снова о функции execve.....	783
9.8.4. Отображение в память на уровне пользователя с помощью функции mmap.....	785
9.9. Динамическое распределение памяти.....	786
9.9.1. Функции malloc и free.....	787
9.9.2. Что дает динамическое распределение памяти.....	790
9.9.3. Цели механизмов распределения памяти и требования к ним.....	791
9.9.4. Фрагментация.....	792
9.9.5. Вопросы реализации.....	793
9.9.6. Неявные списки свободных блоков.....	794
9.9.7. Размещение распределенных блоков.....	796
9.9.8. Разбиение свободных блоков.....	796
9.9.9. Увеличение объема динамической памяти.....	797
9.9.10. Объединение свободных блоков.....	797
9.9.11. Объединение с использованием граничных тегов.....	798
9.9.12. Все вместе: реализация простого механизма распределения памяти.....	800
9.9.13. Явные списки свободных блоков.....	807
9.9.14. Раздельные списки свободных блоков.....	808
9.10. Сборка мусора.....	811
9.10.1. Основы сборки мусора.....	811
9.10.2. Алгоритм сборки мусора Mark&Sweep.....	813
9.10.3. Консервативный алгоритм Mark&Sweep для программ на C.....	814
9.11. Часто встречающиеся ошибки.....	815
9.11.1. Разыменованное недопустимых указателей.....	815
9.11.2. Чтение неинициализированной области памяти.....	816
9.11.3. Переполнение буфера на стеке.....	816
9.11.4. Предположение о равенстве размеров указателей и объектов, на которые они указывают.....	816
9.11.5. Ошибки занижения или завышения на единицу.....	817
9.11.6. Ссылка на указатель вместо объекта.....	817

9.11.7. Неправильное понимание арифметики указателей	818
9.11.8. Ссылки на несуществующие переменные	818
9.11.9. Ссылка на данные в свободных блоках	818
9.11.10. Утечки памяти	819
9.12. Итоги	819
Библиографические заметки	820
Домашние задания	821
Решения упражнений	824
Часть III	
Взаимодействие программ	829
Глава 10. Системный уровень ввода/вывода	830
10.1. Ввод/вывод в Unix	831
10.2. Файлы	832
10.3. Открытие и закрытие файлов	833
10.4. Чтение и запись файлов	835
10.5. Надежные чтение и запись с помощью пакета RIO	836
10.5.1. Функции RIO небуферизованного ввода/вывода	837
10.5.2. Функции RIO буферизованного ввода	838
10.6. Чтение метаданных файла	842
10.7. Чтение содержимого каталога	843
10.8. Совместное использование файлов	845
10.9. Переадресация ввода/вывода	848
10.10. Стандартный ввод/вывод	849
10.11. Все вместе: какие функции ввода/вывода использовать?	849
10.12. Итоги	851
Библиографические заметки	852
Домашние задания	852
Решения упражнений	853
Глава 11. Сетевое программирование	854
11.1. Программная модель клиент-сервер	854
11.2. Компьютерные сети	855
11.3. Всемирная сеть интернет	860
11.3.1. IP-адреса	861
11.3.2. Доменные имена интернета	863
11.3.3. Интернет-соединения	866
11.4. Интерфейс сокетов	867
11.4.1. Структуры адресов сокетов	868
11.4.2. Функция socket	869
11.4.3. Функция connect	869
11.4.4. Функция bind	870
11.4.5. Функция listen	870
11.4.6. Функция accept	870
11.4.7. Преобразование имен хостов и служб	872
11.4.8. Вспомогательные функции для интерфейса сокетов	876

11.4.9. Примеры эхо-клиента и эхо-сервера	879
11.5. Веб-серверы	881
11.5.1. Основные сведения о вебе	881
11.5.2. Веб-контент	882
11.5.3. Транзакции HTTP	884
11.5.4. Обслуживание динамического контента	886
11.6. Все вместе: разработка небольшого веб-сервера TINY	889
11.7. Итоги	896
Библиографические заметки	896
Домашние задания	897
Решения упражнений	898
Глава 12. Конкурентное программирование	901
12.1. Конкурентное программирование с процессами	903
12.1.1. Конкурентный сервер, основанный на процессах	904
12.1.2. Достоинства и недостатки подхода на основе процессов	905
12.2. Конкурентное программирование с мультиплексированием ввода/вывода	906
12.2.1. Конкурентный на основе мультиплексирования ввода/вывода, управляемый событиями	909
12.2.2. Достоинства и недостатки мультиплексирования ввода/вывода	913
12.3. Конкурентное программирование с потоками выполнения	914
12.3.1. Модель выполнения многопоточных программ	914
12.3.2. Потоки Posix	915
12.3.3. Создание потоков	916
12.3.4. Завершение потоков	916
12.3.5. Утилизация завершившихся потоков	917
12.3.6. Обособление потоков	917
12.3.7. Инициализация потоков	918
12.3.8. Конкурентный многопоточный сервер	918
12.4. Совместное использование переменных несколькими потоками выполнения	920
12.4.1. Модель памяти потоков	921
12.4.2. Особенности хранения переменных в памяти	921
12.4.3. Совместно используемые переменные	922
12.5. Синхронизация потоков выполнения с помощью семафоров	922
12.5.1. Граф выполнения	925
12.5.2. Семафоры	928
12.5.3. Использование семафоров для исключительного доступа к ресурсам	929
12.5.4. Использование семафоров для организации совместного доступа к ресурсам	930
12.5.5. Все вместе: конкурентный сервер на базе предварительно созданных потоков	935
12.6. Использование потоков выполнения для организации параллельной обработки	938
12.7. Другие вопросы конкурентного выполнения	944

12.7.1. Безопасность в многопоточном окружении	944
12.7.2. Реентерабельность	946
12.7.3. Использование библиотечных функций в многопоточных программах.....	947
12.7.4. Состояние гонки.....	948
12.7.5. Взаимоблокировка (тупиковые ситуации).....	950
12.8. Итоги.....	953
Библиографические заметки.....	953
Домашние задания.....	954
Решения упражнений	958
Приложение А. Обработка ошибок	963
А.1. Обработка ошибок в системе Unix	963
А.2. Функции-обертки обработки ошибок.....	965
Библиография.....	968
Предметный указатель	975

Предисловие от издательства

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг – возможно, ошибку в основном тексте или программном коде, – мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Если вы найдете какие-либо ошибки в коде, пожалуйста, сообщите о них главному редактору по адресу dmkpress@gmail.com, и мы исправим это в следующих тиражах.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Pearson очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Вступление

Данная книга предназначена для программистов, желающих повысить свой профессиональный уровень изучением того, что происходит «под кожухом системного блока» компьютерной системы.

Целью авторов является попытка разъяснить устойчивые концепции, лежащие в основе всех компьютерных систем, а также демонстрация конкретных видов влияния этих идей на корректность, производительность и полезные свойства прикладных программ. Многие книги по компьютерным системам написаны *для создателей* таких систем и описывают, как сконструировать оборудование или реализовать системное программное обеспечение, включая операционную систему, компилятор и сетевой интерфейс. Эта книга, напротив, написана *для программиста* и рассказывает, как прикладные программисты могут использовать свои знания о системах для создания более качественных программ. Конечно, знакомство с требованиями к системам является хорошим первым шагом в обучении их созданию, поэтому эта книга послужит также ценным введением для тех, кто продолжает заниматься созданием аппаратного и программного обеспечения систем. Большинство книг по компьютерным системам также имеют тенденцию сосредотачиваться только на одном аспекте системы, например на аппаратной архитектуре, операционной системе, компиляторе или сети. Эта книга охватывает все эти аспекты и рассматривает их с позиции программиста.

Доскональное изучение и освоение изложенных в книге концепций позволит читателю со временем превратиться в редкий тип профессионального программиста, понимающего саму суть происходящего и способного решить любую задачу. Вы сможете писать программы, которые эффективнее используют возможности операционной системы и системного программного обеспечения, действуют правильно в широком диапазоне рабочих условий и параметров, работают быстрее и не содержат уязвимостей для кибератак. При этом будет заложена основа для изучения таких специфических тем, как компиляторы, архитектура компьютерных систем, операционные системы, сети и кибербезопасность.

Что нужно знать перед прочтением

Эта книга посвящена системам с аппаратной архитектурой x86-64, являющиеся последним этапом на пути развития, который прошли Intel и ее конкуренты, начинавшие с микропроцессора 8086 в 1978 году. В соответствии с соглашениями об именовании, принятыми в Intel в отношении их линейки микропроцессоров, этот класс микропроцессоров в просторечии называется «x86». По мере развития полупроводниковых технологий, позволяющих размещать на одном кристалле все больше и больше транзисторов, производительность и объем внутренней памяти процессоров значительно увеличились. В ходе этого прогресса они перешли от 16-разрядных слов к 32-разрядным и выпустили процессор IA32, а совсем недавно произошел переход к 64-разрядным словам и появилась архитектура x86-64.

Мы рассмотрим, как машины с этой архитектурой выполняют программы на языке C в Linux. Linux – одна из операционных систем, ведущих свою родословную от операционной системы Unix, первоначально разработанной в Bell Laboratories. К другим членам этого класса операционных систем относятся Solaris, FreeBSD и MacOS X. В последние годы эти операционные системы сохраняли высокий уровень совместимости благодаря усилиям по стандартизации POSIX и Standard Unix Specification. То есть сведения, что приводятся в этой книге, почти напрямую применимы ко всем этим «Unix-подобным» операционным системам.

Еще незнакомы с C? Совет по языку программирования C

В помощь читателям, плохо знакомым или незнакомым с языком C, авторами предлагаются примечания, подобные данному, для подчеркивания функций, особенно важных для C. Предполагается, что читатели знакомы с C++ или Java.

В тексте содержится множество примеров программного кода, которые мы компилировали и опробовали в системах Linux. Мы предполагаем, что у вас есть доступ к такой системе, что вы можете входить в нее и умеете выполнять простые действия, такие как получение списка файлов или переход в другой каталог. Если ваш компьютер работает под управлением Microsoft Windows, то мы рекомендуем установить одну из множества виртуальных машин (например, VirtualBox или VMWare), которые позволяют программам, написанным для одной операционной системы (гостевой ОС), запускаться в другой (несущей ОС, или хост-ОС).

Также предполагается, что читатель знаком с C или C++. Если весь опыт программиста ограничивается работой с Java, переход потребует от него больше усилий, но авторы окажут всю необходимую помощь. Java и C имеют общий синтаксис и управляющие операторы. Однако в C есть свои особенности (в частности, указатели, явное распределение динамической памяти и форматируемый ввод/вывод), которых нет в Java. К счастью, C – не очень сложный язык, он прекрасно описан в классической книге Брайана Кернигана и Денниса Ритчи [61]. Вне зависимости от «подкованности» читателя в области программирования, эта книга послужит ценным дополнением к его библиотеке. Если прежде вы использовали только интерпретируемые языки, такие как Python, Ruby или Perl, то вам определенно стоит посвятить некоторое время изучению C, прежде чем продолжить читать эту книгу.

В начальных главах книги рассматривается взаимодействие между программами на C и их аналогами на машинном языке. Все примеры на машинном языке были созданы с помощью компилятора GNU GCC на процессоре x86-64. Наличия какого бы то ни было опыта работы с аппаратными средствами, машинными языками или программирования в ассемблере не предполагается.

Как читать книгу

Изучение принципов работы компьютерных систем с точки зрения программиста – занятие очень увлекательное, потому что проходит в интерактивном режиме. Изучив что-то новое, вы тут же можете это проверить и получить результат, что называется, из первых рук. На самом деле авторы полагают, что единственным способом познания систем является их *практическое исследование*: либо путем решения конкретных упражнений, либо написанием и выполнением программ в реально существующих системах.

Система является предметом изучения всей книги. При представлении какой-либо новой концепции в тексте она будет сопровождаться иллюстрацией в форме одной или нескольких *практических задач*, которые нужно сразу же постараться решить, чтобы проверить правильность понимания изложенного. Решения упражнений приводятся в конце каждой главы. Пытайтесь сначала самостоятельно решать эти практические задачи и только потом проверяйте правильность выбранного пути. В конце каждой главы также представлены *домашние задания* различной степени сложности. Каждому домашнему заданию присвоен определенный уровень сложности:

- ◆ для решения достаточно нескольких минут; требуется минимальный объем программирования (или не требуется вообще);
- ◆◆ для решения потребуется до 20 минут. Часто нужно написать и опробовать программный код. Многие такие задания созданы на основе задач, приведенных в примерах;

- ◆◆◆ для решения потребуется приложить значительные усилия; по времени на решение может уйти до 2 часов. Как правило, для выполнения этих заданий требуется написать и опробовать значительный объем кода;
- ◆◆◆ лабораторная работа, на выполнение которой может уйти до 10 часов.

Все примеры кода в тексте книги отформатированы автоматически (без всякого ручного вмешательства) и получены из программ на C, скомпилированных с помощью GCC и протестированных в Linux. Конечно, в вашей системе может быть установлена другая версия gcc или вообще другой компилятор, генерирующий другой машинный код, но общее поведение примеров должно быть таким же. Весь исходный код доступен на веб-странице книги csapp.cs.cmu.edu. Имена файлов с исходным кодом документируются с использованием горизонтальных полос, окружающих отформатированный код. Например, программу из листинга 1 можно найти в файле `hello.c` в каталоге `code/intro/`. Мы советуем обязательно опробовать примеры программ у себя по мере их появления.

Листинг 1. Типичный пример кода

```

1 #include <stdio.h>
2
3 int main()
4 {
5     printf("hello, world\n");
6     return 0;
7 }
```

code/intro/hello.c

code/intro/hello.c

Чтобы не раздувать объем и без того большой книги, мы создали несколько приложений, размещенных в интернете, которые содержат сведения, дополняющие основную книгу. Они отмечены в книге заголовками в форме «Приложение в интернете ТЕМА:ПОДТЕМА», где ТЕМА кратко описывает основную тему, а ПОДТЕМА – раздел темы. Например, «Приложение в интернете DATA:BOOL» содержит сведения по булевой алгебре, дополняющие описание представлений данных в главе 2, а «Приложение в интернете ARCH:VLOG» содержит описание приемов проектирования процессоров с использованием языка описания оборудования Verilog, дополняющее обсуждение конструкции процессора в главе 4. Все эти приложения доступны на веб-странице книги (<https://csapp.cs.cmu.edu/3e/waside.html>).

Обзор книги

Книга состоит из 12 глав, охватывающих основные принципы компьютерных систем:

Глава 1. Экскурс в компьютерные системы.

В этой главе описываются основные идеи и темы, относящиеся к компьютерным системам, на примере исследования жизненного цикла простой программы «hello, world».

Глава 2. Представление информации и работа с ней.

Здесь описывается компьютерная арифметика с упором на свойства представлений числа без знака и числа в дополнительном двоичном коде, которые имеют значение для программистов. В данной главе рассматривается представление чисел и, следовательно, диапазон значений, которые можно запрограммировать для отдельно взятого размера слова. Авторы обсуждают влияние

преобразований типов чисел со знаком и без знака и математические свойства арифметических операций. Для начинающих программистов часто оказывается откровением, что сложение (в дополнительном коде) или умножение двух положительных чисел может дать отрицательный результат. С другой стороны, арифметика дополнительного кода удовлетворяет многим алгебраическим свойствам целочисленной арифметики, благодаря чему компилятор может преобразовать операцию умножения на константу в последовательность сдвигов и сложений. Для иллюстрации принципов и применения булевой алгебры авторы используют поразрядные операции С. Формат IEEE с плавающей точкой описывается в терминах представления значений и математических свойств операций с плавающей точкой.

Абсолютное понимание компьютерной арифметики принципиально для создания надежных программ. Например, программисты и компиляторы не могут заменить выражение $(x < y)$ на $(x - y < 0)$ из-за возможности переполнения. Они не могут даже заменить его выражением $(-y < -x)$ из-за асимметричности диапазона отрицательных и положительных чисел в дополнительном коде. Арифметическое переполнение является обычным источником ошибок программирования и уязвимостей в системе безопасности, однако мало в какой книге можно найти описание свойств компьютерной арифметики, сделанное с точки зрения самого программиста.

О чем рассказывается во врезках?

На протяжении всей книги вам будут встречаться подобные примечания. В них приводятся некоторые дополнительные сведения к обсуждаемой теме. Примечания преследуют несколько целей. Одни представляют собой небольшие исторические экскурсы. Например, как появились С, Linux и Internet? Другие разъясняют какие-либо понятия. Например, чем отличаются кеш, множество и блок? Третьи примечания описывают примеры «из жизни». Например, как ошибка в вычислениях с плавающей точкой уничтожила французскую ракету или какие геометрические и функциональные параметры имеют коммерческие жесткие диски. И наконец, некоторые примечания – это всего лишь забавные комментарии.

Глава 3. Представление программ на машинном уровне.

Авторы научат читать машинный код x86-64, созданный компилятором С. Здесь представлены основные шаблоны инструкций для различных управляющих структур, таких как условные операторы, циклы и операторы выбора. Также рассматривается реализация процедур, включая выделение места на стеке, условные обозначения использования реестров и передачу параметров. В главе рассматриваются различные структуры данных, например структуры, объединения и массивы, их размещение в памяти и доступ к ним. Здесь еще будет показано, как выглядят программы с точки зрения машины, что поможет понять распространенные уязвимости, такие как переполнение буфера, и шаги, которые программист, компилятор и операционная система могут предпринять для уменьшения этих угроз. Изучение данной главы поможет повысить профессиональный уровень, потому что при этом появится понимание, как компьютер воспринимает программы.

Глава 4. Архитектура процессора.

В этой главе описываются комбинаторные и последовательные логические элементы, после чего демонстрируется, как эти элементы можно объединить в

информационный канал, выполняющий упрощенный набор инструкций x86-64 с названием «Y86-64». Сначала будет рассматриваться одноктактный тракт данных. Его архитектура проста, но не отличается высоким быстродействием. Затем будет представлено понятие *конвейерной обработки*, в которой различные шаги, необходимые для обработки инструкции, реализуются как отдельные этапы. В каждый конкретный момент этапы конвейера могут обрабатывать разные инструкции. Получившийся в результате пятиступенчатый процессорный конвейер намного более реалистичен. Управляющая логика процессора описывается с использованием простого языка описания аппаратных средств – NCL. Проекты аппаратного обеспечения, написанные на NCL, можно компилировать и объединять в симуляторы, а затем использовать для создания описания Verilog, пригодного для производства реального оборудования.

Глава 5. Оптимизация производительности программ.

В этой главе представлен ряд методов повышения производительности кода, при этом идея состоит в том, что программисты учатся писать код на C так, чтобы компилятор мог затем сгенерировать эффективный машинный код. Сначала рассматриваются преобразования, сокращающие объем работы, которую предстоит выполнить программе, и, следовательно, которые должны стать стандартной практикой при написании любых программ для любых машин. Затем мы перейдем к преобразованиям, повышающим степень параллелизма на уровне команд в сгенерированном машинном коде, чтобы повысить их производительность на современных «суперскалярных» процессорах. Для обоснования этих преобразований будет представлена простая модель работы современных процессоров и показано, как измерить потенциальную производительность программы с точки зрения критических путей с использованием графического представления программы. Вы будете удивлены, насколько можно ускорить программу, применив простые преобразования к коду на C.

Глава 6. Иерархия памяти.

Память является для программистов одной из самых «заметных» частей компьютерной системы. До этой главы читатели полагались на концептуальную модель памяти в форме одномерного массива с постоянным временем доступа. На практике память представляет собой иерархию запоминающих устройств разной емкости, стоимости и быстродействия. В главе рассматриваются разные типы памяти, такие как ОЗУ и ПЗУ, а также геометрические параметры и устройство существующих современных дисковых накопителей, организация этих запоминающих устройств в иерархию. Авторы показывают возможность иерархической организации посредством локальности ссылок. Данные идеи конкретизируются представлением уникального взгляда на систему памяти как на «гору памяти» со «скалами» временной локальности и «склонами» пространственной локальности. В заключение рассказывается, как повысить производительность программных приложений путем усовершенствования их временной и пространственной локальности.

Глава 7. Связывание.

В данной главе описывается статическое и динамическое связывание, включая такие понятия, как: перемещаемые и выполняемые объектные файлы, разрешение символов, перемещение, статические библиотеки, разделяемые библиотеки, перемещаемый код и подмена библиотечных функций (library interpositioning). Тема связывания редко рассматривается в книгах по компьютерным системам, но авторы решили включить ее в эту книгу по двум причи-

нам. Во-первых, некоторые типичные ошибки, с которыми сталкиваются программисты, как раз возникают на этапе связывания и особенно характерны для крупных программных пакетов. Во-вторых, объектные файлы, создаваемые компоновщиками, связаны с такими понятиями, как загрузка, виртуальная память и отображение памяти.

Глава 8. Управление исключениями.

В этой главе авторы отступают от однопрограммной модели, вводя общую концепцию потока управления исключениями (не совпадающего с обычным потоком управления путем ветвления в условных операторах и в точках вызова процедур). Мы рассмотрим примеры потоков управления исключениями, существующих на всех уровнях системы, от аппаратных исключений и прерываний низкого уровня до переключения контекста между параллельными процессами, внезапных изменений в потоке управления, вызванных передачей сигналов Linux, и нелокальных переходов в C, разрывающих стройную структуру стека.

В этой части книги будет представлено фундаментальное понятие *процесса* как абстракции выполняющейся программы. Здесь авторы расскажут, как работают процессы, как их создавать и как ими можно управлять из прикладных программ, и покажут, как прикладные программисты могут запустить несколько процессов с помощью системных вызовов Linux. По окончании этой главы вы сможете написать простую командную оболочку для Linux с поддержкой управления заданиями. Эта глава также станет первым знакомством с недетерминированным поведением, возникающим при параллельных вычислениях.

Глава 9. Виртуальная память.

Описывает представление системы виртуальной памяти с целью дать некоторое понимание ее особенностей и принципов работы. Здесь вы узнаете, как разные процессы, действующие одновременно, могут использовать один и тот же диапазон адресов, совместно использовать одни страницы памяти и иметь индивидуальные копии других. В этой главе также описываются вопросы, связанные с управлением виртуальной памятью и манипуляциями с ней. В частности, мы уделим большое внимание инструментам распределения памяти из стандартной библиотеки, таким как `malloc` и `free`. Обсуждение данной темы преследует несколько целей. Прежде всего оно подкрепляет концепцию о том, что пространство виртуальной памяти является всего лишь массивом байтов, который программа может разделить на блоки разного размера для хранения данных. Помогает понять последствия ошибок обращения к памяти в программах, такие как утечки и недействительные ссылки в указателях. Наконец, многие программисты реализуют свои инструменты распределения памяти, оптимизированные под требования и характеристики конкретного приложения. Эта глава в большей степени, чем любая другая, демонстрирует преимущества неразрывного освещения аппаратных и программных аспектов компьютерных систем. Книжки о традиционных компьютерных архитектурах и операционных системах обычно представляют виртуальную память только с одной стороны.

Глава 10. Системный уровень ввода/вывода.

В этой главе рассматриваются основные концепции ввода/вывода в системе Unix, такие как файлы и дескрипторы. Авторы описывают совместное использование файлов, принципы работы переадресации ввода/вывода и доступ к метаданным файлов. Здесь также представлен пример разработки надежного пакета буферизованного ввода/вывода, прекрасно справляющегося с любопыт-

ным поведением подсистемы ввода/вывода, известным как *недостача*, когда библиотечные функции возвращают только часть ввода. В главе описывается стандартная библиотека ввода/вывода языка C и ее связь с подсистемой ввода/вывода в Linux с упором на ограничения стандартного ввода/вывода, делающие его непригодным для сетевого программирования. Вообще говоря, темы, охваченные в этой главе, служат основой для двух следующих глав, посвященных сетевому и параллельному программированию.

Глава 11. Сетевое программирование.

Сети являются своеобразными устройствами ввода/вывода для программ, объединяющими многие из понятий, описанных ранее: процессы, сигналы, порядок следования байтов, отображение памяти и динамическое распределение пространства запоминающих устройств. Сетевые программы также являются одними из первых кандидатов на применение приемов параллельного программирования, о котором рассказывается в следующей главе. Данная глава – лишь тонкий срез глобального предмета сетевого программирования, необходимый для создания простенького веб-сервера. Здесь будет представлена модель клиент–сервер, лежащая в основе всех сетевых приложений. Авторы представят взгляд программиста на сеть Интернет и покажут, как писать сетевые клиенты и серверы, используя интерфейс сокетов. И наконец, в главе будет представлен протокол HTTP и разработан простой веб-сервер.

Глава 12. Конкурентное программирование.

Эта глава описывает принципы конкурентного (параллельного) программирования на примере сетевого сервера. Авторы сравнивают и противопоставляют три основных механизма, используемых для создания конкурентных программ: процессы, мультиплексирование ввода/вывода и потоки выполнения – и показывают возможность их использования при создании серверов, способных обслуживать множество одновременных соединений. Здесь же описаны основные принципы синхронизации с использованием семафорных операций *P* и *V*, безопасность потоков выполнения и реентерабельность, а также состояние взаимоблокировки. Конкурентное программирование играет важную роль в большинстве сетевых приложений. Также в этой главе описывается конкурентное программирование на уровне потоков выполнения, что позволяет ускорить решение задач на многоядерных процессорах. Чтобы все ядра правильно и эффективно работали над одной вычислительной задачей, требуется тщательная координация потоков, выполняющихся конкурентно.

Что нового в этом издании

Первое издание этой книги было опубликовано в 2003 году, а второе – в 2011. Учитывая быстрое развитие компьютерных технологий, содержимое книги на удивление хорошо сохранило свою актуальность. Принципиальное устройство компьютеров Intel x86, на которых выполняются программы на C под управлением Linux (и других похожих операционных систем), мало изменилось за эти годы. Однако изменения в аппаратных технологиях, компиляторах, интерфейсах программных библиотек и накопленный опыт преподавания потребовали существенного пересмотра материала книги.

Самым большим изменением по сравнению со вторым изданием является переход с представления, основанного на сочетании IA32 и x86-64, к представлению, основанному исключительно на x86-64. Это смещение акцента повлияло на содержимое многих глав. Вот краткое перечисление основных значительных изменений.

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

e-Univers.ru