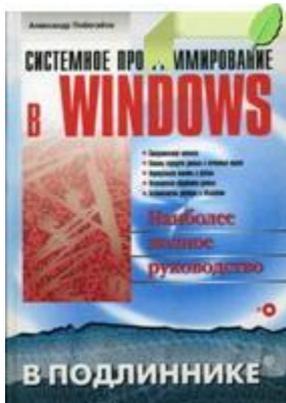


Побегайло А. П. Системное программирование в Windows. — СПб.: БХВ-Петербург, 2006. - 1056 с: ил.



ISBN 5-94157-792-3

Подробно рассматриваются вопросы системного программирования с использованием интерфейса Win 32 API. Описываются управление потоками и процессами, включая их диспетчеризацию; синхронизация потоков; передача данных между процессами, с использованием анонимных и именованных каналов, а также почтовых ящиков; структурная обработка исключений; управление виртуальной памятью; управление файлами и каталогами; асинхронная обработка данных; создание динамически подключаемых библиотек; разработка сервисов. Отдельная часть книги посвящена управлению безопасностью объектов в Windows. Каждая тема снабжена практическими примерами использования функций Win 32 API, которые представлены работающими листингами. Это позволяет использовать книгу в качестве пособия по системному программированию или справочника для системного программиста. Прилагаемый компакт-диск содержит листинги и проекты всех программ, рассмотренных в книге.

Оглавление

Предисловие.	15
Глава 1. Операционные системы и их интерфейсы	19
1.1. Назначение операционной системы	19
1.2. Типы операционных систем	19
1.3. Интерфейс программирования приложений Win 32 API	21
1.4. Типы данных в Win 32 API	22
1.5. Объекты и их дескрипторы в Windows	24
ЧАСТЬ I . УПРАВЛЕНИЕ ПОТОКАМИ И ПРОЦЕССАМИ	27
Глава 2. Потоки и процессы	29
2.1. Определение потока	29
2.2. Контекст потока	31
2.3. Состояния потока	33
2.4. Диспетчеризация и планирование потоков	37
2.5. Определение процесса	40
Глава 3. Потоки в Windows	41
3.1. Определение потока	41
3.2. Создание потоков	42
3.3. Завершение потоков	47
3.4. Приостановка и возобновление потоков	49
3.5. Псевдодескрипторы потоков	52
3.6. Обработка ошибок в Windows	53
Глава 4. Процессы в Windows	58
4.1. Определение процесса	58
4.2. Создание процессов	58
4.3. Завершение процессов	64
4.4. Наследование дескрипторов	67
4.5. Дублирование дескрипторов	75
4.6. Псевдодескрипторы процессов	81
4.7. Обслуживание потоков	82
4.8. Динамическое изменение приоритетов потоков	88
ЧАСТЬ II . СИНХРОНИЗАЦИЯ ПОТОКОВ И ПРОЦЕССОВ	93
Глава 5. Синхронизация	95
5.1. Непрерывные действия и команды	95
5.2. Определение синхронизации	96
5.3. Программная реализация синхронизации	97
5.4. Аппаратная реализация синхронизации	101
5.5. Примитивы синхронизации	104
Глава 6. Синхронизация потоков в Windows	109
6.1. Критические секции	109
6.2. Объекты синхронизации и функции ожидания	115
6.3. Мьютексы	121
6.4. События	128
6.5. Семафоры	137
Глава 7. Взаимоисключающий доступ к переменным	143

7.1.Атомарные операции	143
7.2.Замена значения переменной	144
7.3.Условная замена значения переменной	146
7.4.Инкремент и декремент переменной	148
7.5.Изменение значения переменной	150
Глава 8. Тупики	153
8.1.Определение тупиков	153
8.2.Классификация системных ресурсов	154
8.3.Обнаружение тупиков	156
8.4.Восстановление заблокированного процесса	158
8.5.Предотвращение тупиков	160
8.6.Безопасное завершение потоков в Windows	161
ЧАСТЬ III . ПРОГРАММИРОВАНИЕ КОНСОЛЬНЫХ ПРИЛОЖЕНИЙ	165
Глава 9. Структура консольного приложения	167
9.1.Структура консоли	167
9.2.Входной буфер консоли	167
9.3.Буфер экрана	171
Глава 10. Работа с консолью	172
10.1.Создание консоли	172
10.2.Освобождение консоли	177
10.3.Стандартные дескрипторы ввода-вывода	178
Глава 11. Работа с окном консоли	180
11.1.Получение дескриптора окна консоли	180
11.2.Получение и изменение заголовка консоли	181
11.3.Определение максимального размера окна	183
11.4.Установка координат окна	184
Глава 12. Работа с буфером экрана	188
12.1.Создание и активация буфера экрана	188
12.2.Определение и установка параметров буфера экрана	191
12.3.Функции для работы с курсором	194
12.4.Чтение и установка атрибутов консоли	197
Глава 13. Ввод-вывод на консоль	203
13.1.Ввод-вывод высокого уровня	203
13.2.Ввод низкого уровня	207
13.3.Вывод низкого уровня	215
13.4.Режимы ввода-вывода консоли	225
13.5.Прокрутка буфера экрана	229
ЧАСТЬ IV . ОБМЕН ДАННЫМИ МЕЖДУ ПАРАЛЛЕЛЬНЫМИ ПРОЦЕССАМИ	235
Глава 14. Передача данных	237
14.1.Способы передачи данных между процессами	237
14.2.Связи между процессами	239
14.3.Передача сообщений	240
14.4.Синхронный и асинхронный обмен данными	241
14.5.Буферизация	242
Глава 15. Работа с анонимными каналами в Windows	243
15.1.Анонимные каналы	243
15.2.Создание анонимных каналов	244
15.3.Соединение клиентов с анонимным каналом	245
15.4.Обмен данными по анонимному каналу	246
15.5.Примеры работы с анонимными каналами	247
15.6.Перенаправление стандартного ввода-вывода	257
Глава 16. Работа с именованными каналами в Windows	265
16.1.Именованные каналы	265
16.2.Создание именованных каналов	266
16.3.Соединение сервера с клиентом	268
16.4.Соединение клиентов с именованным каналом	269
16.5.Обмен данными по именованному каналу	272
16.6.Копирование данных из именованного канала	285
16.7.Передача транзакций по именованному каналу	289
16.8.Определение и изменение состояния именованного канала	295
16.9.Получение информации об именованном канале	303
Глава 17. Работа с почтовыми ящиками в Windows	307
17.1.Концепция почтовых ящиков	307
17.2.Создание почтовых ящиков	308
17.3.Соединение клиентов с почтовым ящиком	309
17.4.Обмен данными через почтовый ящик	311
17.5.Получение информации о почтовом ящике	315

17.6.Изменение времени ожидания сообщения	321
ЧАСТЬ V . СТРУКТУРНАЯ ОБРАБОТКА ИСКЛЮЧЕНИЙ	325
Глава 18. Фреймовая обработка исключений	327
18.1.Исключения и их обработчики	327
18.2.Получение кода исключения	330
18.3.Функции фильтра	332
18.4.Получение информации об исключении	334
18.5.Генерация программных исключений	337
18.6.Необработанные исключения	340
18.7.Обработка исключений с плавающей точкой	342
18.8.Обработка вложенных исключений	344
18.9.Передача управления и выход из фрейма	346
18.10.Встраивание SEH в механизм исключений C ++	348
Глава 19. Финальная обработка исключений	351
19.1.Финальные блоки фрейма	351
19.2.Проверка завершения фрейма	353
19.3.Обработка вложенных финальных блоков	354
ЧАСТЬ VI . РАБОТА С ВИРТУАЛЬНОЙ ПАМЯТЬЮ	357
Глава 20. Виртуальная память	359
20.1.Концепция виртуальной памяти	359
20.2.Организация виртуальной памяти	360
20.3.Алгоритмы замещения страниц	362
20.4.Рабочее множество процесса	363
20.5.Организация виртуальной памяти в Windows	363
Глава 21. Работа с виртуальной памятью в Windows	367
21.1.Состояния виртуальной памяти процесса	367
21.2.Резервирование, распределение и освобождение виртуальной памяти	368
21.3.Блокирование виртуальных страниц в реальной памяти	376
21.4.Изменение атрибутов доступа к виртуальной странице	378
21.5.Управление рабочим множеством страниц процесса	380
21.6.Инициализация и копирование блоков виртуальной памяти	383
21.7.Определение состояния памяти	385
21.8.Работа с виртуальной памятью в другом процессе	388
Глава 22. Работа с кучей в Windows	393
22.1.Создание и удаление кучи	393
22.2.Распределение и освобождение памяти из кучи	395
22.3.Перераспределение памяти из кучи	401
22.4.Блокирование и разблокирование кучи	403
22.5.Проверка состояния кучи	406
22.6.Уплотнение кучи	411
ЧАСТЬ VII . УПРАВЛЕНИЕ ФАЙЛАМИ	415
Глава 23. Общие концепции	417
23.1.Накопители на жестких магнитных дисках	417
23.2.Секторы и кластеры	418
23.4.Форматирование дисков	419
23.5.Функции файловой системы	420
23.6.Каталоги	420
23.7.Буферизация ввода-вывода	421
23.8.Кэширование ввода-вывода	421
Глава 24. Работа с файлами в Windows	423
24.1.Именованые файлов в Windows	423
24.2.Создание и открытие файлов	424
24.3.Заккрытие и удаление файлов	427
24.4.Запись данных в файл	428
24.5.Освобождение буферов файла	430
24.6.Чтение данных из файла	433
24.7.Копирование файла	435
24.8.Перемещение файла	437
24.9.Замещение файла	438
24.10.Работа с указателем позиции файла	440
24.11.Определение и изменение атрибутов файла	446
24.12.Определение и изменение размеров файла	449
24.13.Блокирование файла	455
24.14.Получение информации о файле	459
Глава 25. Работа с каталогами (папками) в Windows	468
25.1. Создание каталога	468
25.2. Поиск файлов в каталоге	470
25.3. Удаление каталога	473

25.4. Перемещение каталога	476
25.5. Определение и установка текущего каталога	477
25.6. Наблюдение за изменениями в каталоге	479
ЧАСТЬ VIII . АСИНХРОННАЯ ОБРАБОТКА ДАННЫХ	483
Глава 26. Асинхронный вызов процедур	485
26.1. Механизм асинхронного вызова процедур	485
26.2. Установка асинхронных процедур	486
26.3. Приостановка потока	487
26.4. Ожидание события	489
26.5. Оповещение и ожидание события	494
Глава 27. Асинхронный доступ к данным	499
27.1. Концепция асинхронного ввода-вывода	499
27.2. Асинхронная запись данных	500
27.3. Асинхронное чтение данных	506
24.1. Блокирование файлов	511
27.1. Определение состояния асинхронной операции ввода-вывода	518
27.2. Отмена асинхронной операции ввода-вывода	522
27.3. Процедуры завершения ввода-вывода	528
27.4. Асинхронная запись данных с процедурами завершения	529
27.5. Асинхронное чтение данных с процедурами завершения	532
Глава 28. Порты завершения	536
28.1. Концепция порта завершения	536
28.2. Создание порта завершения	537
28.3. Получение пакета из порта завершения	538
28.4. Посылка пакета в порт завершения	539
Глава 29. Работа с ожидающим таймером	544
29.1. Ожидающий таймер	544
29.2. Создание ожидающего таймера	545
29.3. Установка ожидающего таймера	546
29.4. Отмена ожидающего таймера	549
29.5. Открытие существующего ожидающего таймера	552
29.6. Процедуры завершения ожидания	555
ЧАСТЬ IX. ДИНАМИЧЕСКИ ПОДКЛЮЧАЕМЫЕ	
БИБЛИОТЕКИ	559
Глава 30.Отображение файлов в память	561
30.1. Концепция механизма отображения файлов в память	561
30.2. Создание и открытие объекта, отображающего файл	562
30.3. Отображение файла в память	564
30.4. Обмен данными между процессами через отображаемый в память файл	569
30.5. Сброс вида в файл	573
Глава 31. Динамически подключаемые библиотеки	578
31.1. Концепция динамически подключаемых библиотек	578
31.2. Создание DLL	579
31.3. Динамическая загрузка и отключение DLL	581
31.4. Использование DLL	584
31.5. Использование файла определений	588
31.6. Статическая загрузка DLL	592
Глава 32. Локальная память потока	594
32.1. Динамическая локальная память потока	594
32.2. Распределение и освобождение локальной памяти потока	595
32.3. Запись и чтение из локальной памяти потока	595
32.4. Статическая локальная память потока	602
ЧАСТЬ X . РАЗРАБОТКА СЕРВИСОВ В WINDOWS	605
Глава 33. Сервисы в Windows	607
33.1. Концепция сервиса	607
33.2. Структура сервиса	608
33.3. Организация функции <i>main</i>	609
33.4. Организация функции <i>ServiceMain</i>	611
33.5. Организация обработчика управляющих команд	617
Глава 34. Работа с сервисами в Windows	620
34.1. Открытие доступа к базе данных сервисов	620
34.2. Установка сервиса	621
34.3. Открытие доступа к сервису	627
34.4. Запуск сервиса	627
34.5. Определение и изменение состояния сервиса	630
34.6. Определение и изменение конфигурации сервиса	634
34.7. Определение имени сервиса	641
34.8. Управление сервисом	646

34.9. Удаление сервисов	649
34.10. Блокирование базы данных сервисов	653
ЧАСТЬ XI . УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ В WINDOWS	659
Глава 35. Система информационной безопасности	661
35.1. Контроль доступа к ресурсам	661
35.2. Политика безопасности	662
35.3. Модель безопасности	663
35.4. Дискреционная политика безопасности	664
35.5. Дискреционная модель безопасности	665
35.6. Реализация дискреционной модели безопасности	668
Глава 36. Управление безопасностью в Windows	671
36.1. Модель безопасности в Windows	671
36.2. Учетные записи	672
36.3. Домены	674
36.4. Группы	676
36.5. Идентификаторы безопасности	678
36.6. Дескрипторы безопасности	682
36.7. Списки управления доступом ACL	683
36.8. Маркеры доступа	687
36.9. Создание новых объектов	693
36.10. Контроль доступа к охраняемому объекту	694
36.11. Аудит доступа к охраняемому объекту	696
36.12. Структура системы безопасности	696
Глава 37. Управление пользователями	699
37.1. Создание учетной записи пользователя	699
37.2. Получение информации о пользователе	704
37.3. Перечисление пользователей	706
37.4. Перечисление групп, которым принадлежит пользователь	710
37.5. Изменение учетной записи пользователя	715
37.6. Изменение пароля пользователя	719
37.7. Удаление учетной записи пользователя	721
Глава 38. Управление группами	724
38.1. Создание локальной группы	724
38.2. Получение информации о локальной группе	727
38.3. Перечисление локальных групп	729
38.4. Изменение информации о локальной группе	732
38.5. Добавление членов локальной группы	736
38.6. Установка членов локальной группы	742
38.7. Перечисление членов локальной группы	745
38.8. Удаление членов локальной группы	748
38.9. Удаление локальной группы	754
Глава 39. Работа с идентификаторами безопасности	756
39.1. Структура идентификатора безопасности	756
39.2. Создание идентификатора безопасности	757
39.3. Определение учетной записи по идентификатору безопасности	764
39.4. Определение идентификатора безопасности по имени учетной записи	769
39.5. Получение характеристик идентификатора безопасности	773
39.6. Копирование и сравнение идентификаторов безопасности	777
39.7. Строковое представление идентификатора безопасности	782
Глава 40. Работа с дескрипторами безопасности	788
40.1. Форматы дескрипторов безопасности	788
40.2. Создание нового дескриптора безопасности	791
40.3. Определение длины дескриптора безопасности	797
40.4. Получение дескриптора безопасности по имени объекта	802
40.5. Получение дескриптора безопасности по дескриптору объекта	806
40.6. Получение данных из дескриптора безопасности	810
40.7. Получение состояния управляющих флагов дескриптора безопасности	815
40.8. Изменение дескриптора безопасности по имени объекта	818
40.9. Изменение дескриптора безопасности по дескриптору объекта	823
40.10. Изменение состояния управляющих флагов дескриптора безопасности	827
40.11. Строковое представление дескрипторов безопасности	831
Глава 41. Работа со списками управления доступом на высоком уровне	840
41.1. Структура <i>TRUSTEE</i>	840
41.2. Инициализация структуры <i>TRUSTEE</i>	842
41.3. Структура <i>EXPLICIT_ACCESS</i>	846
41.4. Инициализация структуры <i>EXPLICIT_ACCESS</i>	849
41.5. Создание нового списка управления доступом	850

41.6. Модификация списка управления доступом	862
41.7. Получение элементов из списка управления доступом	870
41.8. Получение информации из структуры <i>TRUSTEE</i>	871
41.9. Получение прав доступа из списка управления доступом	874
41.10. Получение из списка управления доступом прав, которые подвергаются аудиту	878
Глава 42. Работа с привилегиями	885
42.1. Локальные идентификаторы привилегий	885
42.2. Инициализация локального идентификатора	887
42.3. Получение локального идентификатора привилегии	888
42.4. Получение имени привилегии	888
42.5. Получение имени привилегии для отображения	891
Глава 43. Работа с маркерами доступа	894
43.1. Открытие маркера доступа процесса	894
43.2. Открытие маркера доступа потока	896
43.3. Структуры, используемые для работы с маркером доступа	896
43.4. Получение информации из маркера доступа	900
43.5. Изменение информации в маркере доступа	908
43.6. Настройка привилегий	917
43.7. Настройка групп	918
43.8. Создание маркера ограниченного доступа	920
43.9. Дублирование маркеров доступа	927
43.10. Замещение маркеров доступа потока	929
43.11. Проверка идентификатора безопасности на принадлежность маркеру доступа	932
Глава 44. Работа со списками управления доступом на низком уровне	939
44.1. Структура списка управления доступом	939
44.2. Структура элемента списка управления доступом	940
44.3. Инициализация списка управления доступом	943
44.4. Проверка достоверности списка управления доступом	944
44.5. Добавление элементов в список управления доступом	945
44.6. Получение элементов из списка управления доступом	972
44.7. Удаление элементов из списка управления доступом	977
44.8. Получение информации о списке управления доступом	981
44.9. Установка версии списка управления доступом	985
44.10. Определение доступной памяти	986
Глава 45. Управление безопасностью объектов на низком уровне	987
45.1. Доступ к информации о владельце объекта	988
45.2. Доступ к информации о первичной группе владельца объекта	992
45.3. Доступ к списку DACL	997
45.4. Доступ к списку SACL	1004
45.5. Защита файлов и каталогов	1006
45.6. Защита объектов ядра	1016
45.7. Защита сервисов	1024
45.8. Защита ключей реестра	1031
45.9. Защита объектов пользователя	1037
Приложение. Описание компакт-диска	1045
Предметный указатель	1047