

• КЛАССИКА COMPUTER SCIENCE

Марк Руссинович, Дэвид Соломон,
Алекс Ионеску, Павел Йосифович

ВНУТРЕННЕЕ УСТРОЙСТВО WINDOWS

СЕДЬМОЕ ИЗДАНИЕ



Санкт-Петербург • Москва • Минск

2025

Оглавление

Введение	16
История книги	16
Изменения, внесенные в седьмое издание	17
Практические эксперименты	18
Незатронутые темы	18
Предупреждение и предостережение	18
Что мы ожидаем от читателя	19
Структура книги	19
Благодарности	20
Список опечаток и качество книги	21
От издательства	21
Глава 1. Концепции и средства	22
Версии операционной системы Windows	22
Windows 10 и будущие версии Windows	24
Windows 10 и OneCore	24
Фундаментальные концепции и термины	25
Windows API	25
Разновидности Windows API	26
Windows Runtime	27
.NET Framework	28
Службы, функции и процедуры	29
Процессы	30
Потоки	41
Волокна	42
Планирование пользовательского режима (UMS)	42
Задания	44
Виртуальная память	44

Режим ядра и пользовательский режим	47
Гипервизор	53
Микропрограммы	54
Службы терминалов и сеансы	55
Объекты и дескрипторы	56
Безопасность	57
Реестр	59
Юникод	60
Изучение внутреннего устройства Windows	62
Системный монитор и Монитор ресурсов	63
Отладка ядра	65
Средства отладки для Windows	66
Программа LiveKd	70
Windows Software Development Kit	71
Windows Driver Kit	71
Средства Sysinternals	72
Заключение	72
Глава 2. Архитектура системы	73
Требования и цели проектирования	73
Модель операционной системы	74
Обзор архитектуры	75
Портируемость	78
Симметричная многопроцессорная архитектура	80
Масштабируемость	83
Различия между клиентскими и серверными версиями	84
Отладочная сборка	88
Обзор архитектуры безопасности на основе виртуализации	90
Ключевые компоненты системы	93
Подсистемы среды и DLL среды	94
Другие подсистемы	101
Ядро	110
Слой абстрагирования оборудования (HAL)	114
Драйверы устройств	118
Системные процессы	126
Заключение	139

Глава 3. Процессы и задания	140
Создание процесса	140
Аргументы функций CreateProcess*	142
Создание современных процессов Windows	143
Создание других разновидностей процессов	143
Внутреннее устройство процессов	144
Защищенные процессы	153
Облегченные защищенные процессы (PPL)	155
Сторонняя поддержка PPL	160
Минимальные процессы и процессы Pico	161
Минимальные процессы	162
Процессы Pico	162
Трастлеты (безопасные процессы)	165
Структура трастлета	165
Метаданные политики трастлетов	166
Атрибуты трастлета	168
Встроенные системные трастлеты	168
Идентификация трастлета	169
Изолированные службы пользовательского режима	170
Системные функции, доступные для трастлетов	171
Порядок работы функции CreateProcess	173
Этап 1. Преобразование и проверка параметров и флагов	175
Этап 2. Открытие образа, предназначенного для исполнения	180
Этап 3. Создание объекта процесса исполняющей системы Windows	183
Этап 4. Создание исходного потока, а также его стека и контекста	190
Этап 5. Выполнение инициализации, относящейся к подсистеме Windows	193
Этап 6. Начало выполнения исходного потока	195
Этап 7. Выполнение инициализации процесса в контексте нового процесса	196
Завершение процесса	203
Загрузчик образов	204
Ранняя стадия инициализации процесса	206
Разрешение имен DLL-библиотек и перенаправление	210
База данных загруженных модулей	215
Анализ импорта	220
Инициализация процесса после импортирования	222

Технология SwitchBack	223
Наборы API-функций	226
Задания	229
Ограничения заданий	230
Работа с заданиями	232
Вложенные задания	233
Контейнеры Windows (серверные участки)	237
Заключение	247
Глава 4. Потоки	248
Создание потоков	248
Внутреннее устройство потоков	249
Структуры данных	250
Рождение потока	262
Изучение активности потока	263
Ограничения, накладываемые на потоки защищенного процесса	268
Планирование потоков	270
Обзор организации планирования в Windows	270
Уровни приоритета	272
Состояния потоков	280
База данных диспетчера	287
Кванты времени	290
Повышение приоритета	298
Переключения контекста	318
Сценарии планирования	320
Потоки простоя	325
Приостановка потока	329
(Глубокое) замораживание	330
Выбор потока	332
Многопроцессорные системы	334
Выбор потока на многопроцессорных системах	352
Выбор процессора	354
Неоднородное планирование (big.LITTLE)	357
Групповое планирование	359
Распределенное справедливое долевое планирование	361
Ограничения долевого использования процессоров	365
Динамическое добавление и удаление процессоров	368

Рабочие фабрики (пулы потоков)	370
Создание рабочей фабрики	372
Заключение	374
Глава 5. Управление памятью	375
Знакомство с диспетчером памяти	375
Компоненты диспетчера памяти	376
Большие и малые страницы	377
Анализ использования памяти	380
Внутренняя синхронизация	383
Сервисные функции, предоставляемые диспетчером памяти	384
Состояние страниц и выделение памяти	386
Нагрузка подтверждения памяти и предел подтверждения	390
Блокировка памяти	390
Гранулярность выделения памяти	391
Общая память и отображенные файлы	392
Защита памяти	395
Предотвращение выполнения данных	397
Копирование при записи	401
Address Windowing Extensions	403
Кучи режима ядра (пулы системной памяти)	405
Размеры пулов	406
Анализ использования пулов	408
Резервные списки	412
Диспетчер кучи	413
Кучи процессов	414
Типы куч	415
Синхронизация кучи	416
Низкофрагментированная куча	417
Сегментная куча	418
Безопасность кучи в Windows	423
Средства отладки кучи	425
Pageheap	426
Отказоустойчивая куча	429
Структуры виртуального адресного пространства	431
Структура адресных пространств x86	433
Структура системного адресного пространства на платформе x86	436

Пространство сеанса на платформе x86	437
Записи системной таблицы страниц	439
Структура адресного пространства ARM	440
Структура адресных пространств 64-разрядных систем	441
Ограничения виртуальной адресации на платформе x64	443
Динамическое управление системным виртуальным адресным пространством	443
Квоты системного виртуального адресного пространства	449
Структура пользовательского адресного пространства	451
Преобразование адресов	458
Преобразование виртуальных адресов на платформе x86	458
Буфер быстрого преобразования адресов	465
Преобразование виртуальных адресов на платформе x64	469
Преобразование виртуальных адресов на платформе ARM	470
Обработка ошибок страниц	472
Недостоверные PTE-записи	473
Прототипные PTE-записи	475
Страничный ввод/вывод	477
Конфликтные ошибки отсутствия страниц	478
Кластерные ошибки страниц	479
Страничные файлы	480
Показатель подтверждения и системный лимит подтверждения	486
Показатель подтверждения и размер страничного файла	491
Стеки	493
Пользовательские стеки	493
Стеки ядра	495
DPC-стек	496
Дескрипторы виртуальных адресов	496
Дескрипторы виртуальных адресов процесса	497
Чередование дескрипторов виртуальных адресов	499
NUMA	500
Объекты разделов	501
Рабочие наборы	509
Подкачка по требованию	510
Компонент логической предвыборки	510
Политика размещения	515
Управление рабочими наборами	515

108	Диспетчер рабочего баланса и потока подкачки	520
109	Системные рабочие наборы	522
109	События уведомлений в памяти	523
109	База данных номеров страничных блоков	525
110	Динамика списков страниц	529
110	Приоритеты страниц	537
110	Подсистема записи измененных страниц	540
110	Структуры данных PFN-записи	542
110	Резервирование страничных файлов	547
111	Лимиты физической памяти	551
111	Лимиты памяти клиентских версий Windows	552
111	Сжатие памяти	554
111	Пример сжатия	556
111	Архитектура сжатия	559
111	Секции памяти	563
111	Комбинирование памяти	566
111	Фаза поиска	568
111	Фаза классификации	569
111	Фаза комбинирования страниц	570
111	От закрытой PTE-записи к общей	571
111	Освобождение комбинированных страниц	573
111	Анклав в памяти	576
111	Программный интерфейс	577
111	Инициализация анклавов	578
111	Построение анклава	578
111	Загрузка данных в анклав	580
111	Инициализация анклава	581
111	Упреждающее управление памятью (супервыборка)	582
111	Компоненты	583
111	Трассировка и протоколирование	585
111	Сценарии	586
111	Приоритеты страниц и перебалансировка	587
111	Устойчивое функционирование	590
111	ReadyBoost	591
111	ReadyDrive	593
111	Отражение процессов	594
111	Заключение	596

Глава 6. Подсистема ввода/вывода	597
Компоненты подсистемы ввода/вывода	597
Диспетчер ввода/вывода	600
Стандартная обработка ввода/вывода	601
IRQL и отложенные вызовы процедур	603
IRQL	603
Отложенные вызовы процедур	606
Драйверы устройств	608
Типы драйверов устройств	608
Структура драйвера	615
Объекты драйверов и устройств	617
Открытие устройств	624
Обработка ввода/вывода	629
Типы ввода/вывода	629
Пакеты запросов ввода/вывода	633
Запрос ввода/вывода к одноуровневому драйверу	645
Запросы ввода/вывода к многоуровневым драйверам	656
Независимый от программных потоков ввод/вывод	660
Отмена ввода/вывода	660
Порты завершения ввода/вывода	665
Определение приоритетов ввода/вывода	671
Уведомления о сеансах	678
Программа Driver Verifier	679
Параметры проверки, относящиеся к вводу/выводу	681
Параметры проверки, относящиеся к памяти	682
PnP-диспетчер	687
Уровень поддержки технологии Plug and Play	688
Перечисление устройств	689
Стеки устройств	692
Поддержка Plug and Play драйверами	699
Установка драйвера	701
Общая схема загрузки и установки драйверов	706
Загрузка драйверов	706
Установка драйвера	708
Windows Driver Foundation	709
KMDF	711
UMDF	720

Диспетчер электропитания	724
Режим ожидания с подключением и текущий режим ожидания	728
Работа диспетчера электропитания	729
Участие драйверов в управлении электропитанием	730
Управление электропитанием устройств со стороны драйверов и приложений	734
Инфраструктура управления электропитанием	735
Запросы на изменение режима электропитания	738
Заключение	740
Глава 7. Безопасность	741
Оценка безопасности	741
Критерии оценки заслуживающих доверия компьютерных систем	742
Общие критерии	743
Системные компоненты безопасности	744
Безопасность на основе виртуализации	748
Охранник учетных данных	750
Device Guard	757
Защита объектов	759
Проверки прав доступа	762
Идентификаторы безопасности	766
Виртуальные учетные записи служб	790
Дескрипторы безопасности и управление доступом	795
Динамическое управление доступом	814
AuthZ API	815
Условные ACE-элементы	817
Права доступа и привилегии	818
Права учетной записи	819
Привилегии	820
Суперпривилегии	827
Маркеры доступа процессов и потоков	829
Аудит безопасности	830
Аудит доступа к объекту	831
Глобальная политика аудита	835
Конфигурация расширенной политики аудита	836
AppContainer	838
Общие сведения о приложениях UWP	838

AppContainer	841
Брокеры	864
Вход в систему	866
Инициализация Winlogon	868
Этапы входа пользователя в систему	870
Гарантированная аутентификация	876
Биометрическая среда для аутентификации пользователей	877
Windows Hello	880
Управление учетными записями пользователей и виртуализация	881
Файловая система и виртуализация реестра	882
Повышение привилегий	890
Снижение риска атак	898
Защитные меры уровня процессов	899
CFI	905
Заявления безопасности	920
Идентификация приложений (AppID)	925
AppLocker	927
Политики ограниченного использования программ	932
Защита ядра от модификации	934
PatchGuard	936
HyperGuard	940
Заключение	942