

Оглавление

Глава 1. Обзор внутреннего устройства Windows	11
Процессы	11
Виртуальная память	13
Состояние страниц	16
Системная память	17
Потоки	18
Стеки потоков	19
Системные сервисные функции	21
Общая архитектура системы	23
Дескрипторы и объекты	26
Имена объектов	27
Обращение к существующим объектам	30
Глава 2. Первые шаги в программировании для режима ядра	33
Установка инструментов	33
Создание проекта драйвера	34
Функция DriverEntry и функция выгрузки	36
Установка и загрузка драйвера	38
Простая трассировка	41
Упражнения	44
Итоги	44
Глава 3. Основы программирования ядра	45
Общие рекомендации программирования ядра	45
Необработанные исключения	46
Завершение	47
Возвращаемые значения функций	48
IRQL	48
Использование C++	48

Тестирование и отладка	50
Отладочные и конечные сборки	50
API режима ядра	51
Функции и коды ошибок	52
Строки	53
Динамическое выделение памяти	55
Списки	57
Объект драйвера	59
Объекты устройств	60
Итоги	63
Глава 4. Драйвер: от начала до конца	64
Введение	64
Инициализация драйвера	66
Передача информации драйверу	68
Протокол обмена данными между клиентом и драйвером	69
Создание объекта устройства	70
Клиентский код	73
Функции диспетчеризации Create и Close	75
Функция диспетчеризации DeviceIoControl	76
Установка и тестирование	81
Итоги	83
Глава 5. Отладка	84
Средства отладки для Windows	84
Знакомство с WinDbg	86
Основы отладки пользовательского режима	87
Отладка режима ядра	102
Локальная отладка режима ядра	102
Знакомство с локальной отладкой режима ядра	104
Полная отладка режима ядра	110
Настройка управляемой машины	111
Настройка хоста	113
Основы отладки режима ядра	114
Итоги	118

Глава 6. Механизмы режима ядра	119
Уровень запроса прерывания	119
Повышение и понижение IRQL	123
Приоритеты потоков и IRQL	124
Отложенные вызовы процедур	124
Использование DPC с таймером	127
Асинхронные вызовы процедур	128
Критические секции и защищенные секции	129
Структурированная обработка исключений	130
Использование <code>__try/__except</code>	132
Использование <code>__try/__finally</code>	134
Использование RAII-обертки C++ вместо <code>__try/__finally</code>	135
Фатальный сбой	138
Информация дампа	140
Анализ файла дампа	144
Зависание системы	146
Синхронизация потоков	148
Операции со взаимоблокировкой	148
Объекты диспетчеризации	150
Мьютекс	153
Быстрый мьютекс	156
Семафор	157
Событие	158
Ресурс исполнительной системы	159
Синхронизация при высоких уровнях IRQL	160
Спин-блокировка	162
Рабочие элементы	166
Итоги	168
Глава 7. Пакеты запросов ввода/вывода (IRP)	169
Знакомство с IRP	169
Узлы устройств	170
Последовательность действий при работе с IRP	174
IRP и позиция стека ввода/вывода	176
Просмотр информации об IRP	179
Функции диспетчеризации	181
Завершение запроса	182

Обращение к пользовательским буферам	184
Буферизованный ввод/вывод	185
Прямой ввод/вывод	189
Пользовательские буферы для запросов IRP_MJ_DEVICE_CONTROL	193
Всё вместе: драйвер Zero	195
Использование предварительно откомпилированного заголовка	196
Функция DriverEntry	198
Функция диспетчеризации для чтения	199
Функция диспетчеризации для записи	200
Тестовое приложение	201
Итоги	202
Глава 8. Уведомления потоков и процессов	203
Уведомления процессов	203
Реализация уведомлений процессов	207
Функция DriverEntry	209
Обработка уведомлений о выходе из процессов	211
Обработка уведомлений о создании процессов	213
Передача данных в пользовательский режим	215
Клиент пользовательского режима	217
Уведомления потоков	220
Уведомления о загрузке образов	222
Упражнения	224
Итоги	225
Глава 9. Уведомления объектов и реестра	226
Уведомления объектов	226
Обратный вызов перед операцией	229
Обратный вызов после операции	231
Драйвер Process Protector	232
Регистрация уведомлений объектов	233
Управление защищенными процессами	234
Обратный вызов перед операцией	238
Клиентское приложение	238
Уведомления реестра	241
Обработка уведомлений перед операцией	243