

Аннотации к лекциям

К. Коньков “Основы организации операционных систем Microsoft Windows”

Целью настоящего курса практических занятий является иллюстрация основных положений лекционного курса "Основы операционных систем" на примере 32-разрядной версии операционной системы (ОС) Windows (Windows NT, 2000, XP, Vista), разработанной корпорацией Microsoft. Данный курс не является руководством по системному программированию в среде Windows, но его изучение позволит лучше понять особенности функционирования операционных систем и разрабатывать более эффективные приложения. Автор пытался решить задачу создания основы для проведения практических занятий по ОС Windows в рамках курса по операционным системам.

Эти практические занятия базируются на семестровом курсе "Введение в операционные системы", читаемом автором в МФТИ и могут рассматриваться как учебник для студентов, специализирующихся в области информатики. Задача курса ознакомить читателя на практике с отдельными аспектами функционирования операционных систем. Курс состоит из 15 глав. Он имеет традиционное построение и содержит следующие разделы: введение, управление процессами и потоками, организация памяти, структура файловой системы и безопасность. В курсе много иллюстраций. Практические занятия заключаются в разработке небольших программ, иллюстрирующих отдельные аспекты реализации ОС Windows, а также использовании для этих целей различных инструментальных средств. Хотя курс содержит необходимый минимум теоретических сведений, для его успешного освоения целесообразно прослушать курс лекций по операционным системам или ознакомиться с содержанием одной или нескольких монографий по данному предмету.

Лекция 1

Создание ОС Windows. Структура ОС Windows

В лекции говорится о наиболее важных этапах создания ОС Windows наряду с эволюцией операционных систем, структуре системы, а также вводятся некоторые ключевые понятия. Проанализирована ее миграция от микроядерной архитектуры в сторону монолитного дизайна. Описаны возможности и основные структурные компоненты системы. Рассмотрена подсистема Win32, которая объединяет ряд модулей режима ядра и режима пользователя и является базой для разработки приложений

Лекция 2

Разработка Win32 приложений. Инструментальные средства изучения системы

Рассмотрены вопросы, важные с точки зрения практического освоения ОС Windows и разработки Win32-приложений. Приведено краткое описание справочной системы MSDN, средств разработки и отладки. Проанализированы основные типы используемых данных, форматы хранения текстовых строк и способы корректной обработки ошибок. Описаны разнообразные инструментальные средства, которые являются дополнительными источниками сведений о системе

Лекция 3

Базовые понятия ОС Windows

В лекции описаны прерывания, системные вызовы и исключительные ситуации, которые являются фундаментальными механизмами операционных систем, и проанализированы особенности их реализации в ОС Windows. Обработка всех типов событий осуществляется единым образом и связана с сохранением/восстановлением состояния и эффективным поиском программы обработчика по системным таблицам. Важную роль для правильной организации имеет иерархия событий, реализованная в виде набора IRQL-приоритетов

Лекция 4

Объекты. Менеджер объектов. Реестр

В лекции описаны особенности функционирования менеджера объектов — одного из ключевых компонентов ОС Windows. Объекты активно используются для организации доступа к ресурсам, которые нужно защищать, именовать, разделять и т. д. Среди совокупности объектов выделены объекты ядра. Описаны дескрипторы объектов, отвечающие за связь объекта с приложением. Рассмотрены вопросы именования объектов и связь пространства имен объектов с другими пространствами имен. Для управления большим организована специальная централизованная база данных — реестр

Лекция 5

Реализация процессов и потоков

Поток представляет собой набор исполняющихся команд для текущего момента исполнения. С одним или несколькими потоками ассоциирован набор ресурсов, которые объединены в рамках процесса. Для описания процесса в системе поддерживается связанная совокупность структур, главной из которых является структура EPROCESS. В свою очередь, структура ETHREAD и связанные с ней структуры необходимы для реализации потоков. В лекции проанализированы функции CreateProcess и CreateThread и этапы создания процессов и потоков. Важными характеристиками потока являются его контекст и состояние. Наблюдение за состоянием потоков предлагается осуществить при помощи инструментальных средств системы

Лекция 6

Планирование потоков

Процессорное время — ограниченный ресурс, поэтому планирование — важная и критичная для производительности операция. Один из ключевых вопросов — выбор момента для запуска процедуры планирования. В системе реализовано приоритетное вытесняющее планирование с динамическими приоритетами. Для удобства пользователя и мобильности программ поддерживается слой абстрагирования приоритетов. Механизмы привязки позволяют организовать эффективное исполнение программ в многопроцессорных системах

Лекция 7

Межпроцессный обмен

К основным способам межпроцессного обмена традиционно относят каналы и разделяемую память, для организации которых используют разделяемые ресурсы. Анонимные каналы поддерживают потоковую модель, в рамках которой данные представляют собой неструктурированную последовательность байтов. Именованные каналы, поддерживающие как потоковую модель, так и модель, ориентированную на сообщения, обеспечивают обмен данными не только в изолированной вычислительной среде, но и в локальной сети

Лекция 8

Синхронизация потоков

Проблема недетерминизма является одной из ключевых в параллельных вычислительных средах. Традиционное решение — организация взаимного исключения. Для синхронизации с применением переменной-замка используются Interlocked-функции, поддерживающие атомарность некоторой последовательности операций. Взаимоисключение потоков одного процесса легче всего организовать с помощью примитива CriticalSection. Для более сложных сценариев рекомендуется применять объекты ядра, в частности, семафоры, мьютексы и события. Рассмотрена проблема синхронизации в ядре, основным решением которой можно считать установку и освобождение спин-блокировок

Лекция 9

Введение. Виртуальное адресное пространство процесса

Система управления памятью является одной из наиболее важных в составе ОС. Традиционная схема предполагает связывание виртуального и физического адресов на стадии исполнения программы. Для управления виртуальным адресным пространством в нем принято организовывать сегменты (регионы), для описания которых используются структуры данных VAD (Virtual Address Descriptors). Для создания региона и передачи ему физической памяти можно использовать функцию VirtualAlloc. Описана техника использования таких регионов, как куча процесса, стек потока и регион файла, отображаемого в память

Лекция 10

Функционирование менеджера памяти

Рассмотрены особенности поддержки виртуальной памяти. Базовой операцией менеджера памяти является трансляция виртуального адреса в физической с помощью таблицы страниц и ассоциативной (TLB) памяти. В ряде случаев, для реализации разделяемой памяти, интеграции с системой ввода/вывода и др., применяется прототипная таблица страниц, которая является промежуточным звеном между обычной таблицей страниц и физической памятью. Для описания страниц физической памяти поддерживается база данных PFN (Page Frame Number). Локализацию страниц памяти, контроль процессом памяти другого процесса и технику копирования при записи можно отнести к интересным особенностям системы управления памятью ОС Windows

Лекция 11

Интерфейс файловой системы

В настоящей лекции рассматриваются основные функции и интерфейс файловой системы NTFS. Файловая система решает задачи именования и типизации файлов, организации доступа к файлам, защиты, поиска файлов и ряд других. В системе на каждом разделе диска поддерживается иерархическая система каталогов. Для эффективного доступа к файлам могут быть организованы асинхронные чтение и запись

Лекция 12

Реализация файловой системы. Файловая система NTFS

Настоящая лекция описывает отдельные аспекты реализации файловой системы NTFS. Главная функция файловой системы — связь символического имени с блоками диска — реализована за счет поддержки списка блоков в записи о файле в главной файловой таблице MFT. Для быстрого поиска файла по имени каталог может быть организован в виде B+ дерева. Проблемы монтирования дисков и связывания файлов решаются с помощью точек повторного анализа. Производительность файловой системы обеспечивается менеджером кэша, а также путем оптимального размещения информации на диске. Для восстановления системы после отказа питания ведется журнал файловых операций с метаданными. Поддержка нескольких файловых систем в ОС Windows обеспечивается оригинальной структурой подсистемы ввода/вывода, в рамках которой для каждой файловой системы имеется соответствующий драйвер

Лекция 13

Система управления доступом

Подсистема защиты данных является одной из наиболее важных. В центре системы безопасности ОС Windows находится система контроля доступа. Реализованные модели дискреционного и ролевого доступа являются удобными и широко распространены, однако не позволяют формально обосновать безопасность приложений в ряде случаев, представляющих практический интерес. С каждым процессом или потоком, то есть активным компонентом (субъектом), связан маркер доступа, а у каждого защищаемого объекта (например, файла) имеется дескриптор защиты. Проверка прав доступа обычно осуществляется в момент открытия объекта и заключается в сопоставлении прав субъекта списку прав доступа, который хранится в составе дескриптора защиты объекта

Лекция 14

Структура системы защиты. Привилегии

Описана структура менеджера безопасности ОС Windows. Система защиты данных должна удовлетворять требованиям, сформулированным в ряде нормативных документов, которые определяют политику безопасности. Далее в лекции описаны возможности настройки привилегий учетной записи. Поддержка модели ролевого доступа связана с задачами перечисления, добавления и отзыва привилегий пользователя и отключения привилегий в маркере доступа субъекта

Лекция 15

Отдельные аспекты безопасности Windows

В лекции рассмотрены вопросы аутентификации пользователя, системного аудита, защиты от повторного использования объектов и внешнего навязывания, а также возможности тонкой настройки контекста пользователя