

Мартемьянов Ю.Ф., Яковлев Ал.В.,
Яковлев Ан.В.

Операционные системы.

Концепции построения и обеспечения безопасности

*Допущено УМО по университетскому
политехническому образованию в качестве
учебного пособия для студентов высших учебных
заведений, обучающихся по направлению 230400 –
«Информационные системы и технологии»*

Москва
Горячая линия – Телеком
2011

УДК 004.732.056(075.8)

ББК 32.973.2-018.2я73

М29

Рецензенты: доктор техн. наук, профессор Ю. Ю. Громов; канд. техн. наук Д. Б. Петленко

Мартемьянов Ю. Ф., Яковлев Ал. В., Яковлев Ан. В.

М29 Операционные системы. Концепции построения и обеспечения безопасности. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2011. – 332 с.: ил.

ISBN 978-5-9912-0128-5.

В учебном пособии рассмотрены базовые концепции, методы и средства, составляющие архитектуру современных операционных систем (ОС), а также способы и механизмы реализации принципов защиты информации в существующих операционных системах. Изложен теоретический материал о концепциях и принципах построения операционных систем и их компонентах. Рассмотрены методы и алгоритмы управления задачами, процессами, памятью и внешними устройствами. Уделено внимание синхронизации параллельных процессов и методам борьбы с тупиками. Описаны архитектурные решения наиболее распространенных операционных систем семейства Windows, Unix, МСВС, приведены требования к аппаратному обеспечению вычислительных систем для инсталляции рассматриваемых операционных систем. Рассмотрены способы и механизмы защиты информации широко распространенных операционных систем и их дефекты, приводятся основные понятия и положения защиты информации, угрозы безопасности информации. Уделено внимание уровням и моделям безопасности основных операционных систем, а также системам защиты программного обеспечения, протоколированию и аудиту.

Для студентов, обучающихся по направлению 230400 – «Информационные системы и технологии», будет полезно студентам направлений подготовки «Информационная безопасность» и «Информатика и вычислительная техника» и специалистам в области информационных технологий.

ББК 32.973.2-018.2я73

Адрес издательства в Интернет WWW.TECHBOOK.RU

ISBN 978-5-9912-0128-5

© Ю. Ф. Мартемьянов,
Ал. В. Яковлев, Ан. В. Яковлев, 2011

© Оформление издательства
Горячая линия–Телеком, 2011

Введение

Эффективность применения средств вычислительной техники (СВТ) определяется техническим совершенством аппаратной части электронных вычислительных машин (ЭВМ) и вычислительных систем (ВС), качеством программного обеспечения (ПО) и квалификацией персонала, эксплуатирующего СВТ. Вместе с тем не следует забывать, что даже при идеальном программном обеспечении и персонале высочайшей квалификации работа вычислительной системы может быть блокирована или серьезно нарушена вследствие умышленного или случайного разрушения программных кодов или информационных массивов. Основой функционирования современных информационно-вычислительных систем (ИВС) и локальных ЭВМ являются операционные системы (ОС), на которые возложены задачи управления развитием всех внутренних и внешних процессов обработки информации. Поэтому уровень информационной защищенности ИВС напрямую зависит от уровня безопасности ОС.

Дисциплина, изучающая операционные системы, является одной из основных в подготовке бакалавров, дипломированных специалистов и магистров по специальности 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем». Целью дисциплины является изучение базовых концепций, методов и средств, составляющих архитектуру современных ОС, а также способы и механизмы реализации принципов защиты информации в существующих операционных системах.

Пособие состоит из трех разделов.

Первый раздел «Архитектура современных операционных систем» содержит изложение теоретического материала о концепциях и принципах построения операционных систем и их компонентах. Рассмотрены методы и алгоритмы управления задачами, процессами, памятью и внешними устройствами. Уделено внимание синхронизации параллельных процессов и методам борьбы с тупиками.

Во втором разделе «Современные операционные системы» проведен анализ построения и функционирования основных операционных систем, использующихся в современных автоматизированных системах. Учебный материал представлен в систематизированном виде для каждой операционной системы.

Третий раздел «Защита информации в современных ОС» посвящен описанию способов и механизмов защиты информации широко распространенных в настоящее время операционных систем. Приведены основные понятия и положения защиты информации, дано описание угроз безопасности информации в информационно-вычислительных системах, рассмотрены стандарты и спецификации в области информационной безопасности. Внимание уделено уровням и моделям безопасности основных операционных систем, а также системам защиты программного обеспечения, протоколированию и аудиту.

При подготовке пособия использованы сведения из источников, перечисленных в списке литературы, приведенном в конце пособия.

Пособие предназначено для студентов, аспирантов и читателей, интересующихся современными проблемами построения и безопасности операционных систем.

Оглавление

Введение	3
Р а з д е л 1. Архитектура операционных систем	
Тема 1. Принципы построения операционных систем	5
1.1. Понятие об архитектуре аппаратных средств	5
1.1.1. Классификация программных средств	6
1.1.2. Место и функции системного программного обеспечения	7
1.2. Принципы работы вычислительной системы	9
1.3. Режимы работы операционных систем	10
1.3.1. Режимы обработки данных	10
1.3.2. Режимы и дисциплины обслуживания	12
1.4. Классификация операционных систем	14
1.4.1. Особенности алгоритмов управления ресурсами	14
1.4.2. Особенности аппаратных платформ	16
1.4.3. Особенности областей использования	18
1.4.4. Особенности методов построения	20
1.5. Основные принципы построения операционных систем ...	21
1.6. Пользовательский интерфейс операционных систем	23
1.6.1. Классификация интерфейсов	23
1.6.2. Пакетная технология	24
1.6.3. Технология командной строки	25
1.6.4. Графический интерфейс	25
1.6.5. Речевая технология	28
1.6.6. Биометрическая технология	28
1.6.7. Семантический интерфейс	29
<i>Контрольные вопросы к теме 1</i>	30

Тема 2. Концептуальные основы операционных систем..	31
2.1. Концепция процесса	31
2.2. Концепция ресурса	33
2.3. Концепция виртуальности	35
2.4. Концепция прерывания	36
2.5. Понятие ядра и микроядра ОС	40
2.5.1. Понятие ядра ОС	40
2.5.2. Понятие микроядра ОС	40
<i>Контрольные вопросы к теме 2.....</i>	<i>41</i>
Тема 3. Управление задачами	42
3.1. Организация управления задачами	42
3.2. Средства и механизмы управления задачами	43
3.2.1. Средства управления задачами на уровне внешнего планирования	43
3.2.2. Средства управления задачами на уровне внутреннего планирования	45
3.3. Алгоритмы управления задачами	47
3.3.1. Алгоритмы управления задачами на уровне внешнего планирования	47
3.3.2. Алгоритмы управления задачами на уровне внутреннего планирования	49
3.4. Взаимосвязанные и конкурирующие задачи	58
3.4.1. Средства управления ресурсами	58
3.4.2. Механизмы синхронизации процессов	60
3.4.3. Алгоритмы управления ресурсами	68
<i>Контрольные вопросы к теме 3.....</i>	<i>71</i>
Тема 4. Управление памятью в операционных системах.	72
4.1. Понятие об организации и управлении физической памятью	72
4.2. Методы связного распределения основной памяти (без использования дискового пространства)	75
4.2.1. Связное распределение памяти для одного пользователя	75
4.2.2. Связное распределение памяти при мультипрограммной обработке	76
4.2.3. Стратегии размещения информации в памяти	80
4.3. Организация виртуальной памяти (с использованием дискового пространства)	81

4.3.1. Основные концепции виртуальной памяти	81
4.3.2. Схема прямого отображения адресов	83
4.3.3. Отображения адресов при страничной организации виртуальной памяти	84
4.3.4. Отображения адресов при сегментной организации виртуальной памяти	84
4.3.5. Отображения адресов при странично-сегментной организации виртуальной памяти	85
4.4. Управление виртуальной памятью.....	86
4.4.1. Стратегии управления виртуальной памятью	86
4.4.2. Стратегии вталкивания (подкачки)	87
4.4.3. Стратегии размещения	88
4.4.4. Стратегии выталкивания	88
<i>Контрольные вопросы к теме 4</i>	90
Тема 5. Управление файлами и вводом-выводом в ОС...	91
5.1. Методы организации данных в операционных системах ..	91
5.2. Методы доступа к данным	96
5.3. Объединение записей в блоки и буферизация.....	98
5.4. Управление файлами	100
5.4.1. Понятие файлового способа хранения данных и файловой системы	100
5.4.2. Организация файлов	102
5.4.3. Организация хранения файлов	105
5.4.4. Операции над файлами	106
5.4.5. Файловая система	108
5.5. Система ввода-вывода	112
5.5.1. Физическая организация устройств ввода-вывода	114
5.5.2. Организация программного обеспечения ввода-вывода ..	115
<i>Контрольные вопросы к теме 5</i>	120
Р а з д е л 2. Современные операционные системы	
Тема 6. Операционные системы семейства Windows.....	121
6.1. Архитектура ОС семейства Windows.....	121
6.2. Управление задачами	130
6.2.1. Организация многозадачности.....	130
6.2.2. Процессы и нити в Windows.....	135

6.2.3. Алгоритм планирования процессов и нитей	137
6.3. Распределение оперативной памяти в ОС Windows	140
6.3.1. Распределение оперативной памяти в ОС Windows 9х ..	140
6.3.2. Распределение оперативной памяти в ОС Windows NT .	145
6.4. Управление вводом-выводом	149
6.5. Файловые системы Windows NT	152
6.6. Операционная система Windows XP	157
6.6.1. Общие сведения о Windows XP	157
6.6.2. Системные требования операционной системы Windows XP	161
6.7. Операционная система Windows Vista	163
6.7.1. Общие сведения о Windows Vista	163
6.7.2. Аппаратные требования и новые возможности Windows Vista	165
6.8. Операционная система Windows 7	168
6.9. Интерфейс программирования прикладных программ Win32	171
6.9.1. Интерфейс прикладного программирования	171
6.9.2. Реализация функций API на уровне ОС	173
6.9.3. Реализация функций API на уровне системы программи- рования	174
6.9.4. Реализация функций API с помощью внешних библиотек	175
6.9.5. Платформенно-независимый интерфейс POSIX	177
<i>Контрольные вопросы к теме 6.</i>	179
Тема 7. Семейство операционных систем UNIX	180
7.1. Особенности архитектуры операционных систем UNIX...	180
7.2. Управление процессами	184
7.3. Управление памятью	188
7.4. Управление вводом/выводом	194
7.5. Операционная система Linux	199
<i>Контрольные вопросы к теме 7.</i>	203
Тема 8. Операционная система МСВС 3.0	204
8.1. Архитектура операционной системы МСВС 3.0	204
8.2. Архитектура процессов и нитей в ОС МСВС 3.0	213
8.2.1. Архитектура процессов в ОС МСВС 3.0	213
8.2.2. Архитектура нитей в ОС МСВС 3.0	216

8.3. Архитектура файловой системы МСВС 3.0	219
<i>Контрольные вопросы к теме 8.</i>	222

Р а з д е л 3. Защита информации в современных ОС

Тема 9. Основные понятия и положения защиты информации в информационно-вычислительных системах	223
---	-----

9.1. Предмет защиты информации	224
9.2. Объект защиты информации	225
9.2.1. Основные положения безопасности информационных систем	225
9.2.2. Основные принципы обеспечения информационной безопасности в АС	226
<i>Контрольные вопросы к теме 9.</i>	229

Тема 10. Угрозы безопасности информации в информационно-вычислительных системах	230
--	-----

10.1. Анализ угроз информационной безопасности	230
10.2. Методы обеспечения информационной безопасности	240
10.2.1. Структуризация методов обеспечения информационной безопасности	240
10.2.2. Классификация злоумышленников	244
10.2.3. Основные направления и методы реализации угроз ИБ	244
<i>Контрольные вопросы к теме 10</i>	244

Тема 11. Программно-технический уровень информационной безопасности	245
--	-----

11.1. Основные понятия программно-технического уровня информационной безопасности	245
11.2. Требования к защите компьютерной информации	251
11.2.1. Классификация требований к системам защиты	243
11.2.2. Формализованные требования к защите информации от НСД. Общие подходы к построению систем защиты компьютерной информации	254
11.2.3. Различия требований и основополагающих механизмов защиты от НСД	264
<i>Контрольные вопросы к теме 11</i>	266

Тема 12. Модели безопасности основных операционных систем	267
--	-----

12.1. Механизмы защиты операционных систем	268
--	-----

12.2. Анализ защищенности современных операционных систем	273
12.2.1. Анализ выполнения современными ОС формализованных требований к защите информации от НСД.....	273
12.2.2. Основные встроенные механизмы защиты ОС и их недостатки	275
12.2.3. Анализ существующей статистики угроз для современных универсальных ОС. Семейства ОС и общая статистика угроз.....	281
12.2.4. Обзор и статистика методов, лежащих в основе атак на современные ОС. Классификация методов и их сравнительная статистика	283
12.3. Система безопасности ОС Windows NT	286
12.4. Защита в операционной системе Windows Vista.....	294
12.5. Защита в операционной системе UNIX.....	300
<i>Контрольные вопросы к теме 12</i>	306
Тема 13. Системы защиты программного обеспечения...	307
13.1. Классификация систем защиты программного обеспечения	307
13.2. Достоинства и недостатки основных систем защиты.....	310
13.2.1. Упаковщики/шифраторы.....	310
13.2.2. Системы защиты от несанкционированного копирования	311
13.2.3. Системы защиты от несанкционированного доступа....	312
13.3. Показатели эффективности систем защиты	316
<i>Контрольные вопросы к теме 13</i>	318
Тема 14. Протоколирование и аудит	319
14.1. Основные понятия	319
14.2. Активный аудит	321
14.3. Функциональные компоненты и архитектура	323
<i>Контрольные вопросы к теме 14</i>	324
Литература	325