

Оглавление

Предисловие к третьему изданию	3
1. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	7
1.1. Элементы теории информационной безопасности в рамках субъект-сущностного подхода	7
1.1.1. Основные научные направления теории информационной безопасности	7
1.1.2. Сущность, субъект, доступ, информационный поток	9
1.1.3. Классическая классификация угроз безопасности информации	10
1.1.4. Виды информационных потоков	11
1.1.5. Виды политик управления доступом	14
1.1.6. Утечка права доступа и нарушение безопасности КС	18
1.2. Математические основы моделей безопасности	21
1.2.1. Основные понятия	21
1.2.2. Понятие автомата	21
1.2.3. Элементы теории графов	23
1.2.4. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы	24
1.2.5. Модель решётки	25
1.3. Основные виды формальных моделей безопасности	27
1.4. Проблема адекватности реализации модели безопасности в реальной компьютерной системе	27
1.5. Преподавание основных понятий, используемых при описании моделей безопасности компьютерных систем	30
1.5.1. Изучение основных понятий теории информационной безопасности	30
1.5.2. Преподавание модели решётки	32
1.6. Контрольные вопросы и задачи	34
2. Модели компьютерных систем с дискреционным управлением доступом	36
2.1. Модель матрицы доступов Харрисона–Руззо–Ульмана	36
2.1.1. Описание модели	36
2.1.2. Анализ безопасности систем ХРУ	38
2.1.3. Модель типизированной матрицы доступов	45
2.2. Модель распространения прав доступа Take-Grant	55

2.2.1. Основные положения классической модели Take-Grant	55
2.2.2. Расширенная модель Take-Grant	66
2.2.3. Представление систем Take-Grant системами ХРУ	75
2.3. Преподавание моделей компьютерных систем с дискреционным управлением доступом	77
2.3.1. Преподавание базовой модели Take-Grant	77
2.3.2. Преподавание расширенной модели Take-Grant	83
2.3.3. Преподавание модели Харрисона-Руззо-Ульмана	87
2.3.4. Преподавание модели типизированной матрицы до- ступов	90
2.4. Контрольные вопросы и задачи	96
3. Модели компьютерных систем с мандатным управ- лением доступом	99
3.1. Модель Белла-ЛаПадулы	99
3.1.1. Классическая модель Белла-ЛаПадулы	99
3.1.2. Пример некорректного определения свойств безопас- ности	104
3.1.3. Политика low-watermark в модели Белла-ЛаПадулы	106
3.1.4. Примеры реализации запрещённых информационных потоков	108
3.1.5. Безопасность переходов	111
3.1.6. Модель мандатного контроля целостности информа- ции Виба	114
3.2. Модель систем военных сообщений	117
3.2.1. Общие положения и основные понятия	117
3.2.2. Неформальное описание модели СВС	119
3.2.3. Формальное описание модели СВС	120
3.3. Преподавание моделей компьютерных систем с мандат- ным управлением доступом	127
3.3.1. Преподавание модели Белла-ЛаПадулы	127
3.3.2. Преподавание модели СВС	134
3.4. Контрольные вопросы и задачи	138
4. Модели компьютерных систем с ролевым управле- нием доступом	140
4.1. Базовая модель ролевого управления доступом	140
4.2. Модель администрирования ролевого управления до- ступом	143
4.2.1. Основные положения	143
4.2.2. Администрирование множеств авторизованных ролей пользователей	145
4.2.3. Администрирование множеств прав доступа ролей	148

4.2.4. Администрирование иерархии ролей	149
4.3. Модель мандатного ролевого управления доступом....	153
4.3.1. Защита от угрозы конфиденциальности информации	153
4.3.2. Защита от угроз конфиденциальности и целостности информации	156
4.4. Базовая модель атрибутивного управления доступом ..	159
4.5. Преподавание моделей компьютерных систем с ролевым управлением доступом	162
4.5.1. Преподавание базовой модели семейства RBAC	162
4.5.2. Преподавание модели администрирования ролевого управления доступом	164
4.5.3. Преподавание модели мандатного ролевого управления доступом	165
4.5.4. Преподавание базовой модели атрибутивного управления доступом	168
4.6. Контрольные вопросы и задачи	169
5. Модели безопасности информационных потоков	170
5.1. Субъектно-ориентированная модель изолированной программной среды	170
5.2. Автоматная модель безопасности информационных потоков	177
5.3. Вероятностная модель безопасности информационных потоков	180
5.4. Программная модель контроля информационных потоков	183
5.5. Модели децентрализованного контроля информационных потоков	187
5.6. Преподавание моделей изолированной программной среды и безопасности информационных потоков	191
5.6.1. Преподавание субъектно-ориентированной модели изолированной программной среды	191
5.6.2. Преподавание автоматной модели безопасности информационных потоков	193
5.6.3. Преподавание вероятностной модели безопасности информационных потоков	194
5.6.4. Преподавание программной модели безопасности информационных потоков	195
5.6.5. Преподавание моделей децентрализованного контроля информационных потоков	196
5.7. Контрольные вопросы и задачи	197
6. Модели безопасности управления доступом и информационными потоками (ДП-модели)	199
6.1. Базовая ДП-модель	199

6.1.1. Элементы состояния и правила преобразования состояний системы в рамках базовой ДП-модели	199
6.1.2. Монотонные правила преобразования состояний	211
6.1.3. Условия передачи прав доступа	212
6.1.4. Условия реализации информационных потоков	215
6.2. ДП-модели без кооперации доверенных и недоверенных субъектов	218
6.2.1. ДП-модель с функционально ассоциированными с субъектами сущностями	218
6.2.2. ДП-модель с функционально или параметрически ассоциированными с субъектами сущностями	226
6.3. Иерархическое представление мандатной сущностноролевой ДП-модели управления доступом и информационными потоками в операционных системах семейства Linux	232
6.3.1. Переход от «монолитного» к иерархическому представлению модели	232
6.3.2. Базовый уровень модели	235
6.3.3. Уровень мандатного контроля целостности	284
6.4. Преподавание ДП-моделей	310
6.4.1. Преподавание ДП-моделей базового семейства	310
6.4.2. Преподавание МРОСЛ ДП-модели	313
6.5. Контрольные вопросы и задачи	315
Приложение. Примеры решения задач на практических занятиях	318
Практическое занятие № 1. Модель решётки	318
Практическое занятие № 2. Модели ХРУ и ТМД	319
Практическое занятие № 3. Классическая модель Take-Grant	322
Практическое занятие № 4. Расширенная модель Take-Grant	324
Практическое занятие № 5. Классическая модель Белла-ЛаПадулы и её интерпретации	327
Практическое занятие № 6. Модель СВС	331
Практическое занятие № 7. Модели ролевого управления доступом	333
Практическое занятие № 8. Модели безопасности информационных потоков	335
Практическое занятие № 9. Дискреционные ДП-модели	337
Практическое занятие № 10. МРОСЛ ДП-модель	338
Литература	342