

Оглавление

Предисловие	3
Глава 1. Основные термины и определения, используемые при описании формальных моделей управления доступом	8
1.1. Элементы теории информационной безопасности в рамках субъект-сущностного подхода	8
1.1.1. Основные научные направления теории информационной безопасности	8
1.1.2. Сущность, субъект, доступ, информационный поток	10
1.1.3. Угрозы безопасности информации. Виды политик управления доступом	15
1.1.4. Утечка права доступа и нарушение безопасности системы	22
1.2. Математические основы формальных моделей управления доступом	25
1.2.1. Основные понятия	25
1.2.2. Понятие абстрактного автомата	25
1.2.3. Элементы теории графов	27
1.2.4. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы	28
1.2.5. Модель решетки	29
1.3. Основные виды формальных моделей управления доступом	31
1.4. Проблема адекватности реализации формальной модели в реальной системе	33
1.5. Преподавание основных понятий, используемых при описании формальных моделей управления доступом	34
1.5.1. Изучение основных понятий, используемых в формальных моделях	34

1.5.2. Преподавание модели решетки	37
1.6. Контрольные вопросы и задачи	39
Глава 2. Формальные модели дискреционного управления доступом	40
2.1. Модель матрицы доступов Харрисона–Руззо–Ульмана	40
2.1.1. Описание модели	40
2.1.2. Анализ безопасности систем ХРУ	42
2.1.3. Модель типизированной матрицы доступов	50
2.2. Модель распространения прав доступа Take-Grant ...	59
2.2.1. Основные положения классической модели Take-Grant	59
2.2.2. Расширенная модель Take-Grant	71
2.2.3. Представление систем Take-Grant системами ХРУ	81
2.3. Преподавание формальных моделей дискреционного управления доступом	83
2.3.1. Преподавание базовой модели Take-Grant	83
2.3.2. Преподавание расширенной модели Take-Grant ..	89
2.3.3. Преподавание модели Харрисона–Руззо–Ульмана ..	93
2.3.4. Преподавание модели типизированной матрицы доступов	97
2.4. Контрольные вопросы и задачи	103
Глава 3. Формальные модели мандатного управления доступом и мандатного контроля целостности	106
3.1. Модель Белла–ЛаПадулы	106
3.1.1. Классическая модель Белла–ЛаПадулы	106
3.1.2. Пример некорректного определения свойств безопасности	112
3.1.3. Политика «low-water mark» в модели Белла–ЛаПадулы	113
3.1.4. Примеры реализации запрещенных информационных потоков	115
3.1.5. Безопасность переходов	119
3.1.6. Модель мандатного контроля целостности Биба ..	122
3.2. Модель систем военных сообщений	125
3.2.1. Общие положения и основные понятия	125

3.2.2. Неформальное описание модели СВС.....	127
3.2.3. Формальное описание модели СВС	128
3.3. Преподавание формальных моделей мандатного управления доступом и мандатного контроля целост- ности	135
3.3.1. Преподавание модели Белла-ЛаПадулы	135
3.3.2. Преподавание модели СВС.....	143
3.4. Контрольные вопросы и задачи	147
Глава 4. Формальные модели ролевого управления доступом	149
4.1. Базовая модель ролевого управления доступом.....	149
4.2. Модель администрирования ролевого управления до- ступом	152
4.2.1. Основные положения	152
4.2.2. Администрирование множеств авторизованных ролей пользователей.....	154
4.2.3. Администрирование множеств прав доступа ролей.....	158
4.2.4. Администрирование иерархии ролей.....	159
4.3. Модель мандатного ролевого управления доступом..	163
4.3.1. Защита от угрозы конфиденциальности инфор- мации	163
4.3.2. Защита от угроз конфиденциальности и целост- ности информации.....	166
4.4. Базовая модель атрибутивного управления доступом	169
4.5. Преподавание формальных моделей ролевого управ- ления доступом	172
4.5.1. Преподавание базовой модели семейства RBAC	172
4.5.2. Преподавание модели администрирования роле- вого управления доступом.....	174
4.5.3. Преподавание модели мандатного ролевого управления доступом.....	176
4.5.4. Преподавание базовой модели атрибутивного управления доступом.....	178
4.6. Контрольные вопросы и задачи	179
Глава 5. Модели безопасности информационных по- токов	181
5.1. Субъектно-ориентированная модель изолированной программной среды.....	181

5.2. Автоматная модель безопасности информационных потоков	189
5.3. Вероятностная модель безопасности информационных потоков	191
5.4. Программная модель контроля информационных потоков	195
5.5. Модели децентрализованного контроля информационных потоков	199
5.6. Преподавание моделей изолированной программной среды и безопасности информационных потоков	202
5.6.1. Преподавание субъектно-ориентированной модели изолированной программной среды	202
5.6.2. Преподавание автоматной модели безопасности информационных потоков	205
5.6.3. Преподавание вероятностной модели безопасности информационных потоков	206
5.6.4. Преподавание программной модели безопасности информационных потоков	207
5.6.5. Преподавание моделей децентрализованного контроля информационных потоков	208
5.7. Контрольные вопросы и задачи	210
Глава 6. Модели безопасности управления доступом и информационными потоками (ДП-модели)	212
6.1. Базовая ДП-модель	212
6.1.1. Элементы состояния и правила преобразования состояний системы в рамках базовой ДП-модели	212
6.1.2. Монотонные правила преобразования состояний	224
6.1.3. Условия передачи прав доступа	226
6.1.4. Условия реализации информационных потоков	229
6.2. ДП-модели без кооперации доверенных и недоверенных субъектов	232
6.2.1. ДП-модель с функционально ассоциированными с субъектами сущностями	232
6.2.2. ДП-модель с функционально или параметрически ассоциированными с субъектами сущностями	241
6.3. Иерархическое представление мандатной сущностнорелевой ДП-модели управления доступом и информационными потоками в операционных системах семейства Linux	247

6.3.1. Переход от «монолитного» к иерархическому представлению модели	247
6.3.2. Базовый уровень модели	250
6.3.3. Уровень мандатного контроля целостности.....	308
6.4. Преподавание ДП-моделей.....	338
6.4.1. Преподавание ДП-моделей базового семейства .	338
6.4.2. Преподавание МРОСЛ ДП-модели.....	342
6.5. Контрольные вопросы и задачи	345
Глава 7. Семейство национальных стандартов ГОСТ Р 59453 «Защита информации. Формальная модель управления доступом».....	348
7.1. Состав семейства национальных стандартов	348
7.2. Основные критерии, которым по ГОСТ Р 59453.1-2021 должны соответствовать описания формальных моделей управления доступом	350
7.3. Основные рекомендации ГОСТ Р 59453.3-2025 по разработке формальных моделей управления доступом.	356
7.3.1. Рекомендуемые этапы разработки и описания формальной модели	356
7.3.2. Выбор технологий, инструментальных средств и практических приемов разработки формальной модели.....	358
7.3.3. Рекомендации по описанию формальной модели	362
7.3.4. Рекомендации по описанию и доказательству выполнения условий безопасности	372
7.4. Преподавание семейства национальных стандартов ГОСТ Р 59453.....	376
7.5. Контрольные вопросы и задачи	379
Приложение. Примеры решения задач на практических занятиях	382
Практическое занятие № 1. Модель решетки.....	382
Практическое занятие № 2. Модели ХРУ и ТМД	383
Практическое занятие № 3. Классическая модель Take-Grant.....	386
Практическое занятие № 4. Расширенная модель Take-Grant.....	388
Практическое занятие № 5. Классическая модель Белла-ЛаПадулы и ее интерпретации	390

Практическое занятие № 6. Модель СВС.....	394
Практическое занятие № 7. Модели ролевого управления доступом	396
Практическое занятие № 8. Модели безопасности информационных потоков.....	398
Практическое занятие № 9. Дискреционные ДП-модели.....	399
Практическое занятие № 10. МРОСЛ ДП-модель....	401
Практическое занятие № 11. Семейство национальных стандартов ГОСТ Р 59453	403
Литература	409