

УДК 004.056
ББК 32.973.2-018.2я73
Д25

Рецензенты: зав. кафедрой защиты информации и криптографии Томского государственного университета, доктор техн. наук, профессор *Г. П. Агibalов*; зам. зав. кафедрой «Стратегические информационные исследования» МИФИ, канд. техн. наук, доцент *В. А. Петро*к; зам. зав. кафедрой «Информационная безопасность банковских систем» МИФИ, канд. техн. наук, доцент *А. И. Толстой*; руководитель направления по работе с образовательными учреждениями ЗАО «Лаборатория Касперского» *С. И. Ефимова*.

Девянин П. Н.

Д25 Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – 2-е изд., испр. и доп. – М.: Горячая линия–Телеком, 2013. – 338 с.: ил.

ISBN 978-5-9912-0328-9.

Рассмотрены с полными доказательствами положения основных моделей безопасности компьютерных систем: дискреционного, мандатного, ролевого управления доступом, безопасности информационных потоков и изолированной программной среды. Описан используемый в рассматриваемых моделях математический аппарат. Классические модели дополнены ориентированными на применение в современных компьютерных системах моделями безопасности логического управления доступом и информационными потоками (ДП-моделями). Приведены примеры решения задач на практических занятиях. Изложены методические рекомендации по организации изучения моделей безопасности компьютерных систем.

Во втором издании пособия (кроме исправления неточностей и опечаток) включены нескольких дополнительных примеров решения задач для практических занятий и в главе 6 базовая ролевая ДП-модель заменена на мандатную сущностно-ролевую ДП-модель управления доступом и информационными потоками в ОС семейства *Linux*, на основе которой строится механизм управления доступом в отечественной защищенной операционной системе *Astra Linux Special Edition*.

Для студентов вузов, обучающихся по специальностям направления подготовки 090300 – «Информационная безопасность вычислительных, автоматизированных и телекоммуникационных систем» и направления подготовки 090900 – «Информационная безопасность», преподавателей и специалистов в области защиты информации.

ББК 32.973.2-018.2я73

Адрес издательства в Интернет WWW.TECHBOOK.RU

Учебное издание

Девянин Пётр Николаевич

**Модели безопасности компьютерных систем.
Управление доступом и информационными потоками**

Учебное пособие

2-е изд., исправленное и дополненное

Редактор Ю. Н. Чернышов
Компьютерная верстка Ю. Н. Чернышова
Обложка художника В. Г. Ситникова

Подписано в печать 23.03.2013. Печать офсетная. Формат 60×88/16. Уч. изд. л. 21,25. Тираж 500 экз. (1-й з-д 100 экз.)

ISBN 978-5-9912-0328-9

© П. Н. Девянин, 2011, 2013

© Издательство Горячая линия–Телеком, 2013

Оглавление

Предисловие	3
Предисловие ко второму изданию	6
Глава 1. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	8
1.1. Элементы теории компьютерной безопасности	8
1.1.1. Сущность, субъект, доступ, информационный поток ..	8
1.1.2. Классическая классификация угроз безопасности информации	10
1.1.3. Виды информационных потоков	11
1.1.4. Виды политик управления доступом и информационными потоками	13
1.1.5. Утечка права доступа и нарушение безопасности КС ..	16
1.2. Математические основы моделей безопасности	19
1.2.1. Основные понятия	19
1.2.2. Понятие автомата	19
1.2.3. Элементы теории графов	20
1.2.4. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы	22
1.2.5. Модель решетки	22
1.3. Основные виды формальных моделей безопасности	24
1.4. Проблема адекватности реализации модели безопасности в реальной компьютерной системе	26
1.5. Контрольные вопросы и задачи	27
Глава 2. Модели компьютерных систем с дискреционным управлением доступом	29
2.1. Модель матрицы доступов Харрисона–Руззо–Ульмана ..	29
2.1.1. Описание модели	29
2.1.2. Анализ безопасности систем ХРУ	31
2.1.3. Модель типизированной матрицы доступов	38
2.2. Модель распространения прав доступа Take-Grant	47
2.2.1. Основные положения классической модели Take-Grant ..	47
2.2.2. Расширенная модель Take-Grant	58

2.2.3. Представление систем Take-Grant системами ХРУ	67
2.3. Дискреционные ДП-модели	69
2.3.1. Базовая ДП-модель	69
2.3.2. ДП-модель без кооперации доверенных и недоверенных субъектов	95
2.4. Контрольные вопросы и задачи	103
Глава 3. Модели изолированной программной среды . . .	107
3.1. Субъектно-ориентированная модель изолированной программной среды	107
3.2. Корректность субъектов в ДП-моделях КС с дискреционным управлением доступом	115
3.2.1. ДП-модель с функционально ассоциированными с субъектами сущностями	115
3.2.2. ДП-модель для политики безопасного администрирования	122
3.2.3. ДП-модель для политики абсолютного разделения административных и пользовательских полномочий	133
3.2.4. ДП-модель с функционально или параметрически ассоциированными с субъектами сущностями	139
3.2.5. Применение ФАС ДП-модели для анализа безопасности веб-систем	145
3.3. Методы предотвращения утечки прав доступа и реализации запрещенных информационных потоков	149
3.3.1. Метод предотвращения возможности получения права доступа владения недоверенным субъектом к доверенному субъекту	149
3.3.2. Метод реализации политики безопасного администрирования	151
3.3.3. Метод реализации политики абсолютного разделения административных и пользовательских полномочий . . .	153
3.4. Контрольные вопросы и задачи	155
Глава 4. Модели компьютерных систем с мандатным управлением доступом	157
4.1. Модель Белла–ЛаПадулы	157
4.1.1. Классическая модель Белла–ЛаПадулы	157
4.1.2. Пример некорректного определения свойств безопасности	162
4.1.3. Политика low-watermark в модели Белла–ЛаПадулы .	163
4.1.4. Примеры реализации запрещенных информационных потоков	166
4.1.5. Безопасность переходов	169

4.1.6. Модель мандатной политики целостности информации Биба	172
4.2. Модель систем военных сообщений	175
4.2.1. Общие положения и основные понятия	175
4.2.2. Неформальное описание модели СВС	176
4.2.3. Формальное описание модели СВС	177
4.3. Мандатная ДП-модель	184
4.3.1. Правила преобразования состояний мандатной ДП-мо- дели	184
4.3.2. Безопасность в смысле Белла–ЛаПадулы	191
4.3.3. Условия повышения субъектом уровня доступа	192
4.4. Контрольные вопросы и задачи	197
Глава 5. Модели безопасности информационных потоков	199
5.1. Автоматная модель безопасности информационных по- токов	199
5.2. Программная модель контроля информационных пото- ков	201
5.3. Вероятностная модель безопасности информационных потоков	204
5.4. ДП-модели безопасности информационных потоков по времени	208
5.4.1. ДП-модель с блокирующими доступами доверенных субъектов	208
5.4.2. Мандатная ДП-модель с блокирующими доступами до- веренных субъектов	216
5.4.3. Мандатная ДП-модель с отождествлением порожден- ных субъектов	225
5.4.4. Мандатная ДП-модель КС, реализующих политику строгого мандатного управления доступом	227
5.5. Контрольные вопросы и задачи	232
Глава 6. Модели компьютерных систем с ролевым уп- равлением доступом	234
6.1. Понятие ролевого управления доступом	234
6.2. Базовая модель ролевого управления доступом	234
6.3. Модель администрирования ролевого управления дос- тупом	238
6.3.1. Основные положения	238
6.3.2. Администрирование множеств авторизованных ролей пользователей	239
6.3.3. Администрирование множеств прав доступа, которыми обладает роли	243

6.3.4. Администрирование иерархии ролей	244
6.4. Модель мандатного ролевого управления доступом	247
6.4.1. Защита от угрозы конфиденциальности информации .	247
6.4.2. Защита от угроз конфиденциальности и целостности информации	250
6.5. Мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Linux	254
6.5.1. Состояние системы	254
6.5.2. Функционально или параметрически ассоциированные сущности	267
6.5.3. Доступы и права доступа	270
6.5.4. Задание мандатного управления доступом для состояний системы	272
6.5.5. Задание мандатного контроля целостности для состояний системы	280
6.5.6. Фактическое владение	284
6.5.7. Правила преобразования состояний	285
6.6. Контрольные вопросы и задачи	297
Приложение 1. Методические рекомендации по организации изучения моделей безопасности компьютерных систем	299
Анализ требований ФГОС ВПО	299
Организация изучения моделей безопасности КС	302
Приложение 2. Примеры решения задач на практических занятиях	306
Практическое занятие № 1. Модель решетки	306
Практическое занятие № 2. Модели ХРУ и ТМД	307
Практическое занятие № 3. Классическая модель Take-Grant	310
Практическое занятие № 4. Расширенная модель Take-Grant	312
Практическое занятие № 5. Классическая модель Белла-ЛаПадуды и ее интерпретации	315
Практическое занятие № 6. Модель СВС	319
Практическое занятие № 7. Модели безопасности информационных потоков	321
Практическое занятие № 8. Модели ролевого управления доступом	322
Практическое занятие № 9. Дискреционные ДП-модели	325
Практическое занятие № 10. Мандатные и ролевые ДП-модели .	326
Список литературы	333