

П. Н. Десянин

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Управление доступом и информационными потоками

*Рекомендовано Государственным образовательным учреждением
высшего профессионального образования
«Академия Федеральной службы безопасности Российской Федерации»
в качестве учебного пособия для студентов
высших учебных заведений, обучающихся по специальностям
направления подготовки 090300 – «Информационная безопасность
вычислительных, автоматизированных и телекоммуникационных систем»
и направлению подготовки 090900 – «Информационная безопасность».*
*Регистрационный номер рецензии № 742 от 25 февраля 2010 г.
(ГОУ ВПО «Московский государственный университет печати»)*

Москва
Горячая линия – Телеком
2012

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. Петров*; 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*.

Десянин П. Н.

Д25

Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2012. – 320 с.: ил.

ISBN 978-5-9912-0147-6.

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.

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

Десянин Пётр Николаевич

Модели безопасности компьютерных систем.

Управление доступом и информационными потоками

Учебное пособие

Редактор Ю. Н. Чернышов

Компьютерная верстка Ю. Н. Чернышова

Обложка художника В. Г. Ситникова

Подписано в печать 20.08.2010. Печать офсетная. Формат 60×88/16. Уч. изд. л. 20. Доп. тираж 100 экз.

ISBN 978-5-9912-0147-6

© П. Н. Десянин, 2011, 2012

© Издательство Горячая линия–Телеком, 2012

Предисловие

Исследование формальных моделей, особенно моделей безопасности управления доступом и информационными потоками в компьютерных системах (КС), создает предпосылки для развития теории компьютерной безопасности и разработки новых эффективных методов анализа защищенности современных или перспективных КС, например операционных систем, СУБД, электронных почтовых систем.

В существующей литературе по компьютерной безопасности, в том числе учебной, часто приводятся описания моделей безопасности. Однако их изложение, как правило, носит фрагментарный характер. При этом основное внимание уделяется лишь общей формулировке основных определений и результатов моделей либо краткому их перечислению обзорного характера (без подробного рассмотрения, применяемого математического аппарата и приведения доказательств). В то же время в книгах, где доказательства приводятся, они, как правило, даются в общих чертах.

В пособии рассмотрены с полными доказательствами положения классических моделей безопасности КС: дискреционного, мандатного, ролевого управления доступом, безопасности информационных потоков и изолированной программной среды. Приведен используемый в рассматриваемых моделях математический аппарат. Классические модели по сравнению с [6] дополнены семейством моделей безопасности логического управления доступом и информационными потоками (ДП-моделей), адаптированных к условиям функционирования современных КС. Кроме того, приведены контрольные вопросы и задачи, среди которых выделены задачи повышенной сложности (отмечены символом «*»), даны примеры решения задач на практических занятиях, а также изложены методические рекомендации по организации изучения моделей.

Детальное изучение моделей безопасности КС целесообразно по следующим основным причинам.

Во-первых, модели могут быть непосредственно использованы для анализа безопасности существующих или перспективных КС, особенно в случаях, когда требуется получение гарантий защищенности КС. Например, в соответствии с [1] при анализе безопасности КС, которые должны обладать высоким уровнем доверия, начиная с оценочного уровня доверия 5 (ОУД 5), требуется, чтобы при разработке КС была использована формальная модель политики безопасности. При этом, как минимум, требуется моделировать политики управления доступом и информационными потоками (если они

являются частью политики безопасности КС), так как в настоящее время это признается возможным.

Во-вторых, существующие модели безопасности КС могут быть использованы как основа (как «строительный материал») для разработки более совершенных моделей, позволяющих более точно описывать и исследовать особенности функционирования механизмов защиты современных КС.

В-третьих, часто классические модели безопасности КС позволяют формально анализировать свойства механизмов защиты КС, которые уже были хорошо известны из опыта практической разработки или эксплуатации КС. В то же время по мере развития теории компьютерной безопасности могут создаваться новые модели (например, ДП-модели), с применением которых возможно сначала теоретическое описание и исследование свойств механизмов защиты, а затем подтверждение наличия этих свойств у реальных КС.

В-четвертых, владение знаниями о моделях безопасности КС предоставляет специалисту в области компьютерной безопасности возможности для строгого научного и теоретически обоснованного изложения результатов прикладных исследований, что в свою очередь создает дополнительные предпосылки для его научного роста.

Содержание пособия основано на реализации компетентностного подхода, положенного в основу федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) третьего поколения в области информационной безопасности.

Пособие предназначено для преподавания следующих дисциплин:

«Теоретические основы компьютерной безопасности» для магистров направления подготовки **090900 — «Информационная безопасность»;**

«Модели безопасности компьютерных систем» специальности **090301 — «Компьютерная безопасность»;**

«Безопасность информационных и аналитических систем» специальности **090305 — «Информационно-аналитические системы безопасности»;**

«Основы информационной безопасности» для бакалавров направления подготовки **090900 — «Информационная безопасность»** и других специальностей направления подготовки **090300 — «Информационная безопасность вычислительных, автоматизированных и телекоммуникационных систем».**

Пособие разработано на основе пятнадцатилетнего опыта преподавания моделей безопасности КС в ИКСИ Академии ФСБ России.

Оглавление

Предисловие.....	3
Глава 1. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	5
1.1. Элементы теории компьютерной безопасности.....	5
1.1.1. Сущность, субъект, доступ, информационный поток....	5
1.1.2. Классическая классификация угроз безопасности информации	7
1.1.3. Виды информационных потоков	8
1.1.4. Виды политик управления доступом и информационными потоками	10
1.1.5. Утечка права доступа и нарушение безопасности КС ..	13
1.2. Математические основы моделей безопасности	16
1.2.1. Основные понятия	16
1.2.2. Понятие автомата	16
1.2.3. Элементы теории графов	18
1.2.4. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы	19
1.2.5. Модель решетки	20
1.3. Основные виды формальных моделей безопасности	21
1.4. Проблема адекватности реализации модели безопасности в реальной компьютерной системе	23
1.5. Контрольные вопросы и задачи	24
Глава 2. Модели компьютерных систем с дискреционным управлением доступом	26
2.1. Модель матрицы доступов Харрисона–Руззо–Ульмана ..	26
2.1.1. Описание модели	26
2.1.2. Анализ безопасности систем ХРУ	28
2.1.3. Модель типизированной матрицы доступов	35
2.2. Модель распространения прав доступа Take-Grant	44
2.2.1. Основные положения классической модели Take-Grant	44
2.2.2. Расширенная модель Take-Grant	55
2.2.3. Представление систем Take-Grant системами ХРУ	64
2.3. Дискреционные ДП-модели	66
2.3.1. Базовая ДП-модель	66
2.3.2. ДП-модель без кооперации доверенных и недоверенных субъектов	92

2.4. Контрольные вопросы и задачи	100
Глава 3. Модели изолированной программной среды ..	103
3.1. Субъектно-ориентированная модель изолированной программной среды	103
3.2. Корректность субъектов в ДП-моделях КС с дискреционным управлением доступом	111
3.2.1. ДП-модель с функционально ассоциированными с субъектами сущностями	111
3.2.2. ДП-модель для политики безопасного администрирования	118
3.2.3. ДП-модель для политики абсолютного разделения административных и пользовательских полномочий	128
3.2.4. ДП-модель с функционально или параметрически ассоциированными с субъектами сущностями	135
3.2.5. Применение ФАС ДП-модели для анализа безопасности веб-систем	140
3.3. Методы предотвращения утечки прав доступа и реализации запрещенных информационных потоков	144
3.3.1. Метод предотвращения возможности получения права доступа владения недоверенным субъектом к доверенному субъекту	144
3.3.2. Метод реализации политики безопасного администрирования	146
3.3.3. Метод реализации политики абсолютного разделения административных и пользовательских полномочий ...	148
3.4. Контрольные вопросы и задачи	150
Глава 4. Модели компьютерных систем с мандатным управлением доступом	152
4.1. Модель Белла–ЛаПадулы	152
4.1.1. Классическая модель Белла–ЛаПадулы	152
4.1.2. Пример некорректного определения свойств безопасности	157
4.1.3. Политика low-watermark в модели Белла–ЛаПадулы ..	159
4.1.4. Примеры реализации запрещенных информационных потоков	161
4.1.5. Безопасность переходов	164
4.1.6. Модель мандатной политики целостности информации Биба.....	167
4.2. Модель систем военных сообщений	170
4.2.1. Общие положения и основные понятия	170
4.2.2. Неформальное описание модели СВС	171
4.2.3. Формальное описание модели СВС	172

4.3. Мандатная ДП-модель	179
4.3.1. Правила преобразования состояний мандатной ДП-модели	179
4.3.2. Безопасность в смысле Белла–ЛаПадулы	186
4.3.3. Условия повышения субъектом уровня доступа	187
4.4. Контрольные вопросы и задачи	192
Глава 5. Модели безопасности информационных потоков	193
5.1. Автоматная модель безопасности информационных потоков	193
5.2. Программная модель контроля информационных потоков	195
5.3. Вероятностная модель безопасности информационных потоков	198
5.4. ДП-модели безопасности информационных потоков по времени	202
5.4.1. ДП-модель с блокирующими доступами доверенных субъектов	202
5.4.2. Мандатная ДП-модель с блокирующими доступами доверенных субъектов	210
5.4.3. Мандатная ДП-модель с отождествлением порожденных субъектов	218
5.4.4. Мандатная ДП-модель КС, реализующих политику строгого мандатного управления доступом	220
5.5. Контрольные вопросы и задачи	225
Глава 6. Модели компьютерных систем с ролевым управлением доступом	227
6.1. Понятие ролевого управления доступом	227
6.2. Базовая модель ролевого управления доступом	228
6.3. Модель администрирования ролевого управления доступом	231
6.3.1. Основные положения	231
6.3.2. Администрирование множеств авторизованных ролей пользователей	232
6.3.3. Администрирование множеств прав доступа, которыми обладает роли	236
6.3.4. Администрирование иерархии ролей	237
6.4. Модель мандатного ролевого управления доступом	241
6.4.1. Защита от угрозы конфиденциальности информации ..	241
6.4.2. Защита от угроз конфиденциальности и целостности информации	243
6.5. Базовая ролевая ДП-модель	247
6.5.1. Состояния базовой ролевой ДП-модели	247

6.5.2. Правила преобразования состояний базовой ролевой ДП-модели	252
6.5.3. Условия передачи прав доступа с участием двух субъ- ект-сессий	268
6.6. Контрольные вопросы и задачи	281
ПРИЛОЖЕНИЕ 1. Методические рекомендации по ор- ганизации изучения моделей безопасности компьютерных систем	283
Анализ требований ФГОС ВПО	283
Организация изучения моделей безопасности КС	286
ПРИЛОЖЕНИЕ 2. Примеры решения задач на практи- ческих занятиях	290
Практическое занятие № 1. Модель решетки	290
Практическое занятие № 2. Модели ХРУ и ТМД	291
Практическое занятие № 3. Классическая модель Take-Grant ..	294
Практическое занятие № 4. Расширенная модель Take-Grant ...	296
Практическое занятие № 5. Классическая модель Белла–ЛаПа- дулы и ее интерпретации	299
Практическое занятие № 6. Модель СВС	301
Практическое занятие № 7. Модели безопасности информацион- ных потоков	303
Практическое занятие № 8. Модели ролевого управления досту- пом	305
Практическое занятие № 9. Дискреционные ДП-модели	307
Практическое занятие № 10. Мандатные и ролевые ДП-модели	308
Предметный указатель	311
Список литературы	314