

Д.А. Мельников

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОТКРЫТЫХ СИСТЕМ

Учебник

*Рекомендовано Учебно-методическим объединением
по образованию в области прикладной информатики в качестве
учебника для студентов, обучающихся по направлению
«Прикладная информатика»*

3-е издание, стереотипное

Москва
Издательство «ФЛИНТА»
2019

УДК 004.056(075.8)

ББК 32.81я73

М48

Рецензенты:

д-р физ.-мат. наук, проф. кафедры «Информационная безопасность»
факультета «Информатика и системы управления»

МГТУ им. Н.Э. Баумана *В.А. Орлов*;

доц., канд. техн. наук, зав. кафедрой «Автоматизированные системы
обработки информации и управления» института компьютерных
технологий МГУЭСИ *А.А. Микрюков*;

заслуженный деятель науки РФ, д-р техн. наук,
действительный член Международной академии информатизации,
проф. кафедры № 43 «Стратегические информационные
исследования» факультета КИБ НИЯУ МИФИ *А.В. Петраков*

Мельников Д.А.

М48 Информационная безопасность открытых систем [Электронный
ресурс]: учебник / Д.А. Мельников. — 3-е изд., стер. — М. :
ФЛИНТА, 2019. — 444 с.

ISBN 978-5-9765-1613-7

Учебник посвящен теоретическим основам обеспечения ИБ: архитектура ИБ, концептуальные основы (концептуальные понятия) обеспечения ИБ, основы аутентификации, управления доступом, обеспечения неотказуемости, конфиденциальности, целостности, аудита безопасности, оповещения об опасности и обеспечения ключами.

Для студентов государственных образовательных учреждений высшего профессионального образования, обучающихся по направлениям 230700 «Прикладная информатика», 090900 «Информационная безопасность» (ИБ) и 230100 «Информатика и вычислительная техника», а также специальностям 090301 «Компьютерная безопасность», 090303 «Информационная безопасность автоматизированных систем» и 090305 «Информационно-аналитические системы безопасности»; аспирантов и практических работников, занимающихся вопросами синтеза и оптимизации систем обеспечения безопасности открытых (прикладных) информационно-технологических сетей и систем.

УДК 004.056(075.8)

ББК 32.81я73

ISBN 978-5-9765-1613-7

© Мельников Д.А., 2013

© Издательство «ФЛИНТА», 2013

ОГЛАВЛЕНИЕ

Предисловие	11
Введение	14
Глава 1. Архитектура безопасности ИТС	20
1.1. Почему необходимо защищаться?	20
1.2. Источники и последствия реализации угроз ИБ	21
1.3. Функция, способы и средства обеспечения ИБ	31
1.4. Архитектура безопасности ЭМВОС	33
1.4.1. Термины и определения	34
1.4.2. Услуги и способы обеспечения безопасности	38
1.4.3. Принципы архитектуры безопасности ЭМВОС	47
1.5. Принципы архитектуры безопасности сети Интернет	52
Глава 2. Концепции обеспечения информационной безопасности	53
2.1. Общие концепции обеспечения ИБ	55
2.1.1. Информация, необходимая для обеспечения ИБ	55
2.1.2. Сетевой сегмент безопасности	56
2.1.3. Предположения относительно ПЛБ для определенных СЛБ	61
2.1.4. Надежные (доверенные) объекты/субъекты	62
2.1.5. Доверие	63
2.1.6. Третьи доверенные стороны	64
2.2. Общая информация для обеспечения безопасности	64
2.2.1. Метки безопасности	65
2.2.2. Криптографические проверочные суммы	70
2.2.3. Сертификаты безопасности	72
2.2.4. Способы защиты сертификатов безопасности	76
2.2.5. Маркеры безопасности	83
2.3. Общие средства обеспечения безопасности	84
2.3.1. Вспомогательные средства	85
2.3.2. Функциональные средства	86
2.4. Взаимосвязи между СПБ	88
2.5. Отказ в обслуживании и доступность	90
Глава 3. Теоретические основы аутентификации	92
3.1. Общие положения	92
3.1.1. Основные концепции аутентификации	92
3.1.2. Практические аспекты функционирования СЛАУ	97
3.1.3. Принципы, используемые при аутентификации	102
3.1.4. Фазы (этапы) аутентификации	103
3.1.5. Привлечение ДТС	105

3.1.6. Типы участников информационного взаимодействия	111
3.1.7. Аутентификация физического лица (гражданина, пользователя), или персонификация	112
3.1.8. Типы атак на процедуру аутентификации	112
3.2. Вспомогательная информация и средства аутентификации	116
3.2.1. Вспомогательная информация для аутентификации	116
3.2.2. Средства аутентификации	123
3.3. Свойства способов аутентификации	131
3.3.1. Симметричные/асимметричные методы аутентификации	131
3.3.2. Использование криптографических/некриптографических методов	132
3.3.3. Типы аутентификации	132
3.4. Способы аутентификации	134
3.4.1. Классификация по критерию уязвимости	134
3.4.2. Инициирование доставки	147
3.4.3. Использование СЕРТ АУ	148
3.4.4. Обоюдная аутентификация	148
3.4.5. Характеристики классов способов аутентификации	149
3.4.6. Классификация на основе конфигурации	151
3.5. Взаимодействие с другими службами и способами обеспечения безопасности	156
3.5.1. Управление доступом	156
3.5.2. Целостность данных	156
3.5.3. Конфиденциальность данных	157
3.5.4. Неотказуемость	157
3.5.5. Аудит	158
3.6. Персонификация (аутентификация пользователей)	158
3.6.1. Общие положения	158
3.6.2. Процессы, действующие от имени пользователя	162
3.7. Аутентификация в ЭМВОС и Интернет-архитектуре	162
3.7.1. Аутентификация объекта	162
3.7.2. Аутентификация источника данных	163
3.7.3. Использование аутентификации уровнями ЭМВОС и Интернет-архитектуры	163
3.8. Практические аспекты парирования атак типа «повторная передача» на основе применения уникальных чисел или встречных запросов	165
3.8.1. Уникальные числа	165
3.8.2. Встречные запросы	166
3.9. Защита процедуры аутентификации	167
3.9.1. Атаки типа «прослушивание/повторная передача»	167
3.9.2. Атаки типа «повторная передача одной и той же проверяющей стороне»	167

3.9.3. Атаки типа «повторная передача разным проверяющим сторонам»	168
3.9.4. Атаки типа «перехват/повторная передача»	168
3.9.5. Использование индикатора «приглашение/запрос» для защиты от атак нарушителя	170
3.9.6. Протокол на основе встречных вызовов	170
3.9.7. Протокол на основе уникальных чисел	172
3.10. Примеры способов аутентификации	172
3.10.1. Способ аутентификации с использованием уникального числа и интерактивного СЕРТ АУ	173
3.10.2. Способ аутентификации с использованием встречного запроса и интерактивного СЕРТ АУ	175
Глава 4. Теоретические основы управления доступом	180
4.1. Общие положения	180
4.1.1. Цель управления доступом	180
4.1.2. Основные аспекты УД	181
4.1.3. Распределение компонентов УД	193
4.1.4. Распределение компонентов УД в нескольких ССБ	195
4.1.5. Угрозы УД	196
4.2. Политики УД	196
4.2.1. Отображение политики УД	197
4.2.2. Управление политиками	199
4.2.3. Детализация и локализация	200
4.2.4. Унаследованные правила	201
4.2.5. Приоритет среди правил ПЛУД	202
4.2.6. Правила ПЛУД в режиме «по умолчанию»	203
4.2.7. Отображение политики среди взаимодействующих ССБ	203
4.3. Вспомогательная информация и средства УД	204
4.3.1. ВИ для УД	204
4.3.2. Защита ВИУД	208
4.3.3. Средства УД	210
4.4. Классификация способов УД	216
4.4.1. Введение	216
4.4.2. Схема УД на основе списков доступа	219
4.4.3. Мандатная схема	223
4.4.4. Схема на основе меток безопасности	226
4.4.5. Контекстная схема	230
4.5. Взаимодействие с другими СЛБ и СПБ	232
4.5.1. Аутентификация	232
4.5.2. Обеспечение целостности данных	233
4.5.3. Обеспечение конфиденциальности данных	233

4.5.4. Аудит	233
4.5.5. Другие СЛБ, связанные с УД	235
4.6. Обмен СЕРТ УД между компонентами	236
4.6.1. Ретрансляция нескольких СЕРТ УД	236
4.7. Управление доступом в ЭМВОС и Интернет-архитектуре	238
4.7.1. Общие положения	238
4.7.2. Использование УД в рамках уровней ЭМВОС и Интернет-архитектуры	238
4.8. Проблема уникальности (неединственность) параметров подлинности для УД	239
4.9. Распределение компонентов УД	241
4.9.1. Реализационные аспекты	242
4.9.2. Размещение ФПРИ- и ФПРР-модулей	243
4.9.3. Информационное взаимодействие между компонентами УД	244
4.10. Сравнительный анализ УДПР и УДПП	246
4.11. Способ обеспечения ретрансляции ВИУД через инициатора	247
Глава 5. Теоретические основы обеспечения неотказуемости	251
5.1. Общие положения	252
5.1.1. Основные концепции обеспечения неотказуемости	252
5.1.2. Роль и участие ДТС	253
5.1.3. Фазы процедуры обеспечения неотказуемости	255
5.1.4. Некоторые формы служб обеспечения неотказуемости	258
5.1.5. Примеры доказательств при обеспечении неотказуемости в рамках ЭМВОС и Интернет-архитектуры	260
5.2. Политики обеспечения неотказуемости	261
5.3. Вспомогательная информация и средства обеспечения неотказуемости	263
5.3.1. Вспомогательная информация	263
5.3.2. Средства обеспечения неотказуемости	264
5.4. Способы обеспечения неотказуемости	269
5.4.1. СЛНТ, использующая маркеры безопасности (защитные конверты) ДТС	269
5.4.2. СЛНТ, использующая маркеры безопасности и модули, защищающие от несанкционированного вмешательства	270
5.4.3. СЛНТ, использующая ЭЦП	271
5.4.4. СЛНТ, использующая метки времени	273
5.4.5. СЛНТ, использующая промежуточную ДТС	274

5.4.6. СЛНТ, использующая нотариальное заверение	274
5.4.7. Угрозы СЛНТ	275
5.5. Взаимосвязи с другими СЛБ И СПБ	281
5.5.1. Аутентификация	281
5.5.2. Управление доступом	281
5.5.3. Обеспечение конфиденциальности	281
5.5.4. Обеспечение целостности	281
5.5.5. Аудит	282
5.5.6. Обеспечение ключами	282
5.6. СЛНТ в системах ЭМВОС и Интернет-архитектуры	282
5.6.1. СЛНТ с подтверждением источника данных	282
5.6.2. СЛНТ с подтверждением доставки данных	283
5.7. СЛНТ в системах хранения и ретрансляции	284
5.8. Восстановление в СЛНТ	286
5.9. Взаимодействие со Службой единого каталога	289
Глава 6. Теоретические основы обеспечения конфиденциальности	295
6.1. Общие положения	296
6.1.1. Основные концепции обеспечения конфиденциальности	296
6.1.2. Классы СЛКН	301
6.1.3. Типы СПКН	302
6.1.4. Угрозы конфиденциальности	303
6.1.5. Типы атак на конфиденциальность	305
6.2. Политики обеспечения конфиденциальности	306
6.2.1. Отображение (описание) политики	306
6.3. Вспомогательная информация и средства обеспечения конфиденциальности	307
6.3.1. Вспомогательная информация	307
6.3.2. Средства обеспечения конфиденциальности	308
6.4. Способы обеспечения конфиденциальности	310
6.4.1. Обеспечение конфиденциальности на основе предотвращения доступа	311
6.4.2. Обеспечение конфиденциальности на основе шифрования	311
6.4.3. Обеспечение конфиденциальности на основе контекстно-зависимого размещения	315
6.5. Взаимодействие с другими СЛБ и СПБ	316
6.5.1. Управление доступом	316
6.6. Обеспечение конфиденциальности в ЭМВОС и Интернет-архитектуре	316
6.6.1. Услуга по обеспечению конфиденциальности информационного обмена с установлением соединения	317

6.6.2. Услуга по обеспечению конфиденциальности информационного обмена без установления соединения (дейтаграммный режим)	317
6.6.3. Услуга по обеспечению конфиденциальности отдельных полей	317
6.6.4. Услуга по обеспечению конфиденциальности потока трафика	318
6.6.5. Использование услуг по обеспечению конфиденциальности на уровнях ЭМВОС и Интернет-архитектуры	318
6.7. Форматы представления информации	321
6.8. Скрытые каналы передачи	323
Глава 7. Теоретические основы обеспечения целостности	328
7.1. Общие положения	329
7.1.1. Основные концепции обеспечения целостности	332
7.1.2. Типы СЛЦЛ	332
7.1.3. Типы СПЦЛ	333
7.1.4. Угрозы целостности	334
7.1.5. Типы атак на целостность	335
7.2. Политики обеспечения целостности	336
7.2.1. Описание политики	336
7.3. Вспомогательная информация и средства обеспечения целостности	338
7.3.1. ВИ, необходимая для обеспечения целостности	338
7.3.2. Средства обеспечения целостности	340
7.4. Классификация способов обеспечения целостности	341
7.4.1. Обеспечение целостности на основе криптографии	341
7.4.2. Обеспечение целостности на основе контекста сообщения	345
7.4.3. Обеспечение целостности на основе обнаружения нарушений и передачи ответных квитанций	347
7.4.4. Обеспечение целостности путем препятствования (предотвращения)	348
7.5. Взаимосвязи с другими СЛБ и СПБ	349
7.5.1. Управление доступом	349
7.5.2. Аутентификация источника данных	349
7.5.3. Конфиденциальность	349
7.6. Обеспечение целостности в ЭМВОС и Интернет-архитектуре	350
7.6.1. Целостность соединения с восстановлением	350
7.6.2. Целостность соединения без восстановления	350

7.6.3. Целостность отдельных полей при виртуальном соединении	351
7.6.4. Целостность соединения в дейтаграммном режиме	351
7.6.5. Целостность отдельных полей при соединении в дейтаграммном режиме	351
7.6.6. Применение СЛЦЛ в рамках уровней ЭМВОС и Интернет-архитектуры	351
7.7. Целостность внешних данных	353

Глава 8. Теоретические основы аудита безопасности

и оповещения об опасности	358
8.1. Общие положения	360
8.1.1. Модель и функции	361
8.1.2. Фазы процедур АДБ и оповещения об опасности	365
8.1.3. Корреляция аудиторской информации	368
8.2. Политики и другие аспекты аудита безопасности и оповещения об опасности	369
8.2.1. Политика	369
8.2.2. Законодательные аспекты	369
8.2.3. Требования к защите	370
8.3. Вспомогательная информация и средства для аудита безопасности и оповещения об опасности	371
8.3.1. ВИ в интересах СЛАО	372
8.3.2. Средства для СЛАО	373
8.4. Способы проведения АДБ и применения СОП	377
8.5. Взаимосвязи с другими СЛБ и СПБ	377
8.5.1. Аутентификация объекта/субъекта	377
8.5.2. Аутентификация источника данных	378
8.5.3. Управление доступом	378
8.5.4. Обеспечение конфиденциальности	378
8.5.5. Обеспечение целостности	378
8.5.6. Обеспечение неотказуемости	379
8.6. Общие принципы АДБ и СОП в ЭМВОС и Интернет-архитектуре	379
8.7. Реализация модели АДБ и СОП	381
8.8. Регистрация времени возникновения событий, подлежащих аудиторскому контролю	384

Глава 9. Теоретические основы обеспечения ключами

9.1. Общая модель обеспечения ключами	390
9.1.1. Общие положения	390
9.1.2. Защита ключей	390
9.1.3. Общая модель жизненного цикла ключа	393

9.2. Основные концепции обеспечения ключами	398
9.2.1. Службы (услуги по) обеспечения(ю) ключами	398
9.2.2. Обеспечивающие службы (услуги)	405
9.3. Концептуальные модели распределения ключей	
между двумя взаимодействующими сторонами	406
9.3.1. Общие положения	406
9.3.2. Распределение ключей между связанными	
объектами	407
9.3.3. Распределение ключей в рамках одного ССБ	407
9.3.4. Распределение ключей между двумя ССБ	411
9.4. Провайдеры специализированных услуг	414
9.5. Угрозы системе обеспечения ключами	414
9.6. Информационные объекты в службе обеспечения	
ключами	415
9.7. Классы прикладных криптографических систем	416
9.7.1. Единая классификация криптографических	
систем	416
9.7.2. СЛАУ и СЛЦЛ и ключи	417
9.7.3. СЛКН и ключи	419
9.7.4. Совмещенные службы	420
9.8. Обеспечение жизненного цикла СЕРТ ОК	420
9.8.1. Общие положения	420
9.8.2. Удостоверяющий центр	420
9.8.3. Процедура сертификации	422
9.8.4. Распределение и использование СЕРТ ОК	429
9.8.5. Маршруты сертификации	430
9.8.6. Аннулирование сертификатов	430
Список используемых сокращений	434
Литература	436