

УДК 004.56  
ББК 32.972.13  
Б24

Рецензенты:

**С. А. Петренко** — докт. техн. наук, профессор СПбГЭТУ «ЛЭТИ» (Санкт-Петербург)  
**Alec Shcherbakov** — GSSP, SCEA, SCJP, эксперт SATEC (San Jose, USA)

**Барабанов А. В., Дорофеев А. В., Марков А. С., Цирлов В. Л.**  
Б24 Семь безопасных информационных технологий / под ред. А. С. Маркова. — М.: ДМК Пресс, 2017. — 224 с.: ил.

**ISBN 978-5-97060-494-6**

Целью написания книги является ознакомление читателей с зарубежными подходами в области информационной безопасности.

Все разделы подготовлены на базе материалов международных сертификационных учебных курсов в области управления информационной безопасностью. Изложены базовые принципы, концептуальные подходы и информационные технологии, применяемые при многоуровневой защите информации в организациях. Основное внимание уделено структуризации и классификации методов, техник и средств обеспечения безопасности информационных ресурсов компьютерных систем.

Учебник в первую очередь предназначен для специалистов, желающих принципиально повысить свой профессиональный статус и подготовиться к сдаче международных экзаменов в области информационной безопасности. Полезен студентам, обучающимся по специальностям в области информационной безопасности и смежным специальностям, а также всем увлекающимся вопросам компьютерной безопасности.

УДК 004.56  
ББК 32.972.13

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-5-97060-494-6

© А. В. Барабанов, А. В. Дорофеев, А. С. Марков,  
В. Л. Цирлов, 2017  
© Оформление, издание, ДМК Пресс, 2017

# Содержание

<b>Предисловие о семи безопасных информационных технологиях .....</b>	<b>6</b>
<b>Глава 1. Менеджмент информационной безопасности.....</b>	<b>9</b>
1.1. Основные понятия информационной безопасности.....	9
1.2. Система менеджмента информационной безопасности .....	12
1.3. Анализ и управление рисками.....	17
1.4. Классификация информации.....	23
1.5. Порядок использования политик, стандартов и руководств.....	28
1.6. Особенности работы с персоналом .....	31
Вопросы для повторения.....	33
Лабораторная работа .....	36
<b>Глава 2. Обеспечение безопасного доступа .....</b>	<b>38</b>
2.1. Понятие управления безопасным доступом .....	38
2.2. Категории управления доступом .....	39
2.3. Свойство подотчетности и подсистемы управления доступом.....	41
2.4. Средства идентификации и аутентификации .....	43
2.5. Протоколы сетевого доступа .....	54
2.6. Методы управления доступом.....	58
Вопросы для повторения.....	61
Лабораторная работа .....	64
<b>Глава 3. Обеспечение сетевой безопасности.....</b>	<b>65</b>
3.1. Понятие компьютерной сети.....	65
3.2. Базовая эталонная модель взаимосвязи открытых систем.....	74
3.3. Стек протоколов TCP/IP .....	78
3.4. Средства обеспечения сетевой безопасности .....	91
Вопросы для повторения.....	101

<b>Глава 4. Криптографическая защита информации .....</b>	<b>106</b>
4.1. Основные криптографические примитивы .....	106
4.2. Элементарное шифрование.....	108
4.3. Симметричная криптография .....	114
4.4. Асимметричная криптография .....	118
4.5. Электронно-цифровая подпись и криптографическая хэш-функция.....	123
4.6. Инфраструктура открытых ключей .....	127
Вопросы для повторения.....	128
<b>Глава 5. Разработка безопасных программ.....</b>	<b>132</b>
5.1. Модели жизненного цикла программного обеспечения.....	132
5.2. Безопасный жизненный цикл программного обеспечения .....	136
5.3. Обзор мер по разработке безопасного программного обеспечения .....	143
Вопросы для повторения.....	154
<b>Глава 6. Моделирование и оценка соответствия .....</b>	<b>158</b>
6.1. Основные понятия безопасной архитектуры .....	158
6.2. Концептуальные модели управления доступом .....	160
6.3. Принципы безопасной архитектуры ЭВМ .....	166
6.4. Скрытые каналы передачи информации.....	170
6.5. Критерии оценки соответствия.....	173
Вопросы для повторения.....	184
<b>Глава 7. Обеспечение непрерывности бизнеса и восстановления.....</b>	<b>187</b>
7.1. Управление непрерывностью бизнеса и восстановлением .....	187
7.2. Модель менеджмента непрерывности бизнеса .....	188
Вопросы для повторения.....	198
<b>Литература.....</b>	<b>201</b>
<b>Ответы на вопросы для повторения.....</b>	<b>208</b>

---

<b>Приложение 1. Кодекс профессиональной этики .....</b>	<b>214</b>
Четыре заповеди профессиональной этики (ISC)2 .....	214
Семь правил профессиональной этики ISACA .....	214
<b>Приложение 2. Типовые компьютерные атаки .....</b>	<b>216</b>
Криптографические и парольные атаки.....	216
Атаки на отказ в обслуживании .....	217
Атаки на программный код и приложения .....	218
Атаки социальной инженерии и физические атаки .....	219
Сетевые атаки .....	220