

УДК 004.732.056(075.8)

ББК 32.973.2-018.2я73

М21

Рецензенты: доктор пед. наук, профессор *О. А. Козлов*; доктор техн. наук, профессор *А. А. Тарасов*; кандидат техн. наук, доцент *А. С. Кремер*

Малюк А. А.

М21 Защита информации в информационном обществе. Учебное пособие для вузов. — М.: Горячая линия — Телеком, 2015. — 230 с., ил.

ISBN 978-5-9912-0481-1.

Рассмотрены проблемы формирования информационного общества и связанный с этим рост уязвимости информации в условиях развития современных информационных технологий. Проанализированы и классифицированы угрозы безопасности информации, конкретизированы задачи систем ее обеспечения. Дан обзор методов, технических приемов и аппаратуры защиты информации. Основное внимание уделено проблемам опознавания пользователя, криптографическим методам защиты информации, методам защиты от компьютерных вирусов, защите от утечки информации по техническим каналам, организационно-правовому обеспечению безопасности информации. Подчеркнута необходимость комплексного подхода к защите информации, важность методологических проблем организации и обеспечения функционирования комплексной системы защиты. Изложены основы информационной культуры как важнейшего фактора обеспечения безопасного развития информационного общества. При подготовке учебного пособия использованы результаты исследований, полученные при поддержке РГНФ в рамках научного проекта «Проведение научных исследований по направлению «Формирование в обществе культуры информационной безопасности» № 15-03-00248.

Для студентов и аспирантов вузов, слушателей курсов повышения квалификации, а также для широкого круга читателей, интересующихся современными проблемами защиты информации.

ББК 32.973.2-018.2я73

Адрес издательства в Интернет WWW.TECHBOOK.RU

Малюк Анатолий Александрович

Защита информации в информационном обществе

Учебное пособие для вузов

Все права защищены.

Любая часть этого издания не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения правообладателя

© ООО «Научно-техническое издательство «Горячая линия — Телеком»

www.techbook.ru

© А. А. Малюк

ОГЛАВЛЕНИЕ

Вместо предисловия	3
Глава 1. ВВЕДЕНИЕ	5
1.1. Информационное общество и информационная безопасность	5
1.2. Терминология и предметная область	8
1.3. Содержание данного учебного пособия	13
<i>Вопросы для повторения</i>	<i>13</i>
Глава 2. ЗАЩИТА ИНФОРМАЦИИ — КОМПЛЕКСНАЯ ПРОБЛЕМА	14
2.1. Исторический очерк	14
2.2. Эмпирический подход к защите информации	17
2.3. Концептуально-эмпирический подход	18
2.4. Проблема комплексности защиты	21
2.5. Теоретико-концептуальный подход	22
2.6. Формирование теории защиты информации	23
<i>Вопросы для повторения</i>	<i>25</i>
Глава 3. УЯЗВИМОСТЬ И УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ	26
3.1. Определение угрозы и уязвимости информации	26
3.2. Классификация угроз	26
3.3. Вредительские программы	30
3.4. Системная классификация угроз	31

3.5. Количественная оценка угроз	34
3.6. Понятие информационного риска	36
<i>Вопросы для повторения</i>	39

Глава 4. ИНФОРМАЦИОННАЯ ВОЙНА 41

4.1. Информационное общество и изменение пространства военно-силового противоборства	41
4.2. Информационное оружие и информационная война	42
4.3. Основные цели информационной войны	44
4.4. Объекты информационного противоборства	44
4.5. Субъекты информационного противоборства	46
4.6. Психологические ресурсы общества	48
4.7. Краткие выводы	48
<i>Вопросы для повторения</i>	49

Глава 5. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА 50

5.1. Защита информации от несанкционированного доступа	50
5.2. Принципы защиты от несанкционированного доступа	53
5.3. Монитор обращений	55
5.4. Правила разграничения доступа	56
5.5. Вербальная модель разграничения доступа	57
5.6. Модель Хартсона	57
5.7. Модель Лэмпсона, Грэхема, Деннинга	58
5.8. Модель Белла и Ла Падула	60
<i>Вопросы для повторения</i>	62

Глава 6. ОПОЗНАВАНИЕ ПОЛЬЗОВАТЕЛЕЙ 63

6.1. Проблемы опознавания пользователя	63
6.2. Аутентификация по принципу «пользователь знает»	64
6.3. Аутентификация по принципу «пользователь имеет»	65
6.4. Аутентификация по принципу «пользователь есть»	67
6.5. Характеристики устройств аутентификации	70
6.6. Схемы разграничения доступа	71
<i>Вопросы для повторения</i>	74

Глава 7. КРИПТОГРАФИЯ	75
7.1. Криптографические методы защиты информации. Общие сведения	75
7.2. Криптографические алгоритмы	79
7.3. Стойкость криптосистемы	85
7.4. Стандарты криптографической защиты DES и ГОСТ	85
7.5. Несимметричные системы шифрования	88
Вопросы для повторения	89
Глава 8. РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ. ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ	91
8.1. Распределение ключей шифрования	91
8.2. Децентрализованные системы распределения ключей	92
8.3. Централизованные системы распределения ключей	93
8.4. Пример распределения ключей в сети	94
8.5. Защищенный электронный документооборот. Алгоритм электронной цифровой подписи	95
8.6. Криптографические методы защиты информации в персональном компьютере	99
Вопросы для повторения	100
Глава 9. КОМПЬЮТЕРНЫЕ ВИРУСЫ	101
9.1. Программы-вирусы. История проблемы	101
9.2. Компьютерные вирусы как специальный класс программ, обладающих свойством саморепродукции	102
9.3. Фазы существования компьютерного вируса	104
9.4. Средства антивирусной защиты	106
9.5. Вирусное подавление как форма информационной войны	108
Вопросы для повторения	110
Глава 10. ЗАЩИТА ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ	112
10.1. Технические каналы утечки информации. Определение и основные виды каналов и источников утечки	112
10.2. Контроль акустической информации	115
10.3. Контроль информации в каналах связи	116
10.4. Контроль информации, обрабатываемой средствами вычислительной техники	117

10.5. Способы предотвращения утечки информации по техническим каналам	117
10.6. Защита от утечки информации по акустическому каналу	118
10.7. Защита информации в каналах связи	120
10.8. Защита информации от утечки по каналу побочных электромагнитных излучений и наводок	120
<i>Вопросы для повторения</i>	122

Глава 11. ОРГАНИЗАЦИОННО-ПРАВОВАЯ ЗАЩИТА 124

11.1. Организационно-правовое обеспечение защиты информации	124
11.2. Доктрина информационной безопасности Российской Федерации	124
11.3. Концепция правового обеспечения защиты информации	127
11.4. Опыт законодательного регулирования информатизации за рубежом	129
<i>Вопросы для повторения</i>	135

Глава 12. РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ 136

12.1. Состояние правового обеспечения информатизации и защиты информации в России	136
12.2. Основные законы Российской Федерации в области защиты информации	138
12.3. Государственная система защиты информации	143
12.4. Система стандартизации в области защиты информации	145
<i>Вопросы для повторения</i>	148

Глава 13. КУЛЬТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 149

13.1. Гуманитарные проблемы информационной безопасности	149
13.2. Компетенции в области гуманитарных аспектов защиты информации	151
13.3. Формирование информационной культуры общества. Этика в сфере информационных технологий	153
13.4. Глобальная культура кибербезопасности	157
13.5. Всеобуч в области культуры информационной безопасности	158
<i>Вопросы для повторения</i>	163

Глава 14. КОНЦЕПЦИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ	164
14.1. Комплексная система защиты информации	164
14.2. Стратегии защиты	165
14.3. Функции защиты	167
14.4. Задачи защиты	171
14.5. Средства и методы защиты	178
14.6. Система защиты информации	180
<i>Вопросы для повторения</i>	181
Глава 15. УПРАВЛЕНИЕ ЗАЩИТОЙ	182
15.1. Управление защитой информации	182
15.2. Создание и организация функционирования систем комплексной защиты информации	185
15.3. Изначально защищенные информационные технологии	192
<i>Вопросы для повторения</i>	194
ВМЕСТО ПОСЛЕСЛОВИЯ	196
РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА	198
Основная литература	198
Дополнительная литература	199
Научно-технические журналы	199
ТЕСТЫ ДЛЯ САМОКОНТРОЛЯ	201
Ответы на тесты для самоконтроля	214
ПРИЛОЖЕНИЕ	215
П.1. Мошенничество и вредительские программы в сети Интернет	215
П.2. Социальная инженерия	215
П.3. «Троянский конь»	218
П.4. Фишинг	220
П.5. Вирусное программное обеспечение	222