

А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков,
И. В. Голубятников, А. А. Солдатов, С. В. Скрыль

Технические средства и методы защиты информации

Под редакцией А. П. Зайцева и А. А. Шелупанова

*Рекомендовано УМО вузов по образованию
в области информационной безопасности
в качестве учебного пособия для студентов
высших учебных заведений, обучающихся по специальностям
090102 – «Компьютерная безопасность»,
090105 – «Комплексное обеспечение информационной
безопасности автоматизированных систем»,
090106 – «Информационная безопасность
телекоммуникационных систем»*

Москва
Горячая линия – Телеком
2012

УДК 681.3.067

ББК 32.81

Т38

Рецензент: доктор физ.-мат. наук, профессор С. С. Бондарчук

Авторы: А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков, И. В. Голубятников,
А. А. Солдатов, С. В. Скрыль

Т38 Технические средства и методы защиты информации. Учебное пособие для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков и др.; под ред. А. П. Зайцева и А. А. Шелупанова. – 4-е изд., испр. и доп. – М.: Горячая линия–Телеком, 2012. – 616 с: ил.

ISBN 978-5-9912-0084-4.

Рассмотрены технические средства и методы защиты информации от несанкционированного доступа. Описаны возможные технические каналы утечки информации. Основное внимание уделено рассмотрению принципов работы технических средств защиты информации. Отличительной особенностью книги является наличие лабораторных и практических занятий, которые позволят студентам приобрести практические навыки работы с техническими средствами защиты информации.

Для студентов, обучающихся по группе специальностей 090100 – «Информационная безопасность».

ББК 32.81

Адрес издательства в Интернет www.techbook.ru

Учебное издание

**Зайцев Александр Петрович, Шелупанов Александр Александрович,
Мещеряков Роман Валерьевич, Голубятников Игорь Владимирович,
Солдатов Алексей Анатольевич, Скрыль Сергей Васильевич**

Технические средства и методы защиты информации

Учебное пособие для вузов

Редактор Ю. Н. Рысев
Компьютерная верстка Ю. Н. Рысева
Обложка художника В. Г. Ситникова

Подписано в печать 30.09.2008. Печать офсетная. Формат 60×90/16.

Уч. изд. л. 38,5. Доп тираж «по требованию».

ООО «Научно-техническое издательство «Горячая линия–Телеком»

ISBN 978-5-9912-0084-4

© А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков,
И. В. Голубятников, А. А. Солдатов, С. В. Скрыль, 2009, 2012
© Оформление издательства «Горячая линия–Телеком», 2012

Предисловие

Технические средства и методы защиты информации являются одним из главных направлений при подготовке специалистов в области информационной безопасности. В настоящее время в стране практически отсутствуют апробированные учебники и учебные пособия по специальным дисциплинам, которые по существу и формируют профиль специалиста по защите информации. Появившиеся в последние годы учебные пособия известных авторов – А. А. Хорева, А. А. Торокина, Г. А. Бузова, С. В. Калинина, А. В. Кондратьева и других восполняют этот недостаток. Однако, по-прежнему, существует потребность учебных заведений в такого рода учебно-методической литературе.

В данной книге представлены и рассмотрены все аспекты программ обучения по данному направлению. Она может послужить базой для изучения и понимания фундаментальных основ технической защиты информации.

Авторы сочли необходимым уделить значительное внимание систематизации и описанию наиболее известных технических средств защиты информации как зарубежного, так и отечественного производства. Отличительной особенностью данной книги является наличие в ней лабораторного практикума, который может быть весьма полезным особенно для учебных заведений, начинающих образовательную деятельность по подготовке специалистов по защите информации. Часть работ практикума относится к моделированию процессов. Проведение работ по моделированию с помощью компьютеров характеризуется гибкостью вариации исходных условий задачи и не требует особых материальных затрат, так как моделирование проводится в среде свободно распространяемой программы Electronics Workbench.

Кроме того, авторы привели ключевые выдержки из официальных нормативных материалов по доктрине информационной безопасности Российской Федерации, дающие представление о государственной системе защиты информации и направлениях противодействия технической разведке. Перечень сведений из области защиты информации и глоссарий терминов по информационной безопасности согласно ГОСТ и законодательным документам необходимы для адекватного восприятия материала книги.

Оглавление

Предисловие	3
Введение	4
Глава 1. Технические каналы утечки информации.....	7
1.1. Общие понятия	7
1.2. Технические каналы утечки речевой информации	10
1.2.1. Возможные каналы утечки речевой информации	10
1.2.2. Воздушные технические каналы утечки информации	11
1.2.3. Вибрационные технические каналы	12
1.2.4. Электроакустические каналы утечки информации	12
1.2.5. Оптико-электронный технический канал утечки	14
1.2.6. Параметрические технические каналы утечки информации.....	14
1.3. Технические каналы утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи	15
1.3.1. Электрические линии связи.....	16
1.3.2. Электромагнитные каналы утечки информации	26
1.3.2.1. Электромагнитные излучения элементов ТСПИ	26
1.3.2.2. Электромагнитные излучения на частотах работы ВЧ генераторов ТСПИ и ВТСС	27
1.3.2.3. Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ	27
1.3.2.4. Побочные электромагнитные излучения персонального компьютера.....	28
1.3.3. Электрические каналы утечки информации	30
1.3.3.1. Наводки электромагнитных излучений ТСПИ.....	30
1.3.3.2. Просачивание информационных сигналов в цепи электропитания	34
1.3.3.3. Паразитные связи через цепи питания	34
1.3.3.4. Просачивание информационных сигналов в цепи заземления	36
1.3.3.5. Съём информации по электрическим каналам утечки информации	37
1.3.4. Параметрический канал утечки информации	39
1.4. Способы скрытого видеонаблюдения и съёмки	39

1.5. Демаскирующие признаки объектов и акустических закладок	55
1.5.1. Общие положения	55
1.5.2. Демаскирующие признаки объектов	57
1.5.2.1. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра	58
1.5.2.2. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра	62
1.5.3. Демаскирующие признаки радиоэлектронных средств	64
1.5.4. Демаскирующие признаки акустических закладок	67
Глава 2. Средства акустической разведки	72
2.1. Микрофоны	72
2.2. Направленные микрофоны	75
2.2.1. Виды направленных микрофонов	76
2.2.2. Сравнение и оценка направленных микрофонов	79
2.2.3. Примеры технической реализации направленных микрофонов	82
2.3. Проводные системы, портативные диктофоны и электронные стетоскопы	84
2.3.1. Общие сведения	84
2.3.2. Примеры технической реализации диктофонов и транскрайберов	88
2.3.3. Стетоскопы	93
2.4. Радиомикрофоны	94
2.5. Лазерные микрофоны	97
2.6. Гидроакустические датчики	97
2.7. СВЧ- и ИК-передатчики	97
Глава 3. Средства радио- и радиотехнической разведки	99
3.1. Сканирующие компьютерные радиоприемники, радиопеленгаторы	99
3.2. Анализаторы спектра, радиочастотомеры	108
Глава 4. Контроль и прослушивание телефонных каналов связи	120
4.1. Прослушивание телефонных переговоров	120
4.2. Непосредственное подключение к телефонной линии	121
4.3. Подкуп персонала АТС	121
4.4. Прослушивание через электромагнитный звонок	123
4.5. Прослушивание помещений через микрофон телефонного аппарата	124

4.6. «Атаки» на компьютеризованные телефонные системы	127
Глава 5. Системы слежения за транспортными средствами	128
5.1. Системы определения, использующие методы спутниковой радионавигации	128
5.2. Компании, предоставляющие услуги в сфере спутниковых навигационных технологий	129
Глава 6. Обеспечение безопасности объектов	143
6.1. Классификация объектов охраны	143
6.2. Особенности задач охраны различных типов объектов	143
6.3. Общие принципы обеспечения безопасности объектов	145
6.4. Некоторые особенности построения периметровой охраны	146
6.4.1. Периметр – первая линия защиты	146
6.4.2. Функциональные зоны охраны.....	149
6.4.3. Оптимизация построения системы охранной безопасности	149
6.5. Контроль доступа к защищаемым помещениям.....	152
6.6. Охрана оборудования и перемещаемых носителей информации	154
6.7. Быстроразвертываемые охранные системы.....	156
6.8. Анализ состава зарубежных комплексов быстроразвертываемых средств обнаружения	157
6.8.1. Tактическая автоматизированная система безопасности TASS.....	157
6.8.2. Портативная система датчиков Man-Portable Networked System.....	159
6.8.3. Система IREMBASS.....	159
6.9. Анализ состава отечественных быстроразвертываемых средств охраны	163
6.10. Системы защиты территории и помещений	166
6.10.1. Инфракрасные системы	166
6.10.2. Элементы защиты ИК-датчиков.....	174
6.11. Оптоволоконные системы	180
6.12. Емкостные системы охраны периметров	181
6.13. Вибрационные системы с сенсорными кабелями.....	184
6.14. Вибрационно-сейсмические системы	192

6.15. Радиолучевые системы	195
6.16. Системы «активной» охраны периметров	197
6.17. Телевизионные системы	199
Глава 7. Защита электронных устройств и объектов от побочных электромагнитных излучений	205
7.1. Экранирование электромагнитных волн	205
7.1.1. Электромагнитное экранирование и развязывающие цепи	205
7.1.2. Подавление емкостных паразитных связей	209
7.1.3. Подавление индуктивных паразитных связей	209
7.1.4. Экранирование проводов и катушек индуктивности	211
7.2. Безопасность оптоволоконных кабельных систем	222
7.3. Заземление технических средств	230
7.4. Фильтрация информационных сигналов	232
7.5. Основные сведения о помехоподавляющих фильтрах	234
7.6. Выбор типа фильтра	241
7.7. Пространственное и линейное зашумление	245
Глава 8. Устройства контроля и защиты слаботочных линий и сетей	248
8.1. Особенности слаботочных линий и сетей как каналов утечки информации	248
8.2. Рекомендуемые схемы подключения анализаторов к электросиловым и телефонным линиям ..	249
8.3. Устройства контроля и защиты проводных линий от утечки информации	252
8.4. Способы предотвращения утечки информации через ПЭМИН ПК	264
Глава 9. Средства защиты информации в телефонных системах (с использованием криптографических методов)	267
9.1. Универсальные средства защиты	267
9.2. Скремблеры	277
Глава 10. Металлодетекторы	281
10.1. Общие сведения	281
10.2. Металлодетекторы низкой и сверхнизкой частоты	286
10.3. Металлодетекторы с импульсной индукцией	289
10.4. Промышленные образцы некоторых металлодетекторов	291

Глава 11. Нелинейные локаторы	303
11.1. Модель радиолокационного наблюдения в условиях нелинейной локации	303
11.2. Технология нелинейной локации	306
11.3. Эффект затухания	308
11.4. Другие возможности применения аудиодемодуляции в ЛН ...	308
11.5. Тип излучения	309
11.6. Другие характеристики ЛН	309
Глава 12. Технические средства радиомониторинга и обнаружения закладных устройств	318
12.1. Общие сведения	318
12.2. Индикаторы поля	321
12.3. Комплексы радиомониторинга и обнаружения закладок	330
Глава 13. Средства обеспечения информационной безопасности в компьютерных системах.....	349
13.1. Система защиты информации Secret Net 4.0	349
13.1.1. Назначение	349
13.2. Электронный замок «СОБОЛЬ»	353
13.3. USB-ключ	358
13.4. Считыватели «Proximity»	362
13.5. Технологии защиты информации на основе смарт-карт	364
13.6. Система защиты конфиденциальной информации «Secret Disk»	366
13.7. Программно-аппаратный комплекс «Аккорд-1.95»	369
13.8. Кейс «ТЕНЬ»	376
13.9. Аппаратно-программная система криптогра- фической защиты сообщений «SX-1»	377
13.10. Устройство для быстрого уничтожения информации на жестких магнитных дисках СТЕК-Н	378
Лабораторный практикум	380
Лабораторная работа № 1. Изучение принципа работы локатора нелинейностей	381
Лабораторная работа № 2. Сетевые помехоподавляющие пассивные фильтры низких и высоких частот	385
Лабораторная работа № 3. Сетевые пассивные полосно- заграждающие и полосно-пропускающие фильтры.....	390

Лабораторная работа № 4. Изучение и расчет помех (наводок) в каналах связи при внешней параллельной паразитной связи	395
Лабораторная работа № 5. Изучение и расчет помех (наводок) в каналах связи при внешней паразитной связи последовательного вида	401
Лабораторная работа № 6. Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в охраняемом помещении.....	406
Лабораторная работа № 7. Обнаружение сигналов линейных и сетевых закладок.....	423
Лабораторная работа № 8. Обнаружение оптических сигналов передатчиков ИК-диапазона	442
Лабораторная работа № 9. Нелинейная локация.....	453
Лабораторная работа № 10. Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля.....	462
Лабораторная работа № 11. Ознакомление с комплексом для проведения специсследований «Легенда»	472
Лабораторная работа № 12. Обнаружение ПЭМИН по электрической составляющей электромагнитного поля с помощью ПАК «Легенда»	485
Лабораторная работа № 13. Обнаружение ПЭМИН по магнитной составляющей электромагнитного поля с помощью ПАК «Легенда»	506
Лабораторная работа № 14. Обнаружение ПЭМИН в электрических цепях с помощью пробника напряжения «Я6-122»	510
Приложение 1. Краткое руководство по системе моделирования Electronics Workbench.....	514
Приложение 2. Глоссарий.....	572
Приложение 3. Перечень сведений конфиденциального характера	598
Приложение 4. Доктрина информационной безопасности Российской Федерации	599
Список литературы.....	608