

С. В. Ленков, Д. А. Перегудов, В. А. Хорошко

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

ТОМ II

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

- Принципы разведки
- Каналы несанкционированного получения информации
- Акустическая разведка
- Энергетические каналы утечки информации
- Каналы утечки информации при эксплуатации ЭВМ
- Визуально-оптические каналы утечки информации
- Материально-вещественные каналы утечки информации
- Намеренное силовое воздействие
- Методы разрушения информации
- Механизм возникновения ПЭМИ в средствах цифровой электронной техники
- Технические методы и средства защиты информации
- Защита информации в сетях
- Программные методы защиты информации
- Криптографическая защита информации
- Скремблирование
- Стеганография

Рецензенты:

Поповский Владимир Владимирович – д.т.н., проф., заведующий кафедрой Харьковского национального университета радиоэлектроники;

Сбитнев Анатолий Иванович – д.т.н., проф., заслуженный деятель науки и техники Украины, Лауреат государственной премии Украины, профессор Национальной академии обороны Украины.

784715

Ленков, С.В.

Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А., Под ред. В.А. Хорошко. – К. : Арий, 2008. – Том II. Информационная безопасность. – 344 с., ил.

ISBN 978-966-498-21-7.

ISBN 978-966-498-23-1 (т.2)

Книга предназначена широкому кругу читателей: от технического специалиста, связанного с использованием средств защиты информации, до рядового пользователя современными информационными технологиями.

Однако наиболее полезна она будет специалистам в области защиты информации в автоматизированных системах и системах связи, специалистам по организации комплексной защиты информации как государственных так и коммерческих структур, а также руководителям предприятий, учреждений и организаций.

Даную монографию можно рассматривать как учебник по направлению «Информационная безопасность» для студентов и аспирантов.

Краткое оглавление

ТОМ I. НЕСАНКЦИОНИРОВАННОЕ ПОЛУЧЕНИЕ ИНФОРМАЦИИ

Введение	11
Часть I. История и основные принципы разведки	12
Глава 1. Разведка с точки зрения защиты информации и основные принципы разведки.....	13
Глава 2. Краткий очерк истории возникновения и развития разведки.....	22
Часть II. Каналы утечки информации	47
Глава 3. Каналы несанкционированного получения информации	48
Глава 4. Классификация радиоканалов утечки информации	70
Глава 5. Классификация акустических каналов утечки информации	121
Глава 6. Классификация электрических каналов утечки информации	150
Глава 7. Классификация визуально-оптических каналов утечки информации.....	181
Глава 8. Классификация материально-вещественных каналов утечки информации	184
Глава 9. Линии связи	203
Часть III. Методы и средства несанкционированного доступа к информации и ее разрушения	208
Глава 10. Угрозы информации	209
Глава 11. Каналы утечки информации при эксплуатации ЭВМ.....	236
Глава 12. Методы и средства несанкционированного получения информации по техническим каналам	274
Глава 13. Методы и средства несанкционированного получения информации из автоматизированных систем.....	307
Глава 14. Методы и средства разрушения информации.....	320
Глава 15. Вирусы. Виды и классификации	382
Литература.....	461

ТОМ II. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Введение	8
Часть IV. Защита информации	9
Глава 16. Подходы к созданию комплексной системы защиты информации	10
Глава 17. Технические методы и средства защиты информации	22
Глава 18. Программные методы защиты	164
Глава 19. Криптографическая защита.....	206
Глава 20. Скремблирование	297
Глава 21. Стеганография	311
Литература.....	339

Оглавление

Введение	8
Часть IV. Защита информации	9
Глава 16. Подходы к созданию комплексной системы защиты информации	10
Общие вопросы защиты информации от утечки по техническим каналам	11
Показатели оценки информации как ресурса	13
Классификация методов и средств ЗИ	17
Семантические схемы	17
Некоторые подходы к решению проблемы ЗИ	19
Общая схема проведения работ по ЗИ	20
Глава 17. Технические методы и средства защиты информации	22
Классификация технических средств защиты	22
Технические средства защиты территории и объектов	23
Акустические средства защиты	25
Задачи построения СЗ речевой информации	47
Особенности защиты от радиозакладок	51
Методы и средства защиты от радиомикрофонов	53
Защита от встроенных и узконаправленных микрофонов	57
Поисковые средства автоматизированных мониторингов	60
Современные особенности эфирной и внутриобъектовой радиообстановки	60
Пути повышения эффективности современных средств АРМ	62
Выбор обобщенного критерия качества поисковых средств АРМ	63
Основные технические характеристики поисковых средств АРМ	64
Оценка эффективности цифрового радиоприемного устройства	65
Защита от лазерных систем акустической разведки	71
Защита линий связи	73
Способы обнаружения факта и района гальванического подключения устройств съема информации с КЛС	75
Выявление факта и обнаружение места подключения устройств съема информации	77
Электромагнитное зондирование	77
Нелинейное зондирование	81
Способы обнаружения аппаратуры перехвата информации	83
Защита волоконно-оптических линий связи от перехвата информации	90
Методы и средства защиты телефонных линий	90
Пассивная защита	91
Приборы для постановки активной заградительной помехи	101
Методы контроля проводных линий	115
Защита факсимильных и телефонных аппаратов, концентраторов	120
Методы построения проводных линий	124
Скремблеры	124
Анализаторы телефонных линий	125
Односторонние маскираторы речи	127
Экранирование помещений	128
Защита от НСВ по цепям питания	154
Защита от НСВ по коммуникационным каналам	157
Глава 18. Программные методы защиты	164
Стратегия защиты информации в КС	168
Основные принципы построения систем защиты информации в АС	177
Программные средства защиты информации	178
Программы внешней защиты	180
Программы внутренней защиты	182
Простое опознавание пользователя	183
Усложненная процедура опознавания	184
Методы особого надежного опознавания	185
Методы опознавания АС и ее элементов пользователем	186
Проблемы регулирования использования ресурсов	186
Программы защиты программ	189

Защита от копирования	190
Программы ядра системы безопасности	191
Программы контроля	192
Подход к программной реализации оценки агрессивности программных средств	192
Метод определения факта информационного вторжения	196
Вычисление вероятности обнаружения изменений в контролируемых данных	200
Основные свойства алгоритма	201
Экспериментальная проверка алгоритма	202
Использование информационного следа при поиске программных закладок	204
Глава 19. Криптографическая защита	206
Основные понятия	206
Немного истории	208
Классификация криптографических методов	211
Требования к криптографическим методам защиты информации	214
Математика разделения секрета	215
Разделение секрета для произвольных структур доступа	217
Линейное разделение секрета	220
Идеальное разделение секрета и матрицы	222
Секретность и имитостойкость	224
Проблема секретности	225
Проблема имитостойкости	226
Безусловная и теоретическая стойкость	226
Криптографические алгоритмы	229
Криптографические алгоритмы для экспорта	230
Шифрование в каналах связи компьютерной сети	231
Канальное шифрование	232
Сквозное шифрование	232
Комбинированное шифрование	233
Шифрование файлов	233
Аппаратное и программное шифрование	235
Аппаратное шифрование	235
Программное шифрование	236
Сжатие и шифрование	236
Анализ основных криптографических методов ЗИ	237
Классификация криптографических методов	237
Системы подстановок	238
Шифрование методом подстановки (замены)	240
Многоалфавитные системы. Системы одноразового использования	241
Шифрование методом перестановки	243
Шифрование простой перестановкой	243
Усложненный метод перестановки по таблицам	243
Усложненный метод перестановок по маршрутам	244
Шифрование с помощью аналитических преобразований	244
Шифрование методом гаммирования	246
Комбинированные методы шифрования	247
Криптосистемы на основе эллиптических уравнений	248
Кодирование	248
Шифрование с открытым ключом	249
Эллиптические функции — реализация метода открытых ключей	252
Системы с открытым ключом	252
Цифровая подпись	254
Криптографическая система RSA	255
Необходимые сведения из элементарной теории чисел	256
Алгоритм RSA	257
Цифровая (электронная) подпись на основе криптосистемы RSA	264
Стандарт шифрования данных DES	265
Принцип работы блочного шифра	265
Процедура формирования подключей	267
Механизм действия S -блоков	268
Другие режимы использования алгоритма шифрования DES	280
Стандарт криптографического преобразования данных ГОСТ 28147-89	280
Структурный метод (метод белого или стеклянного ящика)	284

Поведенческий метод «черного ящика».....	284
Метод регрессивного тестирования.....	285
Информирует АИС.....	286
Метод «серого ящика».....	286
Метод опытной эксплуатации.....	286
Тестирование эргономичности.....	287
Методология тестирования криптографических программных систем.....	287
Исследование.....	288
Планирование тестирования.....	288
Подготовка.....	294
Тестирование.....	294
Анализ результатов тестирования.....	295
Глава 20. Скремблирование.....	297
Аналоговые скремблеры.....	298
Аналоговое скремблирование.....	300
Цифровое скремблирование.....	305
Критерии оценки систем закрытия речи.....	308
Глава 21. Стеганография.....	311
Стеганографические технологии.....	312
Классификация стеганографических методов.....	313
Классификация стегосистем.....	315
Безключевые стегосистемы.....	315
Стегосистемы с секретным ключом.....	316
Стегосистемы с открытым ключом.....	317
Смешанные стегосистемы.....	317
Классификация методов сокрытия информации.....	318
Текстовые стеганографы.....	320
Методы искажения формата текстового документа.....	321
Синтаксические методы.....	324
Семантические методы.....	324
Методы генерации стеганограмм.....	325
Сокрытие данных в изображении и видео.....	328
Методы замены.....	328
Методы сокрытия в частотной области изображения.....	331
Широкополосные методы.....	332
Статистические методы.....	333
Методы искажения.....	335
Структурные методы.....	335
Сокрытие информации в звуковой среде.....	337
Стеганографические методы защиты данных в звуковой среде.....	337
Музыкальные стегосистемы.....	338
Литература.....	339