

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

# МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

ТОМ I

## НЕСАНКЦИОНИРОВАННОЕ ПОЛУЧЕНИЕ ИНФОРМАЦИИ

- 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.

**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 I. Несанкционированное получение информации. – 464 с., ил.

ISBN 978-966-498-21-7.

ISBN 978-966-498-22-4 (т.1)

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.

ЛЕНКОВ Сергій Васильович  
ПЕРЕГУДОВ Дмитро Олександрович  
ХОРОШКО Володимир Олексійович

784716

**Методи і засоби захисту інформації**

**ТОМ I**

**Несанкціоноване отримання інформації**

*Російською мовою*

Підписано до друку 30.07.08. Формат 70x100/16. Папір офсетний. Гарнітура “Times”.  
Друк офсетний. Умовн.-друк. арк 37,7. Тираж 4000. Зам.5172

«Видавництво “Арій”», Київ, пр. 50-річчя Жовтня, 2-Б, т. 537-2920  
E-mail: ariy@optima.com.ua

Свідоцтво Держкомінформу України ДК № 1727, від 25.03.2004.

ТОВ “Фактор-Друк”, 61030, м. Харків, вул. Саратовська, 51  
тел. 8(057)7-175-185

# Краткое оглавление

## ТОМ I. НЕСАНКЦИОНИРОВАННОЕ ПОЛУЧЕНИЕ ИНФОРМАЦИИ

Введение .....	11
<b>Часть I. История и основные принципы разведки .....</b>	<b>12</b>
Глава 1. Разведка с точки зрения защиты информации и основные принципы разведки .....	13
Глава 2. Краткий очерк истории возникновения и развития разведки.....	22
<b>Часть II. Каналы утечки информации.....</b>	<b>47</b>
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
<b>Часть III. Методы и средства несанкционированного доступа к информации и ее разрушения .....</b>	<b>208</b>
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
<b>Часть IV. Защита информации.....</b>	<b>9</b>
Глава 16. Подходы к созданию комплексной системы защиты информации.....	10
Глава 17. Технические методы и средства защиты информации.....	21
Глава 18. Программные методы защиты .....	162
Глава 19. Криптографическая защита.....	204
Глава 20. Скремблирование.....	295
Глава 21. Стеганография.....	309
Литература .....	339

# Оглавление

Введение.....	11
<b>Часть I. История и основные принципы разведки .....</b>	<b>12</b>
Глава 1. Разведка с точки зрения защиты информации и основные принципы разведки .....	13
Глава 2. Краткий очерк истории возникновения и развития разведки.....	22
История разведки и контрразведки .....	22
Украинская разведка.....	31
Радиоразведка .....	33
Радиоразведка во время Второй мировой войны .....	36
Разведка конца XX века .....	41
<b>Часть II. Каналы утечки информации.....</b>	<b>47</b>
Глава 3. Каналы несанкционированного получения информации .....	48
Технические каналы утечки информации. Классификация, причины и источники образования .....	48
Обобщенная модель технического канала утечки информации .....	52
Сигнал и его описание.....	53
Сигналы с помехами.....	56
Излучатели электромагнитных колебаний .....	58
Низкочастотные излучатели .....	59
Высокочастотные излучатели.....	60
Оптические излучатели .....	62
Глава 4. Классификация радиоканалов утечки информации .....	70
Образование радиоканалов утечки информации.....	70
Электрическое поле.....	72
Магнитное поле .....	76
Электромагнитное поле .....	83
Оценка электромагнитных полей.....	89
Аналитическое представление электромагнитной обстановки .....	92
Обнаружение сигналов в условиях воздействия непреднамеренных помех.....	97
Обнаружение сигнала при детерминированной помехе.....	99
Обнаружение сигнала при квазидетерминированной помехе .....	105
Обнаружение сигнала при случайной и групповой помехах .....	110
Оценка параметров сигналов в условиях воздействия непреднамеренных помех .....	114
Обеспечение электромагнитной обстановки при применении радиосредств безопасности.....	117
Глава 5. Классификация акустических каналов утечки информации.....	121
Основные определения акустики .....	121
Распространение звука в пространстве.....	124
Акустическая классификация помещений .....	126
Физическая природа, среда распространения и способ перехвата.....	127
Заходовые методы .....	129
Перехват акустической информации с помощью радиопередающих средств .....	129
Перехват акустической информации с помощью ИК передатчиков.....	129
Закладки, использующие в качестве канала передачи акустической информации сеть 220 В и телефонные линии.....	129
Диктофоны .....	129
Проводные микрофоны .....	130
“Телефонное ухо” .....	130
Беззаходовые методы .....	130
Аппаратура, использующая микрофонный эффект телефонных аппаратов .....	130
Аппаратура ВЧ навязывания.....	130
Стетоскопы.....	133
Лазерные системы акустической разведки .....	134
Направленные акустические микрофоны (НАМ).....	135
Физические преобразователи.....	136
Характеристики физических преобразователей.....	136

## 6 Оглавление

Воздействие опасных акустических сигналов на технические системы (ТС) .....	138
Электростатическая система .....	140
Электродинамическая система .....	141
Электромагнитная система .....	141
Механострикционная система .....	142
Пьезоэлектрическая система .....	143
Акустоэлектрические преобразователи .....	145
Индуктивные преобразователи .....	146
Микрофонный эффект электромеханического звонка телефонного аппарата .....	147
Микрофонный эффект громкоговорителей .....	148
Микрофонный эффект вторичных электрочасов .....	149
<b>Глава 6. Классификация электрических каналов утечки информации .....</b>	<b>150</b>
Схемы электроснабжения технических средств и систем информатизации .....	150
Тракты распространения информативных сигналов в каналах утечки информации .....	152
Затухание и другие параметры силовых кабелей .....	153
Затухание и другие параметры трансформаторных подстанций и распределительных пунктов .....	155
Затухание участков трактов распространения информативных сигналов в каналах утечки информации .....	158
Паразитные связи и наводки .....	167
Паразитные емкостные связи .....	172
Паразитные индуктивные связи .....	173
Паразитные электромагнитные связи .....	173
Паразитная высокочастотная генерация в усилительных каскадах .....	174
Паразитные электромеханические связи .....	175
Утечка информации по цепям заземления .....	175
Утечка информации по цепям электропитания .....	178
Паразитные обратные связи через источники питания .....	179
<b>Глава 7. Классификация визуально- оптических каналов утечки информации .....</b>	<b>181</b>
Визуально-оптическое наблюдение .....	181
<b>Глава 8. Классификация материально-вещественных каналов утечки информации .....</b>	<b>184</b>
Радиационные и химические методы получения информации .....	186
Основные источники переноса информации в материально-вещественном плане .....	197
Технические средства радиационной разведки .....	199
<b>Глава 9. Линии связи .....</b>	<b>203</b>
Классификация каналов и линий связи .....	203
Взаимные влияния в линиях связи .....	205
<b>Часть III. Методы и средства несанкционированного доступа к информации и ее разрушения .....</b>	<b>208</b>
<b>Глава 10. Угрозы информации .....</b>	<b>209</b>
Модель угроз информации, которая обрабатывается в локальной сети .....	209
Общая классификация угроз информации .....	209
Угрозы информации, которая циркулирует в центральном узле АС .....	211
Модель угроз информации для узла Интернет при проведении типовых удаленных атак .....	218
Анализ сетевого трафика сети Интернет .....	218
Ложный ARP-сервер в сети Интернет .....	219
Ложный DNS-сервер в сети Интернет .....	219
Внедрение в сеть Интернет ложного DNS-сервера путем перехвата DNS-запроса .....	220
Внедрение в сеть Интернет ложного сервера путем создания направленного "шторма" ложных DNS-ответов на атакуемый хост .....	220
Внедрение в сеть Интернет ложного сервера путем перехвата DNS-запроса или создания направленного "шторма" ложных DNS-ответов на атакуемый DNS-сервер .....	221
Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания в сети Интернет ложного маршрутизатора .....	221
Подмена одного из субъектов TCP-соединения в сети Интернет (hijacking) .....	222
Нарушение работоспособности хоста в сети Интернет при использовании направленного "шторма" ложных TCP-запросов на создание соединения, либо при переполнении очереди запросов .....	223
Сетевые атаки .....	227
Снифферы пакетов .....	228
IP-спуфинг .....	229

Отказ в обслуживании (Denial of Service — DoS).....	230
Парольные атаки.....	232
Атаки типа Man-in-the-Middle.....	232
Атаки на уровне приложений.....	233
Сетевая разведка.....	234
Злоупотребление доверием.....	234
Переадресация портов.....	235
Несанкционированный доступ.....	235
<b>Глава 11. Каналы утечки информации при эксплуатации ЭВМ.....</b>	<b>236</b>
Виды и природа каналов утечки информации при эксплуатации ЭВМ.....	236
Анализ возможности утечки информации через ПЭМИ.....	238
Элементарный электрический излучатель (особенности электромагнитного поля в непосредственной близости от источника).....	240
Решение уравнений Максвелла для элементарного магнитного излучателя.....	244
Реальные непреднамеренные излучатели электрического поля ТС.....	246
Реальные магнитные излучатели электромагнитного поля.....	248
Экспериментальная проверка законов убывания электромагнитного поля от модели излучателя и реальных ТС.....	249
Способы обеспечения ЗИ от утечки через ПЭМИ.....	251
Механизм возникновения ПЭМИ средств цифровой электронной техники.....	253
Техническая реализация устройств маскировки.....	253
Устройство обнаружения радиомикрофонов.....	254
Обнаружение записывающих устройств (диктофонов).....	255
Физические принципы.....	255
Спектральный анализ.....	257
Распознавание событий.....	258
Многоканальная фильтрация.....	258
Оценка уровня ПЭМИ.....	259
Метод оценочных расчетов.....	261
Метод принудительной активизации.....	262
Метод эквивалентного приемника.....	262
Методы измерения уровня ПЭМИ.....	262
Ближняя зона.....	265
Дальняя зона.....	265
Промежуточная зона.....	265
Тестовые режимы устройств.....	267
Сигналы, подлежащие измерениям, требования к их параметрам в тест-режиме.....	267
Спектр сигналов и особенности учета его структуры.....	269
Спектр сигналов в низкочастотной области.....	270
Распознавание сигналов.....	270
Детектирование и измерения.....	270
Измерения в линиях.....	272
Измерения с помощью эквивалентов сети.....	272
Измерения с помощью токовых трансформаторов.....	272
Измерения с помощью пробников.....	272
<b>Глава 12. Методы и средства несанкционированного получения информации по техническим каналам.....</b>	<b>274</b>
Средства несанкционированного получения информации.....	274
Средства проникновения.....	275
Устройства прослушивания помещений.....	276
Радиозакладки.....	279
Технические методы защиты каналов утечки информации по электросети.....	280
Устройства для прослушивания телефонных линий.....	282
Методы и средства подключения.....	284
Каналы утечки речевой информации при использовании телефонных аппаратов и методы их закрытия.....	284
Перехват информации с подземных кабельных линий связи.....	292
Перехват информации с полевых кабельных линий связи (КЛС).....	297
Методы и средства удаленного получения информации.....	298
Дистанционный направленный микрофон.....	298
Системы скрытого видеонаблюдения.....	299
Акустический контроль помещений через средства телефонной связи.....	299
Перехват электромагнитных излучений.....	305

Глава 13. Методы и средства несанкционированного получения информации из автоматизированных систем.....	307
Несанкционированное получение информации из АС.....	307
Классификация.....	308
Локальный доступ.....	311
Удаленный доступ.....	315
Сбор информации.....	315
Сканирование.....	316
Идентификация доступных ресурсов.....	317
Получение доступа.....	317
Расширение полномочий.....	318
Исследование системы и внедрение.....	318
Соккрытие следов.....	318
Создание тайных каналов.....	319
Блокирование.....	319
Глава 14. Методы и средства разрушения информации.....	320
Помехи.....	320
Намеренное силовое воздействие.....	323
Намеренное силовое воздействие по сетям питания.....	326
Технические средства для НСВ по сети питания.....	329
Намеренное силовое воздействие по коммуникационным сетям и каналам.....	334
Технические средства для НСВ по проводным линиям связи.....	334
Вирусные методы разрушения информации.....	340
Программное подавление вычислительных систем.....	343
Разрушающие программные средства.....	350
Негативное воздействие закладки на программу.....	351
Модель информационных угроз программным средствам компьютеризированных образцов техники.....	353
Программные закладки в контексте модели угроз системам.....	367
Вербальная модель программной закладки.....	367
Возможный подход к классификации программных закладок.....	368
Сохранение фрагментов информации.....	373
Перехват вывода на экран.....	373
Перехват ввода с клавиатуры.....	374
Перехват и обработка файловых операций.....	377
Разрушение программы защиты и схем контроля.....	379
Глава 15. Вирусы. Виды и классификации.....	382
Определение термина «компьютерный вирус».....	382
Правовой статус.....	389
Файловые вирусы.....	394
Overwriting-вирусы.....	395
Parasitic-вирусы.....	395
Companion-вирусы.....	398
Link-вирусы.....	399
Файловые черви.....	400
OBJ-, LIB-вирусы и вирусы в исходных текстах.....	401
Алгоритм работы файлового вируса.....	401
Особые случаи.....	402
Загрузочные вирусы.....	403
Макровирусы.....	406
Word-, Excel-, Office 97-вирусы.....	407
Алгоритм работы Word-макровирусов.....	410
Алгоритм работы Excel-макровирусов.....	411
AmiPro-вирусы.....	411
Сетевые вирусы.....	412
Прочие вредные программы.....	413
"Троянские кони" (логические бомбы).....	413
Intended-вирусы.....	413
Конструкторы вирусов.....	414
Полиморфные генераторы.....	414
Резидентные вирусы.....	414
DOS-вирусы.....	415
Загрузочные вирусы.....	416

Windows-вирусы.....	417
Макровирусы.....	417
"Стелс"-вирусы.....	418
Загрузочные вирусы.....	418
Файловые вирусы.....	419
Макровирусы.....	419
Полиморфик-вирусы.....	419
Полиморфные расшифровщики.....	420
Уровни полиморфизма.....	421
Изменение выполняемого кода.....	421
Backdoor (утилиты скрытого администрирования).....	422
HTML-вирусы.....	424
Основные источники заражения компьютерными вирусами.....	425
Теория вирусологии.....	425
Классификация компьютерных вирусов.....	430
Теория обнаружения компьютерных вирусов.....	430
Современная ситуация.....	430
Если компьютер заражен или есть подозрения.....	431
Обнаружение неизвестного вируса.....	431
Самое первое правило - не паниковать.....	431
Классические вирусы.....	431
Среда обитания.....	432
Способ заражения.....	432
Файловые вирусы.....	432
Перезаписывающие.....	432
Паразитические.....	432
Companion.....	433
Прочие способы заражения.....	433
Загрузочные вирусы.....	434
Макро-вирусы.....	434
Скрипт-вирусы.....	435
Обнаружение файлового вируса.....	435
Обнаружение макро-вируса.....	436
Сетевые черви.....	436
Email-Worm - почтовые черви.....	436
IM-Worm— черви, использующие интернет-пейджеры.....	437
IRC-Worm — черви в IRC-каналах.....	437
Net-Worm - прочие сетевые черви.....	438
P2P-Worm — черви для файлообменных сетей.....	438
Троянские программы.....	438
Backdoor - троянские утилиты удаленного администрирования.....	438
Trojan-PSW - воровство паролей.....	439
Trojan-Clicker - Интернет-кликеры.....	439
Trojan-Downloader - доставка прочих вредоносных программ.....	439
Trojan-Dropper - инсталляторы прочих вредоносных программ.....	440
Trojan-Proxu - троянские прокси-сервера.....	440
Trojan-Spy - шпионские программы.....	440
Trojan - прочие троянские программы.....	440
Rootkit - сокрытие присутствия в операционной системе.....	441
ArcBomb – «бомбы» в архивах.....	441
Trojan-Notifier – оповещение об успешной атаке.....	441
Повторное заражение.....	443
Macro-вирусы (MS-Word, Excel, Access, PowerPoint и Amipro).....	443
Macro-вирусы.....	444
Word/Excel-вирусы.....	445
AmiPro-вирусы.....	445
Юникс - подобные системы.....	446
Особенности работы «инфицированных компьютеров».....	446
Проблемы антивирусной защиты информации.....	447
Правила компьютерной гигиены.....	449
Общая характеристика антивирусных программ для защиты рабочей станции. Введение в антивирусные программы.....	449
Типы антивирусов.....	449



## 10 Оглавление

---

Сканеры.....	449
Ревизоры .....	450
Резидентные мониторы.....	450
Иммунизаторы.....	451
Планировщик заданий.....	451
Постулаты построения КСАЗ в ЛВС.....	453
Правила антивирусной защиты ЛВС.....	454
Типы АВПО применяемые для построения КСАЗ.....	455
Локализация "вирусной инфекции" в компьютерных системах.....	455
Методики противодействия вирусам.....	455
Резервное копирование.....	456
Переход на защищенные операционные системы.....	456
Уменьшение привилегий пользователей до минимума.....	457
Сокращение избыточной функциональности программ.....	457
Мониторинг изменения файлов.....	458
Контроль за обращениям к файлам.....	458
Контроль за состоянием системы.....	459
Ненормальная сетевая активность.....	459
Анализ полученных из сети файлов.....	460
Методики удаления.....	460
Литература.....	461