

А.П.Зайцев, Р.В.Мещеряков, А.А.Шелупанов

ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

7-е издание

*Рекомендовано Министерством образования и науки
Российской Федерации в качестве учебника
для студентов высших учебных заведений,
обучающихся по группе специальностей –
«Информационная безопасность»*

Москва
Горячая линия - Телеком
2012

УДК 681.3.067

ББК 32.81

3-17

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

Зайцев А. П., Мещеряков Р. В., Шелупанов А. А.,

3-17 Технические средства и методы защиты информации. Учебник для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков. Под ред. А. П. Зайцева и А. А. Шелупанова. – 7-е изд., испр. – М.: Горячая линия–Телеком, 2012. – 442 с: ил.

ISBN 978-5-9912-0233-6.

Изложены вопросы защиты информации техническими средствами. Приведена классификация наиболее важных технических каналов утечки информации, имеющих место в реальных условиях. Значительное внимание уделено физической природе появления информационных сигналов в электромагнитных, электрических, акустических и виброакустических каналах утечки информации. Подробно рассмотрены средства выявления технических каналов утечки информации и защиты информации от утечки. Отдельный раздел посвящен техническим средствам защиты объектов. Рассмотрены вопросы технического контроля эффективности мер защиты информации и аттестации объектов информатизации.

Для студентов вузов, обучающихся по направлению подготовки «Информационная безопасность», будет полезна слушателям курсов профессиональной переподготовки и специалистам.

ББК 32.81

Адрес издательства в Интернет www.techbook.ru

Учебное издание

**Зайцев Александр Петрович, Мещеряков Роман Валерьевич,
Шелупанов Александр Александрович**

Технические средства и методы защиты информации
Учебник для вузов

Обложка художника В. Г. Ситникова

Подписано в печать 30.06.2012. Печать офсетная. Формат 60×90/16. Уч. изд. л. 27,63
ООО «Научно-техническое издательство «Горячая линия–Телеком»

ISBN 978-5-9912-0233-6

© А. П. Зайцев, Р. В. Мещеряков,
А. А. Шелупанов, 2012

© Издательство «Горячая линия–Телеком», 2012

СОДЕРЖАНИЕ

Введение	8
В-1. Виды, источники и носители защищаемой информации.....	8
В-2. Классификация иностранной технической разведки.	
Возможности видов технической разведки.....	14
В-3. Основные этапы и процедуры добывания информации	
технической разведкой	20
В-4. Задачи систем защиты информации	24
1. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ	25
1.1. Общие понятия	25
1.2. Технические каналы утечки информации.	
Структура, классификация и основные характеристики	26
1.3. Технические каналы утечки информации, обрабатываемой ТСПИ.	30
1.3.1. Физическая природа побочных электромагнитных излучений.	
Основные уравнения электромагнитного поля.....	31
1.3.2. Элементарный электрический излучатель	39
1.3.3. Элементарный магнитный излучатель	42
1.3.4. Электромагнитные каналы утечки информации ТСПИ	44
1.3.5. Электрические каналы утечки информации	47
1.3.5.1. <i>Наводки электромагнитных излучений ТСПИ</i>	47
1.3.6. Параметрический канал утечки информации	51
1.4. Технические каналы утечки информации при передаче ее	
по каналам связи	51
1.4.1. Электрические линии связи	51
1.4.1.1. <i>Средства передачи электрических сигналов</i>	51
1.4.1.2. <i>Виды проводных электрических линий связи</i>	
<i>и их параметры</i>	52
1.4.2. Каналы утечки информации за счет паразитных связей	56
1.4.2.1. <i>Опасные сигналы и их источники</i>	56
1.4.3. Электрические каналы утечки информации	61
1.4.3.1. <i>Контроль и прослушивание телефонных каналов связи</i>	61
1.4.4. Электромагнитные каналы утечки информации	68
1.4.5. Индукционный канал утечки информации	68
1.5. Технические каналы утечки речевой информации	68
1.5.1. Краткие сведения по акустике	68
1.5.1.1. <i>Звуковое поле</i>	68
1.5.1.2. <i>Линейные характеристики звукового поля</i>	69
1.5.1.3. <i>Энергетические характеристики звукового поля</i>	71
1.5.1.4. <i>Плоская волна</i>	71
1.5.1.5. <i>Сферическая волна</i>	73
1.5.1.6. <i>Акустические и электрические уровни</i>	75

1.5.1.7. Звуковые сигналы.....	76
1.5.1.8. Маскировка звуковых сигналов	79
1.5.2. Понятность и разборчивость речи	84
1.5.3. Частотный диапазон и спектры	87
1.5.4. Звуковое поле в помещении	89
1.5.5. Звуковой фон в помещении.....	90
1.5.6. Характеристики помещения.....	90
1.5.7. Звукопоглощающие материалы и конструкции.....	91
1.5.8. Звукоизоляция помещений.....	93
1.5.9. Акустические каналы утечки речевой информации.....	97
1.5.9.1. Микрофоны	97
1.5.9.2. Направленные микрофоны	99
1.5.9.3. Проводные системы, портативные диктофоны и электронные стетоскопы.....	104
1.5.9.4. Радиомикрофоны	107
1.5.9.5. Гидроакустические датчики	109
1.5.9.6. СВЧ- и ИК-передатчики.....	109
1.5.10. Виброакустические технические каналы утечки речевой информации	110
1.5.11. Акустоэлектрические каналы утечки речевой информации	110
1.5.12. Оптико-электронный технический канал утечки речевой информации.....	111
1.5.13. Параметрические технические каналы утечки речевой информации.....	113
1.6. Технические каналы утечки видовой информации	115
1.6.1. Способы скрытого видеонаблюдения и съемки.....	115
Вопросы для самопроверки.....	123
2. ДЕМАСКИРУЮЩИЕ ПРИЗНАКИ ОБЪЕКТОВ.....	125
2.1. Общие положения	125
2.2. Демаскирующие признаки объектов.....	126
2.3. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра.....	127
2.4. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра.....	131
2.5. Демаскирующие признаки радиоэлектронных средств	132
Вопросы для самопроверки.....	134
3. СРЕДСТВА ВЫЯВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ	135
3.1. Общие сведения.....	135
3.2. Индикаторы электромагнитного поля.....	139
3.3. Сканирующие радиоприемники	141
3.4. Анализаторы спектра, радиочастотомеры	143

3.5. Многофункциональные комплекты для выявления каналов утечки информации.....	146
3.5.1. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки ПКУ-6М.....	146
3.5.2. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья»	154
3.6. Комплекс RS turbo	163
3.7. Комплексы измерения ПЭМИН	167
3.8. Нелинейные локаторы	173
3.9. Комплекс для измерения характеристик акустических сигналов «Спрут-7»	180
3.10. Металлодетекторы	183
3.11. Портативная рентгенотелевизионная установка «НОРКА».....	193
3.12. Досмотровые эндоскопы	194
Вопросы для самопроверки.....	196
4. СКРЫТИЕ И ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ	197
4.1. Концепция и методы инженерно-технической защиты информации	197
4.2. Экранирование электромагнитных волн	201
4.2.1. Электромагнитное экранирование и развязывающие цепи.....	201
4.2.2. Подавление емкостных паразитных связей	204
4.2.3. Подавление индуктивных паразитных связей	204
4.2.4. Экранирование проводов и катушек индуктивности.....	206
4.2.5. Экранированные помещения	213
4.3. Безопасность оптоволоконных кабельных систем	217
4.4. Заземление технических средств и подавление информационных сигналов в цепях заземления	224
4.5. Фильтрация информационных сигналов	225
4.5.1. Основные сведения о помехоподавляющих фильтрах	225
4.5.2. Выбор типа фильтра	233
4.6. Пространственное и линейное зашумление	235
4.7. Способы предотвращения утечки информации через ПЭМИН ПК	237
4.8. Устройства контроля и защиты слаботочных линий и сети.....	240
4.8.1. Особенности слаботочных линий и сетей как каналов утечки информации.....	240
4.8.2. Рекомендуемые схемы подключения анализаторов к электросиловым и телефонным линиям в здании	241
4.8.3. Устройства контроля и защиты проводных линий от утечки информации.....	243

4.9. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам	252
4.10. Скрытие речевой информации в телефонных системах с использованием криптографических методов.....	256
4.11. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах	264
4.11.1. Secret Net 5.0.....	264
4.11.2. Электронный замок «Соболь»	270
4.11.3. USB-ключ.....	273
4.11.4. Считыватели Proximity	276
4.11.5. Технология защиты информации на основе смарт-карт.....	278
4.11.6. Кейс «Тень»	280
4.11.7. Устройство для быстрого уничтожения информации на жестких магнитных дисках «Стек-Н»	281
Вопросы для самопроверки.....	282
5. МЕТОДЫ И СРЕДСТВА ИНЖЕНЕРНОЙ ЗАЩИТЫ И ТЕХНИЧЕСКОЙ ОХРАНЫ ОБЪЕКТОВ.....	284
5.1. Категории объектов защиты	284
5.2. Особенности задач охраны различных типов объектов.....	284
5.3. Общие принципы обеспечения безопасности объектов	287
5.4. Система охранно-тревожной сигнализации	287
5.5. Система контроля и управления доступом.....	295
5.6. Телевизионные системы	300
5.7. Система пожарной сигнализации	306
5.8. Периметровая охрана.....	310
Вопросы для самопроверки.....	323
6. АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ	324
6.1. Общие сведения.....	324
6.2. Мероприятия по выявлению и оценке свойств каналов утечки информации	329
6.2.1. Специальные проверки	330
6.2.2. Специальные обследования	332
6.2.3. Специальные исследования	342
6.2.3.1. Специальные исследования акустических и виброакустических каналов	343
6.2.3.2. Специальные исследования акустоэлектрических преобразований.....	359
6.2.3.3. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок	365
Вопросы для самопроверки.....	372

7. ТЕХНИЧЕСКИЙ КОНТРОЛЬ ЭФФЕКТИВНОСТИ МЕР ЗАЩИТЫ ИНФОРМАЦИИ	373
7.1. Цели и задачи технического контроля эффективности мер защиты информации	373
7.2. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ	376
7.3. Методы испытаний ПЭВМ	382
7.4. Порядок проведения контроля защищенности АС от НСД	388
7.5. Методы контроля побочных электромагнитных излучений генераторов технических средств	389
7.6. Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации	394
7.6.1. Общие положения	394
7.6.2. Подготовительный этап контроля	396
7.6.3. Акустический и виброакустический контроль	398
7.6.3.1. Методика контроля	398
7.6.3.2. Выбор контрольных точек и размещение элементов измерительных комплексов	399
7.6.3.3. Калибровка передающего измерительного комплекса	401
7.6.3.4. Размещение акустического излучателя передающего измерительного комплекса	402
7.6.3.5. Измерение отношений «сигнал/шум» в контрольных точках при инструментальном контроле рабочих помещений, не оборудованных системой звукоусиления	402
7.6.3.6. Измерение отношений «сигнал/шум» в контрольных точках при инструментальном контроле рабочих помещений, оборудованных системой звукоусиления	403
7.6.4. Контроль технических средств и систем на наличие акустоэлектрических преобразований	404
7.6.4.1. Подготовительный этап контроля	404
7.6.4.2. Методика контроля	405
Вопросы для самопроверки	406
ЛИТЕРАТУРА	408
Приложения	411
Приложение 1	411
Приложение 2	416
Приложение 3	421
Приложение 4	433

ВВЕДЕНИЕ

В-1. Виды, источники и носители защищаемой информации

Значение информации в жизни любого цивилизованного общества непрерывно возрастает. С незапамятных времен сведения, имеющие важное военно-стратегическое значение для государства, тщательно скрывались и защищались. В настоящее время информация, относящаяся к технологии производства и сбыта продукции, стала рыночным товаром, имеющим большой спрос как на внутреннем, так и на внешнем рынках. Информационные технологии постоянно совершенствуются в направлении их автоматизации и способов защиты информации.

Развитие новых информационных технологий сопровождается такими негативными явлениями, как промышленный шпионаж, компьютерные преступления и несанкционированный доступ (НСД) к секретной и конфиденциальной информации. Поэтому защита информации является важнейшей государственной задачей в любой стране. Острая необходимость в защите информации в России нашла выражение в создании Государственной системы защиты информации (ГСЗИ) и в развитии правовой базы информационной безопасности. Приняты и введены в действие законы «О государственной тайне», «Об информации, информатизации и защите информации», «О правовой охране программ для электронных вычислительных машин и баз данных», «Доктрина информационной безопасности Российской Федерации» и др.

Защита информации должна обеспечивать предотвращение ущерба в результате утери (хищения, утраты, искажения, подделки) информации в любом ее виде. Организация мер защиты информации должна проводиться в полном соответствии с действующими законами и нормативными документами по безопасности информации, интересами пользователей информации. Чтобы гарантировать высокую степень защиты информации, необходимо постоянно решать сложные научно-технические задачи разработки и совершенствования средств ее защиты.

Большинство современных предприятий независимо от вида деятельности и форм собственности не может успешно вести хозяйственную и иную деятельность без обеспечения системы защиты своей информации, включающей организационно-нормативные меры и технические средства контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах (АС).

В Законе РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и в ст. 2 Федерального Закона «Об участии в международном информационном обмене» приводятся следующие определения информации и ее конкретных разновидностей:

- информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

- документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

- информация о гражданах (персональные данные) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

- конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

В более общем смысле информация – это сведения об окружающем мире, которые являются объектом хранения, преобразования, передачи и использования для определенных целей. Согласно этому определению человек находится в постоянно изменяющемся информационном поле, влияющем на его образ жизни и действия.

По своему характеру информация может быть политической, военной, экономической, научно-технической, производственной или коммерческой, а также секретной, конфиденциальной или несекретной.

Согласно законодательному определению конфиденциальная информация должна быть документированной и иметь ограниченный доступ в соответствии с законодательством Российской Федерации. Под такое определение попадает любая защищаемая информация, однако на практике принято защищаемую информацию разделять в зависимости от степени ее конфиденциальности.

По степени конфиденциальности (степени ограничения доступа) в настоящее время можно классифицировать только секретную информацию, составляющую государственную тайну. Согласно ст. 8 Закона РФ «О государственной тайне» устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

В соответствии со ст. 2 Закона РФ «О государственной тайне», государственная тайна – вид секретной информации, содержащей защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

К служебной тайне относятся охраняемые государством сведения в любой области науки, техники, производства и управления, разглашение кото-