Г. А. Бузов

Защита информации ограниченного доступа от утечки по техническим каналам



Горячая линия–Телеком

Оглавление

Предисловие 3
Введение 5
Глава 1. ХАРАКТЕРИСТИКИ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ 9
1.1. Модель технического канала утечки 10
1.2. Потенциально возможные технические каналы утечки информации 14
1.2.1. Технические каналы утечки речевой информации (акустическая речевая разведка) 15
1.2.2. Технические каналы утечки вибрационной информации (акустическая сигнальная разведка) 22
1.2.3. Канал побочных электромагнитных излучений и наводок (разведка ПЭМИН) 23
1.2.4. Технические каналы утечки видовой информации (оптико-электронная, визуальная оптическая, фотографическая разведка) 26
1.2.5. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники 27
1.3. Теоретические основы функционирования типовых технических каналов утечки информации 29
1.3.1. Основы теории электромагнитного поля 29
1.3.2. Основы прикладной акустики 35
1.3.3. Основы процессов модуляции и возникновения ПВЧГ 45
1.4. Закладочные устройства и защита информации от них 50
1.4.1. Построение и общие характеристики закладочных устройств 50
1.4.2. Радиозакладочные устройства 52
1.4.3. Радиозакладочные переизлучающие устройства 57
1.4.4. Закладочные устройства типа «длинное ухо» 61
1.4.5. Сетевые закладочные устройства 62
1.4.6. Волоконно-оптические линии связи 66
1.4.7. «Легальные» закладочные устройства 80
1.4.8. Диктофоны 81
1.4.9. Сотовые телефоны 83
1.4.10. Основные направления защиты информации от закладочных устройств 102

Контрольные вопросы для самостоятельной работы 120
Глава 2. СРЕДСТВА ОБНАРУЖЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ 122
2.1. Индикаторы электромагнитных излучений (ИП) 123
2.2. Радиочастотомеры 137
2.3. Радиоприемные устройства 141
2.3.1. Режимы работы сканирующих приемников 150
2.3.2. Рекомендации по выбору сканирующего приемника .. 151
2.4. Селективные микровольтметры, анализаторы спектра 152
2.5. Автоматизированные поисковые комплексы 159
2.5.1. Принципы функционирования комплексов 161
2.5.2. Специальное программное обеспечение 163
2.5.3. Специализированные поисковые программно-аппаратные комплексы 168
2.5.4. Мобильные поисковые комплексы 171
2.5.5. Стационарные комплексы автоматизированного обнаружения радиомикрофонов 175
2.6. Нелинейные локаторы 209
2.6.1. Принцип работы нелинейного локатора 209
2.6.2. Эксплуатационно-технические характеристики локаторов 210
2.6.3. Методика работы с локатором 212
2.6.4. Современные нелинейные локаторы 215
2.7. Досмотровая техника 223
2.7.1. Металлодетекторы 223
2.7.2. Приборы рентгеновизуального контроля 227
2.7.3. Тепловизионные приборы 235
2.7.4. Эндоскопы 239
2.7.5. Средства радиационного контроля 243
Контрольные вопросы для самостоятельной работы 246
Глава 3. ОРГАНИЗАЦИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ 248
3.1. Организационно-методические основы защиты информации 248
3.1.1. Общие требования к защите информации 248
3.1.2. Руководящие и нормативно-методические документы, регламентирующие деятельность в области защиты информации 252
3.2. Методика принятия решения на защиту от утечки информации в организации 257
3.2.1. Алгоритм принятия решения 258
3.2.2. Разработка вариантов и выбор оптимального 270

3.3. Организация защиты информации 275
Контрольные вопросы для самостоятельной работы 277
Глава 4. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ 278
4.1. Организация защиты речевой информации 278
4.1.1. Пассивные средства защиты выделенных помещений 279
4.1.2. Аппаратура и способы активной защиты помещений от утечки речевой информации 282
4.1.3. Рекомендации по выбору систем вибрационной и акустической защиты 296
4.1.4. Защита системы электропитания 301
4.1.5. Защита оконечного оборудования слаботочных линий 302
4.1.6. Защита информации, обрабатываемой техническими средствами 304
4.2. Организация защиты информации от утечки, возникающей при работе вычислительной техники, за счет ПЭМИН 307
4.2.1. Методология защиты информации от утечки за счет ПЭМИН 308
4.2.2. Некоторые особенности контроля ТКУИ для СВТ ... 311
4.2.3. Некоторые особенности ПЭМИН и контроля защищённости устройств и интерфейсов ПЭВМ 314
4.3. Организация защиты ПЭВМ от несанкционированного доступа 327
Контрольные вопросы для самостоятельной работы 341
Глава 5. МЕРОПРИЯТИЯ ПО ВЫЯВЛЕНИЮ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ 343
5.1. Комплексные специальные проверки 344
5.1.1. Порядок проведения комплексной специальной проверки 345
5.1.2. Выполнение поисковых мероприятий 361
5.1.3. Заключительный этап проверки 419
5.2. Специальные исследования 428
5.2.1. Общие положения, термины и определения 428
5.2.2. Постановка задачи на проведение специальных исследований 433
5.2.3. Содержание специальных исследований 434
5.2.4. Специальные исследования в области защиты речевой информации 437
5.2.5. Специальные исследования в области акустоэлектрических преобразований (СИ АЭП) 475
5.2.6. Особенности СИ в области акустоэлектрических преобразований 486
5.2.7. Общий порядок проведения измерения 491

5.2.8. Специальные исследования в области ВЧ навязывания (СИ ВЧН) 502
5.2.9. Специальные исследования в области ВЧ облучения (СИ ВЧО) 507
5.2.10. Специальные исследования в области защиты цифровой информации (СИ ЭВТ) 508
5.2.11. Специальные исследования побочных электромагнитных излучений и наводок 512
Контрольные вопросы для самостоятельной работы 534
Приложения 536
1. Предписание на эксплуатацию средства вычислительной техники 536
2. Предписание на эксплуатацию вспомогательных технических средств и систем (ВТСС) 541
3. Протокол инструментального контроля выполнения норм противодействия акустической речевой разведке в помещении 546
4. Таблицы результатов измерений 558
5. Вариант плана проведения комплексной специальной проверки помещений 560
6. Вариант акта проведения комплексной специальной проверки помещений 565
7. Рекомендации по повышению защищённости помещений и объектов (вариант) 568
Литература 574