

РАГОЗИН Ю.Н.

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

Учебное пособие



Санкт-Петербург, 2019



ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ	6
ГЛАВА 1. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ И СПОСОБЫ ЕЕ ПЕРЕХВАТА	7
1.1. Технические каналы утечки акустической (речевой) информации и способы ее перехвата	8
1.1.1. Акустические и акустовибрационные технические каналы утечки речевой информации	9
1.1.2. Акустоэлектрические технические каналы утечки речевой информации	13
1.1.3. Акустоэлектромагнитные (параметрические)	18
технические каналы утечки речевой информации	18
1.1.4. Акустооптические технические каналы утечки речевой информации	19
1.1.5. Способы перехвата акустической (речевой) информации из защищаемых помещений	22
1.1.6. Оценка защищенности выделенных помещений от утечки речевой конфиденциальной информации по акустическому (виброакустическому) каналу	23
1.1.7. Энергетическое скрытие акустических (речевых) сигналов	29
1.1.8. Виды акустических материалов и их свойства	30
1.1.9. Активные средства противодействия подслушиванию	39
1.2. Утечка информации по каналу побочных электромагнитных излучений и наводок	42
1.2.1. Электромагнитные каналы утечки информации	45
1.2.2. Электрические каналы утечки информации	46
1.2.3. Способы перехвата информации, обрабатываемой ОТСС	47
1.2.4. Методы предотвращения утечки информации по каналу ПЭМИН	49
ГЛАВА 2. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ ПО ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ	53
2.1. Методические указания по проведению практических занятий	53
2.1.1. Подготовка к проведению практического занятия	53
2.1.2. Этапы выполнения сценария проведения практического занятия	53
2.1.3. Этапы и формы проведения контроля знаний	54
2.2. Практические занятия по определению коэффициентов звукоизоляции и виброизоляции защищаемых помещений на базе многофункционального поискового прибора ST-031 «Пирания»	54
2.2.1. Состав средств измерений и вспомогательного оборудования	54
2.2.2. Порядок размещения средств измерений и вспомогательного оборудования при проведении измерений	56
2.2.3. Порядок проведения оценки защищенности помещения	57

2.2.4. Измерение уровней сигналов и шумов в контрольных точках и расчет коэффициентов звукоизоляции (виброизоляции).....	58
2.2.5. Использование прибора ST-031 «Пиранья» для оценки эффективности виброакустической защиты и звукоизоляции помещений	65
2.3. Практические занятия по выявлению каналов утечки информации за счет акустоэлектрических преобразований во вспомогательных технических средствах и системах	70
2.3.1. Методики проведения измерений в канале низкочастотного акустоэлектрического преобразования	70
2.3.2. Состав средств измерений и вспомогательного оборудования, их размещение при проведении измерений	72
2.3.3. Порядок проведения измерений	75
2.3.4. Обработка результатов измерений.....	76
2.4. Практические занятия по определению требуемого радиуса контролируемой зоны для защиты конфиденциальной информации от утечки по каналу побочных электромагнитных излучений.....	79
2.4.1. Описание метода измерений.....	79
2.5. Практические занятия по оценке защищенности ОТСС от наводок ПЭМИ на линии и коммуникации, выходящие за пределы контролируемой зоны	84
2.5.1. Описание канала утечки информации	84
2.5.2. Описание метода измерений и расчета.....	85
2.6. Практические занятия по обнаружению и локализации закладных устройств негласного съема акустической (речевой) информации.....	90
2.6.1. Технические устройства негласного съема речевой информации и их классификация	90
2.6.2. Поиск и обнаружение закладных устройств	94
2.6.3. Мотивация поисковых исследований и особенности их реализации	100
2.6.4. Обнаружение и локализация закладных устройств негласного съема информации измерителем спектра вторичных полей «NR-μ»	102
2.6.5. Обнаружение и локализация закладных устройств негласного съема информации многофункциональным поисковым прибором ST-031 «Пиранья»	107
2.6.6. Обнаружение несанкционированных подключений к внутриофисным телефонным линиям анализатором проводных линий «Отклик-2»	124
2.7. Методические рекомендации по курсовому проектированию системы инженерно-технической защиты информации ...	138
2.7.1. Цели и задачи курсового проектирования.....	139
2.7.2. Руководство и контроль выполнения курсового проекта.....	139
2.7.3. Типовая структура курсового проекта.....	140
2.7.4. Оформление курсового проекта	142

2.7.5. Защита курсового проекта.....	143
2.7.6. Критерии оценки курсового проекта	144
ГЛАВА 3. ПОДХОДЫ К СОЗДАНИЮ ИНТЕГРИРОВАННЫХ СИСТЕМ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ РАЗЛИЧНОГО УРОВНЯ	145
3.1. Моделирование угроз безопасности информации и злоумышленника	145
3.2. Понятие интегрированной системы безопасности	147
3.3. Структура интегрированной системы безопасности.....	149
3.3.1. Система контроля и управления доступом.....	149
3.3.2. Система видеонаблюдения.....	153
3.3.3. Системы охранной и пожарной сигнализации.....	159
3.4. Способы построения интегрированных систем безопасности на объектах защиты.....	161
3.5. Разработка интегрированной системы безопасности для типовой структуры объекта информатизации.....	165
3.5.1. Выбор комплекса управления защитой	165
3.5.2. Интегрированная система охраны «Орион»	167
3.5.3. Интегрированный комплекс безопасности «КОДОС».....	170
3.5.4. Интегрированная система безопасности на базе «Pro-Watch».....	172
3.5.5. Аппаратно-программный комплекс «Бастион 2»	174
3.5.6. Пример выбора комплекса управления защитой объекта информатизации	176
ПРИЛОЖЕНИЯ.....	181
ЛИТЕРАТУРА	200