

Данное пособие является логическим продолжением и переработкой «Практического руководства по выявлению специальных технических средств несанкционированного получения информации», выпущенного автором (Г. А. Бузов) в 2010 году. Основной упор сделан на практический аспект поиска и выявления средств несанкционированного получения информации с учетом развития современных технических средств и новых тенденций в организации поиска. Последовательно и в необходимом объеме изложены практические вопросы и даны методические рекомендации в области организации и осуществления мероприятий по подготовке и проведению работ по выявлению электронных устройств, предназначенных для негласного получения информации. Дано описание физических основ и возможных характеристик современных средств негласного получения как различного вида речевой информации, так и информации, обрабатываемой техническими средствами. Доступным языком изложено назначение, основные характеристики и особенности функционирования современных специальных технических средств. Рассмотрен пакет нормативно-методических документов, регламентирующих деятельность в области осуществления поиска. Приведены методика принятия решения на проведение комплексной специальной проверки помещений, а также динамика и последовательность проведения поисковых мероприятий. В приложении в качестве справочного материала даны данные современных (на момент написания пособия) приборов и оборудования для осуществления поисковых мероприятий.

Для специалистов, работающих в области защиты информации, руководителей и сотрудников служб безопасности, а также студентов и слушателей соответствующих курсов.

Предисловие

Введение

Глава 1. Оценка необходимости выявления закладочных устройств в организации

- 1.1. Общая характеристика закладочных устройств
- 1.2. Характеристики радиозакладок
- 1.3. Закладочные устройства на базе сотовых телефонов
- 1.4. Радиозакладочные переизлучающие устройства
- 1.5. Акустооптический (лазерный) технический канал утечки информации
- 1.6. Закладочные устройства, передающие информацию по проводам

Глава 2. Оценка необходимости проведения комплексной проверки в организации

*Наиболее вероятные причины проведения поисковых работ по выявлению ЗУ
Необходимые шаги, которые следует осуществить непосредственно перед проведением поисковых работ*

Глава 3. Методика принятия управленческого решения о проведении комплексной проверки для выявления закладочных устройств

*Уяснение поставленной задачи
Оценка обстановки
Оценка возможностей вероятного противника (злоумышленника)
Оценка условий, в которых придется решать поставленную задачу
Модели вероятного противника*

Глава 4. Порядок подготовки к комплексной специальной проверке

*Легендирование проверки
Предварительный осмотр объектов проверки
Возможный вариант структуры типового плана проведения комплексной специальной проверки*

Глава 5. Выполнение поисковых мероприятий

- 5.1. Радиомониторинг
- 5.2. Визуальный осмотр помещения

- 5.3. Поиск с помощью поискового оборудования
 - 5.3.1. Поиск радиомикрофонов
 - 5.3.2. Порядок поиска работающих радиомикрофонов при отсутствии данных радиомониторинга
 - 5.3.3. Поиск телефонных радиоретрансляторов
 - 5.3.4. Поиск «сетевых» радиомикрофонов
 - 5.3.5. Поиск радиостетоскопов
 - 5.3.6. Поиск ЗУ, внедренных в электронные приборы
- 5.4. Поиск скрытых видеокамер
 - 5.4.1. Поиск видеокамер, передающих информацию по радиоканалу
 - 5.4.2. Поиск выключенных видеокамер и камер, передающих информацию по проводам
- 5.5. Поиск пространственного высокочастотного облучения
- 5.6. Выявление ЗУ, разработанных на базе сотовых телефонов
- 5.7. Проверка линий и оборудования проводных коммуникаций
- 5.8. Выявление утечки информации с помощью специализированного приборного оборудования
- 5.9. Проверка телефонных линий
 - Визуальный осмотр линий
 - Приборный поиск сигналов
- 5.10. Выявление утечки информации в инфракрасном диапазоне
- 5.11. Выявление утечки информации по низкочастотным магнитным полям
- 5.12. Выявление неработающих во время проверки ЗУ

Глава 6. **Заключительный этап проверки**

- 6.1. Обработка результатов проверки и оформления протоколов
- 6.2. Анализ технических характеристик и свойств обнаруженных и изъятых ЗУ
- 6.3. Составление описания проведенных работ
- 6.4. Разработка рекомендаций по повышению защищенности помещений
- 6.5. Составление акта проведения комплексной специальной проверки помещений
- 6.6. Завершающие работы заключительного этапа

Заключение

Литература

Приложения

- Приложение 1.** *Вариант плана проведения комплексной специальной проверки помещений*
- Приложение 2.** *Вариант акта проведения комплексной специальной проверки помещений*
- Приложение 3.** *Рекомендации по повышению защищенности помещений и объектов (вариант)*
 - Перечень выявленных в проверенных помещениях потенциальных технических каналов утечки информации (ТКУИ)*
 - Оценка вероятности использования противником потенциальных ТКУИ и защищенности помещений.*
 - Рекомендации по мерам и способам предотвращения съёма информации по выявленным потенциальным ТКУИ и повышению защищенности помещений*
 - Предложения по практическому использованию рекомендуемых средств и систем защиты информации*
- Приложение 4.** *Подготовка аппаратно-программного комплекса для проведения поисковых мероприятий*
 - Калибровка комплекса*
 - Рекомендации по применению фильтра по частоте*
 - Рекомендации по применению фильтра по полосе частот*
 - Рекомендации по применению фильтра превышения порога*
 - Рекомендации по применению фильтра по регулярности*
 - Рекомендации по применению фильтра по числу обнаружений*
 - Рекомендации по применению фильтра по отношению уровней*

Рекомендации по применению фильтра по совпадению спектра
Рекомендации по применению режимов экспресс-анализа векторного анализатора сигналов
Рекомендации по применению режима амплитуда
Рекомендации по применению режима спектрограмма
Рекомендации по применению режима вектор
Рекомендации по применению режимов усреднения
Режим усреднения позволяет выделять слабые сигналы на уровне шумов
Рекомендации по применению режимов накопления максимумов
Рекомендации по применению режима регистрации для поиска закладных устройств с ДУ
Рекомендации по поиску радиомикрофонов с системой VOX
Рекомендации по обнаружению новых сигналов

Приложение 5. Краткая характеристика основных поисковых приборов

Анализатор электромагнитного поля «КОРДОН»
Детектор поля ST 111
Селективный индикатор поля RAKSA-120
Индикатор поля SEL SP-222
Индикатор поля SEL SP-77/2M «Ловец»
Портативный измеритель мощности РИЧ-8
Универсальный прибор ST-31M «Пиранья»
Многофункциональное поисковое устройство ST 131 «Пиранья II»
Поисковый приемник ST 167 «БЕТТА»
Поисковый приемник «Контур»
Поисковый приемник радиосигналов «Скорпион XL»
Поисковый многозоновый комплекс ST 154
Комплекс поиска устройств негласного съема информации «Спектр-Professional»
Портативный комплекс поиска устройств негласного съема информации «Спектр-Экспресс»
Аппаратно программный комплекс радиоконтроля Spectrum Jet
Семейство комплексов «Кассандра»
Портативный анализатор спектра OSCOR Blue
Анализатор проводных линий ST 300 SPIDER
Цифровой анализатор «Талан»
Универсальный анализатор линейных коммуникаций «Улан»
Программно-аппаратный комплекс «Сириус»
Анализатор проводных коммуникаций «LBD-50»
Нелинейный локаатор NR-900S
Нелинейный радиолокаатор NR-900EMS
Нелинейный радиолокаатор NR-2000
Нелинейный локаатор «Саутан» ST 400
Семейство локааторов «Лорнет»
Локаатор нелинейностей «Люкс»
Комбинированное устройство «Буклет-МД»