

УДК 681.3.06

Зуев А.В., Мазуренко Л.Н., Хмелько Ю.М., Чирков Д.В. (ГУИКТ)

АППАРАТУРА ПОИСКА ЗАКЛАДНЫХ УСТРОЙСТВ

Технические устройства, используемые для приема, передачи, обработки и хранения информации зачастую имеют конфиденциальный характер; физические процессы, происходящие в подобных устройствах создают в окружающем пространстве различного вида побочные излучения (электромагнитные, акустические и др.), которые представляют интерес для злоумышленников (в частности, конкурирующих фирм).

Утечка информации в результате побочных излучений по сути носит характер непреднамеренной передачи секретной информации по паразитному техническому каналу утечки информации.

К источникам подобных излучений следует отнести:

- сети телефонной связи;
- сети электропитания;
- средства всех видов связи;
- средства звуко- и видеозаписи;
- электронно-вычислительная техника;
- оргтехника;
- акустические излучения в помещениях, где ведутся переговоры.

Закладные устройства (ЗУ) нашли широкое применение для съема информации ввиду сравнительно невысокой стоимости и высокой эффективности.

Вариантов ЗУ чрезвычайно много, конструкция ЗУ разнообразна, при изготовлении ЗУ применяются передовые технологии. Поэтому для их обнаружения и оценке параметров применяют разнообразную специальную аппаратуру, начиная от простейших ручных частотомеров и индикаторов электромагнитного поля до нелинейных локаторов и программно-аппаратных комплексов, использующих различные методы поиска ЗУ.

К универсальным методам поиска ЗУ следует отнести:

- визуальный осмотр;
- нелинейную локацию;
- металлодетектирование;
- рентгеновское просвечивание.

При визуальном осмотре используют:

- досмотровые зеркала;
- осветительные приборы;
- эндоскопы (эндоскопия - метод исследования с помощью введения в объект осмотра инструментов, снабженных оптическими и осветительными системами).

Метод с использованием нелинейной локации основан на свойстве полупроводниковых материалов преобразовывать облучаемый их ВЧ сигнал в кратные гармоники с переизлучением их в пространство с последующим обнаружением 2-й либо 2-й и 3-й гармоники.

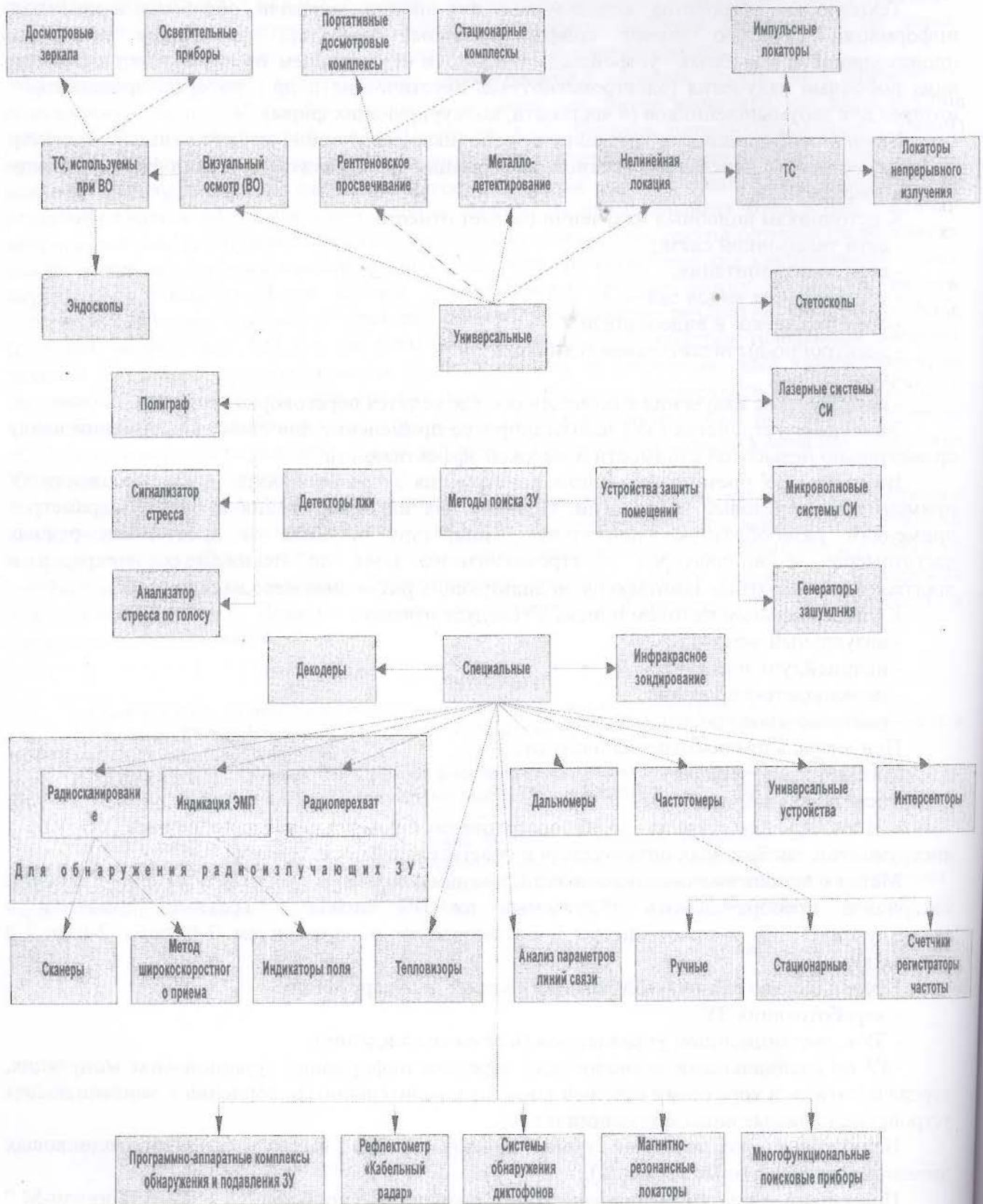
Преимущество нелинейной локации состоит в обнаружении:

- неработающих ЗУ
- ЗУ с дистанционным управлением (в режиме ожидания);
- ЗУ со специальными технологиями передачи информации (узкополосная модуляция, передача сигналов короткими сериями после предварительного накопления в запоминающем устройстве, сложные виды модуляции и т.д.).

Нелинейные локаторы не обнаруживают ЗУ не имеющих полупроводниковых элементов (полуактивные закладки).

Примерами таких локаторов являются – импульсные приборы NR – 900Е; “Циклон-М ” (Россия); локатор непрерывного излучения “Обь” (Россия).

Классификация методов поиска и аппаратуры обнаружения – измерения ЗУ



Метод металлодетектирования

Поиск ЗУ с использованием металлодетекторов (металлоискателей), реагирующих на металлический корпус ЗУ. Применение – ограничено из-за большого числа предметов (не ЗУ) металлических, создающих помехи. Исследуется: мебель, деревянные, пластиковые, строительные конструкции, кирпичные стены, и.т.п..

Метод рентгеновского просвечивания

Используют для обнаружения ЗУ всех типов в помещениях и радиоэлектронной аппаратуре (портативные досмотровые комплексы “Шмель – 80/К”, “Шмель – 90/К”, (Россия). Просвечивают слой стали до 2мм; слой бетона до 100 мм.

Портативный рентгенаппарат (типа 7-Л-2) либо стационарный медицинский изготавливают фотоснимки узлов и деталей аппаратуры в рентгеновских лучах. Снимки сравнивают со снимками стандартных топологий узлов и блоков. При несовпадении топологий делают заключение о наличии ЗУ в радиоэлектронной аппаратуре.

Технология, как известно, (от греческого *topos* - место и ??? - ...логия) - раздел математики, изучающий топологические свойства фигур, т.е. свойства не изменяющиеся при любых деформациях при взаимно однозначных непрерывных отображениях.

К специальным методам обнаружения ЗУ следует отнести:

- радиосканирование;
- индикация электромагнитного поля;
 - радиоперехват;
 - анализ параметров линий связи и проводных коммутаций;
 - рефлектометрия линий связи;
 - инфракрасное зондирование.

Методы радиосканирование, индикации ЭМП и радиоперехвата используются для обнаружения радиоизлучающих ЗУ

Метод радиосканирования заключается в узкополосном радиоприеме в заданном частотном диапазоне с последовательным передвижением по шкале частот.

Идентификация источника сигнала “на слух”.

Режим радиосканирования: “ручной” и “компьютерный”.

Портативные сканирующие приемники (сканеры): фирмы AOR (Япония): AR-3000A в диапазоне 0,1-2036 МГц; AR-8000 в диапазоне 0,5-1900 МГц; AR-2700 в диапазоне 0,5-1300 МГц. С автоматическим выбором модуляции (AM, NFM, WFM, USB, LSB, CW). Новые модели сканеров (AR-3000A, AR-8000) реализуют режим работы с управлением от компьютера. В России – компьютерный комплекс, программы “Смерш” и “Сезиф”.

При радиосканировании и других методах обнаружения ЗУ применяют технологию инициации ЗУ с провоцированием их работы путем генерации известного звукового сигнала (магнитофонная запись, компьютерная акустическая инициация и т.д.). Если частотный диапазон неизвестен применяют широкополосный радиоприем.

Метод широкополосного приема. Этот метод заключается в приеме суперпозиции (в физике результирующий эффект от нескольких независимых воздействий представляет собой сумму эффектов, вызываемых каждым воздействием в отдельности) радиосигналов в широком частотном диапазоне с помощью специальных широкополосных приемников. Суммарный сигнал детектируется на головные телефоны. Прослушивание радиоэфира позволяет опытному оператору сделать вывод о наличии ЗУ, иницированного известным звуковым сигналом. Для широкополосного радиоприемника используют индикаторы поля R-10, R-20 (Optoelectronics, США) с частотным диапазоном 30-2000 МГц, 05,-2500 МГц, либо СРМ-700 (REI, США) с частотой 0,05-3000 МГц.

Метод радиоперехвата – новый метод, основанный на сравнении (принцип действия) уровня сигнала от радиопередатчика и фонового уровня с последующей самонастройкой.

Приборы → специализированные перехватчики радиосигналов.

Пример: Xplorer (Optoelectronics, США) радиоперехват FM сигнала в диапазоне 30-2000 МГц за $t \leq 1с$. Xplorer (как и прибор СРМ-700) используется также в режиме “акустической завязки”, который заключается в самовозбуждении прибора за счет положительной обратной связи. Уровень самовозбуждения зависит от напряженности на ЗУ.

Метод измерения электрических параметров линий связи и проводных коммуникаций

Позволяет обнаружить ЗУ, считывающих информацию либо передающих информацию по проводным линиям.

В телефонных линиях связи контролируется напряжение, ток, активное и реактивное сопротивление линии, наличие ВЧ сигналов. Некоторые приборы помимо контроля обеспечивают подавление ЗУ.

Пример: прибор для контроля и защиты телефонной линии КОМ-1 (Россия) обнаруживает параллельно подключенные и подавляет последовательно подключенные (в том числе индуктивные) подслушивающиеся устройства. Обеспечивает проверку телефонных линий в автоматическом режиме каждые 2мин. и обнаруживает параллельно подключенные подслушивающие устройства на расстоянии до 150 м. Подавление подслушивающих устройств производится на расстоянии до 1000 м. Посредством зашумления телефонных линий в речевом диапазоне частот (практически над уровнем сигнала не менее 10 дБ).

“Скат” (Россия) – анализатор телефонной линии. Конструктивно выполнен в виде телефонной розетки. Факт обнаружения подключения к линии фиксируется путем светодиодной индикации.

Тест-комплект АТ-2 (Россия) выполнен в виде кейса для проверки проводных линий на наличие гальванического подключения подслушивающих устройств.

Способ проверки → с помощью зондирующего сигнала частотой 40 или 400 Гц. Дальность обнаружения до 5000 м.

Система защиты ПТЗ-003 “Прокруст” (Россия)

ЗУ обнаруживают изменением напряжения в линии. Подавление происходит следующим путем:

- поднятие напряжения в линии до 35 В;
- генерации “белого” шума напряжением до 10 В;
- генерации ВЧ-помехи амплитудой до 35В.

Метод идентификации известного звука “на слух”. Для обнаружения ЗУ с передачей акустической информации по телефонной линии, электросети.

Аппаратура - универсальный прибор СРМ – 700 с сетевым фильтром VLF-700.

Метод рефлектометрии применяется для определения расстояния до подозрительного места в линии. Расстояние определяется по осциллографу с фиксацией задержки сигнала (импульса), отраженного от неоднородностей линии (места подключения ЗУ к линии).

Метод инфракрасного зондирования. Используют специальный зонд ИК. Обнаруживают ЗУ, осуществляющих передачу информации по инфракрасному каналу связи.

Пример: ИК-зонд IRP-700 (REI, США), подключаемый к прибору СРМ -700).

При обнаружении ЗУ в головных телефонах прослушивается известный звуковой сигнал, который усиливается при ориентировке ИК-зонда на закладное устройство.

Выводы

При выборе методов и аппаратуры ЗУ естественно принципиальным является учет потерь, связанных с возможной утечкой информации и стоимостью процедур связанных с применением той или иной аппаратуры обнаружения ЗУ, длительностью и периодичностью поиска ЗУ и др.

Например, представляется чрезвычайно важным сравнительная оценка эффективности применения различных алгоритмов обнаружения ЗУ нелинейными локаторами, включая

разработку методики оценки достоверности обнаружения ЗУ в условиях сложной помеховой ситуации.

Литература

1. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия для промышленного шпионажа – С. – Пб.: ООО «Издательство Полигон», 2000. – 896с.
2. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации т.1. – К.: «АРИЙ», 2008. – 464с.; т.2. – К.: «АРИЙ», 2008. – 342с.
3. Максименко Г.А., Хорошко В.А. Методы выявления, обработки и идентификации сигналов радио закладных устройств Кю: Полиграф Консалтинг, 2004. – 317с.
4. Шаповалов П.П. Практическое руководство по поиску устройства съема и передачи информации. – М.: АО «Щит», 2000. – 52с.

Рецензент: д.т.н., проф. Єрохін В.Ф.

Надійшла 10.09.2010

Після доробки 20.12.2010