

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: ЗАКЛАДНЫЕ УСТРОЙСТВА И МЕТОДЫ ИХ ДЕТЕКТИРОВАНИЯ

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Существует множество причин и мотивов, по которым одни люди хотят шпионить за другими. Имея немного денег и старание, злоумышленники могут организовать ряд каналов утечки сведений, используя собственную изобретательность или халатность владельца информации. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.

Для построения системы надежной защиты информации необходимо выявить все возможные угрозы безопасности, оценить их последствия, определить необходимые меры и средства защиты, оценить их эффективность. Выявление угроз безопасности производится квалифицированными специалистами с помощью различных программных и аппаратных средств.

1. Закладные устройства и методы их детектирования

Электронными устройствами перехвата информации (закладными устройствами) называются скрытно внедряемые в места возможного съема информации малогабаритные устройства, предназначенные для несанкционированного съема информации.

Обнаружение электронных устройств перехвата информации, так же, как и для любых других объектов, производится по их демаскирующим

признакам. Это может быть, как визуальный анализ предметов и окружения, так и с помощью технических средств.

1.1. Разновидности закладных устройств

В настоящее время создано огромное количество типов закладных устройств (ЗУ), различающихся принципом функционирования, способом передачи информации, дальностью действия, а также размером и внешним оформлением.

Так, самые миниатюрные ЗУ имеют вес всего 1,5 г и линейные размеры — не более нескольких миллиметров. Дальность передачи информации с таких устройств едва превышает 10 м. Более мощные устройства имеют размеры до нескольких сантиметров и позволяют осуществить передачу перехватываемой информации на дальность от нескольких сот до тысячи и более метров. Обычно ЗУ скрытно устанавливаются в элементах конструкций зданий и интерьера, крепятся под одеждой или камуфлируются под личные вещи.

Для того чтобы систематизировать представление о таких устройствах, целесообразно разделить их на 4 большие группы:

- акустические закладки;
- телефонные закладки;
- телевизионные закладки;
- аппаратные закладки.

Рассмотрим каждый тип закладок более подробно.

1.1.1. Акустические закладки

Акустические закладки используются для перехвата речевой информации, посредством миниатюрных электронных устройств перехвата речевой информации, не санкционированно и скрыто устанавливаемых в

помещениях, автомобилях и т.д. Акустические закладки можно классифицировать по виду исполнения, месту установки, источнику питания, способу передачи информации и её кодирования, способу управления.

Перехватываемая акустическими закладками информация может передаваться по радио или оптическому каналу, по электросети переменного тока, по соединительным линиям (например, телефонной линии), а также по металлоконструкциям зданий, трубам систем отопления и водоснабжения и. Наиболее широко используются акустические закладки, передающие информацию по радиоканалу. Такие устройства часто называют радиозакладками.

Закладки могут быть выполнены в виде отдельного модуля обычно в форме параллелепипеда или закамуфлированы под предметы повседневного обихода: пепельницу, электронный калькулятор, электролампочку, зажигалку, наручные часы, авторучку, вазу, поясной ремень и т.д. (Рисунок 1.1).



Рисунок 1.1 – Внешний вид камуфлированных радиозакладок

- а) предметы обихода; б) зажигалка; в) паркер; г) головной убор; д) лампочка; е) карандаш.

Современные технологии позволяют выполнить акустические закладки размером с рисовое зернышко и весом в несколько граммов. Однако дальность передачи информации с таких закладок составляет несколько десятков метров, а время работы несколько часов.

Акустические закладки могут быть установлены в интерьерах помещения, предметах повседневного обихода, радиоаппаратуре, розетках электросети и электрических приборах, технических средствах связи и их соединительных линиях и т.п. Они также могут быть скрыты в одежде и личных вещах агента, находящегося в помещении.

В зависимости от среды распространения акустических колебаний, перехватываемых радиозакладками, последние можно подразделить на акустические радиозакладки и радиостетоскопы.

Акустические радиозакладки предназначены для перехвата акустических сигналов по воздушному каналу утечки информации. Чувствительным элементом в них является, как правило, электретный микрофон. Поэтому акустические радиозакладки иногда называют радиомикрофонами, но среди специалистов по разведке этот термин используется редко. Подобные средства позволяют улавливать негромкую речь на дальности 5-10 метров.

Радиостетоскопы (контактные микрофоны, конструкционно объединенные с микропередатчиками) перехватывают акустические сигналы по вибрационному каналу утечки информации. В качестве чувствительных элементов в них обычно используются пьезомикрофоны, электретные микрофоны или датчики акселерометрического типа.

Радиостетоскопы способны улавливать звуковые колебания через бетонные стены толщиной 0,3-0,5 м, а также через двери и оконные рамы (Рисунок 1.2).

Питание акустических закладок осуществляется от автономных источников питания (аккумуляторов, батарей), электросети переменного тока,

телефонной сети, а также от источников питания радиоэлектронной аппаратуры, в которой они устанавливаются.

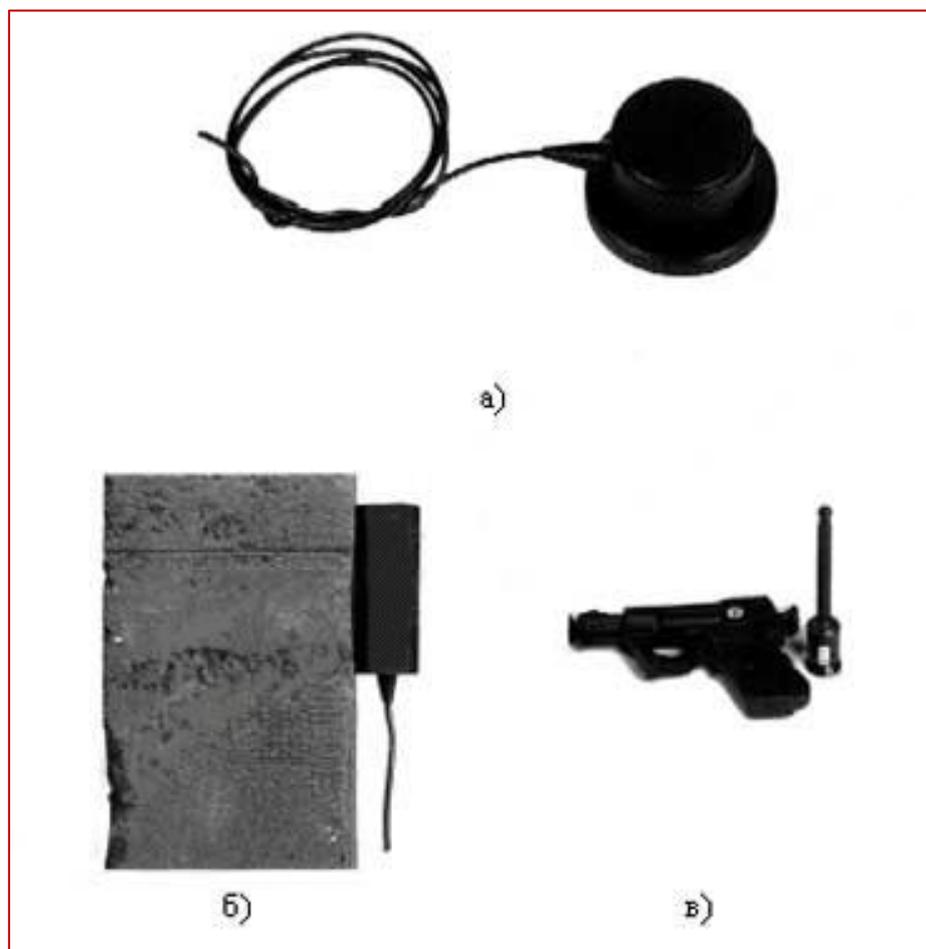


Рисунок 1.2 – Внешний вид радиостетоскопов

- а) стетоскоп для прикладывания к стене; б) стетоскоп, приложенный к стене;
в) бесшумный пистолет со стрелой-радиостетоскопом

В зависимости от мощности излучения и типа источника питания время работы акустической закладки составляет от нескольких часов до нескольких суток и даже месяцев. Например, время работы серийно выпускаемой акустической закладки РК 260 при мощности излучения 7 мВт составляет при питании от двух батарей АА - 10 суток, а при использовании литиевой батареи - 70 суток. При электропитании от сети переменного тока или телефонной линии время работы не ограничено.

1.1.2. Телефонные закладки

Телефонные закладки так же, как и акустические, можно классифицировать по виду исполнения, месту установки, источнику питания, способу передачи информации и ее кодирования, способу управления и т.д.

Выполняются они, как правило, или в виде отдельного модуля, или камуфлируются под элементы телефонного аппарата, например, конденсатор телефонный или микрофонный капсули (Рисунок 1.3) телефонный штекер или розетку и т.д.



Рисунок 1.3 – Примеры исполнения телефонных закладок
а,б) телефонные закладки, выполненные в виде конденсаторов; в,г)
телефонные закладки в виде капсулей.

Телефонные закладки могут быть установлены: в корпусе телефонного аппарата телефонной трубке или телефонной розетке, а также непосредственно в тракте телефонной линии.

Возможность установки телефонной закладки непосредственно в телефонной линии имеет важное значение, так как для перехвата телефонного разговора нет необходимости проникать в помещение, где находится один из абонентов. Телефонные закладки могут быть установлены или в тракте телефонной линии до распределительной коробки, находящейся, как правило, на одном этаже с помещением, где установлен контролируемый аппарат, или в тракте телефонной линии от распределительной коробки до распределительного щитка здания, располагаемого обычно на первом этаже или в подвале.

Телефонные закладки могут быть установлены последовательно в разрыв одного из телефонных проводов, параллельно или через индуктивный датчик (Рисунок 1.4).

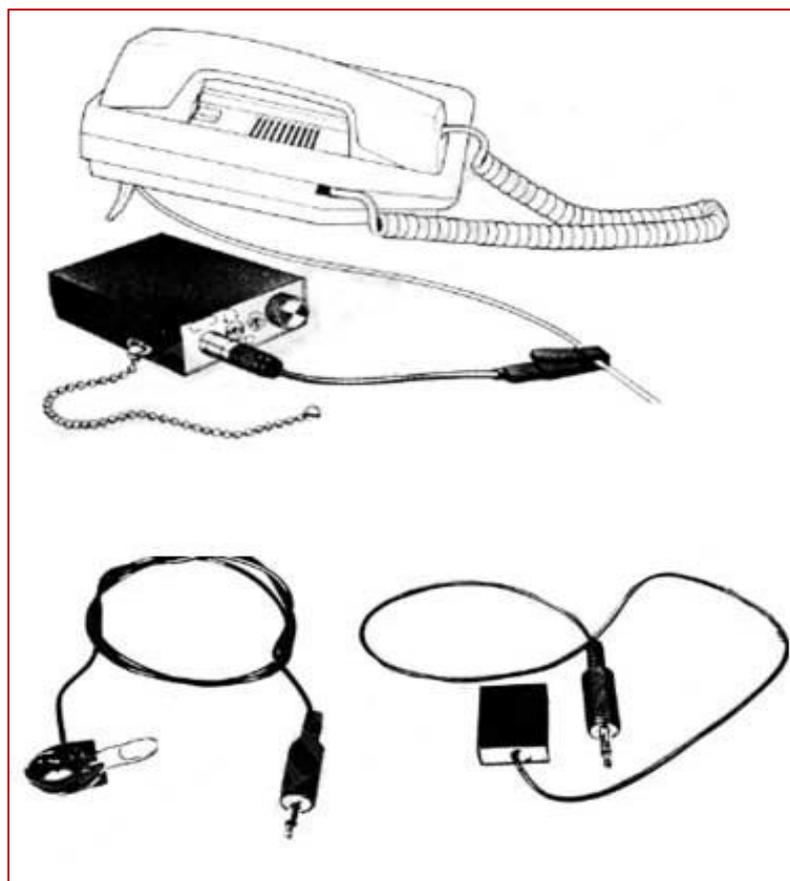


Рисунок 1.4 – Индуктивные датчики съема информации с телефонной линии

При последовательном включении питание закладки осуществляется от телефонной линии, что обеспечивает неограниченное время ее работы. Однако последовательное подключение закладки легко обнаружить за счет изменения параметров линии и в частности падения напряжения. В ряде случаев используется последовательное подключение с компенсацией падения напряжения, но реализация этого требует наличия дополнительного источника питания.

Телефонные закладки с параллельным подключением к линии, особенно имеющие автономное питание, труднее обнаружить.

Наряду с контактным подключением возможен и бесконтактный съем информации с телефонной линии. Для этих целей используются закладки с миниатюрными индукционными датчиками. Конечно, такие закладки питаются от автономных источников питания, но установить факт подключения их к линии даже самыми современными средствами практически невозможно, так как параметры линии при подключении не меняются.

Телефонные закладки перехваченную информацию передают в большинстве случаев по радиоканалу. Обычно в качестве антенны используется телефонный провод.

Как правило, передача информации (работа на излучение) начинается в момент поднятия трубки абонентом. Однако встречаются закладки, производящие запись информации и передающие ее по команде. Такие закладки встречаются крайне редко и имеют сравнительно большие размеры.

Так же, как в акустических, в телефонных закладках передаваемая информация может кодироваться различными методами.

Для приема информации от телефонных закладок используются такие же средства, как и для акустических.

Наряду с чисто телефонными и акустическими используются и комбинированные закладки, которые при ведении телефонного разговора осуществляют его перехват, а по окончании – автоматически переключаются

на перехват акустической информации. К таким закладкам относится, например, передатчик РК-125-GHz.

Способы применения телефонных закладок мало чем отличаются от способов применения акустических закладок и определяются возможностью доступа в контролируемое помещение.

В случае если имеется возможность даже на короткое время проникнуть в помещение, закладка может быть установлена в корпусе телефонного аппарата, телефонной трубке и т.д. Причем для этого необходимо от 10-15 секунд до нескольких минут. Например, замена обычного микрофонного капсюля на аналогичный, но с установленной в нем телефонной закладкой, занимает не более 10 секунд. Причем, визуально их отличить невозможно.

Телефонные закладки, выполненные в виде отдельных элементов схемы телефонного аппарата, впаиваются в схему вместо аналогичных элементов или маскируются среди них. Наиболее часто используются закладки, выполненные в виде различного типа конденсаторов. Для установки таких устройств требуется несколько минут и проводится она, как правило, при устранении неисправностей или профилактическом обслуживании телефонного аппарата.

Не исключена возможность установки закладки в телефонный аппарат еще до поступления его в учреждение или на предприятие. Это относится в основном к телефонным аппаратам иностранного производства, когда спецслужбам становится известно, куда конкретно они поставляются. Причем в этом случае закладки выполняются в виде конкретных элементов и деталей схемы, и визуально факт их установки обнаружить практически невозможно.

Если доступ в контролируемое помещение невозможен, закладки устанавливаются или непосредственно в тракте телефонной линии или в распределительных коробках и щитках обычно таким образом, чтобы их визуальное обнаружение было затруднено.

Чем меньше закладка, тем легче ее замаскировать. Однако небольшие по размерам закладки в ряде случаев не обеспечивают требуемой дальности

передачи информации на большие расстояния. Поэтому для увеличения дальности передачи информации используются специальные ретрансляторы, устанавливаемые, как правило, в труднодоступных местах или в автомашине в радиусе действия закладки.

1.1.3. Телевизионные закладки

Современные средства видеонаблюдения позволяют с расстояния до нескольких километров наблюдать действия лиц, а с расстояния нескольких сот метров распознавать небольшие по размерам объекты, определять номера машин и даже, например, читать содержание плакатов, вывешенных в кабинете или классе на стене, противоположной окну.

В последнее время для видеонаблюдения с близкого расстояния широкое распространение получили видеокамеры, обеспечивающие возможность документирования наблюдений в динамике с фиксацией на изображении времени и даты наблюдения.

Видеокамера состоит из нескольких функциональных узлов, определяющих ее характеристики и, следовательно, возможность применения в тех или иных условиях.

Объектив является неотъемлемой частью телевизионной камеры и формирует все геометрические размеры изображения на приемнике оптического излучения (ПОИ). Используются следующие типы объективов:

- с фиксированным фокусным расстоянием и постоянным относительным отверстием;
- фиксированным фокусным расстоянием и переменным (изменяется вручную) относительным отверстием;
- переменным фокусным расстоянием (изменяется вручную) и переменным относительным отверстием (изменяется вручную);

- фиксированным фокусным расстоянием, фиксированным относительным отверстием и автоматической регулировкой освещенности (автодиафрагмой);

- переменным фокусным расстоянием (изменяется автоматически, постоянным относительным отверстием и автоматической регулировкой освещенности (автодиафрагмой).

Существует самостоятельный класс объективов, применяемых для скрытой съемки, так называемые пинхоул-объективы (pin-hole).

Объектив и приемник излучения, как правило, конструктивно объединяются в одно устройство, но иногда для целей наблюдения требуется их разнесение. В этом случае они соединяются между собой волоконно-оптическим кабелем (световодом), примером такого устройства служит эндоскоп, используемый для наблюдения в закрытых объемах и закрытых помещениях.

Одна из основных характеристик объектива - угол зрения. Он зависит от фокусного расстояния объектива и диагонали ПОИ. В системах ближнего наблюдения используются объективы с углом зрения от нескольких десятков до ста восьмидесяти градусов.

В телевизионных камерах в качестве приемников оптического излучения используются различные типы ЭЛТ и плоские матричные элементы на базе приборов с зарядовой связью (ПЗС).

Однако наиболее широкое применение в системах скрытого наблюдения получили телевизионные камеры с ПОИ на основе матриц ПЗС. Телевизионные камеры с ПОИ на основе матриц ПЗС имеют достоинства, к основным из которых можно отнести: экономичность при потреблении электроэнергии (потребляемый ток 90-200 мА при напряжении питания 12 В), малые размеры и вес, способность работать не только в видимом, но и ближнем инфракрасном диапазонах длин волн, способность получать цветные

изображения с хорошим разрешением при низком уровне освещенности (Рисунок 1.5).



Рисунок 1.5 – Портативная камера с ПЗС матрицей и система скрытого видеонаблюдения

Видеоизображения с телевизионных камер или непосредственно записываются на видеомаягнитофон, или передаются по радиоканалу с использованием специальных видеопередатчиков. С целью сокращения полосы частот передаваемого сигнала, обычно применяют амплитудную модуляцию несущей частоты передатчика видеосигналом с передачей только одной боковой полосы (однополосная модуляция).

Если требуется передавать не только видеоизображение, но и звук, то совместно с видеокамерой устанавливается микрофон, соединенный с видеопередатчиком. Для передачи звукового сопровождения, как правило, используется частотная модуляция. Передатчики видеоизображения или выполняются в виде отдельного блока при этом они имеют небольшие размеры и вес, или конструктивно объединяются с телевизионными камерами, позволяя обходиться только одним блоком (Рисунок 1.6).

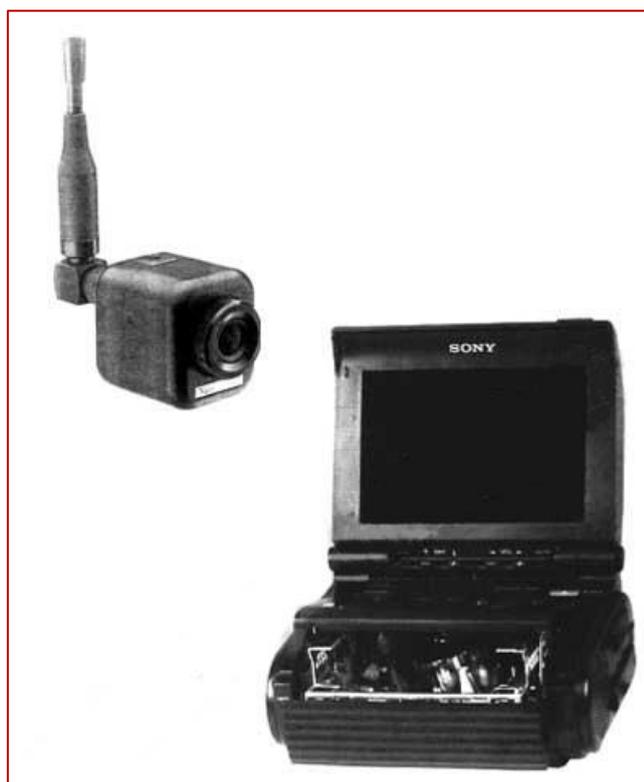


Рисунок 1.6 – Портативный телевизионный передатчик, конструктивно объединенный с телевизионной камерой и портативное записывающее устройство

1.1.4. Аппаратные закладки

Под аппаратной закладкой обычно понимают электронное устройство, скрытно устанавливаемое (внедряемое) в техническое средство обработки и передачи информации с целью обеспечить в нужный момент времени утечку информации, нарушению её целостность или блокированию.

Аппаратные закладки можно классифицировать по типу технического средства, в которые они внедряются, по виду перехватываемой информации, виду исполнения, месту установки, способу передачи информации и её кодирования, способу управления.

Наиболее часто используются аппаратные закладки, устанавливаемые в автоматизированные системы, построенные на основе вычислительной техники.

Аппаратная закладка, как правило, состоит из блока перехвата, блока передачи информации (или модуля записи информации), блока дистанционного управления (при необходимости) и блока питания.

Блок перехвата подключается к информационным кабелям или непосредственно к платам блоков вычислительной техники и осуществляет перехват информационных сигналов, их обработку и преобразование в вид, удобный для записи или передачи на приёмный пункт.

Перехватываемая аппаратными закладками информация может записываться в память закладного устройства или передаваться на приёмный пункт по радиоканалу, электросети 220 В, оптическому каналу, выделенной линии и т.д.

С использованием системы дистанционного управления осуществляется включение\выключение устройства (запуск программы перехвата информации), включение\выключение режима передачи информации, установка параметров процесса съёма информации и ее передачи.

1.2. Методы детектирования закладных устройств

Методы детектирования закладных устройств в зависимости от типа делятся на 2 группы:

1) Первая группа – методы, основанные на поиске закладных устройств как физических объектов с определенными свойствами и массогабаритными характеристиками.

К ней относятся:

- Визуальный осмотр мест возможного размещения закладных устройств, в том числе с применением увеличительных стекол, зеркал, средств специальной подсветки;

- Контроль труднодоступных мест с помощью средств видеонаблюдения;
- Применение металлодетекторов.

2) Вторая группа – методы, использующие свойства закладных устройств, как электронных систем.

Она включает:

- Использование индикаторов поля, реагирующих на наличие излучения радио-закладных устройств и позволяющих локализовать их месторасположение;
- Применение специальных радиоприемных устройств, предназначенных для поиска сигналов по заданными характеристикам и анализа электромагнитной обстановки;
- Применение комплексов радио-контроля и выявления закладных устройств;
- Обследование помещений с помощью нелинейных радиолокаторов.

1.2.1. Методы поиска закладных устройств как физических объектов

Визуальный осмотр – это один из важнейших методов детектирования закладных устройств. Он предназначен для обнаружения закладных устройств как в обычном исполнении, так и в закамуфлированном виде. Осуществляется периодически, а также перед проведением важных мероприятий в тех помещениях, где возможно размещение закладных устройств, например, в конференц-залах, или в местах, куда могут проникнуть посторонние лица.

При проведении визуального осмотра особое внимание обращается на изменения в интерьере, появление свежих царапин, следов подчистки или подкраски. Особенно тщательно осматриваются сувениры, забытые

посетителями личные вещи или другие предметы, которые могут подойти для внедрения закладного устройства. Проводится обязательный осмотр телефонных и других линий связи на участке от аппарата до распределительной коробки. При проведении осмотра особое внимание уделяется скрытым и труднодоступным местам, так как именно они представляют наибольший интерес для лиц, устанавливающих закладные устройства. Для облегчения процедуры поиска используют фонари и зеркала (Рисунок 1.7).



Рисунок 1.7 – Средства для проведения осмотра в труднодоступных местах

Зачастую, использование таких простых приспособлений не удобно и мало эффективно, поэтому целесообразнее использовать технические средства видеонаблюдения, которые специально предназначены для осмотра труднодоступных мест.

К таким средствам видеонаблюдения относят всевозможные оптико-электронные системы, которые можно условно поделить на две основные группы:

- эндоскопическое оборудование;

- досмотровые портативные телевизионные или видеоустановки.

Эндоскопическое оборудование включает в себя целый набор волоконно-оптических, промышленных фиброскопов, жестких бароскопов, а также видеоскопов, позволяющих осуществлять осмотр труднодоступных мест (Рисунок 1.8). Отличительной особенностью этих устройств является миниатюрный объектив, помещенный на конце тонкого гибкого рукава или жесткой трубки, которые служат и направляющим элементом, и защитной оболочкой для оптоволоконного жгута, или же многокомпонентной линзовой системой, предназначенного для передачи изображения с выхода объектива на окуляр либо ПЗС-матрицу. В некоторых типах видеоскопов ПЗС-матрица расположена непосредственно на зондирующем конце рукава или трубки. С выхода матрицы сигнал по кабелю или радиоканалу передается в блок преобразования и далее на монитор.



Рисунок 1.8 – Эндоскопическое оборудование

а) видеоскоп; б) бароскоп; в) фиброскоп.

Гибкие фиброскопы предназначены для проникновения сквозь сложные изгибы различных каналов. Бароскопы используются для осмотра узлов, к

которым может быть осуществлен доступ через узкие прямолинейные каналы. В отличие от фиброскопов, вместо гибкого рукава они оборудованы жесткой штангой. Особенностью видеоскопов является то, что они позволяют в реальном масштабе времени осуществлять вывод изображения на телевизионный монитор, с одновременным фото или видеодокументированием. Кроме того, видеоскопы позволяют вести наблюдение за объектами, находящимися на удалении до 22 м.

Общим недостатком эндоскопических устройств является то обстоятельство, что они, скорее, рассчитаны на статическое скрупулезное обследование, чем на быстрый оперативный осмотр. Кроме того, зачастую эти системы имеют многомодульную конфигурацию с кабельными соединениями, их функциональные блоки не минимизированы по весу и габаритам. Очевидны и проблемы с быстрой подготовкой к работе, переносом системы и сохранением ее целостности. Еще одна существенная особенность заключается в не всегда приемлемом качестве наблюдаемого через окуляр изображения.

Сравнительная оценка эндоскопических устройств различного типа показывает, что наилучшее качество изображения позволяют получать видеоскопы, кроме того, по телевизионному монитору следить за осмотром может практически неограниченное число наблюдателей. В то же время, подобное оборудование не может использоваться одним оператором и не приспособлено для быстрой смены места осмотра и обхода объектов. Для этих целей больше подходят портативные эндоскопические устройства типа фиброскопов.

1.2.2. Методы поиска закладных устройств как электронных средств

Основными способами выявления электронных закладных устройств являются:

- индикаторы поля;
- специальные приемники;
- комплексы радиоконтроля;
- нелинейные локаторы.

Все они основаны на детектировании излучения закладного устройства, которое является их демаскирующим признаком.

Простейшим средством обнаружения факта использования закладного устройства являются индикаторы поля (Рисунок 1.9). По характеристикам, это приемники с очень низкой чувствительностью, поэтому они детектируют излучение на очень малых расстояниях. Главной особенностью индикаторов поля является то, что они способны находить передающее устройство вне зависимости от применяемой в них модуляции.

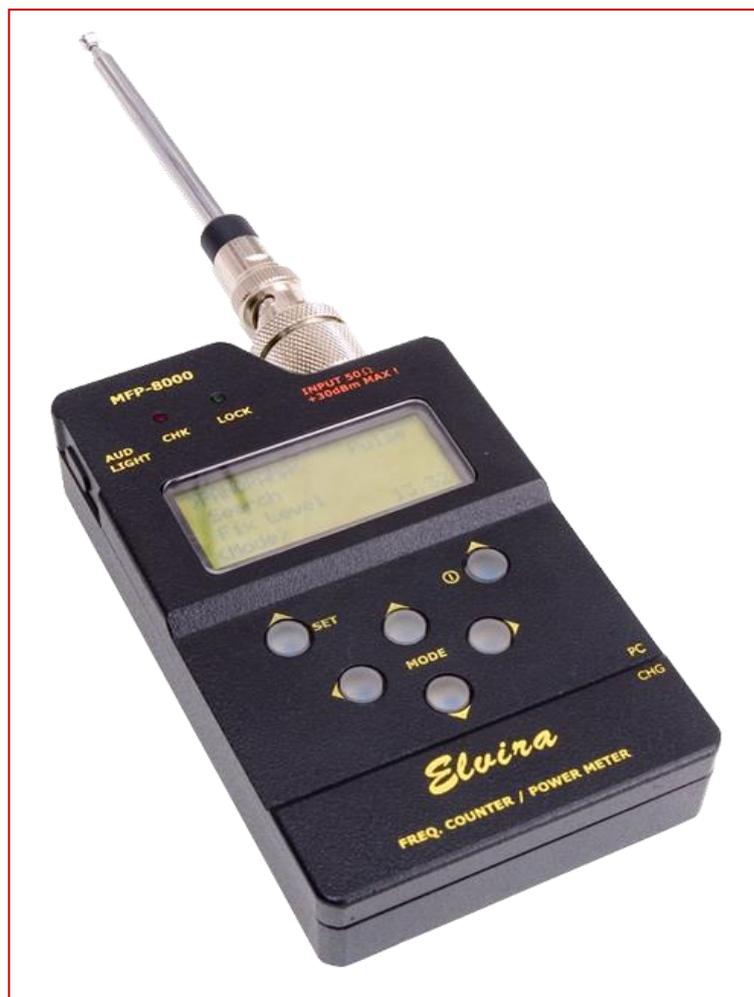


Рисунок 1.9 - индикатор поля

Специальные радиоприемные устройства (Рисунок 1.10) являются более сложными и надежными средствами, чем индикаторы поля. Они позволяют настраиваться на частоту работы устройства, скрытно передающего информацию, обладают функциями выделения сигнала из фоновых помех и имеют возможность демодуляции сигнала.

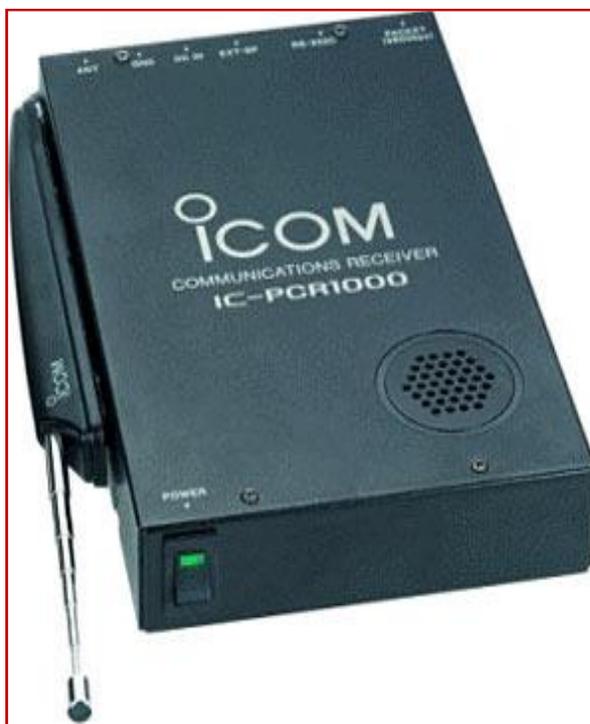


Рисунок 1.10 - специальный радиоприемник для детектирования закладных устройств

Так как закладки передают информацию в большом диапазоне, то специальные приемники позволяют контролировать очень большой диапазон частот, причем, либо контролировать весь диапазон сразу, либо перестраиваться на разные частоты за очень малый промежуток времени.

Более совершенными средствами поиска закладных устройств являются программно-аппаратные комплексы (Рисунок 1.11). У данных устройств можно выделить следующие особенности:

- Выявление излучения закладных устройств;
- Определение дальности до источника;
- Определение потенциально-опасного сигнала

- Контроль слаботочных сетей на наличие посторонних излучений;
- Работа в многоканальном режиме;
- Постановка помех.



Рисунок 1.11 - программно-аппаратный комплект для детектирования закладных устройств