Для аналізу методів та засобів виявлення засобів захисту аудіоінформації, що розповсюджується по радіоканалу потрібно визначитись у тому, які засоби використовуються при інформаційній атаці у цьому випадку. Найбільш поширені у використанні радіозакладні пристрої. До їх основних параметрів відносяться:

- несуча частота радіоканалу;

- потужність радіопередавача;

- вид модуляції;

- ширина займаної смуги частот;

- стабільність частоти;

- режим (замкненість) роботи.

Як витікає з цих даних, в основному використовується діапазон 174….500 МГц. Це є діапазони прикордонні до радіо-, телемовленню та відомчим (залізнодорожний зв’язок, авіадиспетчерський, служби охорони). Це допомагає маскувати радіосигнали і потребує спеціальних заходів їх приймання.

Вважається, що апаратура з потужністю більше 20 мВт призначається для професіоналів.

В основному використовуються 3 види модуляції:

- широкосмугова частотна;

- вузькосмугова частотна;

- цифрова.

Наймогутніші фірми використовують цифрове розширення спектру. Професіонали полюбляють вузькосмугову модуляцію, забезпечуючи себе стабільним прийманням та високою завадозахищеністю. Диктофони та акустичні радіозакладні пристрої мають у своєму складі багато напівпровідникових елементів. Таким чином найбільш ефективним засобом їх виявлення є нелінійний локатор.

Тим більше, що професіонали все частіше використовують метод “опромінювання”, котрий оснований на ефекті додаткової модуляції інформаційним сигналом радіохвиль, що

розповсюджуються на даний момент у зоні роботи технічного засобу, котрий оброблює на даний момент інформацію. Такий канал витоку інформації селектувати дуже важко, бо фактично ситуація схожа на використання методики ВЧ нав’язування без використання спеціального джерела ВЧ випромінювання. У таких випадках використання нелінійного локатора є чи не єдиним способом виявлення закладних пристроїв і розділу каналу витоку на такий, що використовує тактику закладних.

Радіозакладні пристрої можна виявляти, також, детекторами поля, інтерсепторами, радіочастотовимірювачами, скануючими приймачами, програмно-апаратними комплексами, як наприклад приймачWinradio, виконаний у вигляді друкованої плати ISA IBM під’єднуємої до слоту комп’ютера, тощо.

Для виявлення працюючих в режимі запису диктофонів використовують так звані детектори диктофонів. Принцип дії оснований на виявленні слабкого магнітного поля, котре утворюється працюючим генератором підмагнічування або двигуном диктофона. Для прийому таких сигналів використовують магнітні антени. Для виключення хибних спрацювань поріг виявлення необхідно коригувати перед кожним сеансом роботи, що є недоліком подібних приладів.

Активний засіб боротьби з диктофонами оснований на принципі електромагнітного придушення. При цьому генерується в ДМВ діапазоні частот (частіше, близько 900 мГц), потужних шумових сигналів. За рахунок направлених антен ці сигнали наводять в підсилювачах низької частоти та підсилювачах запису завадні сигнали. Інформаційний сигнал при цьому у значній мірі спотворюється. Радіус дії подавляючих пристроїв залежить від потужності передавача та характеристики направленості антени. Звичайно зона придушення має вигляд сектора з кутом 30…80 градусів і радіусом дії 1,5 метри (для диктофонів в екранованому корпусі).

Системи придушення в ультразвуковому діапазоні випромінюють потужні імпульси на частотах, котрі не сприймаються вухом людини (звичайно, це частота 20 кГц). Такі імпульси діють безпосередньо на мембрани мікрофонів диктофонів. Це є їх великою перевагою. Крім спотворення акустичного сигналу на мембрані мікрофону, присутній також ефект перевантаження підсилювачів звукової частоти до рівнів, при котрих система автоматичного регулювання підсилення вже не працює. Крім того, такі системи блокують акустичні приймачі у значно більшому секторі.