Vasko Kyrylo FB-61

17.03.2020

# Пошукові пристрої та пристрої інформаційної атаки. Приклади та характеристики;

Технічні заходи направлені на зачинення каналів витоку інформації за рахунок ослаблення рівня інформаційних сигналів , або зменшення співвідношення сигнал/завада в місцях можливого розміщення засобів розвідки або їх датчиків до рівнів, унеможливлюючих виділення інформаційних сигналів засобами розвідки, і провадяться з використанням активних та пасивних засобів.

До технічних заходів з використанням пасивних засобів відносяться:

\*контроль та обмеження доступу на об’єкти ТЗПІ та виділені приміщення:

- встановлення на об’єктах ТЗПІ та у виділених приміщеннях технічних засобів та систем обмеження і контролю доступу.

\*локалізація випромінювання:

- екранування ТЗПІ та з’єднувальних ліній;

- заземлення ТЗПІ і екранів їх з’єднувальних ліній;

- звукоізолювання виділених приміщень.

\*розв’язування інформаційних сигналів:

- встановлення спеціальних засобів захисту типу “Граніт” у допоміжних технічних засобах та системах, що мають “мікрофонний ефект” і таких, що мають вихід за межі КЗ;

- встановлення спеціальних діелектричних вставок в оплітення кабелів електроживлення, труб систем опалення, водозабезпечення і каналізації, що мають вихід за межі КЗ;

- встановлення автономних або стабілізованих пристроїв електроживлення ТЗПІ (наприклад, мотор-генераторів);

- встановлення в мережах електроживлення ТЗПІ, а також в лініях освітлювальної

та розеточної мережі виділених приміщень завадопоглинаючих фільтрів типу ФП.

То технічних заходів з використанням активних засобів відносяться:

\*просторове зашумлення:

- просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад (при умові виявлення та з’ясування частоти випромінювання закладного пристрою або ПЕМВ ТЗПІ) з використанням засобів створення прицільної завади;

- створення акустичних і вібраційних завад з використанням генераторів акустичного шуму – шумотронів.

- придушення диктофонів в режимі запису з використанням придушуючих пристроїв.

\*лінійне зашумлення:

- лінійне зашумлення ліній електроживлення;

- лінійне зашумлення сторонніх дротів та з’єднувальних ліній ДТЗС, що виходять за межі КЗ.

\*знешкодження закладних пристроїв:

- знешкодження закладних пристроїв, що підключені до лінії, з використанням спеціальних генераторів імпульсів (випалювачів “жучків”).

Виявлення закладних пристроїв здійснюється проведенням спеціальних досліджень та спеціальних перевірок об’єктів ТЗПІ та виділених приміщень.

Спеціальні дослідження виділених приміщень та об’єктів ТЗПІ провадяться шляхом іх візуального огляду без залучення технічних засобів.

Спеціальна перевірка провадиться з використанням технічних засобів. При цьому здійснюється:

\*виявлення закладних пристроїв з використанням пасивних засобів:

- встановлення засобів і систем виявлення лазерного випромінювання (підсвітлення) віконних стекол;

- встановлення стаціонарних виявителів диктофонів;

- розшук закладних пристроїв з використанням індикаторів поля, інтерсепторів, частотомірів, скануючих приймачів та програмно-апаратних комплексів контролю.

- організація радіоконтролю (постійно, або на час проведення конфіденційних заходів) і побічних електромагнітних випромінювань ТЗПІ.

\*виявлення закладних пристроїв з використанням активних засобів:

- спеціальна перевірка виділених приміщень з використанням нелінійних локаторів;

- спеціальна перевірка виділених приміщень, ТЗПІ та допоміжних технічних засобів з використанням рентгенівських комплексів

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.

Ведучими виробниками такої техніки є фірми з більш як 30-річним досвідом роботи і їх продукція відрізняється широким спектром зазначених вище параметрів у різноманітних комбінаціях в залежності від конкретного призначення:

-“РК ELECTRONIC” (ФРН);

-“Knowledge Express Inc.” (USA);

-“SURVEILANCE TECHNOLOGY GROUP (STG)”, Port Chester, USA;

-“CCS”, New York, USA

-“LAW ENFORCEMENT ASSOCIATES, INC.”, Raleigh, USA

-“Westinghouse Audio Intelligence Devices”, USA

-“SIPE ELECTRONIC”.

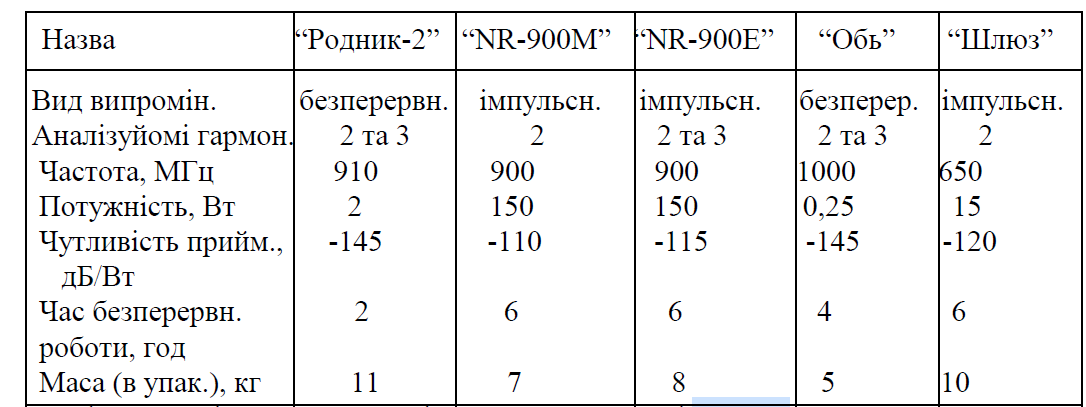
Кожна фірма по-своєму зорієнтована на виготовлення тієї чи іншої продукції. Для отримання наглядності картини про орієнтацію фірм та основні параметри закладних пристроїв, зосередимось на таких параметрах закладних пристроїв:

- несуча частота;

- потужність випромінювання;

- вид модуляції.

Зараз широке використання отримали нелінійні локатори “Родник-2”, “NR-900M”, “NR-900E”, “Обь”, “Шлюз”, “BROOM”, “SUPERBROOM”, “SUPERSCOUT”, “Переход”, “Энвис”, “Сандал-СМ”, “Изумруд-ДМ”, “РК-885-S” та багато інших.



# Об’єкти захисту інформації (ЗІ) та технічні канали її витоку

Основними об’єктами захисту інформації є:

1- інформаційні ресурси, котрі несуть у собі відомості, що можуть відноситись до державної таємниці та конфіденційної інформації:

2- системи та засоби інформатизації (засоби обчислювальної техніки, інформаційно-обчислювальні комплекси, мережі та системи); програмні засоби (операційні системи, системи керування базами даних та інше загальносистемне та прикладне програмне забезпечення), автоматизовані системи керування, системи зв’язку та передачі даних, технічні засоби отримання, передавання та обробки інформації з обмеженим доступом (звукозапис, звукопідсилення, звукосупроводження, переговорні та телевізійні пристрої, засоби тиражування та виготовлення документів та інші технічні засоби обробки графічної, алфавітно-цифрової та змістовної інформації), їх інформативні фізичні поля. Ці засоби часто називають технічними засобами прийому, обробки, зберігання та передавання інформації (ТЗПІ).

3 - технічні засоби і системи, котрі не відносять до засобів та систем автоматизації (ТЗПІ), але розташовані в приміщеннях де оброблюється таємна і конфіденційна інформація. Такі засоби і системи називають допоміжними технічними засобами і системами (ДТЗС). До них відносяться технічні засоби відкритого телефонного, гучномовного зв’язку, системи пожежної та охоронної сигналізації, система енергопостачання, радіотрансляційна мережа, системи часофікації, енергопобутові прилади і т.д., а також самі приміщення, де оброблюється інформація обмеженого поширення.

При організації захисту інформації ТЗПІ слід розглядати як систему, що включає до свого складу основне (стаціонарне) обладнання, кінцеві пристрої, з’єднувальні лінії (сукупність дротів та кабелів, що прокладені між окремими ТЗПІ та їх елементами), розподіляючі та комунікаційні пристрої, системи електроживлення, заземлення.

Окремі технічні засоби або група технічних засобів, що призначаються для обробки конфіденційної інформації, разом з приміщенням, де вони розташовані, складають об’єкт ТЗПІ. Під об’єктом ТЗПІ розуміють також виділені приміщення, що призначені для проведення секретних заходів.

В якості елементів каналів витоку інформації найбільший інтерес представляють ТЗПІ і ДТЗС, котрі мають вихід за межу зони що контролюється (КЗ). КЗ це зона, де виключена можливість появи суб’єктів чи транспортних засобів, котрі не мають постійних чи часових перепусток.

Окрім з’єднувальних ліній ТЗПІ і ДТЗС за межу КЗ можуть виходити дроти та кабелі, котрі не мають до них відношення, але котрі проходять скрізь приміщення, де встановлені технічні засоби, а також металеві труби опалення, водопостачання та інші струмопровідні металоконструкції. Такі дроти, кабелі і струмопровідні елементи називають сторонніми провідниками.

Зона, де є можливим перехват (за допомогою розвідувального приймача) побічних електромагнітних хвиль та подальша розшифровка інформації, котру вони несуть, (це є зона, в межах котрої відношення “сигнал/завада” вище за декотре нормоване значення) називається (небезпечною) зоною 2.

Простір навкруги ТЗПІ, в межах котрого на випадкових антенах наводяться інформаційні сигнали вищі за нормований рівень, називають (небезпечною) зоною 1.

Випадковою антеною є мережа ДТЗС чи сторонні провідники, здатні приймати побічні електромагнітні сигнали. Випадкові антени можуть бути зосередженими та розсередженими.

Зосереджена випадкова антена представляє собою компактний технічний засіб, наприклад телефонний апарат, гучномовець радіотрансляційної мережі і т. п. До розсереджених випадкових антен відносять випадкові антени з розсередженими параметрами: кабелі, дроти, металеві труби та інші струмопровідні комунікації.

Перехоплення інформації, що обробляється на об’єктах ТЗПІ, здійснюється по технічних каналах.

Під технічним каналом витоку інформації (ТКВІ) розуміють сукупність об’єкту розвідки, технічного засобу розвідки (ТЗР), за допомогою котрого отримується інформація про цей об’єкт, та фізичне середовище, по котрій розповсюджується інформаційний сигнал. По суті, під ТКВІ розуміють спосіб отримання за допомогою ТЗР розвідувальної інформації про об’єкт розвідки. При цьому форма представлення інформації може бути довільна.

Сигнали є матеріальними носіями інформації. За своєю фізичною природою сигнали можуть бути електричними, електромагнітними, акустичними.

В залежності від природи сигнали поширюються у визначених фізичних середовищах. Середовищем поширення можуть бути гасові, рідинні, тверді середовища. Наприклад, повітря, конструкції будівель, струмоведучі кабелі та дроти, земляний грунт тощо.

Для прийому та вимірювання параметрів сигналів використовують технічні засоби розвідки (ТЗР).

За фізичним принципом технічні канали витоку інформації можуть бути класифіковані за групами:

- акустичні (включаючи акустоперетворювальні);

- візуально-оптичні (спостереження, фотографування і т.п.);

- електромагнітні (а також з розподілом на електричні і магнітні окремо);

- матеріальні (папір, фото, магнітні носії, відходи різного характеру та ін.).

За способом отримання інформації класифікації можуть підлягати методи несанкціонованого доступу до неї:

- акустичний контроль приміщень, автомобіля, людини, контроль та прослуховуван-ня телефонних каналів зв’язку, перехоплення факсових та модемних сеансів зв’язку;

- перехоплення комп’ютерної інформації (у тому числі радіовипромінювання комп’юте-ра), несанкціонований доступ до бази даних;

- прихована фото- та відеоз’омка з застосуванням спеціальної оптики;

- візуальне спостереження за об’єктом;

- несанкціоноване ознайомлення з документами;

- аналітичне обстеження процесу діяльності підприємства, його корисного продукту та відходів, в тому числі хімічний аналіз зовнішніх викидів;

- аналітичне ознайомлення з публікаціями та рекламними матеріалами підприємства;

- несанкціоноване отримання інформації про особу шляхом підкупу та шантажу службовців, оточення та родичів.