**1. Поєднання технічних та організаційних заходів для захисту ОІД;**

Організаційні заходи – це заходи до захисту інформації, проведення котрих не потребує використання спеціально розроблених технічних засобів.

До основних організаційних заходів відносяться:

- залучення до проведення робіт для захисту інформації організацій, що мають ліцензію на діяльність в області ТЗІ, що надається відповідними органами;

- категоріювання і атестація об’єктів ТЗПІ і виділених для проведення секретних

заходів приміщень (далі **виділених приміщень**) до виконання вимог забезпечення захисту інформації при проведенні робіт з відомостями відповідного ступеня секретності;

- використання на об’єкті сертифікованих ТЗПІ і ДТЗС;

- встановлення контрольованої зони навкіл об’єкту;

- залучення до роботи по будуванню, реконструкції об’єктів ТЗПІ, монтуванню апаратури організацій, що мають ліцензію на діяльність в області захисту інформації за відповідними пунктами;

- організація контролю та обмеження доступу на об’єкти ТЗПІ та у виділені приміщення;

- введення територіальних, частотних, енергетичних, просторових і часових обмежень в режимах використання технічних засобів, що підлягають захисту;

- відключення, на період проведення секретних заходів технічних засобів, що мають елементи з якостями електроакустичних перетворювачів, від ліній зв’язку і т.і.;

***+: можливо побудувати ідеальну систем захисту***

***-: буль-яка інстррукція не змінює фізичних законів***

Технічні заходи – це заходи з захисту інформації, котрі передбачають використання спеціальних технічних засобів, а також реалізацію технічних рішень.

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”).

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.

**2. Захист каналів зв’язку;**

Основною одиницею прийому-передачі даних на канальному рівні є символи або блоки символів. Найпростішим символом передачі даних є біт. Сучасні телекомунікаційні системи використовують більші символи, що містять від 2 до 64 біт і більше. Головна мета боротьби з природними перешкодами в каналі зв'язку - це підвищення достовірності інформації що передається, тобто обмеження ймовірності прийому помилкового символу. Для цього застосовують т.зв. надлишкове кодування, при якому на передавальній стороні змістовні блоки символів відображаються в розширені блоки передачі, аналіз яких на приймальній стороні каналу дозволяє виявити або виправити помилки певних типів. Для захисту інформації в каналі зв'язку від несанкціонованого доступу типу «прослуховування» використовують різні методи криптографії (шифрування даних): заміна (підстановка) символів, перестановка, аналітичні перетворення шифрованих даних та інші. Поширений метод шифрування - це заміна переданих символів на символи з того ж самого алфавіту, здійснювана по секретним таблицям шифрування. На основі цього методу можна побудувати алгоритм, який в принципі не піддається дешифруванню при відсутності таблиці шифрування. Для цього достатньо, щоб множина символів підстановки утворювала випадкову послідовність довжиною не менше переданого повідомлення (з однаковою ймовірністю всіх символів підстановки і незалежністю між будь-якою парою символів підстановки). Обмеження такого методу шифрування Комп’ютерні мережеві технології 74 обумовлені технічними можливостями створення, обміну та зберігання таблиць шифрування великих розмірів. Підвищення швидкості передачі і зменшення енергії на одиницю інформації в оптичних каналах обумовлює появу квантових ефектів, пов'язаних з нечіткою ідентифікацією прийнятих символів. З точки зору детектора сигналу, один і той символ (наприклад, один біт), що генерується на передавальній стороні каналу, може перебувати в двох станах (нуль і одиниця). При цьому відносні частоти появи нулів і одиниць наближаються до можливостям їх появи. Однак при однаковій фізичній швидкості передавання символів, збільшення надмірності переданих блоків символів призводить до зниження кількості корисної інформації. При цьому зменшується ймовірність помилок; це, в свою чергу, дозволяє збільшити фізичну швидкість передачі. В результаті взаємного впливу цих факторів може бути досягнуто загальне підвищення ефективності передавання корисної інформації. Властивості каналу зв'язку з квантовими ефектами визначаються матрицею ймовірностей

Pi,k = p(i,k), де i - значення переданого символу, j - значення прийнятого символу.

Ця матриця є чутливою до змін фізичних властивостей каналу, наприклад, при несанкціонованому доступі до каналу матриця зміниться в тій чи іншій мірі. Дана матриця є унікальною характеристикою каналу зв'язку, яка може бути досліджена в метрологічному експерименті, а далі використана для детектування сигналів та виявлення несанкціонованого доступу. Квантові методи у криптографії поки що знаходяться у стадії активного розвитку. Однією з основних проблем у квантовій криптографії є підвищення швидкості передачі даних на великі відстані.

Захист інформації, що оброблюється ТЗПІ, здійснюється з використанням пасивних та активних методів та засобів.

Пасивні методи захисту направлені на:

1)ослаблення інформаційних сигналів ТЗПІ на межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

2)ослаблення наведень побічних електромагнітних випромінювань ТЗПІ на сторонні провідники та з’єднувальні лінії ДТЗС, що виходять за межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

3)виключення (ослаблення) просочування інформаційних сигналів ТЗПІ до мереж

живлення що виходять за межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

Активні методи захисту спрямовані на:

- створення просторових маскуючих електромагнітних завад з ціллю зменшення

відношення сигнал/завада на межі зони що контролюється до рівнів,

унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

- створення маскуючих електромагнітних завад у сторонніх провідниках та

з’єднувальних лініях ДТЗС з ціллю зменшення відношення сигнал/завада на межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на

шумовому фоні;

**3. Активні засоби. Постановка завад. Види завадових сигналів. Приклади приладів та їх характеристики;**

Для захисту мовної (акустичної) інформації використовують активні і пасивні методи та засоби.

Активні засоби направлені на:

- створення маскуючих акустичних та вібраційних завад з ціллю зменшення рівня с/з на кордоні КЗ до рівнів, унеможливлюючих їх виділення інформаційних сигналів засобами розвідки;

- створення маскуючих електромагнітних завад у з’єднувальних лініях ДТЗС, що мають електроакустичні перетворювачі;

- електромагніте придушення диктофонів у режимі запису;

- ультразвукове подавлення диктофонів у режимі запису;

- створення маскуючих електромагнітних завад в лініях електроживлення ДТЗС, що мають мікрофонний ефект;

- створення прицільної радіозавади акустичним та телефонним закладним радіопристроям;

- знешкодження засобів несанкціонованого підключення до телефонних ліній.

**4. Віброакустичне маскування.**

Метод віброакустичного маскування відноситься до активного методу захисту, за допомогою котрого забезпечується зниження відношення с/з. Метод ефективний для захисту від витоку по прямому акустичному каналу.

Для формування акустичних завад використовуються спеціальні генератори. Кінцевим пристроєм цих генераторів є гучномовці або вібраційні випромінювачі. На рактиці найчастіше використовуються генератори шуму. Тому нерідко таке маскування називають акустичним зашумленням. В якості елемента формування шумових сигналів використовують вакуумні, газорозрядні, напівпровідникові та інші елементи, а також цифрові пристрої.

На цей час створено багато різноманітних систем віброакустичного маскування. Це такі системи, як “Заслон”, “Кабінет”, “Барон”, “Фон-В”, “VNG-006”, “ANG-2000”, “NG-101”, “АД-24”, “Г-002” та інші. Характеристики декотрих з них зведені до таблиці.

Основні характеристики декотрих систем віброакустичного зашумлення

