Завдання №12

1. Об’єкти захисту інформації (ЗІ) та технічні канали її витоку;

2. Захист каналів зв’язку;

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

4. Закриття мовних сигналів в телефонних каналах.

Відповіді:

1. Об’єктами захисту інформації є:

* Інформаційні ресурси (несуть у собі відомості, що можуть відноситись до державної таємниці та конфіденційної інформації)
* Системи та засоби інформатизації, програмні засоби (ОС, БД, , інформаційно-обчислювальні комплекси та ін)
* Технічні засоби, які просто розташовані у приміщеннях, де оброблюється інформація

Під технічними каналами витоку розуміють сукупність об’єкту розвідки, технічного засобу розвідки (тобто за допомогою чого отримується інформація) та фізичне середовище (де розповсюджується сигнал).

За фізичним принципом технічні канали витоку бувають:

* Матеріальні (наприклад папір)
* акустичні
* візуально-оптичні (спостереження)
* електромагнітні

За способом отримання інформації:

* перехоплення комп’ютерної інформації
* прихована зйомка
* спостереження
* акустичний контроль приміщень

2. 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 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. 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.

В ТЗПІ захист інформації здійснюється за допомогою активних та пасивних методів. Активні методи направлені на створення маскуючих електромагнітних завад у сторонніх провідниках (з ціллю зменшення відношення сигнал/завада на межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні) та 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). Активні методи направлені на ослаблення інформаційних сигналів ТЗПІ на межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні, 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 та виключення просочування інформаційних сигналів ТЗПІ до мереж живлення що виходять за межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні.

3. Пошукові пристрої - це пристрої, які здійснюють виявлення засобів розвідки (мікрофоні, жучків).

Пристрої інформаційної атаки - це пристрої, які здійснюють атаку на властивості інформації (порушують конфіденційність, цілісність, доступність)

Найбільш поширені у використанні радіозакладні пристрої.

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.

Наприклад: нелінійні локатори “Родник-2”, “NR-900M”, “NR-900E”, “Обь”, “Шлюз”, “BROOM”, “SUPERBROOM”, “SUPERSCOUT”, “Переход”, “Энвис”, “Сандал-СМ”, “Изумруд-ДМ”, “РК-885-S” та ін.

4. Безпека зв'язку при передачі мовних повідомлень грунтується на використанні великої кількості різних методів приховування повідомлень, що змінюють характеристики мови таким чином, що вона стає нерозбірливою і невпізнанною для підслуховування особи, перехопив закрите мовне повідомлення.

Існують два основні методи закриття мовних сигналів: аналогове скремблирование і дискретизація мови з подальшим шифруванням.

Під Скремблювання розуміється зміна характеристик мовного сигналу так, щоб отриманий сигнал, володіючи властивостями нерозбірливості і невпізнання, займав таку ж смугу частот, що і вихідний, відкритий сигнал. У цифрових пристроях захисту інформації мовні компоненти перетворюються в цифровий потік даних і змішуються з деякою псевдослучайной послідовністю, що виробляється ключовим генератором. Отримане таким чином закрите мовне повідомлення передається в канал зв'язку, на приймальному кінці якого виробляються зворотні перетворення з метою отримання відкритого мовного сигналу.

Для передавання цифрової інформації використовують пристрої серії СМ: кишеньковий телекс-шифратор СМ-11, шифратор для телефаксів СМ-13, радіоперемовний чотириканальний пристрій СМ-21 для діапазону 134….174 мГц, та ін.