Завдання №6

1. Канали витоку інформації ОІД та ТЗПІ;

Технічному захисту підлягає інформація з обмеженим доступом, носіями якої є поля і сигнали, що утворюються в результаті роботи технічних засобів пересилання, оброблення, зберігання, відображення інформації (ТЗПІ), а також допоміжних технічних засобів і систем (ДТЗС).

До ТЗПІ відносяться:

- засоби і системи телефонного, телеграфного (телетайпного), директорського, гучномовного, диспетчерського, внутрішнього, службового та технологічного зв`язку;
- засоби і системи звукопідсилення, звукозапису та звуковідтворення;
- пристрої, що утворюють дискретні канали зв`язку: абонентська апаратура із засобами відображення та сигналізації, апаратура підвищення достовірності пересилання, каналоутворювальна тощо;
- апаратура перетворення, оброблення, пересилання і приймання відеоканалів, що містять факсимільну інформацію.

Можливі канали витоку інформації утворюються:

- - низькочастотними електромагнітними полями, які виникають під час роботи ТЗПІ та ДТЗС;
- - під час впливу на ТЗПІ та ДТЗС електричних, магнітних та акустичних полів;
- - під час виникнення паразитної високочастотної (ВЧ) генерації;
- - під час проходження інформативних (небезпечних) сигналів у колі електроживлення;
- - під час взаємного впливу кіл;
- - під час проходження інформативних (небезпечних) сигналів у колі заземлення;
- - під час паразитної модуляції високочастотного сигналу;
- - внаслідок хибних комутацій і несанкціонованих дій.

Всі канали витоку даних можна розділити на непрямі і прямі.

Непрямі канали не вимагають безпосереднього доступу до технічних засобів інформаційної системи. Прямі відповідно вимагають доступу до апаратного забезпечення і даних інформаційної системи.

Приклади непрямих каналів витоку:

- Крадіжка або втрата носіїв інформації, дослідження не знищеного сміття;
- Дистанційне фотографування, прослуховування;
- Перехоплення електромагнітних випромінювань.

Приклади прямих каналів витоку:

- Інсайдери (людський фактор). Витік інформації внаслідок недотримання комерційної таємниці;
- Пряме копіювання.

Канали витоку інформації можна також розділити за фізичними властивостями і принципам функціонування:

- акустичні — запис звуку, підслуховування і прослуховування;
- акустоелектричні — отримання інформації через звукові хвилі з подальшою передачею її через мережі електроживлення;
- віброакустичні — сигнали, що виникають за допомогою перетворення
- інформативного акустичного сигналу при впливі його на будівельні конструкції і інженерно-технічні комунікації приміщень, які захищаються;
- оптичні — візуальні методи, фотографування, відеозйомка, спостереження;
- електромагнітні — копіювання полів шляхом зняіншихття індуктивних наводок;
- радіовипромінювання або електричні сигнали від впроваджених в технічні засоби і приміщення спеціальних електронних пристроїв знімання мовної інформації «закладних пристроїв», які модульовані інформативним сигналом;
- матеріальні — інформація на папері або фізичних носіях інформації

2. Захист каналів зв’язку;

Технічні заходи захисту:

1. Встановити високочастотні ОТЗ в екрановане приміщення (камеру);
2. Встановити в незахищені канали зв`язку, лінії, проводи і кабелі спеціальні фільтри та пристрої.
3. Прокласти проводи і кабелі в екранувальних конструкціях;
4. Зменшити довжину паралельного пробігу кабелів і проводів різних систем з проводами та кабелями, що несуть ІзОД;
5. Виконати технічні заходи щодо захисту ІзОД від витоку колами заземлення та електроживлення.

Технічні засоби захисту:

1. фільтри-обмежувачі та спеціальні абонентські пристрої захисту для блокування витоку мовної ІзОД через двопровідні лінії телефонного зв`язку, системи директорського та диспетчерського зв`язку;
2. пристрої захисту абонентських однопрограмних гучномовців для блокування витоку мовної ІзОД через радіотрансляційні лінії;
3. фільтри мережеві для блокування витоку мовної ІзОД колами електроживлення змінного (постійного) струму;

4. фільтри захисту лінійні (високочастотні) для встановлення в лініях апаратів телеграфного (телекодового) зв`язку;
5. генератори лінійного зашумлення;
6. генератори просторового зашумлення;
7. екрановані камери спеціальної розробки.

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

4. Закриття мовних сигналів в телефонних каналах.

У мовних системах зв'язку відомі два основні методи закриття мовних сигналів, що відрізняються способом передачі в каналах зв'язку: аналогове ськремблювання і дискретизація мови з подальшим шифруванням (цифрові системи закриття). Кожний з цих методів має свої переваги та недоліки.

Під аналоговим скремблюванням розуміють таку зміну характеристик мовного сигналу, при якому одержаний модульований сигнал, володіючи властивостями нерозбірливості і невпізнання, займає таку ж смугу частот спектру, як і початковий відкритий сигнал. З аналогових методів практичне застосування одержало частотне і тимчасове скремблювання, а також їх комбінація. Частотне скремблювання буває двох видів — інверсне і смугове.

Інверсний скремблер здійснює перетворення мовного спектру, рівносильне повороту спектру мовного сигналу навколо деякої середньої крапки. При цьому нижні частоти перетворяться у високі і навпаки. Цей спосіб володіє невисоким рівнем закриття, оскільки при перехопленні легко встановлюється частота, відповідна середній точці інверсії в смузі спектру мовного сигналу.

Смуговий скремблер розділяє мовний спектр на декілька смуг з подальшим їх перемішуванням і інверсією за деяким правилом, або ключем. Зміна ключа дозволяє підвищити ступінь закриття, але при цьому потрібне введення синхронізації на приймальній стороні системи. Недоліком цього виду скремблювання є те, що основна частина енергії мовного сигналу зосереджена в невеликій області низькочастотного спектру. Тому вибір варіантів перемішування обмежений і багато хто з систем характеризується відносно високою залишковою розбірливістю.

Шифрування мовних сигналів, перетворених в цифрову форму, є альтернативним аналоговому скремблювання методом передачі мови в закритому вигляді. Основою пристроїв, що працюють за таким принципом, є представлення мовного сигналу у вигляді цифрової послідовності, що

закривається по одному з криптографічних алгоритмів (RSA, DES і ін.). Передача даних, що представляють дискретизовані відліки мовного сигналу або його параметрів, по телефонних каналах, як і при шифруванні буквено-цифрової і графічної інформації, здійснюється через модеми.

У цифровому закритті мовних сигналів широко поширені системи на базі вокодеров. У таких системах пристрій кодування мови (вокодер), аналізуючи форму мовного сигналу, оцінює параметри змінних компонент моделі генерації мови і передає значення цих параметрів в цифровій формі по каналу зв'язку на синтезатор, де по прийнятих параметрах синтезується мовне повідомлення. Цифрова послідовність параметрів мови з виходу вокодерного пристрою подається на вхід шифратора, де піддається перетворенню по одному з криптографічних алгоритмів, потім поступає через модем в канал зв'язку, на приймальній стороні якого здійснюються зворотні операції по відновленню мовного сигналу.