Завдання №6

1. Канали витоку інформації ОІД та ТЗПІ;

2. Захист каналів зв’язку;

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

4. Закриття мовних сигналів в телефонних каналах.

3.Активні методи захисту:

-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;

Завади, котрі враховуються при визначенні захищеності інформації від витоку, повинні

задовільняти слідуючим вимогам: - маскуючі властивості завад повинні зберігатись на

заданому рівні при використанні будь-яким з методів обробки суміші сигнал-завада. Інакше кажучи, властивості завад повинні бути стабільними в часі і в просторі. Завади, котрі діють у КВ інформації, як витікає з вище зазначеного, складаються з багатьох компонент з різним ступенем детермінованості, з різними розподіленнями потужності по частоті і стабільністю рівня в часі і просторі. На основі аналізу зазначених джерел завад та вимог до них і

розроблюються методики визначення рівнів завад в КВ інформації. За допомогою

зазначених методик провадять виміри.Використання мінімальних значнь завад гарантує ефективний захист інформації від витоку незалежно від розміщення об’єктів.

4.Закриття мовних сигналів в телефонних каналах.

Безпека зв'язку при передачі мовних повідомлень грунтується на використанні різних методів закриття, що міняють характеристики мови так, що вона стає нерозбірливою і невпізнанною для особи, що підслуховує мовне повідомлення. Метод закриття залежить від вигляду, конкретного застосування і технічних характеристик каналу передачі.

У мовних системах зв'язку відомі два основні методи закриття мовних сигналів, що відрізняються способом передачі в каналах зв'язку: аналоговий скремблінг і дискретизація мови з подальшим шифруванням (цифрові системи закриття).

Під аналоговим скрмблінгом 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 частотний і тимчасови скремблінг, а також їх комбінація.

Скремблер - це програмний або апаратний пристрій, призначений для зміни мовного повідомлення при передачі і його відновлення при прийомі за допомогою певних алгоритмів і ключів.

Методи скремблювання поділяються :

аналогові ,

цифрові.

Аналогові скремблери поділяються на статистичні(схема кодування яких залишається незмінною упродовж всієї передачі мовного повідомлення) та динамічні(які постійно генерують кодові підстановки впродовж передачі).

При аналоговому скремблюванні зазвичай реалізуються два основні способи шифрування : частотні або тимчасові перестановки. При тому і іншому способі характеристики передаваного сигналу змінюються таким чином, що сигнал, виділений за допомогою звичайного телефонного апарату, стає нерозбірливим, але займає ту ж частотну смугу, що дозволяє його передавати по лініях зв'язку в звичайному режимі. При частотному скремблюванні за допомогою частотних фільтрів уся смуга стандартного телефонного сигналу дробиться на якесь число частотних смуг. Ці частотні інтервали перемішуються потім в заданому порядку, наприклад, за законом псевдовипадкової послідовності.

До переваг аналогового способу шифрування слід віднести його простоту і меншу вартість подібних пристроїв в порівнянні з приладами, що реалізовують функцію захисту цифровим способом, а також малі габарити.

Головним недоліком аналогового способу захисту є його менша стійкість до дешифрування. При виборі аналогового скремблера слід звертати увагу на складність ключів і перетворень, вживаних в його системі шифрування.

Динамічні системи забезпечують більш високу степінь захисту, оскільки різко обмежують можливість легкого прослуховування переговорів сторонніми особами.

Рівень захищеності передаваної інформації визначаэться за складністю сигналу.

На даний момент на ринку скремблери представлені багатьма фірмами. Розглянемо детальніше деякі з них.

ST-020

Один з перших на ринку з’явився аналоговий частотний інверсійний скремблер фірми Selectone .

Технічні характеристики:

Виробник : Selectone;

Режим работи: симплекс

Діапазон частот: 300-2400Гц

Кількість частот інверсії: 8

Діапазон напруги живлення: 5,2 -18В

Струм споживання: 4 мА

Діапазон рабочих температур: -30... +70 С

Розміри: 21х38х4 мм

Також існують інші моделі цього виробника, наприклад ST-22.

Модели ST-22 відрізняється розширеним діапазоном частот (до 3000Гц) і напруги живлення (до 24 В), а також меншеними розмірами (20х25х4 мм).

Так само Selectone випускав моделі з тимчасовим перетворенням ST – 50 серії, але наразі вони не є доступними для продажу.

VPU-1

Аналоговий частотний інверсійний скремблер

Технічні характеристики:

Виробник : Midian;

Режим работи: дуплекс;

Діапазон частот: 300-2600Гц

Кількість частот інверсії: 3

Діапазон напруги живлення: 5,5 -24В

Струм споживання: 5 мА

Діапазон рабочих температур: -30... +60 С

Розміри:36х24х6 мм

Midian надає користувачеві вибір конкретної моделі для використання у складі своїх радіозасобів. Для використання в дуплексних станціях виробник надає два скрамблера -VPU - 1 і VPU – 8, які відрізняються габаритами(36х24х6 мм для VPU – 8) та кількістю частот інверсії(1 для VPU – 8). Ціна VPU – 8 в два рази нижча – лише 35 USD

Симплексний режим роботи забезпечують скрамблери VPU – 2, VPU - 7 і VPU - 15 .

KVS-1

Аналоговые частотные инверсионные скремблеры.

Технічні характеристики:

Виробник : Kenwood;

Режим работи: симплекс;

Діапазон частот: 300-2400Гц

Кількість частот інверсії: 8

Діапазон напруги живлення: 5 -12В

Струм споживання: 4 мА

Діапазон рабочих температур: -30... +60 С

Розміри:35х20х5 мм

04ХК100-01

Засоби серії 04ХК100-01 призначені для технічного захисту інформації від прослуховування в каналі зв'язку, а також захисту не категорійованої службової інформації обмеженого поширення, що не відноситься до категорій конфіденційної і такої, що не становить державну таємницю.

Основні характеристики:

кількість незалежних ключів - 232

кількість оперативно змінюваних ключів - не більше 8

смуга частот мовного сигналу від 0,3 до 3,4 кГц

затримка мовної інформації не більше 250 мс

розбірливість відновлюваної мови - 1 клас

прослуховування каналу - не менше 99,9%

1. Канали витоку інформації ОІД та ТЗПІ;

Канали витоку:

1)За фізичним принципом:

- 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).

2)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’ютера), 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

2.Захист інформації, що оброблюється ТЗПІ, здійснюється з використанням пасивних та

активних методів та засобів.

Пасивні методи захисту 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;

- 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;