Колісніченко Ольга, ФБ-62

Варіант 6

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.

1. **Канали витоку інформації ОІД та ТЗПІ;**

ТЗПІ –будь який технічний засіб для отримання, зберігання, обробки Ізод.

1. Витік по мережі опалювання, газо- та водопостачання;

2. Витік по мережі електроживлення;

1. Витік по мережі трансляції і гучномовному зв'язку;
2. Витік через лінії зв'язку;
3. Візуальне зняття з дисплея і принтера;
4. Зняття з дисплея по електромагнітному каналу;
5. Зняття з клавіатури і принтера по акустичному каналу;
6. Зняття інформації за рахунок використовування "телефонного вуха";
7. Несанкціоноване копіювання;
8. Зняття інформації направленим мікрофоном;
9. Високочастотний канал витоку в побутовій техніці;
10. Розкрадання носіїв інформації;
11. Зняття акустичної інформації з використанням диктофонів;
12. Дистанційне зняття відео інформації (оптика);
13. Зняття інформації за рахунок наведень і „ нав'язування " ;
14. Комп'ютерні віруси, логічні бомби і т.п.;
15. Виробничі і технологічні відходи;
16. Лазерне зняття акустичної інформації з вікон;
17. Зняття інформації за системою вентиляції
18. Радіо-закладки в стінах і меблях;
19. Програмно-апаратні закладки в ПЕОМ;
20. Зняття інформації з використанням відео-закладок;
21. Витік за рахунок структурного звуку в стінах і перекриттях

середовища їх поширення та засобів перехоплення ТЗР технічні канали витоку інформації можна розділити на:

електромагнітні, електричні і параметричний - для телекомунікаційної інформації;

повітряні (прямі акустичні), вібраційні (віброакустичні), електроакустичні, оптико-електронний і параметричний - для мовної інформації.

При виявленні технічних каналів витоку інформації ТЗПІ необхідно розглядати|розглядати| як систему, що включає основне (стаціонарне) устаткування|обладнання|, кінцеві пристрої|устрої|, контактні лінії (сукупність дротів|проводів| і кабелів, що прокладаються між окремими ТЗПІ і їх елементами), розподільні і комутаційні пристрої|устрої|, системи електроживлення, системи заземлення.

Електромагнітні канали витоку інформації:

До електромагнітних відносяться канали витоку інформації, що виникають за рахунок різного виду побічних електромагнітних випромінювань (ЕМВ) ТЗПІ: - випромінювань елементів ТЗПІ;

- випромінювань на частотах роботи високочастотних (ВЧ) генераторів ТЗПІ; - випромінювань на частотах самозбудження підсилювачів низької частоти (ПНЧ) ТЗПІ.

Електромагнітні випромінювання елементів ТЗПІ. У ТЗПІ носієм інформації є|з'являється| електричний струм|тік|, параметри якого (сила струму, напруга|напруження|, частота і фаза) змінюються за законом інформаційного сигналу. При проходженні електричного струму|току| по струмопровідним| елементах ТЗПІ навколо|довкола| них (у навколишньому|довколишньому| просторі|простір-час|) виникає електричне і магнітне поле. Через це елементи ТЗПІ можна розглядати|розглядати| як випромінювачі електромагнітного поля, модульованої згідно із законом зміни інформаційного сигналу.

Електричні канали витоку інформації:

Причинами виникнення електричних каналів витоку інформації можуть бути: ·| наведення електромагнітних випромінювань ТЗПІ на контактні лінії ДТЗС і сторонні провідники, що виходять за межі контрольованої зони; · витік інформаційних сигналів в ланцюзі|цепі| електроживлення ТЗПІ; · витік інформаційних сигналів в ланцюзі|цепі| заземлення ТЗПІ.

**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.

1. **Захист каналів зв’язку**

Пасивні методи захисту від ПЕМВН можуть бути розбиті на три групи:

• екранування;

• зниження потужності випромінювань і наведень;

• зниження інформативності сигналів.

Екранування є одним з найефективніших методів захисту від електромагнітних випромінювань. Під екрануванням розуміється розміщення елементів автоматизованої системи, що створюють електричні, магнітні й електромагнітні поля, у просторово замкнених конструкціях. Способи екранування залежать від особливостей полів, що створюються елементами системи при протіканні в них електричного струму.

Залежно від типу створюваного електромагнітного поля розрізняють наступні види екранування:

• екранування електричного поля (електростатичне);

• екранування магнітного поля (магнітостатичне);

• екранування електромагнітного поля.

Екранування дозволяє не тільки захистити обладнання автоматизованих систем від випромінювання власних небезпечних сигналів, а й зменшити ризик небажаного впливу зовнішніх електромагнітних та акустичних полів.

До групи, що забезпечує зниження потужності випромінювань і наведень, ставляться наступні методи:

• зміна електричних схем пристроїв;

• використання оптичних інтерфейсів – оптичних перетворювачів сигналів;

• зміна конструкції пристроїв;

• використання фільтрів;

• гальванічні розв'язки в системі електроживлення.

Зменшення потужності побічних випромінювань шляхом змін електричних схем передбачає використання електро- і радіоелементів з меншим випромінюванням, уникнення регулярності повторень в інформаційних сигналах, зміна форми (крутизни фронтів) сигналів, запобігання виникненню паразитної генерації.

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

**Активні методи захисту –** підвищення ен. Завад. Буває лінійне зашумлення та просторове зашумлення. Активні засоби демаскують захист, повинні відповідати кодексу законів про працю(рівень радіації та ел/ маг випромінювання)

**Зашумлення для ел/маг каналів**

Рівень сигнал/завада на границі КЗ – мінімізувати(фільтрація, екранування, заземл)

* Дотримання КЗОД
* Вимоги – достатньо енергії для зашумлення
* Знайти помеху що максимально исказит сигнал

1. Використання компліментарних сигналів 3-5% випадків
2. АБГШ – 90-95% випадків (адитивний білий гаусів шум)
3. Цветной шум менше 5%

**Шумогенераор з АБГШ – лінійне зашумлення** на сторонні провідники (необхідно нормувати шумову мощность)

* **Просторове зашумлення** – в кожній точці КЗ однаковий рівень шумів. Реалізується за допомогою ел/маг антен та штирьових (мін 4 зверху, 4 знизу)

Прикладом є **генератор шума "Гном-3",** з такими характеристиками

від 10 кГц до 150 кГц……………….не меньше 70 дБ;

від 150 кГц до 30 кГц………………не меньше 70 дБ;

від 30 МГц до 400 кГц………………не меньше 75 дБ;

від 400 МГц до 1 ГГц………………..не меньше 45 дБ

**Акустичний генератор шума ANG-2000**

Технические характеристики:

— диапазон частот………широкополосный шум 250 Гц — 5 кГц

— выходное напряжение….от 0 до 14 В

— вес………………………1,4 кг

— размеры………………..43x152x254 мм

— питание…………………от сети

**Стационарный генератор акустического шума АД-24**

**Генератор белого шума Г-002 (Россия)**

Активні методи захисту спрямовані на:

1)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;

2)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;

**4. Закриття мовних сигналів в телефонних каналах.**

Для закриття мовних сигналів використовують скрамблери

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).

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.

ST-020

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

Вартість: 40 USD

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. 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 .

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.