Завдання №8

1. Канали витоку інформації ОІД та ТЗПІ;

2. Ідеологія та приклади реалізації інформаційної атаки з використанням ВЧ нав’язування;

3. Способи захисту інформації. Зменшення рівнів небезпечних сигналів та протидія;

4. Методи та засоби захисту телефонних ліній зв’язку.

Відповіді:

2) Ідеологія та приклади реалізації інформаційної атаки з використанням ВЧ нав’язування;

Технічний канал витоку інформації шляхом ВЧ нав’язування можна забезпечити шляхом несанкціонованого контактного введення току ВЧ від генератора, підключеного до лінії (кола), що має функціональний зв’язок з нелінійним чи параметричним елементом ДТЗС, на котрих здійснюється модуляція ВЧ сигналу інформаційним. Інформаційний сигнал в даних елементах ДТЗС з’являється як слідство електроакустичного перетворення акустичних сигналів в електричні. Згідно тому, що нелінійні або параметричні елементи ДТЗС для ВЧ сигналу, як правило, являють собою неузгоджене навантаження, промодульований ВЧ сигнал буде відбиватися від неї та поширюватись в зворотному напрямку по лінії, або випромінюватись. Для прийому випромінених або відбитих ВЧ сигналів використовуються спеціальні приймачі з високою чутливістю. Вплив на технічні засоби високочастотних сигналів. В даний час використовуються два способу високочастотного нав'язування:

- За допомогою контактного введення високочастотного сигналу в електричні ланцюги, функціональні або паразитні зв'язку з технічним засобом.

- Шляхом випромінювання високочастотного електромагнітного поля. Можливість витоку інформації при використанні високочастотного нав'язування пов'язана з наявністю в ланцюгах технічних засобів нелінійних або параметричних елементів. Нав'язуванні високочастотні коливання впливають на ці елементи одночасно з низькочастотними сигналами, що виникають при роботі цих коштів і містять конфіденційну інформацію. В результаті взаємодії на таких елементах високочастотні нав'язувані коливання виявляються промодульованої низькочастотними небезпечними сигналами.

4) Методи та засоби захисту телефонних ліній зв’язку.

- Простим методом захисту телефонних ліній є метод **обмеження шкідливих сигналів**.

Метод грунтується на нелінійності вольт-амперної характеристики напівпровідників (частіше діода) при малих значеннях струмів та напруг. Зустрічно-паралельне підключення двох діодів послідовно до дзвінково-визовного пристрою телефону дозволяє створити умови, перешкоджаючі проникненню у дзвінково-визовний пристрій сигналів з малою амплітудою, або від генераторів з великим внутрішнім опором.

**- Фільтрація небезпечних сигналів** використовується для захисту телефонних апаратів від “ВЧ нав’язування”. Як правило, для захисту телефонних апаратів використовують пристрої, котрі об’єднують фільтр та обмежувач.

**- Відключення апарату від лінії** при проведенні конфіденційних переговорів є найбільш радикальним методом захисту.

3) Способи захисту інформації. Зменшення рівнів небезпечних сигналів та протидія;

- **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;

1) Канали витоку інформації ОІД та ТЗПІ;

За фізичним принципом технічні канали витоку інформації можуть бути класифіковані за групами:

- 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 та ін.).

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’юте- ра), 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.