Модульная контрольная работа

Вопросы:

Завдання №11

1. Поєднання технічних та організаційних заходів для захисту ОІД;

2. Первинні перетворювачі. Умови для утворення перетворювальних елементів;

3. Заземлення ТЗПІ;

4. Пристрої для захисту мовної інформації.

Ответы:

1. Організаційні заходи – це ті, які не потребують спеціального технічного обладнання. Технічні – відповідно які потребують і направлені на канали витоку інформації з використанням активних та пасивних засобів.

Ці типи заходів по різному впливають на вирішення проблеми витоку інформації, організаційні методи є скоріше привінтивними, тобто вони в основному націлені на використання якісної техніки, правильної структури КЗ та правильне налогодження контролю доступу. В свою чергу технічні – це спеціально встановлена апаратура, яка умовно кажучи “ закриває дірки” у вже існуючих умовах, бо не завжди можно зробити КЗ, яка без додаткових засобів буде задовольняти ТЗ (офіс не може бути, наприклад, без вікон, тому цим зонам треба приділити окрему увагу)

2. Заземлення також є каналом витоку інформації, тому треба слідкувати яка саме інформація йде до заземлення та не допускати витоку секретної інформації. Існує декілька способів заземлення: однопотокове та багатопотокове за гібридне. Однопотокове є найбільш небезпечним, вся інформація прокікає по одному дроту і в цьому випадку треба контролювати всю довжину заземлення.

Основні вимоги:

- Система має бути з загальним заземлювачем

- Кожен елемент, що заземлюється має бути підключеним до заземлювача за допомогою окремого відгалуження. Варто уникати паралельного підключення декількох заземлюючих елементів.

- Не має бути замкнених контурів

- Не треба використовувати загальний провідник для систем екрануючих заземлень,

захисних заземлень та сигнальних кіл

- Контакти мають бути захищені від корозії

- Не можна використовувати в якості заземлення нульові фази електромереж, металеві

конструкції, труби систем опалення та водопостачання.

4. Є активні та пасивні методи акустичного захисту. Пристрої – це саме активні методи.

Прикладом є віброакустичне маскування за допомогою спеціальних систем (“Заслон”, “Кабінет”, “Барон” і т.п.). Це є гучномовці. вібраційні випромінювачі або генератори шуму. Вони створюють так званий білий гаусовий шум, та перешкоджають витоку інформації. Але ці генератори працюють не на всіх частотах, а лише на заданих і про це варто не забувати. Також є пристрої для вчасного виявлення диктофонів та акустичних радіозакладних пристроїв. Ці пристрої аналізують певні параметри, та на основі них роблять висновки чи наявні шкідливі пристрої чи ні.

Деякі параметри:

- несуча частота радіоканалу;

- потужність радіопередавача;

- вид модуляції;

- ширина займаної смуги частот;

- стабільність частоти;

- режим (замкненість) роботи

Приклади таких пристроїв: “PK Electronic”, “Westinghouse AID”, “Вече”. Також використовують нелінійні локатори, які працюють з методом “опромінювання”.