

## 1. Перетворювальний елемент. Варіанти утворення небезпечних сигналів;

**Перетворювачем** є прилад, що трансформує зміну однієї фізичної величини в зміну іншої. У термінах електроніки перетворювач зазвичай визначається як прилад, що перетворює неелектричну величину в електричний сигнал або навпаки. Кожний перетворювач діє на підставі певних фізичних принципів й утворює властивий цим принципам передавальний канал — тобто канал витоку інформації. За фізичною природою перетворювачі поділяють на численні групи, серед яких слід відзначити фотоелектричні, термоелектричні, п'єзоелектричні, електромагнітні й акустоелектричні перетворювачі, які широко використовуються в сучасних системах зв'язку, обробки інформації й управління. Одними з найнебезпечніших каналів витоку інформації є акустичні канали. Джерелом утворення акустичного каналу витоку інформації є вібруючі, коливні тіла й механізми, такі як голосовий апарат людини, елементи машин, телефонні апарати, звукопідсилювальні системи тощо. Варіанти утворення небезпечних сигналів:

- Наведення електромагнітних сигналів нав'язування
- Акустичний вплив
- Позитивний зворотній зв'язок

## 2. Побічні електромагнітні випромінювання та наведення (ПЕМВН). Суть програм створення засобів, захищених від витоку інформації за рахунок ПЕМВН;

Найбільшу небезпеку з точки зору витоку інформації представляють побічні (паразитні, ненавмисні) випромінювання технічних засобів, які беруть участь в процесі передачі, обробки та зберігання секретної інформації.

Під витоком інформації з каналів ПЕМВН мається на увазі можливість доступу до інформації в ІС, здійснюваного шляхом перехоплення і відповідної обробки побічних (паразитних, ненавмисних) випромінювань технічних засобів передачі інформації, використовуваних в зазначеній системі для збору, обробки, зберігання та обміну інформацією. Канал витоку інформації включає в себе технічні засоби передачі, обробки або зберігання секретної інформації, середовище розповсюдження паразитних електромагнітних або інших випромінювань і засіб перехоплення та первинної обробки побічних (паразитних) випромінювань.

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 взаємного впливу кіл;
- під час проходження інформативних (небезпечних) сигналів у колі заземлення;
- під час паразитної модуляції високочастотного сигналу;
- внаслідок хибних комутацій і несанкціонованих дій;
- під час проходження інформативних (небезпечних) сигналів у колі електроживлення.

Для захисту від витоку інформації за рахунок ПЕМВН ОТЗ повинні розміщуватися, по можливості, ближче до центру будинку або в бік найбільшої частини контрольованої території. Складові елементи ОТЗ повинні розміщуватися в одному приміщенні або в суміжних. Якщо зазначені вимоги невиконувані, слід вжити додаткових заходів захисту:

- установити високочастотні ОТЗ в екрановане приміщення (камеру);
- установити в незахищені канали зв'язку, лінії, проводи і кабелі спеціальні фільтри та пристрої.
- прокласти проводи і кабелі в екранувальних конструкціях;
- зменшити довжину паралельного пробігу кабелів і проводів різних систем з проводами та кабелями, що несуть ІзОД;
- виконати технічні заходи щодо захисту ІзОД від витоку колами заземлення та електроживлення.

Якщо зазначені вимоги невиконувані, слід вжити додаткових заходів захисту:

- установити високочастотні ОТЗ в екрановане приміщення (камеру);
- установити в незахищені канали зв'язку, лінії, проводи і кабелі спеціальні фільтри та пристрої.
- прокласти проводи і кабелі в екранувальних конструкціях;
- зменшити довжину паралельного пробігу кабелів і проводів різних систем з проводами та кабелями, що несуть ІзОД;
- виконати технічні заходи щодо захисту ІзОД від витоку колами заземлення та електроживлення.

### **3. Пасивні та активні методи ЗІ;**

Для забезпечення захисту інформації, яка оброблюється ТЗПІ, використовуються різні методи та засоби, які можна розділити на **пасивні** та **активні**.

**Пасивні методи використовують**, коли на межі контрольованих територій необхідно:

- послабити сигнали ТЗПІ до рівня, коли засоби розвідки не зможуть виділити їх на шумовому фоні.
- послабити наведення побічних електромагнітних випромінювань ТЗПІ на з'єднувальні лінії ДТЗС та сторонні провідники до рівня, коли засоби розвідки не зможуть виділити їх на шумовому фоні. Це здійснюється шляхом екранування та заземлення ТЗПІ та їх ліній заземлення.
- послабити або повністю виключити прочосування інформаційних сигналів ТЗПІ до мереж живлення, з метою унеможливлення їх виділення засобами розвідки на шумовому фоні. Для цього використовується фільтрація інформаційних сигналів.

**Активні методи використовують**, коли на межі контрольованих територій необхідно унеможливити виділення засобами розвідки на шумовому фоні та зменшити такі показники, як відношення сигнал/завада.

Для цього створюють просторові маскуючі електромагнітні завади або створюють маскуючі електромагнітні завади у сторонніх провідниках та з'єднувальних лініях ДТЗС.

#### **4. Методи і засоби виявлення та знешкодження диктофонів.**

**Виявити наявність диктофона** можна за їхніми сигнальними демаскуючими ознаками і демаскуючими ознаками елементів конструкції диктофона й зовнішнього вигляду. За сигнальними демаскуючими ознаками диктофони виявляють із застосуванням спеціалізованих пристроїв.

**Найбільш ефективним засобом виявлення є нелінійний локатор.**

Радіозакладні пристрої можна виявляти **детекторами поля, інтерсепторами, радіочастотовимірниками, скануючими приймачами, програмно-апаратними комплексами.**

Для виявлення працюючих в режимі запису диктофонів використовують **детектори диктофонів**. Для прийому таких сигналів використовують **магнітні антени**.

Виявлення: **нелінійні локатори, детектори поля, інтерсептори, детектори диктофонів, радіочастотовимірники, скануючі приймачі, програмно-апаратні комплекси.**

**Подавлення несанкціонованого запису мови на диктофон може здійснюватися акустичним, ультразвуковим і електромагнітним методами.**

**Акустичний метод придушення** за його традиційною інтерпретацією ґрунтується на постановці просторової акустичної завади в напрямку можливого розташування записуючого пристрою.

**При застосуванні принципу електромагнітного придушення** в ДМВ діапазоні частот (бл. 900 МГц), генеруються потужні шумові сигнали. За рахунок направлених антен ці сигнали наводять в підсилювачах низької частоти та підсилювачах запису завадні сигнали. Інформаційний сигнал при цьому спотворюється.

Радіус дії подавляючих пристроїв залежить від потужності передавача та характеристики направленості антени. Звичайно зона придушення має вигляд сектора з кутом 30...80 градусів і радіусом дії 1,5 метри.

**Системи ультразвукового придушення** випромінюють потужні імпульси на частотах, котрі не сприймаються вухом людини. Такі імпульси діють безпосередньо на мембрани мікрофонів диктофонів. Крім спотворення акустичного сигналу на мембрані мікрофону, присутній також ефект перевантаження підсилювачів звукової частоти до рівнів, при котрих система автоматичного регулювання підсилення вже не працює.

Знешкодження диктофонів: **принцип електромагнітного придушення шумовими безперервними і імпульсними сигналами, акустичний метод, ультразвуковий метод.**