Дослідження проблеми захищеності джерел побічних випромінювань при представленні в них інформації у вигляді паралельного коду

УДК 621.396

Анатолій Голішевський

Державний науково-дослідний інститут спеціального зв'язку та захисту інформації, 380937029549@ukr.net

Одним з напрямків забезпечення конфіденційності державних інформаційних ресурсів на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах (ІТС) є їх захист від витоку технічними каналами, які виникають в результаті небажаних паразитних ефектів. Це побічні випромінювання полів небезпечних сигналів (ПЕМВН), якими супроводжується робота технічних засобів та систем обробки і передачі інформації та які утворюють загрозу щодо її витоку за межі об'єкту.

Метою даної роботи є підвищення ефективності протидії витоку інформації за рахунок ПЕМВН на об'єктах, що використовують ІТС, шляхом аналізу та удосконалення таких технічних умов, які б унеможливлювали реалізацію зловмисниками загроз щодо перехоплення.

Як правило, це унеможливлення зводиться до забезпечення потрібного відношення сигнал/завада в оточуючому середовищі, ланцюгах електроживлення та заземлення, відвідних електричних колах та сторонніх провідниках – місцях, де противник може здійснювати перехоплення.

Зазвичай, сучасні ІТС використовують двійкове представлення інформації у виді послідовного, або паралельного коду.

Паралельна передача цифрового сигналу даних – це така передача, при якій його одиничні елементи, об'єднані в групи, передаються одночасно по окремим каналам передачі даних або на різних несучих частотах по одному каналу. В паралельних портах для одночасної передачі інформації використовується 2^N ліній, що дозволяє побайтову передачу даних. Окрім фізичних ліній даних, до складу паралельних інтерфейсів можуть входити такі такі складові, як: лінія паритету, лінія управляючого сигналу приймача (передавача), лінія готовності приймача (передавача), нульова лінія (GND), помилка передачі (приймання).

З точки зору виявлення, цінність становлять не тільки випромінювання інформаційних байтів, а й сигнали інших ліній, які хоч і досить короткочасні, але можуть служити для ідентифікації типу інтерфейсу обробки даних, або тільки як демаскуюча ознака.

Нехай ланцюгами ІТС циркулює інформація у виді паралельного, для простоти двійкового коду. Нехай посередництвом побічних електромагнітних випромінювань та наведень утворюються технічні канали витоку. В каналі витоку діє завада, що спотворює небезпечний сигнал та може бути використана для убезпечення каналу. Потенційний противник намагається аналізувати ефір, використовуючи оптимальний приймач, та здійснювати виявлення та перехоплення інформації (Рис.1).

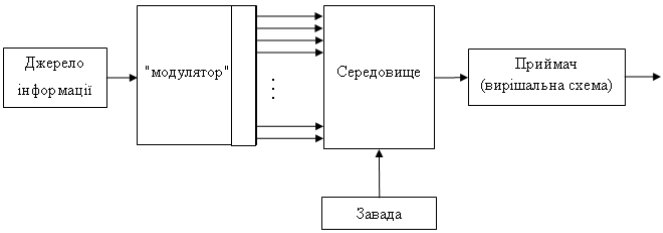

Рис.1. Дискретно-неперервний канал витоку інформації

Під енергетичним показником захищеності інформації за рахунок технічних каналів витоку в цьому випадку розуміється вірогідність виявлення інформативних ПЕМВН. Цей показник базується на теорії рішень двох альтернатив та характеризує тільки можливість виявлення ПЕМВН на фоні завад як функцію від їх енергетики.

З теоретичних основ радіолокації відомо, що вірогідність виявлення одиночного імпульсу на фоні завад розраховується наступним чином:

$$P_{виявл} = 1 - F\left(\sqrt{\frac{E_{імп}}{N_0}}\right) \quad (1)$$

де *F(x)* – інтеграл ймовірності, функція Лапласа, $E_{імп}$– енергія імпульсу, N_0 – спектральна щільність потужності завад на вході приймача.

При формуванні ПЕМВН від багаторозрядного імпульсу має місце сукупне випромінювання від кожної лінії багаторозрядної шини. В зв'язку з цим, сумарне випромінювання декількох розрядів буде формуватися як некогерентне складання випромінювання кожного з них, а вірогідність виявлення буде визначатися за допомогою наступного виразу:

$$P_{виявл} = 1 - F\left(\sqrt{\frac{kE_{імп}}{N_0}}\right) \quad (2)$$

де *k* - кількість розрядів у сигналі – джерелі ПЕМВН.

Виявлення кодової комбінації відрізняється від виявлення одиночного імпульсу збільшенням часу некогерентного накопичування імпульсів, що пропорційно їх кількості в кодовій комбінації. У цьому випадку вираз (2) прийме наступного вигляду:

$$P_{виявл} = 1 - F\left(\sqrt{\frac{\mu M k E_{імп}}{N_0}}\right) \quad (3)$$

де M – загальна кількість імпульсів в комбінації, μ - коефіцієнт, що характеризує відношення логічних одиниць, до загальної кількості імпульсів в кодовій комбінації.

Дані залежності показують зниження захищеності джерел витоку від їх виявлення противником при збільшенні розрядності сигналу, однак у випадку захисту від перехоплення змісту інформації джерел, за певних наукових розрахунків це дозволяє сформувати підхід до побудови засобів захисту, базованих на збільшенні розрядності інформаційних ліній в ІТС за рахунок використання додаткових імітуючих ліній, як альтернативі генераторів шуму.