УДК 621.3

Л.П. Крючкова, д.т.н.,
І.В. Цмоканич,
Державний університет телекомунікацій, Україна

УДОСКОНАЛЕНИЙ МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ ВИСОКОЧАСТОТНОГО НАВ'ЯЗУВАННЯ

На об'єктах інформаційної діяльності циркулює інформація, яка має певний гриф секретності або може містити дані, які певним чином можуть впливати на безпеку держави та її громадян. Через це ця інформація може піддаватися спробам перехоплення. Внаслідок дії багатьох чинників можуть самочинно утворюватися або навмисно формуватись технічні канали витоку конфіденційної інформації. Враховуючи важливість інформації, застосовуються заходи та засоби, спрямовані на забезпечення захисту акустичної інформації та інформації, оброблюваної у інформаційних системах.

Одним з ефективних методів перехоплення конфіденційної інформації є методи високочастотного нав'язування [1]. В даний час застосовуються два способи перехоплення інформації каналами високочастотного нав'язування:

- за допомогою контактного або індукційного введення високочастотного сигналу в електричні кола, які мають функціональні або паразитні зв'язки з основним технічним засобом;
- шляхом опромінення високочастотним електромагнітним сигналом джерела інформації і прийняття відбитого модульованого сигналу.

Нами пропонується застосування активних методів захисту інформації від витоку каналами високочастотного нав'язування. Сутність методу полягає в реалізації системи захисту наступним чином [2]:

1. Методом радіомоніторингу на об'єкті інформаційної діяльності виявляється частота небезпечного сигналу.

2. У випадку виявлення вищезгаданим методом небезпечного сигналу, високочастотним генератором формується сигнал, спрямований на руйнування інформативних параметрів небезпечного сигналу, що унеможливлює перехоплення інформації.

Як відомо, перехоплення інформації може здійснюватись як на основній частоті, так і на гармоніках небезпечного сигналу. Удосконаленням і новизною методу є те, що забезпечується формування захисних сигналів не тільки на основній частоті, а й на гармоніках небезпечного сигналу. Отже, явище «биття» небезпечного і захисних сигналів буде прослідковуватись і на основній частоті, і на гармоніках.

Нами проведено розрахунки та експериментально визначено оптимальні значення захисного сигналу для забезпечення явища «биття». Визначено оптимальний діапазон, а саме: $0{,}005 \leq \Delta\omega \leq 0{,}3$, де $\Delta\omega$ – різниця частот небезпечного сигналу та сигналу, який формується генератором.

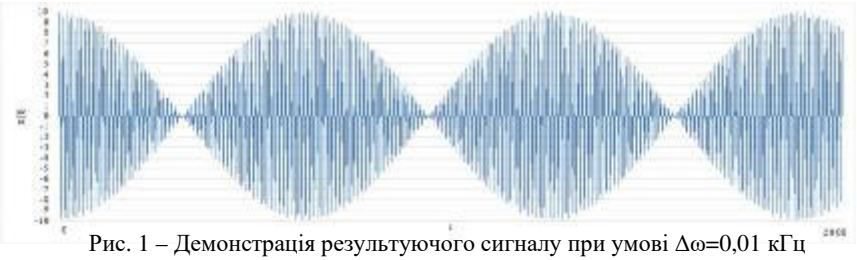

Рис. 1 – Демонстрація результуючого сигналу при умові $\Delta\omega$=0,01 кГц

Отримані спотворення небезпечного сигналу унеможливлюють відтворення перехопленої інформації, що дозволяє забезпечити захист інформації від витоку (рис.1).

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Крючкова Л.П., Провозін О.П. Перехоплення мовленнєвої інформації методами високочастотного "нав'язування" // Сучасний захист інформації – 2017. – №3(31), С.74-80.

2. Патент 95365 Україна, МПК (2011.01) H04K 3/00. Спосіб захисту інформації / Рибальський О.В., Хорошко В.О., Крючкова Л.П., Джужа О.М., Орлов Ю.Ю.; заявник і патентовласник Національна академія внутрішніх справ. - № a200913327; заявл. 22.12.2009; 55 опубл. 25.07.2011, Бюл. № 14.