УДК 621.375 **Форощук І.В.**

ЗАГРОЗА ВИТОКУ ІНФОРМАЦІЇ В УМОВАХ ВПЛИВУ НАДШИРОКОСМУГОВИХ СИГНАЛІВ

Вступ

На протязі останнього десятиліття спостерігається особливо стрімкий розвиток НШС систем і засобів зв'язку. В наукових публікаціях, матеріалах конференцій, друкованих та електронних презентаціях компаній-лідерів світу радіозв'язку постійно з'являються відомості про дослідження, які систематично ведуться в цьому напрямку, та практично створені і функціонуючі засоби НШС зв'язку.

Застосування НШС сигналів надає певні суттєві переваги, які достатньо широко висвітлені як у вітчизняних так і у зарубіжних публікаціях [1-3]. Так, наприклад, застосування їх в радіолокації дозволяє значно збільшувати роздільність, тобто виявляти малогабаритні цілі та проводити розпізнавання великих цілей. При застосуванні НШС сигналів у радіозв'язку користувач отримує можливість передавати інформацію зі швидкостями у сотні мегабіт на секунду.

Компанії Time Domain (США), Symmetrycom (США), Wisair (Ізраїль) на комерційній основі пропонують широкому загалу як окремі системи радіозв'язку, так і модульні рішення для інтеграції у сучасні мультимедійні пристрої. Для державних спеціальних служб запропонований ряд моделей переносних короткоінтервальних локаторів на основі НШС сигналів.

Все зазначене вище свідчить про близькі перспективи широкого вжитку у повсякденному житті НШС сигналів з центральними частотами від 650 МГц до 10 ГГц.

З іншого боку, з точки зору захисту інформації відмітимо, що відповідно до п. 3.8 [4] одним з технічних каналів витоку інформації є такий, що виникає за рахунок надходження високочастотних сигналів у нелінійні (або параметричні) кола, які несуть інформацію з обмеженим доступом (ІзОД), де відбувається модуляція високочастотного сигналу. Таким чином, високочастотні коливання стають носіями інформативних (небезпечних) сигналів.

Випадки виникнення зазначеного каналу витоку в умовах впливу надвисокочастотних вузькосмугових сигналів достатньо широко розглянуті в наукових та публіцистичних друкованих та електронних джерелах, наприклад [5-7]. Проте надширокосмугові надвисокочастотні сигнали мають специфічні, відмінні від вузькосмугових сигналів властивості, які не завжди вкладаються в рамки класичної теорії зв'язку. Специфічними є також процеси взаємодії випадкових антен з НШС сигналами та їх властивості щодо просторового розповсюдження.

Таким чином, на меті поставлено провести класифікацію та порівняльний аналіз відомих НШС сигналів, їх основних характеристик, а також розглянути загрози формування технічних каналів витоку інформації в умовах їх навмисного або ненавмисного надходження у нелінійні (або параметричні) кола, які несуть інформацію з обмеженим доступом.

Визначення надширокосмугових сигналів

Існує цілий ряд визначень НШС сигналів, які фігурують в науковій та технічній літературі. Використовуючи наступне співвідношення

$$\eta = \frac{\Delta f}{f_0}, \qquad (1)$$

де где Δf – смуга частот сигналу, яка визначається як $f_B - f_H$, f_B – верхня частота спектру, f_H – нижня частота спектру, f_0 – центральна частота спектру, надширокосмуговість визначають за відносною смугою частот η. При цьому, якщо $\eta \geq 0{,}25$, то такий сигнал вважають надширокосмуговим.

У 1990 р. агентство DARPA (США) запропонувало інше визначення відносної смуги частот

$$\eta = \frac{f_B - f_H}{f_B + f_H}, \tag{2}$$

при цьому пропонується вважати, що сигнали, у яких:

$\eta \le 0{,}01$ – вузькосмугові;

$0{,}01 \le \eta \le 0{,}25$ – широкосмугові;

$0{,}25 \le \eta \le 1$ – надширокосмугові.

У 2002 р. Федеральною комісією зв'язку (США) було запропоноване нове визначення. І хоча воно стосується лише НШС системи (передавача), а не НШС сигналу як такого, проте воно фактично усуває недоліки вище зазначених визначень, оскільки НШС сигнал не може існувати окремо від НШС передавача. За даним визначенням надширокосмуговим передавачем є випромінювач, який має відносну смугу частот випромінювання більшу за 0,2 або абсолютну смугу частот, яка вимірюється на рівні -10 дБ відносно максимуму випромінювання, більш ніж 500 МГц незалежно від відносної смуги частот. Відносна смуга частот при цьому визначається за наступною формулою

$$\eta = 2 \cdot \frac{f_B - f_H}{f_B + f_H}, \tag{3}$$

де f_B і f_H верхня і нижня частоти спектру відповідно, які визначаються на рівні -10 дБ відносно максимуму випромінювання.

Класифікація та порівняльний аналіз основних типів відомих НШС сигналів

До сигналів, які можуть бути використані в НШС системах відносяться:

- гаусові імпульси;
- радіоімпульси;
- імпульси Ерміта;
- хаотичні сигнали;
- лінійно частотно модульовані сигнали;
- багаточастотні сигнали.

У даний час широкого вжитку зазнали перші два типи сигналів. Розглянемо ці та інші сигнали, а також дамо попередню оцінку їх характеристик з точки зору займаної смуги частот та форм спектрів.

Гаусові імпульси - це набір ортогональних імпульсів, які описуються гаусовою функцією та її похідними вищих порядків. Причому порядок похідної визначає форму імпульсу, тобто з метою отримання гаусового імпульсу потрібної форми необхідно продиференціювати гаусову функцію

$$S_{G0}(t) = A \cdot e^{-\frac{t^2}{2 \cdot a^2}}, \tag{4}$$

де A – амплітуда імпульсу, a – величина, яка характеризує половину довжини імпульсу на рівні 0,607, відповідну кількість разів. Або скористатися виразом

$$S_{Gn}(t) = B \cdot G_n(t) \cdot e^{-\frac{t^2}{2}}, \tag{5}$$

де $G_n(t)$ – n-й поліном гаусової функції ($n = 0, 1, 2, \ldots$)

$$G_n(t) = (-1)^n \cdot e^{\frac{t^2}{2}} \cdot \frac{d^n}{dt^n} e^{-\frac{t^2}{2}};$$

B – нормувальний коефіцієнт, який включає в себе постійні величини.

Частотний спектр потужності гаусової функції визначається виразом

$$S_{RF}(f) = \left| \left(A \cdot a \cdot \sqrt{2 \cdot \pi} \cdot e^{-\frac{a^2 \cdot (2 \cdot \pi \cdot f)^2}{2}} \right)^2 \right|. \quad (6)$$

Частотний спектр потужності для функцій типу (5) знаходять через пряме перетворення Фур'є

$$S_{Gn}(f) = \left| \left(\int_{-\infty}^{\infty} S_{Gn}(t) \cdot e^{-i \cdot 2 \cdot \pi \cdot f \cdot t} dt \right)^2 \right|.$$

НШС радіоімпульси - це імпульси з заповненням гармонічним коливанням. Як правило, вони мають огинаючу форми гаусової функції і містять декілька періодів радіочастотного коливання. Нижче приведені формули, які описують радіоімпульс у часовій та огинаючу спектра потужності в частотній областях:

$$S_{RF}(t) = A \cdot \sin(2 \cdot \pi \cdot f_0 \cdot t) \cdot e^{-\frac{t^2}{2 \cdot a^2}},$$

$$S_{RF}(f) = \left| \left(A \cdot a \cdot \sqrt{2 \cdot \pi} \cdot e^{-\frac{a^2 \cdot [2 \cdot \pi \cdot (f - f_0)]^2}{2}} \right)^2 \right|,$$

де f_0 – частота заповнення радіоімпульсу.

Імпульси Ерміта отримали свою назву від поліному, за яким вони розраховуються. Отримати імпульси Ерміта можливо з наступних виразів:

$$S_{Hn}(t) = B \cdot H_n(t) \cdot e^{-\frac{t^2}{2}}, \quad (7)$$

де $H_n(t)$ – n-й поліном Ерміта ($n = 0, 1, 2, ...$),

B – нормувальний коефіцієнт, який включає в себе постійні величини;

$$H_n(t) = (-1)^n \cdot e^{t^2} \cdot \frac{d^n}{dt^n} e^{-t^2}. \quad (8)$$

Відповідний частотний спектр потужності визначається наступним виразом

$$S_{Hn}(f) = \left| \left(\int_{-\infty}^{\infty} S_{Hn}(t) \cdot e^{-i \cdot 2 \cdot \pi \cdot f \cdot t} dt \right)^2 \right|.$$

Існує також сімейство модифікованих імпульсів Ерміта, основною перевагою яких є зменшення значення постійної складової у спектрі, яка не випромінюється антенною системою. Для їх формального описання через вираз (7) замість поліному (8) застосовують модифікований поліном

$$H_n(t) = (-1)^n \cdot e^{\frac{t^2}{4}} \cdot \frac{d^n}{dt^n} e^{-\frac{t^2}{2}}.$$

Також як НШС сигнали окремо класифікуються хаотичні, лінійно частотно модульовані і багаточастотні сигнали, практичне застосування яких на даний час суттєво обмежене складністю їх генерації і належної реєстрації.

Аналіз можливості утворення технічних каналів витоку інформації в умовах впливу надвисокочастотних сигналів. Як зазначено вище, відповідно до п. 3.8 [4] одним з технічних каналів витоку інформації є такий, що виникає за рахунок надходження

високочастотних сигналів у нелінійні (або параметричні) кола, які несуть інформацію з обмеженим доступом (ІзОД), де відбувається модуляція високочастотного сигналу. Таким чином, високочастотні коливання стають носіями інформативних (небезпечних) сигналів.

Припустимо, що певні складові частини деякого основного технічного засобу утворили випадкову антену з коефіцієнтом спрямованої дії D_{BA}, яка здатна перетворювати електромагнітний сигнал високочастотного впливу в електричний U, і *гальванічно зв'язана* з трактом основного технічного засобу (ОТЗ – технічного засобу, який передає, обробляє, зберігає, відображає, тощо ІзОД), параметри якого змінюються під впливом інформативних (небезпечних) сигналів (рис. 1).

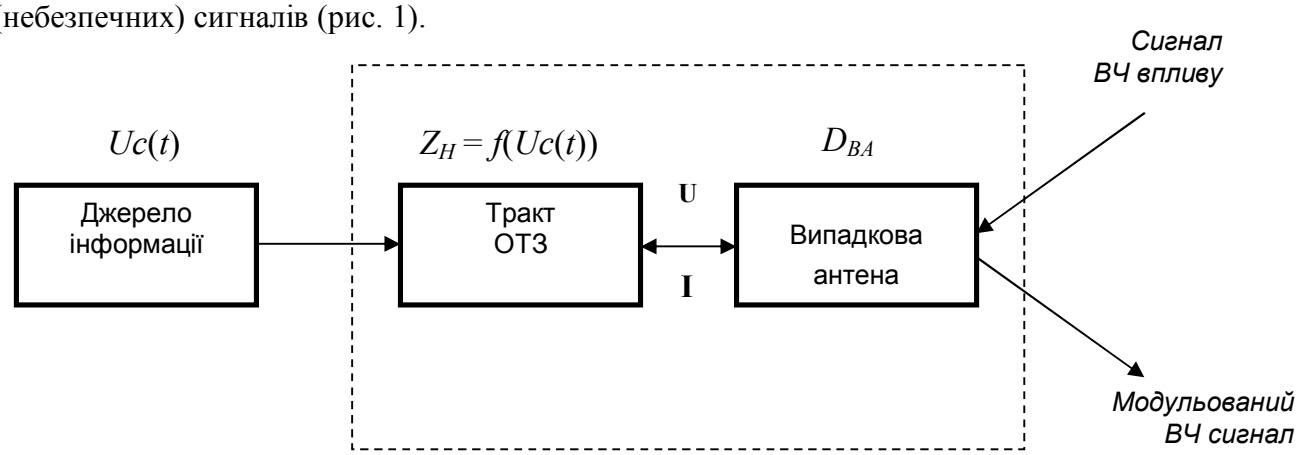

Рис. 1. Здійснення високочастотного впливу на тракт ОТЗ

По відношенню до випадкової антени тракт ОТЗ розглядатимемо у якості двополюсника, який виступає її навантаженням з комплексним опором Z_H. Напругу U, утворену випадковою антеною внаслідок наявності електромагнітного високочастотного сигналу, розглядатимемо як сигнал впливу на двополюсник, а утворений при цьому струм I – як реакцію на вплив. Припускається, що Z_H являється функцією деякого інформативного (небезпечного) сигналу $Uc(t)$, тобто $Z_H = f(Uc(t))$.

При перехопленні утвореного таким чином модульованого високочастотного сигналу основні складності, які заважають здійснювати порушнику його наміри, полягають у наявності шуму і власного потужного високочастотного сигналу впливу, складністю пошуку та (або) навмисного утворення і впровадження випадкових антен з потрібними характеристиками, складністю пошуку ОТЗ з необхідними характеристиками.

Всі перераховані фактори на даному етапі суттєво обмежили загрозу зі сторони застосування високочастотного впливу вузькосмуговими сигналами для утворення технічних каналів витоку інформації.

Проте, з огляду на властивості НШС сигналів, відмітимо:

1) при визначенні максимально припустимих відношень сигнал-шум на границі контрольованої території для НШС сигналів модель ідеального приймача відмінна від класичної і має власні потенційні характеристики;

2) спектр НШС сигналів суттєво ширший по відношенню до вузькосмугових сигналів впливу, що в свою чергу збільшує ймовірність збігу частотних характеристик випадкових антен ОТЗ з частотними характеристиками НШС сигналу впливу;

3) коротка тривалість імпульсів НШС сигналу дозволяє здійснювати перехоплення високочастотного сигналу в інтервалах між ними, тобто вимоги до динамічного діапазону приймача порушника можна суттєво знизити.

4) НШС сигнали по відношенню до вузькосмугових значно краще розповсюджуються в міських умовах.

Тобто застосування НШС сигналів з метою забезпечення високочастотного впливу гіпотетично може мати суттєві переваги перед застосуванням вузькосмугових сигналів і становити загрозу конфіденційності ІзОД.

Висновки

Останнім часом суттєвого розвитку набули системи зв'язку і радіолокації на основі НШС сигналів, що зумовило їх значне розповсюдження у повсякденній діяльності. Властивості НШС сигналів суттєво відрізняються від властивостей, притаманних вузькосмуговим сигналам і не завжди пояснюються класичною теорією зв'язку.

З огляду на зазначене вище пропонується і планується провести достатньо глибокі науково обґрунтовані теоретичні і експериментальні дослідження щодо загрози формування технічного каналу витоку інформації в умовах високочастотного впливу НШС сигналами на тракти основних технічних засобів.

Список літератури

1. Имнореев И.Я. Сверхширокополосные радары: новые возможности, необычные проблемы, системные особенности // Вестник МГТУ, №4, 1998, - С. 25-56.

2. Скосырев В.Н., Особенности и свойства сверхкороткоимпульсной локации. Конспекты лекций. – ССРС, Россия, Муром, Июль 2003, - С. 67-91.

3. Fontana R.J., Recent System Applications of Short-Pulse Ultra-Wideband (UWB) Technology // IEEE Transactions on microwave theory and techniques, vol. 52, № 9, September 2004.

4. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок : затверджено наказом Державної служби України з питань технічного захисту інформації від 09 червня 1995 р. № 25.

5. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия РФ, 1998. 320 с.

6. Каторин Ю.Ф. Антишпионские штучки. Энциклопедия промышленного шпионажа / Каторин Ю.Ф. – СПб. : Полигон, – 1999. – 564 с.

7. Ярочкин В.И. Предпринимательство и безопасность. Ч. 1. Несанкционированный доступ к источнику конфиденциальной информации / Ярочкин В.И. – М. : Экспрессное бюро, – 1994. – 64 с.

Надійшла 3.11.09

УДК 003.26:004.056.55:621.39 **Корченко О.Г., Васіліу Є.В., Гнатюк С.О.**

СУЧАСНІ КВАНТОВІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

На сьогодні першочерговим чинником, що впливає на складові національної безпеки, є ступінь захищеності інформаційного середовища. Питання інформаційної безпеки набуває актуальності як у процесі стрімкого розвитку комп'ютерних технологій, так і у контексті різкого збільшення злочинів та інших протиправних дій, спрямованих на порушення конфіденційності, цілісності та достовірності інформації. Основна роль у забезпеченні інформаційної безпеки в інформаційно-телекомунікаційних системах відводиться криптографії, одними із базових задач якої є: розподіл ключів шифрування, аутентифікація сторін, авторизація легітимних користувачів [1]. Розподіл ключів шифрування (криптографічних ключів) між законними користувачами в умовах суворої секретності є однією з найважливіших проблем криптографії, яка може бути вирішена за допомогою [2]:

- класичної криптографічної схеми з теоретико-інформаційної стійкістю (для її реалізації необхідний канал з перешкодами; ефективність схеми вкрай низька – 1-5%);