

**Література**

1. Патент на винахід № 83505 Україна. Приймально-передавальна антена з керованою поляризацією / Ільницький Л.Я., Осама Турабі. – Опубл. 25.10.2007, Бюл. № 17.
2. Ільницький Л.Я. Антени та пристрої надвисоких частот: Підручник для ВНЗ / Л.Я. Ільницький, О.Я. Савченко, Л.В. Сібрук; За ред. Л.Я. Ільницького. – К.: Укртелеком, 2003. – 496 с.

Рецензент: Ерохин В.Ф.  
Поступила 02.12.2011

УДК 621.396.933

Голубничий О.Г., Антонов В.В.  
Національний авіаційний університет

**АНАЛІЗ КОНФІДЕНЦІЙНОСТІ ПЕРЕДАВАННЯ ДАНИХ У  
ШИРОКОСМУГОВИХ КАНАЛАХ АвіАЦІЙНОЇ руХОМОЇ супуТНИКОВОЇ  
СЛУЖБИ AMSS**

**Постановка проблеми.** Застосування супутникових технологій у глобальній інфраструктурі повітряної навігації дозволяє суттєво підвищити рівень безпеки польотів цивільної авіації. Важливе місце серед таких технологій належить авіаційній рухомій супутниковій службі AMSS (Aeronautical Mobile Satellite Service), з використанням якої може здійснюватись організація повітряного руху (ОПР), авіаційний оперативний контроль, авіаційний адміністративний зв'язок, авіаційний зв'язок для пасажирів [1, с. 336]. Використання AMSS в Україні відповідно до нормативних документів забезпечує взаємодію органів ОПР на території України та за її межами та електрозв'язок органів ОПР з екіпажами повітряних суден у тих випадках, коли традиційні засоби авіаційного електрозв'язку не забезпечують необхідної оперативності обміну інформацією або коли виникають інші ускладнення (передавання інформації на великі відстані, над водними просторами і т.ін.) [2, пп. 2.2.5, 6.3]. Враховуючи важливість для здійснення безпеки польотів інформації, яка передається за допомогою AMSS, постає проблема забезпечення конфіденційності передавання повідомлень у системах, що працюють за цією супутниковою технологією. До складу таких систем зокрема належать широкосмугові канали “вгору” (uplink) та “вниз” (downlink) між фіксованими земними станціями (Fixed Earth Station) та супутниками низькоорбітальної супутникової системи GLOBALSTAR (GLOBALSTAR 2.0) [3].

**Аналіз останніх досліджень і публікацій.** Нормативними документами FCC [4, 5] визначено використання таких параметрів широкосмугових каналів AMSS між наземною станцією (Fixed Earth Station) та супутниками GLOBALSTAR (GLOBALSTAR 2.0): класи випромінювання 1M23G2W або 2M46G2W, використовується розширення спектру за технологією DSSS (функції Уолша  $N = 64$ ), кодове розділення каналів (CDMA), частотний діапазон для лінії зв'язку “вниз” (downlink) 6875 – 7055 МГц, для лінії зв'язку “вгору” (uplink) – 5096 – 5250 МГц (для обох типів ліній передавання використовується С-діапазон).

**Постановка завдання.** Метою статті є аналізування конфіденційності передавання даних у широкосмугових каналах, структура сигнально-кодових конструкцій в яких є типовою для широкосмугових каналів зв'язку авіаційної рухомої супутникової служби AMSS між наземною станцією (Fixed Earth Station) та супутниками GLOBALSTAR (GLOBALSTAR 2.0).

**Виклад основного матеріалу дослідження.** Проаналізуємо конфіденційність передавання даних у супутниковій лінії зв'язку AMSS з класом випромінювання 1M23G2W за таких умов.

1) Несанкціонований користувач використовує стандартну немодифіковану приймальну апаратуру санкціонованого користувача; відсутні експлуатаційні відмови, або їх вплив несуттєвий.

2) Механізм захисту передбачає динамічне перерозподілення функцій Уолша між каналами зв'язку (для розширення спектру цифрового інформаційного сигналу при швидкості передавання даних  $1,2288 \cdot 10^6 / 64 = 19,2 \cdot 10^3$  біт/с у кожний момент часу використовується одна з функцій Уолша, номер якої у базисі визначається за алгоритмом динамічного перерозподілення, – генератором псевдовипадкових чисел, наприклад) та динамічне перерозподілення несних (несні змінюються у кожний момент часу використовується одна з несних, значення якої визначається за алгоритмом динамічного перерозподілення несних); для лінії зв'язку “вниз” кількість несних  $D_d = 144$ , а для лінії зв'язку “вгору” –  $D_u = 123$  при кроці сітки частот 1,25 МГц.

3) Несанкціонованому користувачу у кожен момент часу невідоме розподілення функцій Уолша між каналами зв'язку та значення несної.

Введемо показник конфіденційності передавання даних – імовірність правильного прийому  $p1_{sr}$  одного біта конфіденційного повідомлення. Показник  $p1_{sr}$  має зміст показника структурної прихованості  $p_{sr}$  радіосистеми. Зі зменшенням  $p1_{sr}$  конфіденційність передавання даних збільшується.

Значення  $p1_{sr}$  може бути оцінене таким чином:

$$p1_{sr} = \frac{1}{2} \left( 1 - \frac{1}{V \cdot D} \right) + (1 - p_0) \frac{1}{V \cdot D}, \quad (1)$$

де  $V$  – кількість різних кодів, які використовуються для розширення спектру ( $V = 64$  для випадку функцій Уолша в CDMA);

$D$  – кількість несних у частотному діапазоні роботи системи;

$p_0$  – імовірність бітової помилки при передаванні конфіденційних повідомлень.

Формула (1) була отримана з наступних міркувань: умовна імовірність того, що при передаванні деякого біту конфіденційного повідомлення у налаштуваннях приймального пристрою для обраного каналу співпадуть значення несної та функція Уолша дорівнює  $\frac{1}{V \cdot D}$ , – тоді приймальний пристрій, що використовується несанкціонованим користувачем виконуватиме обробку сигналів так само, як і у випадку санкціонованого користувача; при цьому імовірність правильного прийому одного біта становитиме  $(1 - p_0)$ ; умовна імовірність того, що при передаванні деякого біту конфіденційного повідомлення співпадіння поточних значень несної та функції Уолша не виникне дорівнює  $\left( 1 - \frac{1}{V \cdot D} \right)$ , при цьому імовірність правильного прийому одного біта становитиме  $1/2$  (через стохастичність результату кореляційної обробки у приймальному пристрої для випадку некорельованих сигналів та детерміновану схему прийняття рішень про прийнятий бінарний символ за результатами цієї обробки).

За умов використання у широкосмуговому радіоканалі AMSS для передавання конфіденційної інформації протилежних сигналів (модуляція BPSK), приймального пристрою побудованого за схемою оптимального кореляційного приймача бінарних

сигналів з когерентним детектуванням високочастотного сигналу та ідеальної синхронізації значення  $p_0$  може бути оцінено на основі формули для потенційної завадостійкості протилежних сигналів [6, с. 84, формула (5.35)] з урахуванням вирашу при обробці ширококутового сигналу таким чином:

$$p_0 = 1 - \Phi\left(\sqrt{2 \cdot N \cdot h^2}\right) = 1 - \Phi\left(\sqrt{2 \cdot N \cdot D \cdot h_{шсс}^2}\right), \quad (2)$$

де  $N$  – довжина коду, що використовується для розширення спектру інформаційного сигналу;

$h^2$  – співвідношення сигнал/завади за потужністю у смузі частот шумового (прямокутного) еквіваленту ширококутового сигналу при апріорній визначеності значення несної;

$h_{шсс}^2$  – співвідношення сигнал/завади у смузі частот шумового (прямокутного) еквіваленту ширококутового сигналу при апріорній невизначеності значення несної (з урахуванням стрибків частоти);

$$\Phi(x) = \left(\sqrt{2\pi}\right)^{-1} \int_{-\infty}^x \exp\left(-\frac{t^2}{2}\right) dt - \text{інтеграл імовірності};$$

З урахуванням (1) та (2) конфіденційність передавання даних може бути оцінена виразами:

$$p1_{str} = \frac{1}{2} \left(1 - \frac{1}{V \cdot D}\right) + \frac{1}{V \cdot D} \Phi\left(\sqrt{2 \cdot N \cdot h^2}\right) = \frac{1}{2} \left(1 - \frac{1}{V \cdot D}\right) + \frac{1}{V \cdot D} \Phi\left(\sqrt{2 \cdot N \cdot D \cdot h_{шсс}^2}\right). \quad (3)$$

Формула (3) дає оцінку значення  $p1_{str}$  “зверху” (найбільш песимістична оцінка), оскільки отримана з позицій аналізу потенційної завадостійкості ширококутового каналу зв’язку.

При відсутності завад ( $h_{шсс}^2 \rightarrow \infty$ ) показник конфіденційності передавання даних прямує до значення

$$\lim_{h_{шсс}^2 \rightarrow \infty} p1_{str} = \frac{1}{2} \left(1 - \frac{1}{V \cdot D}\right) + \frac{1}{V \cdot D}. \quad (4)$$

На рис. 1 наведені залежності  $p1_{str}(h_{шсс}^2)$  для зазначених супутникових ліній передавання “вниз” та “вгору” для випадків використання функцій Уолша ( $N = 64, V = 64$ ) та іншої гіпотетично існуючої ортогональної системи сигналів з  $N = 80$  та  $V = 80$  (при цьому швидкість передавання в лінії AMSS зменшиться з 19,2 кбіт/с до  $1,2288 \cdot 10^6 / 80 = 15,36$  кбіт/с, тобто на 20 %).

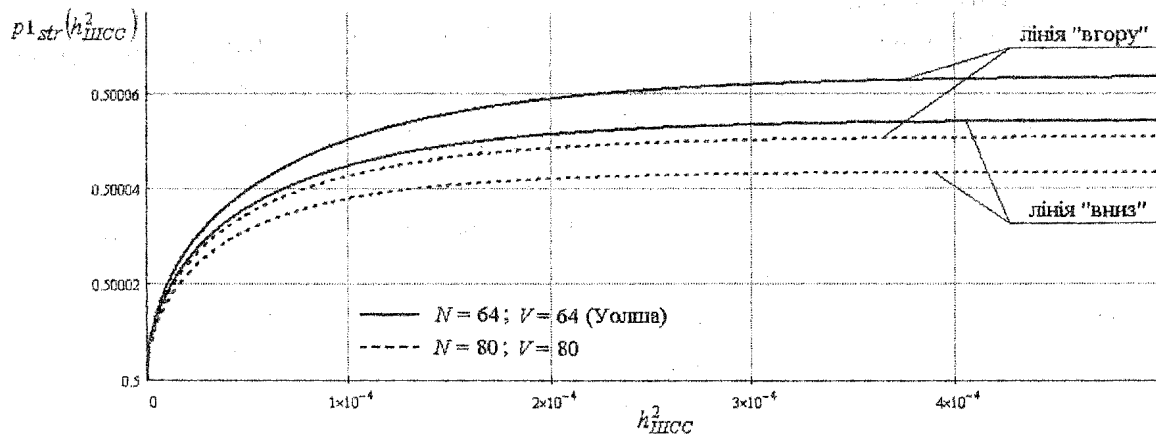


Рис. 1. Залежності показника конфіденційності передавання даних в AMSS

Залежності  $p1_{str}(h^2_{шсс})$  свідчать про підвищення конфіденційності передавання даних при зменшенні співвідношення сигнал-завади та при збільшенні об'єму ансамблю ортогональних сигналів і довжини кодової комбінації, яка використовується для розширення спектру інформаційного сигналу.

Доцільно оцінити вигравш ефективності використання різних ортогональних базисів для забезпечення конфіденційності передавання даних у розглянутих лініях AMSS для різної кількості можливих несних у системі:

$$\alpha = \frac{p1_{str}(N, V = 64)}{p1_{str}(N, V = 80)} = \frac{\frac{1}{2} \left(1 - \frac{1}{64D}\right) + \frac{1}{64D} \Phi(\sqrt{128h^2})}{\frac{1}{2} \left(1 - \frac{1}{80D}\right) + \frac{1}{80D} \Phi(\sqrt{160h^2})} \quad (5)$$

Залежності  $\alpha(D)$  для різних значень  $h^2_{шсс}$  наведені на рис. 2. Вони показують, що ефективність використання ортогональних базисів більшого об'єму та з більшою довжиною кодової комбінації, яка використовується для розширення спектру, зростає при збільшенні кількості можливих несних у системі, а також при зменшенні співвідношення сигнал-завади.

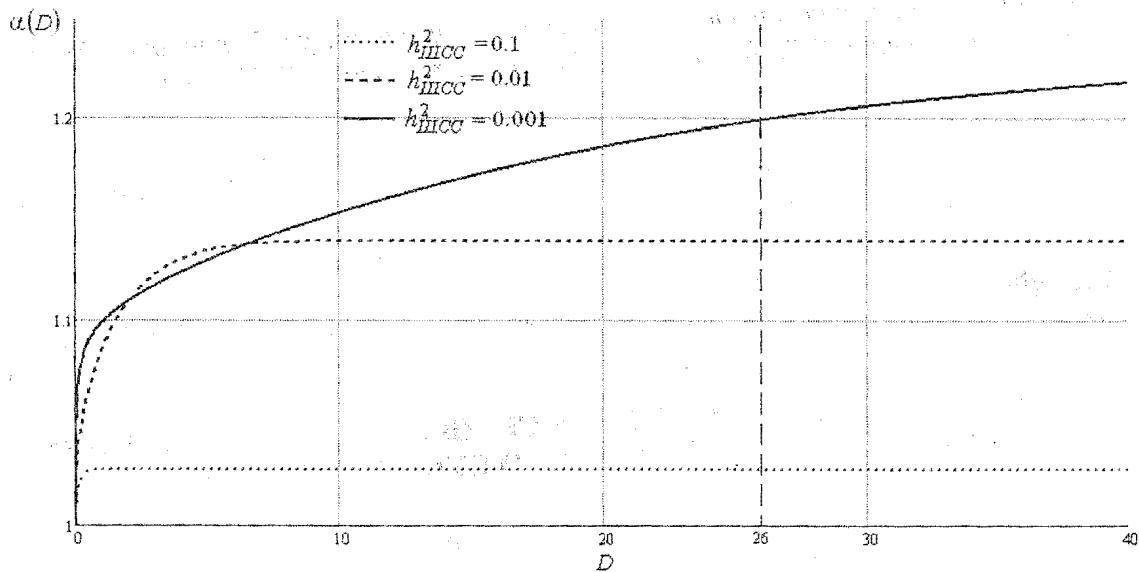


Рис. 2. Залежності виграшу ефективності  $\alpha$  від кількості несних та відношення сигнал-шум

**Висновки та перспективи подальших досліджень.** У статті проаналізовано конфіденційність передавання даних у широкосмугових супутникових лініях зв'язку AMSS між фіксованими наземними станціями та супутниками. Показано, що збільшення довжини кодової комбінації, яка використовується для розширення спектру інформаційного сигналу та об'єму ансамблю призводить до зменшення швидкості передавання інформації, але підвищує рівень конфіденційності передавання даних у системі. Порівнюючи показники розглянутих ліній передавання, встановлено, наприклад, що при зміні базису функцій Уолша ( $N=64$ ,  $V=64$ ) на гіпотетично існуючий ортогональний базис  $N=80$ ,  $V=80$  в системі AMSS відбудеться зменшення швидкості передавання на 20 % (з 19,2 кбіт/с до 15,36 кбіт/с), що компенсуватиметься підвищенням конфіденційності передавання повідомлень теж на 20 % при кількості можливих несних у системі  $D=26$  та за умови  $h^2_{SSC} = 0,001$ . Перспективним напрямом досліджень, який підвищує рівень конфіденційності та гнучкість конфігурації системи є синтез ортогональних систем сигналів необхідної довжини та об'єму.

#### Література

1. Андрусяк А.І. Мережа авіаційного електрозв'язку / Андрусяк А.І., Дем'янчук В.В., Юр'єв Ю.М. – К.: НАУ, 2001. – 448 с.
2. Правила авіаційного електрозв'язку в цивільній авіації України: зі змінами, за станом на 19 липня 2009 р. / Наказ Міністерства транспорту України від 23.09.2003 р., № 736. – Офіц. вид.
3. Globalstar Licensee LLC and GUSA Licensee LLC. DA 11-520, March 18, 2011. FCC [Електронний ресурс] – Режим доступу [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DA-11-520A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-520A1.pdf)
4. Satellite Communications Services Information. Report No. SES-01370, Aug. 03, 2011. Public Notice FCC [Електронний ресурс] – Режим доступу [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-308870A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-308870A1.pdf)
5. Satellite Communications Services Information. Report No. SES-01354, June 08, 2011. Public Notice FCC [Електронний ресурс] – Режим доступу [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-307303A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-307303A1.pdf)

6. *Радиотехнические системы передачи информации: учеб. пособие [для вузов] / [Борисов В.А., Калмыков В.В., Ковальчук Я.М. и др.]; под ред. В.В. Калмыкова. – М.: Радио и связь, 1990. – 304 с.: ил.*

Рецензент: Толюпа С.В.  
Надійшла 14.12.2011

УДК 621.396.1

Толюпа С.В., Дружинін В.А., Гордієвський О.Т.  
ГУІКТ

### РОЗПІЗНАВАННЯ ГРУПОВИХ ОБ'ЄКТІВ У БАГАТОПОЗИЦІЙНИХ СИСТЕМАХ ОПЕРАТИВНОГО СУПРОВОДЖЕННЯ

Рознесення в просторі й синхронізація функціонування структурних елементів багатопозиційних систем оперативного супроводження (БПСОС) дозволяє знаходити додаткові можливості щодо покращення характеристик визначення ознак групового складу повітряних об'єктів. Відомо [1], що важливим напрямком вирішення даної задачі є зменшення імпульсного об'єму зондувальних сигналів радіолокаційних станцій (РЛС), для чого необхідна реалізація механізмів їх стиску за тривалістю в приймальних пристроях системи, а також зменшення ширини діаграми спрямованості антени (ДСА) в кутомісцевій та азимутальній площинах. Якщо здатність РЛС щодо розрішення за дальністю визначається на етапі проектування кожного конкретного радіолокаційного засобу, то розрішення цілі за кутовими координатами, яка залежить від ширини ДСА однопозиційного засобу, може бути покращена також і в процесі експлуатації за допомогою об'єднання окремих РЛС у систему й оптимальною організацією їх спільного функціонування. При оперативному супроводженні повітряних об'єктів, для зручності опису їх відбиваючих здатностей, в умовах багатопозиційного спостереження, доцільне введення поняття багатопозиційної ефективної площі відбиття (БП ЕПВ). Якщо сигнали, випромнені різними передавальними позиціями, приходять на вхід прийомної позиції із запізнюванням відносно один одного більш ніж на величину  $\frac{1}{\Delta f}$ , де  $\Delta f$  - ширина спектра сигналу, БП ЕПВ являє собою матрицю розмірності  $n \times m$ .

$$\sigma_{m(i)} = \begin{pmatrix} \sigma(\vartheta_{1,1}) & \sigma(\vartheta_{1,2}) & \dots & \sigma(\vartheta_{1,m}) \\ \sigma(\vartheta_{2,1}) & \sigma(\vartheta_{2,2}) & \dots & \sigma(\vartheta_{2,m}) \\ \dots & \dots & \dots & \dots \\ \sigma(\vartheta_{n,1}) & \sigma(\vartheta_{n,2}) & \dots & \sigma(\vartheta_{n,m}) \end{pmatrix} \quad (1)$$

Елементами матриці (1) є моностатичні, бістатичні й тіньові ефективні площі відбиття (МЕПВ, БЕПВ, ТЕПВ). Вони відповідають випадку коли станції прийому та передачі розташовані відповідним чином: МЕПВ – станції прийому та передачі просторово сполучені; БЕПВ - станції прийому та передачі просторово рознесені; ТЕПВ - станції прийому та передачі просторово рознесені так, що кут між напрямками візування на об'єкт із обох станцій близький до 180 градусів. Рядки матриці описують відбивні властивості повітряної цілі відносно  $m$  приймальних позицій при випромінюванні  $i$  - передавальної позиції  $i = 1, n$ , а стовпці відносно  $j$  - приймальної позиції  $j = 1, m$  при випромінюванні  $n$  передавальних.

Таке математичне трактування МП ЕПВ має на увазі наступний її фізичний зміст: МП ЕПВ - це сукупність  $n \times m$  ізотропних, (принаймні, у межах апертури прийомних антен)