

УДК 621.391

**Л.Л. Бортнік**, ад'юнкт Військового інституту телекомунікацій та інформатизації  
Національний технічний університет України „КПІ”, м. Київ, Україна

## МЕТОД ОБРОБКИ ШИРОКОСМУГОВИХ СИГНАЛІВ ПІД ЧАС ВПЛИВУ НЕГАУСІВСЬКИХ ЗАВАД

*У роботі запропонований метод демодуляції широкосмугових сигналів у системах радіозв'язку з кодовим розділенням сигналів, які функціонують в умовах негаусівських завад. Метод забезпечує підвищення завадостійкості мобільних CDMA-систем у негаусівських каналах.*

**Вступ.** У сучасних системах радіозв'язку широке застосування знаходить метод багатостанційного доступу з кодовим розділенням сигналів (CDMA – Code-Division Multiple Access). У таких системах передача інформації різними абонентами здійснюється сигналами, які перекриваються за спектром і в часі, але розрізняються за формою [1-5].

Ефективність систем радіозв'язку CDMA обмежена рядом факторів, основними з яких є вплив природних та навмисних завад, нестійкість і різноманіття ймовірнісних розподілів завадового комплексу, нестационарність каналу, випадкові флуктуації комплексних множників каналу, завмирання радіосигналів тощо.

Реальна ефективність CDMA-систем з негаусівськими каналами багато в чому визначається досяжними характеристиками завадостійкості, системної ємності та обчислювальної складності алгоритмів і пристроїв спільної обробки сигналів у складному завадовому комплексі, характерному для сучасних CDMA-систем.

**Аналіз досліджень і публікацій.** Дефіцит частотного, енергетичного та просторового ресурсу радіоканалів, а також особливості завадового комплексу CDMA-систем вимагають використання адекватних моделей імовірнісного опису реальних негаусівських завад, що забезпечують розробку і впровадження нових алгоритмічних та технічних рішень, спрямованих на підвищення ефективності CDMA-систем в інтересах надійної передачі інтегрального пакетного трафіку в складних і мінливих умовах інформаційної взаємодії користувачів.

Відомі методи підвищення ефективності функціонування CDMA-систем [2; 6-10] одержані для випадку передачі інформації по гаусівському каналу без пам'яті. Наявність у каналі селективних завмирань і навмисних завад не дозволяє при прийнятній складності реалізації відомих алгоритмів передачі дискретних повідомлень досягти тієї ж ефективності використання реальних каналів зв'язку, що й ідеального гаусівського півнеперервного каналу.

**Формулювання цілей статті.** Метою роботи є розробка методу обробки сигналів у системі CDMA, який дозволить підвищити завадостійкість і ємність системи під час впливу негаусівських завад.

**Виклад основного матеріалу статті.** У загальному випадку, у рамках багатопроменевої моделі каналу CDMA-системи, прийнятий на вході базової станції груповий сигнал має вигляд [2]:

$$Z(t) = \sum_{n=1}^N \sum_{l=1}^L \sum_{i=1}^I \dot{\mu}_{nl}(t) \dot{a}_{nl} c_{nl}^{(i)} \dot{A}_{nl}(t - i\tau_c - \tau_{nl}) + B_3(t) + B_0(t), \quad (1)$$

де  $N$  – кількість активних абонентів;  $L$  – кількість променів сигналу в багатопроменевому каналі зв'язку;  $\dot{\mu}_{nl}(t)$  – комплексний каналний коефіцієнт, що відображує процеси завмирання сигналу на  $l$ -й траєкторії;  $\tau_c = W\tau_0$  – тривалість інформаційного символу  $c_{nl}^{(i)}$ ;  $\tau_0$  – тривалість елемента інформаційного символу;  $W$  – база широкосмугового сигналу;  $\dot{A}_{nl}(t - i\tau_c - \tau_{nl})$  – сигнальна послідовність  $n$ -го користувача, що відпо-

відає  $i$ -му інформаційному символу із затримкою  $\tau_{nl}$ ;  $\dot{a}_{nl}$  – комплексна амплітуда  $l$ -го променя;  $B_3(t)$  – негаусівська випадкова завада,  $B_0(t)$  – адитивний білий гаусівський шум (АБГШ).

У рамках поданої моделі кожний  $n$ -й абонент,  $n \in \{1, 2, \dots, N\}$  у довільні моменти часу, передає на  $i$ -й позиції комплексний інформаційний символ  $c_{nl}^{(i)}(t) = c_n(t) \in \{-1; +1\}^{NI}$ , ( $i - 1$ ) $\tau_c < t \leq i\tau_c$  де  $I$  – довжина протокового блоку даних, що передається радіоканалом. Дискретна модель групового сигналу може бути подана у вигляді:

$$\tilde{Z} = A_{ac} + B_3 + B_0, \quad (2)$$

де  $A$  – вектор комплексних інформаційних символів сигналів користувачів,  $a$  – матриця комплексних амплітуд сигналів користувачів,  $c$  – матриця користувальницьких сигнальних векторів, узятих для кожного символу. Рішення про оцінку компонентів вектора прийнятих інформаційних символів користувачів виносяться на основі мінімуму метрики:

$$\hat{c}_n = \arg \min_{c \in \{-1; +1\}^N} d^2(\tilde{Z}, A_n), \quad (3)$$

де  $\tilde{Z}, A_n$  – векторні еквіваленти прийнятого і переданого сигналу. Вектор первісних статистик, що обчислюють у  $n$ -х каналах кореляційного приймача, визначається, як:

$$x = \rho ac + \tilde{B}_0, \quad (4)$$

де  $\rho$  – матриця взаємної кореляції сигнатурних сигналів;  $\tilde{B}_0$  – вектор гаусівського шуму з кореляційною матрицею  $\sigma^2 \rho$ ;  $\sigma$  – дисперсія шуму. Відповідно, для довільного  $i$ -го бітового інтервалу проміжна статистика визначається у вигляді:

$$x_n^{(i)} = \langle \tilde{Z}, A_n \rangle_n^{(i)} = a_n^{(i)} c_n^{(i)} + \sum_{n \neq l} \sum_{i=0}^{I-1} a_l^{(i)} c_l^{(i)} \rho_{n,l}^{(i)} + \sigma B_n^{(i)}, \quad (5)$$

де другий доданок відображує внесок сигналів користувачів у каналі.

Оптимальна за критерієм максимальної правдоподібності оцінка  $\hat{c}$  відповідає мінімальній нормі і максимізує функцію правдоподібності вибірки:

$$\hat{n} = \arg \max_{c \in \{-1; +1\}^N} \{2c^T x - c^T H c\}, \quad (6)$$

де  $H = \{h_{ln} = \rho_{ln} a_l a_n\}$  – матриця, обумовлена взаємними кореляціями сигналів користувачів та їх комплексних амплітуд. Прийняттю рішень про символи передують оцінка інтенсивностей та інших неінформативних параметрів абонентських сигналів, які обчислюються блоком оцінки стану каналу зв'язку із заданою точністю.

Для підвищення ефективності роботи CDMA-систем у негаусівських каналах розроблений адаптивний метод багатоабонентського розділення широкосмугових сигналів, заснований на комбінованих рішеннях паралельного відсікання негаусівських завад з інкапсульованими процедурами адаптивної обробки сигналів і поканальної демодуляції-декодування на кожній ітерації.

У процесі роботи приймача на кожній стадії відсікання завад у кожному каналі рекурентно формується множина нових оцінок статистик у вигляді:

$$x = ac + \rho a(c - \hat{c}) + \tilde{B}_0, \quad (7)$$

або в більш загальному вигляді для  $j$ -го каскаду:

$${}_{(j)} = \frac{(J - (J - \rho)^{j+1})x}{\rho}. \quad (8)$$

Процес триває доти, поки всі передані інформаційні послідовності не будуть коректно демодульовані. У результаті врахування оцінок негаусівських завад у кожному з каналів на  $(j + 1)$ -й стадії утворяться уточнені значення „очищеного” групового сигналу:

$$Z^{j+1} = \tilde{Z} - \sum_{n=1, n \neq l}^N A_l a_l \hat{c}_l^j. \quad (9)$$

Таким чином, принцип роботи алгоритму полягає в ітеративному формуванні на приймальному боці самостійних незалежних оцінок завад для кожного абонента для того, щоб відняти всі або деякі з них із прийнятого групового сигналу.

Для оцінки ефективності запропонованого методу у зазначених умовах виконане статистичне моделювання основних методів обробки сигналів у каналах з негаусівськими завадами. У процесі моделювання використовувалося квазікогерентне приймання сигналів з фазовою маніпуляцією у трипроменевому зворотному каналі з негаусівською завадою. Затримки променів вважаються відомими. Застосовувалось згорточне кодування зі швидкістю  $1/2$ .

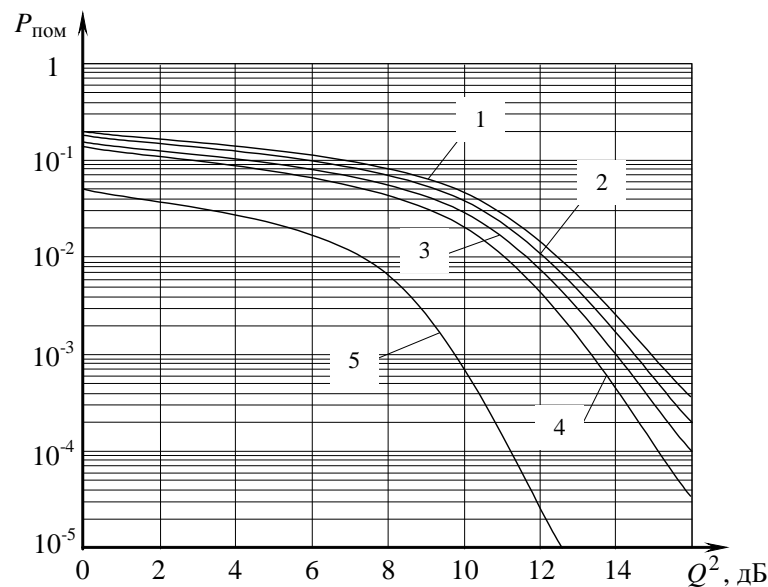


Рис. 1. Завадостійкість методів обробки сигналів у каналах з негаусівськими завадами

На рис. 1 зображено залежності ймовірності помилкового приймання сигналів  $P_{\text{пом}}$  від відношення сигнал/завада  $Q^2$  для різних методів обробки сигналів (крива 1 – традиційне детектування, 2 – метод приймання з мінімальною середньоквадратичною помилкою, 3 – метод приймання з послідовним подавленням завад, 4 – метод приймання з паралельним подавленням завад, 5 – запропонований у роботі метод).

**Висновки.** Отже, як видно з графіків, розроблений метод обробки сигналів забезпечує найкращі характеристики приймання в негаусівському каналі. Виграш у завадостійкості для ідентичних значень бітової помилки  $10^{-3}$  і рівної спектральної ефективності становить 3-4 дБ.

Запропонований метод може бути застосований в адаптивних засобах радіозв'язку при реалізації механізму захисту від природних і навмисних завад.

#### Список використаних джерел

1. Невдяев Л. М. Мобильная связь 3-го поколения / Л. М. Невдяев. – М., 2000. – 208 с. – (Серия изданий «Связь и бизнес»).
2. Широкополосные беспроводные сети передачи информации / В. М. Вишнеvский, А. И. Ляхов, С. Л. Портной, И. В. Шахнович. – М.: Техносфера, 2005. – 592 с.

3. Григорьев В. А. Сети и системы радиодоступа / В. А. Григорьев, О. И. Лагутенко, Ю. А. Распаев. – М.: Око-Трендз, 2005. – 384 с.
4. Волков Л. Н. Системы цифровой радиосвязи: базовые методы и характеристики: учебное пособие / Л. Н. Волков, М. С. Немировский, Ю. С. Шинаков. – М.: Эко-Трендз, 2005. – 392 с.
5. Теорія електричного зв'язку. Ч. 1: Основи теорії сигналів та розподілу інформації: підручник / О. В. Кувшинов, С. П. Лівенцев, О. П. Лежнюк [та ін.]. – К.: ВПІ НТУУ „КПІ”, 2008. – 331 с.
6. Кувшинов О. В. Аналіз способів підвищення ефективності систем рухомого радіозв'язку з кодовим розділенням сигналів / О. В. Кувшинов, С. П. Лівенцев // Збірник наукових праць ВПІ НТУУ “КПІ”. – 2004. – Вип. № 3. – С. 91-96.
7. Ильченко М. Ю. Телекоммуникаційні системи широкопasmового радіодоступу / М. Ю. Ильченко, С. О. Кравчук. – К.: Наукова думка, 2009. – 312 с.
8. Wilton A. Deploying Wireless Networks / Wilton A., Charity T. – Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, Sao Paulo: Cambridge University Press, 2008. – 380 p.
9. Голдсмит А. Беспроводные коммуникации / А. Голдсмит. – М.: Техносфера, 2011. – 904 с.
10. IEEE Std 802.16f-2005: IEEE standard for local and metropolitan area networks. Part 16: air interface for fixed broadband wireless access systems. Amendment 1: management information base (Amendment to IEEE Std 802.16-2004). – New York: IEEE-SA Standards Board, 2005. – 257 p.

УДК 004.99:519.237

**Е.В. Петров**, магістр

**С.А. Нестеренко**, канд. техн. наук

Черниговский государственный технологический университет, г.Чернигов, Украина

## ПОВЫШЕНИЕ СЕКРЕТНОСТИ СТЕГАНОГРАФИЧЕСКОЙ ПЕРЕДАЧИ ДАНЫХ В ИНТЕРНЕТ-ПОТОКЕ

*Сформулировано основныe причины, позволяющие по характеристикам интернет-потока, управляемого протоколом TCP, обнаружить факт передачи стегосообщения. Предложено модификация протокола передачи стегосообщения, способная нивелировать проявление упомянутых выше особенностей передачи, и, таким образом, повысить ее секретность.*

*Сформульовано основні причини, які дозволяють за характеристиками інтернет-потокy, керованого протоколом TCP, виявити факт передачі стегоповідомлення. Запропоновано модифікацію протоколу передачі стегоповідомлення, яка здатна нівелювати прояв згаданих вище особливостей передачі, і, таким чином, підвищити її секретність.*

*In the paper present the basic reasons which allow to detect the fact of stego message transmitting by analysis the statistical flow characteristics of Internet stream driven by TCP protocol. A modification of the transmission protocol which can reverse the expression of the above-mentioned singularities of transmission, and thus, increase the secrecy of the transfer is proposed.*

**Постановка проблемы.** Предметом данной статьи является один из аспектов информационной безопасности, то есть такого состояния информационной системы, при котором обеспечивается сохранность, целостность и необходимая недоступность данных в ней [4].

Задача защиты информации от несанкционированного доступа является неизменно актуальной во многих областях человеческой деятельности: военном деле, государственном управлении, медицине, обеспечении конституционных прав граждан и т. п. Исторически выделились два основных направления решения этой задачи, существующие и по сегодняшний день: криптография и стеганография. Целью криптографии является скрытие содержимого наблюдаемых сообщений за счет их шифрования. В отличие от неё, при стеганографии скрывается не только содержание передаваемого секретного сообщения, но и сам факт его существования или передачи [3]. Назовем это требование «С-принципом».

Сегодня доминируют криптографические методы защиты информации, они весьма совершенны и их множество. Что касается стеганографии, то она развивалась значитель-