УДК621.396.001

Дідковський Р. М., к.т.н.; **Фауре Е. В.,** к.т.н.; **Олексієнко В. В.**
(Черкаський державний технологічний університет)

АНСАМБЛЬ ОРТОГОНАЛЬНИХ ШУМОПОДІБНИХ СИГНАЛІВ ДЛЯ СКРИТНИХ СИСТЕМ З ОБМЕЖЕНИМ СПЕКТРОМ

Дідковський Р. М., Фауре Е. В., Олексієнко В. В. Ансамбль ортогональних шумоподібних сигналів для скритних систем з обмеженим спектром. У роботі запропоновано метод побудови ансамблю фінітних ортогональних шумоподібних сигналів із заданими спектральними характеристиками. Велика розмірність простору параметрів сигналу забезпечує надійний захист переданої інформації. Експериментальні дослідження підтвердили ефективність методу.

Ключові слова: ШУМОПОДІБНИЙ СИГНАЛ, ОРТОГОНАЛЬНИЙ АНСАМБЛЬ СИГНАЛІВ, ПРОЦЕДУРА ОРТОГОНАЛІЗАЦІЇ ГРАМА-ШМІДТА, ФІНІТНА ФУНКЦІЯ,АЛГЕБРА КЛІФОРДА,

Дидковский Р. М., Фаурэ Э. В., Олексеенко В. В. Ансамбль ортогональных шумоподобных сигналов для скрытных систем с ограниченным спектром. В работе предложен метод построения ансамбля финитных ортогональных шумоподобных сигналов с заданными спектральными характеристиками. Большая размерность пространства параметров сигнала обеспечивает надежную защиту переданной информации. Экспериментальные исследования подтвердили эффективность метода.

Ключевые слова: ШУМОПОДОБНЫЙ СИГНАЛ, ОРТОГОНАЛЬНЫЙ АНСАМБЛЬ СИГНАЛОВ, ПРОЦЕДУРА ОРТОГОНАЛИЗАЦИИ ГРАМА-ШМИДТА, ФИНИТНАЯ ФУНКЦИЯ, АЛГЕБРА КЛИФФОРДА

Didkowsky R. M., Faure E. V., Oleksiienko V. V. The ensemble of orthogonal noise-like signals for covert systems with a limited spectral range. This paper presents a method for constructing an ensemble of finite orthogonal noise-like signals with given spectral characteristics. High dimension of the signal parameter space provides reliable securing data transfer. Experimental studies have confirmed the effectiveness of the method.

Key words: NOISE-LIKE SIGNAL, ORTHOGONAL ENSEMBLESIGNAL, GRAM-SCHMIDT ORTHOGONALIZATION PROCEDURE, FINITE FUNCTION, CLIFFORD ALGEBRA

Вступ. У роботі [1] запропонована система скритної передачі цифрової інформації по існуючих проводових лініях зв'язку. При цьому аналоговий сигнал системи зв'язку основного призначення (сигнал проводового радіо, мовний сигнал в лінії фіксованого телефонного зв'язку, тощо) виконує роль маскуючого для сигналу прихованої цифрової системи. Зрозуміло, що сигнали двох систем слугують завадою один для одного. Потужність прихованого цифрового сигналу (аби він не був виявленим) має бути багато меншою ніж потужність основного сигналу. Вірність прийому інформації забезпечується шляхом використання широкосмугового багаторівневого псевдошумового сигналу в режимі бінарної фазової маніпуляції. При цьому тривалість символьного інтервалу також має бути значною.

Експериментальні дослідження показали, що при відношенні сигнал-завада по потужності близько–15 дБ у смузі частот від 0 до 22 кГц швидкість передачі з прийнятним рівнем імовірності помилки може досягати лише 100-200 біт/с.

Отже було виявлено кілька суттєвих проблем у будові системи:– слуховий апарат людини досить чутливий до широкосмугового шуму, тому достатній рівень маскування сигналу досягається лише при дуже низькій його потужності;– сигнали повністю перекриваються по спектральному діапазону, тому неможливо застосувати попередню фільтрацію для підвищення відношення сигнал-завада в приймачі системи;– система має низьку швидкість передачі даних. Основна гіпотеза роботи полягає в тому, що вивівши спектральний діапазон цифрового сигналу на межу діапазону частот сигналу основного призначення можна значно поліпшити показники системи.

Постановка задачі. Із сформульованої гіпотези випливає задача побудови системи шумоподібних сигналів із керованими спектральними характеристиками. При цьому має бути забезпечена значна варіативність форми сигналу, що гарантуватиме високу параметричну скритність системи зв'язку [2]. Крім того, структура сигналу має дозволяти здійснення багатопозиційної модуляції для збільшення швидкості передачі даних.

Вирішення задачі. На шляху вирішення поставленої задачі виникає проблема, яка полягає у суперечності між скінченною тривалістю сигналу та необхідністю обмежити його

спектр [3]. Крім того, неможливо фізично реалізувати канал зв'язку із обмеженою смугою пропускання [4]. Наслідком ігнорування цієї проблеми та практичного застосування ідеалізованих моделей є систематичні похибки (власні системні завади), що проявляються як міжсимвольна та міжканальна інтерференція. Ці явища стають суттєвою перепоною при намаганні збільшити швидкість передачі даних у каналі або кількість паралельно працюючих каналів. У зв'язку з цим задача побудови ансамблю ортогональних сигналів завжди вимагає певних компромісів. На даний час вказана задача не може вважатися однозначно вирішеною, отже є актуальною для теорії і практики телекомунікаційних систем [5, 6].

Будемо вважати обов'язковою вимогу обмеженості носія сигнальної функції тривалістю символьного інтервалу. Для систем, що використовують цифрові методи формування та обробки сигналу, виконання даної вимоги значно спрощує алгоритми функціонування та апаратну реалізацію приймально-передавальних пристроїв.

Системи ортогональних функцій, запропоновані в роботі [5], не обмежені в часі і тому не можуть бути безпосередньо використані для вирішення поставленої задачі.

Цікавий результат у цьому сенсі отримано в роботі [6], однак прийом сигналу у даному випадку здійснюється за результатами вимірювання значень вхідного сигналу лише в трьох точках символьного інтервалу, що веде до значних втрат завадостійкості системи зв'язку. Тому для побудови скритної системи зв'язку даний ансамбль сигналів неприйнятний.

Запропонуємо власну методику формування багатопозиційного шумоподібного сигналу для систем скритної передачі інформації. Методику побудови такого ансамблю покажемо на прикладі системи, інформаційний символ якої складається з 4-х біт (4 базисні функції). На перших двох етапах будемо діяти певною мірою аналогічно до методики, викладеної в [3].

Етап 1. Вибір першої базисної функції.

Розглянемо фінітну функцію

$$x(t)=\begin{cases}\exp\left(-\dfrac{t^2}{2\cdot(\nu\cdot\Theta)^2}\right)\cdot\cos^2\left(\dfrac{\pi}{\Theta}\cdot t\right),\ t\in\left(-\dfrac{\Theta}{2};\dfrac{\Theta}{2}\right),\\ 0,\ t\notin\left(-\dfrac{\Theta}{2};\dfrac{\Theta}{2}\right),\end{cases}$$

де $\Theta>0$ – тривалість імпульсу; $\nu\neq 0$ – параметр форми.

Дана функція має ненульові значення на інтервалі $(-\Theta/2;\Theta/2)$ (носій функції), на кінцях якого дорівнює нулю разом із своєю першою похідною. Це дозволяє досягти неперервності сигналу та його фази при переході від одного символьного інтервалу до іншого. Спектр сигналу $x(t)$ визначається функцією

$$X(\omega)=\frac{\nu\cdot\Theta^2}{\sqrt{2\pi}}\cdot\left(X_0(\omega)+\frac{1}{2}X_0\left(\omega+\frac{2\pi}{\Theta}\right)+\frac{1}{2}X_0\left(\omega-\frac{2\pi}{\Theta}\right)\right),$$

де $X_0(\omega)=\int\limits_{-\infty}^{+\infty}\dfrac{\sin\left(\dfrac{\Theta}{2}\cdot\xi\right)}{\dfrac{\Theta}{2}\cdot\xi}\cdot\exp\left(-\dfrac{(\nu\cdot\Theta\cdot(\omega-\xi))^2}{2}\right)d\xi$.

Наприклад, при $\nu=0{,}2$ отримаємо функцію $x(t)$, графік якої зображено на рис.1,а. Відповідний нормований спектр потужності $X_H^2(\omega)=\left(X(\omega)/X(0)\right)^2$ показано на рис. 1,б. З рисунку видно, що друга пелюстка спектру знаходиться на рівні меншому ніж -75 дБ. Отже за межами основної спектральної пелюстки даний сигнал не створює суттєвих завад іншим системам зв'язку. Приблизна ширина спектра визначається значенням Θ і може бути виражена рівністю $F\approx 9/\Theta$. Отже, вибрана функція задовольняє поставленим вимогам щодо властивостей спектру.

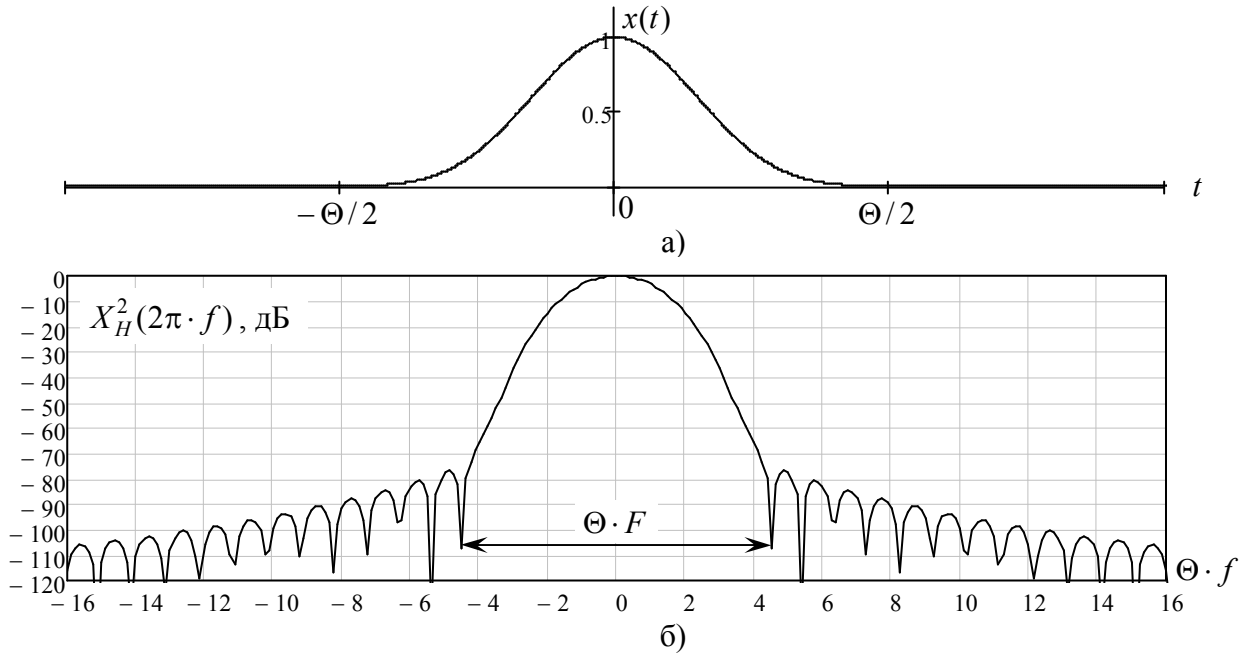

Рис. 1. Графік функції $x(t)$ (а) та її нормований спектр потужності (б)

Етап 2. Побудова лінійно незалежної системи функцій.

Шляхом зсуву сигналу $x(t)$ в часі на чотири різні позиції τ_1, τ_2, τ_3 та τ_4 отримаємо набір сигналів $x_i(t) = x(t-\tau_i)$, $i = 1,2,3,4$. Затримки τ_i мають задовольняти наступні вимоги: *1)*вони всі попарно різні;*2)* $\tau_i \geq \Theta/2$, $i = 1,2,3,4$;*3)* $\tau_i \leq T - \Theta/2$, $i = 1,2,3,4$.

Виконання цих вимог забезпечує лінійну незалежність системи функцій $x_i(t)$, $i = 1,2,3,4$, а також те, що носії цих функції лежать в межах відрізка $[0;T]$. Число T визначає тривалість символьного інтервалу системи зв'язку.

На відміну від [3] ми не вимагаємо рівномірного кроку між часовими зсувами τ_i.

Етап 3. Побудова ортонормованого базису.

Для сигналів $x_i(t)$ тривалості T проведемо процедуру ортогоналізації Грама-Шмідта [7]:

$$y_1(t) = x_1(t),\ y_2(t) = x_2(t) - \frac{< y_1(t), x_2(t) >}{< y_1(t), y_1(t) >} y_1(t),$$

$$y_3(t) = x_3(t) - \frac{< y_1(t), x_3(t) >}{< y_1(t), y_1(t) >} y_1(t) - \frac{< y_2(t), x_3(t) >}{< y_2(t), y_2(t) >} y_2(t),$$

$$y_4(t) = x_4(t) - \frac{< y_1(t), x_4(t) >}{< y_1(t), y_1(t) >} y_1(t) - \frac{< y_2(t), x_4(t) >}{< y_2(t), y_2(t) >} y_2(t) - \frac{< y_3(t), x_4(t) >}{< y_3(t), y_3(t) >} y_3(t),$$

де $< u(t), v(t) >= \frac{1}{T}\int_0^T u(t)v(t)dt$.

Після чого виконаємо нормування середньої потужності отриманих сигналів

$$z_i(t) = \frac{1}{\sqrt{< y_i(t), y_i(t) >}} y_i(t),\ i = 1,2,3,4.$$

Сигнали $z_i(t)$, $i = 1,2,3,4$ утворюють ортонормований базис.

На рис. 2 наведено приклад базису $z_i(t)$, отриманого для затримок $\tau_1 = 7\Theta/8$, $\tau_2 = 4\Theta/8$, $\tau_3 = 6\Theta/8$, $\tau_4 = 5\Theta/8$.

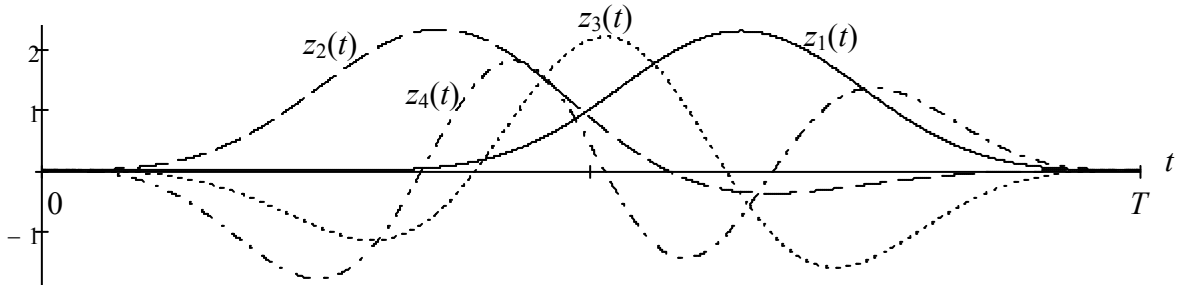

Рис. 2. Ортонормований базис $z_i(t)$, $i = 1, 2, 3, 4$.

Етап 4. Формування випадкового або псевдовипадкового ортогонального базису.

Передавач і приймач скритної цифрової системи зв'язку із взаємно кореляційним прийомом мають бути оснащені ідентичними генераторами псевдовипадкової послідовності, наприклад: з рівномірним або усіченим нормальним розподілом.

Зауважимо, що для систем із передачею опорного сигналу та автокореляційним прийомом (див., наприклад, [8]) генератор передавача повинен бути істинно випадковим, а на приймальній стороні аналогічний генератор взагалі не потрібен.

Позначимо $\overline{b}_1 = (a_1, a_2, a_3, a_4)$ –чотирьохелементнунормовану реалізацію послідовності, що спостерігається на виході генератора.

У [9] на базі апарату алгебри Кліфорда запропонована система лінійних перетворень, що дозволяє отримати ортогональний репер, виходячи з будь-якого ненульового вектора. Для розмірності простору 4 дані перетворення можна записати у вигляді наступних формул перетворення координат вектора $\overline{b}_1$:

$$\overline{b}_2 = (a_4, a_3, -a_2, -a_1),\ \overline{b}_3 = (a_3, -a_4, -a_1, a_2),\ \overline{b}_4 = (a_2, -a_1, a_4, -a_3).$$

Разом з вектором $\overline{b}_1$ результуючі вектори $\overline{b}_2$, $\overline{b}_3$ і $\overline{b}_4$ утворюють ортонормований базис.

Безпосередньою перевіркою можна переконатися, що лінійні комбінації виду $w_i(t) = b_{i1}z_1(t) + b_{i2}z_2(t) + b_{i3}z_3(t) + b_{i4}z_4(t)$, де b_{ij} – координата номер j вектора $\overline{b}_i$, $i = 1,2,3,4$, утворюють ортогональну на відрізку $[0;T]$ систему функцій.

Доведемо, наприклад, ортогональність функцій $w_1(t)$ та $w_2(t)$:

$$< w_1(t), w_2(t) >= \frac{1}{T}\int_0^T w_1(t) \cdot w_2(t)\, dt =$$

$$= \frac{1}{T}\int_0^T (a_1 z_1(t) + a_2 z_2(t) + a_3 z_3(t) + a_4 z_4(t)) \cdot (a_4 z_1(t) + a_3 z_2(t) - a_2 z_3(t) - a_1 z_4(t))\, dt =$$

$$= \frac{1}{T}\int_0^T (a_1 a_4 z_1^2(t) + a_2 a_3 z_2^2(t) - a_3 a_2 z_3^2(t) - a_4 a_1 z_4^2(t) + a_1 a_3 z_1(t) z_2(t) - a_1 a_2 z_1(t) z_3(t) -$$

$$- a_1^2 z_1(t) z_4(t) + ... + a_4 a_3 z_4(t) z_2(t) - a_4 a_2 z_4(t) z_3(t))\, dt.$$

Враховуючи рівність енергії сигналів $z_i(t)$, $i = 1,2,3,4$, інтеграли, що відповідають першому та четвертому, а також другому та третьому доданкам підінтегрального виразу, взаємно знищаться. Всі наступні доданки дадуть нульові значення інтегралу в силу ортогональності системи сигналів $z_i(t)$, $i = 1,2,3,4$. Отже $< w_1(t), w_2(t) >= 0$.

Інші рівності виду $< w_i(t), w_j(t) >= 0$, $i = 1, 2, 3, 4$; $j = 1, 2, 3, 4$, $i \neq j$, доводяться аналогічно.

Етап 5. Модуляція. Нехай тепер λ_i – біт номер i 4-бітного інформаційного символу. Утворимо груповий сигнал за формулою $s(t) = \sum_{i=1}^{4}(2\lambda_i - 1)\cdot w_i(t)$. По суті, тут відбувається фазова маніпуляція 4-х ортогональних носійних.

Сигнал $s(t)$ може бути використаний як для доставки одразу 4-х біт одному споживачеві, так і для доставки по одному біту 4-м різним споживачам. Приймач кожного з них має бути налагоджений на свій тип вектора $\overline{b}_i$ (кодове розділення каналів).

Етапи 1...3 можуть бути виконані заздалегідь (до початку передачі пакету інформації), а етапи 4 і 5 виконуються щоразу при формуванні сигналу наступного символьного інтервалу. Завдяки цьому форма сигналу буде постійно змінюватись навіть при передачі однакової групи біт (за рахунок оновлення координат вектора $\overline{b}_1$). Вказана особливість значно підвищує параметричну скритність запропонованої системи сигналів. Якщо генератор елементів вектора $\overline{b}_1$ досить багатий аби уникнути повторюваності послідовності протягом часу, доступного для спостереження третьою стороною, то переданий сигнал буде сприйматися неуповноваженим спостерігачем як істинно випадковий і такий, що не несе корисної інформації.

На рис. 3,а зображено приклад осцилограми сигналу $s(t)$ протягом чотирьох символьних інтервалів після переносу частот за допомогою балансного модулятора (центральна частота дорівнює $f_0 = 128/\Theta$). На всіх символьних інтервалах даного прикладу передано один і той же символ «0011».

Зауважимо також, що сигнал $s(t)$ є лінійною комбінацією зсунутих у часі копій сигналу $x(t)$, тому ширина основної пелюстки його спектру залишається незмінною (див.рис. 3,б).

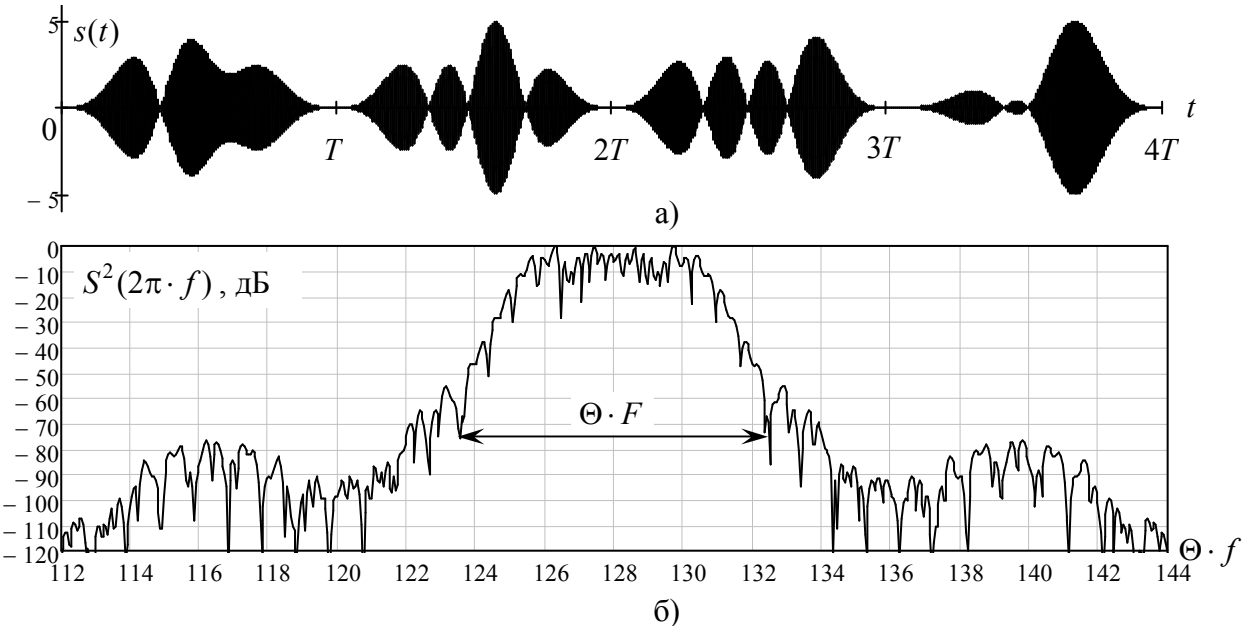

Рис. 3. Сигнал $s(t)$ (а) та його нормований спектр потужності (б)

Відмітимо, що для побудови практичних систем даного типу більш зручним є використання 8-бітних інформаційних символів. Формули для отримання відповідної системи лінійних перетворень можна знайти в [9]. Чотири-бітна (16-ти позиційна) система модуляції прийнята в роботі лише для компактності викладок.

Експериментальні дослідження. Запропонована система дозволяє досить просту реалізацію. Експериментальний макет складається з двох комп'ютерів. Лінійний вихід звукової плати першого з них (передавач) з'єднаний з лінійним входом звукової плати

другого (приймач) за допомогою двожильного кабелю довжиною 12 м. Формування і обробка сигналів здійснюється за допомогою спеціально розробленого програмного забезпечення у відкладеному часі. Звукові плати використовуються для цифро-аналогового (на передавальній стороні) та аналогово-цифрового (на приймальній стороні) перетворення та підсилення сигналів.

На передавальній стороні одночасно відтворюються два звукових файли: 1) музикальна композиція з полосою частот від 0 до 22,05 кГц (частота дискретизації 44,1 кГц); 2) сигнал цифрової системи зв'язку з полосою частот від 22 до 26 кГц (частота дискретизації 96 кГц).

На приймальній стороні відбувається фіксація вхідного сигналу з частотою дискретизації 192 кГц. Результуючий файл обробляється відповідним програмним забезпеченням, яке відновлює інформаційне повідомлення. Прийняте інформаційне повідомлення порівнюється з переданим, що дозволяє встановити наявність та кількість помилок передачі-прийому.

В ході експерименту була досягнута швидкість передачі 1600 біт/с. Загалом було передано 10^5 біт пакетами по 10^4 біт. Жодної помилки виявлено не було.

Висновки. Використання запропонованого у даній роботі ансамблю ортогональних сигналів дозволило підвищити швидкість передачі даних порівняно з системою скритної передачі даних [1] у 8–16 раз. При цьому форма сигналу залежить від великої кількості параметрів (часові зсуви τ_i, псевдовипадковий вектор $\overline{b_1}$), що дозволяє убезпечити передану інформацію від несанкціонованого доступу.

Слід зауважити, що дана система сигналів може бути застосована не лише в системах проводового зв'язку, а й у радіосистемах (при відповідному виборі частотних параметрів).

Подальші дослідження мають бути пов'язані з розробкою надійних методів тактової синхронізації системи, що не порушують скритності передачі даних.

Література

1. Дідковський Р. М. Прихована передача інформації в звуковому частотному діапазоні / Р. М. Дідковський, Е. В. Фауре, В. В. Олексієнко // Зб. тез наук.-техн.конф. «Проблеми телекомунікацій». – К.:, НТУУ «КПІ», 2011. – С.108.

2. Мазурков М. И. Системы широкополосной радиосвязи: учеб.пособие для студ. вузов / М. И. Мазурков. – Одесса: Наука и техника, 2010. – 340 с.

3. Дегтярев А. Н. Разложение сигналов по системе физически реализуемых функций / А. Н. Дегтярев // ВісникСевНТУ. Інформатика, електроніка, зв'язок: зб. наук.пр. – 2010. – Вип. 101. – С.169-176.

4. Сиберт У. М. Цепи, сигналы, системы. В 2 ч. Ч. 2 / Сиберт У. М. – М.: Мир, 1988. – 359 с.

5. Дегтярев А. Н. Быстро сходящиеся ортогональные ряды в теории связи / А. Н. Дегтярев // Радіоелектронні і комп'ютерні системи. – 2010. – №7(48). – С.242-250.

6. Сукачев Э. А. Система многоуровневых сигналов для телекоммуникационных технологий / Э. А. Сукачев, И. В. Стрелковская // Наукові записки УНДІЗ. – 2010. – №3(15). – С.15-20.

7. Ильин В. А. Линейная алгебра / В. А. Ильин, Э. Г. Позняк. – М.: Наука, 1974. – 296 с.

8. Первунінський С. М. Дослідження завадостійкості бінарного автокореляційного приймача шумових сигналів з фазовою маніпуляцією / С. М. Первунінський, Р. М. Дідковський, В. В. Метелап // Наукові записки УНДІЗ. – 2008. – №1(3). – С.56-63.

9. Дидковский Р. М. Получение ортогональных ансамблей дискретных шумовых сигналов с помощью линейных преобразований специального вида / Р. М. Дидковский // Матер. 21-ой Междунар. Крымской конф. «СВЧ-техника и телекоммуникационные технологии». – Севастополь: СевНТУ, 2011. – С.419-420.