УДК 623.618.2

Ю.В. Стасєв[1], Д.О. Медведєв[2], Д.О. Грабенко[1], Д.В. Жуйков[1]

[1] *Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків*
[2] *Харківський національний університет радіоелектроніки, Харків*

МЕТОД ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ З ПОЛІПШЕНИМИ АВТОКОРЕЛЯЦІЙНИМИ ВЛАСТИВОСТЯМИ

В роботі досліджуються основні положення алгебраїчної теорії завадостійкого кодування та її зв'язок з теорією сигналів. Обґрунтовується підхід, що дозволяє за рахунок використання методів алгебраїчного кодування формувати послідовності псевдовипадкових дискретних сигналів з поліпшеними автокореляційними властивостями. Формулюються та доводяться теореми, що встановлюють залежність між значеннями бічних пелюсток функції авто- і взаємної кореляції сформованих дискретних сигналів. Показано, що періодичні функції кореляції послідовностей, утворених кодовими словами еквідистантних кодів, мають дворівневу структуру, сформовані ансамблі сигналів мають поліпшені автокореляційні властивості.

Ключові слова: *функція взаємної кореляції, автокореляційні властивості, нормована функція кореляції, функція автокореляції, автокореляція.*

Вступ

Постановка проблеми у загальному вигляді. Для забезпечення потрібної завадостійкості систем зв'язку у використовують завадостійкий код та складні сигнали на основі псевдовипадкових послідовностей [1–3]. З одного боку, це дозволяє, використовуючи розвинутий математичний апарат алгебраїчної теорії блокових кодів, будувати швидкі алгоритми формування псевдовипадкових послідовностей. З іншого боку, застосування деяких класів блокових кодів дозволяє одержати поліпшені авто- і взаємокореляційні властивості. На основі розробленого методу обґрунтуємо вимоги до сформованих псевдовипадкових послідовностей у термінах кореляційного аналізу.

Мета статті – розробка конструктивного методу формування псевдовипадкових послідовностей з поліпшеними автокореляційними властивостями на основі використання алгебраїчних методів теорії завадостійкого кодування.

Аналіз останніх досягнень і публікацій. Проведені дослідження [2] показали, що розв'язання проблеми підвищення якості функціонування системи зв'язку можливе за рахунок:

– застосування змішаної стратегії поведінки системи зв'язку, що полягає у випадковому виборі алгоритму функціонування системи та використовуваних сигнально-кодових конструкцій (зменшення ймовірності постановки оптимальної перешкоди);

– вибору структури і параметрів системи зв'язку, що збільшують часткові показники якості її функціонування;

– збільшення ймовірності розпізнавання діючої стратегії радіоелектронного подавлення і класу завад та зміни алгоритму функціонування системи зв'язку.

Забезпечувати виконання цих умов, як показали дослідження [1–3], можливо при реалізації динамічного режиму функціонування цифрової системи зв'язку.

Виклад основного матеріалу

Функцією взаємної кореляції (ФВК) $R^{ij}(\tau)$ сигналів й $S^j(t)S^j(t)$, які мають кінцеві енергії, називається функція, обумовлена виразом[4]

$$R^{ij}(\tau) = \int_{-\infty}^{+\infty} S^i(t) \cdot S^j(t-\tau)dt ,$$

де t – час, τ – величина зсуву в часі другого сигналу відносно першого.

Нормована функція кореляції для двійкових дискретних послідовностей описується виразом

$$R_l^{ij}(\tau = lT_e) = \frac{1}{n}\left(S_0^i S_l^j + S_1^i S_{l+1}^j + \cdots + S_{n-1}^i S_{l+n-1}^j\right) = \frac{1}{n}\sum_{\xi=0}^{n-1} S_\xi^i S_{l+\xi}^j , \quad (1)$$

де T_e – тривалість елемента послідовності; l – кількість тактів, на які дві послідовності зсунуті одна відносно іншої; τ – часове зсунення між двома послідовностями; n – кількість елементів у послідовності; S_ξ^i – ξ-й елемент і-ї послідовності; $S_{l+\xi}^j$ – ξ-й елемент j-ї послідовності, зсунутої на l тактів.

Функція автокореляції (ФАК) дискретної послідовності кількісно характеризує міру подібності послідовності їй самій, тільки зсунутій у часі:

$$R_l^{ii}(\tau = lT_e) = \frac{1}{n}\left(S_0^i S_l^i + S_1^i S_{l+1}^i + \cdots + S_{n-1}^i S_{l+n-1}^i\right) = \frac{1}{n}\sum_{\xi=0}^{n-1} S_\xi^i S_{l+\xi}^i .$$

Ця функція має максимальне значення при

$$R_l^{ii}(\tau=0)=\frac{1}{n}\left(S_0^iS_0^i+S_l^iS_l^i+\cdots+S_{n-1}^iS_{n-1}^i\right)=\frac{1}{n}\sum_{\xi=0}^{n-1}\left(S_\xi^i\right)^2=$$
$$=1R_l^{ii}(\tau=0)=\frac{1}{n}\left(S_0^iS_0^i+S_l^iS_l^i+\cdots+S_{n-1}^iS_{n-1}^i\right)=\frac{1}{n}\sum_{\xi=0}^{n-1}\left(S_\xi^i\right)^2=1. \quad (2)$$

Розрізняють дві функції автокореляції:

– аперіодичну функцію автокореляції (АФАК);

– періодичну функцію автокореляції (ПФАК).

АФАК характеризує відклик устаткування на очікуваний сигнал і визначається за виразом

$$R_l^{ii}(\tau=lT_e)=\frac{1}{n}\left(S_0^iS_l^{i*}+S_l^iS_{l+1}^{i*}+\cdots+S_{n-l}^iS_{l+n}^{i*}\right)=\frac{1}{n}\sum_{\xi=0}^{n-1}S_\xi^iS_{l+\xi}^{i*},$$

де * – символ комплексної спряженості, який визначає компоненту аперіодичної функції автокореляції сигналу

$$S_i\left\{S_0,S_1,\cdots,S_{n-1}\right\}.$$

ПФАК характеризує відклик устаткування на періодичну послідовність очікуваних сигналів і може бути визначена за виразом

$$R_l^{ii}(\tau=lT_e)=\frac{1}{n}\left(S_0^iS_l^i+S_l^iS_{l+1}^i+\cdots+S_{n-1}^iS_{(l+n-1)\bmod n}^i\right)=$$
$$=\frac{1}{n}\sum_{\xi=0}^{n-1}S_\xi^iS_{(l+\xi)\bmod n}^i.$$

Для характеристики властивостей послідовностей використовують такі види ФВК:

– аперіодичну функцію взаємної кореляції (АФВК);

– періодичну функцію взаємної кореляції (ПФВК);

– стикову функцію взаємної кореляції (СФВК).

АФВК і ПФВК характеризує відклик устаткування на сигнал, відмінний від очікуваного (АФВК), або періодичну послідовність таких сигналів (ПФВК).

СФВК характеризує відклик устаткування на послідовність, що чергується, сигналів, відмінних від очікуваного.

Бажано, щоб сигнали мали єдиний автокореляційний пік. Інакше кажучи, необхідно, щоб значення ФАК задавалося такими виразами:

$$\begin{cases}R_l^{ii}(\tau=lT_e)=1, \text{ якщо } \tau=0\bmod(n);\\ R_l^{ii}(\tau=lT_e)=0, \text{ якщо } \tau\neq0\bmod(n).\end{cases} \quad (3)$$

Необхідно підібрати пари кодових послідовностей так, щоб ФВК мала мінімальне значення при їх попарній кореляції. Це гарантує мінімальний рівень взаємних перешкод.

Вибір оптимального ансамблю сигналів зводиться до пошуку такої структури кодових послідовностей, в якій центральний пік ФАК має найбільший рівень, а бічні пелюстки ФАК і максимальні викиди ФВК за можливості мінімальні.

Розглянемо множину кодових слів лінійного блокового (n, k, d)-коду над GF(q) [4–7]

C = {C1, C2, …, Cqk},

як підпростір $GF^k(q)$ у $GF^n(q)$, тобто, непуста множина n-послідовностей – кодових слів :

$$C^i=\left\{C_0^i,C_1^i,...,C_{n-1}^i\right\}C^i=\left\{C_0^i,C_1^i,...,C_{n-1}^i\right\}.$$

Зафіксуємо ансамбль дискретних сигналів

S = {S1, S2, …, Sqk}, так, що

S i ∈ {S1, S2, …, Sqk} = C i ∈ {C1, C2, …, Cqk}.

Для q=2 значення S_ξ^i формуються за правилом

$$S_\xi^i=\begin{cases}1, \text{ якщо } C_\xi^i=1;\\ -1, \text{ якщо } C_\xi^i=0.\end{cases}$$

Припустимо, що код C циклічний. Тоді утворений з його допомогою ансамбль сигналів S має кореляційні властивості, що задають такою теоремою.

Теорема 1 Нехай заданий ансамбль дискретних сигналів S, кожна послідовність якого утворена кодовими словами циклічного (n, k, d)-коду. Тоді періодичні авто- і взаємокореляційні властивості задовольняють таким виразам:

$$\begin{cases}R_l^{ii}(\tau=lT_e)=1, \text{ якщо } \tau=0\bmod(n);\\ R_l^{ii}(\tau=lT_e)\le\dfrac{n-2\cdot d}{n}, \text{ якщо } \tau\neq0\bmod(n);\end{cases} \quad (4)$$

$$\begin{cases}R_l^{ij}(\tau=lT_e)=1, \text{ якщо } C^i=C_{\to\tau}^j;\\ R_l^{ij}(\tau=lT_e)\le\dfrac{n-2\cdot d}{n}, \text{ якщо } C^i\neq C_{\to\tau}^j,\end{cases} \quad (5)$$

де $C_{\to\tau}^j$ – кодове слово C^j, циклічно зсунуте на τ символів.

Доказ. Для визначення аналітичної залежності авто- і взаємокореляційних властивостей послідовностей, побудованих за кодовими словами циклічного коду, запишемо значення нормованої функції кореляції за виразом

$$R=\frac{B-L}{n}, \quad (6)$$

де B – кількість збігів символів двох послідовностей на однойменних позиціях; L – кількість розбіжностей символів двох послідовностей на однойменних позиціях; n – кількість елементів у кожній з послідовностей.

Кожна послідовність $S^i\in S$ утвориться кодовим словом $C^i\in C$, отже, кореляційні властивості ансамблю сигналів S задаються властивостями (n, k, d)-коду C. Мінімальна кодова відстань d гарантує відмінність довільних кодових слів C^i і C^j коду C у d позиціях. Отже, виражаючи кількість збігів символів B і розбіжностей L формули (6) через мінімальну кодову відстань, одержимо

$$L\ge d; \quad (7)$$

$$B \le n - d. \quad (8)$$

Підставивши (7–8) у (6), одержимо залежність нормованої функції кореляції від довжини послідовності n і мінімальної кодової відстані

$$R \le \frac{n - 2 \cdot d}{n}. \quad (9)$$

Умова (9) виконується при обчисленні кореляційних властивостей для всіх кодових слів циклічного коду, у тому числі для будь-яких лінійних комбінацій кодових слів. ПФАК за визначенням виражає міру подібності послідовності їй самій, тільки зсунутій (циклічно) у часі. Але циклічне зсунення кодового слова циклічного коду дає кодове слово того ж коду, отже

$$R_l^{ii}(\tau = lT_e) \le \frac{n - 2 \cdot d}{n}. \quad (10)$$

Умова (10) виконується для всіх значень зсунень, які переводять кодове слово циклічного коду в інше кодове слово того ж коду. Однак при

$$\tau = 0 \bmod (n).$$

циклічне зсунення переводить кодове слово у вихідне кодове слово й за визначенням ПФАК у цьому випадку дає максимальне значення. З (1) виходить, що максимальне значення ПФАК дорівнює одиниці, звідки безпосередньо виходить (4). Справедливість першої частини виразу (5) випливає з виконання нерівності (9) для будь-якої лінійної комбінації кодових слів. Визначення циклічного коду гарантує наявність у множині кодових слів усіх циклічних зсунень послідовностей. Для таких послідовностей і відповідних значень τ виконується рівність

$$R_l^{ij}(\tau = lT_e) = 1.$$

Відповідно до загальної постановки завдання синтезу ансамблю дискретних сигналів з необхідними авто- і взаємокореляційними властивостями необхідно сформувати множину псевдовипадкових послідовностей.

Мінімально й максимально припустимі рівні бічних пелюсток функції автокореляції задаються такою теоремою.

Теорема 2 Нехай заданий ансамбль дискретних сигналів S, кожна послідовність якого утворена кодовими словами циклічного (n, k, d)-коду з ваговим спектром коду. Тоді періодичні авто- і взаємокореляційні властивості задовольняють виразам

$$R_{k\,min}^{ij} \ge \frac{n - 2 \cdot d^*}{n}; R_{k\,min}^{ij} \ge \frac{n - 2 \cdot d^*}{n}; \quad (11)$$

$$\begin{cases} R_{k\,max}^{ij} = 1, \text{ якщо } C^i = C^j_{\to\tau}; \\ R_{k\,max}^{ij} \le \dfrac{n - 2 \cdot d}{n}, \text{ якщо } C^i \ne C^j_{\to\tau}. \end{cases} \quad (12)$$

Доказ. Для доказу сукупності нерівностей (11) скористаємося виразом (6). Кількість розбіжностей символів двох послідовностей на однойменних позиціях L не може бути меншою за мінімальну кодову відстань d. У той же час із визначення вагового спектра коду необхідно, щоб цей параметр не перевищував d^*, тобто

$$d \le L \le d^*. \quad (13)$$

З аналогічних міркувань необхідно, щоб кількість збігів символів двох послідовностей на однойменних позиціях задовольняла обмеженням

$$n - d \ge B \ge n - d^*. \quad (14)$$

Після підстановки (13) і (14) в (6) оцінимо мінімальний рівень бічних пелюсток функції кореляції:

$$R \ge \frac{n - 2 \cdot d^*}{n}. \quad (15)$$

Обмеження (15) виконується для циклічного зсунення й будь-якої лінійної комбінації довільних кодових слів, для чого необхідне виконання сукупності нерівностей (11). Виконання нерівностей (12) виходить з (10).

Відзначимо, зокрема, що для деяких кодів справедлива рівність $\#d^* = \#d$ (еквідистантні коди). Так само не виключене виконання рівності $\#d^* = \#n$ для деяких інших кодів. Авто- і взаємокореляційні властивості синтезованих систем сигналів будуть визначатися ваговими властивостями обраного коду.

Найкращий можливий результат синтезу ансамблю сигналів досяжний при використанні еквідистантних кодів, що задається такою теоремою.

Теорема 3 Нехай заданий ансамбль дискретних сигналів S, кожна послідовність якого утворена кодовими словами циклічного еквідистантного (n, k, d)-коду. Тоді періодичні авто- і взаємокореляційні властивості задовольняють таким виразам:

$$R_l^{ii}(\tau = lT_e) = \begin{cases} 1, \text{ якщо } \tau = 0 \bmod (n); \\ \dfrac{n - 2 \cdot d}{n}, \text{ якщо } \tau \ne 0 \bmod (n); \end{cases} \quad (16)$$

$$R_l^{ij}(\tau = lT_e) = \begin{cases} 1, \text{ якщо } C^i = C^j_{\to\tau}; \\ \dfrac{n - 2 \cdot d}{n}, \text{ якщо } C^i \ne C^j_{\to\tau}. \end{cases} \quad (17)$$

Доказ. Загальне вирішення завдання синтезу сигналів з поліпшеними авто- і взаємокореляційними властивостями, що задовольняють обмеженню (3), задає теорема 3. Додамо у постановку завдання обмеження на вихідні дані – використання еквідистантних кодів. Звідки виходить така рівність $d^*=d$. Після підстановки в (11–12) одержимо (16–17).

Висновок 1. Мінімум бічних пелюсток функції автокореляції досягається при значенні

$$d = n/2. \quad (18)$$

Висновок 2. Мінімум бічних пелюсток функції взаємної кореляції для випадку $C^i \ne C^j_{\to\tau}$ досягається при значенні (18).

Як випливає з висновків 1, 2 для побудови ансамблю сигналів з поліпшеними авто- і взаємокореляційними властивостями варто використати циклічний еквідистантний код з мінімальною кодовою відстанню, що дорівнює половині довжини кодового слова.

У [3, 7–9] показано, що код, дуальний коду Хеммінга, є реєстровим кодом максимальної довжини, мінімальна кодова відстань якого дорівнює [7, 8, 10]

$$d = \frac{n+1}{2}. \qquad (19)$$

Вище було показано, що зазначений реєстровий код є циклічним еквідистантним кодом. Отже, використовуючи апарат завадостійкого кодування, можемо одержати послідовності із заданими кореляційними властивостями.

Сформулюємо теорему, відповідно до якої визначаються рівні бічних пелюсток ПФАК і ПФВК послідовностей, сформованих на основі реєстрового коду максимальної довжини.

Теорема 4. Нехай заданий ансамбль дискретних сигналів S, кожна послідовність якого утворена кодовими словами реєстрового (n, k, d)-коду максимальної довжини. Тоді періодичні авто- і взаємокореляційні властивості задовольняють таким виразам:

$$R_l^{ii}(\tau = lT_e) = \begin{cases} 1, \text{ якщо } \tau = 0 \bmod(n); \\ -1/n, \text{ якщо } \tau \neq 0 \bmod(n); \end{cases} \qquad (20)$$

$$R_l^{ij}(\tau = lT_e) = \begin{cases} 1, \text{ якщо } C^i = C^j_{\to\tau}; \\ -1/n, \text{ якщо } C^i \neq C^j_{\to\tau}. \end{cases} \qquad (21)$$

Доказ. Значення нормованої функції кореляції визначається за формулою (6). Підставивши вираз (19) у (6), одержимо

$$R = \frac{n - 2\cdot n + 1/2}{n} = -\frac{1}{n}. \qquad (22)$$

і дорівнює нулю.

Висновки

Таким чином, метод формування псевдовипадкових послідовностей відрізняється від відомих застосуванням алгебраїчних процедур теорії завадостійкого кодування для побудови ансамблів послідовностей, що дозволяє за рахунок врахування вагових властивостей застосовуваного коду теоретично обґрунтувати значення бічних пелюсток функції авто- і взаємної кореляції сформованих дискретних сигналів. Сформульовані й доведені теореми встановлюють аналітичну залежність між дистанційними властивостями завадостійкого коду й кореляційними характеристиками сформованих на його основі ансамблів дискретних сигналів. Нижче розглядаються алгоритми формування дискретних ансамблів сигналів відповідно до методу формування псевдовипадкових послідовностей.

Список літератури

1. Теорія сигнально-кодових конструкцій: монографія / М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов, С.П. Євсеєв – Х.: ХУПС, 2008. – 541 с.

2. Стасєв Ю.В. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов / Ю.В. Стасєв, О.О. Кузнецов // Кибернетика и системный анализ. Международный научно-теоретический журнал. – К.: Институт кибернетики НАН Украины. – 2005. – Вып. 3. – С. 47-57.

3. Стасєв Ю.В. Умови реалізації динамічного режиму функціонування захисту системи зв'язку та управління / Ю.В. Стасєв, О.О. Мелешенко, І.О. Ткаченко // Системи озброєння і військова техніка. – Х.: ХУПС, 2016. – Вип. 12(16). – С. 28-32.

4. Кларк Дж. Кодирование с исправлением ошибок в системах цифровой святи / Дж. Кларк, Дж. Кейн; пер. с англ. – М.: Радио и связь, 1987. – 392 с.

5. Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки / Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн. – М.: Связь, 1979. – 744 с.

6. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. / Пер. с англ. – М.: Мир, 1986. – 576 с.

7. Сорока Л.С. Основы теории минимально-избыточных сигналов. Математические методы и средства обработки / Л.С. Сорока. – Х.:МОУ, ОНИИ ВС, 2005. – 280 с.

Надійшла до редколегії 5.06.2017

МЕТОД ФОРМИРОВАНИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С УЛУЧШЕННЫМИ АВТОКОРРЕЛЯЦИОННЫМИ СВОЙСТВАМИ

Ю.В. Стасев, Д.О. Медведев, Д.О. Грабенко, Д.В. Жуйков

В работе исследуются основные положения алгебраической теории помехоустойчивого кодирования и ее связь с теорией сигналов. Обосновывается подход, позволяющий за счет использования методов алгебраичного кодирования формировать последовательности псевдослучайных дискретных сигналов с улучшенными автокорреляционной свойствами. Формулируются и доказываются теоремы, устанавливающие зависимость между значениями боковых лепестков функции авто- и взаимной корреляции сформированных дискретных сигналов. Показано, что периодические функции корреляции последовательностей, образованных кодовыми словами эквидистантных кодов, имеют двухуровневую структуру, а сформированной ансамбли сигналов имеют улучшенные автокорреляционные свойства.

Ключевые слова: *функция взаимной корреляции, автокорреляционные свойства, нормированная функция корреляции, функция автокорреляции, автокорреляция.*

METHOD FOR FORMING PSEUDO-SILENT SEQUENCES WITH IMPROVED AUTOCORRELATION PROPERTIES

Yu. Stasev, D. Medvedev, D. Grabenko, D. Zhuykov

The paper studies the main provisions of the algebraic theory of noise-immune coding and its relation to signal theory. An approach that allows using the methods of algebraic coding to generate sequences of pseudorandom discrete signals with improved autocorrelation properties is substantiated. Theorems that establish the dependence between the side lobe values of the auto- and cross-correlation function of the generated discrete signals are formulated and proved. It is shown that the periodic correlation functions of the sequences formed by the code words of equidistant codes have a two-level structure, and the generated signal assemblies have improved autocorrelation properties.

Keywords: *cross-correlation function, autocorrelation properties, normalized correlation function, autocorrelation function, autocorrelation.*