УДК 621.396

О.О. Кузнецов[1], А.М. Коваленко[1], О.В. Харченко[2], О.М. Носик[3]

[1]*Харківський університет Повітряних Сил імені Івана Кожедуба, Харків*
[2]*Національний аерокосмічний університет імені М.Є. Жуковського «ХАИ», Харків*
[3]*Метрологічний центр військових еталонів ВР України, Харків*

ФОРМУВАННЯ ВЕЛИКИХ АНСАМБЛІВ ДИСКРЕТНИХ СИГНАЛІВ З ПОЛІПШЕНИМИ КОРЕЛЯЦІЙНИМИ ВЛАСТИВОСТЯМИ

Досліджуються методи формування великих ансамблів псевдовипадкових послідовностей для широкосмугових систем зв'язку з прямим розширенням спектра. Пропонується підхід, який ґрунтується на використанні методів алгебраїчної теорії блокових кодів і теорії захисту інформації, що дозволяє формувати великі ансамблі сигналів з поліпшеними взаємокореляційними властивостями.

псевдовипадкові послідовності, функції взаємної автокореляції, завадостійкі коди

Постановка проблеми в загальному вигляді й аналіз літератури

Важливими показниками ефективності сучасних систем управління і зв'язку є завадозахищеність, імітостійкість і скритність [1, 2]. Перспективним напрямом забезпечення необхідних показників є застосування широкосмугових систем зв'язку з прямим розширенням спектра, в основі якого лежить використання псевдовипадкових послідовностей з необхідними кореляційними властивостями [3, 4].

Відомі методи побудови великих ансамблів псевдовипадкових послідовностей орієнтовані на використання перебірних процедур [1 – 6]. При цьому розробник неминуче стикається з "прокляттям розмірності" для розв'язуваної задачі. Кореляційні властивості оцінюються статистичними методами з використанням генеральної сукупності псевдовипадкових послідовностей [1, 3].

Метою статті є розробка регулярних методів формування великих ансамблів дискретних сигналів з поліпшеними кореляційними властивостями.

1. Суть пропонованого методу

Завадостійкі коди – один з найбільш ефективних засобів забезпечення високої достовірності передачі дискретної інформації. Важливе місце серед завадостійких кодів займають еквідистантні коди, серед яких найбільшого поширення набули регістрові коди максимальної довжини. Еквідистантним називається код, відстань між двома різними кодовими словами якого в метриці Хемінга одна і та ж.

З іншого боку відомо, що завадостійкість прийому сигналів визначається відстанню між сигналами в просторі сигналів, а залежить від енергії сигналів і їх взаємокореляційних властивостей [1, 6]. При використанні в системі зв'язку М-ових ансамблів рівноймовірних сигналів, а також при кодовому розділенні каналів вимога еквідистантності сигналів є очевидною.

Таким чином, завадостійке кодування переслідує ті ж цілі, що і формування сигналів. Як завадостійке кодування, так і побудова сигналів ґрунтуються на використанні абстрактних розділів математики і в першу чергу алгебри. Це робить природним застосування теорії завадостійкого кодування для побудови складних сигналів.

Запропонований метод формування псевдовипадкових послідовностей з поліпшеними кореляційними властивостями ґрунтується на використанні теорії захисту інформації (переставних перетвореннях) [9, 10] і розвиненого математичного апарату алгебраїчної теорії блокових кодів [7, 8]. Використання методів алгебри побудови завадостійких кодів, дозволяє формувати ансамблі дискретних еквідистантних сигналів. Переставні перетворення, що є окремим випадком афінних перетворень, дозволяють у багато разів збільшити об'єм ансамблю сигналів, не змінюючи відстань між сигналами. Структурна схема пристрою формування великих ансамблів еквідистантних сигналів з поліпшеними взаємокореляційними властивостями представлена на рис. 1.

Початкові установки. Перед початком формування сигналів джерело генеральних послідовностей формує послідовність заданої довжини, яка записується в регістр зсуву. Для кожного значення довжини $n = 2^m - 1$ формований сигнал у регістр зсуву записується своя генеральна послідовність. Генеральні послідовності для $n = 2^m - 1$, $m = 4, \ldots, 9$ наводяться далі в таблиці 1.

Формування сигналів здійснюється таким чином. Інформаційні посилки надходять на блок управління, де перетворяться в сигнали, що управляють регістром зсуву (задають кількість зсувів регістра зсуву). Таким чином, для одного фіксованого ключа пристрій може сформувати $2^m - 1$ різний сигнал. Далі, послідовність, записана в регістрі зсуву, надходить на вхід блока перестановок, стан якого задається ключем, що надходить з виходу джерела

ключів. Всього існує $(2^m - 1)!$ можливих станів блока перестановок (можливих ключів). Таким чином, пристрій може сформувати $(2^m - 1)$ різних сигналів по кожному $(2^m - 1)!$ з можливих ключів.

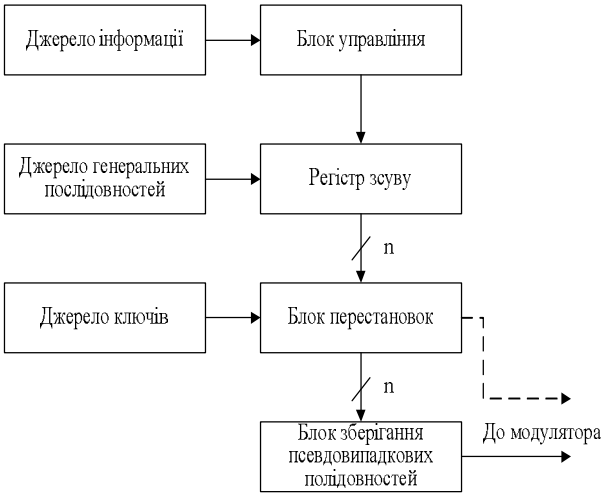

Рис. 1. Структурна схема пристрою формування сигналів

Сформовані сигнали – двійкові дискретні псевдовипадкові послідовності надходять на вхід блока зберігання псевдовипадкових послідовностей або на вхід модулятора (на схемі не наведений).

Структурна схема блока перестановок представлена на рис. 2. Він може бути реалізований різними способами, наприклад, набором з n мультиплексорів.

Суть переставного перетворення, як видно з рисунка, полягає в зміні нумерації вхідних символів, тобто вихідний вектор – суть перенумерований вхідний.

Припустимо, що $a = \{a_1, a_2, ..., a_n\}$ вхідний вектор, а $a^* = \{a^*_1, a^*_2, ..., a^*_n\}$ вихідний вектор, $\forall a_i$, $a^*_i \in GF(q)$.

Тоді переставне перетворення можна представити у вигляді: $a^* = a \cdot P$, де P – переставна матриця, тобто квадратна матриця розміром n×n елементів, у кожному рядку і в кожному стовпці якої знаходиться тільки по одній одиниці.

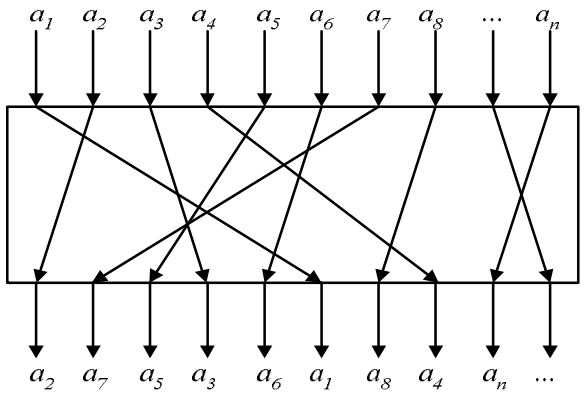

Рис. 2. Структурна схема блоку перестановок

Наприклад, для перших восьми символів вхідної послідовності на рис. 2. переставне перетворення може бути задано у вигляді виразу $a^* = a \cdot P$, де

$$P = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

На практиці переставне перетворення простіше задавати вектором перестановок $p = \{p_1, p_2, \ldots, p_n\}$, координати компонент якого відповідають індексам вхідного вектора, а власні значення компонент – індексам вихідного вектора. Наприклад, для розглянутого прикладу вектор перестановок дорівнює

$$p = \{6, 1, 4, 8, 3, 5, 2, 7\}.$$

Правило формування генеральних послідовностей. Генеральні послідовності формуються регістром зсуву. У загальному випадку структурна схема такого пристрою наведена на рис. 3. Значення зв'язків регістра зсуву задаються коефіцієнтами породжувального многочлена

$$g(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_r x^r$$

циклічного (n, k, d) коду, r = n – k.

Аналогічний результат досягається при використанні регістра зсуву із зворотними зв'язками, значення яких задаються коефіцієнтами перевірочного многочлена $h(x) = h_0 + h_1 x + h_2 x^2 + \ldots + h_k x^k$ иклічного (n, k, d) коду, причому $h(x) \cdot g(x) = x^n - 1$. Структурна схема такого пристрою наведена на рис. 4.

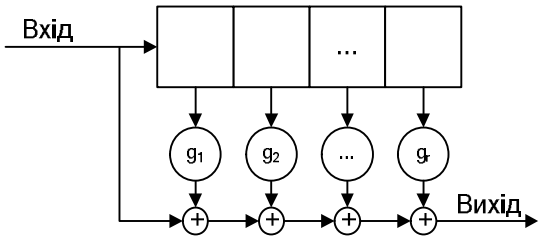

Рис. 3. Структурна схема регістра зсуву

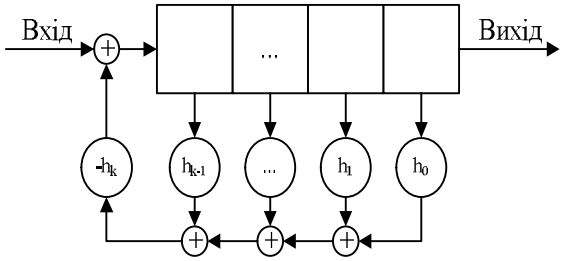

Рис. 4. Структурна схема регістра зсуву із зворотними зв'язками

Нормований коефіцієнт взаємної кореляції між формованими псевдовипадковими послідовностями дорівнює

$$R = \frac{n - 2d}{n}.$$

Параметри еквідистантних регістрових кодів зв'язані співвідношеннями [7, 8]:

$$n = 2^m - 1,\ k = m,\ d = \frac{n+1}{2},$$

отже, маємо: $R = -1/n$.

Генеральні послідовності для формування псевдовипадкових послідовностей при використанні регістрових кодів наведені в табл. 1.

Таблиця 1

Генеральні послідовності для регістрових кодів, m = 4, …, 9

n	Генеральна послідовність
15	100010011010111
31	10000100101100111110001101110 10
63	100000100001100010100111101000111001001011011101100110101011111
127	10000001000100110001011101011011000001100110101001110011110110100001010101111101001010001101110001111111000011101111001011001 00
255	10000000100011100010010111000000110010010011011100100000101011011010110010110000111110110111101000100001101100011110011100110001011010010001010010101001110111011001111011111101001100110101000110000011101010101111100101000010011111111100001011110001 10
511	10000000010000100011000010011100101010110000110111101001101110010001010000101011010011111101100100100101101111100100111010100110011000000011000110010100011010010111111010001011000111010110010011001111000111110111010000011010110110111011100000101101011111010101010000001010010101111001011101110000001110011101001001111010111010100010010000110011100001011110110110011010000111011111000011111111000010111100111000100000100101001110110100011110011111001101100010101001000111000110110101011100010011000 1000

2. Статистичні дослідження властивостей формованих псевдовипадкових послідовностей

У результаті статистичних досліджень оцінювалися такі параметри періодичної функції взаємної кореляції: $M_{|r|}$ – мат. сподівання модулів рівня бічних пелюсток; M_r – мат. сподівання рівня бічних пелюсток; $\sqrt{D_{m_{|r|}}}$ – СКВ модуля середнього значення рівня бічних пелюсток; $\sqrt{D_{m_r}}$ – СКВ середнього значення рівня бічних пелюсток; D_r – дисперсія рівня бічних пелюсток; $D_{|r|}$ – дисперсія модуля рівня бічних пелюсток; $\sqrt{D_{d_r}}$ – СКВ дисперсії рівня бічних пелюсток; $\sqrt{D_{d_{|r|}}}$ – СКВ дисперсії модуля рівня бічних пелюсток; U_{max} – мат. сподивання максимального викиду бічних пелюсток; $\sqrt{D_{U_{max}}}$ – СКВ максимальних викидів бічних пелюсток. У табл. 2 наведені результати порівняння статистичних характеристик лінійних рекурентних послідовностей максимального періоду (ЛРПМ), характеристичних послідовностей, похідних ортогональних послідовностей [1 – 6] з синтезованими послідовностями.

На рис. 5 – 7 наведені аперіодичні кореляційні функції сформованих сигналів для n = 127.

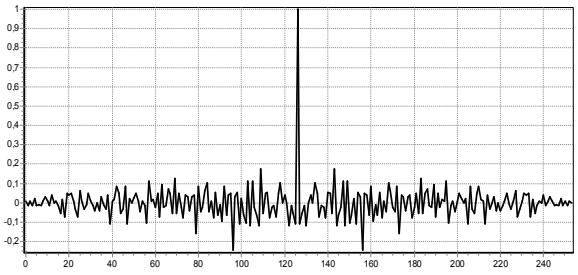

Рис. 5. Аперіодична функція автокореляції

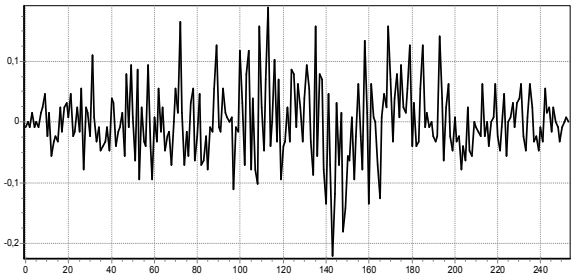

Рис. 6. Аперіодична функція взаємної кореляції

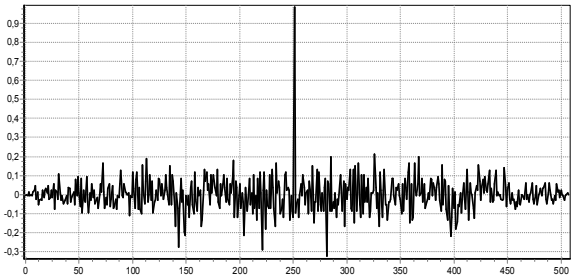

Рис. 7. Аперіодична функція стикової кореляції

Таблиця 2

Порівнювальна таблиця статистичних характеристик ПФВК

Лінійні рекурентні послідовності максимального періоду					
Параметри ПФВК	Кількість елементів у сигналі				
	15	63	255	511	1023
M	0,24	$0{,}85\cdot10^{-1}$	$0{,}46\cdot10^{-1}$	$0{,}32\cdot10^{-1}$	$0{,}93\cdot10^{-2}$
$\sqrt{D_M}$	$0{,}5\cdot10^{-1}$	$0{,}94\cdot10^{-1}$	$0{,}2\cdot10^{-1}$	$0{,}63\cdot10^{-2}$	$0{,}54\cdot10^{-2}$
D	$0{,}21\cdot10^{-1}$	$0{,}91\cdot10^{-2}$	$0{,}17\cdot10^{-2}$	$0{,}93\cdot10^{-3}$	$0{,}67\cdot10^{-3}$
$\sqrt{D_D}$	0,3	$0{,}31\cdot10^{-1}$	$0{,}14\cdot10^{-1}$	$0{,}7\cdot10^{-2}$	$0{,}8\cdot10^{-2}$
U_{max}	$2{,}9/\sqrt{L}$	$2{,}5/\sqrt{L}$	$2{,}9/\sqrt{L}$	$3{,}1/\sqrt{L}$	$3{,}1/\sqrt{L}$
$\sqrt{D_{U_{max}}}$	$0{,}51\cdot10^{-1}$	$0{,}6\cdot10^{-1}$	$0{,}63\cdot10^{-1}$	$0{,}55\cdot10^{-2}$	$0{,}53\cdot10^{-2}$
Характеристичні послідовності					
Параметри ПФВК	Кількість елементів у сигналі				
	16	60	256	508	1020
M	0,21	$0{,}82\cdot10^{-1}$	$0{,}51\cdot10^{-1}$	$0{,}34\cdot10^{-1}$	$0{,}89\cdot10^{-2}$
$\sqrt{D_M}$	$0{,}71\cdot10^{-1}$	$0{,}98\cdot10^{-1}$	$0{,}29\cdot10^{-1}$	$0{,}73\cdot10^{-1}$	$0{,}59\cdot10^{-2}$
D	$0{,}27\cdot10^{-1}$	$0{,}81\cdot10^{-2}$	$0{,}27\cdot10^{-2}$	$0{,}11\cdot10^{-1}$	$0{,}75\cdot10^{-3}$
$\sqrt{D_D}$	0,34	$0{,}35\cdot10^{-1}$	$0{,}19\cdot10^{-1}$	$0{,}66\cdot10^{-2}$	$0{,}84\cdot10^{-2}$
U_{max}	$3{,}1/\sqrt{L}$	$3/\sqrt{L}$	$3{,}8/\sqrt{L}$	$3{,}2/\sqrt{L}$	$3{,}1/\sqrt{L}$
$\sqrt{D_{U_{max}}}$	$0{,}61\cdot10^{-1}$	$0{,}67\cdot10^{-1}$	$0{,}68\cdot10^{-1}$	$0{,}66\cdot10^{-1}$	$0{,}61\cdot10^{-2}$
Похідні ортогональні послідовності					
Параметри ПФВК	Кількість елементів у сигналі				
	16	60	256	508	1020
M	$3{,}8\cdot10^{-2}$	$3{,}3\cdot10^{-2}$	$2{,}9\cdot10^{-2}$	$0{,}35\cdot10^{-1}$	$0{,}25\cdot10^{-1}$
$\sqrt{D_M}$	$7{,}5\cdot10^{-5}$	$0{,}5\cdot10^{-4}$	$8{,}7\cdot10^{-6}$	$0{,}9\cdot10^{-3}$	$0{,}69\cdot10^{-3}$
D	$5{,}6\cdot10^{-2}$	$1{,}5\cdot10^{-2}$	$4{,}4\cdot10^{-3}$	$0{,}71\cdot10^{-3}$	$0{,}36\cdot10^{-3}$
$\sqrt{D_D}$	$0{,}4\cdot10^{-1}$	$6{,}4\cdot10^{-7}$	$1{,}2\cdot10^{-6}$	$0{,}64\cdot10^{-3}$	$0{,}57\cdot10^{-3}$
U_{max}	0,38	0,33	0,19	$3{,}2/\sqrt{L}$	$3{,}8/\sqrt{L}$
$\sqrt{D_{U_{max}}}$	$2{,}1\cdot10^{-3}$	$1{,}8\cdot10^{-3}$	$1{,}1\cdot10^{-3}$	$0{,}85\cdot10^{-1}$	$0{,}77\cdot10^{-3}$
Одержані послідовності						
Параметри ПФВК	Кількість елементів у сигналі					
	31	63	127	255	511	1023
M	$1{,}1\cdot10^{-3}$	$0{,}26\cdot10^{-3}$	$6{,}24\cdot10^{-5}$	$1{,}54\cdot10^{-5}$	$3{,}74\cdot10^{-6}$	$9{,}85\cdot10^{-7}$
$\sqrt{D_M}$	$0{,}28\cdot10^{-2}$	$0{,}1\cdot10^{-2}$	$0{,}35\cdot10^{-3}$	$0{,}12\cdot10^{-3}$	$4{,}32\cdot10^{-5}$	$1{,}53\cdot10^{-5}$
D	$0{,}34\cdot10^{-1}$	$0{,}16\cdot10^{-1}$	$0{,}8\cdot10^{-2}$	$0{,}39\cdot10^{-2}$	$0{,}2\cdot10^{-2}$	$0{,}98\cdot10^{-3}$
$\sqrt{D_D}$	$0{,}85\cdot10^{-2}$	$0{,}29\cdot10^{-2}$	$0{,}1\cdot10^{-2}$	$0{,}35\cdot10^{-3}$	$0{,}12\cdot10^{-3}$	$0{,}1\cdot10^{-3}$
U_{max}	0,37 $2{,}08/\sqrt{L}$	0,296 $2{,}347/\sqrt{L}$	0,23 $2{,}6/\sqrt{L}$	0,18 $2{,}82/\sqrt{L}$	0,135 $3{,}04/\sqrt{L}$	0,102 $3{,}25/\sqrt{L}$
$\sqrt{D_{U_{max}}}$	$0{,}88\cdot10^{-1}$	$0{,}57\cdot10^{-1}$	$0{,}37\cdot10^{-1}$	$0{,}24\cdot10^{-1}$	$0{,}16\cdot10^{-1}$	$0{,}11\cdot10^{-1}$

Як показали статистичні дослідження, одержані послідовності мають поліпшені, у порівнянні з відомими, кореляційні властивості.

Висновки

Використання алгебраїчних методів побудови завадостійких кодів дозволяє формувати ансамблі дискретних еквідистантних сигналів з поліпшеними кореляційними властивостями. Переставні перетворення, що задаються випадково і незалежно сформованими ключовими даними, дозволяють генерувати великі ансамблі псевдовипадкових послідовностей значно не погіршуючи їх кореляційних властивостей. У загальному випадку кількість послідовностей в ансамблі дорівнює добутку потужності мно-

жини інформаційних послідовностей і потужності множини ключів.

Список літератури

1. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.

2. Горбенко И.Д., Стасев Ю.В., Замула А.А. Теория дискретных сигналов. Ортогональные сигналы. – МО СССР, 1988. – 119 с.

3. Стасев Ю.В., Горбенко И.Д. и др. Применение сложных сигналов в командно-телеметрических радиолиниях // Космічна наука і технологія. – 1997. – Т.3, № 5/6. – С. 104-108.

4. Горбенко И.Д., Стасев Ю.В. Безопасность информации в космических системах связи и управления // Космічна наука і технологія. – 1996. – Т. 2, № 5/6. – С. 24-28.

5. Гряник М.В., Фролов В.И. Технология CDMA – будущее сотовых систем в Украине // Мир связи. – 1998. – № 3. – С. 40-43.

6. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.

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

8. Науменко М.І., Стасєв Ю.В., Кузнецов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів: Монографія. – Х.: ХУ ПС, 2005. – 267 с.

9. Шеннон К. Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы. – 1963. – С. 333-402.

10. Horst Feistel. Cryptography and Computer Privacy. // Scientific American. – May 1973. – Vol. 228, No.5. – P. 15-23.

Надійшла до редколегії 6.03.2007

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.