ISSN 2707-1898 (print)
Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2022.02.056
Article received 13.10.2022 p.
Article accepted 17.10.2022 p.
UDK 004.421:519.15:621.372

Correspondence author
V. V. Riznyk
volodymyr.v.riznyk@lpnu.ua

В. В. Різник
Національний університет "Львівська політехніка", м. Львів, Україна

КОМБІНАТОРНА ОПТИМІЗАЦІЯ СИСТЕМ НЕЙРОМЕРЕЖЕВОГО КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ

Розглядається проблема підвищення надійності криптографічного захисту даних в нейромережевих системах з гнучким налаштуванням для забезпечення можливості шифрування (дешифрування) та пересилання повідомлень за допомогою використання сучасних методів комбінаторної оптимізації. В основу комбінаторної оптимізації покладено принцип оптимальних структурних відношень, суть якого полягає в досягненні максимальної різноманітності системи за встановлених обмежень на число структурних елементів і їх взаємного розміщення в просторі-часі. Запропоновано використати для нейромережевого захисту даних сигнально-кодові послідовності, які характеризуються високою завадостійкістю і низьким рівнем функції автокореляції. Здійснено порівняльний аналіз запропонованих послідовностей з класичними кодами. Встановлено взаємозв'язок між інформаційними параметрами оптимізованих сигнально-кодових послідовностей, за яких мінімізується значення функції автокореляції таких послідовностей та досягається їх максимальна коректувальна спроможність. Для криптографічного шифрування (дешифрування) даних запропоновано використати кодові послідовності, в яких кількість різнойменних бінарних символів відрізняються між собою не більше, ніж на один символ, що дає змогу мінімізувати значення функції автокореляції кодованого сигналу при фіксованій розрядності кодових послідовностей. Окреслено можливість формування шифрування (дешифрування) повідомлень шляхом використання різного виду оптимізованих сигнально-кодових послідовностей залежно від поставлених вимог до функціонування системи нейромережевого криптографічного захисту даних за конкретних умов забезпечення необхідної надійності охорони зашифрованих повідомлень з урахуванням обмежень на тривалість надсилання та рівня шумів в каналах зв'язку.

Ключові слова: принцип оптимальних структурних відношень; ідеальна кільцева в'язанка; кодова ІКВ-послідовність; кодова послідовність Баркера; функція автокореляції.

Вступ / Introduction

Сучасні інформаційні технології охоплюють широку сферу досліджень – від космічної радіоастрономії до систем опрацювання великих масивів даних. Аналіз наявних методів забезпечення надійності на підставі штучного введення апаратної надмірності показав, що більшість з них призводять до погіршення показників швидкодії, складності, порушуючи модульність апаратури та роблять її менш технологічною з точки зору сучасної елементної бази. Негативний наслідок збільшення вразливості інформаційних нейромережевих систем пов'язаний зі збільшенням ймовірності виникнення помилок та можливого підслуховування під час пересилання повідомлень.

Особливо важливих акцентів набувають дослідження, пов'язані з розробкою алгоритмічних методів оптимізації багатоелементних кодових послідовностей (шумоподібні коди, псевдовипадкові послідовності, *M*-послідовності тощо). Однак більшість традиційних методів завадостійкого кодування інформації від несанкціонованого доступу не забезпечують належної надійності систем. Актуальність вирішення проблеми полягає в необхідності вдосконалення шифрування повідомлень під час налаштування систем нейромережевого криптографічного захисту даних.

Об'єкт дослідження – метод використання оптимізованих кодових послідовностей для нейромережевого криптографічного захисту даних.

Предмет дослідження – оптимізовані кодові послідовності.

Мета роботи – удосконалення системи нейромережевого криптографічного захисту даних шляхом використання оптимізованих кодових послідовностей, в яких кількість різнойменних бінарних символів відрізняються між собою не більше, ніж на один символ, що дає змогу мінімізувати значення функції автокореляції кодованого сигналу, практично зводячи його до нуля при збільшенні довжини цих послідовностей.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

- визначити інформаційні параметри оптимізованих кодових послідовностей;
- здійснити порівняльний аналіз кореляційних властивостей оптимізованих кодових послідовностей з іншими видами сигнально-кодових конструкцій;
- обговорити отримані результати дослідження та зробити відповідні висновки.

Аналіз останніх досліджень та публікацій. Сучасні системи нейромережевого криптографічного захисту й передачі даних включають розроблення нових методів і засобів, кожен з яких має свої переваги і недоліки, що враховуються під час розроблення конкретних криптосистем з високим рівнем захисту та передачі даних. Для забезпечення техніко-економічних показників криптосистеми її доповнюють спеціалізованими модулями нейроподібних елементів мережі з можливістю навчання та гнучкого налаштування для криптографічного шифрування даних [8]. У цьому контексті заслуговує уваги метод поєднання кількох потоків даних в один спільний простір – метод мультиплексування

OFDM (англ. *Orthogonal Frequency-Division Multiplexing*), який перерозподіляє заданий радіоспектр для пересилання інформації на набір ортогональних піднесучих. При цьому вхідний потік даних поділяється на кілька паралельних підпотоків, кожен з яких передається з меншою швидкістю ніж початковий вхідний, де промодульовані цифрові підпотоки є взаємно ортогональними, що виключає взаємні завади між підпотоками та дає змогу використовувати частотний спектр максимально щільно без потреби додаткового простору між піднесучими. У роботі [3] викладено підхід до модуляції сигналу на підставі традиційного мультиплексування з ортогональним частотним поділом та квадратурної амплітудної модуляції з масштабуванням сузір'я. За заданим алгоритмом символ модуляції нижчого порядку розпізнається на приймальній стороні як символ модуляції вищого порядку. При цьому сузір'я модуляції вищого порядку буде складатися із множини сузір'я нижчих порядків, які передаються на окремих піднесучих OFDM сигналу з коефіцієнтом мультиплікації: 4-QAM×4 → 16-QAM, 4-QAM× 16 → 64-QAM, 16-QAM× 16 → 256-QAM, і т. п. Новизна цієї системи полягає в тому, що тільки один компонент сигналу фізично передається по каналу, а інший додається в отриманий за особливими правилами. Приймач додає другий компонент з урахуванням амплітуди прийнятого сигналу, індекс піднесучої та режим передачі даних. Усі можливі комбінації цих параметрів зведені в таблицю відображення, яку знають тільки передавач і приймач. Запропонований підхід дає можливість змішувати сигнал у великій кількості доступних піднесучих і створити тисячі можливих варіантів, щоб заплутати підслуховувача.

З розвитком криптографії та стеганографії виникла потреба отримання псевдовипадкової послідовності великої довжини. Встановлення вимог до високої завадостійкості даних послужило підставою для подальших досліджень при синтезі складних псевдовипадкових кодових послідовностей, за допомогою яких кодують символьні біти дискретних сигналів. До найвідоміших послідовностей належать коди Баркера [1] і *M* – послідовності [4]. Відомо тільки дев'ять кодів Баркера, найдовший з яких має довжину 13. Доведено, що не існує ніяких інших кодів непарної довжини, або парної довжини коротше ніж $N<10^{22}$ [1]. Для отримання більшої послідовності, ніж у наявних кодів Баркера з бажаним значенням автокореляційної функції, використовують вкладені коди Баркера. Вкладені коди утворюються з допомогою добутка Кронекера двох звичайних кодів Баркера: для довільного коду Баркера кожен з його однойменних елементів замінюється на інший код Баркера, а протилежний – на його інверсний аналог [2]. Оптимальні автокореляційні властивості можна встановити і для *M*-послідовностей. *M*-послідовності, – послідовності максимальної довжини (англ. *Maximum length sequence*, *MLS*) – псевдовипадкові послідовності, що знайшли широке вживання в широкосмугових системах зв'язку [4].

Результати дослідження та їх обговорення / Research results and their discussion

Синтез оптимізованих кодових послідовностей. В основу розробки системи нейромережевого криптографічного захисту даних закладено ідею використання унікальних властивостей комбінаторних конфігурацій – ідеальних кільцевих в'язанок (ІКВ) як концептуально нових математичних моделей оптимальних комбінаторних систем [5]. ІКВ можна представити як послідовність $K_n=(k_1,k_2,...,k_i,...,k_n)$ цілих додатних чисел, на якій всі можливі кільцеві суми перелічують натуральний ряд $1,2,\ldots S=n(n-1)$ становить R разів, де кільцевою вважається сума будь-якої кількості послідовно впорядкованих чисел ІКВ – від одного до $(n-1)$. Сума S_n всіх n елементів ІКВ визначають параметрами, які взаємопов'язані рівнянням [5] (с. 13):

$$S_n=n(n-1)/R+1 \qquad (1)$$

Алгоритм побудови кодової послідовності за допомогою ІКВ з параметрами S_n,n,R передбачає виконання наступних операцій.

Пронумерувати одновимірний масив довжиною S_n і заповнити його комірки інформаційними "одиницями", порядкові номери яких збігаються з числами z_l, $(l=1,2,\ldots,n)$, визначеними за елементами $k_i,(i=1,2,\ldots,n)$ ІКВ згідно формули:

$$z_l=\sum_{i=1}^{l}k_i,\ \ l=1,2,\ldots,n\,. \qquad (2)$$

Заповнити порожні комірки масиву інформаційними "нулями". Циклічними зсувами отриманої кодової послідовності знайти решта S_n-1 комбінацій. Результати побудови занести в таблицю кодових комбінацій.

Приклад побудови кодової послідовності за допомогою ІКВ (1, 1, 2, 3) з параметрами $S_n=7, n=4, R=2$ ілюструє табл. 1.

Табл. 1. Кодова послідовність, побудована на підставі ІКВ (1,1,2,3) / Code sequence built on the basis of IRB (1,1,2,3)

з/п	Нумерація позицій кодових символів						
	1	2	3	4	5	6	7
1	1	1	0	1	0	0	1
2	1	1	1	0	1	0	0
3	0	1	1	1	0	1	0
4	0	0	1	1	1	0	1
5	1	0	0	1	1	1	0
6	0	1	0	0	1	1	1
7	1	0	1	0	0	1	1

У табл. 1 будь-яка пара комбінацій містить тільки $R=2$ із $n=4$ "одиничних" символів в однойменних розрядах, що випливає із властивостей ІКВ. Решта $2(n-R)$ пар символів завжди відрізняються від символів, що знаходяться в однойменних розрядах. Звідси випливає формула для визначення числа d різнойменних символів, що знаходяться в однойменних розрядах:

$$d=2(n-R)\,, \qquad (3)$$

У побудованому коді кожна з $S_n(S_n-1)/2=21$ всіх можливих утворених парах кодових комбінацій міститься становить два $(R=2)$ одиничні символи в однойменних розрядах, що випливає із властивостей ІКВ з параметрами $S_n=7$, $n=4$, $R=2$. Решта $n-R=2$ символів однієї і стільки ж іншої кодових комбінацій відрізняються від символів, розміщених в однойменних розрядах. Значення мінімальної кодової відстані становить $d_{min}=d=2(n-R)=4$.

Кількість t_1 помилок, які підлягають виявленню чи виправленню t_2 за допомогою циклічного коду, побудо-

ваного за допомогою ІКВ з параметрами n, R, S_n визначають за формулами [5] (с. 102–104):

$$t_1 \le 2(n-R)-1\,;\ t_2 \le n-R-1\,. \qquad (4)$$

Потужність методу кодування збільшується вдвічі (від S_n до $2S_n$), якщо таблицю кодових комбінацій доповнити таблицею таких же розмірів, у якій символи "1" в усіх кодових комбінаціях замінити символами "0", і навпаки. Кодову відстань d_2 для коду вдвічі збільшеної потужності визначають як різницю

$$d_2 = S_n - 2(n-R)\,, \qquad (5)$$

оскільки будь-яка комбінація з однієї таблиці є доповненням кодової комбінації з другої. Мінімальна кодова відстань для коду, який об'єднує обидві таблиці, визначають як менший з двох результатів, одержаних за (3) та (5). Отже, потужність методу кодування зросла вдвічі при незмінній довжині S_n кодових комбінацій. Із (3), (4) і (5) випливають формули для визначення кількості помилок, які можна виявити і виправити циклічним ІКВ-кодом:

$$\left.\begin{aligned} t_1 &\le 2(n-R)-1 \\ t_2 &\le (n-R)-1 \end{aligned}\right\},\ \text{якщо}\ \ S_n \ge 4(n-R)\,; \qquad (6)$$

$$\left.\begin{aligned} t_1 &\le S_n - 2(n-R)-1 \\ t_2 &\le \frac{S_n - 2(n-R+1)}{2} \end{aligned}\right\},\ \text{якщо}\ \ S_n < 4(n-R)\,. \qquad (7)$$

Формули (6) і (7) визначають коректувальну здатність циклічних ІКВ-кодів збільшеної потужності [5] (с. 103). У загальному випадку співвідношення між числовими значеннями n і R можуть обиратися довільно в межах, які встановлені формулою (1). У зв'язку з цим виникає питання щодо знаходження найвигіднішого співвідношення між n і R, за якого ІКВ-код заданої потужності дає змогу виявляти і виправляти найбільшу кількість помилок. У монографії [5] (с. 103–104) розглянуто задачу поліпшення коректувальної здатність ІКВ-коду шляхом збільшення різниці $(n-R)$ при фіксованому значенні довжини S_n кодових комбінацій. З'ясовано, що ІКВ-код здатний виявляти і виправляти найбільшу кількість помилок за встановлення умови:

$$S_n = 2n \qquad (8)$$

Після підстановки (8) у (1) і розв'язання рівняння в цілих числах знайдено співвідношення між параметрами n і R, коли ІКВ-код набуває здатності виявляти і виправляти найбільшу кількість помилок:

$$\begin{aligned} R &= n/2 \ \text{ – для парних значень } n; \\ R &= (n-1)/2 \ \text{ – для непарних значень } n. \end{aligned} \qquad (9)$$

Підставляючи (9) у (4), легко бачити, що ІКВ-коди, інформаційні параметри яких обрані згідно співвідношення (9), здатні виявляти до $n-1$ та виправляти до $n/2-1$ помилок для парних, і виявляти до n та виправляти до $(n-1)/2$ помилок для непарних значень n.

Отже, в принципі будь-який ІКВ-код здатний виявляти і виправляти помилки. Однак коди з параметрами, які пов'язані співвідношенням (9), здатні виявляти до 50% і виправляти до 25% хибних символів в S_n –розрядних кодових комбінаціях [7] (с. 131). Завдяки описаним властивостям, ІКВ-коди з параметрами n, R, S_n, які відповідають співвідношенню (9), їх можна виокремити в групу оптимізованих ІКВ- кодів.

Для підвищення надійності систем нейромережевого криптографічного захисту й передачі даних з використанням кодових послідовностей належить скористатися правилом оптимізації ІКВ-кодів [7] (с. 129): найвищої завадостійкості набувають кодові ІКВ-послідовності, в яких кількість різнойменних бінарних символів відрізняється між собою не більше, ніж одним символом.

У табл. 2 наведено характеристику оптимальних кодових ІКВ-послідовностей довжиною $7 \le S_n \le 39$ за спроможності розпізнавання сигналів при відношенні сигнал/шум менше одиниці. Функцію автокореляції обчислюють за множиною покрокових зсувів цієї послідовності за результатом підсумовування усіх елементів +1 і –1, після повного циклу покрокових зсувів. Результати обчислень не змінюються від реверсування порядку чи зміни знаків елементів на протилежні в будь-якому з варіантів кодових ІКВ-послідовностей [7] (с. 124).

Табл. 2. Характеристика оптимальних кодових ІКВ-послідовностей довжиною / Characteristics of optimal code sequences with lengths $7 \le S_n \le 39$

Параметри оптимізованих ІКВ				Функція автокореляції кодових ІКВ-послідовностей			
n	R	S_n	t_2	+1	-1	Δ	Δ/S_n, 100%
4	2	7	1	3	4	-1	14,286
5	2	11	2	5	6	-1	9,0909
6	3	11	2	5	6	-1	9,0909
7	3	15	3	7	8	-1	6,6667
8	4	15	3	7	8	-1	6,6667
9	4	19	4	9	10	-1	5,2631
10	5	19	4	9	10	-1	5,2631
11	5	23	5	11	12	-1	4,3478
12	6	23	5	11	12	-1	4,3478
13	6	27	6	13	14	-1	3,7037
14	7	27	6	13	14	-1	3,7037
15	7	31	7	15	16	-1	3,2258
16	8	31	7	15	16	-1	3,2258
17	8	35	8	17	18	-1	2,8571
18	9	35	8	17	18	-1	2,8571
19	9	39	9	19	20	-1	2,5641
20	10	39	9	19	20	-1	2,5641

З табл. 2 випливає, що оптимізовані ІКВ-послідовності довжиною S елементів, дають змогу виправляти до $(S_n-3)/4$ помилок, а функція автокореляції цих послідовностей за результатом підсумовування елементів +1 і –1 на будь-якому кроці циклічного зсуву для послідовності будь-якої великої апріорі довжини S не перевищує одиниці з точністю до реверсування порядку і зміни знаків кожного з її елементів. Таблиця дає змогу легко визначити числове співвідношення рівня бічних пелюстків і головного піку функції автокореляції за результатом підсумовування усіх елементів +1 і –1 відповідної кодової ІКВ-послідовності. Основна ідея полягає в тому, щоб від вузькосмугового спектру сигналу, що виникає при звичайному потенційному кодуванні, перейти до широкосмугового спектру. Саме це дає змогу значно підвищити завадостійкість даних.

Порівняння ІКВ-послідовностей з кодовими послідовностями Баркера. Для порівняння ІКВ-послідовностей з кодовими послідовностями Баркера скористаємося правилом переходу від ІКВ до коду Баркера [6] (с. 17).

Для кожного числа k_i, $(i = 1,2,\ldots,n)$ ІКВ з параметрами n, R, S_n знайдемо відповідний цьому числу i-й фрагмент кодової послідовності Баркера $(K_1, K_2, \ldots, K_i, \ldots, K_n)$, $K_i = (a_1, a_2, \ldots, a_j, \ldots, a_k)$, $k = k_i$, де $a_1 = +1$, $\{a_j\} = -1$, $j = 2,3,\ldots,k_i$.

Наприклад, за описаним правилом легко перейти від ІКВ (1,1,4,3,2) з параметрами $n=5$, $R=2$ до кодової послідовності Баркера $(+1,+1,+1,-1,-1,-1,+1,-1,-1,+1,-1)$, що складається з п'яти $(n=5)$ послідовно впорядкованих фрагментів $K_1,\ldots,K_5$, де $K_1=(+1)$, $K_2=(+1)$, $K_3=(+1,-1,-1,-1)$, $K_4=(+1,-1,-1)$, $K_5=(+1,-1)$ і має мінімальний рівень бічних пелюстків автокореляційної функції $1/S_n=1/11$.

Відомо, що існують кодові послідовності Баркера тільки з довжинами $N=2,\ 3,\ 4,\ 5,\ 7,\ 11,\ 13$. Цим послідовностям взаємно однозначно відповідають наступні варіанти ІКВ $(k_1,k_2,\ldots,k_n)$ з параметрами n, R, S_n; $n=2,3,4,5,7,11,13$ (табл. 3).

Табл. 3. Відповідність ІКВ-послідовностей кодовим послідовностям Баркера / Compliance of numerical IRBs with Barker code sequences

ІКВ				Код Баркера	
n	R	S_n	$(k_1, k_2, \ldots, k_n)$	N	$(a_1, a_2, \ldots, a_N)$
2	2	2	1,1	2	+1,+1
2	1	3	1,2	3	+1,+1,-1
3	2	4	1,1,2	4	+1,+1,+1,-1
3	2	4	1,2,1	4	+1,+1,-1,+1
4	3	5	1,1,2,1	5	+1,+1,+1,-1,+1
4	2	7	1,1,3,2	7	+1,+1,+1,-1,-1,+1,-1
5	2	11	1,1,4,3,2	11	+1,+1,+1,-1,-1,-1,+1,-1,-1,+1,-1
9	6	13	1,1,1,1,3,1,2,2,1	13	+1,+1,+1,+1,+1,+1,-1,-1,+1,+1,-1,+1,-1,-1,+1

Отже, для кожного з восьми варіантів кодових N-послідовностей Баркера існує відповідна ІКВ-послідовність з параметрами n, R, S_n, яку можна перетворити в послідовність Баркера з мінімальним рівнем бічних пелюстків автокореляційної функції $1/S_n$. Вищенаведені приклади демонструють можливість застосування принципу оптимальних структурних відношень (ОСВ) [5] (с. 146) для оптимізації систем нейромережевого криптографічного захисту й передачі даних.

Обговорення результатів дослідження. Використання квадратурної амплітудної модуляції в системах нейромережевого криптографічного захисту й передачі даних забезпечує кращу продуктивність з точки зору частоти бітових помилок через відсутність IQ-дисбалансу та фазових шумів у змінених формах сигналів. Однак ортогональність піднесучих, окрім важливих переваг, обумовлює недоліки методу OFDM: обмежена спектральна ефективність при використанні широкої смуги частот; неможливість маневру частотою піднесучих для відгородження лаштування від зосереджених за спектром завад. Окрім цього, чутливість до допплерівського зсуву частоти знижує можливості реалізації високошвидкісного зв'язку з рухомими об'єктами. Основною перевагою кодів Баркера і M-кодових послідовностей є добрі автокореляційні властивості, які визначають автокореляційною функцією (АКФ). Проте розрахунок таких фільтрів з необхідними імпульсними характеристиками є складною задачею. Через обмежену кількість кодів Баркера на практиці обирають коди з низьким рівнем бокових пелюсток, які не є кодами Баркера, оскільки не виконується вимога щодо рівня бокових пелюсток $\{|c_j|>1\}$, але при цьому мають кращі показники відношення рівня бокових пелюсток, ніж у кодів Баркера.

Внаслідок порівняння оптимізованих ІКВ-послідовностей з баркероподібними кодами за трьома чинниками – коректувальною здатністю, потужністю методу кодування та складністю процедури декодування, з'ясовано, що за оцінкою коректувальної здатності вони вигідно відрізняються від баркероподібних послідовностей меншим значенням функції автокореляції. Оптимізовані ІКВ-послідовності довжиною S_n елементів, дають змогу виправляти до $(S_n-3)/4$ помилок, а функція автокореляції цих послідовностей за результатом підсумовування елементів +1 і –1 на будь-якому кроці циклічного зсуву для як завгодно великої апріорі оптимізованої ІКВ-послідовності не перевищує одиниці з точністю до реверсування порядку і зміни знаків кожного з її елементів.

Дослідження методів підвищення надійності систем нейромережевого криптографічного захисту й передачі даних за допомогою використанням кодових послідовностей з'ясовано, що завдяки описаним властивостям, ІКВ-коди з інформаційними параметрами n, R, S_n, які відповідають співвідношенню $n=2R$, $S_n=2n$, їх можна виокремити в групу оптимізованих ІКВ-кодів.

Досліджені кодові послідовності об'єднують велику групу завадостійких кодів, пов'язаних із загальною теорією комбінаторних конфігурацій, циклічними групами розширених полів Ґалуа і досконалими комбінаторними конструкціями – "ідеальними кільцевими в'язанками" (ІКВ).

Отже, за результатами виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – розроблено комбінаторні методи оптимізації ІКВ-послідовностей з низьким рівнем функції автокореляції, що дало змогу підвищити надійність криптографічного захисту даних в нейромережевих системах кодування та пересилання даних.

Практична значущість результатів дослідження – підвищення надійності криптографічного захисту даних в нейромережевих системах захисту та кодування даних завдяки використанню оптимізованих ІКВ-послідовностей з низьким рівнем функції автокореляції завдяки їх унікальним властивостям, які здатні виявляти до 50 і виправляти до 25% помилок від числа S_n розрядів оптимізованих ІКВ-послідовностей, причому функція автокореляції цих послідовностей за результатом підсумовування елементів +1 і –1 на будь-якому кроці циклічного зсуву для як завгодно великої апріорі оптимізованої ІКВ-послідовності не перевищує одиниці з точністю до реверсування порядку і зміни знаків кожного з її елементів.

Висновки / Conclusions

Методи комбінаторної оптимізації здатні поліпшити якісні показники систем нейромережевого криптографічного захисту даних шляхом використання оптимальних сигнально-кодових послідовностей, побудованих на підставі ІКВ з оптимізованими параметрами. Такі ІКВ-послідовності характеризуються високою завадостійкістю, малим значенням числового співвідношення рівнів бічних пелюстків і головного піку функції автокореляції, а також широким діапазоном обрання інформаційних параметрів. Це дає змогу вдосконалити шифрування даних в реальному часі, де важливе значення має поліпшення відношення сигнал/шум під час перетворення отриманого приймачем шумоподібного сигналу в потрібний інформаційний сигнал. При цьому найвищої завадостійкості набувають ІКВ-послідовності, в яких кількість різнойменних бінарних символів відрізняється між собою не більше, ніж на один символ. Встановлено, що існує апріорі нескінченно багато оптимальних ІКВ-кодів з функцією автокореляції не більше 1. Широкий спектр оптимальних сигнально-кодових послідовностей фіксованої довжини дають змогу вдосконалити методи нейромережевого криптографічного захисту даних завдяки гнучкому налаштуванню та навчанню системи в розширеному діапазоні функціонування. Використання оптимізованих комбінаторних конфігурацій для поліпшення нейромережевого криптографічного захисту даних розкриває нові перспективи нейромережевого криптографічного шифрування з розширеними функціональними можливостями.

References

[1] Barker's code. Retrieved from: https://uk.wikipedia.org/wiki/. [In Ukrainian].

[2] Kronecker's product. Retrieved from: https://uk.wikipedia.org/wiki/. [In Ukrainian].

[3] Maksymyuk, T., Beshiey, M., Klymash, M., Petrenko, O. & Matsevityi, Y.(2018). Eavesdropping-resilient wireless communication system based on modified OFDM/QAM air interface. Proceedings of the 14-th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Slavske, 1127–1130. https://doi.org/10.1109/TCSET.2018.83363921

[4] M-sequence. Retrieved from: https://uk.wikipedia.org/wiki/. [In Ukrainian].

[5] Riznyk, V. V. (1989). Synthesis of optimal combinatorial systems. Lviv: Vyshcha Shkola. [In Ukrainian].

[6] Riznyk, V. V. (2016). Models of optimum discrete signals on the vector combinatorial configurations. Visnyk NTUU KPI. Seria-Radiotekhnika Radioaparatobuduvannia, (65), 13–25. https://doi.org/10.20535/RADAP.2016.65.13-25

[7] Riznyk, V. V. (2019). Combinatorial optimization of multidimensional systems. Models of multidimensional intelligent systems. Lviv: Vydavnyctvo Lvivskoji Politekhniky. [In Ukrainian].

[8] Tsmots, I., Rabyk, V., Lukashchuk, Yu., Teslyuk, V., & Liubun, Z. (2021). Neural Network Technology for Protecting Cryptographic Data. https://doi.org/10.1109/ELIT53502.2021.9501094

V. V. Riznyk

Lviv Polytechnic National University, Lviv, Ukraine

COMBINATORIAL OPTIMIZATION OF SYSTEMS OF NEURAL NETWORK CRYPTOGRAPHIC DATA PROTECTION

The problem of improving the reliability of cryptographic data protection in neural network systems with flexible configuration is considered. To ensure the possibility of encrypting/decrypting messages it is proposed to use combinatorial optimization methods for the tasks of forming encoded sequences with improved quality indicators for correcting ability, noise immunity, and autocorrelation properties. The basis of combinatorial optimization is the principle of optimal structural relationships, the essence of which is to achieve the maximum diversity of the system under the established restrictions on the number of structural elements and their mutual placement in space-time. It is proposed to use signal-code sequences for neural network data protection, which are characterized by high noise immunity and low level of the autocorrelation function, using various types of optimized code sequences depending on the set of requirements for work under specific conditions, taking into account restrictions on the duration of sending encrypted messages and the presence of noise in communication channels. The system for neural network cryptographic data protection has been developed using encoded signal sequences, where the number of binary characters of different names differs by no more than one character, which minimizes the value of the autocorrelation function of the encoded signal at a fixed bit depth. To ensure high technical and economic indicators of the cryptosystem, it is advisable to equip it with specialized modules of neuro-similar elements of the network with the possibility of training and flexible configuration for cryptographic data encryption. The relationship between the parameters of optimized encoded signal sequences, in which the value of the autocorrelation function is minimized, and the maximum achievable number of detected and corrected errors has been established. It is proposed to use unique properties of combinatorial configurations with a non-uniform distribution of structural elements, which are distinguished by the fact that the set of all ring sums of their numerical values occurs a fixed number of times. A comparative analysis of cryptographic methods for data protection and transfer using non-standard codes built on the so-called IRB code sequences together with other signal-code constructions was carried out.

Keywords: principle of optimal structural relationships; ideal ring bundle (IRB); IRB code sequence; Barker code sequence; autocorrelation function.

Інформація про автора:

Різник Володимир Васильович, д-р техн. наук, професор, кафедра автоматизованих систем управління.
Email: volodymyr.v.riznyk@lpnu.ua; https://orcid.org/0000-0002-3880-4595

Цитування за ДСТУ: Різник В. В. Комбінаторна оптимізація систем нейромережевого криптографічного захисту даних. *Український журнал інформаційних технологій.* 2022, т. 4, № 2. С. 56–60.

Citation APA: Riznyk, V. V. (2022). Combinatorial optimization of systems of neural network cryptographic data protection. *Ukrainian Journal of Information Technology, 4*(2), 56–60. https://doi.org/10.23939/ujit2022.02.056