УДК 621.391
DOI: 10.15587/1729-4061.2021.234674

Розробка методів синтезу дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно-комунікаційних системах

І. Д. Горбенко, О. А. Замула

До інформаційно-комунікаційних систем (*ІКС*) *пред'являються все більш жорсткі вимоги щодо забезпечення достовірності і швидкості передачі інформації, завадозахищеності, інформаційної безпеки. У роботі наведено*: *методи синтезу дискретних складних криптографічних сигналів, основою для побудови яких є випадкові* (*псевдовипадкові*) *процеси*; *методи синтезу характеристичних дискретних складних сигналів, побудова яких базується на використанні характеру мультиплікативної групи кінцевого поля*; *результати досліджень властивостей зазначених систем сигналів. Показано, що отримані методи забезпечують більш високу продуктивність синтезу ніж відомі методи і дають можливість алгоритмізувати процеси синтезу для побудови програмно-апаратних пристроїв формування таких сигналів. Виграш у часі синтезу нелінійних сигналів в кінцевих полях із застосуванням розробленого методу, в порівнянні з відомим методом, для періоду* 9972 *елементів становить* 1039,6 *рази. Запропонований метод синтезу всієї системи таких сигналів, на основі операції децимації, перевершує за швидкодією відомий метод різнисних множин. Так, для періоду сигналу* 2380 *елементів виграш у часі становить понад* 28 *разів. Показано також, що застосування таких систем складних сигналів дозволить поліпшити показники ефективності сучасних ІКС. Так, імітостійкість системи, при застосуванні складних дискретних криптографічних сигналів з періодом сигналу* 1023 *елемента, на чотири порядки вище, ніж при застосуванні лінійних класів сигналів* (*наприклад, М-послідовностей*). *Для періоду сигналу* 1023 *елементи виграш* (*з погляду структурної скритності*) *при використанні отриманих у роботі систем сигналів, порівняно з сигналами лінійної форми* (*М-послідовностями*), *при періоді* 8192, *становить понад* 300 *разів.*

Ключові слова: *завадостійкість прийому, завадозахищеність, скритність, інформаційна безпека, дискретні послідовності, синтез сигналів*.

1. Вступ

Світові тенденції посилення загроз інформаційної та кібербезпеки обумовлюють необхідність розробки та впровадження нових моделей, методів і технологій управління телекомунікаційними мережами, інформаційною безпекою, послугами і якістю обслуговування. З’являється необхідність розробки методів інформаційного обміну, методів синтезу нових класів складних дискретних сигналів-переносників даних з необхідними ансамблевими, кореляційними і структурними властивостями.

Серед основних напрямків поліпшення показників інформаційної безпеки, завадозахищеності і скритності ІКС можна виділити напрямки, які пов'язані із застосуванням каналів з великою частотною надмірністю, значною просторовою, структурною, енергетичною та часовою скритністю. Для забезпечення частотної надмірності на фізичному рівні широке застосування отримали дискретні сигнали, у яких маніпульовані параметри змінюються через строго фіксовані інтервали часу. Закон зміни зазначених параметрів задається дискретними послідовностями, які повністю визначають властивості дискретних сигналів.

Зусилля дослідників спрямовані на пошук ансамблів сигналів, характеристики яких наближуються до границі «щільної упаковки» [1]. Саме такі сигнали мають ідеальну періодичну функцію автокореляції (ПФАК) і періодичну функцію взаємної кореляції (ПФВК), та володіють значним об’ємом.

Широко розповсюдженим критерієм подібного наближення є мінімаксний критерій, який орієнтується на синтез ансамблю за мінімізацією максимальних значень бокових піків на множині всіх небажаних кореляцій. У [1, 2] наведено границі для середньоквадратичних і максимальних (пікових) значень авто- і взаємно-кореляційних функцій. Зокрема, принципово досяжні значення максимальних бічних піків періодичної функції автокореляції R^a_{max} (межі «щільної упаковки») для заданого періоду послідовності N визначаються з співвідношення:

$$R^a_{\max} \geq \begin{cases} 0, \text{ якщо } N \equiv 0 \pmod 4; \\ 1, \text{ якщо } N \equiv 1 \pmod 4; \\ 2, \text{ якщо } N \equiv 2 \pmod 4; \\ -1, \text{ якщо } N \equiv 3 \pmod 4. \end{cases}$$

Наведені граничні значення встановлюють критерії синтезу множини послідовностей (сигнатур). Ансамблі, зі значеннями, що відповідають зазначеній границі, є оптимальними, і називаються мінімаксними. Для ідеального гіпотетичного ансамблю $R_{\max}$ дорівнює нулю, а для будь-якого реального ансамблю мінімальне значення кореляційної функції може служити адекватною мірою його близькості до ідеального.

Застосовувані в ІКС сигнали-фізичні переносники даних, володіють низькою структурною скритністю та незадовільними ансамблевими характеристиками. Зазначене не дозволяє забезпечити необхідні (особливо для об’єктів критичної інфраструктури) показники інформаційної безпеки та завадозахищеності передачі даних в ІКС. Саме тому, поліпшення показників завадозахищеності та інформаційної безпеки ІКС на основі розробки теоретичних основ, методів та засобів синтезу нових класів оптимальних складних сигналів з необхідними ансамблевими, кореляційними і структурними властивостями, є актуальним дослідженням.

2. Аналіз літературних даних та постановка проблеми

В дослідженні [1] наведено загальний опис і аналіз властивостей різних класів сигналів, введені показники ефективності функціонування багатокорис-

тувачевих систем зв’язку. Зазначене дає можливість комплексно підходити до вирішення питань застосування тих чи інших систем сигналів для вирішення задач забезпечення відповідних показників ефективності функціонування таких систем. Тим не менш у цій роботі не визначено: яким чином можна вирішувати проблеми забезпечення необхідних показників інформаційної безпеки, скритності функціонування систем. Причиною неможливості забезпечити необхідні (особливо для ІКС, які функціонують на об’єктах критичної інфраструктури) зазначені показники є класи широкосмугових сигналів, які надані у даній роботі. Розвиток поглядів на забезпечення необхідних показників функціонування систем передачі даних може бути знайдено у роботі [2]. У роботі наведено теоретичні основи синтезу великої кількості систем сигналів, у тому числі характеристичних сигналів. Це дає можливість, при проектування систем передачі даних, обґрунтовано приймати рішення щодо застосування тих чи інших класів сигналів як фізичних носіїв інформації Не дивлячись на очевидно правильне рішення щодо застосування нелінійних класів сигналів, у цьому дослідженні не наведено опис методів, які б дозволили алгоритмізувати процеси синтезу систем сигналів для створення сучасних програмно-апаратних комплексів синтезу, формування і обробки сигналів. У роботі [3] наведено принципи побудови телекомунікаційних систем и вибору сигналів, що можуть бути застосовані в них. Це дає можливість приймати проектні рішення щодо створення таких систем, оцінювати показники функціонування таких систем, насамперед тих, які визначаються властивостями застосовуваних у системах сигналів. При цьому відсутні відомості про можливість практичної реалізації методів синтезу систем сигналів. Дослідження [4] присвячено опису суто теоретичних питань оптимального прийому і обробки сигналів. Використовуваний у роботі підхід орієнтовано на застосуванні в інформаційно-комунікаційних сигналів, які засновано лише на лінійних законах побудови. Це, у свою чергу, не дозволяє вирішувати проблеми, які притаманні сучасним системам, для яких критичними є забезпечення завадозахищеності і інформаційної безпеки. В дослідженні [5] наведено принципи побудови сучасних бездротових цифрових систем зв'язку, практичні рекомендації щодо застосування видів сигналів (OFDM), методів кодування, синхронізації, передачі даних. Показано, що при вирішенні проблем забезпечення інформаційної і частотної ефективності, завадостійкості прийому сигналів, швидкості передачі даних можуть знайти широке впровадження методи інформаційного обміну і певні класи сигналів. При цьому не наведено рішень щодо вирішення проблем забезпечення інформаційної безпеки (криптографічної стійкості, імітозахищеності) на фізичному рівні телекомунікаційної мережі. У роботі [6] наведено досить глибокий аналіз щодо класифікації і методів синтезу великої кількості сигналів. Однак відсутні конкретні рішення щодо можливої практичної реалізації цих методів і існуючих обмежень при застосуванні тих чи інших сигналів для безлічі додатків комунікаційних систем. Вільною від зазначених обмежень може бути робота [7]. В ній показана можливість вирішення проблем забезпечення інформаційної безпеки, завадозахищеності на рівні джерела складних сигналів, Показано, що в основу побудови сигналів, повинні бути покладені нелінійні правила, а обмін даними в системі повинен бути засно-

вано на динамічній зміні відповідності: повідомлення - складний сигнал. Однак у цій роботі не наведено практичні методи побудови таких сигналів. У роботі [8] наведено підходи до визначення вимог щодо властивостей сигналів, застосування яких в інформаційних системах дозволяло б забезпечувати необхідні показники захисту від впливів з боку зловмисників. Тим не менш, у даній роботі відсутні детальний опис властивостей сигналів, які пропонуються, і не даються оцінки показникам ефективності функціонування систем. У роботі [9] наведено опис і характеристики стандарту блокового симетричного шифрування. Алгоритм шифрування, який визначено цим стандартом застосовується при реалізації запропонованого у роботі методу синтезу складних нелінійних дискретних криптографічних сигналів як джерело псевдовипадкового процесу. У роботі [10] наведено опис вимог до вихідних послідовностей алгоритмів криптографічного перетворення інформації. Саме ці вимоги використовуються для формулюванні вимог при синтезі систем нелінійних сигналів. При цьому у даній роботі не наведено методів щодо синтезу сигналів як фізичного переносника даних у комунікаційних системах. Один з класів сигналів, що пропонується у статті, повинен мати властивості, які притаманні випадковим послідовностям символів. Саме робота [11] визначає критерії (вимоги) до таких послідовностей. При синтезі досліджуваних у роботі сигналів, необхідно застосовувати алгоритми блокового шифрування даних, а також враховувати вимоги щодо властивостей випадкових послідовностей символів. Правила і вимоги до таких послідовностей (так званих випадкових підстановок) наведено у роботі [12]. Тим не менш, у цій роботі не наведено принципи, обмеження, практичні методи щодо синтезу систем сигналів.

Систематизація результатів наведених досліджень дозволяє вважати, що існуючі підходи до застосування сигналів з лінійним законом формування не дозволяють забезпечити необхідні показники завадозахищеності і інформаційної безпеки. Дана проблема може бути вирішена шляхом створення теоретичних основ, практичних методів і програмно-технічних засобів синтезу, формування, обробки систем нелінійних дискретних складних сигналів з необхідними властивостями.

3. Мета і задачі досліджень

Метою роботи є синтез, на основі розроблених методів, дискретних складних сигналів з поліпшеними ансамблевими, кореляційними, структурними властивостями, що дасть можливість покращити показники ефективності функціонування ІКС, а саме, продуктивності синтезу сигналів, інформаційної безпеки, завадозахищеності (завадостійкості прийому сигналів і скритності функціонування) системи.

Для досягнення мети були поставлені наступні задачі:

– визначити математичну залежність елементів та індексів елементів простого та розширеного полів Галуа для отримання методу синтезу складних сигналів;

– розробити моделі структури складних нелінійних дискретних сигналів у кінцевих полях та дослідити структурну скритність, кореляційні і ансамблеві

властивості нелінійних дискретних характеристичних сигналів для оцінки показників завадозахищеності та інформаційної безпеки ІКС;

– визначити умови щодо функцій кореляції сигналів, які задані сукупністю систем нелінійних параметричних нерівностей, і які застосовуються для розробки методу синтезу дискретних складних криптографічних сигналів;

– дослідити властивості синтезованих класів нелінійних дискретних складних криптографічних сигналів для використання в ІКС як фізичного переносника інформації.

4. Матеріали і методи дослідження

Суть гіпотези дослідження полягає у наступному. Чи можливо розробити методи синтезу систем складних дискретних сигналів з необхідними (визначеними) кореляційними, ансамблевими, структурними властивостями, застосування яких у сучасних ІКС дозволить поліпшити показники ефективності таких ІКС.

Припущення щодо даної гіпотези полягають у наступному:

– методи синтезу сигналів повинні бути засновані на нелінійних правилах;

– повинна існувати можливість синтезувати сигнали для будь-якого значення періоду сигналу (натуральний ряд чисел);

– сигнали повинні володіти високою структурною скритністю (для визначення правила його синтезу необхідно знати не менш половини символів сигналу);

– повинна існувати можливість програмно-апаратної реалізації методів синтезу сигналів.

У якості однієї з форм наукових досліджень застосовано моделювання. Експериментальна складова полягає у застосуванні створеного програмного комплексу, який реалізує функції синтезу сигналів, у відповідності із запропонованими у роботі методами (надані як послідовність дій, що описані математично, і які дозволяють досягти певного результату), і дослідження властивостей отриманих у результаті синтезу сигналів (надалі - Комплекс). До переліку основних варіантів використання розробленого Комплексу можна віднести:

– формування дискретних складних сигналів (КС);

– розрахунок функцій кореляції в періодичному і аперіодичному режимах роботи;

– розрахунок статистичних характеристик (математичного очікування, дисперсії, середньо квадратичного відхилення, коефіцієнту ексцесу) функцій кореляції сигналів в періодичному і аперіодичному режимах;

– розрахунки найбільшого і найменшого значень бокових піків функцій кореляції, їх кількості та порівняння їх значень з оптимальною границею для відповідної функцій кореляції;

– синтез систем дискретних складних сигналів із застосуванням процесу децимації;

– знаходження параметрів, які застосовуються при синтезі сигналів (первісного елементу поля, функцій Ейлера, взаємно простих чисел з деяким заданим тощо).

Наукове дослідження на теоретичному рівні здійснювалося шляхом:

– узагальнення положень теорії груп, полів, кілець з метою застосування цього математичного апарату для створення методів синтезу систем складних сигналів у кінцевих полях, підходів теорії криптографічного захисту інформації відносно побудови блокових симетричних шифрів при розробці методів синтезу складних дискретних криптографічних сигналів;

– порівняння відомих положень теорії систем сигналів з отриманими у ході досліджень результатами, стосовно синтезу систем сигналів та властивостей сигналів;

– математичної формалізації відображення структури об'єкта для визначення кроків реалізації розроблених методів синтезу сигналів, яка дає можливість відтворити ці методи та отримати досліджувані сигнали.

5. Результати дослідження методів синтезу і властивостей нелінійних дискретних складних сигналів

5. 1. Визначення математичної залежності елементів та індексів елементів простого та розширеного полів Галуа для отримання методу синтезу сигналів

До дискретних сигналів пред'являється ряд вимог: хороші кореляційні властивості, рівномірний спектр, допустимий рівень максимальних піків авто – і взаємно-кореляційних функцій, великий об'єм, існування для великої кількості значень тривалостей. Розглянуті N – позиційні коди (характеристичні дискретні сигнали, – далі ХДС) з дворівневою періодичною функцією автокореляції (ПФАК), побудова яких базується на використанні характеру ψ мультиплікативної групи [2] поля $GF(p^n)$ для $N = 4x + 2 = p^n - 1$ і $N = 4x = p^n - 1$.

В [2] показано, що об'єм системи сигналів (M) дорівнює числу класів неінверсно-ізоморфних коефіцієнтів, які можуть бути отримані розкладанням мультиплікативної групи на суміжні класи по класу автоморфних коефіцієнтів, і визначається як $M=\Psi(N)/2$, де $\Psi(N)$ – функція Ейлера. Відомо так само [2], що значення максимальних бокових піків періодичної функції автокореляції ХДС приймають значення $R_\mu=\{-2, 2\}$, або $R_\mu=\{0, -4\}$. Аналіз показує, що ХДС існують для значно більших значень тривалостей ніж M-послідовності [1, 2]. У той же час ХДС, як і M-послідовності є оптимальними за ПФАК і близькі до оптимальних за аперіодичною функцією автокореляції (АФАК).

Метод формування ХДС [2] тривалістю N, який орієнтується на складені в теорії чисел таблиці елементів та індексів елементів поля Галуа, вже при $n\geq 1$ і $N\geq 100$ стає важко реалізованим. Зазначене пояснюється насамперед тим, що при гомоморфності відображення елементів поля a_i в безліч символів дискретної послідовності при використанні комплексно-значної функції $\psi(a_i)=W_i=-e^{j\pi Ui}$, необхідно вирішувати в середньому $N/2$ порівнянь виду

$$a_i \equiv \Theta_j^{U_i} \left(\mathrm{mod\ P}\right),\ \ i = \overline{0, P-1}, \qquad (1)$$

де $U_i = \overline{0, P-2}$ – індекс елемента поля $GF(P)$;

$\Theta_j^{U_i}$ – j-й первісний елемент поля;

P – характеристика поля Галуа.

Саме, для вирішення порівнянь виду (1) використовуються попередньо розраховані таблиці елементів та індексів елементів полів Галуа. Обчислювальна складність такого методу формування ХДС визначається зі співвідношення:

$$t_\Sigma = N \cdot \left(t_{\text{м}} + t_{\text{дод}} + 3 \cdot t_{\text{з}} + \left(N - 2 \right) \cdot t_{\text{зч}} + \left(N + 1 \right) \cdot t_{\text{пор}} \right), \tag{2}$$

де $t_{\text{м}}$, $t_{\text{дод}}$, $t_{\text{з}}$, $t_{\text{зч}}$, $t_{\text{пор}}$ – час виконання операцій множення, додавання, запису, зчитування і порівняння відповідно.

Аналіз виразу (2) показує, що основні часові витрати при побудові ХДС пов'язані з членами $N\left(N - 2 \right) \cdot t_{\text{зч}}$ та $N\left(N + 1 \right) \cdot t_{\text{пор}}$.

В ході досліджень отримано вдосконалений метод синтез ХДС, який володіє значно меншою обчислювальною складністю в порівнянні з методами, розглянутими в [2]. Синтез ХДС базується на використанні найменшого за значенням первісного елемента поля $GF(P)$ і задається твердженням 1.

Твердження 1. Нехай характер мультиплікативної групи поля фіксується функцією

$$\psi\left(a_i \right) = e^{j\pi U_i}. \tag{3}$$

Тоді, математична залежність елементів та індексів елементів простого поля Галуа може бути описана такими кроками.

Формується масив елементів – чисел A_i, $i = \overline{0, P-2}$ поля $GF(P)$:

$$A(i) = \Theta_j^i \left(\bmod P \right). \tag{4}$$

Формується група чисел поля $GF(P)$, що зсунена за значеннями на одиницю, відповідно до правила:

$$H\left(i \right) = A\left(i \right) + 1, \text{ якщо } \Theta_j^i + 1 = 0\left(\bmod P \right);$$

$$H\left(i \right) = 1, \text{ якщо } \Theta_j^i + 1 \equiv 0\left(\bmod P \right). \tag{5}$$

Формується масив індексів $X(i)$, $i = \overline{0, P-2}$, значеннями якого є відповідні елементу поля індекси i+1, впорядковані по вмісту з адресом:

$$A(i) : X\left(i \right) = X\left[A(i) \right]. \tag{6}$$

Будується масив індексів $J(i)$, значеннями якого є індекси масиву $X(i)$, вибрані за адресом $H(i)$; $J(i)=X[H(i)]$, $i=\overline{0,\,P-2}$.

Обчислюється характер елементів поля за правилом [2]:

$$\psi\left(a_i\right)=\psi\left[J\left(i\right)\right]=\begin{cases}1, \text{ якщо } J\left(i\right)\equiv 0\left(\mathrm{mod}\ 2\right);\\ -1, \text{ якщо } J\left(i\right)\equiv 0\left(\mathrm{mod}\ 2\right).\end{cases} \tag{7}$$

Нехай $\varphi(a_i)$, $i=\overline{1,\,p^n-1}$ є поле Галуа $GF(p^n)$ ступеня n розширення і елементами-поліномами, ступінь яких не перевищує n, і обчислюються над полем, $GF(p^n)$, $\Phi_k(x)$ та θ_j – відповідно k-й первісний примітивний поліном та j-й первісний елемент поля. Функція характерів гомоморфного відображення елементів поля $GF(p^n)$ на полі $GF(2)$, зафіксована функцією $\psi(a_i)= e^{j\pi ui}$, причому елемент-поліном поля a_i визначається з рішення порівняння $a_i\equiv\theta_j^{u_i}\left(\mathrm{mod}\,\Phi_k\left(x\right),P\right)$, а u_i є безліч чисел-індексів, упорядкованих за зростанням.

Встановимо аналітичну залежність елементів та індексів елементів для випадку розширеного поля Галуа.

1) Формується масив зсунутих за значенням індексів $u_i'=u_i+1$, $i=\overline{0,\,p^n-2}$, упорядкованих за зростанням, і масив елементів-поліномів a_i поля $GF(p^n)$:

$$A\left(i\right)=\theta_j^i\left(\mathrm{mod}\,\Phi_k\left(x\right),P\right). \tag{8}$$

2) Формується масив $H(i)$ елементів-поліномів поля $GF(p^n)$, зсунутий за значеннями на одиницю відносно значень масиву $A(i)$:

$$H\left(i\right)=A\left(i\right)+1, \text{ якщо } \theta_j^i+1\neq 0\left(\mathrm{mod}\,\Phi_k\left(x\right),P\right);$$

$$H\left(i\right)=1, \text{ якщо } \theta_j^i+1\equiv 0\left(\mathrm{mod}\,\Phi_k\left(x\right),P\right). \tag{9}$$

3) Масив індексів u_i записується в масив $X(i)$ за адресами, визначеними значеннями коефіцієнтів при поліномі $H(i)$ в P-ічній системі числення.

4) Формується масив індексів $J(i)$, $i=\overline{1,\,p^n-2}$, значеннями якого є індекси u_i, які зчитані з масиву за адресами, які задані значеннями коефіцієнтів при елементах-поліномах $H(i)$ в P-ічній системі числення.

5) Обчислюється для всіх значень масиву індексів $J(i)$ двозначний характер

$$\psi\left(a_i\right)=\psi\left(\theta_j^i+1\right)=-\psi\left(J\left(i\right)\right)=$$
$$=\begin{cases}1, \text{ якщо } J=0\left(\mathrm{mod}\,2\right);\\ -1, \text{ якщо } J\neq 0\left(\mathrm{mod}\,2\right).\end{cases} \tag{10}$$

У якості прикладу у табл. 1 наведено ХДС з числом елементів 256. Зазначений сигнал отримано шляхом реалізації кроків (4)–(7) методу синтезу сигналів, що розроблено. В таблиці також наведені значення максимальних бокових піків періодичної функції автокореляції (ПФАК) для цього сигналу.

Таблиця 1

ХДС з числом елементів 256 зі значеннями бокових піків ПФАК

Характеристичні сигнали	ПФАК
[1, 1, 1, 1, –1, 1, 1, –1, –1, –1, –1, –1, –1, 1, –1, 1, 1, –1, 1, 1, 1, –1, 1, –1, 1, 1, –1, 1, –1, –1, 1, –1, –1, 1, 1, 1, 1, 1, 1, 1, –1, 1, 1, –1, –1, 1, –1, –1, –1, 1, 1, 1, 1, 1, –1, –1, –1, –1, –1, –1, 1, 1, –1, 1, 1, –1, 1, –1, 1, 1, 1, 1, –1, 1, –1, 1, 1, 1, 1, –1, –1, –1, –1, –1, 1, –1, –1, 1, 1, –1, –1, –1, 1, 1, 1, –1, –1, 1, –1, –1, –1, 1, 1, –1, –1, 1, 1, 1, –1, 1, 1, 1, –1, 1, –1, –1, 1, 1, –1, 1, 1, –1, 1, 1, 1, –1, –1, 1, –1, –1, 1, –1, –1, 1, 1, –1, –1, 1, 1, –1, –1, –1, 1, –1, 1, –1, 1, –1, –1, –1, 1, 1, –1, 1, –1, 1, –1, –1, 1, –1, –1, –1, –1, –1, 1, –1, 1, 1, 1, 1, 1, –1, –1, –1, 1, 1, –1, 1, –1, 1, –1, –1, 1, –1, 1, 1, –1, 1, –1, –1, –1, 1, 1, –1, –1, 1, –1, –1, –1, 1, 1, 1, –1, –1, –1, –1, 1, 1, 1, 1, 1, –1, 1, 1, 1, –1, –1, –1, 1, 1, 1, 1, –1, 1, –1, 1, –1, –1, 1, 1, 1, –1, 1, –1, 1]	[256, 0, 0, 0, 0, 0, –4, 0, 0, 0, 0, 0, –4, 0, 0, 0, –4, 0, 0, 0, –4, 0, –4, 0, 0, 0, –4, 0, 0, 0, –4, 0, –4, 0, –4, 0, –4, 0, –4, 0, –4, 0, –4, 0, –4, 0, –4, 0, 0, 0, –4, 0, –4, 0, 0, 0, 0, 0, 0, 0, 0, –4, 0, 0, 0, –4, 0, –4, 0, –4, 0, 0, 0, 0, 0, –4, 0, –4, 0, –4, 0, 0, 0, –4, 0, 0, 0, –4, 0, –4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, –4, 0, 0, 0, 0, 0, –4, 0, –4, 0, –4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, –4, 0, –4, 0, –4, 0, 0, 0, 0, 0, –4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, –4, 0, –4, 0, 0, 0, –4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, –4, 0, 0, 0, –4, 0, –4, 0, –4, 0, 0, 0, 0, 0, –4, 0, 0, 0, 0, 0, 0, 0, –4, 0, 0, 0, –4, 0, 0, 0, 0, 0, 0, 0, –4, 0, –4, 0, 0, 0, –4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, –4, 0, –4, 0, 0, 0, –4, 0, –4, 0, –4, 0, 0, 0, 0, 0, –4, 0, –4, 0, –4, 0, –4, 0, –4, 0, –4, 0, 0, 0, –4, 0, 0, 0, –4, 0, –4, 0, 0, 0, –4, 0, 0, 0, –4, 0, 0, 0, 0, 0, 0, –4, 0, 0, 0, 0, 0, 0, 256]

Аналіз даних табл. 1 підтверджує, що саме такими значеннями бокових піків ПФАК володіє даний клас сигналів [2]. Багаточисельні розрахунки, які отримані із застосуванням комп'ютерного моделювання виразів (4)-(7) для сигналів тривалістю від 16 до 4000 елементів показали, що саме зазначені кроки визначають метод синтезу нелінійних дискретних складних сигналів у кінцевих полях.

Обчислювальна складність методу синтезу сигналів (час t_c побудови) ХДС, як випливає з твердження 1, може бути визначена з виразу:

$$\begin{aligned} \mathrm{t}_c &= N \cdot \left(t_{\text{м}} + t_{\text{дод}} + t_{\text{пор}} + 4 \cdot t_{\text{зч}} + t_{\text{з}} \right) = \\ &= N \cdot \left(t_{\text{м}} + t_{\text{дод}} + t_{\text{пор}} + 5 \cdot t_{\text{з}} \right). \end{aligned} \tag{11}$$

У виразі (11) враховано, що час, необхідний для виконання операцій запису $t_{\text{з}}$ і зчитування $t_{\text{зч}}$ рівні. Аналіз (11) показує, що час побудови ХДС із застосуванням запропонованого методу лінійно залежить від періоду послідовності, що формується, тоді як для відомого методу (вираз (2)) залежність квадратична.

Виграш у часі синтезу ХДС із застосуванням розроблених методів в порівнянні з відомим методом становить: для періоду N=256, складає 25,5 рази; для періоду N=9972–1039 рази.

Авторами отримано метод побудови характеристичних сигналів, який володіє меншою обчислювальною складністю у порівнянні з методом, що засно-

вано на використанні різницевих множин [2]. Зазначений метод побудови системи ізоморфізмів ХДС задається наступним твердженням.

Твердження 2. Якщо послідовність $\{W_i\}$, $i=\overline{1,N}$, яка є одним з ізоморфізмів ХДС з числом елементів (періодом) N піддати операції децимації з коефіцієнтом децимації C, де C – число, що є взаємно простим з N ($C \in \phi(N)$), то результуюча послідовність $\{v_i\}$ є ізоморфізмом відносно послідовності $\{w_i\}$.

Процедура децимації означає вибір кожного C-го символу коду і запис отриманих таким чином символів, так що

$$v_i = \left(w_i + C\right) \bmod N. \tag{13}$$

Для доказу цього твердження досить показати, що характеристичний код $\left\{w_i\right\}$, побудований на основі різнисних множин, з точністю до циклічного зсуву (автоморфізму) є послідовністю $\{v_i\}$.

Приклад 1. Нехай Θ=2, N=10. Ізоморфізм ХДС для даних параметрів має вигляд: $w_i = \left\{-1,1,1,1,-1,1,-1,-1,1,-1\right\}$, а неінверсно-ізоморфні коефіцієнти мають значення: T={1,3,7,9}. Побудовані з використанням методу різнисних множин (у відповідності до зазначених коефіцієнтів T) характеристичні коди, мають вигляд

$$w^1_{t=1} = \left\{-1,1,1,1,-1,1,-1,-1,1,-1\right\},$$

$$w^2_{t=3} = \left\{-1,-1,-1,1,1,1,1,-1,-1,1\right\},$$

$$w^3_{t=7} = \left\{-1,1,-1,-1,1,1,1,1,-1,-1\right\},$$

$$w^4_{t=9} = \left\{-1,-1,1,-1,-1,1,-1,1,1,1\right\}.$$

Неінверсні та інверсні ізоморфізми характеристичного коду, які побудовані на основі використання методу децимації, мають вигляд

$$v^1_{c=1} = \left\{1,1,1,-1,1,-1,-1,1,-1,-1\right\},$$

$$v^2_{c=3} = \left\{1,-1,-1,1,1,1,1,-1,-1,-1\right\},$$

$$v^3_{c=7} = \left\{-1,-1,1,1,1,1,-1,-1,1,-1\right\},$$

$$v^4_{c=9} = \left\{-1,1,-1,-1,1,-1,1,1,1,-1\right\}.$$

Для формування ізоморфізму характеристичного коду необхідно реалізувати (відповідно до (13)) N операцій вибірки елементів за відповідним коефіцієнтом децимації та N операцій додавання. Час виконання даних операцій позначимо відповідно $t_{виб}$ на і $t_{дод}$ відповідно. Тоді обчислювальна складність методу децимації, може бути оцінена за допомогою виразу:

$$T_{дец} = N\left(t_{дод} + t_{виб}\right). \tag{14}$$

Аналіз операцій, що виконуються при реалізації методу різнисних множин показує, що обчислювальна складність останнього $T_{різн.мн.}$ визначається із співвідношення:

$$T_{різн.мн.} = N\left(2t_{зч} + t_{пор} + 0,5t_{множ}\right), \tag{15}$$

де $t_{зн}$, $t_{пор}$, $t_{множ}$ – час виконання операцій зчитування, порівняння, множення відповідно.

Результати комп'ютерного моделювання і розрахунки, які проведені із застосуванням (14), (15), показують, що запропонований метод істотно перевершує за швидкодією відомий методу різнисних множин. Так, для періоду сигналу 2380 елементів виграш у часі становить понад 28 разів.

5. 2. Розробка моделі структури складних нелінійних дискретних сигналів у кінцевих полях та дослідження властивостей сигналів

Відомо, що ймовірність нав'язування супротивником хибних повідомлень (сигналів) визначається, у тому числі, ансамблевими властивостями використовуваних сигналів (об'єм системи, спектр значень періоду сигналів, для яких можуть бути синтезовані сигнали).

У табл. 2 наведено узагальнені дані щодо кількості значень довжин сигналів і об'єму системи сигналів для M-послідовностей і характеристичних дискретних сигналів.

Таблиця 2

Ансамблеві властивості систем сигналів

ΔL	Число значень N		Об'єм системи	
	ХДС	M-послідовності	ХДС	М-послідовності
$0–10^2$	30	4	456	8
$0–10^3$	186	9	29291	79
$0–10^4$	1269	11	2152943	554

Аналіз наведених аналітичних співвідношень, даних табл. 2, свідчить про те, що ХДС є кращими в порівнянні з широко використовуваними M-послідовностями, послідовностями Лежандра та інших.

Відомо, що скритність функціонування ІКС у значній мірі залежить від складності визначення станцією протидії закону модуляції дискретного сигналу (структурною скритністю використовуваної системи сигналів). Виконаємо оцінку структурної скритності нелінійних дискретних характеристичних сигналів. Для цього, сформулюємо і доведемо твердження, що визначають зв'язки елементів кінцевого поля.

Твердження 3. Нехай $a_1, a_2, \ldots, a_{(P-1)/2}$ – елементи поля $GF(p^n)$, тоді елементи поля $a_{(P-1)/2+1}, a_{(P-1)/2+2}, \ldots, a_{P-1}$ залежать від $(P-1)/2$ перших елементів і визначаються з виразу:

$$a_{(P-1)/2+i} = P - a_i, \tag{16}$$

$$i = \overline{1, (P-1)/2}.$$

Проілюструємо на прикладі можливість побудови $((P-1)/2+i)$ - елементів поля за умови, що відомі перші $(P-1)/2$ елементи.

Нехай характеристика поля $P=13$, первісний елемент поля $\Theta=2$.

Запишемо елементи даного поля:

$$a_1 = 2^0 \bmod 13 = 1;\ \ a_2 = 2^1 \bmod 13 = 2;$$

$$a_3 = 2^2 \bmod 13 = 4;\ \ a_4 = 2^3 \bmod 13 = 8;$$

$$a_5 = 2^4 \bmod 13 = 3;\ \ a_6 = 2^5 \bmod 13 = 6;$$

$$a_7 = 2^6 \bmod 13 = 12;\ \ a_8 = 2^7 \bmod 13 = 11;$$

$$a_9 = 2^8 \bmod 13 = 9;\ \ a_{10} = 2^9 \bmod 13 = 5;$$

$$a_{11} = 2^{10} \bmod 13 = 10;\ \ a_{12} = 2^{11} \bmod 13 = 7. \tag{17}$$

Скористаємося виразом (16) для отримання $((P-1)/2+i)$ елементів поля $\left(i = \overline{1, (P-1)}\right)$:

$$a_7 = a_{(P-1)/2+1} = P - a_1 = 12;\ \ a_8 = a_{(P-1)/2+2} = P - a_2 = 11;$$

$$a_9 = a_{(P-1)/2+3} = P - a_3 = 9;\ \ a_{10} = a_{(P-1)/2+4} = P - a_4 = 5;$$

$$a_{11} = a_{(P-1)/2+5} = P - a_5 = 10;\ \ a_{12} = a_{(P-1)/2+6} = P - a_6 = 7. \tag{18}$$

Порівняння відповідних елементів поля, наведених в (17) з елементами поля (18) показує, що ці елементи є ідентичними. У зв'язку з зазначеною властивістю поля Галуа залежними виявляються, очевидно, і характери елементів поля або символи ХДС, що побудовані у полі. Ця залежність визначається твердженням 4.

Твердження 4. Нехай характер елементів $\psi(a_i)$ поля (символи ХДС в полі $GF(p^n)$ визначаються зі співвідношення

$$W_i = \psi\left(a_i\right) = \exp \le \left(j\pi u_i\right), \tag{19}$$

а індекси елементів поля U_i знаходять з рішення порівняння

$$a_i = \Theta_l^i + 1 = \Theta_l^{U_i} \left(\mathrm{mod}\ P\right).$$

Тоді характери елементів поля $\left(P-1\right)/2+1+i$ $\left(i=\overline{1,\left(P-1\right)/2-1}\right)$ (символи послідовності) залежать від характерів $\left(\left(P-1\right)/2-i\right)$ перших елементів поля, причому

$$W_{P-i} = \left(-1\right)^i W_{i+1}. \tag{20}$$

Проілюструємо справедливість твердження 4 на прикладі.

Нехай характеристика поля $GF(p^n)$ є P=13, а первісний елемент поля Θ=2. Ізоморфізм ХДС в даному полі: $W = \left\{-11-111-1111-1-1-1\right\}$.

Встановимо залежність характерів (символів ХДС) у полі GF(13). При i=1: W_2=–W_2; i=2: W_{11}=–W_3; i=3: W_{10}=–W_4; i=4: W_9=W_5; i=5: W_8=–W_6.

Результат буде таким же, якщо для встановлення залежності символів ХДС застосувати (4). Використання твердження 3 дозволяє визначити ((P–1)/2+i) символи ХДС $\left(i=\overline{1,\left(P-1\right)/2}\right)$ за відомими першими (P–1)/2 і символах. В цьому випадку є не визначеними лише перший і ((P–1)/2+i)-й символи ХДС, але ((P–1)/2+i)-й символ ХДС визначається за правилом кодування [2]. Для ХДС число символів К K, що приймають значення «1», дорівнює K=N/2. Це означає, що перший символ ХДС може бути довизначино, якщо відомі P–2 символів сигналу. Неважко переконатися в тому, що твердження та справедливі і для випадку розширеного поля Галуа $GF(p^n)$, тобто для випадку, коли n>1.

Виявлені і описані в твердженнях 3 та 4 зв'язки елементів і характерів елементів поля дозволяють не менш ніж у два рази підвищити швидкодію пристроїв формування ХДС.

Відомо [2], що до статистичних характеристик кореляційних функцій відносяться: математичне очікування викидів (m_u); математичне очікування модулів максимальних бічних викидів $\left(m_{|u_{\text{макс}}|}\right)$; середньоквадратичне відхилення бічних викидів $\left(D_u^{1/2}\right)$; середньоквадратичне відхилення модулів бічних викидів

$\left(D_{|u|}^{1/2}\right)$. З використанням розробленого спеціального програмного забезпечення, були виконані дослідження кореляційних властивостей складних нелінійних дискретних сигналів в кінцевих полях. У табл. 3 наведено узагальнені статистичні характеристики різних кореляційних функцій найбільш широко застосовуваних дискретних послідовностей.

Таблиця 3

Статистичні характеристики кореляційних функцій сигналів

Характеристики	$\frac{m_u}{\sqrt{N}}$	$\frac{m_{\lvert u_{\text{макс}}\rvert}}{\sqrt{N}}$	$\frac{D_{\lvert u\rvert}^{1/2}}{\sqrt{N}}$	$\frac{D_u}{\sqrt{N}}$
ХДС				
АФАК	1,1–1,8	0,28	0,32	0,43
ПФАК	0,1–1,9	0,15	0,02	0,14
АФВК	1,9–3,2	0,54	0,47	0,72
ПФВК	2,5–3,6	0,81	0,61	1,01
М-послідовності				
АФАК	0,7–1,25	0,32	0,26	0,41
ПФАК	$1/\sqrt{N}$	$1/\sqrt{N}$	0	0
Меандро-інвертовані ФАК	1,3–2,3	0,66	0,49	0,82
АФВК	1,4–5,0	0,54	0,48	0,73
ПФВК	1,9–6,0	0,80	0,62	1
Стикові ФВК	2,0–5,1	0,83	0,62	1
Випадкові послідовності				
АФАК	1,5–3,1	0,51	0,65	0,70
ПФАК	2,0–4,0	0,83	0,68	1
АФВК	2,4–4,3	0,54	0,48	0,70
ПФВК	2,75–4,5	0,82	0,62	1
Сегменти М-послідовностей				
АФАК	1,45–4,1	0,52	0,90	0,71
ПФАК	1,6–4,3	0,79	0,58	1
АФВК	1,4–4,3	0,52	0,49	0,72
ПФВК	1,6–5,0	0,80	0,60	1

Аналіз даних табл. 2 свідчить, що статистичні характеристики кореляційних функцій ХДС не поступаються аналогічним характеристикам інших сигналів, що наведені у даній таблиці.

5. 3. Визначення умов щодо функцій кореляції сигналів, які задані сукупністю систем нелінійних параметричних нерівностей

На основі дослідження алгебраїчної структури систем нелінійних параметричних нерівностей (СНПН) сформульована і в загальному вигляді вирішена задача синтезу нового класу складних нелінійних дискретних сигналів - крип-

тографічних сигналів (КС). Під КС пропонується розуміти сукупність послідовностей (векторів) символів певного алфавіту, які мають необхідні (задані) структурні, ансамблеві і кореляційні властивості.

Синтез таких сигналів засновано на використанні випадкових або псевдовипадкових процесів, в тому числі, алгоритмів криптографічного перетворення інформації [7–9].

Під задачею синтезу КС будемо розуміти задачу побудови підмножин послідовностей $\left(W_l^q\right)$, $q=\overline{1,N}$, $l=\overline{1,L}$, сукупність яких утворює систему сигналів алфавіту розмірності $M_k=N\times L$. В кожній із підмножин виконуються умови щодо структурних, ансамблевих, кореляційних властивостей, просторової та часової складності генерування сигналів. Синтез КС ґрунтується на використанні і аналізі періодичних і аперіодичних функцій кореляції.

Математична модель процесу синтезу даного класу сигналу має вигляд, що наводиться нижче.

1. Забезпечення умов виконання вимог до структурних та ансамблевих властивостей, можливостей формування підмножини КС з допустимою часовою та просторовою складністю, в тому числі з використанням ключів.

2. Побудова КС W^q, періодична функція автокореляції (ПФАК) кожного з яких, задовольняє системі нелінійних параметричних нерівностей (СНПН):

$$R_{a_1}^q(l)\le\sum_{i=1}^{L}W_i^q\left(W_{i+l}^q\right)^*\le R_{a_2}^q(l),\ l=\overline{1,L-1},\ q=\overline{1,N},\tag{21}$$

де $R_{a_1}^q(l)$ і $R_{a_2}^q(l)$ – задані значення реалізації ПФАК, а індекси обчислюються за модулем $(i+1)\bmod L$.

При $1=L$ для усіх $q=\overline{1,N}$ (21) дає згортку зі значенням L

$$\sum_{i=1}^{L}W_i^qW_{i+L}^q=\sum_{i=1}^{L}W_i^qW_i^q=L,\ q=\overline{1,N}.\tag{22}$$

3. Побудова пар КДС W^q та W^p, функції взаємної кореляції (ФВК) яких задовольняють вимогам, що визначаються сукупністю систем НПН (21), а також задовольняють вимогам до стикових функцій взаємної кореляції (СФВК) пар КС W^q та W^p зі стиковими дискретними словами W^{qp} та W^{pq}:

$$R_{b_{1,1}}^{qp}(l)\le\sum_{i=0}^{L-K}W_i^q\times\left(W_{i+l}^p\right)^*+\sum_{i=L-K+1}^{L-1}W_i^q\times\left(W_{i-l+K}^p\right)^*\le R_{b_{2,1}}^{qp}(l);\tag{23}$$

$$R_{b_{1,2}}^{qp}(l)\le\sum_{i=0}^{L-K}W_i^q\times\left(W_{i+l}^q\right)^*+\sum_{i=L-K+1}^{L-1}W_i^q\times\left(W_{i-l+K}^p\right)^*\le R_{b_{2,2}}^{qp}(l);\tag{24}$$

$$R_{b_{1,3}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times \left(W_{i+l}^p\right)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times \left(W_{i-l+K}^q\right)^* \le R_{b_{2,3}}^{qp}(l); \quad (25)$$

$$R_{b_{1,4}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times \left(W_{i+l}^p\right)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times \left(W_{i-l+K}^q\right)^* \le R_{b_{2,4}}^{qp}(l); \quad (26)$$

$$R_{b_{1,5}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times \left(W_{i+l}^q\right)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times \left(W_{i-l+K}^p\right)^* \le R_{b_{2,5}}^{qp}(l); \quad (27)$$

причому $l = \overline{1, L-1}$ для всіляких поєднань q і p, $q = \overline{1, N}$, $p = \overline{1, N}$, $q \ne p$, де $R_{b_{1,j}}^{qp}(l)$ і $R_{b_{2,j}}^{qp}(l)$, задані (необхідні) реалізації ПФВК і СФВК відповідно, $j = \overline{1,5}$.

В системах нелінійних параметричних нерівностей (21)–(24) W_i^q та W_i^p є невідомими значеннями випадкових чи псевдовипадкових символів КС W^q та W^p, $q = \overline{1, N}$, що належать визначенню в процесі їх побудування. В подальшому системи (21)–(27) будемо називати моделлю підмножини (словника) КС.

Проведемо аналіз систем нелінійних параметричних квадратичних нерівностей (далі систем) (21)–(27), використовуючи введену модель.

Системи (24), (25) при 1=L для усіх $q = \overline{1, N}$ повинно дати повну згортку зі значенням L, тобто

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, \ q = \overline{1, N}, \quad (28)$$

а (25) дає

$$\sum_{i=1}^{L} W_i^p W_{i+L}{}^p = \sum_{i=1}^{L} W_i^p W_i^p = L, \ p = \overline{1, N}. \quad (29)$$

Системи (23), (25) та (27) при 1=L для усіх пар W^q та W^p дають значення функції взаємної кореляції при нульовому значенні зсуву відповідно виду:

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0), \ q, p = \overline{1, N}, \quad (30)$$

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0), \ q, p = \overline{1, N}, \quad (31)$$

$$\sum_{i=1}^{L} W_i^p W_{i+L}{}^q = \sum_{i=1}^{L} W_i^p W_i^q = R^{pq}(0), \ p, q = \overline{1, N}. \quad (32)$$

Проведемо аналіз систем (21), (22) на предмет існування рішень та незалежності. Безпосередньо із (21) маємо, що до кожного з q КС W^q є L невідомих - $W_1^q, W_2^q, ..., W_L^q$. Для їх знаходження згідно (21) можна скласти систему із L–1 незалежних СНПН. Далі, використовуючи (22), отримуємо ще один вираз, але уже рівняння. Особливістю системи (21) є те, що ця система дає згортку кожного з q КС зі значенням L. На основі (21), (22) при побудові кожної з N підмножини КС можна скласти N незалежних СНПН, кожна з яких буде містити L–1 квадратичних нерівностей виду (21) і формально одне рівняння, так що всього їх буде L.

Для N=2 серед (28), (29) СНПН є збиткові нелінійні квадратичні рівняння. Рівняння (22) співпадає з (28), (29), тому останні два уже входять в систему (24), є залежними, тому не можуть бути використаними. Далі, рівняння (30), (32) співпадають, а рівняння (28) є симетричним в частині кореляційної функції, по відношенні до рівнянь (30), (31). Тому для кожної пари p та q незалежним є (30).

На основі детального аналізу маємо, що усі (23)–(27) СНПН визначають різні реалізації ПФВК та СФВК конкретно тільки двох КС - W^q та W^p. Тому математична модель побудови двох КС W^q та W^p однозначно визначається п'ятьма СНПН у вигляді (23)–(27), та, як уже було обгрунтовано, рівнянням (30).

Наведені вище результати аналізу дозволяють визначити складність моделі та на її основі складність побудування підмножини з N КС. При побудуванні одного КС необхідно, у залежності від допустимих значень $R_{a_1}^q(l)$ і $R_{a_2}^q(l)$, що визначаються межами щільної упаковки, розглянути $\upsilon \geq k$ систем виду (22). При побудуванні двох КС необхідно розглянути $\upsilon_2 \geq k_2$ систем виду (23)–(27), де K_2 визначається $R_{b_{1,j}}^{qp}(l)$ та $R_{b_{2,j}}^{qp}(l)$. При побудуванні N КС необхідно розглянути $\upsilon \geq K \cdot N$ систем виду (30)–(32), де $K{\cdot}N$ визначається $R_{a_1}^q(l)$ і $R_{a_2}^q(l)$ та $R_{b_{1,j}}^{qp}(l)$ і $R_{b_{2,j}}^{qp}(l)$ допустимими значеннями.

Таким чином, на основі врахування меж фізичної упаковки підмножини КС [4] існують можливості побудови підмножин КС згідно (22) та (30)–(32). Аналогічно (21), (23)–(27) задається модель підмножини (словника) КС через аперіодичні функції автокореляції (АФАК). В даному випадку можливі спрощення. Так систему (21) по аналогії можна подати у вигляді системи НПН на основі аперіодичних функцій кореляції, тобто

$$r_{a_1}^q(l) \leq \sum_{i=1}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r_{a_2}^q(l), \; l = \overline{1,L}, \; m = \overline{1,L}, \tag{33}$$

де $r_{a_1}^q(l)$ і $r_{a_2}^q(l)$ – задані, але допустимі реалізації з точки зору «щільної упаковки».

Далі, системи (21)–(27) також можна надати через аперіодичні функції взаємної кореляції (АФВК) у вигляді системи нелінійних параметричних нерівностей

$$r_{b_{1,1}}^{qp}(l) \le \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \le r_{b_{1,2}}^{qp}(l); \quad (34)$$

$$l = \overline{1,L},\ \ m = \overline{1,L},$$

$$r_{b_{2,1}}^{qp}(l) \le \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^p \left(W_{i+1}^q\right)^* \le r_{b_{2,2}}^{pq}(l); \quad (35)$$

$$l = \overline{1,L},\ m = \overline{1,L},$$

де $r_{b_{1,1}}^{qp}$, $r_{b_{1,2}}^{qp}$, $r_{b_{2,1}}^{qp}$, $r_{b_{2,2}}^{qp}$, – допустимі, з точки зору «щільної упаковки», значення АФАК та АФВК.

З урахуванням необхідності забезпечення криптографічної стійкості та структурної скритності пар чи підмножин КС, в якості джерела дискретних послідовностей може бути застосовано алгоритми блокового симетричного перетворення або інше джерело випадкових чи псевдовипадкових послідовностей.

З урахуванням формул (21)–(27) визначені кроки методу синтезу дискретних складних криптографічних сигналів:

1. Формування випадкових чи псевдовипадкових дискретних послідовностей.
2. Оцінка статистичних властивостей потенційних КС.
3. Побудова необхідного числа потенційних КС W^q згідно системи (21) та ключових даних.
4. Знаходження пар чи підмножин КС W^q та W^p , які задовольняють вимогам (23)–(27), застосовуючи методу «гілок та меж».
5. Побудова матриці станів взаємно-кореляційних функцій всіх можливих пар потенційних КС, які пройшли відбір за результатами попереднього кроку та мають усі необхідні властивості.
6. Аналіз матриці станів та формування необхідного числа підмножин чи пар КС згідно (21), (23)–(27) та відбір в підмножину лише тих, що задовольняють вимогам.

5. 4. Дослідження властивостей синтезованих класів нелінійних дискретних складних криптографічних сигналів для використання в ІКС як фізичного переносника інформації

Для низки додатків ІКС потрібні сигнали, що володіють високою структурною скритністю, необхідними кореляційними властивостями і значним об’ємом (ансамблем). Проведемо оцінку ансамблевих, кореляційних і структурних властивості даної системи сигналів.

Необхідно відзначити, що КС, на відміну від відомих класів сигналів, що застосовуються в різних додатках ІКС, можуть бути синтезовані для будь-яких значень періоду дискретних сигналів. Об’єм системи нелінійних КС визначається вимогами, що пред'являються до системи, з точки зору таких показників ефективності функціонування ІКС, як завадостійкість прийому сигналів, скрит-

ність і інформаційна безпека системи. Користувачам (власникам) системи, виходячи із зазначених обмежень, необхідно приймати компромісні рішення щодо вибору ансамблю нелінійних КС з необхідними властивостями.

У табл. 4 наведено дані, що характеризують кореляційні і ансамблеві властивості КС різного періоду. Зокрема, наведено: період КС; граничні значення бічних піків автокореляційних функцій і число сигналів, які відповідають граничним значенням в класі КС; найменші значення бічних піків різних функцій кореляції і їх кількість.

Аналіз даних, що наведено в табл. 4, свідчить, що значення максимальних бічних викидів, статистичні характеристики КС не поступаються відповіднім характеристикам сигналів, які побудовані з використання *M*-послідовностей. Так, для періоду послідовності 1023 елементів, число пар КС, що задовольняють граничному значенню для бічних пелюсток ФВК – 100, становить 5293538. Для *M*-послідовностей число пар, які відповідають даній границі, становить – 435, тобто перевищення об'єму системи КС становить більш ніж 10^4 разів. Варіюючи граничними значеннями рівня бічних пелюсток відповідної функції кореляції, можуть бути вирішені завдання досягнення необхідних значень показників завадостійкості прийому сигналів, завадозахищеності та інформаційної безпеки системи.

Таблиця 4

Кореляційні і ансамблеві властивості КС

№	Розмірність сегмента КС	Граничні значення функції невизначеності	ПФАК			АФАК	ПФВК			АФВК
			Число КС, що задовольняють границі	Найменше значення u_{max}	Число КС з найменшим u_{max}	Число КС, що задовольняють границі	Загальна кількість пар	Число КС, що задовольняють границі	Найменше значення u_{max}	Число КС, що задовольняють границі
1	31	9	7743	5	155	3622	2997 7024	1 465 137	5	14 537 423
2	63	17	10868	9	14	7166	5905 6712	12 214 869	11	54 822 445
3	127	23	3482	17	51	1302	6062 162	47 053	19	1 619 780
4	511	59	3819	45	6	1951	7292 380	122 835	51	3 466 713
5	1023	100	8513	77	9	6 194	3623 5584	5 293 538	79	35 083 491

Для дослідження структурних властивостей КС застосовують методики тестування генераторів випадкових (псевдовипадкових) послідовностей, які визначену у [10, 11]. Результати тестування показали, що КС задовольняють вимогам, що пред'являються до випадкових послідовностей [12]: непередбачуваність символів, незворотність, випадковість, рівноймовірність, незалежність і ін. Таким чином, структурні властивості КС не відрізняються від властивостей випадкових послідовностей.

6. Обговорення результатів досліджень методів синтезу дискретних складних сигналів для застосування у сучасних інформаційно-комунікаційних системах

Отримані результати свідчать, що запропоновані методи синтезу характеристичних дискретних сигналів (ХДС) у кінцевих полях дозволяють суттєво підвищити продуктивність синтезу зазначених сигналів. Дійсно, виграш у часі синтезу нелінійних сигналів в кінцевих полях із застосуванням розробленого методу (твердження 1), в порівнянні з відомим методом, для періоду ХДС 256 елементів, становить 25,5 рази, а для періоду 9972–1039,6 рази. Отримано метод синтезу всієї системи ХДС на основі процедури децимації (твердження 2). Результати комп'ютерного моделювання і розрахунки, які проведені із застосуванням (14), (15), показують, що запропонований метод синтезу на основі операції децимації перевершує за швидкодією відомий методу різнисних множин. Так, для періоду сигналу 2380 елементів виграш у часі становить понад 28 разів. Виявлені і описані в твердженнях 3 та 4 зв'язки елементів і характерів елементів поля дозволяють не менш ніж у два рази підвищити швидкодію пристроїв формування ХДС. Проведені дослідження кореляційних властивостей ХДС показали, що значення максимальних бокових піків, а також статистичні характеристики різних кореляційних функцій (табл. 1) не поступаються аналогічним характеристикам кращих відомих лінійних сигналів. Це, у свою чергу, означає, що показники завадостійкості при прийомі сигналів, що пропонуються, будуть не гіршими, ніж при застосуванні відомих систем сигналів. При цьому структурні властивості ХДС, що пов'язують зі складністю визначення станцією протидії закону формування сигналу, суттєво поліпшені у порівнянні з відомими системами сигналів. Зазначене безпосередньо слідує з твердження 4. Необхідно відмітити, що застосування зазначених сигналів дозволяє поліпшити показники інформаційної безпеки, а саме ймовірність нав'язування супротивником хибних повідомлень (сигналів). Відомо, що цей показник визначається, у тому числі, ансамблевими властивостями використовуваних сигналів (об'єм системи, спектр значень періоду сигналів, для яких можуть бути синтезовані сигнали). Аналіз наведених аналітичних співвідношень, даних табл. 1 свідчать про те, що ХДС, з точки зору ансамблевих властивостей, є кращими в порівнянні цілим рядом використовуваних послідовностей, таких як М-послідовності, послідовності Лежандра та інших.

На основі дослідження алгебраїчної структури систем нелінійних параметричних нерівностей, а також аналізу періодичних і аперіодичних функцій кореляції, отримана математична модель процесу синтезу дискретних складних сигналів (21)–(27) і практичні методи синтезу нелінійних дискретних складних криптографічних сигналів (далі – КС). Для синтезу КС використовують випадкові або псевдовипадкові процеси (в тому числі, криптографічні алгоритми), що дозволяє створювати послідовності символів (сигналів) певного алфавіту. Такі послідовності задовольняють вимогам незворотності, випадковості, непередбачуваності, і володіють необхідними структурними, ансамблевими і кореляційними властивостями, що витікає з даних, які наведено у табл. 4.

Отримані результати дозволяють стверджувати, що застосування КС призводять до поліпшення показників завадозахищеності, інформаційної безпеки, скритності інформаційно-комунікаційних систем, завадостійкості прийому сигналів в умовах впливу різних видів перешкод. Застосований програмний комплекс, особливостями якого є модульність і гнучкість, використання єдиного веб-сервісу для одночасного використання можливостей комплексу багатьма користувачами, дозволив реалізовувати функції синтезу, формування, обробки і дослідження властивостей сигналів. Зазначене свідчить про можливість впровадження отриманих результатів в діючи і перспективні зразки програмно-технічних засобів фізичного рівня інформаційно-комунікаційних систем.

Дані дослідження стосуються виключено процесів синтезу, формування, обробки двох класів дискретних складних сигналів, а саме, криптографічних сигналів та сигналів у кінцевих полях. Програмі засоби, що реалізують функції синтезу, формування, обробки і дослідження властивостей зазначених систем сигналів, практично готове до можливого застосування у складі дослідних зразків і елементів цифрових комунікаційних засобів сучасних ІКС. Можливості застосування розроблених методів синтезу зазначених класів сигналів у сучасних комунікаційних системах можуть бути обмежені лише характеристиками застосовуваних апаратних засобів та особливостями реалізації програмного комплексу (мова програмування, принципи побудови інтерфейсу тощо).

Напрямами подальшого розвитку дослідження можуть бути розробка методів синтезу і дослідження властивостей систем дискретних складних сигналів, які утворені шляхом посимвольного перемноження так званих вихідних сигналів та сигналів, що продукують. Причому, у якості вихідних сигналів пропонується використовувати ортогональні дискретні сигнали, а як сигнали, що продукують – дискретні складні криптографічні сигнали та дискретні складні сигнали у кінцевих полях. І у цьому сенсі, результати досліджень, що пропонуються у даній роботі, виявляться корисними. Є підстави вважати, що отримані таким чином сигнали будуть мати поліпшені ансамблеві, кореляційні і структурні властивості, що дозволить використовувати їх як фізичний носій даних в ІКС, для яких критичними є вимоги інформаційної безпеки та завадозахищеності.

7. Висновки

1. На основі визначеної математичної залежності елементів та індексів елементів простого та розширеного полів Галуа розроблено методи синтезу нелінійних складних характеристичних дискретних сигналів (ХДС) у кінцевих простих і розширених полях. Зазначені методи дозволяють суттєво підвищити швидкодію синтезу сигналів. Підтвердження цього факту може бути знайдено і у результатах проведеного чисельного моделювання. Таке моделювання показало, що виграш у часі синтезу окремого ХДС із застосуванням розробленого методу, в порівнянні з відомим методом, для числа елементів 256, складає 25,5 рази, а для числа елементів 9972–1039,6 рази. Щодо отриманого методу синтезу всієї системи сигналів на основі методу децимації, то виграш у часі синтезу становить (при числі елементів сигналу 2380) понад 28 разів.

2. Для оцінки показників завадозахищеності та інформаційної безпеки функціонування інформаційно-комунікаційних систем (ІКС), ефективним інструментом є дослідження властивостей сигналів-фізичних переносників даних у таких системах. Отримана у ході досліджень модель структури складних нелінійних дискретних сигналів у кінцевих полях, ансамблеві, статистичні і кореляційні властивості таких сигналів дозволяють стверджувати, що зазначені показники ІКС, суттєво поліпшуються. Так, для періоду сигналу 1023 елементи виграш, з точки зору структурної скритності при використанні ХДС, по відношенню до застосування лінійних сигналів, становить 50 разів, а для числа елементів 8192 - більш ніж 300 разів. Для тривалості ХДС 256 елементів виграш, у порівнянні із застосування лінійних *M*-послідовностей, становить 3 дБ. Оскільки показники інформаційної безпеки, а саме, ймовірності нав'язування супротивником хибних повідомлень, залежать від ансамблевих характеристик сигналів, покращені ансамблеві властивості нелінійних ХДС дозволяють суттєво поліпшити і цей показник ефективності функціонування системи.

3. Визначені умови щодо функцій кореляції сигналів, які задані сукупністю систем нелінійних параметричних нерівностей, дали змогу розробити метод синтезу дискретних складних криптографічних сигналів. Відмінними особливостями такого підходу при розробці теоретичних основ і методів синтезу є: застосування випадкових (псевдовипадкових) процесів можливість відтворення сигналів в просторі і часі за допомогою параметрів, які застосовуються при їх синтезі, у тому числі, криптографічних ключів. Зазначені особливості підходу до синтезу сигналів дозволяють формувати сигнали, які є нелінійними за законом їх створення, оскільки використовують випадкові (псевдовипадкові процеси). Крім того, такі сигнали можуть бути синтезовані для будь-якого періоду (парне число елементів або непарне).

4. Отриманий клас нелінійних КС, як показали дослідження із застосуванням методів комп'ютерного моделювання, володіє покращеними, у порівнянні з відомими лінійними класами сигналів, структурними, ансамблевими і кореляційними властивостями. Такі сигнали (послідовності) задовольняють вимогам незворотності, випадковості, непередбачуваності, тобто не відрізняються від випадкових послідовностей. Зазначене дозволяє поліпшити показники скритності і інформаційної безпеки системи. Так, для періоду послідовності 1023 елементи, об'єм системи КС, більш ніж в 15 разів перевищує об'єм системи сигналів з 3-х рівневою функцією взаємної кореляції, і більш ніж в 1200 разів - об'єм системи, складеної з М-послідовностей. За рахунок поліпшених ансамблевих властивостей КС і динамічної зміни відповідності: біт повідомлення - складний сигнал, з'являється можливість поліпшити показники інформаційної безпеки. Так, імітостійкість системи (ймовірність нав'язування хибних повідомлень) при застосуванні КС з періодом сигналу 1023 елемента на чотири порядки вище, ніж при застосуванні лінійних класів сигналів (наприклад, М-послідовностей).

Подяка

Певний внесок у проведенні дослідження внесли співробітники кафедри безпеки інформаційних систем і технологій Харківського національного уніве-

рситету імені В. Н. Каразіна Семенко Є. С, Хо Чи Лик. Дякуємо керівництву АТ «Інститут інформаційних технологій» за фінансову підтримку при підготовці рукопису до опублікування.

Література

1. Варакин, Л. Е. (1985). Системы связи с шумоподобными сигналами. М.: Радио и связь, 384.
2. Свердлик, М. Б. (1975). Оптимальные дискретные сигналы. М.: Радио и связь, 200.
3. Liang, Q., Liu, X., Na, Z., Wang, W., Mu, J., Zhang, B (2018). Communications, Signal Processing, and Systems. Proceedings of the CSPS Volume III: Systems. Springer, 1219. doi: https://doi.org/10.1007/978-981-13-6508-9
4. Ipatov, V. P. (2005). Spread Spectrum and CDMA. Principles and Applications. John Wiley & Sons Ltd. doi: https://doi.org/10.1002/0470091800
5. Michael Yang, S.-M. (2019). Modern Digital Radio Communication Signals and Systems. Springer, 664. doi: https://doi.org/10.1007/978-3-319-71568-1
6. Гантмахер, В. Е., Быстров, Н. Е., Чеботарев, Д. В. (2005). Шумоподобные сигналы. Анализ, синтез, обработка. СПб.: Наука и Техника, 400.
7. Gorbenko, I. D., Zamula, A. A., Morozov, V. L. (2017). Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts. Telecommunications and Radio Engineering, 76 (19), 1705–1717. doi: https://doi.org/10.1615/telecomradeng.v76.i19.30
8. Gorbenko, I. D., Zamula, A. A. (2017). Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems. Telecommunications and Radio Engineering, 76 (12), 1079–1100. doi: https://doi.org/10.1615/telecomradeng.v76.i12.50
9. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення (2015). К.: Міністерство економрозвитку України.
10. Kuznetsov, A. A., Moskovchenko, I. V., Prokopovych-Tkachenko, D. I., Kuznetsova, T. Y. (2019). Heuristic methods of gradient search for the cryptographic boolean functions. Telecommunications and Radio Engineering, 78(10), 879–899. doi: https://doi.org/10.1615/telecomradeng.v78.i10.40
11. NIST 800-90 b. Recommendation for the Entropy Sources Used for Random Bit Generation (2012).
12. Tesař, P. (2017). Influence of Non-Linearity on Selected Cryptographic Criteria of 8x8 S-Boxes. Acta Informatica Pragensia, 6 (2), 162–173. doi: https://doi.org/10.18267/j.aip.107