УДК 621.391 **DOI:10.30837/rt.2020.1.200.15**

І.Д. ГОРБЕНКО, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук, ХО ЧІ ЛИК

МЕТОДИ ПОШУКУ ОПТИМАЛЬНИХ ЗА МІНІМАКСНИМ КРИТЕРІЄМ СИСТЕМ СКЛАДНИХ НЕЛІНІЙНИХ ДИСКРЕТНИХ СИГНАЛІВ

Вступ

На сьогодні для найважливіших додатків інформаційно-комунікаційних систем (ІКС), а саме: супутникових систем зв'язку, високошвидкісних систем стільникового мобільного телефонного зв'язку, систем радіолокації, радіонавігації, цифрового телебачення і радіо, актуальними є дослідження, що пов'язані з використанням сигналів – фізичних переносників даних в ІКС. Значне число сучасних ІКС відносяться до багатокористувачевих систем. У таких системах безліч каналів розміщуються в межах загального частотно-часового ресурсу. Одним із способів підвищення ефективності використання діапазону частот, з урахуванням електромагнітної сумісності, є використання множинного доступу з кодовим розділенням абонентів, що працюють в загальній смузі частот. Зазначений спосіб доступу є найбільш перспективним за багатьма характеристиками: висока завадозахищеність каналів і забезпечення конфіденційності даних; висока швидкість передачі і ефективність використання смуги частот; висока енергетична економічність і абонентська ємність мережі. Оскільки кодове розділення каналів ТКС грунтується на відмінності сигналів, що надаються абонентам системи, то побудова таких систем і їх характеристики визначаються вибором сигналів і їх властивостями. Дослідження показали, що перспективним напрямком забезпечення безпеки інформаційних ресурсів є використання технології розподіленого спектра (широкосмугових шумоподібних сигналів). Такі сигнали утворюють шляхом амплітудно-фазової модуляції дискретних послідовностей (сигнатур) користувача потоком даних. Наприклад, виконується множення бітового інформаційного потоку $B_k(t)$-го абонента на специфічну для кожного користувача (в багатокористувачевих системах, наприклад в CDMA додатках) на сигнатуру $S_k(t)$, а результат добутку $S_k(t)\cdot B_k(t)$ модулює безперервну несучу, тобто

$$S_k(t,b_k)=S_k(t)\cdot B_k(t)\cdot\cos(2\cdot\pi\cdot f_0\cdot t), \qquad (1)$$

де $b_k=(\ldots,b_{k,-1},b_{k,0},b_{k,1}\ldots)$ – бітовий потік k-го користувача, а $B_k(t)=b_{k,i}=\pm1,(i-1)\cdot T_b<t<i\cdot T_b$ (T_b – тривалість імпульсів позитивної і негативної полярності інформаційного сигналу k-го користувача).

В описаному прикладі потік бітів спочатку модулює бінарну сигнатуру, а результат використовується для бінарної фазової маніпуляції несучої.

При цьому маніпулюючі дискретні послідовності (ДП), які не залежать від бітового інформаційного потоку, повністю визначають властивості сигналів і часто ототожнюються з ними [1].

Як показують дослідження [2 – 4], основні показники ефективності ІКС: інформаційна безпека (в тому числі, конфіденційність, захищеність від нав'язування хибних повідомлень, режимів роботи системи – автентичність), завадозахищеність (завадостійкість прийому сигналів і скритність функціонування), значною мірою визначаються властивостями сигналів – фізичних переносників даних в ІКС. Тому увага дослідників сфокусована на аналізі, синтезі і обробці ДП з необхідними кореляційними, ансамблевими, статистичними, структурними та іншими властивостями.

Основні результати досліджень

При проектуванні багатокористувачевих ІКС основною проблемою є вибір способу множинного доступу, тобто можливості одночасного використання багатьма абонентами каналу зв'язку з мінімальним взаємним впливом. Оскільки кодове поділ грунтується на відмінності сигналів, то побудова багатокористувацьких комунікаційних систем і показники ефективності зазначених систем визначаються вибором сигналів і їх властивостями.

Зазвичай число абонентів в сучасних ІКС досить велике, тому вибір сигналів для систем зводиться до визначення систем сигналів із заданими властивостями. Зусилля дослідників направлені на пошуки ансамблів складних сигналів, характеристики яких з ростом довжини наближаються до кордонів щільної упаковки, або характеристик так званого гіпотетичного ансамблю, тобто ансамблю, всі представники якого мають нульову постійну складову, ідеальну періодичну функцію автокореляції (ПФАК) і нульові пелюстки періодичної функції взаємної кореляції (ПФВК) [5]:

$$\tilde{a}_{k,0} = 0;\ \rho_{kk}(m) = 0, m \neq 0 \bmod N;\ \rho_{kl}(m) = 0, k, l = 1, 2, ..., K. \qquad (2)$$

Широко застосовуваним критерієм подібного наближення є мінімаксний критерій, який орієнтує синтез ансамблю на мінімізацію максимального значення на множині всіх небажаних кореляцій. Для ідеального гіпотетичного ансамблю кореляційний пік $\rho_{\max}$ визначають як найбільшу з двох величин: максимуму серед усіх бічних пелюсток автокореляцій $\rho^a_{\max}$ послідовностей і максимуму серед значень взаємних кореляцій $\rho^c_{\max}$ всіх пар послідовностей

$$\rho_{\max} = \max\left\{\rho^a_{\max}, \rho^c_{\max}\right\}, \rho^a_{\max} = \max_{k, m\neq 0}\left|\rho_{p,kk}(m)\right|, \rho^c_{\max} = \max_{k,l,mk\neq l}\left|\rho_{p,kl}(m)\right|. \qquad (3)$$

Природно, що для ідеального гіпотетичного ансамблю $\rho_{\max}$ дорівнює нулю, а для будь-якого реального ансамблю може служити адекватною мірою його близькості до ідеального.

Мінімізація рівня бічних пелюсток автокореляційної функції (АКФ) має найбільше значення при конструюванні сигналу для таких додатків як виявлення сигналу, синхронізація, оцінка часу запізнювання і ін. При побудові багатокористувачевих широкосмугових систем з багатостанційним доступом і кодовим ущільненням каналів найбільш важливими проблемами є синтез, формування і обробка сигналів із заданими взаємно кореляційними властивостями.

В даний час відсутні регулярні методи синтезу дискретних послідовностей (ДП) оптимальних за мінімаксним критерієм. Більш того, не представляється можливим відповісти на питання: наскільки відомі сигнали з великим числом позицій (періодом) близькі до оптимальних.

Відомо, що будь-який сигнал $S(t)$ кінцевої енергії може бути представлений як сума незліченого числа гармонійних коливань, амплітуди і фази яких в межах нескінченно малого діапазону частот $[f, f + df]$ визначаються спектральною щільністю або спектром $\bar{S}(f)$. Математичним відображенням цього факту служить пара зворотного і прямого перетворень Фур'є:

$$S(t) = \int_{-\infty}^{\infty} \bar{S}(f)\cdot\exp(j\cdot 2\cdot\pi\cdot f\cdot t)df, \tilde{S}(f) = \int_{-\infty}^{\infty} S(t)\cdot\exp(-2\cdot\pi\cdot f\cdot t)dt. \qquad (4)$$

У теорії зв'язку найбільш поширеною моделлю служить канал з адитивним білим гаусовським шумом, в якому ймовірність трансформації каналом заданого вхідного сигналу в те чи інше вихідне спостереження $y(t)$ (перехідна ймовірність – $P\left[y(t)\,|\,S(t)\right]$) експоненціально зменшується зі зростанням квадрата Евклідової відстані між переданим сигналом і вихідним коливанням [5]:

$$P\left[y(t)\middle|S(t)\right] = \kappa \cdot \exp\left(-\frac{1}{N_0} d(s,y)\right), \tag{5}$$

де κ – константа, що не залежить від $S(t)$ і $y(t)$, N_0 – спектральна щільність потужності одностороннього білого шуму, а Евклідова відстань між $S(t)$ і $y(t)$ визначається як

$$d(S,y) = \sqrt{\int_0^T \left[y(t) - S(t)\right]^2 dt} \tag{6}$$

Відповідно до співвідношень (5) і (6) схожість сигналу (ймовірність того, що він перетворений каналом в спостереження) $y(t)$ зменшується зі збільшенням Евклідової відстані між $S(t)$ і $y(t)$. У разі рівної ймовірності всіх повідомлень джерела (що досягається при правильному проектуванні системи) оптимальною стратегією спостерігача, що забезпечує мінімальну помилку щодо прийняття рішення відносно сигналу, який передано, є правило (критерій) максимальної правдоподібності (МП). Згідно з цим критерієм, після того, як коливання $y(t)$ прийнято, рішення приймається на користь того сигналу, для якого ймовірність трансформації його каналом в прийняте спостереження $y(t)$ є найбільшою (в порівнянні з ймовірностями для інших сигналів). З урахуванням викладеного МП рішення для гаусова каналу може бути перетворено в правило мінімуму відстані:

$$d(S_j, y) = \min d(S_j, y) \Rightarrow H_j, \tag{7}$$

тобто рішення приймається на користь сигналу $S_j(t)$, оскільки він найбільш близький (в сенсі Евклідової відстані) до спостереження $y(t)$ серед всіх конкуруючих сигналів.

Важливою геометричною характеристикою оптимального правила пошуку систем сигналів у відповідності до правила максимальної правдоподібності (МП) є скалярний добуток двох сигналів:

$$(U,V) = \int_0^T U(t) \cdot V(t) dt, \tag{8}$$

яке може трактуватися як гранична форма скалярного добутку двох n – мірних векторів. Ця ж характеристика може бути обчислена за допомогою довжини векторів і косинуса кута α між ними: $(U,V) = \|U\|\|V\|\cos\alpha$ і, таким чином, скалярний добуток векторів свідчить про близькість або схожість сигналів, оскільки, чим ближче сигнали однакової довжини (енергії) один до одного, тим менше $\cos\alpha$ відрізняється від одиниці , і тим більше скалярний добуток. На підставі цього скалярний добуток (8) називають також кореляцією сигналів.

Розкривши дужки в (6), приходимо до співвідношення

$$d^2(S_i, y) = \int_0^T y^2(t) dt - 2 \cdot \int_0^T y(t) \cdot S(t) dt + \int_0^T S^2(t) dt = \|y\|^2 - 2 \cdot Z_i + \|S_i\|^2, \tag{9}$$

де Z_i – відповідає кореляції між спостереженням $y(t)$ та i -м сигналом $S(t)$

$$Z_i = (y_i, S_i) = \int_0^T y(t) \cdot S(t) dt. \tag{10}$$

Перший доданок в правій частині співвідношення (9) фіксовано для даного спостереження і не впливає на відстані і рішення, що аналізуються, відносно того, який з сигналів був прийнятий. Останній член суми є ні що інше, як енергія i-го сигналу E_i. З огляду на це, правило мінімуму відстані (7) може бути сформульовано як правило максимуму кореляції:

$$Z_j - \frac{E_j}{2} = \max(Z_i - \frac{E_j}{2}) = H_j . \qquad (11)$$

Останній вираз означає, що з M можливих сигналів з однаковою енергією фактично прийнятим вважається той, який має максимум кореляції зі спостереженням $y(t)$.

Наведені міркування вказують на спосіб конструювання безлічі сигналів. На рис. 1 зображено сигнальні вектори.

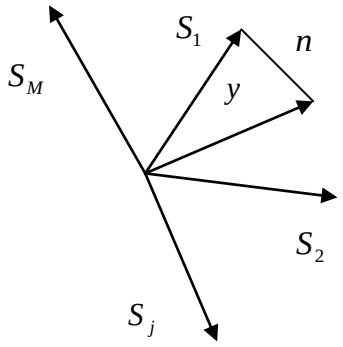

Рис. 1. Геометрична інтерпретація оптимального правила пошуку систем сигналів

Припустимо, що передавався сигнал S_1 і що він піддається спотворенню в каналі з адитивним білим гаусовим шумом, наслідком чого служить додавання до вектору S_1 шуму *n*. Вектор спостереження $y = S_1 + n$ буде випадковим чином (оскільки гаусовський вектор n характеризується симетричним ймовірнісним розподілом, що експоненціально спадає зі збільшенням довжини вектору *n,* що очевидно випливає з (1) після видалення з нього сигналу (тобто при підстановки $S(t) = 0$), переміщатися навколо, як це показано на рисунку, і тоді, згідно з правилом мінімуму відстані (7), як тільки y виявиться ближче до певного іншого, ніж сигнал S_1, то буде прийнято помилкове рішення. Для мінімізації ймовірності виникнення такого роду помилки слід розташовувати інші сигнали на максимально великій відстані від S_1. Оскільки будь-який з M сигналів може передаватися рівноймовірно, тобто займати місце S_1, то, очевидно, що всі відстані між сигналами $d(S_i, S_j), 1 \le i \le j \le M$ слід робити максимально великими.

Завдання побудови безлічі максимально віддалених один від одного сигналів (що входить в клас так званих задач упаковки) виявляється досить складним, і поки що не має спільного рішення. Одним з обмежень при синтезі сигналів є розмірність сигнального простору, всередині якого здійснюється їх упаковка. Фізична сутність цього обмеження обумовлена практичним ресурсом, наприклад шириною частотної смуги ΔF. Якщо частотно-часовий ресурс, в якому можуть розташовуватися M сигналів, обмежений параметрами ΔF і тривалістю сигналу T відповідно, то відповідно до теореми відліків є близько ΔFT незалежних відліків, які можуть бути використані при синтезі *M* сигналів, причому кожен з сигналів трактується як вектор в просторі розмірності $n_S = \Delta FT$.

Задача вибору безлічі сигналів може бути сформульована таким чином: знайти в просторі заданої розмірності n_S сузір'я з *M* векторів, що задовольняє енергетичним обмеженням і володіє максимально можливим мінімумом відстані між векторами $\mathrm{d}\min = \max$. У світлі виразів (2) – (3), а також (8) – (10) перевагу надають сигналами з найменшим значенням максимального бічного пелюстка. Ця вимога завжди супроводжується обмеженням на метод модуляції або на алфавіт, якому належать символи кодової послідовності. Таким чином, вимоги, що пред'являються до найкращого сигналу, можуть бути сформульовані у вигляді такої

оптимізаційної задачі: на безлічі всіх можливих послідовностей довжини N з символами з заздалегідь обраного алфавіту знайти послідовність або послідовності з мінімальною величиною максимального бічного пелюстка кореляційної функції.

В даний час відсутні регулярні методи синтезу дискретних послідовностей (ДП), оптимальних за мінімаксним критерієм. Більш того, не представляється можливим відповісти на питання: наскільки відомі сигнали з великим числом позицій N близькі до оптимальних. Тому актуальним залишається пошук ефективних методів розрахунку ДП з хорошими мінімаксними властивостями.

Наявність в N-вимірному лінійному просторі не більше N ортогональних векторів (сигналів) робить гіпотетичним ідеальний, з точки зору мінімаксного критерію, ансамбль дискретних послідовностей з нульовими боковими пелюстками функції авто- і взаємної кореляції, і обмежує потенціал зниження кореляційного викиду R при фіксованих N і числі абонентів K багатокористувачевої мережі.

При вирішенні низки задач теорії оптимального прийому сигналів, зокрема, виявлення сигналу, оцінка параметрів сигналів (затримки, амплітуди, початкової фази) та ін., важливим є автокореляційні властивостей систем сигналів, що використовуються.

Задача оцінювання часової затримки сигналу є типовою для телевізійних систем (канали синхронізації), цифрових систем мобільного радіозв'язку (пілотні канали, схеми стеження за часом), систем локації (вимір дальності до цілі), систем навігації космічного і наземного базування (вимірювання відстані до маяків) і ін. Фактично для адекватної роботи будь-якої сучасної системи обробки інформації необхідно відновити часову шкалу, що міститься в прийнятому коливанні, і це саме те, що відомо як оцінка затримки по часу [5].

Задача оцінки параметрів може бути сформульована таким чином. Нехай спостереження $y(t)$ поряд з шумом містить детермінований сигнал $s(t;\lambda)$, в якому єдиним невідомим є точне значення постійного параметра λ. Спостерігач, ґрунтуючись на аналізі $y(t)$, повинен прийняти рішення про те, яке значення з діапазону можливих прийняв параметр сигналу. Це рішення прийнято називати оцінкою і позначати як $\hat{\lambda}$. Оскільки в прийнятому спостереженні $y(t)$ завжди присутній шум, то при кожному сеансі прийому оцінка $\hat{\lambda}$ відрізняється від невідомого істинного значення параметра λ. У зв'язку з цим виникає питання: як прийняти оптимальне рішення, яке гарантувало б найменшої шкоди, зумовленої цими відмінностями. В принципі, задача оцінювання нічим не відрізняється від задачі розрізнення M сигналів. Тому для оцінки параметрів може бути застосована оптимальна стратегія рішень – правило максимальної правдоподібності. Це означає, що серед всіх конкуруючих значень λ в якості оцінки $\hat{\lambda}$ слід вибирати те, яке максимізує ймовірність трансформації каналом сигналу $s(t;\lambda)$ в спостережуване коливання $y(t)$. Для каналу з адитивним білим гаусовським шумом це правило еквівалентно правилу мінімуму відстані, яке з використанням введених позначень представимо у вигляді

$$d(s_\lambda, y) = \min_{\lambda} d(s_\lambda, y) \Rightarrow \lambda, \tag{12}$$

де s_λ – векторне позначення сигналу.

Застосування даного правила забезпечує отримання максимально правдоподібної (МП) оцінки $\hat{\lambda}$ в результаті знаходження такого значення, при якому сигнал найбільш близький за відстані Евкліда до спостереження $y(t)$. Достовірність (точність) оцінювання можна характеризувати величиною відхилення $\varepsilon = \hat{\lambda} - \lambda$ оцінки параметра $\hat{\lambda}$ від його істинного значення λ. Представляється розумною вимога: математичне очікування помилки ε, усереднене по

всіх можливих спостереженнях $y(t)$ при фіксованому істинному значенні λ, має дорівнювати нулю, тобто оцінка $\hat{\lambda}$ в середньому повинна збігатися з істинним значенням λ:

$$\bar{\varepsilon} = \overline{\hat{\lambda} - \lambda} = 0 \Leftrightarrow \bar{\lambda} = \lambda, \forall\lambda . \quad (13)$$

Суттєве значення для якісної оцінки параметрів сигналу має також величина розкиду оцінки відносно істинного значення. Традиційною і адекватною мірою розкиду служить дисперсія помилки $D\{\varepsilon\} = \overline{(\hat{\lambda} - \lambda)^2}$. Тоді, правило прийняття рішення повинно забезпечувати отримання оцінки з мінімальним значенням дисперсії для всіх дійсних значень λ:

$$D\{\varepsilon\} = \overline{(\hat{\lambda} - \lambda)^2} = \min, \forall\lambda . \quad (14)$$

У теорії оцінювання фундаментальна межа Крамера – Рао [5] встановлює нижню межу величини дисперсії будь оцінки:

$$D\{\lambda\} = D\{\varepsilon\} \approx -\frac{1}{\rho''(0) \cdot q^2}, q >> 1. \quad (15)$$

Присутність у (15) відношення сигнал-шум $q^2 = 2E / N_0$ в знаменнику правої частини співвідношення означає: що для будь-якого правила оцінювання справедливим є твердження: чим вище відношення сигнал-шум, тим менше помилка і тим вище точність вимірювань. Друга похідна говорить про кривизну або гостроту функції в даній точці і для випуклої кривої є негативною. У свою чергу, гострота $\rho(\lambda)$ в нульовій точці показує чутливість сигналу по відношенню до неузгодженості в величині λ: чим гостріше $\rho(\lambda)$, тим швидше копія сигналу з неузгодженістю за величиною втрачає свою подобу з вихідної копією.

Поряд з $\rho_o''(0)$ як індикатор гостроти автокореляційної функції (АКФ) сигналу може використовуватися характеристика, звана протяжністю кореляції, або часом кореляції τ_c. Зазначений параметр характеризує ширину АКФ сигналу. У світлі визначення АКФ будемо вважати, що копії сигналу, які зсунуті в часі на величину $\tau < \tau_C$, мають значну схожість, тоді як при $\tau < \tau_C$ їх схожість зневажливо мала. Зазначене дозволяє зробити висновок: сигнали з вузькою АКФ, тобто малим часом кореляції, є кращими для здійснення точного оцінювання з часової затримки.

Таким чином, якщо визначено закон внутрішньої кутової модуляції, що забезпечує час кореляції сигналу значно менше його тривалості, тобто $\tau_c << T$, тоді автокореляційна функція сигналу має яскраво виражений гострий характер, забезпечуючи високу точність оцінювання часової затримки, незважаючи на велику тривалість самого сигналу T . Але з урахуванням існуючої залежності між часом кореляції τ_C і смугою W частот ($\tau_C \approx 1/W$) нерівність $\tau_C << T$ означає, що сигнал характеризується великим значенням частотно-часового добутку $WT >> 1$, тобто є сигналом з розподіленим (широким) спектром. Тоді стає очевидним, що залучення технології розподіленого спектра дозволяє зняти протиріччя між величиною миттєвої потужності і точністю оцінювання: необхідна енергія вкладається в сигнал за рахунок його тривалості, а не потужності, тоді як висока точність вимірювання досягається завдяки синтезу систем сигналів з відповідним законом модуляції.

В [6] вказані принципово досяжні значення максимальних бічних піків періодичної функції автокореляції (межі «щільної упаковки») для заданого періоду послідовності N :

$$\rho \geq \begin{cases} 0, \text{если } N \equiv 0 (\text{mod } 4); \\ 1, \text{если } N \equiv 1 (\text{mod } 4); \\ 2, \text{если } N \equiv 2 (\text{mod } 4); \\ -1, \text{если } N \equiv 3 (\text{mod } 4), \end{cases} . \quad (16)$$

Наведені в (12) межі «щільної упаковки» встановлюють критерій синтезу безлічі ДП. Ансамблі з відповідним законом модуляції, зі значеннями кореляції, що досягають межі (12), є оптимальними за критерієм кореляційного піку, і називаються мінімаксними.

Аналіз [2, 5 – 6] показав, що на сьогодні відсутні регулярні методи синтезу ДП оптимальних за мінімаксним критерієм. Завдання синтезу ДП виявляється ще складнішим, якщо висуваються вимоги до розмірності (об'єму) системи сигналів, структурним властивостям і числу елементів ДП. Таким чином, досить актуальною проблемою залишається пошук ефективних методів синтезу дискретних сигналів (послідовностей), що відповідають потенційно можливим граничним характеристикам кореляційних функцій (границі «щільної упаковки») і володіють необхідними кореляційними, структурними, ансамблевими властивостями.

Хорошим інструментом для оцінки нижньої границі кореляції ρ KN векторів (K – число користувачів в системі, N – число елементів (період) ДП) є границя Велча [7]. Для числа $K > 2$ маємо

$$\rho \geq [K - 1/\, NK - 1]^{1/2}. \tag{17}$$

Ця нерівність визначає фундаментальну нижню границю, нижче якої кореляція між усіма циклічними копіями всіх K ДП (сигнатур), включаючи власні копії кожної сигнатури, опуститися ніколи не може. При числі користувачів близько десяти або більше ця версія границі Велча має вид

$$\rho \geq 1/\, N, K >> 1 \tag{18}$$

Таким чином, у відповідність з (16) – (18) для відповідних значень періоду сигналів можуть бути встановлені межі значень функцій кореляції і здійснюватися відбір сигналів, значення бічних пелюсток функції кореляції яких, не перевищує ці границі.

Для ідеального гіпотетичного ансамблю максимальні значення кореляційних функцій авто- і взаємної кореляції дорівнюють нулю, а для будь-якого реального ансамблю – може служити адекватною мірою його близькості до ідеального.

До числа ансамблів сигналів, які відповідають умовам (16) – (18), можна віднести нелінійні характеристичні дискретні сигнали, нелінійні криптографічні дискретні сигнали, багатофазні сигнали; троїчні сигнали, бінарні послідовності з непротилежною модуляцією та ін.

Побудова характеристичних сигналів (ХС) [6] базується на використанні характеру ψ мультиплікативної групи поля $GF(p^n)$ для $N = 4x + 2 = p^n - 1$ і $N = 4x = p^n - 1$. Правила кодування ХС приводять до коду з дворівневою періодичною функцією автокореляції з значеннями максимальних бічних функції автокореляції: $\mathrm{R}_\mu = \{-2, 2\}$, та $\mathrm{R}_\mu = \{0, -4\}$.

Об’єм системи характеристичних сигналів визначається зі співвідношення

$$M = \phi(L)/\, n, \tag{19}$$

де n – ступінь розширення поля Галуа.

Під криптографічними дискретними сигналами (КС) пропонується розуміти сукупності послідовностей (векторів) символів певного алфавіту, які обов’язково мають необхідні (задані) структурні, ансамблеві та кореляційні властивості, часову та просторову складності та можливості формування на основі ключів. Правила побудови КС [8] грунтуються на використанні випадкових чи псевдовипадкових процесів (в тому числі, методів криптографічного перетворення). КС повинні володіти: абсолютною структурною скритністю щодо законів їх формування та зміни сигналів в динамічному режимі; поліпшеними ансамблевими властивостями (існувати практично для будь-якого значення періоду, мати значний обсяг системи сигналів); необхідними (для забезпечення заданого значення завадостійкості прийому) кореляційними властивостями. Для захищених радіоканалів використання системи сигналів визначається додатками, в яких вони застосовуються. Зокрема, це можуть бути як окремі

сигнали або пари сигналів, так і великі безлічі дискретних сигналів з необхідними, але об'єктивно обмеженими значеннями «щільної упаковки», авто- і взаємно-кореляційними, ансамблевими властивостями.

Результати досліджень властивостей нелінійних ХС та нелінійних КС наведено в [9] і [10 – 15] відповідно. З точки зору границь «щільної упаковки» (16), ХС та КС можуть бути віднесені (за мінімаксним критерієм) до оптимальних сигналів.

Крім важливості застосовування у ряді додатків ІКС оптимальних сигналів в якості сигналів – фізичних переносників інформації, при вирішенні задач синхронізації (процеси пошуку, супроводження), оцінки параметрів сигналів, доцільним є застосування сигналів, які мають нульові значення піків кореляції поблизу центрального піку (області найбільшої кореляції τ_c).

В табл. 1 – 3 наведено приклади ізоморфізмів ХС та КС з числом елементів $N = 256$ і $N = 1020$ зі значеннями нульових бокових піків кореляції поблизу центрального піку ПФАК для цих сигналів. На рис. 2 – 5 наведено (у відповідності до табл. 1 – 3) вид ПФАК для ХС та КС з числом елементів $N = 256$ і $N = 1020$.

Таблиця 1

№	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, 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, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 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, -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, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 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, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 256]
2	[-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, 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, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 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, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 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, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 256]

Таблиця 2

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, 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, -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, -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,	[1020, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 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, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, - 4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, - 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 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, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, - 4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 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, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, - 4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 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, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0,

-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]	0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 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, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 1020]

Таблиця 3

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]	[256, 0, 0, 0, 0, -8, 20, -20, 8, 20, -16, -8, 8, -8, -16, -8, 20, 4, 24, -20, 16, 20, -8, 4, 28, 4, -8, 16, -20, 12, -28, -32, 0, 8, -4, -4, 0, -8, 16, 16, 16, 16, -8, -8, 12, 28, -16, 24, -16, 0, 0, -24, -12, 12, -12, 0, 24, -12, -8, -16, -24, 20, 12, -4, 0, 20, 4, 20, 8, -16, -12, -12, -4, -28, 12, -20, 12, 8, 24, -12, 0, -4, 4, 8, -12, -12, -4, -8, 24, -12, 0, -8, 0, -16, -8, -28, 0, -24, -24, 8, 24, 4, 0, -20, 0, -4, 8, -28, -8, -16, -12, -4, 4, -20, 0, 16, -4, 16, 0, -24, -16, 0, 4, 28, 16, 4, -4, -8, -4, -8, -4, 4, 16, 28, 4, 0, -16, -24, 0, 16, -4, 16, 0, -20, 4, -4, -12, -16, -8, -28, 8, -4, 0, -20, 0, 4, 24, 8, -24, -24, 0, -28, -8, -16, 0, -8, 0, -12, 24, -8, -4, -12, -12, 8, 4, -4, 0, -12, 24, 8, 12, -20, 12, -28, -4, -12, -12, -16, 8, 20, 4, 20, 0, -4, 12, 20, -24, -16, -8, -12, 24, 0, -12, 12, -12, -24, 0, 0, -16, 24, -16, 28, 12, -8, -8, 16, 16, 16, 16, -8, 0, -4, -4, 8, 0, -32, -28, 12, -20, 16, -8, 4, 28, 4, -8, 20, 16, -20, 24, 4, 20, -8, -16, -8, 8, -8, -16, 20, 8, -20, 20, -8, 0, 0, 0, 0, 256]

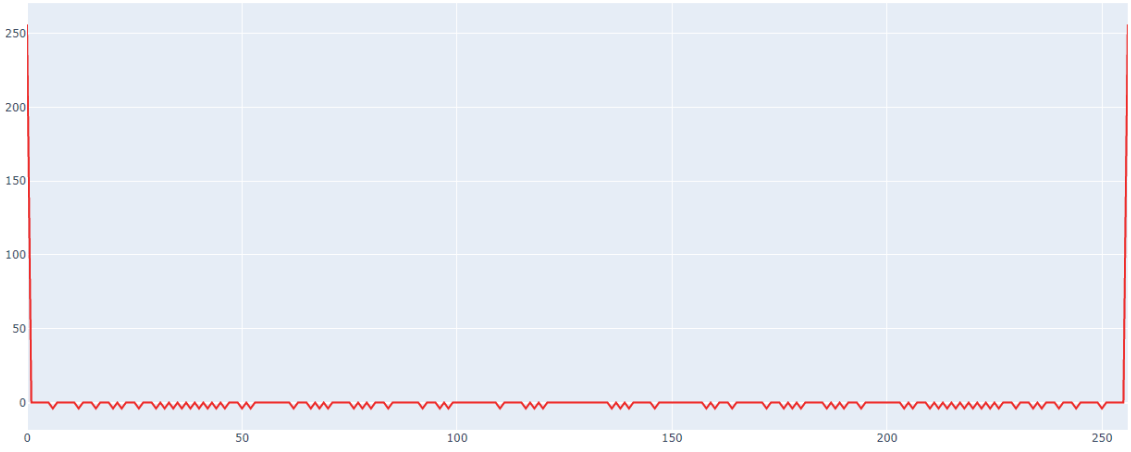

Рис. 2. Вид ПФАК для ХС з $N = 256$ (табл. 1, №1)

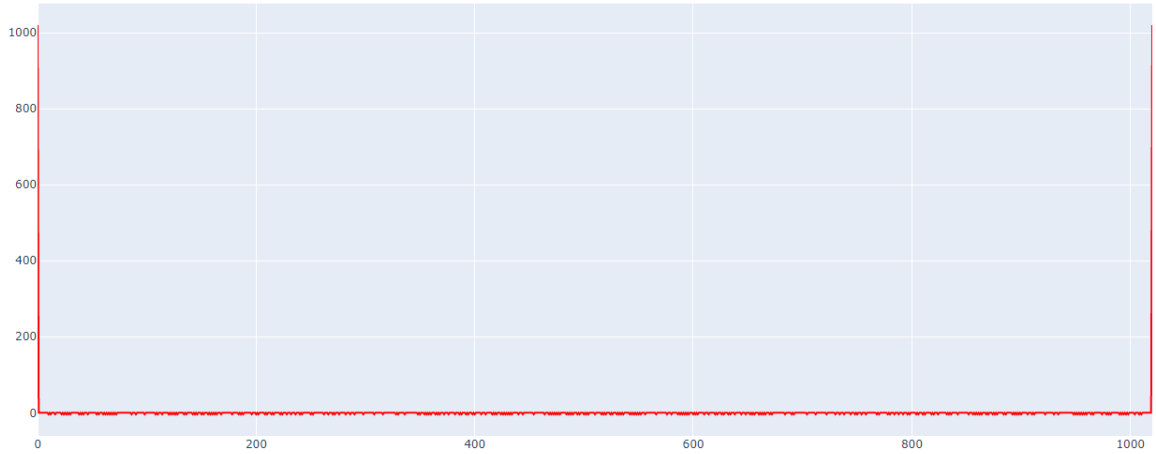

Рис. 3. Вид ПФАК для ХС з N = 1020 (табл. 2)

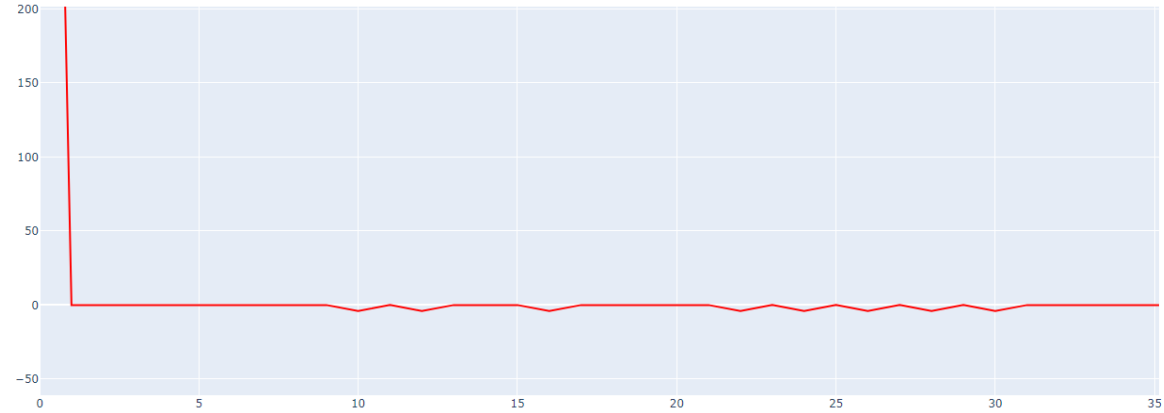

Рис. 4. Збільшений фрагмент ПФАК (щодо рис. 2), який свідчить про наявність нульових піків ПФАК в області найбільшої кореляції τ_c

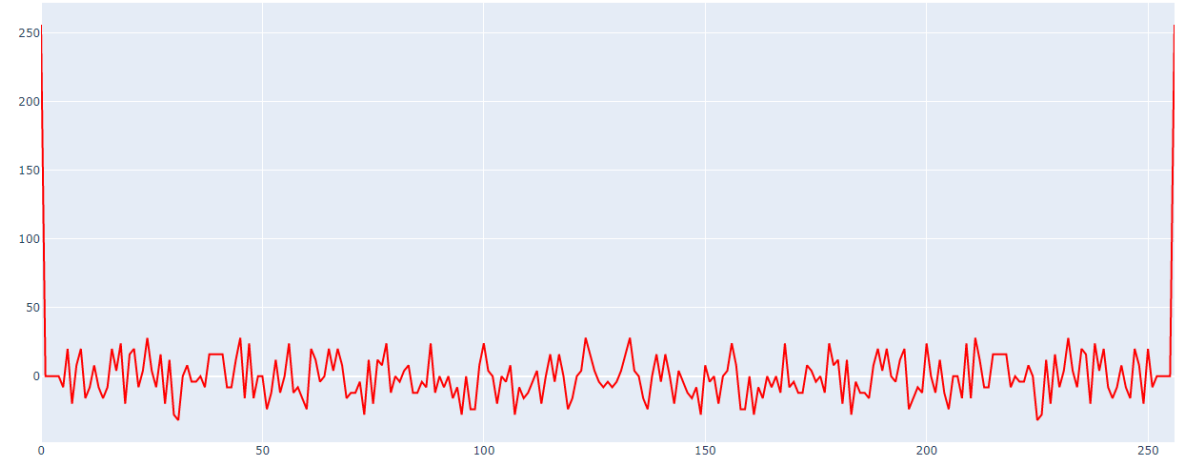

Рис. 5. Вид ПФАК для КС з N = 256 (табл. 3)

При побудові захищених ІКС загального та спеціального призначення, для яких в якості основних вимог висуваються вимоги забезпечення конфіденційності інформаційного обміну, цілісності даних, завадостійкості прийому сигналів, захищеності від нав'язування хибних повідомлень, важливими завданнями, які потребують вирішення, є пошук методів синтезу, формування і обробки ансамблів сигналів, які володіють покращеними не тільки кореляцій-

ними, а й ансамблевими, структурними (в сенсі складності визначення (стороною протидії) закону (правила) побудови таких сигналів, технологічними та іншими властивостями.

В табл. 3 наведено дані відносно ансамблевих і кореляційних властивостей КС, в тому числі, зазначено кількість сигналів, що мають нульові значення бокових піків функцій автокореляції в області максимальної кореляції. Як випливає з даних табл. 3, КС володіють суттєво покращеними у порівнянні з лінійними класами сигналів ансамблевими властивостями. Так, ансамбль КС з числом елементів 256, сигнали якого задовольняють границі «щільної упаковки», більш ніж на порядок перевищує ансамбль, складений з лінійних сигналів, отриманих на основі M -послідовностей. Крім того, КС, як показали результати проведеного тестування [15], за своїми статистичними властивостями, близькі до властивостей випадкових послідовностей, тобто володіють практично ідеальною структурної скритністю, що дає можливість поліпшити показники інформаційної безпеки функціонування ТКС. До ансамблю КС з періодом 256 елементів входить 302 сигналів, для яких бічні піки ПФАК мають один і більше нульових викидів функції кореляції поблизу центрального піку.

Таблиця 4

Число елементів КС (N)	Граничні значення (границя «щільної упаковки»)	ПФАК			
		Число КС, що задовольняють границі «щільної упаковки»	Найменше значення $R6_{max}$, що досягається для КС з числом елементів N	Кількість КС з найменшим значенням $R6_{max}$	Кількість КС, які мають один або більше нульових піків ПФАК в області найбільшої кореляції
64	17	9545	8	14	2041
256	33	680	28	48	81
256	36	2940	28	48	302
1024	80	247	72	3	7
1024	90	2209	72	3	123
2048	129	409	116	12	39

Висновки

На основі застосування мінімаксного критерію запропоновано методи пошуку оптимальних нелінійних дискретних складних сигналів для низки додатків ІКС загального та спеціального призначення при вирішенні задач теорії оптимального прийому, зокрема, виявлення сигналу, розрізнення сигналів, оцінка параметрів сигналів. Показано, що застосування запропонованих систем сигналів дозволить поліпшити показники завадостійкості прийому сигналів, точності оцінки параметрів сигналів, інформаційної безпеки та скритності функціонування ІКС в умовах кібератак, дії природніх та організованих, в тому числі, структурних, ретрансльованих і інших завад.

Список літератури:

1. Sarvate D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Parsley // IEEE Trans. Commun. 1980. Vol. Com 68 P. 59–90.

2. Варакин Л. Е. Системы связи с шумоподобными сигналами 1985. 384 с.

3. Gorbenko I.D., Zamula A. A., Morozov V. L. Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts // Telecommunications and Radio Engineering. 2017. Vol. 76, Issue 19. P. 1705-1717 DOI: 10.1615/TelecomRadEng.v76.i19.30.

4. Gorbenko I., Zamula A., Morozov V. Information and communication systems based on signal systems with improved properties building concept // Workshop Proceedings 2019 CEUR.

5. Ipatov V. Spread Spectrum and CDMA. Principles and Applications / University of Turku, Finland and St. Petersburg Electrotechnical University 'LETI', Russia // John Wiley & Sons Ltd. The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. 2005. 385 p.

6. Свердлик М.Б. Оптимальные дискретные сигналы. Москва : Сов. радио, 1975. 200 с.

7. Welch L. R. Lower bound on the maximum cross-correlation of signals // IEEE Trans. Inform. Theory. 1974. Vol. 20. P. 397-399.

8. Gorbenko I., Zamula A. Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems // Telecommunications and Radio Engineering. 2017. Vol.76, Issue 12. P. 1079-1100. DOI: 10.1615/TelecomRadEng.v76.i12.50.

9. Горбенко І.Д., Замула О.А., Хо Чі Лик Оптимізація пошуку дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно-комунікаційних системах // Математичне та комп'ютерне моделювання. Серія: Техн. науки : Зб. наук. праць / Ін-т кібернетики імені В.М. Глушкова Національної академії наук України, 2019. Вип. 19. 160 с.

10. Горбенко І.Д., Замула О.А., Хо Чі Лик Оптимізація синтезу нелінійних дискретних складних сигналів з визначеними властивостями // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали дев'ятої міжнародної науково-технічної конференції. 11-12 квітня 2019. С. 5-6.

11. Горбенко И.Д., Замула А.А. Аналитическая оценка значений максимальных боковых выбросов функций корреляции сложных нелинейных дискретных сигналов // Радиотехника. 2017. Вып. 191. С. 76 88.

12. Замула А.А. Перспективы применения нелинейных дискретных сигналов в современных телекоммуникационных системах и сетях / Замула А.А., Семенко Е.А // Системи обробки інформації. Харків : ХУПС, 2015.

13. Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. 2016. Vol. 75, Issue 2. P. 169-178. DOI: 10.1615/TelecomRadEng.v75.i2.60.

14. Methods for implementing communications in info-communication systems based on signal structures with specified properties / I. Gorbenko, A. Zamula, V. Morozov // 2017 4th International Scientific-Practical Conference Problems of Info communications Science and Technology, PIC S and T 2017 Proceedings. DOI: 10.1109/INFOCOMMST.2017.8246359.

15. Gorbenko I., Zamula A., Morozov V. Information and communication systems based on signal systems with improved properties building concept systems with improved properties building concept 2019 CEUR Workshop Proceedings.

АТ «Інститут інформаційних технологій»;
Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 15.02.2020