УДК 621.391 **DOI:10.30837/rt.2021.1.204.03**

І.Д. ГОРБЕНКО, д-р техн. наук, О.В. ПОТІЙ, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук

КОНЦЕПЦІЯ СИНТЕЗУ ОДНОГО КЛАСУ САМОСИНХРОНІЗУЮЧИХ ДИСКРЕТНИХ СИГНАЛІВ

Вступ

Відомо, що для мінімізації помилки при прийомі сигналів в широкосмугових комунікаційних системах (ШКС) відстань між векторами (сигналами) слід робити максимально великою [1]. У разі досить великої кількості сигналів завдання одночасної максимізації відстаней між усіма сигналами може виявитися складним, оскільки сигнали конфліктують між собою, «відсуваючи» один вектор від іншого, наближаючи його до деякого третього. Завдання побудови безлічі максимально віддалених сигналів входить в клас так званих завдань «упаковки». Очевидно, що для максимізації відстані між двома векторами їх слід вибирати протилежними. Саме ця умова забезпечує максимально досяжну ймовірність помилки при передачі двійкових даних сигналами з фіксованою енергією.

До теперішнього часу немає єдиної теорії синтезу систем дискретних сигналів (ДС) з заданими авто-, взаємно-, стиковими кореляційними властивостями. По суті, до сьогоднішнього дня в основному розвинена теорія аналізу і синтезу двійкових лінійних рекурентних послідовностей максимального періоду (ЛРПМ) і лінійних рекурентних послідовностей з трирівневою функцією взаємної кореляції (ЛРПТ) [1]. Однак, як показали дослідження [1, 2], введення жорстких обмежень на вид періодичної функції автокореляції (ПФАК) ДС суттєво обмежує можливість джерел сигналів з точки зору ансамблевих і структурних властивостей, а також, в більшості випадків, визначає лінійність законів їх формування. Авторами вперше отримано методи синтезу нового класу нелінійних складних дискретних сигналів – криптографічних сигналів [3 – 7]. Використання такого класу сигналів в якості фізичних переносників даних в комунікаційних системах, завдяки їх особливим ансамблевим, кореляційним, структурним і іншим властивостям, дозволяє поліпшити показники ефективності функціонування таких систем, зокрема інформаційної безпеки та завадозахищеності [8 – 10]. При цьому, кращим є вибір так званих, самосинхронізуючих систем сигналів (ССС) як переносників даних в комунікаційних системах. Використання таких систем сигналів передбачає реалізацію циклової синхронізації в режимі розрізнення сигналів безпосередньо за інформаційними сигналами. При проектуванні і використанні багатокористувачевих комунікаційних систем важливо застосовувати сигнали з максимальним індексом самосинхронізації, який визначається як максимальна відстань між всілякими стиковими словами і всіма інформаційними сигналами.

Основні результати досліджень

Сформулюємо в загальному вигляді, на основі комплексного використання апарату теорії поля Галуа, різницевих множин, комбінаторики, а також теорії чисел та наведемо рішення задачі синтезу ССС.

Нехай джерело ДС Q_W, що володіє з максимальною ентропією $H(Q_W) = \log P^L$, видає L – значні над полем $GF(P)$ дискретні послідовності (ДП) символів, закон формування яких задається t-мірними функціями N_p і f, що входять у вираз (1).

Простір станів каналу ШКС може бути описано функціоналом:

$$\psi = \varphi(L, N, \rho, R_a, R_b, R_H, R_C, D, x, y, S, I, N_p, f) \ , \qquad (1)$$

де L – безліч функцій, що описують закони розподілу тривалості сигналів L_i в словниках $\{W_j\}, i = \overline{1, N}$, ρ – безліч функцій, що описують закони розподілу величин бічних піків апері-

одичних і періодичних функцій взаємної кореляції (АФВК та ПФВК, відповідно); D – функції взаємної невизначеності (ФВН); x, y – безліч функцій, що описують різницю значень максимальних піків функції кореляцій щодо числа символів L_i дискретної послідовності; S – безліч функцій, що описують структурну скритність сигналів; I – безліч функцій, що описують імітостійкість системи, N_p і f – функції, що визначають алгоритм побудови ДП; R_a, R_b, R_H – значення бічних піків авто-, взаємної і стикової функції кореляції відповідно.

Рішення задачі синтезу сигналів з максимальним індексом самосинхронізації може бути засноване на використанні ітераційного рішення систем нелінійних параметричних нерівностей.

Введемо поняття абсолютної «розмитості» систем і сигналів $\{k^j\}$ при $j=\overline{1,N}$.

Система сигналів $\{x^j\}$ є абсолютно «розмитою» за автозгорткою, якщо відносні значення функцій кореляцій векторів (сигналів) $R'_{a_1}(k)$, $R'_{a_2}(k)$, $R'_{b_1}(k)$, $R'_{b_2}(k)$ не погіршуються при зміні x в інтервалі

$$L-x_2 \le k \le L+x_1. \tag{2}$$

Розмитість сигналів будемо представляти сукупністю систем нелінійних нерівностей (СНН):

$$\begin{aligned}
&R_{a_1}(k) \le \sum_{i=\delta}^{L-K} W_i^{\vartheta}(W_{i+k}^{\vartheta})^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta}(W_{i-L+K}^{\vartheta})^* + \sum_{i=1}^{L-K} W_i^{\vartheta}(W_{i+K}^{\vartheta}) + \\
&+ \sum_{i=L-K+1}^{L} W_i^{\vartheta}(W_{i-L+K}^{\vartheta})^* + \sum_{i=1}^{x_1-L+\vartheta} W_i^{\vartheta}(W_{i+K}^{\vartheta})^* \le R'_{a_2}(k);\ k=\overline{0,L+x_2}, \qquad \text{а)} \\
&R_{a_1}(k) \le \sum_{i=\delta}^{L-K} W_i^{\vartheta}(W_{i+k}^{\vartheta})^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta}(W_{i-L+K}^{\vartheta})^* + \sum_{i=1}^{L-K} W_i^{\vartheta}(W_{i+K}^{\vartheta}) + \\
&+ \sum_{i=L-K+1}^{L} W_i^{\vartheta}(W_{i-L+K}^{\vartheta})^* \le R'_{a_2}(k);k=\overline{0,L+x_1}, \qquad \text{б)} \\
&R_{a_2}(k) \le \sum_{i=1}^{L-x_1} W_i^{\vartheta}(W_{i-k}^{\vartheta})^* \le R'_{a_2}(k),\ k=\overline{0,L-x_2}, \qquad \text{в)} \\
&R_{a_1}(k) \le \sum_{i=L-\delta}^{L-K} W_i^{\vartheta}(W_{i+k}^{\vartheta})^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta}(W_{i-L+K}^{\vartheta})^* + \\
&+ \sum_{i=1}^{L-x_2-\vartheta} W_i^{\vartheta}(W_{i+K}^{\vartheta})^* \le R'_{a_2}(k), k=\overline{0,L-x_2}, \qquad \text{г)}
\end{aligned} \tag{3}$$

де $R'_{a_1}(k)$ та $R'_{a_2}(k)$ – різні реалізації ПФАК, які задають при синтезі сигналів.

У разі розмитості за ПФВК та стикової функції взаємної кореляції (СФВК) у інтервалі k, який визначається як: $L-x_2 \le k \le L+x_1$, різниця може бути задана як сукупність СНН виду:

$$\begin{aligned}
&R'_{b_1}(k) \le \sum_{i=\delta}^{L-K} W_i^{q}(W_{i+k}^{\vartheta_1})^* + \sum_{i=L-k+1}^{L} W_i^{q}(W_{i-L+K}^{\delta_2})^* + \sum_{L=1}^{L-K} W_i^{p} \times (W_{L+K}^{\vartheta_2})^* + \\
&+ \sum_{i=L-K+1}^{L} W_i^{p}(W_{i-L+K}^{\vartheta_3})^* + \sum_{i=1}^{L-K} W_i^{r} \times (W_{i+K}^{\vartheta_3})^* \le R'_{b_2}(k);k=\overline{0,L+x},
\end{aligned} \qquad \text{а)}$$

$$R'_{b_1}(k) \le \sum_{i=\delta}^{L-K} W_i^q (W_{i+k}^{\vartheta_1})^* + \sum_{i=L-k+1}^{L} W_i^q (W_{i-L+K}^{\delta_2})^* + \sum_{L=1}^{L-K} W_i^p \times (W_{L+K}^{\vartheta_2})^* +$$

$$+ \sum_{i=L-K+1}^{L} W_i^p (W_{i-L+K}^{\vartheta_3})^* \le R'_{b_2}(k); k = \overline{0, L+x}, \quad \text{б)} \qquad (4)$$

$$R'_{b_2}(k) \le \sum_{i=L-\delta}^{L-K} W_i^q * (W_i^{\vartheta_1} + k)^* \le R_{b_2}(k),\ k = \overline{0, L-x_2}, \quad \text{в)}$$

$$R'_{b_1}(k) \le \sum_{i=L-\delta}^{L-K} W_i^q (W_{i+k}^{\vartheta_2})^* + \sum_{i=L-k+1}^{L} W_i^q (W_{i-L+K}^{\delta_2})^* + \sum_{i=1}^{L-x_2-\delta} W_i^p (W_{i+K}^{\vartheta_2})^* \le R'_{b_2}(k), k = \overline{0, L-x_2}, \quad \text{г)}$$

Розглянемо спочатку теоретичні основи синтезу двох самосинхронізуючих сигналів (СС) x^q і x^p без внесення обмежень розмитості виду (3), (4), а потім зробимо ряд узагальнень на випадок синтезу N дискретних сигналів, що володіють, в тому числі, і розмитими властивостями. При цьому будемо вимагати, щоб ССС володіли ідеальними структурними властивостями, тобто такою структурної скритністю, що під час перехоплення і поелементній обробці будь-якого числа l символів сигналів не можна однозначно передбачити $L-1$ символів, що залишилися. Це може бути виконано, якщо символи ССС незалежні і з'являються з однаковою ймовірністю [11].

Запишемо умови, що визначають деякі граничні умови, яким повинні задовольняти авто- і взаємно кореляційні властивості сигналів x^q і x^p:

$$\xi^1_{a_1}(l) \le \sum_{i=1}^{L} x_i^q \times (x_{i+1}^q)^* \le \xi_{a_2}(l), l = \overline{0, L'}, \quad \text{а)}$$

$$\xi^2_{a_1}(l) \le \sum_{i=1}^{L} x_i^p \times (x_{i+1}^p)^* \le \xi_{a_2}(l), l = \overline{0, L'}, \quad \text{б)}$$

$$\xi^1_{a_1}(l) \le \sum_{i=1}^{L-K} x_i^q \times (x_{i+1}^q) + \sum_{i=L-K+1}^{L-1} x_i^q \times (x_{i-L+K}^p)^* \le \xi^1_{b_2}(l), l = \overline{1, L-1}, \quad \text{в)}$$

$$\xi^2_{b_1}(l) \le \sum_{i=1}^{L-1} x_i^q \times (x_{i+l}^q) + \sum_{i=L-K+1}^{L-1} x_i^q \times (x_{i-L+K}^p)^* \le \xi^2_{b_2}(l), l = \overline{1, L-1}, \text{г)} \qquad (5)$$

$$\xi^3_{b_1}(l) \le \sum_{i=1}^{L-1} x_i^q \times (x_{i+l}^p) + \sum_{i=L-K+1}^{L-1} x_i^q \times (x_{i-L+K}^q)^* \le \xi^3_{b_2}(l), l = \overline{1, L-1}, \text{д)}$$

$$\xi^4_{b_1}(l) \le \sum_{i=1}^{L-1} x_i^p \times (x_{i+l}^p) + \sum_{i=L-K+1}^{L-1} x_i^p \times (x_{i-L+K}^q)^* \le \xi^4_{b_2}(l), l = \overline{1, L-1}, \quad \text{е)}$$

$$\xi^5_{b_1}(l) \le \sum_{i=1}^{L-1} x_i^p \times (x_{i+l}^q) + \sum_{i=L-K+1}^{L-1} x_i^p \times (x_{i-L+K}^p)^* \le \xi^5_{b_2}(l), l = \overline{1, L-1}, \quad \text{ж)}$$

Аналіз виразу (5) показує, що число різних білінійних форм визначає вирази:

$$C_r = 6L - 4, \text{ якщо } L \text{ – парне}, \qquad (6)$$

і

$$C_r = 6L - 5, \text{ якщо } L \text{ – непарне}. \qquad (7)$$

Підкреслимо, що вираз (5) визначає мінімальну сукупність систем нелінійних нерівностей, виконання яких дасть достатні умови побудови двох ДС x^q і x^p з заданими реалізаціями за ПФАК, ПФВК, СФВК.

Твердження 1 однозначно встановлює алгебраїчну структуру сукупності систем нелінійних нерівностей для випадку синтезу v сигналів.

Твердження 1. Нехай x^{υ}, $\upsilon=\overline{1,N}$ – є дійсні або комплексні послідовності символів, а $\xi^{j}_{a_1}(l),\xi^{j}_{a_2}(l),\xi^{i}_{b_1}(l),\xi^{i}_{b_2}(l)$, $j=\overline{1,N}, i=\overline{1,b^2_N}$ – реалізації авто- і взаємних згорток, тоді усі білінійні форми, що утворюють сукупність *N* систем нелінійних нерівностей, що визначені системами (5, а) і сукупність C^2_N систем нелінійних нерівностей (5, в) – (5, ж) не збігаються, а число різних білінійних форм визначається виразом:

якщо L –парне, то

$$C_r = N\left(\frac{N(5L-4)-4L+3}{2}\right), \tag{8}$$

якщо L – непарне, то

$$C_r = N\left(\frac{N(5L-4)-4L+4}{2}\right). \tag{9}$$

Сукупність систем (5) може бути представлена з використанням аперіодичних авто- і взаємних згорток $C^{qp}(l)$, якщо аперіодична згортка є

$$C^{qp}(l)=\sum_{j=0}^{L-1+l} x^q_j (x^p_{j+l})^*, \text{ якщо } \ 0\le l\le L-1, \tag{10}$$

$$C^{qp}(l)=\sum_{j=0}^{L-1+l} x^q_{j-e} (x^p_{j+l})^*, \text{ якщо } 1-N\le l\le 0, \text{ та} \tag{11}$$

$$\text{якщо } |l|\ge N.$$

Тоді, застосовуючи (11), система (10) прийме вид:

$$\begin{cases} \xi^1_{a_1}(l)\le c^{q,q}(l)+c^{q,q}(L-l)\le \xi^1_{a_2}(l), l=\overline{1,L}; \\ \xi^2_{a_1}(l)\le c^{p,p}(l)+c^{p,p}(L-l)\le \xi^2_{a_2}(l), l=\overline{1,L}; \\ \xi^1_{b_1}(l)\le c^{q,p}(l)+c^{q,p}(L-l)\le \xi^1_{b_2}(l), l=\overline{0,L-1}; \\ \xi^2_{b_1}(l)\le c^{q,p}(l)+c^{q,p}(L-l)\le \xi^2_{b_2}(l), l=\overline{0,L-1}; \\ \xi^3_{b_1}(l)\le c^{q,p}(l)+c^{q,q}(L-l)\le \xi^3_{b_2}(l), l=\overline{0,L-1}; \\ \xi^4_{b_1}(l)\le c^{p,p}(l)+c^{p,q}(L-l)\le \xi^4_{b_2}(l), l=\overline{0,L-1}; \\ \xi^5_{b_1}(l)\le c^{q,p}(l)+c^{p,p}(L-l)\le \xi^5_{b_2}(l), l=\overline{0,L-1}. \end{cases} \tag{12}$$

У (12) l приймає ті ж значення, що і в системі (11). Система (12) є аналогом систем (10) і, в разі відсутності вимог розмитості векторів x^q і x^p, являє собою сукупність систем нелінійних нерівностей, кожне з яких є сумою аперіодичних згорток або в часовій області, або в області узагальнених теоретичних перетворень. Останнє дозволить підвищити обчислювальну ефективність як у випадку синтезу, так і при розкритті закону формування сукупності використовуваних кодових форм.

Зокрема розглянемо можливості подання систем (5) з використанням аперіодичної згортки. Введемо поняття усіченої аперіодичної згортки, визначивши її як

$$C^{q,p}_{\delta}=\begin{cases} \sum_{j=\delta}^{L-1-l} x^q_j (x^p_j+e)^*, \text{ при } \upsilon<l<L-\delta-1; \\ 0, \text{ при } l\ge L-\delta. \end{cases} \tag{13}$$

Тоді (4) як найбільш загальна сукупність систем, що включає, зокрема і (3), з урахуванням (13), має вид

$$\begin{cases} R_{b_1}(k) \le C_{\delta}^{q,v_1}(l-k-1) + C_{\delta}^{q,v_2}(L-l) + C_{\delta}^{p,v_2}(l) + \\ C_{\delta}^{p,v_3}(L-l) + C_{\delta}^{r,v_3}(L-l) \le R_{b_2}(k), k = \overline{0, L+X_1}; \ \text{а)} \\ R_{b_1}(k) \le C_{\delta}^{q,v_1}(l-k-1) + C_{\delta}^{q,v_2}(L-l) + C_{\delta}^{p,v_2}(l) + \\ C_{\delta}^{p,v_3}(L-l) \le R_{b_2}(k), k = \overline{0, L+X_1}; \ \text{б)} \\ R_{b_1}(k) \le C_{L-\delta}^{q,v_1}(l-\delta-1) \le R_{b_2}(k), k = \overline{0, L-X_2}; \ \text{в)} \\ R_{b_1}(k) \le C_{L-\delta}^{q,v_1}(l-\delta-1) + C_{\delta}^{q,v_2}(L-l) + \\ C_{\delta}^{p,v_2}(l), k = \overline{0, L-X_2}. \ \text{г)} \end{cases} \quad (14)$$

В (14) відсутні обмежень на область уявлення аперіодичних згорток в часовій області або в області узагальнених теоретичних перетворень.

З порівняння сукупності систем (14) випливає, що білінійні форми (14, а) відрізняються від білінійних форм (14, б) складовою $C_{\delta}^{r,v_s}(l)$, а (14, г) від (14, в) складовими $C_{\delta}^{q,v_2}(L-l) + C_{\delta}^{p,v_2}(l)$.

Зазначену властивість може бути використано при оптимізації процедур визначення закону побудови форм застосовуваних сигналів (векторів) ω^{ϑ}.

Висновки

Аналіз показав, що до теперішнього часу не існує математичного апарату рішення систем нелінійних нерівностей (СНН) другого порядку виду (5). Ще більш жорсткі обмеження на можливість вирішення сукупності такого роду систем накладаються функціоналом (1). На наш погляд, з урахуванням відсутності регулярних (однозначних) обмежень, що вводяться для забезпечення відповідних значень скритності S джерела сигналів Q_W і імітостійкості І передачі даних в (1), єдиним математичним апаратом, що застосовується до вирішення даної задачі, є апарат теорії дослідження операцій і, зокрема, методи нелінійного, динамічного і схоластичного цілочисельного програмування. Дійсно, функціонал (1) можна розглядати як цільову функцію, яка залежить від керованих і некерованих функцій, значення (реалізації) яких можуть визначатися фізичною реалізуємістю ССС із заданими властивостями. Аналіз можливих методів рішень задачі синтезу досліджуваних в даній роботі сигналів показує, що вони повинні відноситися до методів типу «укладання ранця», процедура рішень для яких вимагає значних і, за деяких умов, нескінченних ресурсів.

Сформульовано і у загальному виді вирішено задачу синтезу класу сигналів із заданими кореляційними, ансамблевими і структурними властивостями, а також властивостями «розмитості» за кореляційними характеристиками. Зазначена властивість («розмитість») означає, що збільшення або зменшення довжини дискретного сигналу не змінює кореляційні властивості дискретної послідовності, на основі якої синтезовано сигнал. Застосування безлічі зазначених систем сигналів в сучасних інформаційно-комунікаційних системах дозволить поліпшити показники ефективності функціонування таких систем, насамперед, завадозахищеності, скритності функціонування, інформаційної безпеки, завадостійкості прийому сигналів.

Список літератури:

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

2. 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.

3. Горбенко І.Д., Замула О.А. Моделі та методи синтезу криптографічних сигналів та їх оптимізація за критерієм часової складності // Математичне та комп'ютерне моделювання. Сер.: Фізико-математичні науки: зб. Наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2017. Вип. 15. 272 с.

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

5. Gorbenko I.D., Zamula A.A. Theoretical bases of synthesis of quasi-orthogonal systems of complex signals // Радіотехніка. 2020. Вип. 200. С. 162 – 175.

6. Gorbenko I., Zamula A., Ho L., Rodionov S. Derived signals systems for information communication systems applications: synthesis, formation, processing and properties // Problems of Info communications Science and Technology (PIC S and T). Proceedings of 2020 International Scientific-Practical Conference, 6–9 Oct. 2020. Kharkiv : KNURE, 2020. P. 13-20.

7. ISCI'2020: Information Security in Critical Infrastructures. Collective monograph / Edited by Ivan D. Gorbenko, Victor A. Krasnobayev and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2020, 308 p. – ISBN: 978-1-7362833-0-1 (Hardback). ISBN: 978-1-7362833-1-8 (Ebook).

8. Gorbenko I., Zamula A., Morozov V. Information and communication systems based on signal systems with improved properties building concept // Workshop Proceedings 2019 CEUR, 2353, с. 974-991.

9. Gorbenko I.D., Zamula A.A., Ho Tri Luk. Synthesis of derivatives of complex signals based on nonlinear discrete sequences with improved correlation properties // Радіотехніка. 2019. Вип. 199. С. 110-120.

10.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, pages 1705-1717 DOI: 10.1615/TelecomRadEng.v76.i19.30.

11.Горбенко І.Д. Прикладна криптологія : монографія / І.Д. Горбенко, Ю.І. Горбенко. Харків : Форт. 2012. 868 с.

Надійшла до редколегії 03.02.2021

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ «Інститут інформаційних технологій», головний конструктор; Україна; e-mail: GorbenkoI@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449

Потій Олександр Володимирович – д-р техн. наук., професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації; Україна; e-mail: potav@ua.fm; ORCID: https://orcid.org/0000-0002-2366-0541

Замула Олександр Андрійович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; email: zamylaaa@gmail.com; ORCID: http://orcid.org/0000-0002-8973-6190