5. Самарский А. А., Вабищевич П. Н. Численные методы решения обратных задач математической физики. М.: Едиториал УРСС, 2004. 480 с.
6. Гладкий А. В. Исследование и оптимизация волновых процессов в неоднородных средах с импедансной границей. *Кибернетика и системный анализ*. 2013. № 2. С. 94–105.
7. Гладкий А. В., Гладкая Ю. А. Об одной задаче управления в средах с условиями неидеального сопряжения. *Компьютерная математика*. 2016. № 1. С. 3–9.

The problems of numerical modeling and formation of acoustic fields on the basis of parabolic wave equation in an inhomogeneous waveguide with subtle inclusions is considered. Criterion of optimality is formulated. Differential properties of the proposed quality functional are investigated. A numerical method for modelling and optimization of acoustic fields is proposed.

Key words: *acoustic field, Schrödinger-type equation, extremal problem, difference scheme, stability.*

Одержано 20.02.2017

УДК 004.728:004.728.3,004.056.055

І. Д. Горбенко, д-р. техн. наук, професор,
О. А. Замула, д-р. техн. наук

Харківський національний університет імені В. Н. Каразіна, м. Харків

МОДЕЛІ ТА МЕТОДИ СИНТЕЗУ КРИПТОГРАФІЧНИХ СИГНАЛІВ ТА ЇХ ОПТИМІЗАЦІЯ ЗА КРИТЕРІЄМ ЧАСОВОЇ СКЛАДНОСТІ

Сформульована в загальному вигляді і вирішена задача синтезу та аналізу криптографічних дискретних сигналів методом «гілок і меж», зроблені пропозиції з оптимізації.

Ключові слова: *складений сигнал, структурна та інформаційна скритності, імітостійкість.*

Вступ. Множинний доступ з кодовим поділом абонентів в багатокористувацьких телекомунікаційних системах (ТКС) здійснюється за допомогою використання при розширенні спектру специфічних дискретних послідовностей. При цьому властивості ТКС залежать від кореляційних, структурних, ансамблевих та енергетичних властивостей дискретних сигналів [1–3].

Метою цієї статті є викладення основних теоретичних та практичних положень та проблемних питань побудови дискретних послідовностей, що названі криптографічними дискретними сигналами (КДС), які повинні мати задані кореляційні, структурні та ансамблеві властивості, будуватися за допомогою ключових даних.

1. Моделі дискретних криптографічних сигналів. Під криптографічними дискретними сигналами (КДС) 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 [1]. Правила побудови КДС грунтуються на використанні випадкових чи псевдовипадкові процесів, вони повинні відповідати вимогам випадковості, незворотності, непомітності та непередбачуваності [4–7].

Сформулюємо в загальному вигляді задачу синтезу КДС. Під задачею побудування (синтезу) КДС будемо розуміти задачу побудови підмножин дискретних послідовностей (W_l^q), $q = \overline{1, N}$, $l = \overline{1, L}$, сукупність яких утворює систему дискретних сигналів заданого алфавіту розмірності $M_k = N \times L$, таких, що в кожній із підмножин (словнику) виконуються умови, що висуваються до підмножини КДС в частині структурних, ансамблевих, кореляційних властивостей, просторової та часової складності їх генерування [1–3].

Побудова КДС грунтується на основі аналізу та використанні періодичних та аперіодичних функцій кореляції та зводиться до наступних етапів.

1. Забезпечення умов виконання вимог до структурних та ансамблевих властивостей, можливостей формування підмножини КДС з допустимою часовою та просторовою складністю, в тому числі з використанням ключів.
2. Побудова КДС W^q, періодична функція автокореляції (ПФАК) кожного з яких, задовольняє системі нелінійних параметричних нерівностей (НПН):

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

де $R_{a_1}^q(l)$ і $R_{a_2}^q(l)$ — задані значення реалізації ПФАК, а індекси обчислюються по модулю $(i + l)$ mod$L$.

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

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, q = \overline{1, N}. \tag{2}$$

3. Побудова пар КДС W^q та W^p, функції взаємної кореляції (ФВК) яких задовольняють вимогам, що визначаються сукупністю систем НПН:

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

$$R^{qp}_{b_{1,2}}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R^{qp}_{b_{2,2}}(l); \qquad (4)$$

$$R^{qp}_{b_{1,3}}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^q)^* \le R^{qp}_{b_{2,3}}(l); \qquad (5)$$

$$R^{qp}_{b_{1,4}}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^q)^* \le R^{qp}_{b_{2,4}}(l); \qquad (6)$$

$$R^{qp}_{b_{1,5}}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^p)^* \le R^{qp}_{b_{2,5}}(l), \qquad (7)$$

причому $l = \overline{1, L-1}$ для будь-яких поєднань q і p, $q = \overline{1, N}$, $p = \overline{1, N}$, $q \ne p$, де $R^{qp}_{b_{1,j}}(l)$ і $R^{qp}_{b_{2,j}}(l)$, задані (необхідні) реалізації ПФВК і СФВК відповідно, $j = \overline{1, 5}$, а також задовольняють вимогам до стикових функцій взаємної кореляції (СФВК) пар КДС W^q та W^p зі стиковими дискретними словами W^{qp} і W^{pq}.

В системах нелінійних параметричних нерівностей (1), (2) та (3)–(7) W_i^q та W_i^p є невідомими значеннями випадкових чи псевдовипадкових символів КДС W^q та W^p, $q = \overline{1, N}$, що належать визначенню в процесі їх побудови.

Проведемо аналіз систем нелінійних параметричних квадратичних нерівностей (далі систем) (1), (2) та (3)–(7), використовуючи введену модель.

Системи (4) та (6) при $l = L$ для усіх $q = \overline{1, N}$ мають дати повну згортку зі значенням L, тобто (4):

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, q = \overline{1, N}, \qquad (8)$$

а (2d) дає

$$\sum_{i=1}^{L} W_i{}^p W_{i+L}{}^p = \sum_{i=1}^{L} W_i{}^p W_i{}^p = L, p = \overline{1, N}, \qquad (9)$$

Системи (3), (5) та (7) при $l = L$ для усіх пар W^q та W^p дають значення функції взаємної кореляції при нульовому значенні зсуву відповідно вигляду:

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i{}^p = R^{qp}(0); q, p = \overline{1, N}, \qquad (10)$$

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i{}^p = R^{qp}(0), q, p = \overline{1, N}, \qquad (11)$$

$$\sum_{i=1}^{L} W_i^p W_{i+L}^q = \sum_{i=1}^{L} W_i^p W_i^q = R^{pq}(0),\ p,q = \overline{1,N}\ . \qquad (12)$$

В подальшому системи (1), (2), (3)–(7) та квадратичне рівняння (10) будемо називати моделлю підмножини (словника) КДС.

Проведемо аналіз систем (1), (2) на предмет існування рішень та незалежності. Безпосередньо із (1) маємо, що щодо кожного із q КДС W^q є L невідомих — $W_1^q, W_2^q \cdots W_L^q$. Для їх знаходження згідно (1) можна скласти систему із $L-1$ незалежних НПН. Далі, використовуючи (2), отримуємо ще один вираз, але уже рівняння.

Особливістю системи (1), (2) є те, що вона дає згортку кожного із КДС зі значенням L. На основі (1) та (2) при побудові кожної N підмножини КДС можна скласти N незалежних систем квадратичних НПН, кожна з яких буде містити $L-1$ квадратичних нерівностей вигляду (1) і формально одне рівняння, так що всього їх буде L.

Також проведемо аналіз сукупності систем параметричних нерівностей (3)–(7), з урахуванням (8)–(12), на предмет існування рішень та незалежності систем та окремих рівнянь. Системи (3)–(7) визначають допустимі взаємнокореляційні властивості щодо ПФВК та СФВК кожної пари КДС — W^q та W^p. Вони визначають вимоги щодо ПФВК та СФВК конкретно тільки двох КДС — W^q та W^p. При побудові трьох КДС будемо мати 3!/2 систем вигляду (3)–(7), а при N КДС відповідно — $N!/2$ таких систем. Таким чином, з ростом N число систем вигляду (3)–(7) збільшується експоненційно (по факторіалу).

Для $N = 2$ серед (8)–(12) систем НПН є збиткові нелінійні квадратичні рівняння. Рівняння (2) збігається з (8) та (9), тому останні два уже входять у систему (2), є залежними, тому не можуть бути використані. Далі, рівняння (10) та (11) збігаються, а, рівняння (12) є симетричним в частині кореляційної функції щодо рівнянь (10) та (11). Тому для кожної пари p та q незалежним є (10).

На основі детального аналізу маємо, що усі (3)–(7) системи НПН визначають різні реалізації ПФВК та СФВК конкретно тільки двох КДС — W^q та W^p. Тому математична модель побудови двох КДС W^q та W^p однозначно визначається п'ятьма системами НПН у вигляді (3)–(7), та, як уже було обгрунтовано, рівнянням (10).

Наведені вище результати аналізу дозволяють визначити складність моделі та на її основі складність побудування підмножини із N КДС.

1. При побудові одного КДС необхідно, у залежності від допустимих значень $R_{a_1}^q(l)$ і $R_{a_2}^q(l)$, що визначаються межами щільної упаковки, розглянути $v \geq k$ систем вигляду (1), (2).

2. При побудові двох КДС необхідно розглянути $v_2 \geq K_2$ систем вигляду (3)–(7), де K_2 визначається $R^{qp}_{b_{1,j}}(l)$ та $R^{qp}_{b_{2,j}}(l)$.

3. При побудові N КДС необхідно розглянути $v_N \geq K_N$ систем вигляду (3)–(7), де K_N визначається $R^{q}_{a_1}(l)$ і $R^{q}_{a_2}(l)$ та $R^{qp}_{b_{1,j}}(l)$ і $R^{qp}_{b_{2,j}}(l)$ допустимими значеннями.

Таким чином, на основі врахування меж фізичної упаковки підмножини КДС [1] існують можливості побудови підмножин КДС згідно (1), (2) та (3)–(7).

У постановці, що наведена вище, можна формулювати та вирішувати в межах «щільної» упаковки і задачу побудови розмитих підмножин КДС. В певній мірі вона розглянута в [1, 2].

Аналогічно (1), (2) та (3)–(7) задається модель підмножини (словника) КДС через аперіодичні функції автокореляції (АФАК). В даному випадку можливі спрощення. Так систему (1), (2) по аналогії можна подати у вигляді системи НПН на основі аперіодичних функцій кореляції, тобто

$$r^{q}_{a_1}(l) \leq \sum_{i=1}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r^{q}_{a_2}(l),\ l=\overline{1,L},\ \ m=\overline{1,L}, \qquad (13)$$

де $r^{q}_{a_1}(l)$ і $r^{q}_{a_2}(l)$ — задані, але допустимі реалізації з точки зору щільної упаковки. Далі системи (1), (2) та (3)–(7) також можна подати через аперіодичні функції взаємної кореляції (АФВК) у вигляді системи нелінійних параметричних нерівностей

$$r^{qp}_{b_{1,1}}(l) \leq \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r^{qp}_{b_{1,2}}(l);\ \ l=\overline{1,L},\ \ m=\overline{1,L}, \qquad (14)$$

$$r^{qp}_{b_{2,1}}(l) \leq \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^p \left(W_{i+1}^q\right)^* \leq r^{pq}_{b_{2,2}}(l);\ \ l=\overline{1,L},\ \ m=\overline{1,L}, \qquad (15)$$

де $r^{qp}_{b_{1,1}}, rr^{qp}_{b_{1,1}}, r^{qp}_{b_{2,1}}, r^{qp}_{b_{2,2}}$ допустимі з точки зору щільної упаковки АФАК та АФВК.

2. Розв'язання задачі побудови (синтезу) підмножин КДС. Побудова (синтез) підмножини КДС ґрунтується на застосуванні ключових даних та використанні випадкових чи псевдовипадкових дискретних послідовностей.

Дослідження показали [1, 2], що вказаний клас задач може розв'язуватись при застосуванні методу «гілок і меж», наприклад, зведений до таких етапів.

1. Формування випадкових чи псевдовипадкових дискретних послідовностей з використанням ключових даних.

2. Оцінка статистичних властивостей потенційних КДС [4, 8].
3. Побудова необхідного числа потенційних КДС W^q згідно системи (1) та ключових даних.
4. Знаходження пар чи підмножин КДС W^q та W^p, які задовольняють вимогам (3)–(7), застосовуючи метод «гілок та меж».
5. Побудова матриці станів взаємно-кореляційних функцій всіх можливих пар потенційних КДС, які пройшли відбір за результатами попереднього кроку та мають усі необхідні властивості.
6. Аналіз матриці станів та формування необхідного числа підмножин чи пар КДС згідно (1), (2) та (3)–(7) та відбір у підмножину лише тих, що задовольняють вимогам.

З урахуванням необхідності забезпечення криптографічної стійкості та структурної скритності пар чи підмножин КДС як джерело дискретних послідовностей застосовується алгоритм блокового симетричного перетворення ДСТУ 7624:2014, що є стійким у пост квантовий період.

У роботах [1, 2] наведено приклади пар та підмножин КДС.

3 Оптимізація методу синтезу криптографічних сигналів. В ході досліджень запропоновано вдосконалений метод побудування КДС, що заснований на використанні властивості та взаємного зв'язку АФАК та ПФАК, а також методу «великих» та «малих» кроків.

Перше прискорення грунтується на симетрії ПФАК [1, 2].

Вирішення задачі подальшої оптимізації грунтується на використанні методу «великих» та «малих» кроків (теорема 1 та наслідок теореми 1).

Теорема 1. Нехай максимальні (мінімальні) значення реалізацій функцій $Ra_1^1(l)$ і $Ra_2^1(l)$ в (1) є такими, що величина δ, визначена як

$$\delta = \left|Ra_1'(l) - Ra_1(l)\right| \text{ або } \delta = \left|Ra_2'(l) - Ra_2(l)\right|, \qquad (16)$$

$\delta \neq 0,1,2,...P-1,P$ більше P, а W^j — сигнал, який визначений над полем $GF(P)$ або над кільцем чисел по модулю P, тоді безліч значень циклічної згортки (функції автокореляції (ФАК)) $Ra^Z(l)$ може належати інтервалу

$$(\min Ra_1(l), \max Ra_2(l)), \qquad (17)$$

крайньою мірою, при «відкиданні» r останніх і «додаванні» r перших символів сигналу W, де $r = \frac{\delta}{P}$, якщо $\delta \mid P$ і $r = \frac{\delta + t}{P}$, якщо $\delta \neq P$.

Доведення теореми наведено в [1, 2].

Наслідок теореми 1. Якщо $W_i \in GF(P)$, то $r = \frac{\delta}{2}$, якщо δ парне і $r = \frac{\delta + 1}{2}$, якщо δ — не парне.

Аналіз результатів досліджень показав, що прискорення в побудуванні підмножин КДС з використанням запропонованих методів залежить від обмежень на кореляційні властивості, розмірів підмножин , довжин КДС та джерела КДС і розмірів ключів.

Висновки. В роботі сформульована в загальному вигляді і вирішена задача синтезу підмножин КДС, ансамблеві, кореляційні властивості яких можуть бути встановлені в залежності від вимог, що пред'являються до завадозахищеності та інформаційної безпеки ТКС.

Список використаних джерел:

1. 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.
2. Горбенко И. Д., Замула А. А. Криптографические сигналы: требования, методы синтеза, свойства, применение в телекоммуникационных системах. *Радиотехника: Всеукр. межвед. науч.-техн. сб.* Харьков: ХНУРЭ, 2016. Вып. 186. С. 7–24.
3. Замула А. А. Ансамбли дискретных сигналов с минимальными значениями боковых лепестков функций. *Системи обробки інформації*. Х.: ХУПС, 2015. Вип. 10 (135). С. 35–39.
4. Горбенко Ю. І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем: Монографія / За загальною редакцією Професора Горбенко Івана Дмитровича. Харків: Форт, 2015. 959 с.
5. Варакин Л. Е. Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с.
6. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Введ. 01–07–2015. К.: Мінекономрозвитку України, 2015.
7. Sarvate D. V., Pursley M. V. Crosleration Properties of Pseudorandom and Related Sequences. *IEEE Trans. Commun*. 1980. Vol. 68. P. 59 -90.
8. NIST 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000.

Formulated in general view and solved problem of synthesis nonlinear discrete complex cryptographic signals, by branch and bounds method, presented proposal for synthesis methods optimization.

Key words: *complex signal, structural and information secrecy, imitation resistance.*

Одержано 20.02.2017