where the countries with lower probabilities of mistakes on all stages are specialized on the later stages of production. Using the simple theoretical basis, one may suggest a form of vertical specialization for interdependent countries.

Policy makers, business leaders, economists equally pay attention to the phenomenon of vertical specialization. The option of transboundary fragmentation for production processes affects amounts, features, and consequences of international trade. The issues how global and local technology changes influnce on participation of various countries in the same supply chain, how vertical specialization influence on interdependence of countries remain opened.

As the general equilibrium models with an arbitrary (large) number of products and countries, regardless of sequential production presence, do not give clear comparative static predictions, a simple trade theory with sequential production is needed. It requires some ideas about hierarchies in partial equilibrium models of a closed economy. The environment where production may contain mistakes is the focus. Models of hierarchies have been applied to the international trade questions. For instance, the kowledge economy model is used for research of transboundary matching between agents with nonuniform abilities and corresponding consequences for inequality in a given country. Inequality in a country due to hierarchies at trade has been investigated by other models as well. It is assumed all people of a given country have equal abilities.

Key words: *equilibrium, supply chains, production stages, final good, intermediate products.*

Одержано 15.02.2019

УДК 004.728:004.728.3,004.056.055
DOI: 10.32626/2308-5916.2019-19.37-43

І. Д. Горбенко*,**, д-р техн. наук,
О. А. Замула*, д-р техн. наук,
Хо Чі Лик**

*Харківський національний університет імені В. Н. Каразіна, м. Харків,
******АТ «Інститут інформаційних технологій», м. Харків

ОПТИМІЗАЦІЯ ПОШУКУ ДИСКРЕТНИХ СКЛАДНИХ СИГНАЛІВ З НЕОБХІДНИМИ ВЛАСТИВОСТЯМИ ДЛЯ ЗАСТОСУВАННЯ У СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Серед основних напрямків покращення показників ефективності функціонування інформаційно-комунікаційних систем (ІКС), зокрема, завадозахищеності, скритності, інформаційної безпеки, можна виділити напрямки, пов'язані із застосуванням фазоманіпульованих широкосмугових сигналів (ФМ ШПС) і частотно-фазоманіпульованих (ЧФМ) сигналів. Оскільки в багатокористувачевих системах, кодовий поділ каналів ґрунтується на відмінності сигналів, то побудова ІКС і показ-

ники ефективності зазначених систем визначаються вибором сигналів і їх властивостями. При цьому, як дискретні послідовності (ДП), які розширюють спектр (маніпулюють несучу частоту), повинні бути використані ДП, які засновані на нелінійних правилах побудови і мають покращені кореляційні, ансамблеві і структурні властивості. Зокрема, при використанні таких сигналів як фізичного переносника інформації або сигналів синхронізації часові витрати на розкриття структури використовуваних сигналів зростають і постановка «оптимальних», з точки зору станції протидії, перешкод стає проблематичною. Складні сигнали, отримані на основі таких послідовностей, володіють, з одного боку, структурними властивостями, аналогічними властивостям випадкових (псевдовипадкових) послідовностей, а з іншого — необхідними ансамблевими і кореляційними властивостями. Мінімізація рівня бічних пелюсток АКФ має найбільше значення при конструюванні сигналу для таких додатків як вимір часу запізнювання, часовий дозвіл й ін. У даній роботі сформульована і вирішена задача оптимізації синтезу нелінійних дискретних послідовностей, які мають покращені ансамблеві, структурні і автокореляційні властивості. Застосування нелінійних дискретних сигналів, які утворені на основі таких послідовностей, дозволить забезпечити необхідні значення завадозахищеності, інформаційної та структурної скритності функціонування ІКС.

Ключові слова: *дискретна послідовність, криптографічний сигнал, функція кореляції, ізоморфізм, кінцеве поле.*

Вступ. До інформаційно-комунікаційних систем (ІКС), особливо, критичного призначення, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування (продуктивності, достовірності передавання інформації, живучості, завадозахищеності, інформаційної безпеки) [1, с. 154–156]. Існує протиріччя між жорсткими вимогами щодо забезпечення зазначених показників, з одного боку, і існуючими моделями, методами і технологіями керування ІКС, інформаційною безпекою, з іншого боку. Основними шляхами вирішення зазначеного протиріччя є підвищення завадозахищеності та інформаційної безпеки ІКС на основі розробки методів синтезу нових класів сигналів — переносників даних з необхідними ансамблевими, кореляційними і структурними властивостями.

Синтез систем сигналів із заданими кореляційними властивостями. В роботі [2] показано, що процес вибору раціональних по тих чи інших критеріях дискретних сигналів (ДС) тотожний синтезу відповідних дискретних послідовностей (ДП), за допомогою яких маніпулюють, наприклад, фазу несучої частоти. Як критерій вибору класу ДС (як правило), орієнтуються на мінімаксний критерій. Такий критерій має на

увазі побудову ансамблів сигналів, які як можна помітніше відрізняються один від одного. Кількісною мірою відмінності ДП служать максимальні рівні бічних пелюсток функції автокореляції в аперіодичному (АФАК) і періодичному режимах передачі (ПФАК).

Виходячи з цього широкосмугові сигнали (ШСС), повинні володіти такими кореляційними властивостями, коли бічні піки кореляційних функцій ШСС є якомога меншими, тобто в ідеальному випадку повинні прагнути до нуля. У теорії складних сигналів відомий ряд інтегральних рівності [2]. Нехай C множина комплексних чисел, а C^N множина векторів з комплексними компонентами. Елементи множини $w, x, y, z \in C^N$ довільні вектори, а w, x, y, z відповідні їм дискретні послідовності. Чотири взаємно-кореляційні функції $R_{w,x}$, $R_{y,z}$, $R_{w,y}$, $R_{x,z}$ пов'язані співвідношенням

$$\sum_{l=0}^{N-1} R_{w,y}(l)[R_{x,z}(l+n)]^* = \sum_{l=0}^{N-1} R_{w,x}(l)[R_{y,z}(l+n)]^* . \quad (1)$$

Поклавши в (1) $z = y$, отримаємо

$$\sum_{l=0}^{N-1} R_{w,y}(l)[R_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} R_{w,x}(l)[R_{y}(l+n)]^* . \quad (2)$$

Поклавши в (2) $w = x$, отримаємо

$$\sum_{l=0}^{N-1} R_{x,y}(l)[R_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} R_{x}(l)[R_{y}(l+n)]^* . \quad (3)$$

Нарешті, поклавши в (5) $n = 0$, отримаємо

$$\sum_{l=0}^{N-1} \left|R_{x,y}(l)\right|^2 = \sum_{l=0}^{N-1} R_{x}(l)[R_{y}(l)]^* . \quad (4)$$

За допомогою (1)–(4) отримано ряд важливих границь оцінки кореляційних функцій. Рівність (3) означає, що автокореляційна функція (АКФ) послідовності $R_{x,y}$ збігається з взаємно-кореляційною функцією (ВКФ) послідовностей R_x і R_y. Крім того, з (4) слід, що середнє значення квадрата модуля функції взаємної кореляції сигналів x і y дорівнює середньому значенню твору їх АКФ. Фактично це означає, що сигнали, що володіють хорошими автокореляційними властивостями будуть володіти і хорошими властивостями ВКФ. ПФАК послідовності $\{a_0, a_1, \ldots . a_{N-1}\}$ має вид [3, с. 141–143]:

$$\rho_p(m) = \frac{1}{\left\|a^2\right\|} \sum_{i=m}^{N-1} a_i \cdot a_{i-m}^* + \frac{1}{\left\|a^2\right\|} \sum_{i=0}^{m-1} a_i \cdot a_{i-m}^* , m \geq 0 . \quad (5)$$

Перший доданок у виразі (5) є АФАК, тоді як другий — дорівнює $p_a(m-N)$. В результаті отримуємо співвідношення, що зв'язує ПФАК із своїм аперіодичним аналогом:

$$\rho_p(m) = \rho(m) + \rho_a(m-N), m = 0,1,....N\ . \quad (6)$$

Рівність нулю всіх бічних пелюсток неможливо для аперіодичних ФМ сигналів. Тоді крайній правий боковий пік нормованої АФАК ДП сигналу буде:

$$P_a(N-1) = \frac{a_0 a_{N-1}}{\|a\|^2} \neq 0\ . \quad (7)$$

Останнє співвідношення призводить до застосування мінімаксного критерію при синтезі сигналів. Формальна запис даного критерію має вигляд:

$$\rho_{a,\max} = \max_{m\neq 0}\left\{\left|\rho_a(m)\right|\right\} = \min. \quad (8)$$

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 обраного алфавіту знайти послідовності з мінімальною величиною максимального бічного пелюстка АФАК. Загальна ідея алгоритмів, спрямованих на вирішення цієї задачі, полягає у попередньому відборі деякої обмеженої множини послідовностей, і подальшому пошуку послідовностей з мінімальним значенням серед послідовностей, які увійшли у зазначену множину. Одним із прикладів такої стратегії, є використання співвідношення (6). Позначаючи $\rho_{p,\max}$, максимальний бічний пелюсток ПФАК: $\rho_{p,\max} = \max_{m=1,2,...n-1}\left\{\left|\rho_p(m)\right|\right\}$, і використовуючи нерівність: $\max\left\{|x+y|\right\} \le \max\left\{|x|+|y|\right\} \le \max\left\{|x|\right\} + \max\left\{|y|\right\}$, приходимо до оцінки $\rho_{p,\max} \le \rho_{a,\max}$ або:

$$\rho_{a,\max} \ge \frac{1}{2}\rho_{p,\max}\ . \quad (9)$$

Випливає, що ДП з хорошою АФАК можуть бути знайдені серед послідовностей з хорошими характеристиками ПФАК.

Таким чином, ДП з відповідними значеннями бокових піків АФАК, можуть бути відібрані з множини ДП, значення бокових піків ПФАК яких є оптимальними. Саме ці обставини були застосовані для проведення оптимізації пошуку ДС з покращеними характеристиками АФАК. До оптимальних (з точки зору ПФАК) за мінімаксним критерієм відносяться нелінійні характеристичні дискретні сигналів (ХДС) [4, с. 125–129]. Досліджені автокореляційні властивості даного

класу сигналів у аперіодичному режимі передачі. Зокрема, встановлено, що для періоду ДП 256 елементів існує 56 ДП, для яких значення максимальних бічних піків АФАК не перевищує значення 18 (1,1√N). Було синтезовано 470 ХДС, нормовані значення максимальних бічних піків АФАК яких, не перевищують величини 20/256. У стандарті системи з кодовим поділом UMTS як код первинної синхронізації використовується бінарна синхропослідовність (СП) з періодом 256 елементів, які володіють $\rho_{a,\max}$ аж до ¼, тобто $\rho_{a,\max}$ = 64. При виборі ХДС як СП, у порівнянні з сигналами, що застосовуються в стандарті UMTS, виграш, з точки зору завадостійкості прийому сигналів, складе більше 4 дБ. В роботах [5–7] показано, що застосування криптографічних сигналів (КС) дозволить суттєво покращити показники інформаційної безпеки, скритності функціонування ІКС. З метою підвищення завадостійкості прийому сигналів була висунута гіпотеза щодо можливості застосування саме КС як фізичних переносників даних, а також як СП. Для перевірки гіпотези синтезовано 680 КС, $\rho_{a,\max}$ АФАК для яких, не перевищує значень 33. В цьому випадку, як показали розрахунки, виграш з точки зору завадостійкості прийому СП у порівнянні з використання ДП, що застосовуються в стандарті UMTS, складає 3 дБ. Якщо висуваються більш жорсткі умови до завадозахищеності прийому сигналів в ІКС, можна запропонувати застосовувати КС, для яких $\rho_{a,\max}$ АФАК менше ніж 33. В таблиці наведено дані щодо деяких КС, для яких $\rho_{a,\max}$ не перевищують значення 26, а на рисунку показано вид АФАК для одного з таких КС.

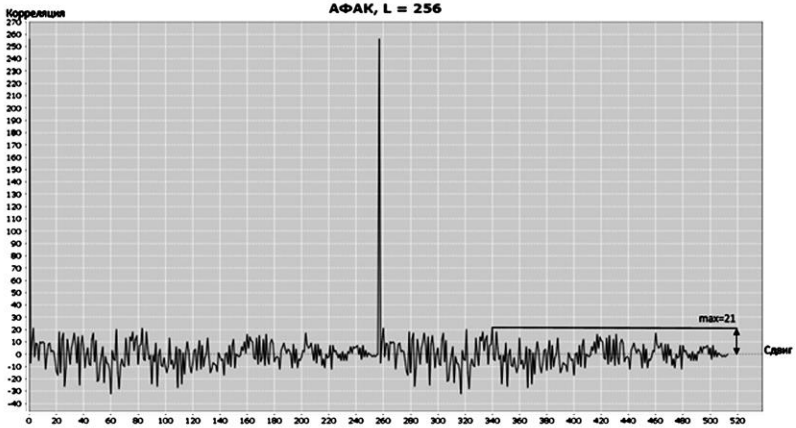

Рисунок. *АФАК КС для N = 256. Циклічний зсув* {83}

Таблиця

КС для N = 256 з найменшими бічними пелюстками АФАК

Сигнал №	Значення максимальних бокових піків АФАК	Відповідні зсуви КС
1	25	{31}
2	25	{61}
3	26	{60}
4	26	{10,22}
5	24	{212}
6	26	{48}
7	21	{3,83}
8	26	{66}

Висновки. На основі застосування мінімаксного критерію та рівностей, що встановлюють залежність авто- і взаємно-кореляційних функцій ДС, вирішена задача оптимізації пошуку нелінійних ДС з покращеними властивостями. Показано, що застосування синтезованих систем сигналів дозволить підвищити завадостійкість прийому сигналів, показники інформаційної безпеки та скритності функціонування ІКС в умовах кібератак, дії природніх та організованих, у тому числі, структурних, ретрансльованих й інших завад.

Список використаних джерел:

1. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування : монографія. Харків : Форт, 2012. 880 с.
2. Sarvate D. V., Pursley M. V. Crosleration Properties of Pseudorandom and Related Sequences. *IEEE Trans. Commun.* 1980. Vol. 68. P. 59–90.
3. Ipatov Valery P. Spread Spectrum and CDMA. Principles and Applications. University of Turku, Finland and St. Petersburg Electro technical University «LETI», Russia. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chi Chester, West Sussex PO19 8SQ, England.
4. Свердлик М. Б. Оптимальные дискретные сигналы. М. : Сов. радио, 1975. 200 с.
5. Горбенко І. Д., Замула О. А. Моделі та методи синтезу криптографічних сигналів та їх оптимізація за критерієм часової складності. *Математичне та комп'ютерне моделювання.* Серія: Фізико-математичні науки : зб. наук. праць. Інститут кібернетики імені В. М. Глушкова Національної академії наук України, 2017. Вип. 15. 272 с.
6. 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. P. 1079–1100. DOI: 10.1615/TelecomRadEng.v76.i12.50.
7. Gorbenko D., Zamula A. A., Semenko A. E., Morozov V. L. Method for synthesis of performed signals systems based on cryptographic discrete sequences of symbols. *Telecommunications and Radio Engineering.* 2017. Vol. 76, Issue 17. P. 1523–1533.

OPTIMIZATION OF DISCREET COMPLEX SIGNALS SEARCH WITH NECESSARY PROPERTIES FOR APPLICATION IN MODERN INFORMATION AND COMMUNICATION SYSTEMS

Among the main areas of the performance indicators improvement of information and communication systems (ICS), in particular, noise immunity, secrecy, and information security, it is possible to identify the areas associated with the use of phase-manipulated broadband signals and frequency-phase-manipulated signals. Since in multi-user systems, the code division of channels is based on the difference in signals, then the construction of ICS and performance indicators of these systems are determined by the choice of signals and their properties. In this case, discrete sequences (DS), that extend the spectrum (manipulate carrier frequency), should be based on nonlinear construction rules and have improved correlation, ensemble and structural properties. In particular, when using signals such as the physical carrier of information or synchronization signals, the time expenditures on the disclosure of the structure of the signals used are increasing and the setting of «optimal», from the standpoint of the counter-station, obstacles becomes problematic. Complex signals obtained on the basis of such sequences, possess, on the one hand, structural properties, similar to the properties of random (pseudorandom) sequences, and on the other hand, necessary ensemble and correlation properties. The side petals minimization levels of the ACF is of greatest importance when designing a signal for such applications as measuring the lag time, time resolution, etc. In this paper, the problem of optimizing the synthesis of nonlinear discrete sequences, which have improved ensemble, structural and autocorrelation properties, is formulated and solved. The use of non-linear discrete signals, which are formed on the basis of such sequences, will provide the necessary values of impedance protection, information and structural secrecy of the ICS operation.

Key words: *discrete sequence, cryptographic signal, correlation function, isomorphism, finite field.*

Одержано 08.02.2019