ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОММУНІКАЦІЙНИХ СИСТЕМАХ

УДК 681.3.06:519.248.681 **DOI:10.30837/rt.2020.3.202.09**

І.Д. ГОРБЕНКО, д-р техн. наук, Е.А. СЕМЕНКО, О.А. ЗАМУЛА, д-р техн. наук

МЕТОДИ ТА ЗАСОБИ СИНТЕЗУ І ГЕНЕРАЦІЇ СИГНАЛІВ – ФІЗИЧНИХ ПЕРЕНОСНИКІВ ДАНИХ У СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Вступ

Сучасні радіолокаційні, супутникові радіонавігаційні і інформаційно-комунікаційні системи (ІКС) виконують різноманітні завдання, основним з яких є пошук, виявлення, класифікація, обмін, обробка, цілевказівки, зберігання даних, освоюють все більшу кількість функцій, при цьому намітилися наступні тенденції:

- постійне зростання кількості корпоративних, індивідуальних і мобільних абонентів;
- зростання трафіку;
- обмежена кількість радіоканалів;
- обмежена пропускна здатність;
- великий час зчитування, запису та доставки інформації споживачеві;
- низька завадозахищеність, інформаційна і кібербезпека і ін.

Для вирішення цих та інших проблем приймаються такі технічні рішення:

- впровадження складних видів модуляції, кодування, шифрування даних;
- застосування технологій багаторівневого ущільнення інформаційних потоків;
- збільшення бази, об’єму сигналу і каналу;
- застосування адаптивних систем комплексного використання методів розділення сигналів, трас поширення та інформаційних каналів.

Однією зі складних проблем створення ІКС залишається синтез системи сигналів – фізичних переносників даних. При цьому повинна бути визначена необхідність та способи реалізації синхронізації, оцінені завадостійкість, скритність, інформаційна безпека при дії різних перешкод і впливів зловмисника, синтезовано структуру передавальної, приймальної апаратури, здійснено розподіл функції між програмної та апаратної частинами і інше [1].

Ключові технології побудови перспективних ІКС включають такі:

- застосування вузько-, широко- і понадширокосмугових сигналів;
- модернізація методів поділу каналів;
- побудова приймачів і антенних решіток з малим рівнем власних і взаємних шумів;
- розширення теорії ортогональних інформаційних просторів;
- побудова методів багатоетапного оборотного перетворення сигналів;
- стандартизація та уніфікація транспортних протоколів обміну на всіх рівнях системи;
- розробка методів управління точністю вимірювання параметрів;
- застосування бортового обладнання супутників зв’язку і космічних апаратів для побудови мереж з розподіленою обробкою інформації;
- поєднання в системі технологій радіо- та інших діапазонів, форм сигналів, в тому числі і неенергетичних;
- розробка технологій міжсупутникових ліній зв'язку, електромагнітних, оптичних та інших;
- підвищення надійності функціонування за рахунок адаптації системи інформаційного обміну в реальних умовах.

Аналіз наведених інформаційних технологій показує актуальність розробки нових і вдосконалення існуючих способів і засобів їх реалізації в сучасних ІКС. Зокрема, в теорії

сигналів накопичений величезний потенціал інформаційних технологій, однак на практиці використовується обмежений набір традиційних методів і технічних рішень.

Пошук нових систем сигналів повинен бути заснований на законі синергії, завдяки якому стає можливим отримання ефектів, що перевищують просту суму властивостей явищ, що входять в систему сигналів. Потрібно узагальнити накопичений потенціал, визначити закони, принципи та методи їх застосування. Для цього слід провести системну класифікацію та уніфікацію інформаційних потоків для вирішення завдань формування та обробки інформації в ІКС, систематизацію моделей, методів, технічних і програмних засобів їх реалізації. Принципи побудови нових технологій в області ІКС повинні охоплювати весь спектр перетворень інформації в комплексі, від джерела до споживача. І повинні бути засновані не тільки на ефективній передачі інформації, але і на забезпеченні скритності, електромагнітної та іншої сумісності, екології, інформаційної безпеки, захищеності від нав'язування (введення в систему) помилкових даних і інше.

Мета статті – представлення та аналіз моделей, методів і засобів генерації і обробки одного з класів сигналів з розширенням спектру, що є фізичному переносником даних в ІКС.

1. Аналіз сигналів – фізичних переносників даних у сучасних інформаційно-комунікаційних системах

Розвиток технологій бездротових комунікацій постійно формувався на основі досліджень форм сигналів. Як приклад можна навести використання технології мультиплексування сигналів з ортогональним частотним розділенням каналів (Orthogonal frequency – division multiplexing, далі – OFDM) в сучасних бездротових системах зв'язку широкосмугового доступу (WiMAX, WiFi, LTE та ін.). Застосування такої технології дозволяє підвищити інформаційну ємність системи при обмеженій смузі пропускання, швидкість прийому-передачі даних, наблизивши її до пропускної здатності каналу, збільшити скритність передачі і стійкість перед перешкодами прийому сигналів, і, як наслідок, забезпечити постійно зростаючі потреби користувачів мереж в високошвидкісних з'єднаннях і мультимедійних сервісах [2, 3].

По суті OFDM – це схема модуляції, що використовує множину несучих. Канал ділиться на кілька субканалів. В OFDM високошвидкісний потік даних конвертується в кілька паралельних бітових потоків меншої швидкості, кожен з яких модулюється своєю окремою несучою. Вся ця множина несучих передається одночасно. Одна з переваг OFDM полягає в тому, що тривалість символу в допоміжній несучій значно більше в порівнянні з затримкою поширення, ніж в традиційних схемах модуляції. Це робить OFDM набагато стійкішою до між символьної інтерференції.

Аналітично OFDM сигнал може бути представлений у вигляді [2]:

$$S(t) = \sum_{k=0}^{N-1} S_k(t) = \sum_{k=0}^{N-1} A_k \, e^{j2\pi kf/T}, 0 \le t \le T, \quad (1)$$

де k – індекс піднесучої, $S_k(t)$ – сигнал на k-піднесучий, A_k – амплітудна складова послідовності інформаційних символів, N – кількість піднесучих, T – тривалість інформаційного символу.

Основна ідея OFDM полягає в тому, що для досягнення високої швидкості передачі в частотної області застосовується розподіл повного діапазону частот сигналу на деяке число частотних підканалів з меншими швидкостями. При цьому кожен підканал (піднесуча) модулюється окремим символом, потім ці канали мультиплексуються за частотою і дані передаються паралельно по ортогональних підканалах. У порівнянні з передачею з однієї несучої цей підхід забезпечує підвищену стійкість до вузькополосної інтерференції і спотворень в каналі. Більш того, з цього випливає високий рівень гнучкості системи, так як параметри модуляції, такі як розмір сузір'я, швидкість кодування, можуть бути незалежно вибрані для кожного з підканалів.

Структура OFDM сигналу може бути досить складною, оскільки складається з множини компонентів:

- структура частотно-часового розподілу, що задана початковою частотою, кроком сітки частот, кількістю піднесучих;
- за часовими слотами, що задані тривалістю символу, тривалістю захисного інтервалу;
- вид маніпуляції: фазова (BPSK, QPSK, 8-PSK) або амплітудно-фазова квадратурна модуляція (QAM);
- дискретні послідовності, які визначають закон (правило) маніпуляції фази високочастотної несучої і задаються розмірністю сигнального простору;
- вид символьної синхронізації;
- наявність і вид завадостійкого кодування (код Ріда – Соломона, код Боуза – Чоудхурі Хоквінгема, турбокод і ін.);
- наявність і вид перемеження даних і ін.

Наведені особливості структури OFDM сигналу можуть бути використані при побудові ІКС, для яких вимоги забезпечення заданих показників захищеності від введення (нав'язування) неправдивих повідомлень, фальсифікації повідомлень, порушення цілісності даних, конфіденційності, завадостійкості прийому, скритності функціонування є визначальними.

Численні дослідження показали, що поліпшення якісних показників, зокрема завадозахищеності та інформаційної безпеки ІКС і мереж, може бути досягнутий, в тому числі, шляхом розробки методів синтезу, формування і обробки складних дискретних сигналів-фізичних переносників даних з необхідними ансамблевими, структурними і кореляційними властивостями [4 – 6].

Ряд досліджень [7, 8] показали, що подальше поліпшення основних якісних показників деяких додатків радіоканалів може бути досягнуто на основі використання сигналів з лінійною частотною модуляцією (ЛЧМ), ФМ ЛЧМ і в загальному випадку складових нерівномірних за тривалістю ЛЧМ сигналів з внутрішньоімпульсною ФМ (СНЛЧМ-ФМ) сигналів.

Аналітичне представлення СНЛЧМ-ФМ сигнали має вигляд

$$S^{(p)}(t) = S_0{}^{(p)} \sum_{n=1}^{N} \sum_{l=1}^{Q} V_e{}^{(p)} \operatorname{rect}\left(\frac{t - \sum_{r=0}^{n-1} T_r}{T_n} \right) \operatorname{rect}\left(\frac{t - (l-1)\tau_э}{\tau_э} \right) \times$$

$$\times \exp\left(j \left(\omega_n \left(t - \sum_{r=0}^{n-1} T_r \right) + \frac{\mu_n}{2} \left(t - \sum_{r=0}^{n-1} T_r \right)^2 + \varphi_n \right) \right), \qquad (2)$$

де $S_0{}^{(p)}$ – амплітуда огибаючої сигналу; N – число радіоімпульсів, що складають СНЛЧМ – ФМ сигнал; Q – число елементів двійкової маніпулюючої послідовності; $V_e{}^{(p)}$- символ p-й маніпулюючої послідовності, причому $V_l^{(p)} \in \{1, -1\}$; $\operatorname{rect}(x)$ – є функція, що має вигляд

$$\operatorname{rect}(x) = \begin{cases} 1 \text{ при } 0 \le x \le 1, \\ 0 \text{ при } x < 0, x > 1 \end{cases}; \qquad (3)$$

$\tau_э$ – тривалість елемента маніпулюючої послідовності; ω_n, φ_n – несуча частота і початкова фаза n-го ЛЧМ радіоімпульсу; μ_n – коефіцієнт нахилу маніпулюючої характеристики n-го ЛЧМ радіоімпульсу, що пов'язаний з девіацією частоти ΔF_n і тривалістю T_n співвідношенням $\mu_n = \pm 2\pi \Delta F_n / T_n$.

Одним з головних напрямків розвитку ІКС є впровадження складних, широкосмугових, шумоподібних сигналів [4 – 6], зокрема сигналів, отриманих шляхом зміни фази гармонійного коливання в дискретні моменти часу за законом псевдовипадкових кодових послідовностей. Застосування широкосмугових і досить протяжних в часі сигналів, як правило з внутрішньоімпульсною модуляцією, в сукупності з ефективними алгоритмами їх обробки дозволяє підвищити завадостійкість прийому сигналів при впливі навмисних і ненавмисних перешкод, енергетичну скритність сигналів від радіотехнічної розвідки, дає можливість реалізувати кодове розділення каналів при багатостанційному доступі, вимірювати час приходу сигналів з великою точністю і високою роздільною здатністю, встановлювати надійний зв'язок в каналах при наявності багатопроменевого характеру поширення радіохвиль і ін. Безліч таких сигналів має володіти хорошими кореляційними властивостями. Кожен з таких сигналів повинен відрізнятися від своєї зрушеною в часі копії і від будь-якого іншого сигналу цієї множини з довільним тимчасовим зрушенням.

Множинний доступ з кодовим поділом абонентів в багатокористувачевих інформаційно-комунікаційних системах (ІКС) здійснюється через використання при розширенні спектру специфічних дискретних послідовностей (ДП). При цьому кореляційні, структурні, ансамблеві та енергетичні властивості дискретних сигналів ототожнюють з відповідними властивостями ДП, які застосовують для утворення таких сигналів, і саме ДП, значною мірою визначають показники завадостійкості і скритності функціонування ТКС, а також інформаційної безпеки таких систем [4]. Тому розробка ефективних методів синтезу ДП (за законом яких маніпулюють параметри інформаційних бітів даних) з визначеними структурними, ансамблевими, кореляційними та іншими властивостями є актуальним завданням.

Авторами вперше сформульовано і у загальному вигляді вирішено задачу синтезу нового класу нелінійних дискретних складних сигналів – криптографічних дискретних сигналів (КДС).

Під КДС пропонується розуміти сукупності послідовностей (векторів) символів певного алфавіту, які обов’язково володіють необхідними (заданими) структурними, ансамблевими та кореляційними властивостями, часовою та просторовою складністю відтворення та мають можливість формування їх на основі ключів [9]. Правила побудови КДС грунтуються на використанні випадкових чи псевдовипадкових процесах, вони повинні відповідати вимогам випадковості, незворотності, непомітності, непередбачуваності та іншим [10 – 12]. Такі сигнали мають покращені, у порівнянні з іншими відомими класами сигналів, кореляційними і ансамблевих властивостями, і які обмежені значеннями «щільної упаковки».

2. Постановка і вирішення в загальному вигляді задачі синтезу криптографічних дискретних сигналів (КДС)

Під задачею побудування (синтезу) 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 [13].

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):

$$R^q_{a_1}(l) \le \sum_{i=1}^{L} W_i^q (W_{i+l}^q)^* \le R^q_{a_2}(l),\ l=\overline{1,L-1},\ q=\overline{1,N}, \tag{4a}$$

де $R^q_{a_1}(l)$ і $R^q_{a_2}(l)$ – задані значення реалізації ПФАК, а індекси обчислюються за модулем $(i+l)\ mod\ L$.

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

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, q=\overline{1,N},\ . \tag{4b}$$

3. Побудова пар КДС W^q та W^p, функції взаємної кореляції (ФВК) яких задовольняють вимогам, що визначаються сукупністю систем НПН (5a), 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} (5b – 5d):

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

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

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

$$R^{qp}_{b_{1,4}}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^q)^* \le R^{qp}_{b_{2,4}}(l); \tag{5d}$$

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

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

В системах нелінійних параметричних нерівностей (4a) – (4b) та (5a) – (5e) 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 побудування. В подальшому системи (4a)– (4b), (5a) – (5e) та квадратичне рівняння (5h) будемо називати моделлю підмножини (словника) КДС.

Проведемо аналіз систем нелінійних параметричних квадратичних нерівностей (далі систем) (4a) – (4b) та (5a) – (5e), використовуючи введену модель.

Системи (5b) та (5d) при $l=L$ для усіх $q=\overline{1,N}$ повинні дати повну згортку зі значенням L, тобто (5b)

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, q=\overline{1,N}, \tag{5f}$$

а (5d) дає

$$\sum_{i=1}^{L} W_i^p W_{i+L}{}^p = \sum_{i=1}^{L} W_i^p W_i^p = L, p=\overline{1,N},. \tag{5g}$$

Системи (5a), (5c) та (5e) при $l=L$ для усіх пар W^q та W^p дають значення функції взаємної кореляції при нульовому значенні зсуву відповідно виду

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0); q, p=\overline{1,N}, \tag{5h}$$

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0), q, p = \overline{1, N}, \tag{5i}$$

$$\sum_{i=1}^{L} W_i^p W_{i+L}{}^q = \sum_{i=1}^{L} W_i^p W_i^q = R^{pq}(0), p, q = \overline{1, N}, . \tag{5j}$$

Проведемо аналіз систем (4a) – (4b) на предмет існування рішень та незалежності. Безпосередньо із (4a) 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 з (4a) можна скласти систему із L – 1 незалежних НПН. Далі, використовуючи (4b), отримуємо ще один вираз, але уже рівняння. Особливістю системи (4) є те, що вона дає згортку кожного із q КДС зі значенням L. На основі (4a) та (4b) при побудові кожної N підмножини КДС можна скласти N незалежних систем квадратичних НПН, кожна з яких буде містити L-1 квадратичних нерівностей виду (4a) і формально одне рівняння, тобто всього їх буде L.

Також проведемо аналіз сукупності систем параметричних нерівностей (5a) – (5e), з урахуванням (5f) – (5j), на предмет існування рішень та незалежності систем та окремих рівнянь. Системи (5a) – (5e) визначають допустимі взаємно кореляційні властивості відносно ПФВК та СФВК кожної пари КДС – W^q та W^p . Вони визначають вимоги відносно ПФВК та СФВК конкретно тільки двох КДС – W^q та W^p . При побудові трьох КДС будемо мати 3!/2 систем виду (5), а при N КДС відповідно – N!/2 систем виду (5). Таким чином, з ростом N число систем виду (5) збільшується експоненційно (за факторіалом).

Для N = 2 серед (5f) – (5j) систем НПН є збиткові нелінійні квадратичні рівняння. Рівняння (4b) співпадає з (5f) та (5g), тому останні два уже входять у систему (1b), є залежними, тому не можуть бути використаними. Далі, рівняння (5h) та (5i) співпадають, а рівняння (5j) є симетричним в частині кореляційної функції по відношенню до рівнянь (5h) та (5i). Тому для кожної пари p та q незалежним є (5h).

На основі аналізу маємо, що усі (5a) – (5e) 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 (5a) – (5e) та, як уже було обґрунтовано, рівнянням (5h).

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

1. При побудуванні 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 $\upsilon \geq k$ систем виду (4).

2. При побудуванні двох КДС необхідно розглянути $\upsilon_2 \geq K_2$ систем виду (5), де K_2 визначається $R_{b_{1,j}}^{qp}(l)$ та $R_{b_{2,j}}^{qp}(l)$.

3. При побудуванні N КДС необхідно розглянути $\upsilon \geq K_N$ систем виду (5), де K_N визначається $R_{a_1}^q(l)$ і $R_{a_2}^q(l)$ та $R_{b_{1,j}}^{qp}(l)$ і $R_{b_{2,j}}^{qp}(l)$ допустимими значеннями.

Таким чином, на основі врахування меж фізичної упаковки підмножини КДС [1] існують можливості побудови підмножин КДС згідно (4) та (5).

Аналогічно (4) та (5) задається модель підмножини (словника) КДС через аперіодичні функції автокореляції (АФАК). В даному випадку можливі спрощення. Так, систему (4) за аналогією можна подати у вигляді системи НПН на основі аперіодичних функцій кореляції, тобто

$$r_{a_1}^q(l) \leq \sum_{i=1}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r_{a_2}^q(l), \; l = \overline{1, L}, \quad m = \overline{1, L}, \tag{6}$$

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

Далі системи (4) та (5) також можна подати через аперіодичні функції взаємної кореляції (АФВК) у вигляді системи нелінійних параметричних нерівностей

$$r_{b_{1,1}}^{qp}(l) \le \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \le r_{b_{1,2}}^{qp}(l); \tag{7a}$$

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

$$r_{b_{2,1}}^{qp}(l) \le \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^p \left(W_{i+1}^q\right)^* \le r_{b_{2,2}}^{pq}(l); \tag{7b}$$

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

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

Побудування (синтез) підмножини КДС ґрунтується на застосуванні ключових даних блокового симетричного алгоритму або на використанні випадкових чи псевдовипадкових дискретних послідовностей (наприклад, алгоритм AES з міжнародного стандарту ISO/IEC 18033 [1]). З урахуванням необхідності забезпечення криптографічної стійкості та структурної скритності пар чи підмножин КДС в якості джерела дискретних послідовностей може бути застосовано алгоритми блокового симетричного перетворення, які є стійкими у постквантовий період, або інше джерело випадкових чи псевдовипадкових послідовностей (наприклад, алгоритм AES з міжнародного стандарту ISO/IEC 18033).

Вказаний клас задач синтезу КДС може розв’язуватись при застосуванні методу «гілок і меж» і може бути зведений до реалізації таких етапів [13]:

1.Формування випадкових чи псевдовипадкових дискретних послідовностей.

2. Оцінка статистичних властивостей потенційних КДС.

3. Побудова необхідного числа потенційних КДС W^q згідно з системою (4) та ключовими даними.

4. Знаходження пар чи підмножин КДС W^q та W^p, які задовольняють вимогам (5a) – (5d), з застосуванням методу «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 з (1) та (2) та відбір в підмножину лише тих, що задовольняють вимогам.

3. Принципи побудови і загальна характеристика програмно-апаратного комплексу для синтезу, дослідження властивостей, генерації та обробки сигналів – фізичних переносників даних у сучасних ІКС

Наявність власного комплексу для розробки, аналізу та тестування запропонованих математичних моделей і теоретичних даних є важливою складовою. Крім того, практична реалізація запропонованої теоретичної моделі дозволяє оцінити якість досліджень та підтвердити теорію реальними даними. Саме для цього протягом декількох років ведеться розробка програмних засобів, що поєднують усі запропоновані принципи формування сигналів різних типів та різних конфігурацій у одному програмному засобі.

На початковому етапі було побудовано декілька окремих та незалежних модулів, які дозволяли проводити необхідні маніпуляції, а саме:

- комплексний програмний засіб для генерації/синтезу сигналів за заданими параметрами згідно із наявними закладеними моделями (доступні моделі побудови закладені на етапі програмування, змінними є лише параметри конфігурації). Даний засіб поєднував декілька наробок у сфері моделювання сигналів та декілька принципів побудови, що робило його доволі багаторазовим та цікавим з точки зору його варіаційних можливостей та повної незалежності. Результатом роботи цього засобу були згенеровані файли із дискретними

послідовностями (ДП), які у подальшому можна використовувати для проведення аналізу або для впровадження у налагоджену ІКС (систему зв'язку), як основу для утворення сигналів – фізичних переносників даних;

- комплексний програмний засіб для проведення аналізу сигналів щодо підтвердження (чи спростування) очікуваних властивостей послідовностей, що синтезуються. Даний засіб використовувався для аналізу статистичних, кореляційних, ансамблевих та криптографічних властивостей послідовностей, що синтезуються. Особливу увагу приділено аналізу криптографічних властивостей ДП, задля якого використовуються тести NIST. Як результат роботи – комплекс генерує вихідні файли, що у подальшому можуть бути використані для графічного відображення результатів у виді 2D та 3D графіків та для аналізу запропонованої моделі побудови;
- програмний засіб для побудови графічного відображення результатів досліджень.

У якості вихідних даних можна було використовувати як вихідні файли комплексного програмного засобу для генерації/синтезу сигналів, так і вихідні файли комплексного програмного засобу для проведення аналізу сигналів. Користувач отримував у якості результату побудовані зображення різноманітних видів кореляційних функцій, таблиці, що містять результати розрахунків (досліджень) статистичних, кореляційних, ансамблевих та криптографічних властивостей сигналів – фізичних переносників даних.

Усі результати генеруються із збереженням вихідних даних та параметрів системи, що дозволяє у будь-який момент відтворити отриманий результат.

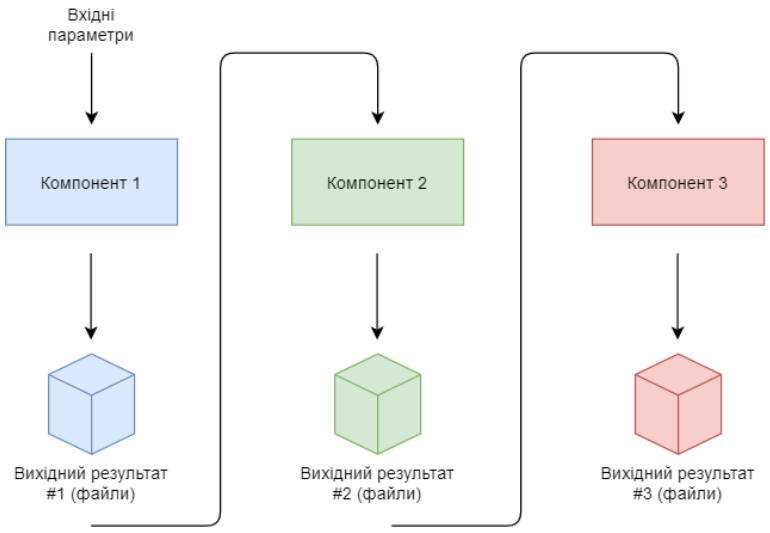

Рис. 1. Схема роботи та взаємодії між компонентами першої версії програмного рішення

Зазначені компоненти активно використовувалися у минулих дослідженнях. Проте, попри доведені властивості швидкодії та якості отриманих результатів досліджень, побудовані засоби мали низку якостей, а саме: 1) необхідність розуміння принципів налаштування та роботи, 2) необхідність знання однієї з використаних при розробці мов програмування, 3) необхідність наявності навичок роботі із декількома різними засобами для редагування зображень та інші, що значно ускладнювали та інколи унеможливлювали роботу із засобом для нових користувачів. Через це було прийнято рішення уніфікувати та поєднати зазначені компоненти у єдиний веб-сервіс. Основною ідеєю стала розробка доступного інтерфейсу користувача, що дозволяв би навіть користувачу, що не має знань у сфері побудови та аналізу сигналів ,за декілька кроків згенерувати послідовність, подаючи на вхід лише бажані параметри, отримати вихідний результат у прийнятній формі, а також провести аналіз із графічним відображенням результатів (2D/3D графіки та діаграми). На рис. 1 наведено приклад схеми взаємодії компонентів, яка була використана у першій версії імплементації, де Компонент 1 – модуль генерації послідовностей, Компонент 2 – модуль

аналізу, та Компонент 3 – це модуль графічної побудови результатів або сторонні програмні засоби, наприклад MathCad, MatLab при необхідності обробки вхідних даних, або Grafana.

Вихідні результати Компонентів 1 та 2 представлені у вигляді текстових файлів, а на виході Компоненту 3 користувач отримує графічні зображення.

Структурна схема нової версії програмного рішення наведена на рис. 2.

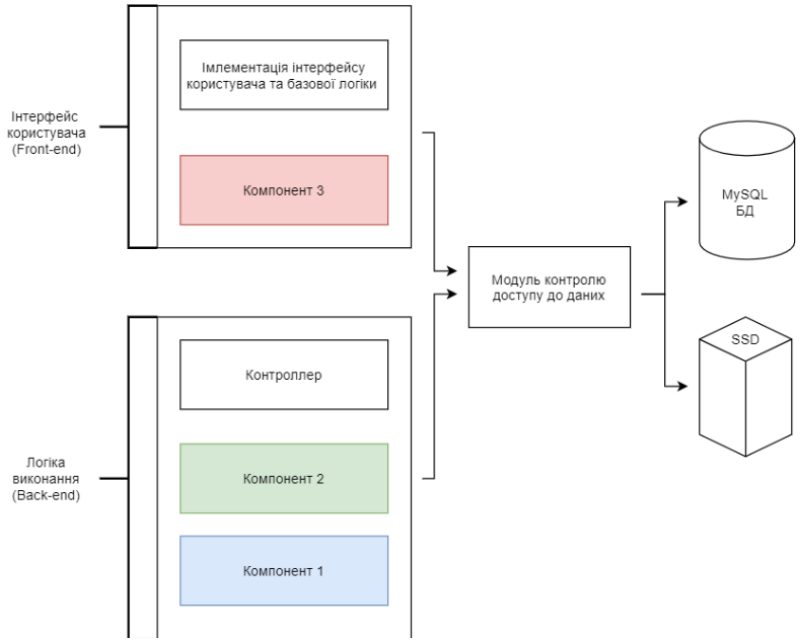

Рис. 2. Схема роботи та взаємодії між компонентами обраної архітектури веб-сервісу (оновлена версія програмного рішення)

Компоненти 1 – 3, які були використані раніше, знайшли місце у оновленій архітектурі, крім того, було розроблено окремий модуль для контролю доступу до даних (БД та системний диск). Рішення проводити дуплікацію отриманих результатів пов'язане з бажанням мінімізувати ризик втрати даних, а також мати декілька джерел. Той факт, що від сталого рішення без багатокористувачевого доступу ми змінюємо вектор на веб-сервіс із можливістю одночасного використання багатьма користувачами також мав вплив на наявну архітектуру. Було розроблено систему автентифікації та авторизації за логіком/паролем і токенами сесії, що дозволяє користувачам одночасно працювати без перешкод, отримувати доступ до своїх результатів, та ставити «задачі» на генерацію, які після завершення будуть відправляти листа на електронну пошту користувача із отриманими результатами.

Генерація послідовностей та сигналів проходить у відповідності із наведеними у теоретичній частині моделями. Наразі комплекс знаходиться на фінальній стадії розробки. Закладено можливість побудови та аналізу декількох досліджуваних типів послідовностей (М-послідовності, характеристичні дискретні сигнали, криптографічні дискретні сигнали (КДС), OFDM-сигнали). Увагу було приділено варіативності та розширенню можливостей з генерації КДС, оскільки цікавою частиною є методологія генерації криптографічного ключа. Якщо на початкових стадіях та у першій версії комплексу ми не мали змоги змінювати «на льоту» постачальника криптографічної бібліотеки, яка імплементує той чи інший алгоритм, у другій версії користувачу надано можливість обирати бібліотеку, алгоритм, вводити бажану довжину ДП, що генерується, а також особистий ключ, і все це – без втручання до програмного коду. Також однією з особливостей комплексу є модульність та відкритість до розширення новими типами сигналів і новими засобами для аналізу. Наявність інтерфейсу користувача дозволила розширити можливості з фільтрації отриманого результату без необхідності внесення змін до програмного коду, а також у декілька разів пришвидшила

загальний час роботи із комплексом. Тепер користувач має змогу візуалізувати отриманий результат та моментально перезапустити генерацію у разі необхідності. На фінальній стадії буде також запроваджено переклад порядку роботи з комплексом на три мови: російська, українська, англійська.

Апаратні характеристики робочої машини, що використовується для побудови та аналізу (вказано лише параметри, що мають прямий вплив на швидкість роботи комплексу та збереження отриманих результатів):

- центральний процесор: Intel iCore i7, 7^{th} Gen (2.9 – 3.4 GHz);
- оперативна пам'ять: 16 Gb;
- тип носія: SSD Kingston (до 550 Mb/s на запис та до 520 Mb/s зчитування);

Програмні особливості побудованого комплексу (мови програмування, деталі побудови інтерфейсу):

- мова програмування back-end частини: Java 8 (із використанням останніх особливостей для паралельної обробки);
- додаткові бібліотеки та залежності (back-end): Spring Boot, Spring Security, BouncyCastle security lib;
- мова програмування front-end (UI) частини: JavaScript, TypeScript, HTML, SCSS;
- додаткові бібліотеки та залежності (front-end): Angular 8;
- компоненти для побудови графічних елементів (графіки, діаграми): елементи, побудовані із використанням засобів та модулів Angular Framework, Grafana;
- зберігання результатів: файлова система (для вихідних файлів) + дублювання у MySQL database.

Для підвищення швидкодії під час генерації сигналів та їх аналізу використано адаптивний алгоритм конфігурації кількості одночасних потоків на центральному процесорі. Цей підхід дозволяє підвищити рівень загальної швидкості роботи програмного рішення в залежності від того, на якому апаратному комплексі він запущений.

У подальшому планується повна міграція із локальної машини до хмари (Amazon AWS, MS Azure чи Google Cloud), що дозволить, по-перше, підвищити швидкодію та, по-друге – надати повний доступ зацікавленим користувачам, які зможуть протестувати запропоновані моделі генерації та допомогти у виявленні недоліків чи запропонувати потенційні шляхи до покращення.

Крім того, ми впевнені, що завдяки відмові від власних компонентів візуалізації на користь всесвітньо визнаних засобів ми зможемо підвищити якість результатів та їх відображення, а також підвищити рівень відтворюваності отриманого результату. За бажанням кожен зможе використати запропонований комплекс для проведення власного аналізу і підтвердити достовірність наведених результатів, що є важливим для кожного дослідника.

Висновки

Авторами отримано метод синтезу нелінійних складних криптографічних дискретних сигналів (КДС) для застосування у ІКС в якості фізичного переносника даних, який використовує випадкові (псевдовипадкові) процеси і дозволяє створювати сигнали з необхідними ансамблевими, структурними і кореляційними властивостями, що дає можливість поліпшити показники ефективності інформаційно-телекомунікаційних систем, що функціонують в умовах зовнішніх і внутрішніх впливів, обумовлених, з одного боку, дією природних перешкод, перешкод від інших радіотехнічних систем, що функціонують на близьких частотах або в спільній ділянці діапазону частот, з іншого боку – навмисних перешкод, створених з метою радіоелектронного придушення діючих систем, станціями протидії. Поліпшення зазначених показників ефективності досягається, зокрема, за рахунок можливості формування із застосуванням отриманого методу великих ансамблів дискретних послідовностей практично будь-якого періоду з необхідними (для тих чи інших додатків

системи) значеннями бічних пелюсток функцій авто взаємної і стикової функцій кореляції в періодичному і аперіодичному режимах роботи, а так само статистичними характеристиками кореляційних функцій (КФ), які не поступаються аналогічним характеристикам кращих, з точки зору КФ, лінійних класів сигналів. Зазначене дає можливість підвищити завадостійкість прийому сигналів. КДС мають поліпшені в порівнянні з лінійними класами сигналів ансамблевими властивостями. Так, для періоду послідовності N=1023 обсяг системи, складений з КДС, більш ніж в 15 разів перевищує обсяг системи сигналів з трирівневою функцією взаємної кореляції, і більш ніж в 1200 разів обсяг системи, складеної з M-послідовностей. За рахунок поліпшених ансамблевих властивостей КДС і динамічної зміни відповідності біт повідомлення – складний сигнал з'являється можливість поліпшити показники інформаційної безпеки, насамперед, захищеності від нав'язування (вводу у систему) хибних повідомлень. Крім того, синтезовані з використанням розробленого методу сигнали, як показали результати тестування, за своїми статистичними властивостями близькі до властивостей випадкових послідовностей, тобто мають практично ідеальну структурну скритність, що дозволяє збільшити скритність функціонування системи.

Розроблено комплекс програмних засобів, який реалізує методи синтезу і дослідження властивостей нових класів складних нелінійних дискретних сигналів. Такий комплекс дозволяє: генерувати нелінійні КДС, нелінійні послідовності символів в кінцевих полях Галуа [14, 15], M-послідовності, OFDM-сигнали практично будь-якої тривалості; визначати значення мінімальних і максимальних бічних викидів різних КФ; порівнювати отримані значення з відомими, потенційно досяжними границями для відповідних КФ; синтезувати на основі КДС і ортогональних систем сигналів похідні системи сигналів із заданими властивостями; визначити синтезованим послідовностям унікальні ідентифікатори (спеціальні радіодані), які необхідні для оптимальної обробки даних; визначати і досліджувати статистичні, ансамблеві характеристики синтезованих нелінійних сигналів. Програмне та математичне забезпечення методів синтезу, формування, обробки і дослідження властивостей систем нелінійних сигналів, практично готове до можливого застосування в складі дослідних зразків і елементів цифрових комунікаційних засобів сучасних ІКС.

Можливості отриманого програмно-апаратного комплексу із застосуванням додаткового відповідного математичного апарату дозволяють здійснювати синтез та аналіз безлічі класів сигналів, у тому числі й тих, які наведено у даній публікації.

Список літератури:

1. 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 Volume 76, 2017 Issue 19, pages 1705-1717 DOI: 10.1615/TelecomRadEng.v76.i19.30.

2. Gorbenko I.D., Zamula A. A., Morozov V. L., Rodionov S.V. Mathematical model of orthogonal frequency distribution and multiplexing (OFDM) signals // Радіотехніка. 2019. Вип. 198. С. 32 44.

3. Замула О.А. Технологии формирования OFDM сигналов в современных информационно-коммуникационных системах // Радіотехніка. 2018. Вип. 193. С. 152 159.

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

5. Варакин Л. Е. Системы связи с шумоподобными сигналами. Москва : Сов. радио, 1985. 384 с.

6. Ipatov Valery P. 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.

7. Горбенко І.Д., Замула О.А. Вдовенко С.Г. Аналіз функції невизначеності і структури спектрів ЛЧМ-сигналів // Вісник інженерної академії України. 2018. Вип.2. С.52-56.

8. Горбенко І.Д., Замула О.А. Дослідження структури спектрів сигналів з лінійною частотною модуляцією // Радіотехніка. 2018. Вип. 193. С.192 -199.

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

10. 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. Vol. 75, 2016 Issue 2. Pages 169-178. DOI: 10.1615/TelecomRadEng.v75.i2.60.

11. Methods for implementing communications in info-communication systems based on signal structures with specified properties / Gorbenko I., Zamula A., Morozov V. // 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.

12. Gorbenko I. D., Zamula A. A., Semenko A. E., Morozov V. L. Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes // Telecommunications and Radio Engineering Vol. 76, 2017 Issue 18, pages 1581-1594. DOI: 10.1615/TelecomRadEng.v76.i18.10.

13. 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: Технічні науки : зб. наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2019. Вип. 19. 160 с.

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

15. Gorbenko Ivan, Zamula Alexander, Morozov Vladyslav. Information and communication systems based on signal systems with improved properties building concept // Workshop Proceedings 2019 CEUR.

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

Надійшла до редколегії 03.09.2020

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, головний конструктор АТ «Інститут інформаційних технологій», Україна, e-mail: GorbenkoI@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-4616-3449

Семенко Евген Олександрович – Харківський національний університет імені В.Н. Каразіна, пошукач наукового ступеня «кандидат технічних наук», кафедра безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна.

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, e-mail: zamylaaa@gmail.com, ORCID: http://orcid.org/0000-0002-8973-6190