МЕТОДИ СИНТЕЗУ ТА АНАЛІЗУ СИГНАЛІВ

УДК 621.391 **DOI:10.30837/rt.2020.4.203.12**

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

МЕТОДИ СИНТЕЗУ І ФОРМУВАННЯ СИСТЕМ НЕЛІНІЙНИХ ДИСКРЕТНИХ СИГНАЛІВ ДЛЯ СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Вступ

Один з основних напрямків розвитку сучасних інформаційно-комунікаційних систем (ІКС) базується на розробці і впровадженні методів багатостанційного доступу із застосуванням кодового розподілення шумоподібних складних сигналів (ШСС), які належать абонентам. Їх застосування дозволяє забезпечити високоефективне використання смуги частот, високу завадостійкість прийому сигналів, скритність, конфіденційність і імітозахищеність передавання даних при впливі сукупності різноманітних завад та наявності завмирань у радіоканалах, які обумовлені як умовами розповсюдження сигналів, так і багатопроміневістю каналів зв'язку. Основними задачами, які необхідно вирішувати при реалізації зазначеного напрямку, є синтез класів ШСС у залежності від умов функціонування і призначення ІКС, а також ефективних алгоритмів обробки ШСС на фоні сукупності структурних широкосмугових та вузькосмугових завад.

Процес вибору раціональних по тих чи інших критеріях структур складних сигналів тотожний синтезу відповідних маніпулюючих дискретних послідовностей (ДП). Як критерії вибору класу дискретних сигналів (ДС), як правило, орієнтуються на критерій мінімуму взаємних перешкод (мінімаксний критерій). Застосовувані в ІКС широкосмугові сигнали повинні володіти такими кореляційними властивостями, коли бічні піки кореляційних функцій (КФ) ШСС є якомога меншими, тобто в ідеальному випадку повинні прагнути до нуля [1 – 2]. Використовувані в ІКС методи інформаційного обміну, а також класи ШСС, що застосовуються в якості фізичного переносника даних (множини лінійних рекурентних послідовностей (М-послідовності), Касамі, Голда, Камалєтдінова і ін.), які мають порівняно невеликі значення бічних пелюсток авто- і взаємних КФ, не дозволяють забезпечити необхідні (для відповідних додатків ІКС) показники інформаційної безпеки і завадозахищеності [3].

До ІКС, що створені і функціонують на об'єктах критичної інфраструктури, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування: достовірності і швидкості передачі інформації, живучості, завадозахищеності, інформаційної і кібербезпеки. У таких умовах особливого значення набуває наявність і застосування захищених ІКС. Під захищеністю систем необхідно розуміти, в широкому сенсі, їх здатність забезпечувати необхідні показники з завадозахищеності, імітостійкості, інформаційної, енергетичної і структурної скритності, швидкості передавання інформації, частотної і енергетичної ефективності.

Метод синтезу систем нелінійних дискретних сигналів із застосуванням випадкових (псевдовипадкових) процесів

Дослідження [4 – 5] показали, що дискретні послідовності (ДП) повинні бути засновані на нелінійних правилах побудови і мати покращені кореляційні, ансамблеві і структурні властивості.

Продуктивним кроком, з точки зору нового напряму використання систем складних сигналів у захищених ІКС, є синтез систем нелінійних дискретних сигналів (КС). Такі дискретні сигнали володіють необхідними, але обмеженими (значеннями «щільної упаковки»), кореляційними і ансамблевих властивостями.

Авторами сформульована у загальному вигляді і вирішена задача синтезу нового класу сигналів-фізичних переносників даних для застосування у сучасних ІКС, – нелінійних складних дискретних криптографічних сигналів (КС) [6 – 7]. Крім того, теоретично обґрунтовано [6] комплексне вирішення проблеми забезпечення завадозахищеності та інформаційної безпеки функціонування ІКС на основі реалізації динамічного режиму передачі інформації, при якому відповідність: біт повідомлення – складний сигнал змінюється з плином часу за законом, визначення якого можливо з імовірністю, що не перевищує допустимого в системі значення, і застосування (в якості фізичних переносників даних) сигналів з необхідними кореляційними, ансамблевими, структурними властивостями. При цьому системи сигналів повинні ґрунтуватися на нелінійних правилах побудови. Під криптографічними дискретними сигналами (КС) пропонується розуміти сукупність послідовностей (векторів) символів певного алфавіту, які мають необхідні (задані) структурні, ансамблеві і кореляційні властивості, часову і просторову складності, і існує можливість їх формування на основі криптографічних ключів. Необхідно відзначити особливі властивості систем КС: синтез таких сигналів засновано на використанні випадкових або псевдовипадкові процесів, у тому числі алгоритмів криптографічного перетворення інформації; можливість їх відновлення в просторі і в часі із застосуванням параметрів, які обумовлені принципами їх синтезу, у тому числі ключів, причому довжина ключа може бути істотно менше за період (тривалість) самого сигналу. Подальші дослідження [8] показали, що саме такий спосіб інформаційного обміну і застосування саме КС як фізичних переносників даних забезпечують можливість побудови захищених каналів ІКС, у яких можуть бути реалізовані необхідні значення показників інформаційної безпеки та завадозахищеності в умовах впливу структурних, загороджувальних, ретрансльованих та інших видів перешкод. При такому підході структурна скритність і інформаційна безпека ІКС забезпечуються шляхом застосування (як основи синтезу) випадкових або псевдовипадкових процесів (з використанням криптографічних ключів), і формування, таким чином, ДП, властивості яких близькі до властивостей випадкових послідовностей. Завадостійкість прийому забезпечується необхідними кореляційними властивостями системи сигналів, що синтезується. 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.

Постановка задачі синтезу нелінійних дискретних криптографічних сигналів (КС)

Під задачею побудування (синтезу) КС будемо розуміти [9] 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 КС в частині структурних, ансамблевих, кореляційних властивостей, просторової та часової складності їх генерування. Правила синтезу КС ґрунтуються на основі використання та аналізу періодичних та аперіодичних функцій кореляції та зводиться до наступних етапів.

1. Побудова КС W^q, періодична функція автокореляції (ПФАК) кожного з яких, задовольняє системі нелінійних параметричних нерівностей (НПН):

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

де $R_{a_1}^q(l)$ і $R_{a_2}^q(l)$ – задані значення реалізації ПФАК, а індекси обчислюються по модулю $(i+1) \bmod L$.

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

$$\sum_{i=0}^{L} W_i^q W_i^q = L,\ q=\overline{1,N}. \qquad (2)$$

3. Побудова пар КС W^q та W^p, функції взаємної кореляції (ФВК) яких задовольняють вимогам, що визначаються сукупністю систем НПН (3-7), а також задовольняють вимогам до стикових функцій взаємної кореляції (СФВК) пар КС W^q та W^p зі стиковими дискретними словами W^{qp} і W^{pq}:

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

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

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

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

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

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

Дослідження показали [10], що вказаний клас задач може розв'язуватись при застосуванні методу, який включає такі етапи:

1. Формування дискретних послідовностей з використанням випадкових (псевдовипадкових процесів, у тому числі із використанням алгоритмів криптографічного перетворення інформації).

2. Побудова необхідного числа потенційних КС W^q згідно системи (1).

4. Знаходження пар чи підмножин КС W^q та W^p, які задовольняють вимогам (3) – (7).

5. Побудова матриці станів взаємно-кореляційних функцій всіх можливих пар потенційних КС, які пройшли відбір за результатами попереднього кроку та мають необхідні ансамблеві, кореляційні властивості.

6. Аналіз матриці станів та формування необхідного числа підмножин чи пар КС згідно з (1) – (2) та (3) – (7) та відбір в підмножину лише тих, що задовольняють встановленим вимогам, у тому числі граничним значенням бічних пелюсток функцій кореляції для відповідних значень періоду послідовностей.

Аналіз зазначених кроків показує, що продуктивність синтезу системи КС у ряді випадків не може задовільнити вимоги власників (користувачів) ІКС. Дійсно, загальний час синтезу одного з безлічі КС може бути обчислено за виразом

$$T_{CS} = h \cdot (T_{GEN} + T_{PFAC} + T_{R_{\max}} + T_{IF} + (R_{\max} \le R_{\max}^*) \cdot T_{write}) \ , \quad (8)$$

де: h – кількість спроб вибору КС W^q, який задовольняє умові (1) (етапи 1 - 2 методу);

T_{GEN} – час, необхідний для генерації КС (етап 1 методу);

T_{PFAC} – час, необхідний для обчислення значень ПФАК;

$T_{R_{\max}}$ – час, необхідний для пошуку максимальних значень бокових пелюсток $R_{\max}$ ПФАК;

T_{IF} – час, необхідний для порівняння $R_{\max}$ з встановленим граничним значенням $R_{\max}$ (перевірка вимог (3) – (7) (етап 4 методу));

T_{write} – час, необхідний для запису обраного КС у структуру даних (список, файл та інше).

Останній доданок $R_{\max} \le R^*_{\max}$ приймає значення: якщо цей вислів істинно, то буде 1 помножене на T_{write} (тобто сформований сигнал записується в ту чи іншу структуру даних) і 0 помножене на T_{write} - в іншому випадку (тобто сигнал відкидається і час T_{write} не буде враховано).

Наведемо приклад синтезу множини сигналів з застосуванням наведеного методу.

Приклад: Припустимо для формування одного сигналу нам треба застосувати три спроби, другого сигналу – десять спроб. Тоді, загальний час формування множини сигналів:

$$T_{CS} = \begin{array}{l} 3\cdot(T_{GEN} + T_{PFAC} + T_{R_{\max}} + T_{IF} + (R_{\max} \le R^*_{\max})\cdot T_{write}) + \\ +10\cdot(T_{GEN} + T_{PFAC} + T_{R_{\max}} + T_{IF} + (R_{\max} \le R^*_{\max})\cdot T_{write})\cdot \end{array} \quad (9)$$

Узагальнюючи наведені міркування, можна отримати вираз для розрахунку часу, який є необхідний для синтезу всієї системи КС для визначеного періоду N.

Тобто, вираз для часу формування ансамблю КС із заданими властивостями буде мати наступний вигляд:

$$T_{total} = \sum_{i=1}^{M} T_{CS\,i} \ , \quad (10)$$

де M – об'єм системи сигналів для числа елементів послідовності N.

Метод синтезу систем нелінійних дискретних сигналів із застосуванням операції децимації

Пропонується новий метод синтезу системи КС для визначеного періоду ДП N.

Твердження. Якщо криптографічну послідовність W_i періоду N піддати операції децимації з індексом децимації k, причому k є взаємно простим з N, то результуюча послідовність V_{ik} буде такою ж криптографічною послідовністю, такого ж періоду з властивостями, що є ідентичними властивостям вихідної послідовності W_i.

Операція децимації зводиться до вибору кожного k-го символу послідовності W_i і запису отриманих таким чином елементів послідовності один за одним, так що $W_i = V_{ik}$.

У табл. 1 наведено приклад вихідної послідовності W_i з числом елементів $N = 256$.

Таблиця 1

Signal: [-1, 1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, -1, 1, 1, 1, 1, -1, 1, -1, -1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1, 1, -1, 1, 1, 1, -1, 1, -1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, -1, 1, 1, -1, 1, 1, -1, 1, 1, -1, 1, -1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, 1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, -1, -1, -1, -1, -1, -1, 1, 1, -1, 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, -1, -1, 1, 1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1]

У табл. 2 – 3 наведено приклади реалізації процедури децимації послідовності G_i з числом елементів $N = 256$ за індексами децимації $k = 3$ і $k = 5$ відповідно.

Таблиця 2

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, 1, 1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, 1, -1, -1, -1, 1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, 1, 1, -1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, 1, 1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, 1, -1, 1, 1, 1, -1, -1, 1]

Таблиця 3

1) [-1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1, 1, -1, -1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, 1, -1, -1, -1, 1, 1, -1, -1, -1, -1, 1, -1, -1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1, 1, -1, 1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1, 1, -1, -1, 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, 1, 1, 1, -1, 1, -1, -1, -1, 1, 1, -1, -1, -1, -1, -1, -1, 1, 1, -1, 1, 1, -1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, -1, -1, 1, -1, 1, 1, -1, 1, 1, -1, -1, 1, -1, -1, 1, -1, 1, -1, 1, -1, -1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1]

Оцінимо час, необхідний для реалізації синтезу системи КС із застосуванням запропонованого методу.

Аналіз операцій, які визначені вищенаведеним твердженням, показує, що час, який необхідно для синтезу одного з множини КС із застосуванням операції децимації, може бути визначено, як

$$T_D = T_{read} + T_{pos} + T_{perm} + T_{write}, \tag{11}$$

де: T_{read} – час, необхідний для зчитування вихідних даних (вихідна послідовність (W_i), індекс децимації);

T_{pos} – час, необхідний для розрахунку позиції за індексом децимації, що використовується;

T_{perm} – час, необхідний для запису елементів вихідної послідовності (W_i) за новими позиціями, які визначені відповідним індексом децимації (k);

T_{write} – час, необхідний для запису сформованої шляхом децимації послідовності (V_{ik}) у структуру даних.

Час, необхідний для формування всієї системи (ансамблю) КС, для числа елементів N, може бути визначено (за умови, що вихідний сигнал (W_i) попереднє сформовано), як

$$T_{total} = T_{coprimes} + \varphi(N) \cdot T_D, \tag{12}$$

де: $\varphi(N)$ – функція Ейлера;

$T_{coprimes}$ – час, необхідний для розрахунку множини чисел, які є взаємно простими з N;

T_D – час, необхідний для реалізації процедури децимації для формування однієї з послідовностей (V_{ik}) за методом децимації.

Якщо попередньо вихідний сигнал (W_i) не сформовано, вираз (12) буде мати вигляд

$$T_{total} = T_{CS} + T_{coprimes} + \varphi(N) \cdot T_D. \tag{13}$$

Програмне моделювання процесу синтезу КС із застосуванням методу, що використовує випадкові (псевдовипадкові) процеси (вирази (1) – (7)) показує, що середній час на синтез ансамблю КС (128 послідовностей) з числом елементів $N = 256$, у середньому складає 60.821875 секунд. Середній час на синтез ансамблю КС (128 послідовностей) з числом елементів $N = 256$, із застосуванням запропонованого методу децимації у середньому складає 0.009375 секунди (за умови, що попередньо вихідний сигнал W_i сформовано). Таким чином, виграш у часі формування системи сигналів із застосуванням методу децимації для наведеного прикладу складає приблизно $6{,}5 \cdot 10^3$. Якщо вихідний сигнал W_i попереднє не сформовано (вираз (13)) виграш у часі формування системи сигналів із застосуванням методу децимації складає більш ніж 10^2.

У табл. 4 наведено розраховані нормовані статистичні характеристики ($\frac{R_{б\max}}{\sqrt{N}}$ – максимальне значення бокових піків кореляційних функцій (КФ); $\frac{m_{|R|}}{\sqrt{N}}$ – математичне очікування модуля бокових піків КФ; $\frac{D_{|R|}}{\sqrt{N}}$ – дисперсія модуля бокових піків КФ; $\frac{D_{|R|}^{1/2}}{\sqrt{N}}$ – середнєквадратичне відхилення модуля бокових піків КФ; $\frac{D_R^{1/2}}{\sqrt{N}}$ – середнєквадратичне відхилення бокових піків КФ; $\frac{\gamma}{\sqrt{N}}$ - коефіцієнт ексцесу) різних КФ для КС (ПФАК, АФАК – періодична і аперіодична функції автокореляції, відповідно; ПФВК, АФВК – періодична і аперіодична функції взаємної кореляції, відповідно).

Таблиця 4

Тип функції кореляції (КФ)	Сигнал	N	$\frac{R_{б\max}}{\sqrt{N}}$	$\frac{m_{\|R\|}}{\sqrt{N}}$	$\frac{D_{\|R\|}}{\sqrt{N}}$	$\frac{D^{1/2}_{\|R\|}}{\sqrt{N}}$	$\frac{D^{1/2}_{R}}{\sqrt{N}}$	$\frac{\gamma}{\sqrt{N}}$
ПФАК	Вихідний сигнал	256	1.996105	0.764257	4.051119	0.502695	0.914000	5.882533
	Сигнали, що отримані методом децимації	256	1.996105	0.762401	4.058512	0.503153	0.914000	5.882533
АФАК	Вихідний сигнал	256	1.996105	0.507131	2.954548	0.429301	0.664171	10.894494
	Сигнали, що отримані методом децимації	256	1.954520	0.505330	2.675348	0.407925	0.649360	11.255518
ПФВК	Вихідний сигнал з іншими ізоморфізмами	256	2.966434	0.807777	6.096691	0.616376	1.015907	0.047603
	Сигнали, що отримані методом децимації	256	2.876332	0.807561	6.147075	0.618564	1.017259	0.049834
АФВК	Вихідний сигнал з іншими ізоморфізмами	256	2.273342	0.535305	3.353158	0.456910	0.703664	0.132458
	Сигнали, що отримані методом децимації	256	2.380771	0.543414	3.555152	0.470007	0.718335	0.126386

Аналіз даних табл. 4 показує, що значення максимальних бокових піків (пелюсток), а також статистичних характеристик різних КФ для КС, що отримані із використанням методу, заснованому на застосуванні випадкових (псевдовипадкових) процесів і методу децимації практично ідентичні.

Висновки

Запропоновано методи синтезу і формування системи сигналів одного класу нелінійних дискретних складних сигналів, а саме, так званих, криптографічних сигналів. Наведено математичну модель синтезу зазначених систем сигналів. Перший метод, що представлено, використовує випадкові (псевдовипадкові) процеси, у тому числі, алгоритми криптографічного

перетворення інформації із застосуванням секретних ключів, і заснований на використанні та проведенні аналізу періодичних та аперіодичних функцій кореляції. Інший метод засновано на реалізації операції децимації вихідної дискретної послідовності символів, яка отримана за результатами реалізації першого методу і забезпечує синтез системи сигналів для визначеної тривалості сигналу. Отримано аналітичні вирази для визначення часу синтезу системи сигналів із застосуванням запропонованих методів. На основі реалізованої програмної моделі показано, що швидкодія методу формування сигналів на основі операції децимації, для визначеної тривалості сигналу, більш ніж на три порядки перевищує швидкодію методу, що засновано на використанні випадкових (псевдовипадкових) процесів. При цьому, на основі проведеного комп'ютерного моделювання показано, що сигнали, які отримані із застосуванням запропонованих методів, володіють ідентичними властивостями (кореляційними, ансамблевими, структурними).

Отримані результати можуть знайти застосування при побудові захищених сучасних інформаційно-комунікаційних систем, до яких висуваються підвищені вимоги до завадостійкості прийому сигналів при впливі різноманітних завад, скритності, конфіденційності, імітозахищеності і швидкості передачі інформації.

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 Volume 76, 2017 Issue 19, pages 1705-1717 DOI: 10.1615/TelecomRadEng.v76.i19.30.
4. Methods for implementing communications in info-communication systems based on signal structures with specified properties / I. D. Gorbenko, A. A. Zamula, V. L. 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.
5. 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.
6. Gorbenko I. D., Zamula A. A. Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems // Telecommunications and Radio Engineering Volume 76, 2017. Issue 12, pages 1079-1100. DOI: 10.1615/TelecomRadEng.v76.i12.50.
7. Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic sig-nals 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.
8. Gorbenko I. D., Zamula A. A., Morozov V. L. Information and communication systems based on signal systems with improved properties building concept. Workshop Proceedings 2019 CEUR.
9. 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: Фіз.-мат. науки : зб. наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2017. Вип. 15. 272 с.
10. 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 / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2019. Вип. 19. 160 с.

Надійшла до редколегії 17.09.2020

Відомості про авторів:

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

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

Хо Чі Лик – магістрант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна,Україна.