

УДК 621.391.8:517.587

doi: 10.32620/reks.2021.3.07

К. С. ВАСЮТА¹, У. Р. ЗБЕЖХОВСЬКА¹, В. В. СЛОБОДЯНЮК¹,
І. В. ЗАХАРЧЕНКО¹, О. Л. КАЩИШИН¹, М. С. ДУБИНСЬКИЙ¹,
Ю. М. РЯБУХА², О. В. КОВАЛЬ¹

¹ Харківський національний університет Повітряних Сил імені Івана Кожедуба,
Харків, Україна

² Харківський національний університет імені В. Н. Каразіна, Харків, Україна

МЕТОД ПІДВИЩЕННЯ СКРИТНОСТІ СИСТЕМ ПЕРЕДАЧІ ІНФОРМАЦІЇ НА ОСНОВІ МОДУЛЯЦІЇ З ОРТОГОНАЛЬНИМ ЧАСТОТНИМ РОЗДІЛЕННЯМ І МУЛЬТИПЛЕКСУВАННЯМ ХАОТИЧНИХ ПІДНЕСУЧИХ

Предметом дослідження є процеси формування та обробки сигналів з ортогональним частотним розділенням та мультиплексуванням (OFDM – orthogonal frequency division multiplexing) хаотичних послідовностей для забезпечення необхідного рівня скритності передачі даних. *Метою* дослідження є синтез методу підвищення скритності систем передачі інформації, які використовують сигнали з OFDM-модуляцією, за допомогою формування піднесучих із застосуванням аналітичного сигналу та хаотичного відображення поліному Чебишева першого роду третього порядку. Це надасть можливість забезпечити надійний захист інформації в радіотехнічних системах передачі інформації, які використовують сигнали з OFDM-модуляцією, завдяки високому рівню структурної та Independent and Identically Distributed (IID) (ступінь маскуванню сигналу під шум) - скритності сигналів. *Завдання:* дослідити ефективність розробленого методу підвищення скритності систем передачі інформації за допомогою чисельного оцінювання рівня структурної та IID-скритності. Дослідити якість відновлення замаскованої інформації на приймальній стороні. Використовуваними *методами* є: для формування та обробки хаотичних піднесучих в сигналі з OFDM-модуляцією – методи нелінійної динаміки, підходи формування аналітичного хаотичного сигналу та методи статистичної теорії обробки спостережень; для оцінки рівня структурної та IID-скритності – теорія стегаєнографії, метод нелінійного аналізу часового ряду, заснований на використанні Brock Dechert Scheinkman (BDS) - статистики. *Отримано наступні результати:* синтезовано метод підвищення скритності систем передачі інформації, заснований на використанні сигналів з OFDM-модуляцією хаотичних піднесучих. Проведено оцінювання рівня структурної та IID-скритності сигналів, які сформовано за допомогою запропонованого методу. Встановлено, що в порівнянні з системами, які застосовують гармонічні сигнали з OFDM-модуляцією, хаотичні сигнали з OFDM-модуляцією здатні забезпечити вищий рівень IID-скритності. Це підтверджується отриманими результатами візуального, частотного, статистичного та динамічного аналізу. Для оцінювання рівня структурної скритності оцінено затрати на виявлення сформованих сигналів із заданою ймовірністю. *Отримані результати* показали, що рівень структурної скритності збільшився у 2...2,5 рази. Показано, що для забезпечення необхідного рівня відновлення сформованого сигналу відношення сигнал/шум на вході приймача має бути більшим 4 дБ. *Висновки.* Наукова новизна отриманих результатів полягає у наступному: вперше отримано метод формування піднесучих для сигналів з OFDM-модуляцією на основі використання аналітичного сигналу та поліному Чебишева першого роду третього порядку. Запропонований метод забезпечує необхідний рівень структурної та IID-скритності систем передачі інформації, в порівнянні зі звичайними методами формування сигналів з OFDM-модуляцією, через схожість сформованих сигналів з “білим” шумом. При цьому запропонований метод надає можливість використовувати такі сигнали у радіотехнічних системах передачі інформації.

Ключові слова: система передачі інформації; IID-скритність; OFDM-модуляція; псевдофазовий простір; BDS-статистика.

Вступ

Стрімкий розвиток систем передачі інформації (СПІ) зумовлює застосування різних підходів до розроблення нових та вдосконалення існуючих видів сигналів, де одним з найбільш перспективних є широкосмугові сигнали (ШСС) [1]. ШСС широко застосовуються в сучасних високошвидкісних СПІ

стандартів WiMax, LTE (long term evolution), під час передачі інформації цифрового телебачення (DVB-T (digital video broadcasting-terrestrial)) і радіо (DRM (digital radio mondiale)). При цьому в перерахованих стандартах використовуються ШСС з ортогональним частотним розділенням з мультиплексуванням (OFDM – orthogonal frequency division multiplexing) [2]. Сигнали з OFDM-модуляцією до-

звляють не лише підвищити інформаційну ємність системи при обмеженій смузі пропускання, але і швидкість прийомо-передачі інформації, збільшити скритність і завадозахищеність СПІ [3-5].

Однак зі збільшенням об'ємів інформації, що передається актуальним стає питання її надійного захисту від несанкціонованого доступу [6, 7]. Це може бути досягнуто шляхом забезпечення [8, 9]:

- енергетичної скритності сигналів, яка направлена на суттєве ускладнення виявлення сигналу засобами радіоелектронної розвідки (РЕР);

- структурної скритності сигналів, яка характеризується затратами засобів РЕР, які необхідні для виявлення структури і параметрів сигналу [10];

- інформаційної скритності сигналів, яка характеризується здатністю протистояти мірам, направленим на викриття змісту інформації, що передається. Вона може бути забезпечена криптографічними методами шифрування інформації;

- Independent and Identically Distributed (IID) - скритності сигналів, яка характеризує скритність сигналів із точки зору їх маскуванню під шум [9, 13]. А саме, показує близькість "образу" сигналу в псевдофазовому просторі до "образу" "білого" шуму.

В умовах масового застосування СПІ із сигналами з OFDM-модуляцією, криптографічні методи приховування інформації здатні забезпечити необхідний рівень її інформаційної скритності. Наприклад, у роботі [12] запропоновано здійснювати шифрування інформації за допомогою використання алгоритму кубика Рубіка. Проведенні статистичні тести показують, що така система здатна забезпечити високий рівень інформаційної скритності. Але в той же час, у роботах авторів [13] показано, що такі сигнали мають низький рівень структурної та IID-скритності, що робить обмеженим їх подальше використання під час організації скритного радіозв'язку, особливо в СПІ спеціального призначення. Тому необхідно розробити такі методи формування сигналів з OFDM-модуляцією для скритної передачі інформації, при використанні яких витрати часу й технічних засобів РЕР на їх пошук були б настільки великими, що стали б недоцільними, тобто сигнали мали б високий рівень структурної та IID-скритності.

Таким чином, актуальність наукового дослідження полягає у розробленні методу скритної передачі інформації з одночасно високим рівнем структурної та IID-скритності з використанням сигналів з OFDM-модуляцією.

Для вирішення цієї проблеми в роботі [14] запропонована схема, використання якої надає змогу суттєво підвищити рівень захисту інформації від перехвату при використанні сигналів з OFDM-модуляцією. Авторами пропонується здійснювати

збільшення арсеналу можливих реалізацій сигналів з OFDM-модуляцією, за рахунок використання псевдовипадкової зміни декількох параметрів сигналу, як по частоті, так і за часом. Отримані результати вказують на високий рівень структурної скритності такої СПІ, однак рівень IID-скритності залишається незадовільним. Також, у роботі [15] запропоновано варіант підвищення структурної скритності СПІ заснованої на використанні сигналів з OFDM-модуляцією. Він полягає в тому, що для передачі повідомлень пропонується використовувати сформовані стохастичним чином ортогональні системи сигналів, які описуються власними векторами діагональних позитивно визначених симетричних матриць. При цьому, використовується властивість ортогональності власних векторів. Запропонований метод дає змогу значно підвищити структурну скритність сигналів з OFDM-модуляцією. Але він є обчислювально складним та не забезпечує високий рівень IID-скритності.

Останнім часом для вирішення питання, щодо підвищення одночасно рівня і структурної, і IID-скритності СПІ пропонується використовувати хаотичні сигнали та послідовності [16-18]. У таких СПІ, навіть невелика зміна керуючого параметра дає надійно зафіксовану зміну характеру сигналу, що створює велику кількість можливих реалізацій для модуляції повідомлень. Також хаотичні сигнали здатні забезпечити необхідний рівень IID-скритності, оскільки під час спектрального та кореляційного аналізу є візуально схожими із шумом спостереження.

Під час розроблення перших СПІ з використанням хаотичних послідовностей були зроблені припущення, що спостережуваний сигнал є шумоподібним, тобто сигнал маскується під шум і має близькі до нього статистичні характеристики. У подальшому методами нелінійної динаміки було показано, що для більшості простих моделей динамічного хаосу можна знайти "образи" в псевдофазовому просторі, які є структурованими, на відміну від, шуму спостереження з незалежними значеннями. Таким чином, аналіз ступеню однорідності "образів" хаотичних сигналів у псевдофазовому просторі може привести до компрометації сигналів. Для підвищення рівня скритності хаотичних сигналів, тобто "руйнування" структури "образу" в псевдофазовому просторі в роботі [19] авторами запропоновано використовувати лінійне інтегральне перетворення "білого" шуму з ядром Мандельброта і його дискретні апроксимації. Лінійно-перетворена хаотична послідовність отримується шляхом заміни в перетворенні "білого" шуму хаотичною послідовністю. У роботі [9] для "руйнування" структурованості "образу" хаотичного сигналу запропоновано викорис-

товувати аналітичні хаотичні послідовності (АХП), представлені у вигляді коливального процесу. Проведені дослідження були направлені на вибір частоти модуляції АХП, яка впливає на структуру “образу” в псевдофазовому просторі і варіант використання АХП для скритної передачі бінарних повідомлень. Результати показали, що правильний вибір частоти модуляції дає можливість забезпечити необхідний рівень ПД-скритності. Запропоновані авторами методи дають змогу суттєво змінити статистичні характеристики вихідної послідовності (сигналу), приближуючи їх до характеристик “білого” шуму. Однак, недоліком запропонованих методів є те, що сформовані сигнали є дискретними. Це унеможлиблює їх практичне застосування в радіотехнічних СП.

В роботі [20] запропоновано метод попереднього кодування сигналів з OFDM-модуляцією з застосуванням хаотичних послідовностей. Використання даного методу дає змогу досягти більшу пропуску здатність СП, порівняно з класичним методом формування сигналів з OFDM-модуляцією. В [21] на прикладі динамічної системи Лоренца та відображень Енона й Бернуллі, проведено моделювання інформаційного каналу з використанням хаотичних сигналів нелінійних динамічних систем. Аналіз автокореляційних функцій сформованих сигналів показав, що вони мають вигляд, подібний до автокореляційної функції стаціонарного “білого” шуму. Це може вказувати на високий рівень ПД-скритності. Однак авторами не проводились дослідження рівня скритності сигналів, сформованих запропонованими методами, що робить неможливим її подальше використання для організації скритного радіозв’язку.

В роботі [11] авторами запропоновано метод прихованої передачі інформації в системах з OFDM-модуляцією. Кожна піднесуча сигналу з OFDM-модуляцією генерувалась з використанням поліномів Чебишева першого роду різних порядків. Отримані результати вказують на високий рівень ПД-скритності. Але авторами не показано спосіб відновлення такого повідомлення на приймальній стороні, що унеможлиблює його використання в СП.

В [22] запропоновано метод шифрування даних у сигналах з OFDM-модуляцією на фізичному рівні. При цьому псевдовипадкова послідовність для шифрування інформації формується за допомогою логістичного відображення, властивістю якого є те, що при певних початкових умовах воно показує хаотичну поведінку. В [23] запропоновано метод шифрування даних у сигналах з OFDM-модуляцією з використанням фракталів в хаотичній формі. Об’єднання вхідних даних з псевдовипадковою фрактальною послідовністю, у вигляді хаосу, дає змогу покращи-

ти інформаційну скритність системи. Це підтверджується тим, що час, витрачений на отримання інформації сторонньою особою без знання ключа, складає роки. В [24] запропоновано метод захисту даних від несанкціонованих атак з використанням матриці скремблювання символів сузір’я сигналів з OFDM-модуляцією, яка базується на ключі, отриманому за допомогою одновимірної нелінійної динамічної системи, з використанням логістичного відображення. При введенні неправильних початкових умов, навіть з 4-ма знаками після коми, буде отримана абсолютно інша послідовність, що призведе до формування помилкових сузір’їв, і як наслідок, це забезпечить надійний захист даних від несанкціонованого доступу. Запропоновані методи забезпечують необхідний рівень інформаційної скритності, але при цьому рівень структурної та ПД-скритності залишається незадовільним. Також у роботах авторів [25, 26] запропоновані способи підвищення рівня інформаційної скритності сигналів з OFDM-модуляцією за допомогою використання хаотичних послідовностей. Отримані технічні рішення дають змогу забезпечити високий рівень інформаційної скритності, при цьому, їх загальними недоліками є незадовільний рівень структурної, ПД-скритності та можливість застосування лише під час передачі інформації оптичними лініями зв’язку.

Зазначене вище вказує, що проблема забезпечення одночасно високого рівня структурної та ПД – скритності сигналів у радіотехнічних СП є досить гострою й до цього часу невирішеною в більшості прикладних задач. При цьому враховуючи широке використання СП, що застосовують сигнали з OFDM-модуляцією, постає питання забезпечення надійного захисту інформації, що циркулює в них. Перераховані проблеми можуть бути вирішені за допомогою використання хаотичних послідовностей під час формування піднесучих у сигналах з OFDM-модуляцією. Таким чином, науково-прикладною задачею є розроблення методу формування сигналів з OFDM-модуляцією з використанням хаотичних послідовностей, який зможе забезпечити одночасно високий рівень структурної та ПД-скритності.

Метою дослідження є розроблення методу підвищення скритності СП з використанням сигналів з OFDM-модуляцією та хаотичних піднесучих.

1. Метод підвищення скритності передачі інформації в системах з ортогональним частотним розділенням і мультиплексуванням

Основою існуючого методу формування сигналів з OFDM-модуляцією є те, що смуга пропускання каналу розбивається на групу з N ортогональних

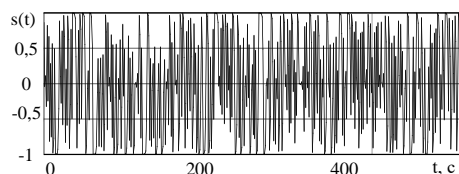
вузких смуг (піднесучих). При цьому, сигнал на всіх піднесучих передається одночасно, що дає змогу забезпечити високу швидкість передачі даних при невеликій швидкості передачі в кожній піднесучій. Формування підканалів з ортогональними піднесучими відбувається за допомогою використання процедури оберненого швидкого перетворення Фур'є, а відновлення – прямого швидкого перетворення Фур'є. Проте формування піднесучих у сигналах з OFDM-модуляцією відбувається за допомогою використання гармонічних функцій, які не здатні забезпечити необхідний рівень структурної та IID-скритності.

Тому, метод підвищення скритності в системах, що використовують сигнали з OFDM-модуляцією, пропонується будувати за допомогою використання піднесучих, модуляцію інформації, у яких здійснювати за допомогою хаотичних послідовностей.

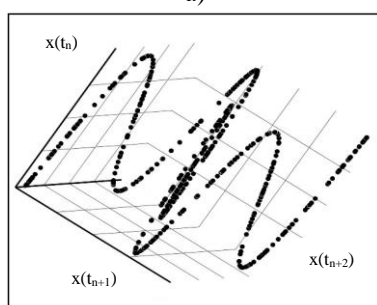
Під час формування хаотичних піднесучих для сигналів з OFDM-модуляцією будемо використовувати одномірне хаотичне відображення поліному Чебишева першого роду 3-го порядку (рис. 1):

$$x_{n+1} = 4x_n^3 - 3x_n, \quad (1)$$

де $n=0 \dots N-1$ – кількість відліків у послідовності;
 x_0 – початкове значення послідовності.



а)



б)

Рис. 1. Реалізація одномірного хаотичного відображення поліному Чебишева 1-го роду 3-го порядку (а) та “образ” в псевдофазовому просторі (б)

Використання хаотичних сигналів, сформованих відображеннями поліномів Чебишева, обумовлено тим, що всі характеристики таких відображень є ідентичними незалежно від порядку поліному, а

енергетичні спектри рівномірні, як у “білого” шуму. Це вказує на здатність сформованих таким чином сигналів забезпечити необхідний рівень структурної та IID-скритності СП.

Для “руйнування” структурованості “образу” (1) у псевдофазовому просторі, так як і в роботі [9], будемо використовувати концепцію аналітичного сигналу. З цією метою для виразу (1), на множині дискретних значень можливо отримати аналітичний сигнал у комплексній формі, відповідно до виразу:

$$\dot{x}_n = x_n + jy_n, \quad (2)$$

де $y_n = \{y_0, y_1, \dots, y_{N-1}\}$: уявна частина аналітичного сигналу задана перетворенням Гільберта вхідної послідовності $x_n = \{x_0, x_1, \dots, x_{N-1}\}$:

$$y(n) = \sum_{k=0}^{N-1} \frac{x(n)}{\pi(n-k)}. \quad (3)$$

Застосування перетворення Гільберта забезпечує однозначне визначення обвідної A_n і повної фази ψ_n сигналу, значення яких обчислюються відповідно до виразів:

$$A_n = |\dot{A}_n| = \sqrt{x_n^2 + y_n^2}, \quad (4)$$

та

$$\psi_n = |\dot{A}_n| = \arctan\left(\frac{x_n}{y_n}\right). \quad (5)$$

Після перенесення комплексної амплітуди на гармонічну частоту модуляції ω одержимо аналітичну хаотичну послідовність (АХП) у вигляді:

$$s_n = \text{Re}(A_n e^{j\omega n}) = A_n \cos(\psi_n + \omega n). \quad (6)$$

На рис. 2 показаний “образ” у псевдофазовому просторі АХП із параметрами $x_0=0,86$, $N=500$, $\omega=4,25$.

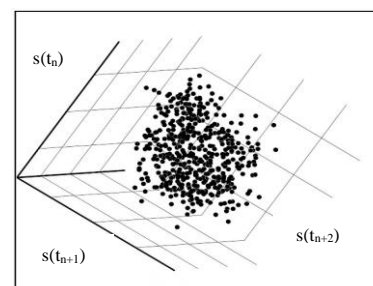


Рис. 2. “Образ” в псевдофазовому просторі сформованої аналітичної хаотичної послідовності

З аналізу рис. 1, 2 видно, що запропонований метод перетворення хаотичного процесу значно ускладнює структуру “образу” в псевдофазовому просторі, а також зменшує взаємну кореляцію між значеннями процесу, тобто робить його візуально близьким до “образу” “білого” шуму (рис. 3). Це надає можливість говорити про ймовірне підвищення скритності сформованих АХП.

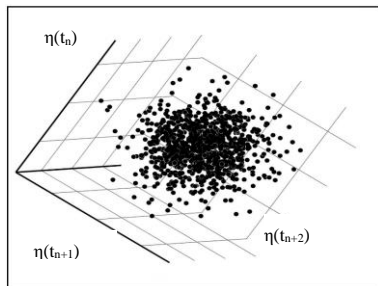


Рис. 3. “Образ” в псевдофазовому просторі “білого” шуму

Для підтвердження цього необхідно розрахувати значення BDS-статистики w^{BDS} , яка вважається чисельною мірою IID-скритності сигналу. В ній за допомогою статистичної величини w^{BDS} перевіряється нульова гіпотеза про незалежність та однаковий розподіл значень часового ряду за наступним виразом [9, 27, 28]:

$$w_{m,N}(\epsilon) = \sqrt{N-m+1} \frac{C_{m,N}(\epsilon) - C_{1,N-m}(\epsilon)^m}{\sigma_{m,N}(\epsilon)}, \quad (7)$$

де m – розмірність псевдофазового простору;

N – кількість елементів часового ряду (сигналу);

ϵ – радіус гіперсфери, якою покривається фазовий простір;

$C_{m,N}$ – кореляційний інтеграл;

$\sigma_{m,N}(\epsilon)$ – середньоквадратичне відхилення чисельника $C_{m,N}(\epsilon) - C_{1,N-m}(\epsilon)^m$.

Для незалежних однаково розподілених випадкових величин (“білого” шуму) значення BDS-ста-

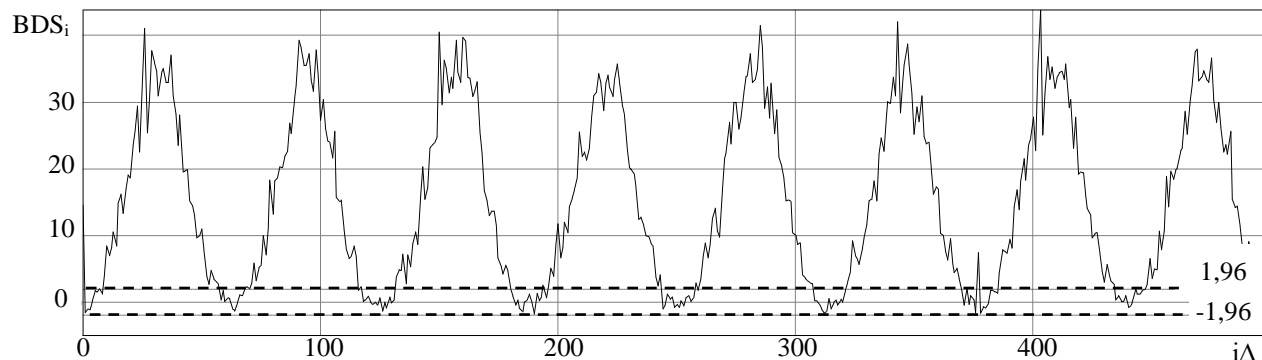


Рис. 4. Залежність значень BDS-статистики аналітичної хаотичної послідовності від частоти

тики перебувають в інтервалі $(-1,96; 1,96)$, який відповідає рівню значимості $\alpha=0,05$ і дозволяє прийняти для них гіпотезу H_0 про незалежність і тотожний розподіл часового ряду $s=(s_1, s_2, \dots, s_N)$.

На рис. 4 показана залежність значень BDS-статистики АХП від частоти, яка демонструє квазі-періодичну поведінку на множині частот $\{\omega_i = i\Delta_\omega\}_{i=1}^{500}$, які під час моделювання змінювались із кроком $\Delta_\omega=0,05$.

Аналіз отриманої залежності (рис. 4) показує, що не всі частоти попадають в інтервал IID-скритності. Тобто значення BDS-статистики залежно від частоти буде різним. Враховуючи це, під час організації скритної передачі інформації елементи “1” інформаційної послідовності $(\Pi) \left\{ \tau_q \right\}_{q=1}^Q$ ($r \in 0,1$) необхідно передавати з частотою модуляції ω_1 , а елементи “0” з ω_2 . Тоді Π , сформована маніпуляцією частоти, може бути записана:

$$s_n = \begin{cases} A_n \cos(\psi_n + \omega_1 n), & n = 0, \\ A_n \cos(\psi_n + \omega_2 n), & n = 1. \end{cases} \quad (8)$$

З метою забезпечення скритності Π близької до інтервалу IID, проаналізуємо різні пари частот модуляції ω_1 та ω_2 в АХП, які можуть використовуватися для маніпуляції елементами Π . У табл. 1 наведено результати розрахунків значень BDS – статистики для послідовності із 16 біт з параметрами $\chi_0=0,86$, $N=500$ та різними значеннями ω в АХП.

Таблиця 1
Значень BDS-статистики для різних пар частот в Π

Характеристики	Пари частот					
	1		2		3	
ω	0,1	0,3	1,2	1,45	1,85	2,9
$w_{m,N}$ на ω	-1,106	1,74	22,436	36,511	34,842	-0,217
$w_{m,N}$ для Π	3,107		105,626		14,342	

Аналізуючи табл. 1, можна зробити висновок, що для скритної передачі інформації елементи ПП треба передавати АХП на частотах, які попадають в інтервал ПД-скритності. Оскільки у такому випадку значення BDS-статистики ПП будуть знаходитися ближче до інтервалу ПД. Зауважимо, що сформована АХП є дискретною, тому для подальшої передачі такої послідовності по радіоканалу треба здійснити її перетворення в аналоговий сигнал у заданій смузі частот у діапазоні від 0 до деякої верхньої граничної частоти $f_b=F$. Для цього можна використати метод інтерполяції Шеннона – Котельникова [29]. Припустимо, що вираз (8) представляє собою вузькосмуговий процес з обмеженим спектром ($f_b=F$). Він повністю визначається послідовністю своїх миттєвих значень $\{s_n=s(nT_0), n=0, \pm 1, \pm 2, \dots, \pm N-1\}$, відстань між якими дорівнює інтервалу $T_0 \leq 1/2F$. При цьому вираз (8) можна записати:

$$s(t) = \sum_{n=0}^{N-1} s_n \gamma_n(t), \quad (9)$$

$$\text{де } \gamma_n(t) = \frac{\sin(2\pi F(t - nT_0))}{2\pi F(t - nT_0)}.$$

Вираз (9) узагальнюється на часову дискретизацію вузькосмугових сигналів:

$$s(t) = \sum_{n=0}^{N-1} s_n \gamma_n(t) \cos(2\pi f_1(t - nT_0)). \quad (10)$$

Для формування сигналу з OFDM-модуляцією необхідно кожен з піднесучих генерувати відповідно до виразу (8), тоді результуючий сигнал, який буде передаватися у радіоканалі, можна записати в такому вигляді:

$$s(t) = \sum_a \left(\sum_n s_{a,n} \gamma_n \cos(2\pi f_a(t - nT_0)) \right), \quad (11)$$

де $f_a=a \cdot F$, $f_1=2F$, $a=1 \dots A$ – номери переданих хаотичних піднесучих.

Необхідно відмітити, що для правильного відновлення сформованого хаотичного сигналу з OFDM-модуляцією на приймальній стороні відстань між піднесучими не повинна бути менше ніж $2F$. Оскільки, під час зменшення відстані та збільшення кількості піднесучих, у результуючому сигналі, з'являється велика кількість помилок під час відновлення ПП.

2. Оцінювання рівня ПД-скритності

З метою оцінювання рівня ПД-скритності сформованих сигналів у програмному середовищі Mathcad було сформовано інформаційні послідовності (піднесучі) по 16 біт у кожній з параметрами $\omega_1=0,07$, $\omega_2=0,55$, $x_0=0,86$ та кількістю відліків $N=512$. При цьому в сигналах сформованих відповідно до (13) було 8 та 32 піднесучих. Енергетичні спектри 4 піднесучих гармонічного сигналу з OFDM-модуляцією, сформованого хаотичного сигналу з OFDM-модуляцією та, для порівняння, спектр “білого” шуму показані на рис. 5.

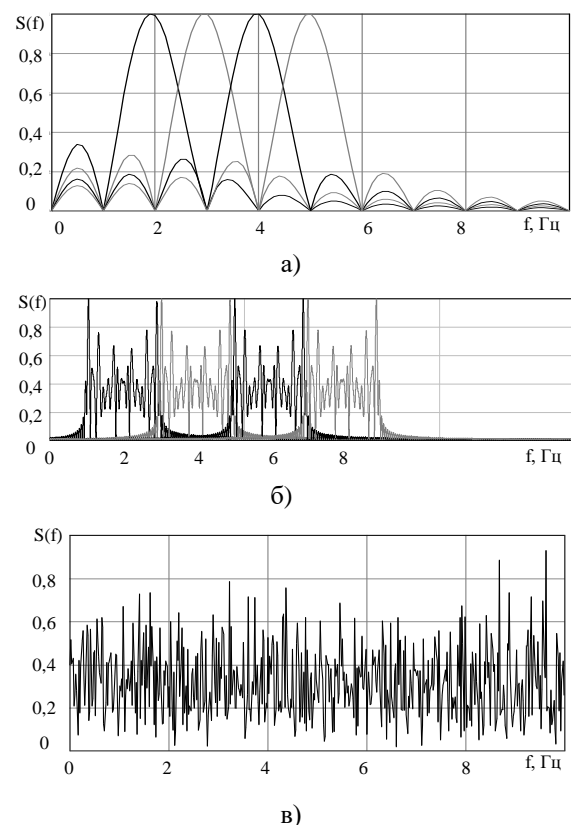


Рис. 5. Енергетичні спектри для 4 піднесучих: гармонічного сигналу з OFDM-модуляцією (а), хаотичного сигналу з OFDM-модуляцією (б), спектр “білого” шуму (в)

З аналізу рис. 5 можна зробити висновок, що енергетичні спектри піднесучих, сформованих за допомогою хаотичних сигналів з OFDM-модуляцією, є візуально схожими із спектром “білого” шуму. Реалізація та енергетичний спектр на виході передавача сумарного хаотичного OFDM-сигналу та гармонічного OFDM-сигналу показані на рис. 6.

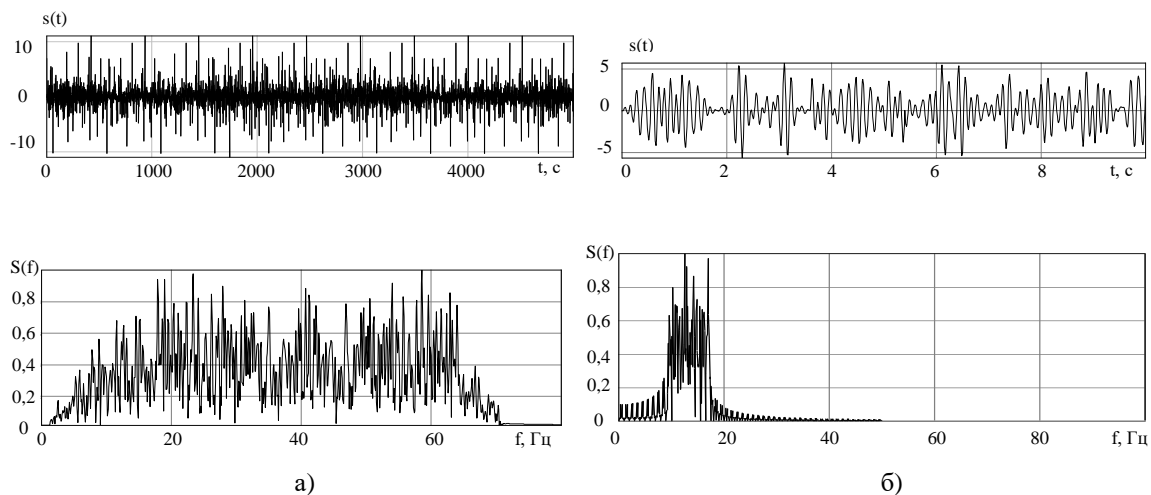


Рис. 6. Реалізація та енергетичний спектр на 8 піднесучих: хаотичного сигналу з OFDM-модуляцією (а), гармонічного сигналу з OFDM-модуляцією (б)

З рис. 6 видно, що запропонований метод формування хаотичних сигналів з OFDM-модуляцією, значно підвищує IID-скритність СПІ, за рахунок схожості сформованих сигналів із випадковим процесом. Це підтверджується виглядом “образів” в псевдофазовому просторі для різної кількості піднесучих у хаотичному сигналі з OFDM-модуляцією (рис. 7), оскільки в них зменшена ступінь залежності в значеннях процесу, відсутні регулярність та структурованість фазових траєкторій.

Однак візуальний аналіз “образів” сигналів в псевдофазовому просторі не являється достатнім для об’єктивної оцінки скритності сигналів. Для чисельної оцінки IID-скритності сигналу розрахуємо значення BDS статистики $w_{m,N}(n)$ для виразу (11) від кількості піднесучих n у сигналі з OFDM-моду-

ляцією та порівняємо отримані значення з гармонічними сигналами з OFDM-модуляцією. Результати розрахунків наведені в табл. 2.

Таблиця 2

Значення BDS-статистики залежно від кількості піднесучих у хаотичних та гармонічних сигналах з OFDM-модуляцією

n	$w_{m,N}(n)$	хаотичні OFDM	гармонічні OFDM
4		11,448	54,439
8		5,724	85,174
16		0,925	123,767
32		-4,789	188,962
64		-9,539	278,552

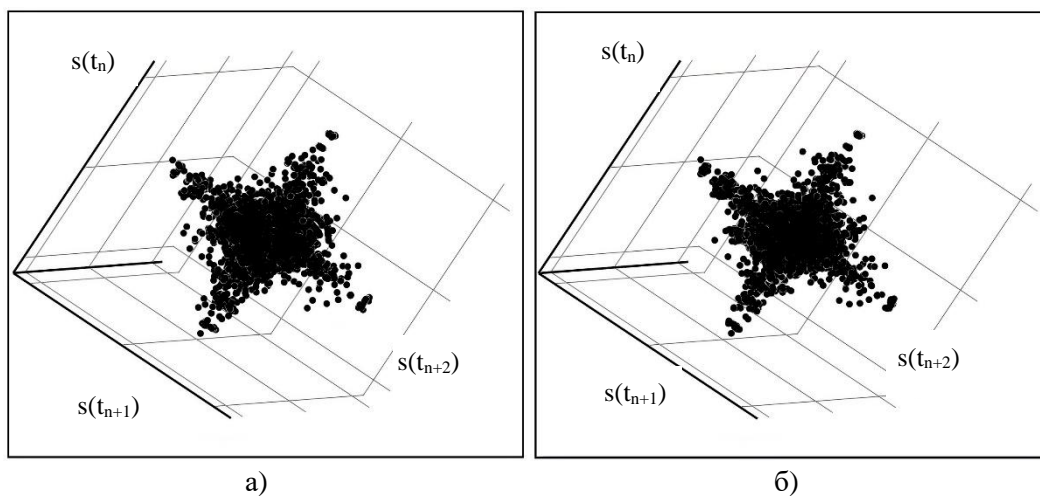


Рис. 7. “Образи” в псевдофазовому просторі хаотичного сигналу з OFDM-модуляцією на: (а) – 8 піднесучих, (б) – 32 піднесучих

З табл. 2 видно, що хаотичні сигнали з OFDM-модуляцією забезпечують вищий рівень IID-скритності, в порівнянні з гармонічними сигналами з OFDM-модуляцією. При кількості піднесучих у хаотичному сигналі з OFDM-модуляцією $n=16$, BDS-статистика приймає значення з інтервалу $|w_{m,N}(\epsilon)| \leq 1,96$. Це дає змогу з ймовірністю 95 % прийняти гіпотезу H_0 (IID) і стверджувати, що сигнал не відрізняється від “білого” шуму. Однак під час зменшення або збільшення кількості піднесучих у реалізації рівень IID-скритності сформованих сигналів падає. Але незважаючи на це, можна стверджувати, що вони забезпечують вищий рівень IID-скритності.

3. Оцінювання рівня структурної скритності

Під час ведення радіоелектронної розвідки протидіюча сторона прагне виявити робочі параметри системи радіозв'язку, яка у свою чергу, повинна затрудняти розвідку, управляючи розподілом ймовірностей своїх станів. При цьому, необхідно встановити розподіл ймовірностей робочих параметрів системи зв'язку так, щоби навіть при оптимальних діях противника його часові та апаратні затрати на пошук були б максимальними. Для вирішення цієї задачі можна використати поняття структурної скритності. При вибраних параметрах системи зв'язку визначається структурна скритність і відповідний алгоритм пошуку, далі, змінюючи параметри, визначаються умови, за яких структурна скритність максимальна [8, 14].

Структурна скритність залежить від ансамблю (арсеналу) A реалізації сигналу і визначається числом двійкових вимірювань (двим), які необхідно здійснити для розкриття структури ШСС. Загальний вираз для оцінювання структурної скритності ШСС має вигляд:

$$S = \log_2 A = \log_2 B, \quad (12)$$

де A – арсенал реалізації параметрів сигналу;

B – база сигналу, яка визначається за відносною смугою частот $\frac{\Delta f}{f_0}$, де $\Delta f = f_v - f_n$ – смуга частот;

f_v , f_n – верхня та нижня частоти спектру, $f_0 = \frac{f_v + f_n}{2}$ – центральна частота спектру [16].

З огляду на вище сказане, необхідно здійснити розрахунки структурної скритності сигналів сформованих відповідно до виразу (11) та порівняти їх із гармонічними сигналами з OFDM-модуляцією в залежності від кількості піднесучих у сигналі.

Отримані результати дадуть змогу показати рівень структурної скритності сигналів та вибрати стан сигналу з максимальним рівнем структурної скритності.

Для гармонічних сигналів з OFDM-модуляцією структурна скритність буде визначатися [14]:

$$S_{\text{OFDM}} = \log_2 B + \log_2 N + \log_2 M + \log_2 K, \quad (13)$$

де B – база сигналу;

N – кількість піднесучих у сигналі;

M – кількість станів (точок сигнального сузір'я) модуляції;

K – кількість біт інформації в кожній піднесучій.

Сформовані хаотичні сигнали з OFDM-модуляцією будемо оцінювати за виразом:

$$S_{X\text{-OFDM}} = \left(\begin{array}{l} \log_2 B + \log_2 N + \log_2 K + \\ + \log_2 X + \log_2 T + \log_2 W \end{array} \right), \quad (14)$$

де B – база сигналу;

N – кількість піднесучих у сигналі;

K – кількість біт інформації в кожній піднесучій;

X – кількість можливих значень початкового параметру (точність представлення після коми);

T – кількість можливих відображень поліномів Чебишева першого роду;

W – кількість можливих значень частоти ω в аналітичному сигналі (11).

Під час проведення розрахунків для оцінювання рівня структурної скритності використовувалися наступні обмеження (табл. 3).

Таблиця 3

Параметри сигналів, які використовувалися для оцінювання структурної скритності

Тип сигналу	Параметри сигналів				
	M	K	X	T	W
гармонічні OFDM	2	16	–	–	–
хаотичні OFDM	–	16	84	20	500

У табл. 4 наведені результати розрахунків структурної скритності гармонічних та сформованих хаотичних сигналів з OFDM-модуляцією, в залежності від кількості піднесучих у сигналі.

Таблиця 4

Значення структурної скритності для хаотичних та гармонічних сигналів з OFDM-модуляцією

n	S	хаотичні OFDM (двим)	гармонічні OFDM (двим)
	8		30
16		32	14
32		34	15
64		36	17

Отримані результати (табл. 4) вказують на високий рівень структурної скритності сформованих хаотичних сигналів з OFDM-модуляцією, в порівнянні з гармонічними. При цьому, для збільшення рівня структурної скритності сформованих сигналів необхідно розширювати ансамбль реалізації, наприклад, за рахунок використання різних частот в АХП для кожної піднесучої.

4. Оцінювання якості відновлення сигналів

Оцінювання якості відновлення сигналів, сформованих за допомогою розробленого методу скритої передачі інформації, було проведено методом статистичного моделювання. Для проведення статистичного моделювання використовувалась імітаційна модель, структурна схема якої наведена на рис. 8.

Інформаційна послідовність (ІП), яку необхідно передати, поступає в модулятор АХП, у якому кожен біт інформації модулюється АХП із різною частотою ($S_{\omega_1}, S_{\omega_2}$). На виході модулятора отримуємо хаотичну інформаційну послідовність (s_n), яка далі

поступає на послідовно-паралельний блок (S/P), де розділяється на паралельні потоки даних. Паралельні потоки поступають на блок оберненого швидкого перетворення Фур'є (ОШПФ), на виході якого формуються піднесучі. Зі сформованих піднесучих у паралельно-послідовному блоці (P/S) утворюється послідовний потік даних. Після чого послідовний сформований інформаційний потік поступає в цифро-аналоговий перетворювач (ЦАП), на антенно-фідерний пристрій (А) і далі розповсюджується в канал зв'язку.

На приймальній стороні спостерігається адитивна суміш $Y = \{y_t\}_{t=0}^{M-1}$ ($y_t = s_t + \eta_t$) інформаційної послідовності (рис.6а), яка задана елементами множини $S = \{s_t\}_{t=0}^{M-1}$ і "білого" Гаусівського шуму $N = \{\eta_t\}_{t=0}^{M-1}$ з нульовим математичним очікуванням та дисперсією σ_n^2 . Після проходження отриманої реалізації через аналого-цифровий перетворювач (АЦП), блок S/P, блок швидкого перетворення Фур'є (ШПФ) та блок P/S сигнал поступає в демодулятор АХП.

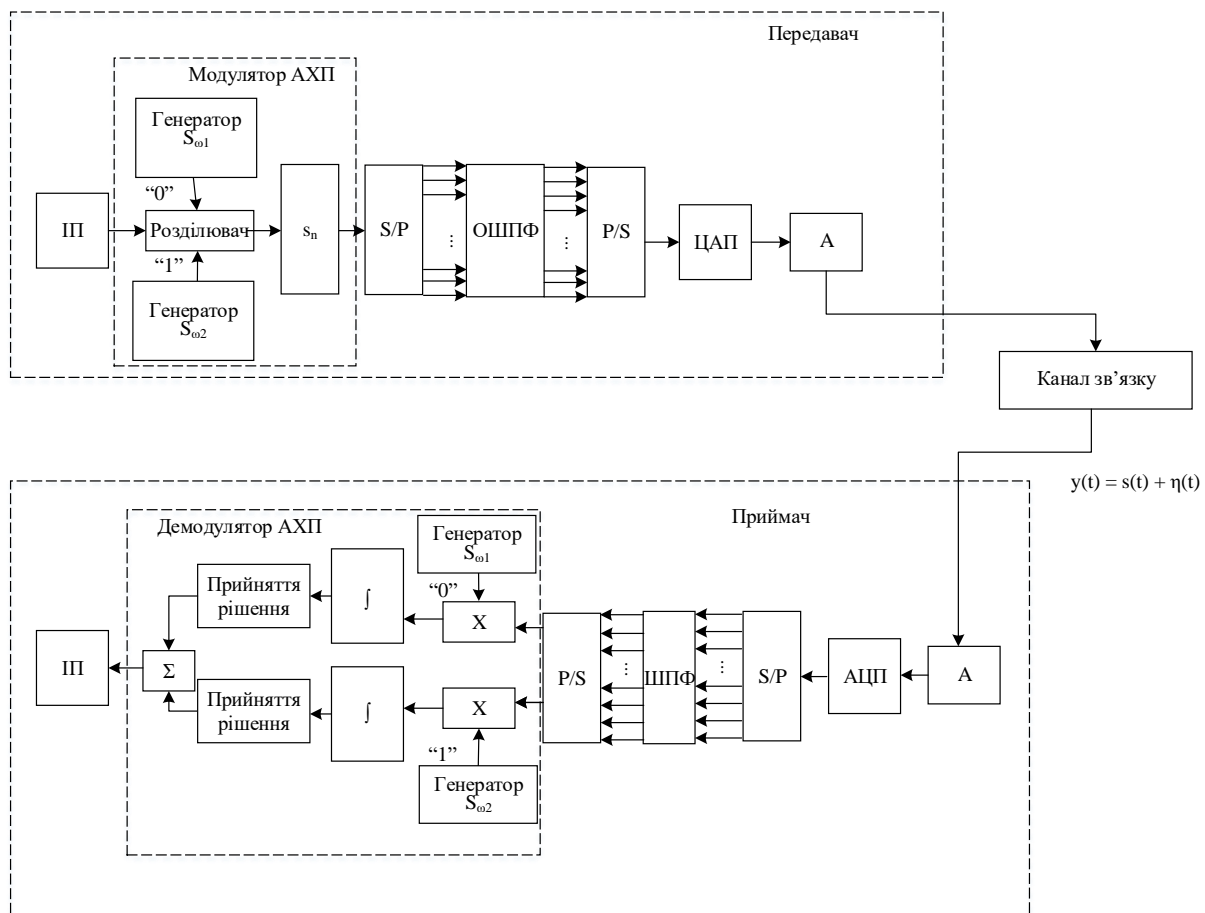


Рис. 8. Структура схема системи передачі інформації заснована на використанні сигналів з OFDM-модуляцією та аналітичними хаотичними послідовностями

У демодуляторі АХП необхідно за спостереженням $\{y_t\}_{t=0}^{M-1}$ відновити повідомлення $\{r_q\}_{q=1}^{L_n}$ (L_n – загальна кількість елементів бінарного повідомлення).

Знаючи на приймальній стороні інформацію про вид хаотичного відображення, його початкове значення $x_0 = 0,86$, кількість відліків у кожному біті інформації $N = 512$ і частоти $\omega_1=0,07$ та $\omega_2=0,55$, які використовуються для передачі $r_q=0$ та $r_q=1$ відповідно, можна реалізувати когерентну обробку прийнятого сигналу за рахунок формування опорних реалізацій очікуваних сигналів $S_{\omega_1}(t)$ та $S_{\omega_2}(t)$ [30, 31].

На рис. 9 показані результати розрахунків ймовірності правильного оцінювання $P_r(n, L, q) = 1 - P_{\text{err}, \hat{r}}(n, L, q)$ повідомлення \hat{r} від кількості піднесучих n в сигналі, кількості елементів бінарного повідомлення L в кожній піднесучій та відношення сигнал/шум на вході приймача $q = 10 \lg(\sigma_s^2 / \sigma_n^2)$. Величина $P_{\text{err}, \hat{r}} = d_H(\hat{r}, \tilde{r}) / L_n$ визначає долю помилок в оцінюванні елементів повідомлення й рівна відношенню відстані Хеммінга $d_H(\hat{r}, \tilde{r})$ між передавальною бінарною послідовністю \tilde{r} та її оцінюванням \hat{r} до загальної кількості L_n її елементів. При моделюванні кількість символів у кожній піднесучій була фіксованою $L=10$, а кількість піднесучих вибиралася рівною $n = 16$ та $n = 32$.

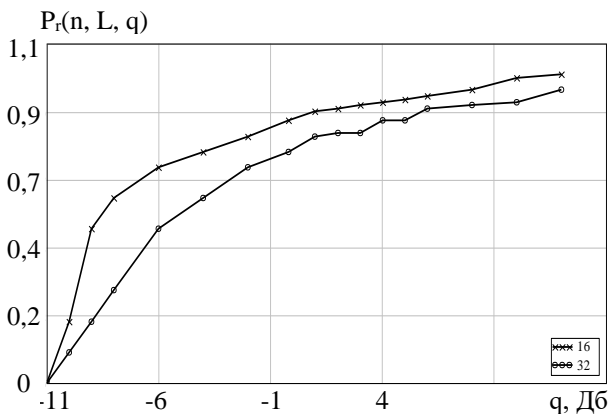


Рис. 9. Залежність ймовірності правильного оцінювання повідомлення від кількості піднесучих хаотичного сигналу з OFDM-модуляцією n й відношення сигнал/шум на вході приймача

З рис. 9 видно, що зі збільшенням кількості піднесучих у хаотичному сигналі з OFDM-модуляцією, зростає кількість помилок при відновленні повідомлення. Тому, з метою ефективного використання запропонованого методу для забезпечення

заданого рівня відновлення $P_r > 0,9$, відношення сигнал/шум на вході приймача має бути $q > 4$.

Висновки

Вперше синтезовано метод підвищення скритності систем передачі інформації з використанням сигналів з OFDM-модуляцією та хаотичних піднесучих. Його відмінність від відомих полягає в тому, що формування піднесучих відбувається з використанням аналітичних хаотичних послідовностей, утворених за допомогою поліному Чебишева першого роду третього порядку. Це надає змогу забезпечити одночасно необхідний рівень структурної та IID-скритності систем передачі інформації. При цьому, на відміну від відомих методів формування хаотичних сигналів [9, 19-24], запропонований – надає змогу передавати інформацію у каналах радіозв'язку.

Забезпечення необхідного рівня IID-скритності підтверджується чисельними розрахунками значень BDS-статистики. Однак під час формування хаотичних сигналів з OFDM-модуляцією, необхідно враховувати кількість піднесучих у реалізації, оскільки їх зміна не завжди дає можливість прийняти гіпотезу про близькість отриманого сигналу до “білого” шуму. Найоптимальніше використовувати сигнали на 16 піднесучих, адже в такому випадку значення BDS-статистики перебувають в інтервал IID-скритності.

Високий рівень структурної скритності підтверджується тим, що для виявлення структури хаотичних сигналів з OFDM-модуляцією, необхідно зробити у 2...2,5 рази більше двійкових операцій, ніж для гармонічних сигналів з OFDM-модуляцією. При цьому, для збільшення рівня структурної скритності сформованих сигналів необхідно розширювати ансамбль реалізації, наприклад, за рахунок використання різних частот в АХП та поліномів Чебишева 1 роду різних порядків для кожної піднесучої.

Оцінювання ефективності відновлення хаотичних сигналів з OFDM-модуляцією показала, що для забезпечення необхідного рівня відтворення повідомлення на приймальній стороні, відношення сигнал/шум на вході приймача має бути $q > 4$.

Наша подальша робота буде полягати в розробці експериментальної СПІ з використанням хаотичних сигналів з OFDM-модуляцією та дослідженні її характеристик під час роботи в реальних умовах задовою обстановки. Також вони будуть полягати в оптимізації алгоритмів відновлення хаотичних сигналів з OFDM-модуляцією з метою підвищення ймовірності правильного відновлення повідомлень.

Подяка. Авторський колектив висловлює подяку доктору технічних наук, професору Костенку Павлу Юрійовичу за допомогу, надану під час проведення даного дослідження.

Література

1. Єрохін, В. Ф. Застосування технології OFDM у широкосмугових бездротових мережах [Текст] / В. Ф. Єрохін, Б. А. Гиндич // Збірник наукових праць ВІТІ НТУУ “КПІ”. – 2012. – № 2. – С. 29-36.

2. Liu, H. OFDM – Based Broadband Wireless Networks: Design and Optimization [Text] / H. Liu, G. Li. – New York : John Wiley, 2005. – 264 p.

3. Vasylyshyn, V. Channel Estimation Method for OFDM Communication System using Adaptive Singular Spectrum Analysis [Text] / V. Vasylyshyn // Proc. IEEE 40th International Conference on Electronics and Nanotechnology (ELNANO). – Kyiv, 2020. – P. 884-887. DOI: 10.1109/ELNANO50318.2020.9088787.

4. Krishna, E. H. New channel estimation method using singular spectrum analysis for OFDM systems [Text] / E. H. Krishna, K. Sivani, K. A. Reddy // Wireless Personal Communications. – 2018. – Vol. 101. – P. 2193-2207. DOI: 10.1007/s11277-018-5811-5.

5. Shaik, M. Comparative Study of FBMC-OQAM and OFDM Communication System [Text] / M. Shaik, R. S. Yarrabothu // 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). – Tirunelveli, India, 2018. – P. 559-563. DOI: 10.1109/ICOEI.2018.8553689.

6. Liu, F. Incremental-data stealth-transmission method in DSSS [Text] / F. Liu, J. Liu, Y. Feng // Wireless Network. – 2021. – No. 27. – P. 2441-2449. DOI: 10.1007/S11276-021-02590-6.

7. Shao, Z. Your Noise, My Signal: Exploiting Switching Noise for Stealthy Data Exfiltration from, M Desktop Computers [Text] / Z. Shao, M. A. Islam, S. Ren // Proceedings of the ACM on Measurement and Analysis of Computing Systems. – 2020. – Vol. 4, Iss. 1. – Article No. 07. – P. 1-39. DOI: 10.1145/3379473.

8. Основы теории скрытности [Текст] : учеб. пособие / под общ. ред. З. М. Каневского. – Воронеж : Воронежский государственный технический университет, 2006. – 202 с.

9. Kostenko, P. Yu. Stealthiness of analytical chaotic signals [Text] / P. Yu. Kostenko, V. V. Slobodyanuk, A. N. Barsukov // Radioelectronics and Communications Systems. – 2017. – No. 60. – P. 132-140. DOI: 10.3103/S0735272717030050.

10. Кувшинов, О. В. Оцінка структурної секретності широкосмугових сигналів [Текст] / О. В. Кувшинов, Р. М. Вознюк // Збірник наукових праць ВІТІ НТУУ “КПІ”. – 2011. – № 1. – С. 106-111.

11. Метод прихованої передачі інформації в системах з Orthogonal frequency division multiplexing (OFDM) модуляцією [Текст] / К. С. Васюта, У. Р. Збежховська, В. В. Слободянюк, В. С. Загривий,

В. І. Чистов // Наука і техніка Повітряних Сил Збройних Сил України. – 2021. – № 2(43). – С. 132-139. DOI: 10.30748/nitps.2021.43.18.

12. Dharavathu, Krishna. Secure image transmission through crypto-OFDM system using Rubik's cube algorithm over an AWGN channel [Text] / Krishna Dharavathu, Anuradha Mosa // International Journal of Communication Systems. – 2020. – Vol. 33. Iss. 8. DOI: 10.1002/dac.4369.

13. Stealth Evaluation of the OFDM Communication System [Text] / K. Vasiuta, U. Zbezhkowska, V. Slobodyanuk, O. Kovalchuk // Proc. 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T). – 2020. – P. 363-367. DOI: 10.1109/PICST51311.2020.9468046.

14. Анализ структурной скрытности много-частотных сигналов широкополосных систем связи [Текст] / А. И. Цона, Д. Г. Ганишин, А. А. Дудка, А. Н. Битченко // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2016. – № 184. – С. 127-134.

15. Жук, А. П. Повышение структурной секретности системы передачи информации с кодовым разделением каналов [Текст] / А. П. Жук, А. С. Иванов // Научные технологии в космических исследованиях Земли. – 2011. – № 3. – С. 26-28.

16. Петрович, Н. Т. Системы связи с шумоподобными сигналами [Текст] / Н. Т. Петрович, М. К. Размахнин. – М. : Советское радио, 1969. – 231 с.

17. Радзиевский, В. Г. Обработка сверхширокополосных сигналов и помех [Текст] / В. Г. Радзиевский, П. А. Трифонов. – М. : “Радиотехника”, 2009. – 288 с.

18. Скрытность передачи в системах связи с хаотическими сигналами [Текст] / Н. В. Захарченко, С. М. Горохов, В. В. Корчинський, Б. К. Радзимовський // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2013. – № 3. – С. 161-164.

19. Kostenko, P. Yu. Improving communication security by complicating chaotic process attractor using linear transform with mandelbrot kernel [Text] / P. Yu. Kostenko, K. S. Vasiuta, S. N. Symonenko // Radioelectronics and Communications Systems. – 2010. – No. 53. – P. 636-643. DOI: 10.3103/S0735272710120022.

20. Litvinenko, Anna. Chaos based linear precoding for OFDM [Text] / Anna Litvinenko, Arturs Aboltins // 2015 Advances in Wireless and Optical Communications (RTUWO). – Riga, Latvia, 2015. – P. 13-15. DOI: 10.1109/RTUWO.2015.7365709.

21. Насыров, И. К. Моделирование информационного канала с использованием хаотических сигналов нелинейных динамических систем [Текст] / И. К. Насыров, В. В. Андреев // Известия высших учебных заведений. Проблемы энергетики. – 2020. – Т. 22, № 4. – С. 79-87. DOI: 10.30724/1998-9903-2020-22-4-79-87.

22. Wang, Z. A Chaos-Based Encryption Scheme for DCT Precoded OFDM-Based Visible Light Communication Systems [Text] / Z. Wang, S. Chen // *Journal of Electrical and Computer Engineering*. – 2016. – Vol. 2016. – Article ID: 2326563. – P. 1-7. DOI: 10.1155/2016/2326563.
23. Chaotic Interleaving for Secured OFDM [Text] / N. R. Raajan, B. Monisha, R. Vishnupriya, Niranjana Rangarajan, G. N. Jayabhavani, C. Nishanthini // *Research Journal of Information Technology*. – 2013. – Vol. 5, Iss. 3. – P. 449-455. DOI: 10.3923/rjit.2013.449.455.
24. On secure OFDM system: Chaos based constellation scrambling [Text] / M. A. Khan, M. Asim, V. Jeoti, R. S. Manzoor // *2007 International Conference on Intelligent and Advanced Systems*. – 2007. – P. 484-488, DOI: 10.1109/ICIAS.2007.4658435.
25. Olewi, H. I. Hybrid Chaotic Scheme for Secure OFDM-PON Transmission [Text] / H. I. Olewi, R. S. Fyath // *2020 International Conference on Computer Science and Software Engineering (CSASE)*. – Duhok, Iraq, 2020. – P. 232-237. DOI: 10.1109/CSASE48920.2020.9142120.
26. Real-time secure optical OFDM transmission with chaotic data encryption [Text] / Zong Jianyou, Hajomer Adnan, Zhang Liuming, Hu Weisheng, Yang Xuelin // *Optics Communications*. – 2020. – Vol. 473. – Article Id: 126005. DOI: 10.1016/j.optcom.2020.126005.
27. A Generalized BDS Statistic [Text] / K. Matilla-García, M. Queralt, R. Sanz, F. J. Vázquez // *Computational Economics*. – 2004. – No. 24. – P. 277-300. DOI: 10.1007/S10614-004-4657-Y.
28. A test for independence based on correlation dimension [Text] / W. A. Brock, J. A. Scheinkman, W. D. Dechert, B. LeBaron // *Econometric Reviews*. – 1996. – Vol. 15, Iss. 3. – P. 197-235. DOI: 10.1080/07474939608800353.
29. Аналіз IID-скритності безперервних хаотичних сигналів [Текст] / П. Ю. Костенко, В. В. Слободянюк, С. В. Волинець, М. Л. Крючка // *Системи обробки інформації*. – 2018. – № 1(152). – С. 20-26. DOI: 10.30748/soi.2018.152.03.
30. Фалькович, С. Е. Основы статистической теории радиотехнических систем [Текст] / С. Е. Фалькович, П. Ю. Костенко. – X. : НАУ ХАИ, 2006. – 390 с.
31. Метод обробки відеоданих з можливістю їх захисту після квантування [Текст] / Д. С. Гаврилов, С. С. Бучік, Ю. М. Бабенко, С. С. Шульгін, О. В. Слободянюк // *Радіоелектронні та комп'ютерні системи*. – 2021. – № 2(98). – С. 64-77. DOI: 10.32620/reks.2021.2.06.
- technology in broadband wireless networks]. *Zbirnyk naukovykh prats' VITI NTUU "KPI"*, 2012, no. 2, pp. 29-36.
2. Liu, H., Li, G. *OFDM – Based Broadband Wireless Networks: Design and Optimization*. New York, John Wiley Publ., 2005. 264 p.
3. Vasylyshyn, V. Channel Estimation Method for OFDM Communication System using Adaptive Singular Spectrum Analysis. *Proc. IEEE 40th International Conference on Electronics and Nanotechnology (ELNANO)*. Kyiv, 2020, pp. 884-887. DOI: 10.1109/ELNANO50318.2020.9088787.
4. Krishna, E. H., Sivani, K., Reddy, K. New channel estimation method using singular spectrum analysis for OFDM systems. *Wireless Personal Communications*, 2018, vol. 101, pp. 2193-2207. DOI: 10.1007/s11277-018-5811-5.
5. Shaik, M., Yarrabothu, R. S. Comparative Study of FBMC-OQAM and OFDM Communication System. *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*. Tirunelveli, India, 2018, pp. 559-563. DOI: 10.1109/ICOEI.2018.8553689.
6. Liu, F., Liu, J., Feng, Y. Incremental-data stealth-transmission method in DSSS. *Wireless Network*, 2021, no. 27, pp. 2441-2449. DOI: 10.1007/S11276-021-02590-6.
7. Shao, Z., Islam, M. A., Ren, S. Your Noise, My Signal: Exploiting Switching Noise for Stealthy Data Exfiltration from, M Desktop Computers. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 2020, vol. 4, iss. 1, Article No. 07, pp. 1-39. DOI: 10.1145/3379473.
8. Kanevskiy Z. M. *Osnovy teorii skrytnosti [Fundamentals of stealth theory]*. Voronezh, Voronezhskiy gosudarstvennyy tekhnicheskii universitet Publ., 2006. 202 p.
9. Kostenko, P. Yu., Slobodyanuk, V. V., Barsukov, A. N. Stealthiness of analytical chaotic signals. *Radioelectronics and Communications Systems*, 2017, no. 60, pp. 132-140. DOI: 10.3103/S0735272717030050.
10. Kuvshynov, O. V., Voznyuk, R. M. Otsinka strukturnoyi skrytnosti shyrokosmuhovykh syhnaliv [Estimation of structural secrecy of broadband signals]. *Zbirnyk naukovykh prats' VITI NTUU "KPI"*, 2011, no. 1, pp. 106-111.
11. Vasyuta, K. S., Zbezhkhovs'ka, U. R., Slobodyanyuk, V. V., Zahryvyy, V. S., Chystov, V. I. Metod prykhovanoyi peredachi informatsiyi v systemakh z Orthogonal frequency division multiplexing (OFDM) modulyatsiyeyu [method of stealth information transmission in systems with orthogonal frequency division multiplexing (OFDM) modulation]. *Nauka i tekhnika Povitryanykh Syl Zbroynykh Syl Ukrayiny*, 2021, no. 2(43), pp. 132-139. DOI: 10.30748/nitps.2021.43.18.
12. Dharavathu, Krishna., Mosa, Anuradha. Secure image transmission through crypto-OFDM system using Rubik's cube algorithm over an AWGN channel.

References

1. Yerokhin, V. F., Hyndych, B. A. Zastosuvannya tekhnolohiyi OFDM u shyrokosmuhovykh bezdrotovykh merezhakh [Application of OFDM

International Journal of Communication Systems, 2020, vol. 33, iss. 8. DOI: 10.1002/dac.4369.

13. Vasiuta, K., Zbezhkowska, U., Slobodyanuk, V., Kovalchuk, O. Stealth Evaluation of the OFDM Communication System. *Proc. 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, 2020, pp. 363-367. DOI: 10.1109/PICST51311.2020.9468046.

14. Tsopa, A. I., Ganshin, D. G., Dudka, A. A., Bitchenko, A. N. Analiz strukturnoy skrytnosti mnogochastotnykh signalov shirokopolosnykh sistem svyazi [Analysis of the structural secrecy of multifrequency signals of broadband communication systems]. *Radiotekhnika. Vseukrainskiy mezhvedomstvennyy nauchno-tekhnicheskyy sbornik*, 2016, no. 184, pp. 127-134.

15. Zhuk, A. P., Ivanov, A. S. Povyshenie strukturnoy skrytnosti sistemy peredachi informatsii s kodovym razdeleniem kanalov [Increasing the structural secrecy of the code division multiplexing information transmission system]. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli*, 2011, no. 3, pp. 26-28.

16. Petrovich, N. T., Razmakhnin, M. K. *Sistemy svyazi s shumopodobnymi signalami* [Communication systems with noise-like signals]. Moscow, Sovetskoe radio Publ., 1969. 231 p.

17. Radzievskiy, V. G., Trifonov, P. A. *Obrabotka sverkhshirokopolosnykh signalov i pomekh* [Ultra-wideband signal and interference processing]. Moscow, "Radiotekhnika" Publ., 2009. 288 p.

18. Zakharchenko, N. V., Gorokhov, S. M., Korchins'kiy, V. V., Radzimovs'kiy, B. K. Skrytnost' peredachi v sistemakh svyazi s khaoticheskimi signalami [Secrecy of transmission in communication systems with chaotic signals]. *Vimiryuval'na ta obchislyuval'na tekhnika v tekhnologichnikh protsesakh*, 2013, no. 3, pp. 161-164.

19. Kostenko, P. Yu., Vasiuta, K. S., Symonenko, S. N. Improving communication security by complicating chaotic process attractor using linear transform with mandelbrot kernel. *Radioelectronics and Communications Systems*, 2010, no. 53, pp. 636-643. DOI: 10.3103/S0735272710120022.

20. Litvinenko, Anna., Aboltins, Arturs. Chaos based linear precoding for OFDM. *2015 Advances in Wireless and Optical Communications (RTUWO)*. Riga, Latvia, 2015, pp. 13-15. DOI: 10.1109/RTUWO.2015.7365709.

21. Nasyrov, I. K., Andreev, V. V. Modelirovanie informatsionnogo kanala s ispol'zovaniem khaoticheskikh signalov nelineynykh dinameskikh sistem [Modeling of information channel using pseudorandom signals of nonlinear dynamical systems]. *Power engineering: research, equipment, technology*, 2020, vol. 22, no. 4, pp. 79-87. DOI: 10.30724/1998-9903-2020-22-4-79-87.

22. Wang, Z., Chen, S. A Chaos-Based Encryption Scheme for DCT Precoded OFDM-Based Visible Light Communication Systems. *Journal of Electrical and Computer Engineering*, 2016, vol. 2016, Article ID: 2326563, pp. 1-7. DOI: 10.1155/2016/2326563.

23. Raajan, N. R., Monisha, B., Vishnupriya, R., Rangarajan, Niranjana., Jayabhavani, G. N., Nishanthini, C. Chaotic Interleaving for Secured OFDM. *Research Journal of Information Technology*, 2013, vol. 5, iss. 3, pp. 449-455. DOI: 10.3923/rjit.2013.449.455.

24. Khan, M. A., Asim, M., Jeoti, V., Manzoor, R. S. On secure OFDM system: Chaos based constellation scrambling. *2007 International Conference on Intelligent and Advanced Systems*, 2007, pp. 484-488, DOI: 10.1109/ICIAS.2007.4658435.

25. Olewi, H. I., Fyath, R. S. Hybrid Chaotic Scheme for Secure OFDM-PON Transmission. *2020 International Conference on Computer Science and Software Engineering (CSASE)*. Duhok, Iraq, 2020, pp. 232-237. DOI: 10.1109/CSASE48920.2020.9142120.

26. Jianyou, Zong., Adnan, Hajomer., Liuming, Zhang., Weisheng, Hu., Xuelin, Yang. Real-time secure optical OFDM transmission with chaotic data encryption. *Optics Communications*. 2020, vol. 473, Article Id: 126005. DOI: 10.1016/j.optcom.2020.126005.

27. Matilla-García, K., Queralt, M., Sanz, R., Vázquez F. J. A Generalized BDS Statistic. *Computational Economics*, 2004, no. 24, pp. 277-300. DOI: 10.1007/S10614-004-4657-Y.

28. Brock, W. A., Scheinkman, J. A., Dechert, W.D., LeBaron, B. A test for independence based on correlation dimension. *Econometric Reviews*, 1996, vol. 15, iss. 3, pp. 197-235. DOI: 10.1080/07474939608800353.

29. Kostenko, P. Yu., Slobodyanyuk, V. V., Volynets', S. V., Kryuchka, M. L. Analiz IID-skrytnosti bezperervnykh khaotychnykh syhnaliv [Analysis of IID-stealthiness of continuous chaotic signals]. *Sistemy obrobky informatsiyi – Information Processing Systems*, 2018, no. 1(152), pp. 20-26. DOI: 10.30748/soi.2018.152.03.

30. Fal'kovich, S. E., Kostenko, P. Yu. *Osnovy statisticheskoy teorii radiotekhnicheskikh sistem* [Fundamentals of the statistical theory of radio engineering systems]. Kharkiv, NAU KhAI Publ., 2006. 390 p.

31. Havrylov, D. S., Buchyk, S. S., Babenko, Yu. M., Shulgin, S. S., Slobodyanyuk, O. V. Metod obrobky videodanykh z mozhlyvystyu yikh zakhystu pislya kvantuvannya [Method of processing video data with the possibility of their protection after quantization]. *Radioelectronic and computer systems*, 2021, no. 2(98), pp. 64-77. DOI: 10.32620/reks.2021.2.06.

МЕТОД ПОВЫШЕНИЯ СКРЫТНОСТИ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ МОДУЛЯЦИИ С ОРТОГОНАЛЬНЫМ ЧАСТОТНЫМ РАЗДЕЛЕНИЕМ И МУЛЬТИПЛЕКСИРОВАНИЕМ ХАОТИЧЕСКИХ ПОДНЕСУЩИХ

*К. С. Васюта, У. Р. Збежховская, В. В. Слободянюк, И. В. Захарченко, О. Л. Каццишин,
М. С. Дубинский, Ю. М. Рябуха, О. В. Коваль*

Предметом исследования являются процессы формирования и обработки сигналов с ортогональным частотным разделением и мультиплексированием (OFDM – orthogonal frequency division multiplexing) хаотических последовательностей для обеспечения скрытности передачи данных. Целью исследования является синтез метода повышения скрытности систем передачи информации, которые используют сигналы с OFDM-модуляцией, путем формирования поднесущих с помощью применения аналитического сигнала и хаотического отображения полинома Чебышева первого рода третьего порядка. Это дает возможность обеспечения надежной защиты информации в радиотехнических системах передачи информации, использующих сигналы с OFDM-модуляцией, за счет высокого уровня структурной и Independent and Identically Distributed (IID) (степень маскировки сигнала под шум) – скрытности сигналов. Задача: исследовать эффективность разработанного метода повышения скрытности систем передачи информации с помощью численной оценки уровня структурной и IID-скрытности. Исследовать качество восстановления замаскированной информации на приемной стороне. Используемыми методами являются: для формирования и обработки хаотических поднесущих в сигнале с OFDM-модуляцией – методы нелинейной динамики, подходы формирования аналитического хаотического сигнала и методы статистической теории обработки наблюдений; для оценки уровня структурной и IID-скрытности – теория стеганографии, метод нелинейного анализа временного ряда, основанного на использовании Brock Dechert Scheinkman (BDS) -статистики. Получены следующие результаты: синтезирован метод повышения скрытности систем передачи информации, основанный на использовании сигналов с OFDM-модуляцией и хаотических поднесущих. Проведена оценка уровня структурной и IID-скрытности сигналов, сформирован с помощью предложенного метода. Установлено, что по сравнению с системами, которые используют гармоничные сигналы с OFDM-модуляцией, хаотичные сигналы с OFDM-модуляцией способны обеспечить высокий уровень IID-скрытности. Это подтверждается полученными результатами визуального, частотного, статистического и динамического анализа. Для оценки уровня структурной скрытности дана оценка затратам на выявление сформированных сигналов с заданной вероятностью. Полученные результаты показали, что уровень структурной скрытности увеличился в 2...2,5 раза. Показано, что для обеспечения необходимого уровня восстановления сформированного сигнала отношение сигнал / шум на входе приемника должно быть больше 4 дБ. Выводы. Научная новизна полученных результатов заключается в следующем: впервые получен метод формирования поднесущих для сигналов с OFDM-модуляцией на основе использования аналитического сигнала и полинома Чебышева первого рода третьего порядка. Предложенный метод обеспечивает необходимый уровень структурной и IID-скрытности систем передачи информации по сравнению с обычными методами формирования сигналов с OFDM-модуляцией, за счет сходства сформированных сигналов с “белым” шумом. При этом предложенный метод позволяет использовать такие сигналы в радиотехнических системах передачи информации.

Ключевые слова: система передачи информации; IID-скрытность; OFDM-модуляция; псевдофазовое пространство; BDS-статистика.

THE METHOD OF INCREASING THE STEALTHINESS OF INFORMATION TRANSMISSION SYSTEMS BASED ON MODULATING WITH ORTHOGONAL FREQUENCY DIVISION AND MULTIPLEXING OF CHAOTIC SUBCARRIERS

*K. Vasiuta, U. Zbezhkhovska, V. Slobodyanuk, I. Zakharchenko, O. Kashchysyn,
M. Dubinsky, Y. Ryabukha, O. Koval*

The subject of the research is the processes of formation and processing of signals with orthogonal frequency division and multiplexing (OFDM) of chaotic sequences to ensure the stealthiness of data transmission. The research synthesizes the method for increasing the stealthiness of information transmission systems based on signals with OFDM-modulation on the basis of forming an analytical signal and chaotic mapping of Chebyshev polynomial. It would enable ensuring reliable information protection in radio transmission systems that use signals with OFDM-modulation, at the cost of the high level of structural and independent and Identically distributed (IID) (the degree of signal masking under noise) stealthiness of the signals. The tasks are to investigate the effectiveness of the developed method for increasing the stealthiness of information transmission systems by numerical assessment of the level of structural and IID-stealthiness and the quality of recovery of the masked information on the receiving side. The methods used are for the formation and processing of chaotic subcarriers in the signal with OFDM-modulation – methods of nonlinear dynamics, approaches to the formation of analytical chaotic signal and methods of the statistical theory of observation processing; to assess the level of structural and IID-stealthiness – steganography theory, a method of nonlinear time series analysis based on the use of BDS-statistics. The following results are obtained: the method for increasing the stealthiness of information transmission systems based on the use of signals with OFDM-

modulation and chaotic subcarriers has been synthesized, has also evaluated the level of structural and IID-stealthiness of signals, that generated using the proposed method. It is established that compared with systems that use harmonic signals with OFDM-modulation, chaotic signals with OFDM-modulation can provide a higher level of IID-stealthiness. It was confirmed by the obtained results of visual, frequency, statistical and dynamic analysis. To assess the level of structural stealthiness, the expenditure of detecting the generated signals with a given probability has been estimated. The obtained results showed that the level of structural stealthiness increased by 2...2.5 times. It has shown that to ensure the required level of recovery of the generated signal, the signal-to-noise ratio at the input of the receiver must be greater than 4 dB. Conclusions. The scientific novelty of the obtained results lies in the following: for the first time, the method of subcarrier formation for signals with OFDM-modulation based on the use of analytical signal and Chebyshev polynomial of the first kind of tertiary is obtained. The proposed method provides the required level of structural and IID-stealthiness of information transmission systems, compared with conventional methods of signal generation with OFDM-modulation, due to the similarity of the generated signals with "white" noise.

Keywords: information transmission system; IID-stealthiness; OFDM-modulation; pseudo-phase space; BDS-statistics.

Васюта Костянтин Станіславович – д-р техн. наук, проф., заст. начальника університету з навч. роботи, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна.

Збежховська Уляна Романівна – ад'юнкт, каф. радіоелектронних систем пунктів управління ПС, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна.

Слободянюк Валерій Валерійович – канд. техн. наук, старш. викл., каф. авіаційних радіотехнічних систем навігації та посадки, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна.

Захарченко Ірина Вікторівна – канд. техн. наук, старш. викл., каф. математичного та програмного забезпечення автоматизованих систем управління, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна.

Кащишин Олександр Леонтійович – ад'юнкт, каф. авіаційних радіотехнічних систем навігації та посадки, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна.

Дубинський Марко Сергійович – ад'юнкт, каф. бойового застосування та експлуатації автоматизованих систем управління, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна.

Рябуха Юрій Миколайович – д-р техн. наук, доцент, каф. фізики надвисоких частот, Харківський національний університет імені В. Н. Каразіна, Харків, Україна.

Коваль Олексій Васильович – ад'юнкт, каф. радіоелектронних систем пунктів управління ПС, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна.

Konstantyn Vasiuta – doctor of technical sciences, professor, deputy chief in academic work, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine, e-mail: kohafish@ukr.net, ORCID: 0000-0002-1978-3717.

Uliana Zbezhkhovska – PhD student, department of radioelectronic systems of control points of Air Forces, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine, e-mail: lyasya3@gmail.com, ORCID: 0000-0001-6213-5531.

Valerii Slobodyanuk – PhD, senior instructor in department of aviation radiotechnical navigation and landing systems, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine, e-mail: sloval@i.ua, ORCID: 0000-0002-8291-8194.

Iryna Zakharchenko – PhD, senior instructor in department of mathematical and software support for automated control systems, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine, e-mail: irishka310379@gmail.com, ORCID: 0000-0002-8534-1888.

Oleksandr Kashchishyn – PhD student, department of aviation radiotechnical navigation and landing systems, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine, e-mail: kaschishin@ukr.net, ORCID: 0000-0003-4447-9415.

Marko Dubinsky – PhD student, department of combat application and operation of automated control systems, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine, e-mail: midlends@ukr.net, ORCID: 0000-0002-3885-8382.

Yurii Ryabukha – doctor of technical sciences, docent, department of physics of microwave frequencies, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine, e-mail: ryabukhayun@gmail.com, ORCID: 0000-0001-9821-598X.

Oleksii Koval – PhD student, department of radioelectronic systems of control points of Air Forces, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine, e-mail: hnups@ukr.net, ORCID: 0000-0002-9997-6884.