УДК 621.391 **DOI:10.30837/rt.2020.3.202.11**

І.Д. ГОРБЕНКО, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук, Хо Чі Лик

КОМПЛЕКСНЕ ВИРІШЕННЯ ПРОБЛЕМИ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Вступ

Більшість сучасних інформаційно-комунікаційних систем (ІКС), у тому числі бездротові мобільні системи зв'язку, системи радіонавігації, радіоуправління відносяться до систем, розрахованих на багато користувачів. У таких системах безліч каналів розміщуються в межах загального частотно-часового ресурсу, так що кожен абонент із впровадженням методів дистанційного доступу має можливість передавати і приймати інформацію одночасно з іншими абонентами і незалежно від них. При проектуванні таких систем основною проблемою є вибір способу множинного доступу, тобто можливості одночасного використання багатьма абонентами каналу зв'язку з мінімальним взаємним впливом. При необхідності обслуговування великої кількості абонентів частотно-часовий ресурс повинен бути значним. Одним з методів підвищення ефективності використання діапазону частот є застосування кодового поділу каналів (абонентів), які працюють в загальній смузі частот (CDMA). При такому методі передачі інформації кожному абоненту виділяється широкосмуговий сигнал (ШСС) з безлічі сигналів, і кожен сигнал займає всю смугу і весь часовий інтервал. Безумовно, саме для таких бездротових ІКС проблема електромагнітної сумісності є однією з найбільш пріоритетних. Електромагнітна сумісність (ЕМС) має на увазі безконфліктне існування різних радіотехнічних систем (в тому числі ІКС) в умовах, коли кожна з цих систем має можливість приймати свої сигнали і сигнали інших систем. Завданням розробника (користувача) системи (наприклад, ІКС) є вилучення або зведення до допустимого рівня негативного впливу системи (наприклад, випромінювання електромагнітних хвиль) на інші системи. До числа методів забезпечення ЕМС відносять: частотне планування у відповідності до вимог міжнародних і національних нормативних документів, контроль за дотриманням яких здійснюють відповідні інституції (служби); застосування антен з вузькою направленістю; ретельна розробка високочастотних вузлів та ін. На наш погляд, проблема ЕМС для сучасних бездротових ІКС може бути вирішена завдяки впровадженню технології розподіленого спектру.

Основні результати досліджень

Основними напрямками побудови ІКС з багатостанційним доступом на основі технології розподіленого спектру, на наш погляд, є: синтез та вибір ансамблів сигналів та сигнально-кодових конструкцій на їх основі в залежності від умов функціонування ІКС; розробка оптимальних і квазіоптимальних алгоритмів і пристроїв їх обробки, які забезпечують виявлення, пошук, оцінювання параметрів сигналів в умовах різного роду параметричної і непараметричної апріорної невизначеності відносно статистичних характеристик сигналів, каналів на фоні усієї сукупності можливих завад; синтез алгоритмів і пристроїв слідкування за часовим зміщенням, частотою і фазою складних ШСС. Крім того, не менш важливим напрямом підвищення ефективності ІКС з багатостанційним доступом на основі кодового поділу каналів є підвищення точності синхронізації ШСС за часом і частотою у сукупності з кодовою адресацією безлічі абонентів. При цьому об'єм ансамблів сигналів і бази ШСС повинні бути значними. Це дозволить підвищити пропускну здатність багатопроміневих каналів на основі виміру з високою точністю параметрів ШСС в умовах багатостанційного доступу при роботі у загальній смузі частот одночасно безлічі абонентів.

Застосування ШСС (з метою синхронізації, а також як фізичних переносників даних) в ІКС дозволяє забезпечити високоефективне використання смуги частот, високу завадостійкість пристроїв обробки сигналів, скритність і конфіденційність передачі інформації при впливі всієї сукупності шумових, структурних, зосереджених, вузькосмугових, імпульсних,

імітаційних, ретрансляційних і інших завад при наявності завмирань в радіоканалах, які обумовлені як умовами розповсюдження сигналів, так і багатопроміневістю каналів зв'язку.

При асинхронному способі множинного доступу абонентів до інформаційних ресурсів ІКС затримки різних сигналів на вході приймального пристрою можуть змінюватися в широкому діапазоні. В цьому випадку процедура синхронізації ШСС (сигнатур) стає проблематичною. Зазначене обумовлено тим фактом, що сигнатури різних абонентів володіють спектрами, що перекриваються, і тому не можуть залишатися ортогональними в широкому діапазоні взаємних затримок. Наслідком зазначеного є виникнення завад множинного доступу, проявом яких служить ненульовий відклик приймача, який налаштовано на *i*-го абонента, від сигналів інших абонентів. Для додатків ІКС, в яких використовується асинхронний метод з CDMA, вибір сигналів необхідно здійснювати таким чином, щоб мінімізувати взаємні перешкоди, тобто забезпечити електромагнітну сумісність.

При вивченні проблеми ЕМС будемо вважати, що в процесі інформаційного обміну беруть участь дві сторони. Перша з них – це система, що здійснює передачу даних (назвемо її «система, що аналізується»). Друга – це система, що наближена до першої («стороння» система»). Для системи, що аналізується, сигнали сторонньої системи можуть трактуватися як завади (вузькосмугові, загороджувальні шумові, внутрішні, структурні, ретрансляційні і ін.). Так само будемо вважати, що в каналі діє найбільш характерний вид завади, що описується гаусівським випадковим процесом, спектр якого збігається зі спектром сигналу. При такому підході ймовірність помилки залежить тільки від відношення потужності сигналу до потужності загального впливу, що заважає.

Характерною ситуацією для практики впливу на нормальне функціонування ІКС, є вузькосмугова завада. Причому даний тип завад може бути реалізовано як станцією протидії з метою порушення роботи системи, так і сусідніми станціями, що створюють перешкоди внаслідок свого звичайного функціонування.

Розглянемо два випадки. По перше, припустимо, що ІКС не впроваджує заходів щодо протидії заваді за виключенням вибору відповідного класу сигналів, тобто система не є адаптованою і у ній не запроваджуються заходи щодо вибору закону модуляції або алгоритму обробки сигналу відповідно до існуючої завадової обстановки. Тоді відношення q_i^2 потужності сигналу до завадового впливу на виході узгодженого фільтру може бути визначено як [1]

$$q_i^2 = 2 \cdot E / (N_0 + P_j / F), \qquad (1)$$

де E – енергія сигналу; F – смуга частот, яку займає сигнал; P_j – потужність сигналу; N_0 – спектральна щільність потужності шуму.

Аналіз останнього виразу свідчить, що не дивлячись на те, що вузькосмугова завада має відповідне значення смуги F_j, відношення q_i^2 приймає таке ж значення, якби потужність завади була рівномірно розподілена у смузі F сигналу, утворюючи додатковий абелевий білий гаусів шум (АБГШ) зі спектральною щільністю P_j / F.

Ішим варіантом є пристосування приймального пристрою до вузькосмугової завади. При такому варіанті оптимальною процедурою обробки є фільтрація, яка враховує завадовий вплив із урахуванням вузькосмугової завади. Така обробка по суті еквівалентна видаленню смуги частот, у якій зосереджена завада. Але при цьому виявляється видаленими і компоненти сигналу, які знаходяться у межах тієї ж смуги частот завади. У такому разі енергія сигналу (оскільки сигнал займає тільки частину полоси F, яка вільна від завади) дорівнює $E \cdot (1 - F_j / F)$, де F_j – смуга частот, яку займає завада. Тоді узгоджений фільтр забезпечує відношення сигнал шум у вигляді

$$q_j^2 = 2 \cdot E \cdot (1 - F_j / F) / N_0 = q^2 \cdot (1 - F_j / F), \qquad (2)$$

де $q^2 = 2 \cdot E / N_0$ – відношення потужностей сигналу та шуму на виході узгодженого фільтру при відсутності завади.

Аналіз відношень (1) – (2) показує, що чим ширше смуга сигналу F у порівнянні з полосою завади F_j, тим менша додаткова спектральна щільність у першому випадку та енергетичні втрати – у другому і, відповідно, більше q^2 і q_j^2.

Таким чином, досягнення високої завадостійкості прийому сигналів при впливі вузькосмугової завади, не вдаючись до збільшення енергії сигналу або пікової потужності сигналу, можливо тільки при розширенні спектру сигналу незалежно від його тривалості. Зазначене безумовно має велике значення для вирішення проблеми електромагнітної сумісності при функціонуванні широкосмугової ІКС і системи, що займає смугу частот, яка менша смуги ІКС і є області, де спектр сигналу не схильний до спотворення завадою.

Можливим сценарієм, який не може бути залишеним без уваги (якщо проводиться аналіз проблеми електромагнітної сумісності ІКС, розрахованих на багато користувачів), є функціонування сторонньої (по відношенню до системи, яка аналізується) системи, спектр якої покриває (без проміжку) спектр системи. Така завада (назвемо її «загороджувальна шумова завада») впливає на сигнал як додатковий АБГШ зі спектральною щільністю потужності, що дорівнює $N_j = P_j / F$. Тому відношення сигнал-завада на виході узгодженого фільтру системи, яка аналізується, буде визначатися як

$$q_j^2 = 2 \cdot E \cdot (N_0 + N_j) = 2 \cdot E / (N_0 + P_j / F). \quad (3)$$

При розгляді сценарію впливу загороджувальної завади як окремий випадок можна припустити, що відношення P_j/F буде суттєво перевищувати спектральну щільність потужності шуму N_0. Такий випадок є цілком припустимим, якщо мати на увазі, що стороння система буде прагнути здійснити ефект придушення, що істотно більший, ніж це можливо при впливі білого шуму. Тоді відношення (3) набирає вигляду

$$q_j^2 = 2 \cdot E \cdot F = 2 \cdot P \cdot (F \cdot T) / P_j. \quad (4)$$

Аналіз (4) показує, що при накладенні обмежень на пікову потужність сигналу системи, що аналізується, та потужність сигналу сторонньої системи, єдиним шляхом вирішення проблеми ЕМС систем при впливі з боку однієї з систем шумової загороджувальної завади є застосування сигналів з великим значенням частотно-часового добутку $F \cdot T$, тобто ШСС (технології розподіленого спектру).

Результати, що наведені вище, справедливі для випадку, коли завада є нормальним випадковим процесом і має рівномірну спектральну щільність. Стороння система може в процесі інформаційного обміну використовувати сигнали, подібні (з точки зору закону маніпуляції) тим, які використовує система, яка аналізується, створюючи так звані структурні взаємні завади з нерівномірним спектром. В таких умовах, внаслідок роботи великого числа абонентів в загальному частотному діапазоні, показники завадостійкості прийому сигналів в ІКС в значній мірі визначаються подібністю (відмінністю) структур сигналу і перешкоди, тобто тим, як придушуються окремі елементи сигналу завадою.

Розглянемо вплив взаємної завади на завадостійкість прийому даних в ІКС.

Нехай ширина загальної смуги частот системи дорівнює F. Припустимо, що ширина спектра всіх сигналів в ТКС дорівнює ширині загальної смуги частот і всі активні абоненти l створюють на вході *k*-го приймача сигнали однакової потужності P_C. У цьому випадку потужність взаємної перешкоди, яка утворюються l абонентами, буде дорівнювати $l \cdot P_C$. Припустимо, що спектральна щільність потужності Nv взаємної завади постійна в межах загальної смуги частот:

$$Nv = \frac{l \cdot P_C}{F}, \tag{5}$$

і взаємна заваду (за своїми статистичними властивостями) наближається до нормального випадкового процесу. Таким чином, зроблені припущення дозволяють вважати взаємну заваду нормальним випадковим процесом з рівномірною спектральною щільністю потужності. Неважко переконатися, що відношення сигнал – шум на вході вирішального пристрою приймача визначається з виразу

$$q^2 = \frac{B}{l} = F \cdot R / l, \tag{6}$$

де R – швидкість передавання інформації.

З (6) випливає, що при заданому числі активних абонентів l збільшення завадостійкості можливо тільки за рахунок збільшення бази (B) сигналів. Це пояснюється тим, що зі збільшенням бази (зі збільшенням ширини спектра сигналів при постійній швидкості передачі інформації R) зменшується спектральна щільність потужності завади $N_П$.

У практиці роботи ІКС можливі випадки, коли потужність одного або декількох сигналів, що заважають у багато разів більше потужності корисного сигналу. Яким чином в цих умовах забезпечити необхідну завадозахищеність.

Нехай потужність корисного сигналу P_C, а потужність сигналу сторонньої станції $P_П$ Потужність сигнальної складової на виході узгодженого фільтра в момент прийняття рішення пропорційна P_C, а потужність складової, що викликана дією завади – $P_П \cdot R_{jk}^2(\tau)$, де $R_{jk}(\tau)$ – взаємнокореляційна функція (ВКФ) корисного *k*-го сигналу і *j*-го сигналу, що заважає. Величина τ визначається зміщенням ВКФ щодо моменту відліку. Відношення сигнал/перешкода на виході пристрою оптимального прийому визначається співвідношенням [2]:

$$q^2(\tau) = \frac{P_C}{P_П \cdot R_{jk}^2(\tau)}, \tag{7}$$

Найменше відношення сигнал/завада

$$q^2(\tau) = \frac{P_C}{P_П \cdot R_{max}^2(\tau)}, \tag{8}$$

де R_{max} – є максимальне значення $R_{jk}(\tau)$.

З (8) стає очевидним, що для підвищення завадозахищеності ІКС необхідно вибирати сигнали, у яких максимальні піки ВКФ мінімальні.

Якщо максимальні піки ВКФ зменшені до середньоквадратичного рівня складає $\sigma_{j,k} = \sigma^2$, то відношення сигнал/завада дорівнюватиме

$$q^2(\tau) = \frac{P_C}{P_П} \cdot \sigma^2. \tag{9}$$

Наприклад, якщо $\sigma^2 = \frac{1}{2 \cdot F \cdot T}$, то

$$q^2(\tau) = \frac{P_C}{P_П} \cdot F \cdot T. \tag{10}$$

Для дискретних фазоманіпульованих широкосмугових сигналів (ФМШПС) $\sigma^2 = \frac{1}{2 \cdot N}$ (де N – число елементів сигналу). Для такого класу сигналів відношення сигнал/завада визначається з виразу

$$q^2(\tau) = \frac{P_C}{P_П} 2 \cdot N . \qquad (11)$$

З виразів (10) – (11) випливає, що збільшення бази сигналу призводить до збільшення q^2 (а значить, до збільшення завадостійкості прийому сигналів в системі) і може компенсувати зменшення відношення $\frac{P_C}{P_П}$ в разі, коли стороння станція вибере стратегію збільшення потужності завади ($P_П$).

Для реалізації вимог ЕМС різних додатків ІКС задача полягає у отриманні такого виграшу від обробки сигналу, який би гарантував достатньо низький рівень спектральної щільності сигналу, що використовується відносно спектральної інтенсивності природнього шуму на вході приймального пристрою сторонньої системи. Застосування широкосмугових сигналів (ШСС) дозволяє поліпшити показники завадостійкості прийому сигналів в ІКС при впливі вузькосмугових, структурних (взаємних), ретрансльованих і організованих завад. При цьому реальна завадостійкість буде нижчою за потенційну. Причинами зниження завадостійкості при входженні в синхронізм і при розрізненні сигналів є наявність бічних піків кореляційних функцій (КФ).

Як критерій вибору класу дискретних сигналів, які використовуються в системах, розрахованих на багато користувачів, як правило, орієнтуються на критерій мінімуму взаємних завад (мінімаксний критерій). Такий критерій має передбачає побудову ансамблів сигналів обсягу K, маніпульованих ДП, як можна помітніше відрізняються один від одного. Причому типовим для теорії зв'язку є підхід, що полягає у використанні безлічі сигналів, що володіють щонайменше однією з наступних властивостей:

1) кожен з сигналів даної безлічі легко відрізнити від своєї зрушеною за часом копії;

2) кожен з сигналів даної безлічі легко відрізнити від будь-якого іншого (в тому числі, зрушеного в часі) сигналу цієї множини.

Перша властивість важлива для радіолокаційних систем, систем синхронізації, а також для широкосмугових систем зв'язку, друга – для систем, розрахованих на багато користувачів, з кодовим поділом абонентів. Найчастіше використовуваним критерієм розрізнення є середньоквадратична відстань. Критерій полягає в тому, що два сигнали, що легко розрізнюються, тоді і тільки тоді, коли середньоквадратична відстань між ними значна. Будемо вимагати також, щоб сигнал $Y(t)$ відрізнявся не тільки від сигналу $X(t)$, але і від $-X(t)$. Необхідність спільного розгляду $Y(t)$ і $X(t)$ виникає при використанні маніпуляції, наприклад в тих випадках, коли сигнал модулюється двійковою послідовністю або коли їм самим модулюється деяка несуча. Таким чином, в якості запобіжного розрізнення сигналів будемо використовувати величину [3]:

$$T^{-1}\int_0^T \left[Y(t) \pm X(t) \right]^2 = -T^{-1}\left\{ \int_0^T \left[Y^2(t) + X^2 \right] dt \pm 2\int_0^T X(t) \cdot Y(t) dt \right\}, \qquad (12)$$

де T – період сигналів $X(t)$ и $Y(t)$.

Перший інтеграл в правій частині (12) є сума енергій сигналів $X(t)$ і $Y(t)$, $0 \le t \le T$. Отже, при фіксованих енергіях сигнал $Y(t)$ сильно відрізняється як від сигналу $X(t)$, так і від сигналу $-X(t)$ тільки в тому випадку, коли параметр

$$r = \int_0^T X(t) \cdot Y(t) dt \tag{13}$$

малий. Параметр r в системах зв'язку, які використовують узгоджену фільтрацію або кореляційний прийом, має сенс відгуку узгодженого з сигналом $Y(t)$ фільтра на вхідний сигнал $X(t)$. Наприклад, якщо в системі зв'язку з багатостанційним доступом сигнали $Y(t)$ і $X(t)$ виділені двом різним станціям, то параметр r є мірою рівня взаємних завад, які створюються кожним із сигналів прийому іншого.

У виразі (12) сигнали $X(t)$ і $Y(t)$ вважалися дійсними. Для переходу до комплексно-значної форми представлення сигналів досить замінити $Y(t)$ комплексно-поєднаним сигналом. У більшості додатків практичний інтерес представляють сигнали, які є послідовностями елементарних імпульсів кінцевої тривалості. Такий сигнал можна записати у вигляді

$$X(t) = \sum_{n=-\infty}^{\infty} x_n \cdot a(t - n \cdot T_c), \tag{14}$$

де $a(t)$ – функціональний вид елементарного імпульсу, T_c – його тривалість.

Якщо умова (14) виконується для всіх t, то період T повинен бути кратний T_c, а послідовність повинна бути з періодом, який дорівнює $N = T / T_c$. Якщо $X(t)$ і $Y(t)$ – періодичні сигнали, і $X(t)$ задається виразом (14), а $Y(t)$ має вигляд

$$Y(t) = \sum_{n=-\infty}^{\infty} Y_n \cdot a \cdot (t - n \cdot T_c), \tag{15}$$

то, у такому випадку, вираз (13) для параметра r зводиться до виду

$$r = \lambda \cdot \sum_{n}^{N-1} X_n \cdot Y_n, \tag{16}$$

$$\text{де} \quad \lambda = \int_0^{T_c} a^2(t) dt. \tag{17}$$

Якщо $a(t) = P \cdot T_c(t)$ – прямокутний імпульс одиничної амплітуди і тривалості T_c, $\lambda = T_c$. Згідно з (16) скалярний добуток двох періодичних сигналів з безперервним часом пропорційний скалярному добутку відповідних дискретних векторів $(x_0, x_1, x_2, ..., x_{N-1})$ і $(x_0, x_1, x_2, ..., x_{N-1})$. Узагальнивши (16) на випадок $r = l \cdot T_c$, отримаємо

$$r_{x,y}(r) = \lambda \cdot \sum_{n=0}^{N-1} X_n \cdot Y_{n+1} \tag{18}$$

що дорівнює скалярному добутку векторів $(x_0, x_1, x_2, ..., x_{N-1})$ і $(y_0, y_1, y_2, ..., y_{N-1})$, помноженому на постійну λ (17).

Наведені міркування є достатньою мотивацією для розгляду періодичної функції взаємної кореляції (ПФВК) послідовностей (X_n) і (Y_n), яка визначається співвідношенням

$$\theta_{x,y}(l) = \sum_{N=0}^{N-1} X_n \cdot Y_{n+1}. \tag{19}$$

З (18) слід, що при $r = l \cdot T_c$, $r_{x,y}(r) = \lambda \cdot \theta_{x,y}(l)$.

При довільних r значення $r_{x,y}(r)$ також визначається ПФВК. Наприклад, якщо $a(t) = P \cdot T_c(t)$, то при любому $0 \le r \le T$

$$r_{x,y}(r) = T_c \cdot \theta_{x,y}(l') + (r - l'T_c) \cdot \left[\theta_{x,y}(l'+1) - \theta_{x,y}(l') \right], \tag{20}$$

де l – найбільше ціле, таке, що $l \cdot T_c \le r$. Відзначимо також, що незалежно від функціонального виду імпульсу $a(t)$

$$\max \left\{ \left| r_{x,y}(r) \right| : 0 \le r \le T \right\} = \lambda_{max} \left\{ \left| \theta_{x,y}(t) \right| : 0 \le l \le N-1 \right\}. \tag{21}$$

Оскільки періодичні кореляційні параметри сигналів (14) і (15) з безперервним часом повністю визначаються взаємно-кореляційною функцією (ВКФ) відповідних послідовностей, завдання синтезу сигналів зводиться до пошуку множин періодичних послідовностей з наступними властивостями:

для будь-якої послідовності $X = (x_n)$ функція $\left| \theta_{x,y}(l) \right|$ мала при всіх $1 \le l \le N-1$;

для будь-якої пари послідовностей $X = (x_n)$ и $Y = (y_n)$ функція $\left| \theta_{x,y}(l) \right|$ мала при всіх 1.

В [3] отримано границі для середньоквадратичних і максимальних (пікових) значень авто- і ВКФ. Пікове значення ВКФ θ_c можна представити у вигляді

$$\theta_c = \max\{ \left| \theta_{x,y}(l) \right| : 0 \le l \le N-1,\ x \in X, y \in X, x \ne y \}, \tag{22}$$

де X _ безліч періодичних дискретних послідовностей.

Максимальне значення бокового піку (пелюстки) автокореляційної функції представимо у вигляді

$$\theta_a = \max\{ \left| \theta_x(l) \right| : 1 \le l \le N-1, x \in X \}, \tag{23}$$

Якщо X – це ансамбль, який складається з K послідовностей, то

$$\left(\frac{\theta_c^2}{N} \right) + \frac{N-1}{N \cdot (K-1)} \left(\frac{\theta_a^2}{N} \right) \ge 1. \tag{24}$$

З (24) слід:

$$\theta_{max} \overset{\Delta}{=} \max\{\theta_a, \theta_c\} \ge N \cdot \left[\frac{K-1}{N \cdot K - 1} \right]^{1/2}. \tag{25}$$

В [4] вказані принципово досяжні значення максимальних бічних піків періодичної функції автокореляції (межі «щільної упаковки») для заданого періоду послідовності N:

$$\theta_{a_{max}} \ge \begin{cases} 0, \text{если } N \equiv 0 \pmod 4 \\ 1, \text{если } N \ne 1 \pmod 4 \\ 2, \text{если } N \equiv 2 \pmod 4 \\ -1, \text{если } N \ne 3 \pmod 4 \end{cases}. \tag{26}$$

Дані значення можуть бути досягнуті для ряду класів дискретних послідовностей: *m*-послідовності, характеристичні коди, багатофазні послідовності (коди Чу, коди Франка), трійчасті послідовності і ін. В [1, 2, 4] запропоновано методи формування і результати дослідження властивостей зазначених сигналів.

Границі (24) задовольняють деякі пари m-послідовностей (кращі пари), що володіють трирівневою функцією взаємної кореляції. Однак для більшості додатків, зокрема, для широкосмугових систем з багатостанційним доступом, інтерес представляють не пари, а великі безлічі послідовностей з хорошими взаємно-кореляційними властивостями. У деяких системах число одночасно використовуваних послідовностей може перевищувати сотні тисяч. Відомі періодичні послідовності (безлічі Касамі, Голда), що володіють покращеними (у порівнянні з *m*-послідовностями) взаємно-кореляційними і ансамблевими властивостями. При цьому правила побудови зазначених класів послідовностей обумовлюють їх низьку структурну скритність, і отже, сигналів, що формуються на їх основі, і які є фізичними переносниками даних у ІКС. Під структурною скритністю розуміється складність визначення сторонньою системою (станцією протидії) правила (закону) побудови дискретної послідовності, що використовується для утворення широкосмугового сигналу.

Дослідження [5, 6] показали, що дискретні послідовності (ДП), які розширюють спектр, повинні бути засновані на нелінійних правилах побудови і мати покращені кореляційні, ансамблеві і структурні властивості. Зокрема, при використанні таких сигналів як фізичного переносника інформації або сигналів синхронізації, часові витрати на розкриття структури використовуваних сигналів зростають і постановка «оптимальних», з точки зору станції протидії, завад стає проблематичною.

В [6, 7] сформульовано у загальному вигляді і вирішено задачу синтезу нового класу сигналів-фізичних переносників даних для застосування у сучасних ІКС, – нелінійних складних дискретних криптографічних сигналів (КС). Під КС пропонується розуміти сукупність послідовностей (векторів) символів певного алфавіту, які мають необхідні (задані) структурні, ансамблеві і кореляційні властивості, часову і просторову складності. Правила побудови КС ґрунтуються на використанні випадкових або псевдовипадкових процесів (в тому числі, із застосуванням алгоритмів криптографічного перетворення інформації), які повинні відповідати вимогам випадковості, незворотності, непередбачуваності і ін. [8]. Необхідно відзначити особливу властивість систем КС: можливість їх відновлення в просторі і в часі із застосуванням ключів. Закон формування кожного з КС визначається ключем, причому довжина ключа може бути суттєво менше періоду (тривалості) самого сигналу. У табл. 1, 2 наведені результати досліджень ансамблевих і кореляційних властивостей різних класів, в тому числі криптографічних сигналів, що дозволяють проілюструвати можливість застосування КС для ряду додатків ІКС [9, 10]. Так, в табл. 1 представлено результати синтезу дискретних послідовностей для деяких значень періоду дискретних послідовності (ДП), зокрема, наведені: граничні значення для максимальних викидів кореляційних функцій (границі «щільної упаковки» [2]); кількість пар послідовностей, що складає повний ансамбль сигналів; кількість сигналів, які за своїми кореляційними властивостями відповідають граничним значенням. У табл. 2 наведені дані щодо числа пар послідовностей різного класу (*m*-послідовності, послідовності з трирівневою функцією взаємної кореляції – ПФВКТ, криптографічні послідовності (КП)), які відповідають граничним значенням («щільній упаковці») для відповідного числа елементів послідовності.

Таблиця 1

Число елементів ДП	Граничні значення ПФВК («щільної упаковки»)	Загальне число пар ДП	Число пар ДП, ПФВК яких задовольняє границі «щільної упаковки»	Найменше значення $R_{бmax}$
64	17	45 553 512	5 451 589	10
63	17	59 056 712	12 214 869	11
127	25	23 106 402	1 266 098	19
127	27	50 060 018	9 006 648	19
511	63	29 353 122	2 666 671	51
1 023	100	36 235 584	5 293 538	81
1 024	90	2 439 840	26 638	82

Таблиця 2

Клас сигналів	Число елементів ДП	Досяжне значення ПФВК для відповідного класу сигналів (границя «щільної упаковки»)	Число пар ДП, ПФВК яких задовольняє границі «щільної упаковки»
m-послідовності	31	9	3
ПФВКТ	31	9	495
КП	31	9	1465137
m-послідовності	127	27	36
ПФВКТ	127	17	11610
КП	127	23	47 053
m-послідовності	255	36	28
ПФВКТ	_	_	_
КП	255	36	17599
m-послідовності	511	63	276
ПФВКТ	511	33	147500
КП	511	63	2666671
m-послідовності	1023	100	435
ПФВКТ	1023	65	338000
КП	1023	100	5293538

Аналіз даних табл. 1, 2 показує, що запропонований метод синтезу криптографічних сигналів [7] дозволяє формувати великі ансамблі дискретних послідовностей практично будь-якого періоду з заданими, але фізично реалізованими, обмеженими границями «щільної упаковки» (24), (25) значеннями бічних пелюсток авто -, взаємної і стикової функцій кореляції в періодичному і аперіодичному режимах роботи, а також статистичними характеристиками кореляційних функцій, які не поступаються аналогічним характеристикам кращих лінійних класів сигналів. Так, для періоду послідовності $N=63$ число пар криптографічних ДП, які відповідають відомому граничному значенню максимальних бічних пелюсток ПФВК – 17, становить 12 214 869. Для представника класу лінійних послідовностей – послідовностей з трирівневою функцією взаємної кореляції (наприклад, безлічі Голда, які є оптимальними з точки зору ФВК [2]), число пар сигналів, які відповідають даній границі, становить – 975. Перевищення обсягу криптографічних сигналів над ансамблем, складеним з *m*-послідовностей, становить більш ніж 10^7 разів. Для періоду послідовності 1023 елементи, число пар криптографічних ДП, що задовольняють встановленому граничному значенню для бічних пелюсток ФВК – 100, становить 5293538, тоді як для *m*-послідовностей число пар, які відповідають даній границі, становить – 435 , тобто перевищення обсягу системи КС становить більш ніж 10^5 разів. Особливості процесів синтезу КС дозволяють варіювати пріоритетністю у досягненні необхідних (для відповідних додатків ІКС) показників ефективності функціонування таких систем. Це обумовлено, насамперед, можливістю проводити синтез КС для будь-якого числа елементів ДП і встановлювати при цьому необхідне граничне значення максимальних бокових пелюсток ФВК, яке у свою чергу визначає фактичні показники завадостійкості прийому сигналів. При незначному зниженні вимог до граничного значення максимального бічного піку ВКФ, відповідно до якого здійснюється відбір сигналів як фізичних переносників даних (по суті, зниження завадостійкості прийому), можуть бути суттєво поліпшені показники захищеності від нав'язування (вводу) хибних даних, режимів роботи ІКС тощо. Саме показники захищеності від імітації, нав'язування, порушення цілісності даних суттєво залежать від ансамблевих властивостей (об'єму ансамблю) застосовуваних систем сигналів. Так, для періоду послідовності $N = 127$ збільшення значення границі допустимих максимальних бокових піків ФВК на 1,2 дБ відносно границі «щільної упаковки» ($R_{б\max} = 17$), дозволить збільшити об'єм ансамблю з $M = 11610$ до 9 006 648 сигналів, тобто в 776 разів.

Виконані розрахунки і проведене імітаційне моделювання свідчить про те, що значення максимальних бічних викидів кореляційних функцій КС, а також статистичні характеристики даного класу сигналів не поступаються відповідним характеристикам лінійних *m*-послідовностей [9].

Висновки

Комплексне вирішення проблем забезпечення електромагнітної сумісності (ЕМС), завадозахищеності та інформаційної безпеки функціонування ІКС, розрахованих на багато користувачів, може бути досягнуто, в тому числі, на основі використання в якості фізичних переносників даних нелінійних дискретних широкосмугових систем сигналів. Пропоновані в роботі нелінійні дискретні криптографічні сигнали, на відміну від відомих класів сигналів, використовуваних в різних додатках ІКС, формуються на основі випадкових (псевдовипадкових) процесів, в тому числі із застосуванням алгоритмів криптографічного перетворення даних, і можуть бути синтезовані для будь-яких значень періоду дискретних сигналів. Системи КС мають структурні властивості, які притаманні аналогічним властивостям випадкових (псевдовипадкових) послідовностей. Синтез даного класу сигналів ґрунтується на обмеженнях, пов'язаних з граничними значеннями функцій авто- і взаємної кореляції сигналів в періодичному і аперіодичному режимах передачі інформації. Характеристики авто – і взаємних функцій кореляції таких сигналів не поступаються характеристикам кращих, з точки зору кореляційних властивостей, лінійних дискретних послідовностей. Обсяг системи нелінійних КС визначається, по-перше, вимогами, зумовленими сферою застосування даного класу сигналів і, по-друге, – вимогами, що пред'являються до системи, з точки зору таких показників ефективності функціонування ІКС, як ЕМС, завадостійкість прийому сигналів, інформаційна безпека системи. Показано, що варіюючи граничними значеннями рівня бічних пелюсток відповідної функції кореляції, в залежності від вимог, що висуваються до ІКС, можна вирішити завдання досягнення необхідних значень показників завадостійкості прийому сигналів і інформаційної безпеки ІКС.

Список літератури:

1. Ipatov, Valery P. Spread Spectrum and CDMA.Principles and Applications / Valery P. Ipatov. 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.

2. Варакин Л. Е. Системы связи с шумоподобными сигналами. 1985. 384 с.

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

4. Свердлик М. Б. Оптимальные дискретные сигналы. Москва : Радио и связь, 1975. 200 с.

5. Gorbenko I., Zamula A., Morozov V. Information and communication systems based on signal systems with improved properties building concept systems with improved properties building concept 2019 CEUR Workshop Proceedings.

6. 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.

7. Gorbenko I., Zamula 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.

8. Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001.

9. 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. Volume 75, 2016 Issue 2. pages 169-178.

10. D. Gorbenko, A. A. Zamula, Ho Tri Luk. Synthesis of derivatives of complex signals based on nonlinear discrete sequences with improved correlation properties // Радиотехника. 2019. Вып. 199. С. 110-120.

Надійшла до редколегії 06.09.2020

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, Україна, email: gorbenkoivan03@gmail.com, ORCID: https://orcid.org/0000-0003-4616-3449

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

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