**УДК 004.728:004.728.3, 004.056.055** **DOI:10.30837/rt.2019.3.198.13**

*О.А. ЗАМУЛА, д-р техн. наук*

# ОПТИМІЗАЦІЯ МЕТОДІВ СИНТЕЗУ ДИСКРЕТНИХ СКЛАДНИХ СИГНАЛІВ У СУЧАСНИХ БАГАТОКОРИСТУВАЧЕВИХ СИСТЕМАХ ЗВ'ЯЗКУ ШИРОКОСМУГОВОГО ДОСТУПУ

## Вступ

У багатокористувачевих системах зв'язку з кодовим поділом необхідні сімейства широкосмугових дискретних складних сигналів з особливими ансамблевими, структурними, технологічними, кореляційними властивостями. Застосування складних широкосмугових сигналів дозволяє підвищити захищеність систем зв'язку при впливі навмисних перешкод у вигляді: загороджувальних перешкод (перешкода у вигляді стаціонарного гаусова шуму з нульовим середнім і рівномірним розподілом спектральної щільності потужності, принаймні, в області частот, зайнятої сигналом), і яка створюється навмисно як засіб радіоелектронної протидії; вузькополосної перешкоди; потужних структурних перешкод з нерівномірним спектром і деяких інших типів перешкод. При радіоелектронній протидії ефективна перешкода може бути організована тільки після виявлення присутності системи, що протистоїть в ефірі і оцінки таких її параметрів як частотний діапазон, яку смугу займає сигнал, форми використовуваних сигналів. Для запобігання можливості виявлення сигналу станцією протидії інфокомунікаційна система (ІКС) повинна використовувати сигнали з розподіленим або широким спектром, які мають максимально можливе значення виграшу від обробки (твір смуги частот, займаної сигналом на його тривалість), і структуру, що практично не розкривається.

## Основні результати досліджень

Проектування і створення сучасних систем зв'язку передбачає використання ансамблів сигналів, які володіють однією з властивостей [1]:

- кожен з сигналів даного ансамблю легко може бути розрізнено від своєї копії, що зсунена у часі;
- кожен з сигналів даного ансамблю легко може бути розрізнено від іншого сигналу цього ансамблю.

Перша властивість є важливою для радіолокаційних, сонарних систем, систем синхронізації, а також для широкосмугових систем зв'язку, друга – для широкосмугових систем зв'язку з багатостанційним доступом і кодовим ущільненням каналів.

Типовим для теорії зв'язку є підхід, що полягає в розробці оптимального приймального пристрою, який з найкращою якістю відновить інформацію, що міститься в коливанні, що спостерігається. Визначення оптимального алгоритму обробки, що базується на обліку специфічних властивостей переданого сигналу, дозволяє синтезувати оптимальним чином і сам сигнал, тобто вибрати найкращий метод його кодування і модуляції.

У теорії зв'язку найбільш поширеною моделлю служить канал з адитивним білим гаусовським шумом, в якому ймовірність трансформації каналом заданого вхідного сигналу в те чи інше вихідне спостереження $y(t)$ (перехідна ймовірність – $P\left[y(t)|S(t)\right]$) експоненціально зменшується зі зростанням квадрата Евклідової відстані між переданим сигналом і вихідним коливанням [2]:

$$P\left[y(t)|S(t)\right]=\kappa\exp\left(-\frac{1}{\mathrm{N}_0}\,d(s,y)\right), \qquad (1)$$

де $\kappa$ – константа, що не залежить від $S(t)$ і $y(t)$, $\mathrm{N}_0$ – спектральна щільність потужності одностороннього білого шуму; а Евклідова відстань між $S(t)$ і $y(t)$ визначається як

$$d(S,y)=\sqrt{\int_0^T[y(t)-S(t)]^2\,dt}\,. \qquad (2)$$

Згідно з співвідношеннями (1) і (2) схожість сигналу (ймовірність того, що він перетворений каналом в спостереження $y(t)$ зменшується зі збільшенням Евклідової відстані між $S(t)$ і $y(t)$. У разі рівної ймовірності всіх повідомлень джерела (що досягається при правильному проектуванні системи) оптимальною стратегією спостерігача, що забезпечує мінімальну помилку визначення дійсно переданого з деяким іншим сигналом, є правило (критерій) максимальної правдоподібності (МП). Згідно з цим алгоритмом, після того, як коливання $y(t)$ стало прийнято, рішення приймається на користь того сигналу, для якого ймовірність трансформації його каналом в прийняте спостереження є найбільшим (в порівнянні з можливостями для інших сигналів). З урахуванням викладеного, МП рішення для гаусова каналу може бути перетворено в правило мінімуму відстані:

$$d(S_j,y)=\min d(S_i,y)\Rightarrow H\ j\,, \qquad (3)$$

тобто рішення приймається на користь сигналу $S_j(t)$, оскільки він найбільш близький (в сенсі Евклідової відстані) до спостереження $y(t)$ серед всіх конкуруючих сигналів.

При виборі класу дискретних сигналів орієнтуються, як правило, на критерій мінімуму взаємних перешкод (мінімаксний критерій). Такий критерій має на меті побудову ансамблів сигналів обсягу M, маніпульованих дискретними послідовностями (ДП), які як можна помітніше відрізняються один від одного при можливих циклічних зрушеннях. Кількісною мірою відмінності маніпулюючих ДП служать максимальні за ансамблями рівні бічних пелюсток періодичної функції автокореляції (ПФАК) і рівні бічних пелюсток періодичної функції взаємної кореляції (ПФВК), що визначаються відповідно як [2]:

$$p_p(m)=\frac{1}{\left\|a^2\right\|}\sum_{i=0}^{n-1}a_i\cdot a^*_{i-m}\,,\ \rho_p,k_l(m)=\frac{1}{\left\|a_k\right\|\left\|a_l\right\|}\cdot\sum_{i=0}^{N-1}a_{k,i}\cdot a^*_{l,i-m}\,, \qquad (4)$$

де $a_k$ ($a_l$) – комплексна амплітуда k(l)-ї дискретної послідовності.

Виходячи з цього, широкосмугові сигнали (ШПС), що застосовуються в системах зв'язку, мають володіти такими кореляційними властивостями, коли бічні піки кореляційних функцій ШПС є якомога меншими, тобто в ідеальному випадку повинні прагнути до нуля. При цьому, процес вибору раціональних по тих чи інших критеріях структур складних сигналів тотожний синтезу відповідних маніпулюючих ДП. Однак вимога ідеальності (нульові значення бічних піків) авто- і взаємно-кореляційних функцій між всіма циклічними зрушеннями K послідовностей і різними ізоморфізмами системи сигналів з періодом N не здійснена, оскільки значення бічних піків не можуть опуститися нижче $1/2\sqrt{B}$ (де B – база сигналу) [3]. Зазначене пояснюється наступним. Оптимальний прийом сигналів здійснюється за допомогою узгодженого фільтра (УФ) або корелятора. Нормований відгук УФ визначається за допомогою інтеграла згортки [3]

$$R_{ij}=\ 1/E\int U_j(t)\ U_k(t-\tau)dt\,, \qquad (5)$$

де $U_j(t)$ – сигнал на вході фільтра, узгодженого з сигналом.

Залежно від того, узгоджений або не узгоджений сигнал з фільтром, чи є додаткове допплерівське зміщення частоти сигналу, кореляційна функція має різні представлення. Одним з таких представлень є взаємна функція невизначеності (ВФН) сигналів з номерами j і k. ВФН може бути представлена через комплексні обхідні сигналів і через їх спектри наступним чином:

$$R_{jk}(\tau,\Omega)\ =\ 1/2E\int_{-\infty}^{\infty}U_j(t)\ U^*_k(t-\tau)\ e^{i\Omega t}dt\ =\ 1/4E\int_{-\infty}^{\infty}G_j(\omega-\Omega)\ G^*_k(\omega)\ e^{i\omega t}d\omega\,, \qquad (6)$$

де $\tau$ – зсув за часом між сигналами; $\Omega$ – допплерівській зсув частоти.

Відгук узгодженого фільтра пов'язаний з ВФН співвідношенням

$$r_{jk}(\tau,\Omega) = \mathrm{Re}\, R_{jk}(\tau,\Omega)\exp(i\omega_0\tau). \quad (7)$$

Об'єм ВФН $R_{jk}$ (τ, Ω) сигналів j і k (обсяг, укладений між поверхнею, яка описується квадратом модуля ВФН і площиною невизначеності), дорівнює одиниці, тобто

$$1/2\pi\int\int_{-\infty}^{\infty} \left| R_{jk}(\tau,\Omega)\right|^2 d\tau\, d\Omega = 1 \quad . \quad (8)$$

і не залежить від номерів і форми сигналів. Іншими словами, отримати тіло невизначеності з нульовими бічними пелюстками неможливо. Тіло невизначеності за умови, що всі бічні піки рівні і рівномірно розподілені в квадраті (2T, 2F) (в цьому випадку бічні піки мінімальні за амплітудою), зображено на рис. 1. Вузький основний пік розташовується на підставі, висота якої $R_0 = ½\sqrt{B}$. Розгляд властивостей ФН дозволяє визначити основні правила побудови сигналів, які можуть бути використані для передачі в сучасних високошвидкісних системах стільникового зв'язку, бездротових дискретних комунікаційних системах, при передачі інформації цифрового телебачення і радіо, в системах радіолокації тощо. Інтегральні відношення, що витікають з властивостей інваріантності об'єму, свідчать, що сигнал, який має єдиний пік у началі координат плоскості невизначеності знайти неможливо. Так звана «кнопочна» функція невизначеності (рис. 1) є найбільш близькою апроксимацією поверхні невизначеності з єдиним піком. Наявність в N – вимірному лінійному просторі не більше N ортогональних векторів (сигналів) робить гіпотетичним ідеальний, з точки зору мінімаксного критерію, ансамбль дискретних послідовностей з нульовими бічними пелюстками функції авто – і взаємної кореляції, і обмежує потенціал зниження кореляційного викиду R при фіксованих N і числі абонентів K.

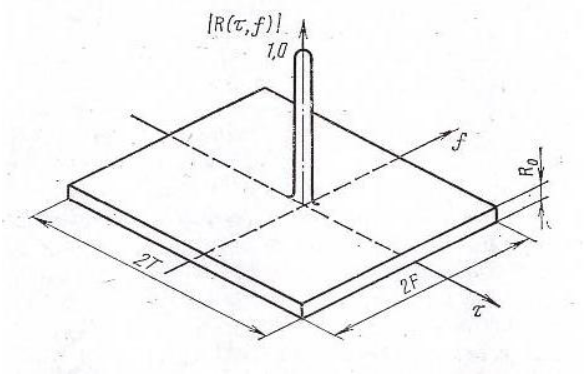


Рис. 1. Тіло невизначеності

У зв'язку з наведеним, при проектуванні і створенні ІКС важливим завданням є вибір сигналів, що забезпечують мінімально можливий рівень взаємних перешкод, який в основному визначається допустимим рівнем максимальних піків взаємно кореляційних функцій (ВКФ). Для режиму виявлення важливо мати систему, складену з сигналів, що володіють малими піками періодичних і аперіодичних автокореляційних функцій (ПФАК і АФАК).

В теорії складних сигналів відомий ряд інтегральних рівності [1]. Нехай $C$ – множина комплексних чисел, а $C^N$ множина векторів з комплексними компонентами. Елементи множини $w, x, y, z \in C^N$ – довільні вектори, а $w, x, y, z$ – відповідні їм дискретні послідовності. Чотири взаємно-кореляційні функції $R_{w,x}$, $R_{y,z}$ , $R_{w,y}$, $R_{x,z}$ пов'язані співвідношенням

$$\sum_{l=0}^{N-1} R_{w,y}(l)[R_{x,z}(l+n)]^* = \sum_{l=0}^{N-1} R_{w,x}(l)[R_{y,z}(l+n)]^* . \quad (9)$$

Поклавши в (1) $z = y$, отримаємо

$$\sum_{l=0}^{N-1} R_{w,y}(l)[R_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} R_{w,x}(l)[R_y(l+n)]^* . \quad (10)$$

Поклавши в (2) $w = x$, отримаємо

$$\sum_{l=0}^{N-1} R_{x,y}(l)[R_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} R_x(l)[R_y(l+n)]^* . \quad (11)$$

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

$$\sum_{l=0}^{N-1} \left|R_{x,y}(l)\right|^2 = \sum_{l=0}^{N-1} R_x(l)[R_y(l)]^* . \quad (12)$$

За допомогою (9) – (12) отримано ряд важливих границь оцінки кореляційних функцій. Рівність (11) означає, що автокореляційна функція (АКФ) послідовності $R_{x,y}$ збігається з взаємно-кореляційною функцією(ВКФ) послідовностей $R_x$ і $R_y$. Крім того, з (12) видно, що середнє значення квадрата модуля функції взаємної кореляції сигналів $x$ і $y$ дорівнює середньому значенню добутку їх АКФ. Фактично це означає, що сигнали, що володіють хорошими автокореляційними властивостями, будуть володіти і хорошими властивостями ВКФ. Це фундаментальне положення теорії систем сигналів було покладено в основу синтезу ансамблів сигналів з відповідними покращеними кореляційними властивостями.

На сьогодні немає єдиної теорії синтезу (з «щільно упакованою» по ПФАК) ДП для довільних довжин послідовностей. У той же час, для вирішення завдань як циклової синхронізації, так і забезпечення необхідної завадостійкості, скритності функціонування системи зв'язку, необхідно використовувати дискретні сигнали з довільними значеннями тривалості послідовностей і мінімальними значеннями бічних пелюсток ПФАК. Процес вибору раціональних по тих чи інших критеріях структур складних сигналів тотожній синтезу відповідних маніпулюючих ДП.

В [4] вказані принципово досяжні значення максимальних бічних піків періодичної функції автокореляції (межі щільної упаковки) для заданого періоду послідовності N. Наведені границі встановлюють критерії синтезу множини ДП (сигнатур). Ансамблі зі значеннями, що передбачають відповідність цим границям, є оптимальними і називаються мінімаксними:

$$\mathrm{R}^{\mathrm{a}}_{\max} \geq \begin{cases} 0, \text{ якщо } \mathrm{N} \equiv 0 (\mathrm{mod}\ 4); \\ 1, \text{ якщо } \mathrm{N} \equiv 1 (\mathrm{mod}\ 4); \\ 2, \text{ якщо } \mathrm{N} \equiv 2 (\mathrm{mod}\ 4); \\ -1, \text{ якщо } \mathrm{N} \equiv 3 (\mathrm{mod}\ 4), \end{cases} \quad (13)$$

Для ідеального гіпотетичного ансамблю $\mathrm{R}_{\max}$ дорівнює нулю, а для будь-якого реального ансамблю мінімальне значення кореляційної функції може служити адекватною мірою його близькості до ідеального.

Ансамблі дискретних послідовностей, що застосовуються у широкосмугових системах зв’язку з прямим розширенням спектру можуть виправдовувати своє призначення тільки в ситуаціях, коли взаємні тимчасові зрушення користувачевих сигналів повністю контролюються системою і можуть бути утримані в рамках передбаченого діапазону. Якщо ж це не виконується, то асинхронний тип широкосмугової системи з множинним доступом і кодовим поділом каналів, заснований на використанні зрушених копій однієї і тієї ж послідовності, схильний до виникнення колізій: сигнал одного з користувачів може придбати затримку, що не дозволяє відрізнити його від сигналу деякого іншого користувача. Останнє може бути підставою для використання ансамблів мінімаксних сигналів. Оскільки кореляційний пік мінімаксного ансамблю отримано в результаті максимізації на всьому періоді, то його мале значення (досягнуте за рахунок досить великої довжини N) забезпечує близькість кореляційних властивостей ансамблю до ідеальних характеристик. Інтерес до послідовностей з хоро-

шою періодичною АКФ не обмежується тільки їх роллю вихідного матеріалу для побудови хороших аперіодичних послідовностей. Існує безліч програм, заснованих на використанні періодичних дискретних сигналів (CW – локація, навігація, пілотний канал і канал синхронізації в мобільних системах радіозв'язку, радарні і сонарні системи з безперервним випромінюванням і ін.), що зумовлює важливість періодичної АКФ щодо системних характеристик. Прийнято вважати «ідеальною» таку ПФАК, яка володіє нульовими бічними пелюстками, тобто нульовими значеннями між періодичними основними пелюстками, що повторюються з періодом N. При цьому можлива ситуація, коли прийнятне значення вимагає досить великої довжини N. Наприклад, для локаційних дальномірних і сонарних систем вимоги часового розрішення сигналів в динамічному діапазоні, що перевищує 80дБ, є досить звичайним. Для виконання цієї умови потрібні оптимальні бінарні послідовності довжини, що перевищують $10^4$, що може уповільнити початкову процедуру пошуку сигналу [2]. Очевидно, що для подібних випадків може служити ідеальна ПФАК (13), яка є недосяжною на безлічі бінарних кодів.

Розглянемо можливі шляхи досягнення ідеальної ПАКФ для випадків, коли алфавіт не обмежений вимогою бінарності сигналів {± 1}.

**Бінарні послідовності з непротилежною модуляцією**

Сутність побудови таких послідовностей полягає у заміні алфавіту {+1,-1} на деякий інший алфавіт є додаванням константи *c* до вихідного алфавіту {+1,-1} послідовності $a_o, a_1, ....a_{n-1}$, а саме: символи +1 і - 1 змінюються на + 1 + *c* і - 1 + *c* відповідно. В [1] наведено правило перетворення бінарної мінімаксної послідовності з ПФАК виду (14) в нову з ідеальною АКФ: елементи, що відповідають - 1, замінюють на $-1 \pm \frac{2}{\sqrt{N+1}}$, а елементи +1 залишаються без зміни. Даний метод визначає використання значень комплексних амплітуд тоді, коли установка і підтримування їх може виявитися утрудненою на практиці.

**Багатофазні коди**

Одним з правил конструювання недвійкової фазової модуляції з основою M> 2 з ідеальною ПФАК є алгоритм, відповідний кодам квадратичних лишків [2]. Зазначені коди існують при довільному значенні довжини N і формуються як [3]:

$$a_i = \begin{Bmatrix} \exp\left(\frac{j\pi i^2}{N}\right), N - четное \\ \exp\left(\frac{j2\pi i^2}{N}\right), N - нечетное \end{Bmatrix}, \quad (14)$$

де *i* = ……. -1,0,1 ……..

Практична реалізація кодів квадратичних лишків, незважаючи на те, що ці коди є переконливим прикладом ФМ послідовності з ідеальною АКФ, проблематична. Зазначене обумовлено наступним: розмір фазового алфавіту лінійно зростає зі збільшенням довжини і відстань між сусідніми фазами стає надзвичайно малою. Цим, в свою чергу, обумовлена зростаюча вимогливість до точності формування символів коду, якості відтворення фаз, умовам експлуатації та ін. До множини багатофазних кодів відносять коди Франка. Вони здійснюють так само як і коди квадратичних лишків покрокову апроксимацію лінійної частотної модуляції і існують при значеннях довжин, що представляють квадрат цілого числа $N = h^2 = 4,9,16,25,36,49$ .... Правило їх формування описується співвідношенням

$$a_i = \exp\left(\frac{j\pi i}{h}\left[\frac{i}{h}\right]\right), i = .....-1,0,1...., \quad (15)$$

де [ x ] позначає округлення x в меншу сторону.

З (14) і (15) випливає, що збільшення обсягу алфавіту з ростом N відбувається значно повільніше. Аналіз багатофазних кодів показує, що технологічно дані коди не настільки привабливі в порівнянні з бінарними протилежними кодами.

**Троїчні послідовності**

На відміну від бінарних послідовностей елементи троїчних послідовностей $a^2$ на додаток до значень ± 1 приймають ще й нульове значення, тобто використовується трійчастий алфавіт {-1,0,1}. Такий алфавіт означає комбінування бінарної ФМ з паузами, тобто інтервалами часу, протягом яких відсутня передача символів. В [2] розглянуто способи конструювання троїчних послідовностей. Суть одного із способів полягає в наступному. Нехай $d_i, i = ....-1,0,1,....p$ - на *m*-послідовність, де *p* – просте непарне число. Кожен символ послідовності є елементом простого поля GF(P). Послідовність перетворюється в троїчну шляхом відображення нульового елемента в уявний нуль, а ненульові елементи – в їх двозначні характери. Після подібного перетворення змінюють знаки всіх елементів, що стоять на непарних позиціях. Формально, алгоритм може бути представлений таким співвідношенням

$$a_i = \begin{Bmatrix} (-1)^i \Psi(d_i) d_i \neq 0 \\ 0, d_i = 0 \end{Bmatrix}, \quad (16)$$

де *i* = ….., -1,0,1……

Однією з основних причин появи інтересу до розширення спектра в задачах часового виміру служить прагнення досягнути високих показників при низькій пікової потужності, тобто при розподілі енергії сигналу на великому часовому інтервалі. Як показник ефективності розподілу енергії в часі використовують величину пік-фактору V, тобто відношення пікової та середньої потужності. Для будь-якої ФМ, і зокрема бінарної, енергія послідовності сигналу рівномірно розподілена на періоді так, що пікова і середня потужності однакові і, отже, V = 1. Зведення $N_p$ пауз на періоді троїчної послідовності порушує рівномірність розподілу енергії і збільшує пік-фактор в $\frac{N}{N-Np}$ раз. Таким чином, цільовою функцією синтезу є побудова троїчних послідовностей не тільки з ідеальною ПФАК, але і малим числом нулів $N_p$ на періоді, тобто пік-фактором, який незначно перевищує одиницю. Троїчна послідовність може бути утворена за допомогою посимвольного множення отриманої відповідно до правила (17) послідовності на єдину бінарну послідовність 1,1,1, – 1, яка має ідеальну ПФАК. Результуюча троїчна послідовність буде характеризуватися учетверо більшою довжиною без зміни значення пік-фактору і ідеальності АКФ. Крім того, послідовності, що утворюються шляхом посимвольного добутку двох троїчних послідовностей з ідеальною ПФАК і взаємно простими довжинами $N_1$, $N_2$, так само будуть мати ідеальну АКФ, довжину $N_1 \cdot N_2$ і пік-фактор $V = V_1 \cdot V_2$. В [1] показано, що такі послідовності володіють ідеальною періодичною АКФ:

$$P_p(m) = \begin{Bmatrix} P^n - 1, m \neq 0 \bmod N \\ 0, m = 0 \bmod N \end{Bmatrix}, \quad (17)$$

де $N = \frac{P^n - 1}{P - 1}$ – істинний період троїчної послідовності.

**Характеристичні коди**

До числа привабливих, з точки зору кореляційних властивостей, відносяться характеристичні дискретні сигнали (характеристичні коди, далі – ХДС) з числом позицій $N = 4x + 2$ і, $N = 4x, x = 1,2$ [4]. Максимальні бічні викиди ПФАК таких сигналів складають {- 4, 0}, тобто даний клас сигналів відноситься (у відповідності до (14)) до оптимальних або мінімаксних

сигналів. Обсяг системи ХДС визначається зі співвідношення [4]: $M = \phi(N)/n$, (φ (N) – функція Ейлера, *n* – ступінь розширення поля $GF(P^n), n \geq 1$.

**Криптографічні сигнали**

Під час досліджень [5, 6] вперше отримано метод синтезу складних нелінійних криптографічних сигналів ( КС), що дозволяє створювати: великі ансамблі дискретних послідовностей практично будь-якого періоду з необхідними (для відповідних задач, що стоять перед ІКС) значеннями бічних пелюсток авто, взаємної і стикової функцій кореляції в періодичному і аперіодичному режимах роботи; послідовності з статистичними характеристиками кореляційних функцій (КФ), аналогічними характеристиками кращих, з погляду кореляційних функцій, лінійних класів сигналів; послідовності, які відповідають вимогам незворотності, нерозрізненості, непередбачуваності і володіють необхідними структурними та ансамблевими властивостями. КС засновані на нелінійних правилах побудови, оскільки при їх створенні застосовують випадкові (псевдовипадкові) процеси, зокрема, алгоритми криптографічного перетворення даних. Зазначене дозволяє покращити показники завадозахищеності, імітостійкості, структурної скритності ІКС, а також завадостійкості прийому сигналів в умовах впливу структурних, загороджувальних, ретрансльованих та інших видів завад і мають покращені кореляційні, ансамблеві і структурні властивості. Зокрема, при використанні таких сигналів як фізичного переносника інформації або сигналів синхронізації часові витрати на розкриття структури використовуваних сигналів зростають і постановка «оптимальних», з точки зору станції протидії, перешкод стає проблематичною.

Будь-який циклічний зсув послідовності довжини N володіє такою ж періодичною ПФАК, що і вихідна послідовність, оскільки періодична ПФАК – інваріантна до циклічного зсуву. Аперіодична ФАК (АФАК) циклічно зрушеної копії може відрізнятися від АКФ первісної. Даний факт разом з границею (13) становить основу методу (алгоритму) пошуку послідовностей з прийнятною АКФ. Очевидно, що знаходження оптимальних бінарних послідовностей великої довжини практично не піддається реалізації. Така задача може бути сформульована у вигляді: найти бінарній код з задовільно малим рівнем бічної пелюстки. Загальна ідея алгоритмів, спрямованих на вирішення цієї задачі, полягає в попередньому відборі деякої обмеженої множини послідовностей, яка здається багатообіцяючою в плані кореляційних властивостей, и подалі – в пошуку коду з мінімальним значенням тільки серед послідовностей, які увійшли у зазначену множину. На першому етапі для заданої довжини N деяким чином формується безліч послідовностей з хорошою ПФАК. Вона може включати всі відомі послідовності заданої довжини N, рівень бічних пелюсток ПФАК яких згідно (14) дозволяє сподіватися на отримання низького значення $R_{max}$. Наприклад, якщо необхідні бінарні коди довжиною N = 63, то початкова множина може бути обмежена *m*-послідовностями, криптографічними сигналами, або включати інші послідовності з задовільною ПФАК.

На другому етапі здійснюється пошук за критерієм найменшого рівня максимуму АФАК серед усіх одноперіодних сегментів послідовностей кандидатів. Зокрема, береться одноперіодний сегмент першої послідовності кандидата, обчислюється його АФАК і запам'ятовується в пам'яті рівень максимального бічного пелюстка поряд з номерами послідовності кандидата і його зсуву. Потім здійснюється циклічний зсув сегмента на одну позицію і проводяться необхідні обчислення. Якщо нове значення максимуму аперіодичної бокової пелюстки виявиться нижче попереднього, то його значення і номер нового зсуву замінюють раніше записані в пам'яті дані, в іншому випадку зареєстровані значення зберігаються без зміни. Дана процедура повторюється N раз, тобто для всіх циклічних зрушень першої послідовності кандидата. Результатом пошуку є послідовність з мінімальним значенням $R_{max}$ серед послідовностей, відібраних на першому етапі. Ансамбль можливих сигналів може бути складений, поряд з іншими кодами, і з характеристичних кодів. Для кожного з кодів слід шляхом циклічного зсуву його символів знайти оптимальні за мінімаксним критерієм аперіодичні коди і відібрати з них найкращі.

Дослідження автокореляційних властивостей ХДС в аперіодичному режимі передач показали [7], що для періоду ДП 256 символів існує 56 характеристичних ДП, для яких значення максимальних бічних піків АФАК не перевищує значення 18 (1,1√N). Такі значення бічних піків є меншими ніж бічні піки одних з кращих, з точки зору кореляційних властивостей, *m*-послідовностей. Форму АФАК для однієї з таких ДП показано на рис. 2. Дані про деякі з характеристичних сигналів (коефіцієнт децимації, який використаний для отримання відповідного ізоморфізму ДП, і циклічний зсув цих ізоморфізмів) наведено в табл. 1. Було синтезовано 470 ХДС, нормовані значення максимальних бічних піків АФАК яких не перевищують величини 20/256. У стандарті системи з кодовим поділом UMTS в якості коду первинної синхронізації використовується бінарна синхропослідовність (СП) з періодом 256 двійкових елементів, які володіють аперіодичними бічними пелюстками аж до ¼, тобто $R_{max}$ = 64 (або -12 дБ) [2]. При виборі ХДС як СП, у порівнянні з сигналами, що застосовуються в стандарті UMTS, виграш, з точки зору завадостійкості прийому сигналів, становитиме більше 4 дБ [2]. Необхідно зауважити, що для періоду ХДС з періодом 256 символів існує 64 ізоморфних сигналів, що суттєво перевищує обсяг системи лінійних сигналів (М-послідовностей) для даного періоду.

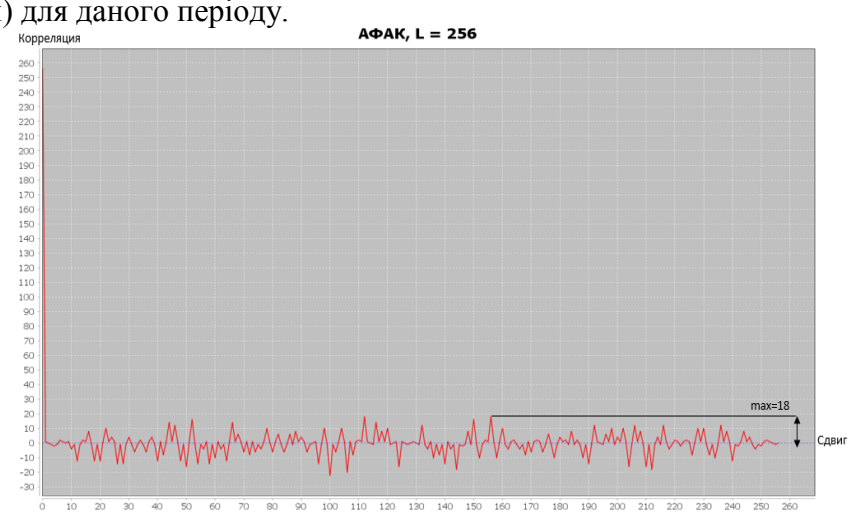


Рис. 2. АФАК ХДС (циклічний зсув {112}, коефіцієнт децимації – 7)

Зазначене має істотне значення для систем, однією з вимог до яких, є забезпечення захищеності від нав'язування (введення) неправдивих повідомлень, помилкових режимів роботи і інше. Для перевірки гіпотези щодо можливості застосування (з метою покращення показників інформаційної безпеки, завадостійкості прийому сигналів, скритності функціонування ІКС) криптографічних сигналів було синтезовано 680 сигналів даного класу, величина $R_{max}$ АФАК для яких, не перевищує значень 33 (це найкраще граничне значення для максимальних бічних піків двійкових сигналів з періодом 256 елементів).

Таблиця 1

| Період (N) | Коефіцієнт децимації | Максимальні бокові піки АФАК | Відповідні зсуви ізоморфізмів ХДС |
|---|---|---|---|
| 256 | 7 | 18 | {112,156 } |
| 256 | 13 | 18 | {44,66 } |
| 256 | 37 | 18 | {58} |
| 256 | 47 | 18 | {114} |
| 256 | 61 | 18 | {84,114,146,160} |
| 256 | 101 | 18 | {92,94} |
| 256 | 127 | 18 | {132,180} |

В цьому випадку, виграш з точки зору ймовірності правильного прийому, в порівнянні з використанням послідовностей, що застосовуються в стандарті мобільного зв'язку UMTS, складає 3 дБ. Якщо висуваються більш жорсткі умови до завадозахищеності прийому сигналів в ІКС, можна запропонувати застосовування КС, для яких значення $R_{max}$ АФАК менше ніж 33 [8, 9]. В табл. 2 наведено дані щодо деяких КС, $R_{max}$ для яких не перевищують значення 26, а на рис. 3 наведено вид АФАК для одного з таких КС.

Таблиця 2

| Номер сигнала | Значення максимальних бокових піків АФАК | Відповідні зсуви КС |
|---|---|---|
| 1 | 25 | {31} |
| 2 | 25 | {61} |
| 3 | 26 | {60} |
| 4 | 26 | {10,22} |
| 5 | 24 | {212} |
| 6 | 26 | {48} |
| 7 | 21 | {3,83} |
| 8 | 26 | {66} |
| 9 | 26 | {62} |
| 10 | 24 | {6} |
| 11 | 23 | {57} |
| 12 | 26 | {8,90} |
| 13 | 25 | {111} |
| 14 | 25 | {39,77,123} |
| 15 | 24 | {26,90} |
| 16 | 23 | {5,23,37,39} |
| 17 | 26 | {16,86} |
| 18 | 24 | {80} |
| 19 | 24 | {70} |
| 20 | 25 | {19} |

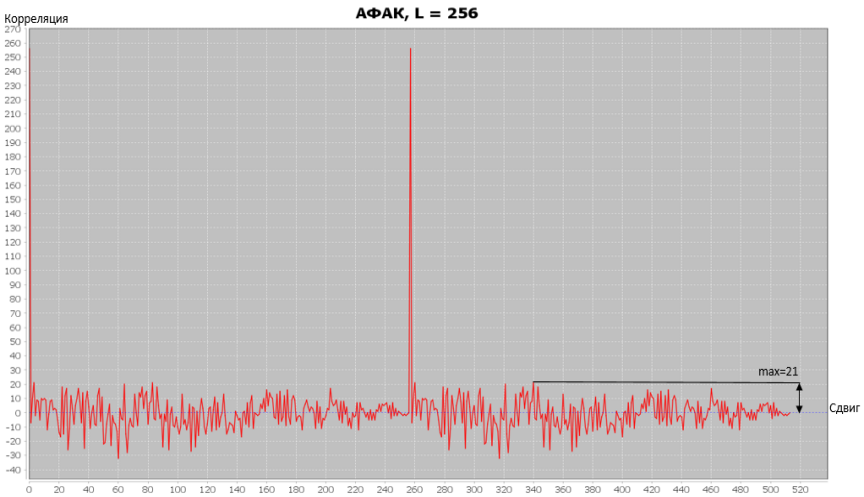


Рис. 3. АФАК КС для N = 256. Циклічний зсув{83}

**Висновки**

Оскільки кодовий поділ абонентів в багатокористувачевих інфокомунікаційних системах ґрунтується на відмінності сигналів, то побудова багатокористувачевих ІКС і показники

ефективності зазначених систем визначаються вибором сигналів і їх властивостями. Зазвичай число абонентів в сучасних інфокомунікаційних системах досить велике, тому вибір сигналів зводиться до визначення систем сигналів із заданими властивостями. Показано, що дискретні послідовності (ДП), властивості яких тотожні властивостям дискретних сигналів з необхідними характеристиками АФАК, насамперед з відповідними значеннями бокових піків АФАК, можуть бути відібрані з множини ДП, значення бокових піків ПФАК яких відповідають (13). Саме ці обставини було застосовано для оптимізації пошуку ДС з покращеними характеристиками АФАК. На основі застосування критерію мінімуму взаємних перешкод (мінімаксний критерій) та існуючих в теорії систем сигналів рівностей, що встановлюють залежність авто- і взаємно-кореляційних властивостей дискретних сигналів, вирішена задача оптимізації пошуку нелінійних дискретних сигналів с покращеними ансамблевими, структурними і кореляційними властивостями. Показано, що застосування синтезованих систем сигналів дозволить підвищити завадостійкість прийому сигналів (ймовірність правильного прийому сигналів) та показники інформаційної безпеки та скритності функціонування інформаційно-комунікаційних систем в умовах кібератак, дії природніх та організованих, в тому числі, структурних, ретрансльованих і інших завад. Показано, що при побудові криптографічних сигналів ІКС, до яких висуваються підвищені вимоги щодо інформаційної безпеки, завадостійкості прийому та скритності функціонування, до джерела сигналів слід включати всі відомі послідовності заданої довжини, рівень бічних пелюсток ПФАК яких відповідає граничним оптимальним значенням. У таку множину сигналів в якості кандидатів можуть увійти, зокрема, як свідчать представлені результати, і нелінійні дискретні сигнали, синтез яких заснований на використанні властивостей елементів кінцевого поля, а також сигнали, які створені із застосуванням випадкових (псевдовипадкових) процесів, криптографічних сигналів. Для кожної послідовності-кандидата шляхом циклічної перестановки його символів знаходять оптимальні за мінімаксним критерієм аперіодичні коди і відбирають з них найкращі.

**Список літератури:**


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

2. Ipatov Valery P. Spread Spectrum and CDMA. Principles and Applications / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electro technical University ‘LETI’, Russia. John Wiley & Sons Ltd, the Atrium, Southern Gate, Chi Chester, West Sussex PO19 8SQ, England.

3. Варакин Л. Е. Системы связи с шумоподобными сигналами. Москва : Радио и связь, 1985. 384 с.

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

5. Горбенко І.Д., Замула О.А. Моделі та методи синтезу криптографічних сигналів та їх оптимізація за критерієм часової складності // Математичне та комп’ютерне моделювання. Серія: Фіз.-мат. науки: зб. наук. праць / Ін-т кібернетики імені В.М. Глушкова Національної академії наук України, 2017. Вип. 15. 272 с.

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

7. Замула А.А. Перспективы применения нелинейных дискретных сигналов в современных телекоммуникационных системах и сетях / Замула А.А., Семенко Е.А // Системи обробки інформації. Харьков : ХУПС, 2015. Вип. 5 (130). С. 129–134.

8. Горбенко И.Д., Замула А.А. Аналитическая оценка значений максимальных боковых выбросов функций корреляции сложных нелинейных дискретных сигналов // Радиотехника. 2017. Вып. 191. С. 76 – 88.

9. Gorbenko I.D., Zamula A.A. Morozov Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts // Telecommunications and Radio Engineering Volume 76, 2017 Issue 19, pages 1705-1717 DOI: 10.1615/TelecomRadEng.v76.i19.30.



*Харківський національний університет*
*імені В.Н. Каразіна*



*Надійшла до редколегії 28.09.2019*