УДК 621.391 **DOI:10.30837/rt.2020.4.203.13**

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

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАВАДОСТІЙКОСТІ ПРИЙОМУ НЕЛІНІЙНИХ СКЛАДНИХ ДИСКРЕТНИХ СИГНАЛІВ ЗІ СТАНДАРТНИМИ СИГНАЛАМИ АФМ-16 BPSK

Вступ

Підвищені вимоги до ефективності функціонування інформаційно-комунікаційних систем (ІКС) в умовах внутрішніх і зовнішніх впливів в значній мірі не враховуються існуючими інформаційними технологіями. Має місце суперечність між жорсткими вимогами щодо забезпечення достовірності, скритності, конфіденційності, цілісності даних, що передаються по лініях зв'язку ІКС [1], з одного боку, і існуючими моделями, методами і технологіями управління ІКС, інформаційною безпекою (ІБ), послугами і якістю обслуговування – з іншого боку.

Проектування ІКС багато в чому ґрунтується на знаходженні дискретно-кодованих сигналів (ДКС) з відповідними ансамблевими, кореляційними, структурними, технологічними та іншими властивостями. В якості маніпулюючих (які розширюють спектр) в широкосмугових системах використовуються сигнали з лінійним законом формування. Такі сигнали володіють досить обмеженими ансамблевими характеристиками і мають низьку кодову стійкість проти розкриття законів їх формування (низьку структурну скритність) [2]. Підвищення показників ефективності функціонування ІКС, а саме: завадостійкість прийому сигналів, інформаційна скритність і імітостійкість системи може бути досягнуто за рахунок використання ДКС, які існують для широкого спектру значень періоду сигналу, мають покращені ансамблеві, кореляційні, структурні властивості. Однак лінійні класи сигналів, що застосовуються у сучасних ІКС, мають незадовільні (особливо для систем критичного призначення) кореляційні, спектральні, ансамблеві та структурні властивості, що, в свою чергу, призводить до погіршення зазначених вище показників функціонування ІКС. Основними шляхами вирішення зазначеного протиріччя є підвищення завадозахищеності (зокрема, енергетичної і структурної скритності, завадостійкості прийому сигналів) і ІБ (зокрема, іміто -і криптостійкості) ІКС на основі удосконалення методологічних основ побудови ІКС шляхом створення нових моделей, методів і технологій управління телекомунікаційними мережами, інформаційною безпекою, послугами і якістю обслуговування, розробки методів інформаційного обміну, методів синтезу нових класів складних дискретних сигналів – переносників даних з необхідними ансамблевими, кореляційними і структурними властивостями.

У роботі наведена статистична імітаційна модель для дослідження завадостійкості різних класів сигналів в гауссовому каналі. Для порівняльного аналізу в якості нелінійних дискретних складних сигналів застосовуються характеристичні дискретні сигнали та криптографічні сигнали.

Характеристичні дискретні сигнали: основні властивості, метод синтезу (ХДС)

ХДС – це нелінійні складні дискретні сигнали, синтез яких базується на використанні характеру ψ мультиплікативної групи поля *GF (P)* [3-4]. ХДС існують для числа позицій (період послідовності): $L = 4x+2$ та $L = 4x$. Відомо, що для $L = 4x+2$ ХДС мають дворівневу періодичну функцію автокореляції $R_{\mu} = \{-2, 2\}$; Для $L = 4x$ – $R_{\mu} = \{-4, 0\}$ і $R_{\mu} = \{0, 4\}$ відповідно. Щодо ансамблевих властивостей, ХДС існують для усіх $N = P^n - 1$ (P – просте, а n – ціле число), кількість ізоморфізмів (об'єм системи сигналів): $\varphi(N)$ – функція Ейлера.

Синтез ХДС базується на використанні найменшого за значенням первісного елемента Θ_j поля $GF(P)$ і задається твердженням 1.

Твердження 1 [4]. Нехай характер мультиплікативної групи поля фіксується функцією

$$\psi(a_i) = e^{j\pi U_i}, \tag{1}$$

тоді алгоритм побудови характеристичного сигналу описується наступними кроками:

1) Формується масив елементів-чисел A_i, $i = \overline{0, P-2}$ поля $GF(P)$:

$$A(i) = \Theta_j^i (\mathrm{mod}\, P). \tag{2}$$

2) Формується група чисел поля $GF(P)$, зрушена за значеннями на одиницю, відповідно до правила:

$$\begin{aligned} &H(i) = A(i)+1, \text{ якщо } \Theta_j^i + 1 \neq 0(\mathrm{mod}\, P); \\ &H(i) = 1, \text{ якщо } \Theta_j^i + 1 \equiv 0(\mathrm{mod}\, P). \end{aligned} \tag{3}$$

3) Формується масив індексів $X(i)$, $i = \overline{0, P-2}$, значеннями якого є відповідні елементу поля індекси $i+1$, впорядковані за вмістом за адресом

$$A(i) : X(i) = X[A(i)]. \tag{4}$$

4) Будується масив індексів $J(i)$, значеннями якого є індекси масиву $X(i)$, які вибрані за адресом $H(i) : J(i) = X[H(i)]$, $i = \overline{0, P-2}$.

5) Обчислюється характер поля за правилом [1, 3]:

$$\psi(a_i) = \psi[J(i)] = \begin{cases} 1, \text{ якщо } J(i) \neq 0(\mathrm{mod}\, 2); \\ -1, \text{ якщо } J(i) \equiv 0(\mathrm{mod}\, 2). \end{cases} \tag{5}$$

Для розкриття закону формування ХДС необхідно знати $\frac{P^n - 1}{2}$ символів послідовності, у той час, як для m-послідовностей та послідовностей Голда необхідно знати сегменти з лише $2 \cdot m$ і $4 \cdot m$ (m – ступінь поліному, у відповідності до якої формується m – послідовність) символів. У зв'язку з тим, що ХДС володіють високою структурною скритністю і відносяться до оптимальних (з точки зору періодичної функції автокореляції (ПФАК)) сигналів, володіють покращеними у порівнянні з взаємно-кореляційними властивостями m-послідовностей, викликає інтерес провести оцінку завадостійкості прийому таких сигналів при застосуванні їх у сучасних ІКС.

Криптографічні сигнали (КС): основні властивості, метод синтезу

КС – нелінійний клас дискретних послідовностей, які мають покращені, у порівнянні з більшістю лінійних класів сигналів, ансамблеві, структурні, кореляційні, а також – криптографічні властивості. Для синтезу складних нелінійних дискретних криптографічних сигналів використовуються випадкові або псевдовипадкові процеси і, на відміну від ХДС, ці сигнали можуть бути побудовані для будь-яких значень періоду. Розмір ансамблю таких сигналів залежить від вимог до кореляційних властивостей, що визначаються границями «щільної упаковки» [2].

Метод синтезу КС з заданими властивостями включає такі етапи [5 – 6]:

1. Генерація масиву псевдовипадкових послідовностей символів заданого періоду з використанням криптографічного алгоритму (джерел випадкових або псевдовипадкових послідовностей символів).

2. Тестування отриманих послідовностей із застосуванням критеріїв та показників якості генераторів, визначених міжнародними та відомчими стандартами [7 – 9].

3. Формування дискретних послідовностей (ДП) символів визначено періоду.

4. Відбір ДП, значення бічних пелюсток періодичної функції автокореляції (ПФАК) яких близькі до границі «щільної упаковки»:

5. Отримання матриці станів взаємно-кореляційних функцій всіх можливих пар послідовностей, які пройшли відбір за результатами попереднього кроку.

6. Обробка матриці, яка полягає в тому, що здійснюється відбір послідовностей, що задовольняють межам «щільної упаковки» для відповідних кореляційних функцій.

Використання наведеного методу дозволяє формувати великі ансамблі дискретних послідовностей практично будь-якого періоду з заданими, але фізично реалізованими, значеннями бічних пелюсток функцій автовзаємної і стикової функції кореляції в періодичному і аперіодичному режимах роботи, а також статистичними характеристиками кореляційних функцій, які не поступаються аналогічним характеристикам кращих класів лінійних сигналів. Що стосується структурної скритності цих сигналів, то вони володіють абсолютною скритністю, тобто володіють властивостями, які притаманні випадковим процесам. Тому оцінки завадостійкості прийому таких сигналів у порівнянні із завадостійкістю для існуючих сигналів також, з точки зору побудови сучасних ІКС, представляє інтерес.

Основні результати дослідження

Найбільш поширеною моделлю безперервних каналів з завадами є гауссов канал. Пов’язано це з тим, що: багато реальних каналів добре описуються даною моделлю; завада в такому каналі має максимальну приведену диференціальну ентропію у порівнянні з будь-якими іншими моделями завад; Гауссов канал відноситься до числа небагатьох каналів, для яких в явному вигляді розраховано величину пропускної здатності. З точки зору умов передачі інформації, гауссов канал є найбільш несприятливим випадком. Результати дослідження завадостійкості, які отримані для гауссового каналу, можуть бути тільки покращені для будь-яких інших моделей каналів та завад [10]. Завада в гауссовому каналі являє собою стаціонарний випадковий процес, в якому два будь-яких вимірювання некорельовані та незалежні. Такий процес володіє рівномірним, нескінченим, за смугою частот, спектром, а отже має нескінчену потужність. Через наявність нескінченого спектру такий процес називають «білим» і, оскільки він взаємодіє з сигналами простим підсумуванням, то – «адитивним» [10]. На рис. 1 представлена загальна структурна схема каналу зв’язку з адитивним білим гауссовим шумом (АБГШ). При моделюванні гауссового шуму обмежуються деякою фіксованою смугою частот, в якій формуються гармонічні коливання з випадковими амплітудами та фазами. Амплітуда гармоніки шуму розподілена за нормальним законом розподілу з нульовим математичним сподіванням та дисперсією N_0, яку називають спектральною щільністю потужності шуму, оскільки вона характеризує середню потужність, яка приходить на 1 Гц смуги частот [10]. При побудові імітаційних моделей каналів з АБГШ формування випадкового шуму здійснюється таким чином, щоб ширина його ефективного спектру та тривалість реалізації були не менше аналогічних сигналів, які випробовуються в моделі.

Була створена модель для випробування сигналів в умовах адитивного білого гауссового шуму.

У створеній моделі реалізовано наступні функції:

– визначення відношення сигнал/шум в діапазоні від 1 до N;

– виконання M обчислювальних експериментів імітації передачі та демодуляції сигналу при різних випадкових реалізаціях завади з підрахунком кількості біт, прийнятих з помилкою із повідомлення довжиною k;

– обчислення ймовірності помилки «на біт» при кожному значенні сигнал/шум;

– повернення вектору, який містить N знайдених значень ймовірностей;

– побудова графіків залежності ймовірності помилки від відношення сигнал/шум.

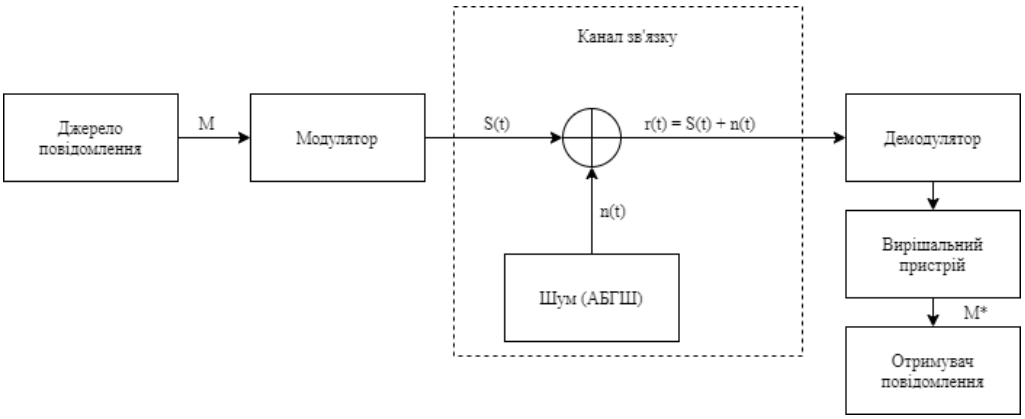

Рис. 1. Структурна схема каналу зв’язку з АБГШ

Реалізація моделі здійснюється у відповідності з блок-схемою (рис. 2).

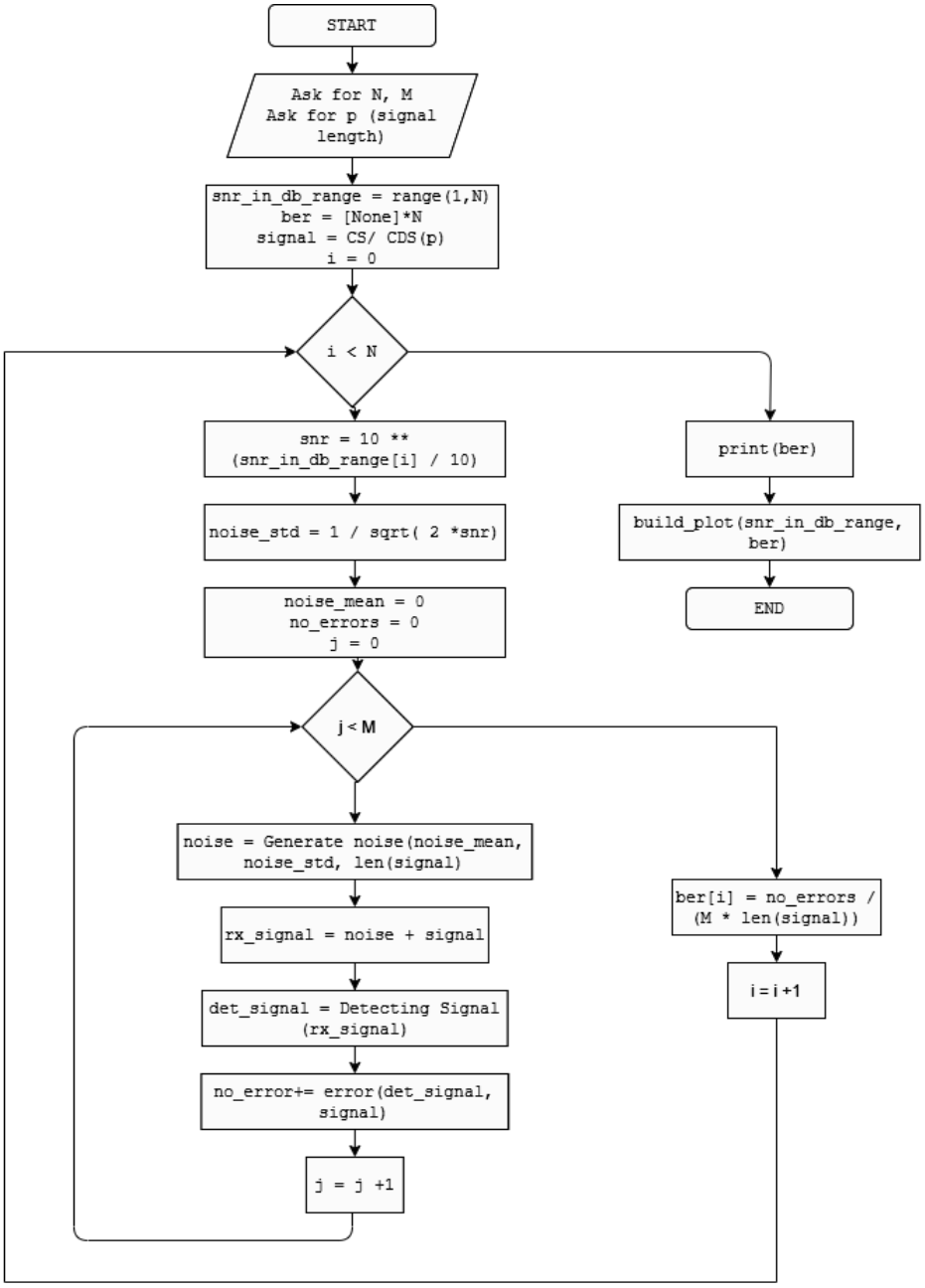

Рис. 2. Блок – схема імітаційної моделі для дослідження завадостійкості прийому сигналів в каналі з АБГШ

На рис. 2 наведено такі операції:

snr_in_db_range – діапазон відношень сигнал/шум (приймає значення від 1 до N);

snr – значення відношення сигнал/шум;

ber – структура даних, в яку буде записано отримані значення ймовірності помилки на біт при заданому SNR;

signal – початковий сигнал, що досліджується (це може бути CS (КС) або CDS (ХДС));

noise_std – середньо-квадратичне відхилення (СКВ), за яким формуються випадкові (гауссові) коефіцієнти амплітуд;

noise_mean – математичне сподівання, за яким сформовано шум;

no_errors – кількість знайдених помилок;

noise – шум, який сформовано за параметрами: noise_mean і noise_std;

rx_signal – сигнал, який передається по каналу з АБГШ (початковий сигнал + шум);

det_signal – сигнал, який виявлено вирішальним пристроєм;

Detecting Signal – процедура виявлення сигналу. Параметри, які приймає ця процедура: rx_signal;

error – процедура, яка підраховує кількість біт, які не збіглися, між signal і det_signal. Параметри, які приймає ця процедура: det_signal, signal;

build_plot – процедура, яка виконує функції побудування графіків для оцінки BER (ймовірність помилки на біт). Параметри, які приймає ця процедура: snr_in_db_range, ber;

Логіка, за якою працює вирішальний пристрій зображена на рис. 3: якщо отримане значення більше 0, то отримали «1», в противному випадку – «-1». Підрахунок кількості біт, які не збіглися, між отриманим сигналом та сигналом, який було відправлено, виконується за алгоритмом, блок-схема якого зображена на рис. 4.

На рис. 3 наведено такі операції:

Reading received signal (rx_signal) – зчитування по каналу з АБГШ сигналу, що передається;

det_sig –сигнал, що виявлено;

len(rx_signal) – тривалість сигналу rx_signal.

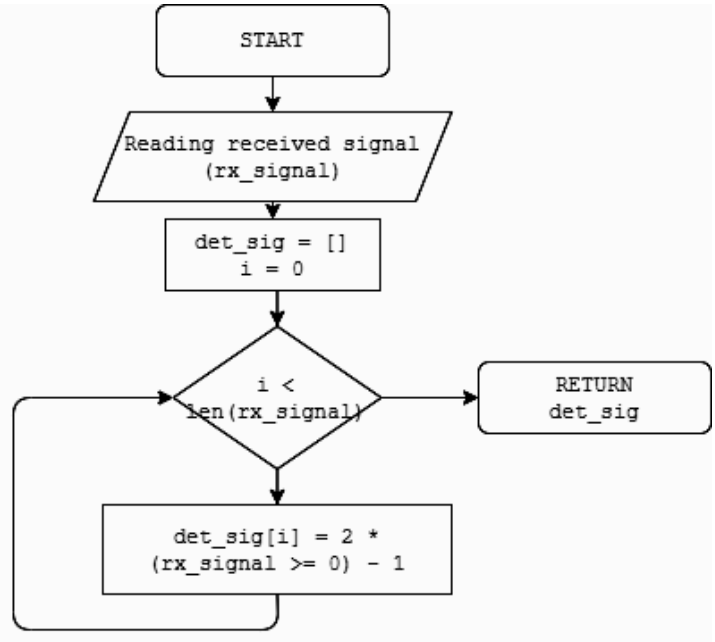

Рис. 3. Вирішальний пристрій

На рис. 4 наведено такі операції:

Reading received signal (det_signal, tx_signal) – зчитування виявленого сигналу та початкового сигналу (того, що було сформовано джерелом повідомлення);

cnt – змінна, яка зберігає кількість біт, що не збіглися;

len(det_signal) – тривалість сигналу det_signal

Програмна реалізація моделі виконувалася на комп'ютері з наступними системними характеристиками:

– Intel Core i7-4500U 1.80 – 2.40 GHz;
– 8 ГБ оперативної пам'яті;
– Windows 10 x64;

Відеокарта Nvidia 740m 2GB.

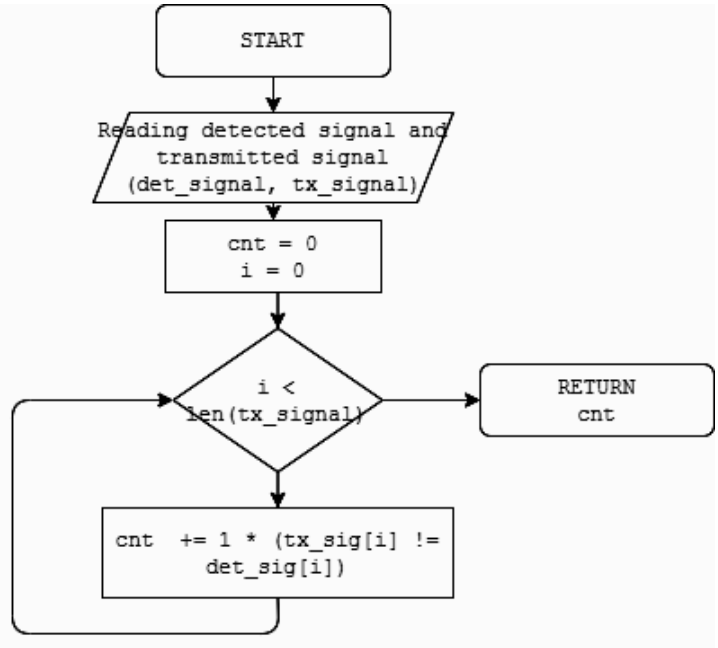

Рис. 4. Підрахунок кількості біт, які не збіглися

Тестування моделі здійснювалося за таких параметрів: відношення сигнал/шум в діапазоні від $N=1$ до $N=10$. Виконання $M=10000$ обчислювальних експериментів імітації передачі та демодуляції сигналу при різних випадкових реалізаціях завади з підрахунком кількості біт, прийнятих з помилкою із повідомлення довжиною $k=256$. Результатами, які отримані на виході моделі, є кількість знайдених помилок та ймовірність помилки на біт при заданому відношенні сигнал/шум (табл. 1).

З використанням отриманих результатів були побудовані графіки залежності ймовірності помилки на біт від значення відношення сигнал/шум (рис.).

Таблиця 1

SNR	Кількість помилок		Ймовірність помилки	
	ХДС	КС	ХДС	КС
1	144237	143922	0.056342578125	0.05621953125
2	96032	96267	0.0375125	0.037604296875
3	58362	58563	0.02279765625	0.022876171875
4	31976	31919	0.012490625	0.012468359375
5	15304	15180	0.005978125	0.0059296875
6	6136	6193	0.002396875	0.002419140625
7	1978	2055	0.00077265625	0.000802734375
8	481	525	0.000187890625	0.000205078125
9	90	78	3.515625e-05	3.046875e-05
10	12	9	4.6875e-06	3.515625e-06

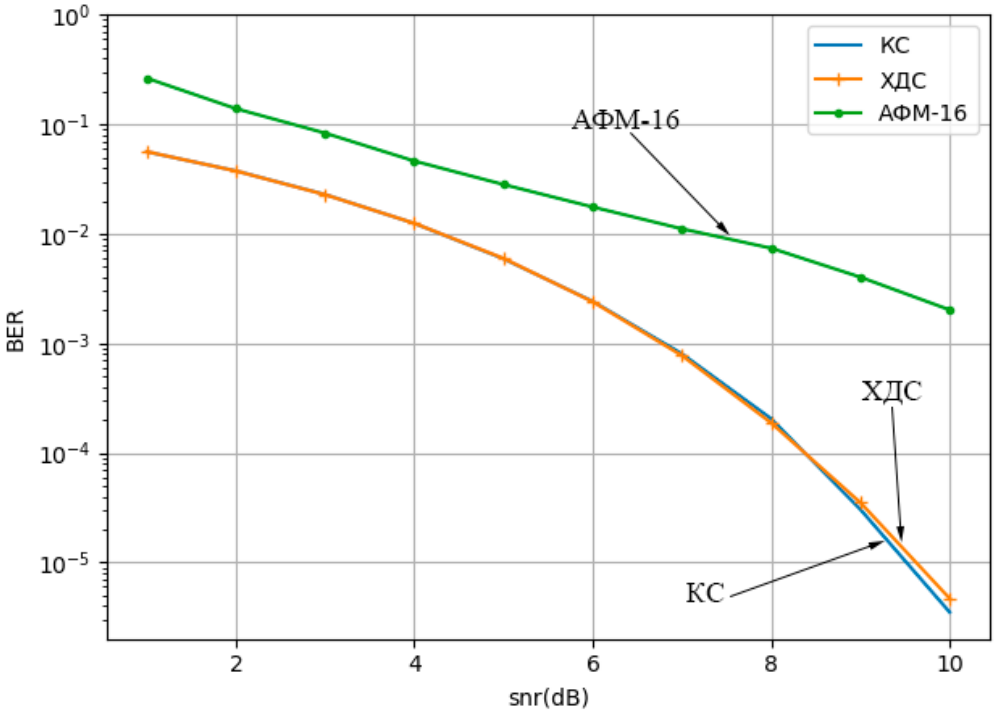

Рис. 5. Графік залежності ймовірність помилки на біт (BER) від відношення сигнал/шум

Для АФМ-16 отриманий вектор BER виглядає наступним чином [0.264275, 0.1391, 0.0832, 0.04625, 0.028225, 0.0176, 0.011125, 0.0074, 0.004025, 0.002025, 0.001375, 0.00085, 0.0008, 0.0003, 0.000125, 0.000125, 7.5e-05, 5e-05, 2.5e-05]. Аналіз отриманих результатів, які наведено у табл. 1, та порівняння їх з результатами для АФМ-16, показують, що сигнали ХДС та КС володіють достатньо низькою ймовірністю помилки, нижчою за АФМ-16.

Висновки

Результати дослідження завадостійкості, які були отримані при використанні розробленої моделі, можуть бути тільки покращені для будь-яких інших моделей каналів та завад. Тому порівняльні дослідження будь-яких ІКС проводять саме в умовах моделі каналу з АБГШ. Для низьких відношень сигнал/шум, ХДС та КС забезпечують низьку ймовірність помилки (0.056 для $SNR = 1$), тому використання саме таких сигналів в «поганих» каналах є ефективним. Порівняння застосування ХДС та КС з АФМ-16 показує, що саме сигнали, що досліджувалися, мають нижчу ймовірність помилки. Так, для відношення сигнал/шум – 10 ймовірність помилки для ХДС складає 4.6875e-06, для КС – 3.515625e-06, а для – АФМ-16 – 0.002025. Таким чином, використання нелінійних складних дискретних сигналів, зокрема ХДС та КС, дозволяє суттєво підвищити завадостійкість прийому сигналів у сучасних ІКС. При цьому, зважаючи на покращені ансамблеві і структурні властивості зазначених нелінійних сигналів, є можливість значно поліпшити показники крипто- і імітозахищеності функціонування систем.

Список літератури:

1. Горбенко, І.Д. Прикладна криптологія / І.Д. Горбенко, Ю.І. Горбенко. Харків : ХНУРЕ, 2012. 868 с.
2. Варакин Л. Е. Системы связи с шумоподобными сигналами. 1985. 384 с. 1
3. Свердлик М. Б. Оптимальные дискретные сигналы. Москва : Радио и связь, 1975. 200 с.
4. Горбенко И.Д., Замула А.А., Морозов В.Л. Информационная безопасность и помехозащищенность в телекоммуникационных системах условиях различных внутренних и внешних воздействий // Радиотехника. 2017. Вып. 189. С. 107 – 116.
5. 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, p.p. 1079-1100. DOI: 10.1615/TelecomRadEng.v76.i12.50.

6. Горбенко І.Д., Замула О.А. Моделі та методи синтезу криптографічних сигналів та їх оптимізація за критерієм часової складності // Математичне та комп'ютерне моделювання. Серія: Фіз.-мат. науки : зб. наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2017. Вип. 15. 272 с.
7. Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999.
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. NIST 800-90 b Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.
10. Rassomakhin, S.G. Mathematical and physical nature of the channel capacity // Telecommunications and Radio Engineering. 2017. 76(16). P. 1423-1451.

Надійшла до редколегії 05.11.2020

Відомості про авторів:

Рассомахін Сергій Геннадійович – д-р техн. наук, професор, завідувач кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна.

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

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

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