УДК 621.391

канд. техн. наук Залужний О. В. (ВІТІ)
д-р техн. наук, ст. наук. співр. Чевардін В. Є. (ВІТІ)
Артемчук М. В. (ВІТІ)
Андрєєв А. О. (ВІТІ)

ШЛЯХИ ПІДВИЩЕННЯ ДОСТОВІРНОСТІ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ ОДНОСТОРОННІХ РАДІОКАНАЛІВ

При функціонуванні сучасних інформаційно-комунікаційних систем з використанням односторонніх радіоканалів основним завданням є максимізація достовірності та інформаційної скритності передачі повідомлень. Більшої актуальності це завдання набуває в умовах впливу засобів радіоелектронної боротьби та зростання числа інцидентів, пов'язаних з експлуатацією вразливостей бездротових технологій. Його розв'язання є корисним при використанні технологій інтернету речей з односторонніми протоколами взаємодії, розгортанні систем управління безпілотними літальними апаратами в рамках організації та забезпечення кіберзахисту об'єктів критичної інфраструктури держави.

Метою роботи є визначення шляхів підвищення достовірності передачі повідомлень в інформаційно-комунікаційних системах з використанням односторонніх радіоканалів.

У статті наведено приклади застосування цифрових методів модуляції та завадостійкого кодування в сучасних інформаційно-комунікаційних технологіях з односторонньою радіопередачею. Отримано результати аналізу ефективності використання цифрових методів модуляції та завадостійкого кодування за критерієм мінімуму значення ймовірності помилки на біт. Розглянуто особливості застосування комбінованого випадкового кодування, яке передбачає використання поєднання завадостійкого і стохастичного кодування.

З використанням програми NIST Statistical Test Suite 2.1.2 здійснено тестування стандартизованих генераторів псевдовипадкових послідовностей.

Результати досліджень обґрунтовують доцільність використання сигналів з бінарною відноснофазовою маніпуляцією в поєднанні з мажоритарним кодуванням для підвищення достовірності прийому повідомлень при односторонній радіопередачі. В цьому випадку ми повинні розв'язати завдання щодо вдосконалення існуючих схем оцінки фази прийнятого сигналу та оптимального вибору надлишковості мажоритарного кодування.

Для одночасного підвищення достовірності прийому повідомлень та забезпечення скритності передачі інформації запропоновано застосування принципу комбінованого випадкового кодування. При цьому для формування кодової книги доцільно використовувати Blum-Blum-Shub генератори псевдовипадкових послідовностей. За результатами тестування пакетом NIST Statistical Test Suite був обраний Blum-Blum-Shub генератор.

Ключові слова: *односторонняя радіопередача, достовірність передачі повідомлень, цифрові методи модуляції, комбіноване випадкове кодування.*

Zaluzhnyi O., Chevardin V., Artemchuk M., Andreiev A. Ways to improve the reliability of message transmission in information and communication systems that use one-way radio channels.

Modern information and communication systems which use one-way radio channels have the main task to maximize the reliability and information transmission stealth. This task becomes more relevant in conditions of the radio-electronic warfare and growing of the cyber incidents with wireless vulnerabilities exploitation. This solution is useful for Internet of Things technologies with one-way interaction protocols and unmanned aerial vehicle control systems for organization and critical infrastructure cyber security support.

The purpose of this work is the fading of possible ways for increasing of the message transmission reliability in the information and communication systems with one-way radio channels.

The examples of digital modulation methods applications, interference-resistant coding which are used in modern information and communication technologies with one-way radio transmission are considered in the article. In the work were received results of digital modulation methods and interference-resistant coding analysis with minimum bit error rate criterion. The usage futures of combined random coding which is based on interference-resistant and stochastic coding combination were researched.

Standard random bit generators were tested by the NIST Statistical Test Suite 2.1.2 application.

This research results give us the possibility to increase the reliability of message transmission by way using binary phase-shift keying in combination with majority coding. In this case we should solve tasks to improve the phase estimation schemes of received signal and optimal choice of majority coding redundancy.

In order to increase the reliability and information stealth of message transmission the using of combined random coding was proposed. At the same time, we recommend to use Blum-Blum-Shub random bit generator for the codebook creating. Blum-Blum-Shub random bit generator was chosen according to estimation results, obtained with the help of NIST Statistical Test Suite.

Keywords: *one-way radio transmission, reliability of message transmission, digital modulation methods, combined random coding, information transmission stealth.*

Постановка завдання в загальному вигляді. В наш час активно розвиваються системи телеметрії, моніторингу віддалених об'єктів та оповіщення, засоби дистанційного управління безпілотними літальними апаратами (БпЛА), системи збору інформації з індикаторів кіберінцидентів, в яких окреме місце знаходить одностороння радіопередача. При функціонуванні таких систем основним завданням є підвищення достовірності та інформаційної скритності передачі повідомлень. Більшої актуальності ця задача набуває в умовах впливу засобів радіоелектронної боротьби (РЕБ) та зростання числа інцидентів, пов'язаних з уразливістю криптографічних додатків і програмних засобів, таких як CVE-2022-21449, CVE-2022-23806, CVE-2020-9283, CVE-2016-6303, CVE-2018-6594. Останнє є особливо важливим при проведенні спеціальних операцій, організації кіберзахисту об'єктів критичної інфраструктури держави, коли здійснюється передача інформації, зокрема і радіоканалами. Тому актуальним завданням є визначення можливих шляхів підвищення достовірності передачі повідомлень односторонніми радіоканалами.

Аналіз останніх публікацій.

Результати проведеного аналізу наукових досліджень у даній предметній області свідчать про те, що для підвищення достовірності прийому повідомлень при односторонній радіопередачі застосовується повторна передача повідомлень як на одній частоті, так і на наборові частот, використовуються коригуючі коди з виправленням помилок [1–5]. Такі способи є ефективними в умовах відсутності зворотного каналу зв'язку, проте мають достатньо високу та фіксовану надлишковість. Недостатньо дослідженим залишається напрямок, що пов'язаний з оцінкою особливостей застосування цифрових методів модуляції та завадостійкого кодування з метою визначенням можливих шляхів підвищення достовірності прийому повідомлень в системах з односторонньою радіопередачею. Останнє є особливо важливим для LPWAN (Low Power Wide Area Networks) систем з односторонніми протоколами взаємодії, в яких використовується ультравузькосмуговий діапазон частот, а швидкість передачі інформації не перевищує 100 біт/с [1; 2].

Мета статті: визначення шляхів підвищення достовірності передачі повідомлень в інформаційно-комунікаційних системах (ІКС) з використанням односторонніх радіоканалів.

Виклад основного матеріалу.

В якості прикладів систем з односторонньою радіопередачею розглянуто технології Internet of Things (IoT) з односторонніми протоколами взаємодії (технологія Sigfox та Weightless-N).

Технологія Sigfox [1] підтримує як односторонній, так і двосторонній режими роботи. В односторонньому режимі передача інформації здійснюється тільки висхідною лінією. Для досягнення великої дальності зв'язку при обмеженій потужності передавача (максимальна потужність передавача становить 25 мВт) система функціонує в ультравузькосмуговому діапазоні частот. Ширина смуги частот каналу висхідної лінії зв'язку становить 100 Гц (в Європі). Бітова швидкість на фізичному рівні – 100 біт/с (в Європі). Використовується differential binary phase-shift keying (DBPSK) маніпуляція. Завадостійкі коди з виправленням помилок не застосовуються [6].

Технологія Weightless-N [2] повністю базується на односторонній радіопередачі висхідною лінією. Всі пристрої відправляють повідомлення на центральну базову станцію без синхронізації та підтвердження. В системі використовується DBPSK маніпуляція в поєднанні зі згортковим кодом, що дозволяє виправляти помилки [7]. Виділений діапазон частот розподілений на шість широких смуг (табл. 1).

Таблиця 1

Смуги частот технології Weightless-N

Група №	Нижня смуга, МГц	Верхня смуга, МГц	Смуга частот, МГц	Кількість каналів
1	863	864,998	1,998	9990
2	865	868	3	15000
3	868	868,6	0,6	3000
4	868,7	869,2	0,5	2499
5	869,4	869,64	0,24	1200
6	869,7	870	0,3	1500

Кожна смуга призначена для окремої базової станції. Кінцеві пристрої працюють в вузькій смузі частот 200 Гц (мікроканал). Окрім того, кожна широкосмугова мережа ділиться на три підсмуги (макроканали), кожен з яких містить декілька мікроканалів. Наприклад, кожен макроканал в діапазоні 0,6 МГц містить 1000 каналів. Максимальна швидкість передачі даних – 100 біт/с. Таким чином, вказані системи функціонують в умовах обмеженого часового, частотного та енергетичного ресурсу. В них використовується бінарна відноснофазова маніпуляція. Підвищення достовірності прийому повідомлень шляхом застосування завадостійких кодів можливе тільки за рахунок зменшення швидкості передачі інформації (інформаційної швидкості).

Для визначення шляхів підвищення достовірності передачі повідомлень необхідно проаналізувати можливість використання різних методів маніпуляції в розглянутих системах. З цією метою було здійснено розрахунки середнього значення ймовірності помилки на біт в каналі з білим гаусовим шумом та в релеєвському каналі.

При когерентній (КГ) обробці сигналів з binary phase-shift keying (BPSK), binary frequency shift keying (BFSK) та binary amplitude shift keying (BASK) маніпуляцією ймовірність помилки на біт ($p_{\text{біт}}$) визначається за узагальненою формулою [8]:

$$p_{\text{біт}} = \mathrm{Q}(\sqrt{\alpha\gamma_{\text{біт}}}), \tag{1}$$

де коефіцієнт α = 2 (сигнали з BPSK), α = 1 (сигнали з BFSK), α = 0,5 (сигнали з BASK);

$\gamma_{\text{біт}} = E_{\text{біт}}/N_0$ – відношення енергії біта $E_{\text{біт}}$ до спектральної щільності потужності шуму N_0;

$Q(x)$ – функція, яка використовується для визначення площі під частиною гаусівської функції щільності розподілу ймовірностей.

Ймовірність помилки на біт для КГ приймання сигналів з DBPSK розраховується за наступним аналітичним виразом [9]:

$$p_{\text{біт}} = 2\mathrm{Q}\left(\sqrt{2\gamma_{\text{біт}}}\right)\cdot\left(1-\mathrm{Q}\left(\sqrt{2\gamma_{\text{біт}}}\right)\right). \tag{2}$$

Ймовірність помилки на біт при некогерентній (НКГ) DBPSK визначається за формулою [9]:

$$p_{\text{біт}} = 0{,}5\cdot \mathrm{e}^{-\gamma_{\text{біт}}}. \tag{3}$$

Результати розрахунків за формулами (1)–(3) наведено на рис. 1, з яких видно, що найменша ймовірність помилки забезпечується при використанні сигналів з фазовою або відноснофазовою (при КГ чи НКГ прийомі) маніпуляцією. Перехід від BPSK до DBPSK призводить до погіршення достовірності, яке стає все суттєвішим зі зменшенням відношення сигнал-шум (ВСШ) (при $p_{\text{біт}} = 10^{-1}$ енергетичний програш становить 2 дБ (рис. 1)). Використання когерентної DBPSK порівняно з некогерентною дає незначний виграш.

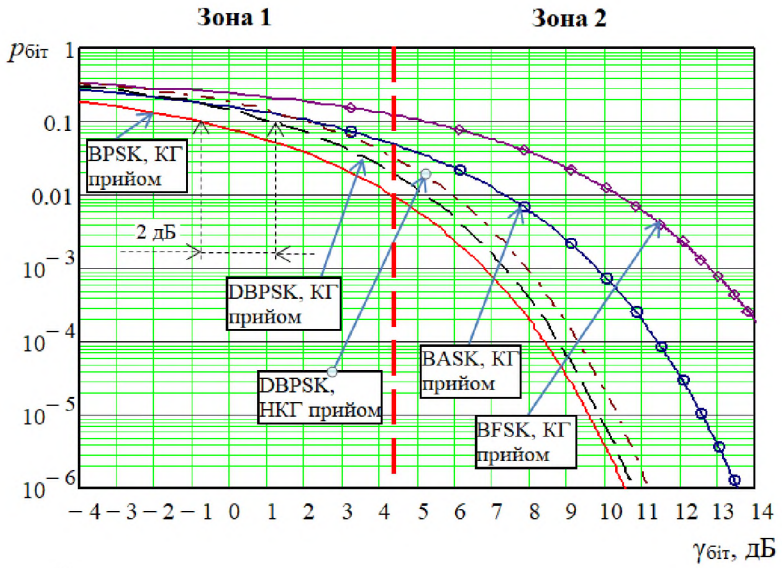

Рис. 1. Ймовірність помилки на біт для сигналів з BPSK, BFSK, BASK, DBPSK при когерентному та некогерентному прийомі

З метою здійснення аналізу завадостійкості сигналів з різними видами фазової маніпуляції в релеєвському каналі було проведено розрахунки за аналітичними виразами, які наведено в [9; 10].

Ймовірність помилки на біт в релеєвському каналі для сигналів з BPSK визначається як:

$$p_{біт} = \frac{1}{2}\left(1 - \sqrt{\frac{\gamma_b}{\gamma_b + 1}}\right). \tag{4}$$

Ймовірність помилки на біт в релеєвському каналі при КГ прийомі сигналів з DBPSK обчислюється за наступним аналітичним виразом:

$$p_{біт} = \frac{1}{2}\cdot\left(1 - \frac{4}{\pi}\sqrt{\frac{\gamma_b}{\gamma_b + 1}}\cdot \arctan\sqrt{\frac{\gamma_b}{\gamma_b + 1}}\right). \tag{5}$$

Ймовірність помилки на біт в релеєвському каналі при НКГ прийомі сигналів з DBPSK розраховується за формулою:

$$p_{біт} = \frac{1}{2\gamma_b + 2}. \tag{6}$$

Результати розрахунків за формулами (4)–(6) наведено на рис. 2. З них видно, що перехід від BPSK до DBPSK призводить до погіршення завадостійкості на 2–2,5 дБ. Втрати при переході від КГ DBPSK до НКГ DBPSK є незначними.

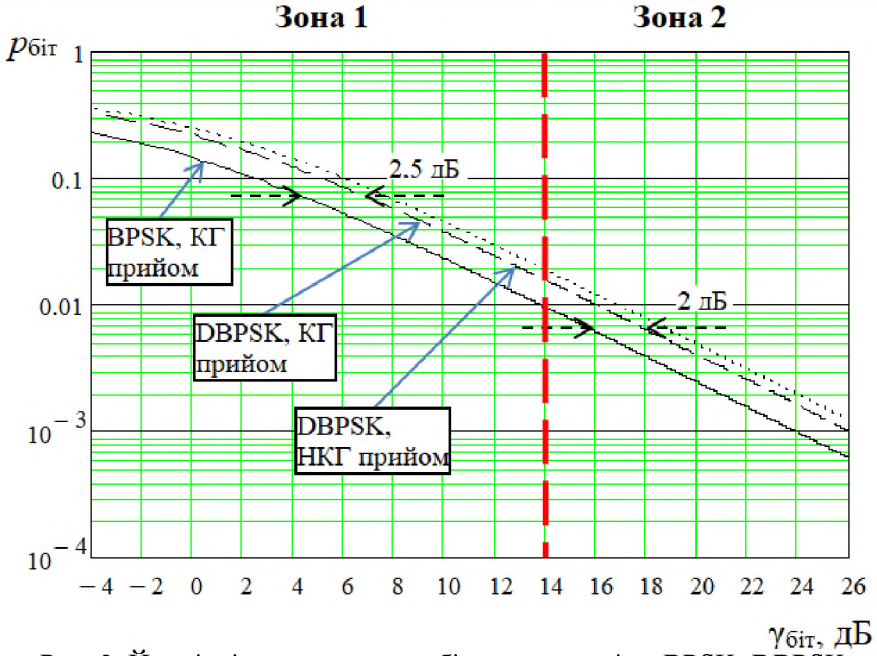

Рис. 2. Ймовірність помилки на біт для сигналів з BPSK, DBPSK при КГ та НКГ прийомі в релеєвському каналі

Оскільки наведені вище технології у більшості випадків використовуються в цивільній сфері, то вибір сигналів з DBPSK маніпуляцією є цілком обґрунтованим, оскільки забезпечує достатній рівень достовірності прийому в каналах, де потужність корисного сигналу значно перевищує потужність шуму (рис. 1 та рис. 2, зона 2).

Сигнали з BPSK дозволяють отримати більшу достовірність прийому при однакових значеннях ВСШ, однак потребують складних схем оцінки фази, які б забезпечили когерентний прийом та мінімізували можливість виникнення явища зворотної роботи [9]. При односторонній радіопередачі в системах спеціального призначення необхідно забезпечити максимально можливу достовірність прийому повідомлень в складній завадовій обстановці (рис. 1 та рис. 2, зона 1), що може бути зумовлена активним впливом засобів РЕБ противника.

Тому одним зі шляхів, що дозволить досягти підвищення достовірності передачі інформації в таких системах, є використання сигналів з BPSK та розв'язання завдань з вдосконалення існуючих схем оцінки фази прийнятого сигналу.

Серед відомих способів підвищення достовірності прийому повідомлень ефективним є завадостійке кодування, але його використання в складній завадовій обстановці, що зумовлена активним впливом засобів РЕБ, є обмеженим, оскільки в таких умовах може призвести до збільшення кількості помилок на етапі декодування (ефект розмноження помилок) [11]. У цьому випадку доцільно використовувати мажоритарний принцип кодування, який дозволяє уникати ефекту розмноження помилок.

Мажоритарний принцип полягає в тому, що в канал посилається непарна кількість разів одного повідомлення, а на приймальній стороні відбувається порівняння між собою однойменних кодових комбінацій (або однойменних двійкових розрядів). На прийомі обирається та кодова комбінація (або біт), яка була прийнята більшу кількість разів [12].

Ймовірність помилкового прийому двійкового символу повідомлення при використанні мажоритарного кодування (порівняння однойменних двійкових розрядів повідомлення, яке повторюється) можна визначити за виразом [12]:

$$p_{\text{біт маж}} = \sum_{i=\frac{c+1}{2}}^{c} C_c^i \cdot p_{\text{біт0}}^i \cdot \left(1 - p_{\text{біт0}}\right)^{c-i}, \qquad (7)$$

де c – кількість повторів передачі повідомлення або біта;

$p_{\text{біт0}}$ – бітова помилка без використання надлишкового кодування.

Результати розрахунків за формулою (7) для різної міри надлишковості наведено на рис. 3.

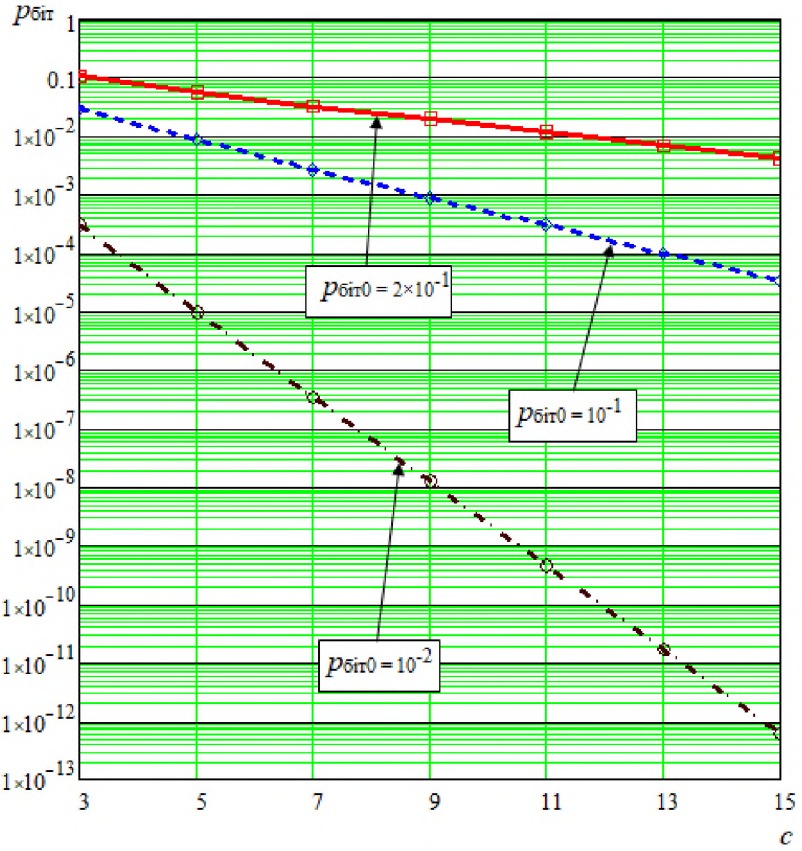

Рис. 3. Залежність $p_{\text{біт}}$ від кратності мажоритарного кодування

Вони свідчать про те, що використання такого способу завадостійкого кодування призводить до підвищення достовірності прийому повідомлень навіть в критичній завадовій обстановці, коли значення бітової помилки в каналі без застосування коригуючих кодів $p_{\text{біт0}} = [2\times10^{-1}; 10^{-1}; 10^{-2}]$.

Недоліком мажоритарного кодування є надлишковість інформації, яка зростає пропорційно кількості повторень одного і того ж повідомлення (біта), тому при його використанні необхідно враховувати часові обмеження на передачу повідомлень.

Варто зазначити, що для систем телеметрії, моніторингу віддалених об'єктів, систем управління БпЛА та інших систем спеціального призначення, крім підвищення достовірності прийому інформації, особливо важливим завданням є забезпечення інформаційної скритності передачі повідомлень. Одним із підходів, що дозволяє розв'язувати такі завдання, є застосування комбінованого випадкового кодування (КВК) [13].

Метод КВК, який запропонований в [13], передбачає використання поєднання завадостійкого кодування і псевдовипадкової зміни ансамблю кодових комбінацій – стохастичного кодування інформації. При цьому висока достовірність передачі повідомлень забезпечується за рахунок завадостійкого кодування, а інформаційна скритність і захищеність від несанкціонованого доступу – за рахунок кодування, що відноситься до некриптографічних методів захисту інформації. При КВК забезпечується теоретико-інформаційний рівень захисту інформації, який визначається рівнем невизначеності вибору ансамблю кодових комбінацій, що відповідають переданому повідомленню, для зловмисника, який здійснює радіоперехоплення [13].

Схема перетворення повідомлень методом КВК наведена на рис. 4 [13].

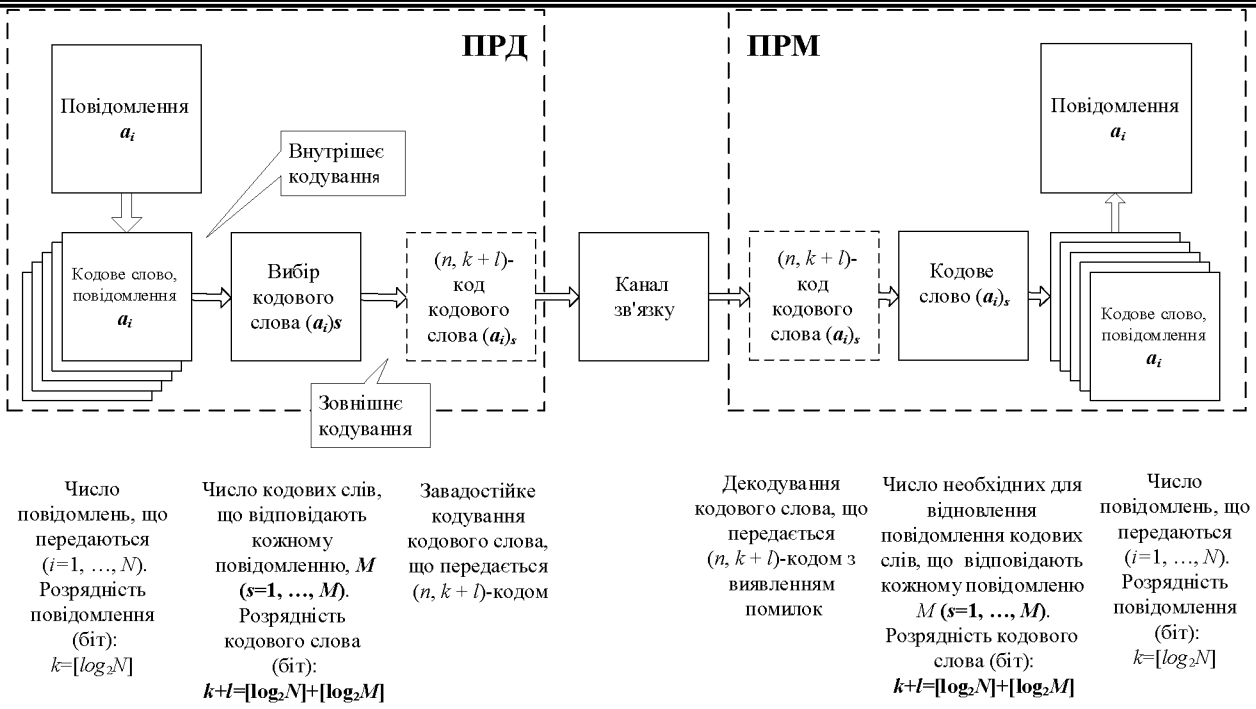

Рис. 4. Схема перетворення повідомлень при їх передачі методом КВК

В цій схемі стохастичне кодування є внутрішнім кодуванням, а завадостійке кодування – зовнішнім. Відповідно, формування кодового слова a_i, $i = 1, \ldots, N$ і його відновлення при прийомі здійснюється в два етапи.

Першим етапом є стохастичне кодування. На цьому етапі, з використанням кодової книги, формується M кодових слів $(a_i)_s$ $s = 1, \ldots, M$, що відповідають повідомленню a_i, і з них за допомогою генератора псевдовипадкових послідовностей (ПВП) вибирається деяке s-те кодове слово. Розрядність вихідного повідомлення a_i відповідає $k = [\log_2 N]$, де $[\cdot]$ означає округлення до найближчого цілого в сторону збільшення, а розрядність кодового слова, що передається $(a_i)_s$, складає $k+l$, де $l = [\log_2 M]$.

Другим етапом формування кодового слова є завадостійке кодування. На цьому етапі здійснюється канальне кодування кодового слова, вибраного з кодової книги, блочним коригуючим $(n, k + l)$-кодом.

При прийомі повідомлення на першому етапі проводиться декодування прийнятого блочного коду з виправленням помилок і виділення кодового слова $(a_i)_s$, що передавалось. На другому етапі в кодовій книзі вибирається повідомлення a_i, що відповідає виділеному при декодування кодовому слову. Для цього кодові книги в пунктах прийому і передачі повинні бути ідентичними, а для порушника структура кодової книги має бути невідомою.

Підвищення інформаційної скритності при стохастичному кодуванні досягається завдяки використанню книги, в якій кожному повідомленню джерела відповідає набір кодових слів, з яких кодове слово для передачі радіоканалом вибирається випадковим чином, що ускладнює несанкціонований доступ до інформації у випадку радіоперехоплення. Принцип стохастичного кодування на основі кодової книги наведено на рис. 5 [13]. Дискретні повідомлення довжини k, що формуються джерелом, утворюють ансамбль повідомлень a_i, $i = 1, \ldots, N$. Загальна кількість повідомлень (об'єм ансамблю) $N = 2^k$. Кожному повідомленню ставиться у відповідність $M = 2^l$ кодових слів, які зберігаються у визначеному рядку кодової книги і випадковим чином обираються для передавання радіоканалом. Загальне число слів кодової книги $K = MN = 2^{k+l}$. Тоді стохастичний код V може бути представлений як лінійний код, що утворений множиною двійкових послідовностей V_i, $i = 1, \ldots, N$, таких, що $V = \bigcup_{i=1}^{N} V_i$, $V_i \cap V_j = \varnothing$, $i \neq j$. Кожному k-розрядному повідомленню a_i однозначно відповідає одна з підмножин V_i, яка містить M $(k+l)$-розрядних кодових слів $(a_i)_s$, $s = 1, \ldots, M$, одне з яких випадково та рівноймовірно вибирається для передачі радіоканалом. Надалі, в процесі зовнішнього завадостійкого

кодування вибране для передачі кодове слово кодується блоковим коригуючим кодом, при цьому загальне число розрядів кодових слів дорівнює $n = k+l+r$.

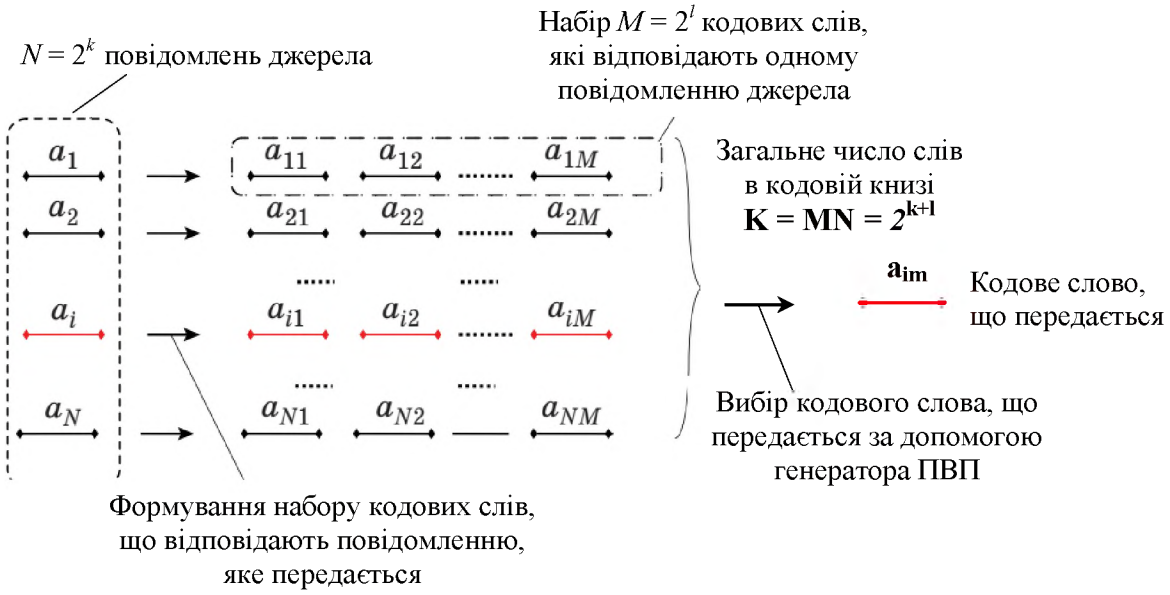

Рис. 5. Принцип стохастичного кодування з використанням кодової книги

Результати досліджень, які отримані в [13], свідчать про те, що застосування стохастичного кодування в поєднанні з завадостійким кодуванням призводить до незначного збільшення ймовірності помилки на біт, але зумовлює зниження швидкості передачі повідомлень в $(n-r)/(n-r-l)$ разів, де n – кількість розрядів повідомлення, r – число перевірочних символів, l – кількість символів стохастичного коду, проте при цьому підвищується інформаційна скритність передачі повідомлень.

В якості кількісної міри інформаційної скритності при стохастичному кодуванні в [13] запропоновано використовувати узагальнений показник рівня інформаційної доступності, який визначається за наступним аналітичним виразом [13]:

$$\delta = \frac{\log_2(Q+1)}{\log_2(M+1)}, \tag{8}$$

де $Q \le 2^t - 1$ – число кодових комбінацій, що правильно виділені зловмисником, $0 \le t \ge l$.

Зрозуміло, що значення Q буде залежати від властивостей конкретних кодів.

В ході проведених досліджень було проаналізовано відомі генератори ПВП, які дозволяють отримувати кодові послідовності для формування кодової книги стохастичного коду.

Тестування генераторів ПВП проводилось за допомогою програми NIST Statistical Test Suite 2.1.2, де використовується пакет статистичних тестів. До його складу входять 188 тестів, метою яких є визначення міри випадковості двійкових послідовностей, згенерованих або апаратними, або програмними генераторами [14].

Досліджувалися стандартизовані генератори двійкових послідовностей, а саме: Linear Congruential Generator (LCG), Quadratic Congruential Generator-I (QCG-I), Quadratic Congruential Generator-II (QCG-II), Cubic Congruential Generator (CCG), Exclusive OR Generator (XORG), Modular Exponentiation Generator (MODEXPG), Blum-Blum-Shub Generator (BBSG), Micali-Schnorr Generator (MSG) та Secure Hash Generator (G-SHA1).

Вихідні дані для здійснення обчислень: довжина послідовностей для тестування $\boldsymbol{n}$ = 387840 біт (мінімально-необхідна довжина послідовності для проведення Universal Statistical тесту); загальна кількість послідовностей $\boldsymbol{m}$ = 1000; рівень значимості $\boldsymbol{\alpha}$ = 0,01; кількість тестів $\boldsymbol{q}$ = 188. Результати обчислень наведено на рис. 6–8.

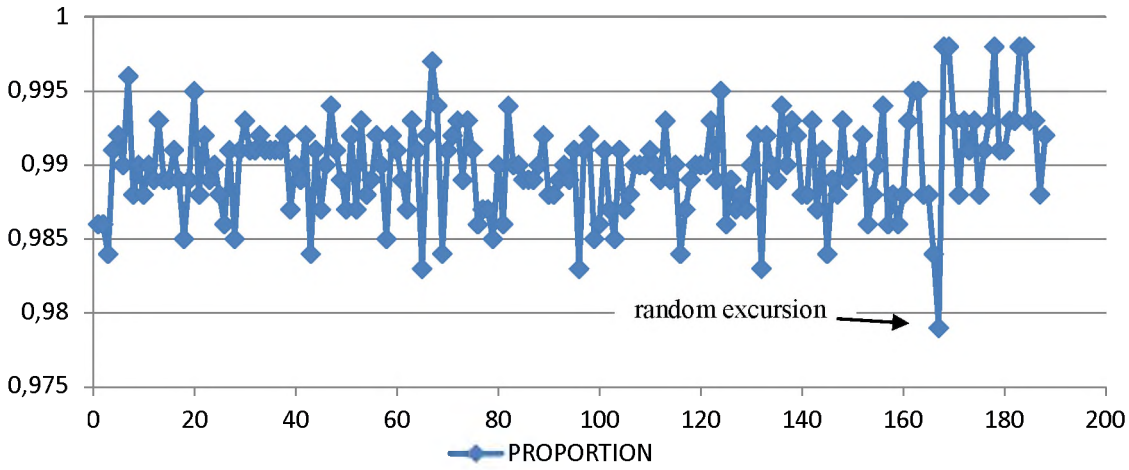

Рис. 6. Micali-Schnorr Generator

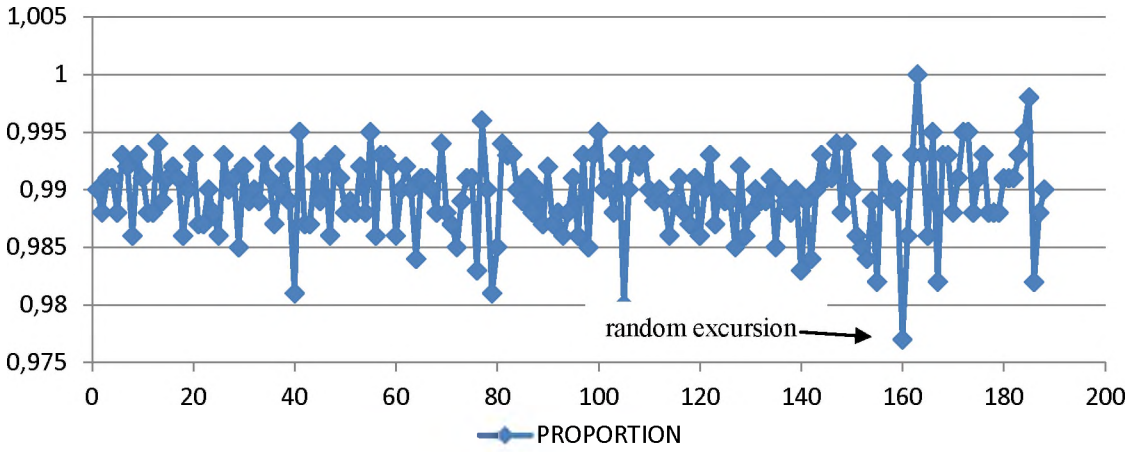

Рис. 7. Linear-Congruential Generator

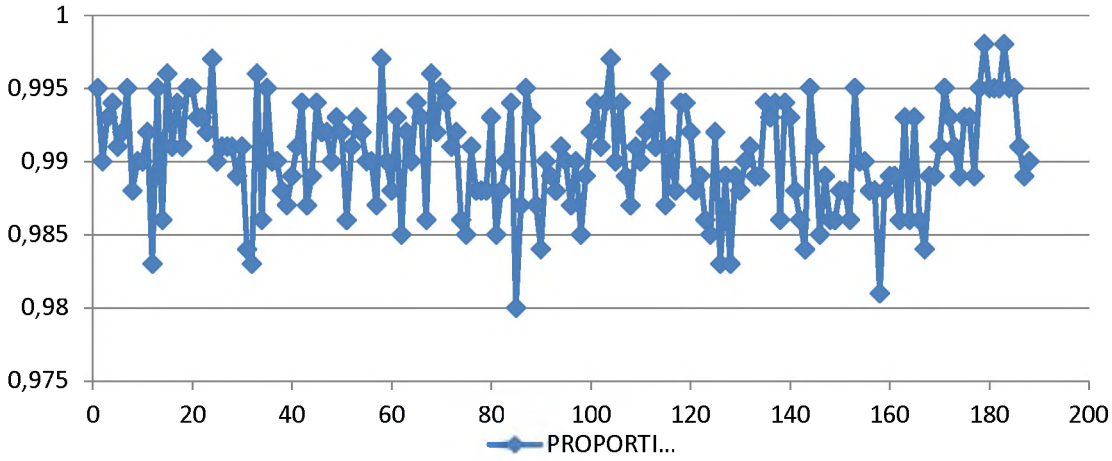

Рис. 8. Blum-Blum-Shub Generator

Відповідно до критеріїв, які визначені в [14], двійкові послідовності, що були згенеровані генераторами LC, BBS та MS, можна вважати такими, що задовольняють сучасним вимогам до ПВП, оскільки більше ніж 98 % із них пройшли всі тести, окрім random excursion (variant) тесту, який пройшли більше ніж 97 % послідовностей.

Висновки. Таким чином, можливими шляхами підвищення достовірності передачі повідомлень односторонніми радіоканалами в сучасних ІКС є вдосконалення існуючих схем оцінки фази прийнятого сигналу та застосування мажоритарного принципу кодування. Перше дозволить використовувати BPSK маніпуляцію, яка порівняно з DBPSK маніпуляцією має

енергетичний виграш до 2 дБ. Виграш по достовірності прийому повідомлень за рахунок мажоритарного кодування залежатиме від обмежень на час передачі інформації.

Крім того, для одночасного підвищення достовірності прийому повідомлень та забезпечення скритності передачі інформації доцільним є застосування принципу КВК. Комбіноване випадкове кодування може здійснюватися як в поєднанні з мажоритарним кодуванням, так і з іншим коригуючим кодом.

Отримані результати досліджень свідчать про те, що для формування кодової книги доцільно використовувати BBS генератори ПВП, оскільки згенеровані ними двійкові послідовності проходять всі тести, що визначені в [14], з найкращими показниками.

У подальших дослідженнях планується розглянути можливість забезпечення криптостійкості кодових конструкцій.

ЛІТЕРАТУРА

1. A Sigfox Energy Consumption Model. Carles Gomez, Juan Carlos Veras, Rafael Vidal, Lluís Casals // Journal Sensors. 2019. Vol. 19. P. 681. URL: https://www.researchgate.net/publication/330947889_A_Sigfox_Energy_Consumption_Model/fulltext/5c5ced9d45851582c3d5a09e/A-Sigfox-Energy-Consumption-Model.pdf.

2. Abbas R., Al-Sherbaz A., Bennecer A., Picton P. A New channel selection algorithm for the Weightless-N Frequency Hopping with lower collision probability. 8th International Network of the Future (NoF) Conference Proceedings. London: IEEE (In Press). 2017. URL: http://nectar.northampton.ac.uk/id/eprint/9777.

3. Ашимов Н. М., Кравцов А. В., Фомин В. В. Надежность управления радиолинии при повторении команд управления на одной частоте. *Спецтехника и связь*. 2009. № 3. С. 38–41.

4. Фрейман В. И. Разработка и исследование моделей систем управления, использующих структурные методы обеспечения помехоустойчивости. *Современные наукоемкие технологии*. 2016. № 8, Часть 1. С. 86–90.

5. Мальцев Г. Н. Чернявский Е. В. Кодирование сообщений в системах радиоуправления без обратного информационного канала. *Информационно-управляющие системы.* 2011. № 4. С. 60.

6. B. Buurman, J. Kamruzzaman, G. Karmakar and S. Islam. *Low-Power Wide-Area Networks: Design Goals, Architecture, Suitability to Use Cases and Research Challenges*. in *IEEE Access.* Vol. 8. P. 17179–17220. 2020. **DOI:** 10.1109/ACCESS.2020.2968057.

7. Bembe, M., Abu-Mahfouz, A., Masonta, M. *A* Survey on low-power wide area networks for IoT applications. *Telecommun Syst* 71, 249–274 (2019). URL: https://doi.org/10.1007/s11235-019-00557-9.

8. Теорія електрозв'язку: підруч. / О. В. Корнєйко, О. В. Кувшинов, О. П. Лежнюк, С. П. Лівенцев; за ред С. П. Лівенцева. Т. 2. Київ: НВП Славутич-Дельфін, 2006. 292 с.

9. Окунев Ю. Б. Цифровая передача информации фазоманипулированными сигналами. Москва: Радио и связь, 1991. 296 с.

10. Лошаков В. А., Лихограй В. Г., Хуссам Дхеа Ал-Джанаби, Таха Насиф Нух. Адаптивная пространственная обработка сигналов в системах LTE С MIMO. *Вісник Національного технічного університету «ХПІ»*. Серія: Нові рішення в сучасних технологіях. 2013. № 11. С. 101–108. http://nbuv.gov.ua/UJRN/vcpinrct_2013_11_17.

11. Золотарев В. В., Овечкин Г. В. Помехоустойчивое кодирование. Методы и алгоритмы: справочник / под. ред. Ю. Б. Зубарева. Москва: Горячая линия-Телеком, 2004. 126 с.

12. Спилкер Дж. Цифровая спутниковая связь / пер. с англ.; под ред. В. В. Маркова. Москва: Связь, 1979. 592 с.

13. Мальцев Г. Н. Помехоустойчивость и скрытность передачи информации по радиоканалам на основе комбинированного случайного кодирования. *Информационно-управляющие системы*, (2), 82-89. https://doi.org/10.15217/issn1684-8853.2015.2.82.

14. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo: A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, Version STS-2.1, NIST Special Publication 800-22rev1a, April, 2010. http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf