https://doi.org/10.31891/2219-9365-2025-83-37
УДК 004.056

КОРЧИНСЬКИЙ Володимир
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-3972-0585
e-mail: vkadkorchin@ukr.net
ГАВЕЛЬ Сергій
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0002-0484-5620
e-mail: arkominer@gmail.com
СЄДОВ Костянтин
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0001-6071-2179
e-mail: sedovmail2@gmail.com
СЕВАСТЄЄВ Євген
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-1165-1119
e-mail: seva.odessa@gmail.com
ЛІМАРЬ Ігор
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0002-8972-9935
e-mail: quantum.biology@outlook.com

МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ ПРИ ФОРМУВАННІ ТАЙМЕРНИХ СИГНАЛІВ

У статті розглядається метод захисту інформації на основі таймерних сигнальних конструкцій, імпульси яких формуються з використанням системи залишкових класів. Використання таймерних сигналів ускладнює структуру комбінацій, що підвищує їх структурну прихованість. Система залишкових класів дозволяє поділити цілісну інформацію на множину незалежних залишків за заздалегідь обраними взаємно простими модулями, що відкриває нові можливості для побудови сигнальних конструкцій, які можна використовувати для підвищення завадостійкості передавання даних.

Особливу увагу приділено використанню системи залишкових класів у поєднанні з надлишковими модулями для формування коригувальних кодів, які забезпечують виявлення та виправлення помилок, спричинених завадами, навмисними впливами або технічними збоями. У роботі детально проаналізовано практичні алгоритми застосування системи залишкових класів для формування таймерних сигнальних конструкцій, в яких інформація позначається у виді імпульсів із визначеним часовим інтервалом. При цьому, сигнальні конструкції набувають властивості завадостійкого коду та структурної прихованості, що в певній мірі забезпечують захист від несанкціонованого доступу за рахунок невизначеності структури сигналу. Властивості структурної прихованості ускладнює процес визначення структури сигналу у випадку перехоплення повідомлення засобами радіоелектронної розвідки противника. Наведено математичні приклади формування залишкових векторів та формування таймерних сигнальних конструкцій. Отримані результати свідчать про доцільність використання системи залишкових класів як одного з перспективних напрямів у проєктуванні захищених комунікаційних та інформаційно-керуючих систем, зокрема, у військовій сфері, критичній інфраструктурі та пристроях реального часу.

Ключові слова: захист інформації; система залишкових класів; коригувальні коди; таймерні сигнали; структурна прихованість, виявлення і корекція помилок; радіоелектронна боротьба.

KORCHYNSKYI Volodymyr, HAVEL Serhii,
SIEDOV Kostiantyn, SEVASTIEIEV Ievhen, LIMAR Ihor
State University of Intellectual Technologies and Communications

INFORMATION PROTECTION METHOD BASED ON THE SYSTEM OF RESIDUAL CLASSES IN THE FORMATION OF TIMER SIGNALS

The article considers information protection method based on timer signal constructions, the impulses of which are formed using the system of residual classes. The use of timer signals allows to complicate the structure of combinations, which increases their structural secrecy. The system of residual classes allows to divide integral information into a set of independent residues according to pre-selected mutually simple modules, which opens the new possibilities for building signal constructions that can be used to increase the noise immunity of data transmission.

Particular attention is given to the use of the residual class system combined with redundant modules for the formation of correction codes, which provide detection and correction of errors caused by interference, intentional influences or technical failures. The paper analyses in detail practical algorithms for applying the residual class system to form timer signal constructions, in which information is indicated in the form of pulses with a certain time interval. At the same time, the signal constructions acquire the properties of noise immunity code and structural secrecy, which to certain extent provide protection against unauthorized access due to the uncertainty of the signal structure. The properties of structural secrecy complicate the process of determining the signal structure in the event of interception of message by enemy electronic intelligence. Mathematical examples of the formation of residual vectors and the formation of timer signal constructions are given. The obtained results indicate the feasibility of using the residual

class system as one of the promising areas in the design of secure communication and information and control systems, particularly in the military sector, the Internet of Things, critical infrastructure, and real-time devices.

Keywords: information protection; system of residual classes; correction codes; timer signals; structural secrecy, error detection and correction; radio electronic warfare.

Стаття надійшла до редакції / Received 17.07.2025
Прийнята до друку / Accepted 14.08.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ТА ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасних умовах ведення інформаційної боротьби дедалі актуальнішою стає проблема забезпечення надійної передачі даних. Особливої гостроти це питання набуває у військових інформаційно-керуючих системах, які функціонують в умовах радіоелектронної боротьби (РЕБ) противника [1]. Традиційні методи захисту, що базуються лише на криптографії або класичних завадостійких кодах, часто не забезпечують необхідного рівня стійкості у складних та динамічних радіоелектронних умовах [1, 2]. Тому, актуальним напрямом є розробка складних сигнальних конструкцій, які поєднують в собі структурну та енергетичну прихованість, а також забезпечують можливість виявлення та корекції спотворених даних.

Одним із перспективних підходів у цьому напрямі є використання системи залишкових класів (СЗК), що базується на китайській теоремі про залишки [2]. Представлення інформації у вигляді набору залишків за взаємно простими модулями дозволяє забезпечити розподіл інформації між незалежними каналами передачі, ускладнити структуру сигнальних конструкцій та підвищити їх структурну прихованість для забезпечення стійкості до цілеспрямованих атак. При цьому, впровадження надлишкових модулів при формуванні таймерних сигнальних конструкцій (ТСК) дає змогу реалізовувати коригувальні коди, які виявляють і виправляють помилки.

Значна кількість наукових праць присвячена питанням застосування СЗК у цифровій обробці сигналів, криптографії та системах числення [2, 3]. Зокрема, дослідження в роботі [2] свідчать про ефективність залишкового представлення в обчислювальних системах реального часу. У роботах [3, 4] описано методи виявлення та локалізації помилок із використанням надлишкових модулів, а в [4] наведено приклади застосування СЗК у схемах цифрової модуляції. Проте, питання використання СЗК саме у ТСК в умовах завад, а також їхній потенціал як носіїв структурно прихованої інформації, залишаються недостатньо дослідженими.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою даної статті є розробка та обґрунтування методів захисту інформації з використанням СЗК для формування ТСК. У роботі пропонується математична модель системи, демонструються принципи кодування ТСК на основі СЗК, а також аналізується рівень структурної прихованості отриманих комбінацій.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Питання підвищення захищеності інформації в умовах радіоелектронних впливів є предметом активного дослідження впродовж останніх десятиліть. Основну увагу науковці приділяють методам завадостійкого кодування, технологіям розширення спектра сигналів [], шифрування, а також алгоритмам синтезу складної структури сигнальних конструкцій.

У роботах [2, 3] докладно розглядаються методи застосування СЗК у задачах цифрової обробки сигналів і чисельних обчислень. Зокрема, автори [2] демонструють, що залишкове представлення чисел дозволяє забезпечити незалежність каналів передачі інформації та паралелізм операцій в системах зв'язку. Дослідження [3] присвячено методам виявлення та виправлення помилок у СЗК шляхом введення надлишкових модулів – такий підхід дозволяє реалізовувати ефективні коригувальні коди з малою та великою кратністю помилок.

У роботі [4] розглядаються особливості застосування СЗК у криптографічних системах, зокрема для формування багатоканальних ключових послідовностей та реалізації структур із високим ступенем заплутаності. Автори показують, що така архітектура підвищує криптостійкість та ускладнює атакуючим зловмисникам задачу відновлення вихідної інформації.

Окремий напрям досліджень пов'язаний із застосуванням СЗК у телекомунікаційних системах у вигляді таймерних сигналів [5, 6]. Ці роботи демонструють можливість кодування даних не значеннями сигналів, а часовими інтервалами між подіями, що значно ускладнює їхню інтерпретацію для сторонніх спостерігачів, особливо в умовах дії засобів РЕБ. Разом з тим, дослідження показують, що поєднання СЗК з таймерними сигналами дозволяє досягти не лише структурної прихованості, а й забезпечити енергетичну прихованість при розширенні їх спектра [7, 8], що є критично важливим для військових та спеціальних застосувань.

Попри наявні здобутки, комплексного підходу до використання СЗК для захищеної передачі інформації в умовах навмисного радіоелектронного впливу досі бракує. Недостатньо вивченими залишаються питання формування залишкових кодів для таймерних сигналів, їхньої синхронізації, стійкості до порушення часового ритму, а також ефективності відновлення інформації за умов спотворень.

Отже, подальше дослідження інтеграції СЗК з таймерними сигналами є актуальним і необхідним кроком для підвищення завадостійкості та структурної прихованості сигнальних конструкцій.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Розглянемо можливості використання СЗК для формування імпульсів ТСК. Відзначимо, що СЗК – це особливий тип непозиційної системи числення, в якій будь-яке ціле додатне число представляється у вигляді набору найменших додатних залишків (відрахувань) від ділення цього числа на фіксований набір взаємно простих чисел $p_1, p_2,\ldots, p_l$, які називаються основами або модулями системи [2, 3].

Формально, якщо задано набір l взаємно простих модулів $\{ p_1, p_2,\ldots, p_l\}$, то для будь-якого цілого числа A, яке не перевищує добуток усіх модулів:

$$A < P = p_1 \times p_2 \times \ldots, p_l, \tag{1}$$

його представлення в СЗК задається як набір:

$$(A_1, A_2, \ldots, A_l), \tag{2}$$

де

$$A_i = A \bmod p_i,\ i=1, 2, \ldots, l. \tag{3}$$

Це представлення є однозначним у межах проміжку [0; P) за умови, що всі модулі $\{ p_1, p_2,\ldots, p_l\}$ є попарно взаємно простими. СЗК має низку корисних властивостей:

1) операції додавання, множення та віднімання можуть виконуватися незалежно над кожним із залишків:

$$A \pm B \bmod P \longleftrightarrow (A_1 \pm B_1 \bmod p_1, \ldots, A_l \pm B_l \bmod p_l) \tag{4}$$

2) можливість паралельної обробки даних у кожному каналі;

3) стійкість до помилок, особливо при введенні одного або кількох надлишкових модулів, що дозволяє виявляти й виправляти похибки.

Відновлення числа з його залишкового представлення здійснюється за допомогою китайської теореми про залишки, згідно з якою існує єдине число A∈[0; P), що одночасно задовольняє систему конгруенцій:

$$\begin{cases} A \equiv A_1 \bmod p_1 \\ A \equiv A_2 \bmod p_2 \\ \vdots \\ A \equiv A_l \bmod p_l \end{cases} \tag{5}$$

Методи, засновані на СЗК, можуть бути ефективно адаптовані для побудови зашумлених або малопомітних сигнальних конструкцій, де передані значення кодуються не через безпосереднє передавання числа, а у вигляді послідовностей подій (наприклад, таймерних інтервалів), які відповідають залишкам. Це значно ускладнює перехоплення або підробку сигналу в умовах дії засобів радіоелектронної боротьби.

Отже, система залишкових класів не лише забезпечує математичну основу для ефективного подання й обробки інформації, а й відкриває широкі можливості для формування прихованих, коригувальних і розподілених форм сигналів, що є перспективними для застосування в умовах завад та цілеспрямованих атак на канали зв’язку.

Основою для формування ТСК [9, 10] є базовий часовий елемент Δ, якій менше інтервалу Найквіста t_0. Кількість Δ на інтервалі t_0 позначимо як s, тобто:

$$s = \frac{t_0}{\Delta}. \tag{6}$$

Для формування ТСК обирається часовий інтервал T_c за допомогою інтервалів Найквіста t_0. Побудова ТСК відбувається за наступним алгоритмом:

1) тривалість позитивних та негативних імпульсів t_c повинна бути не менше t_0, тобто:

$$t_\text{c} \geq t_0 \quad ; \tag{7}$$

2) тривалість імпульсів визначають з урахуванням кількості Δ, тобто:

$$t_\text{c} = t_0 + \Delta k, \tag{8}$$

де $k = 0, 1, \ldots$;

3) обирається кількість значущих моментів модуляції (ЗММ) $i = 1, 2, \ldots, m$ в межах ТСК;

4) обирається часовий інтервал побудов ТСК:

$$T_\text{c} = t_0 \times m, \tag{9}$$

де m – кількість інтервалів Найквіста.

Характерним є те, що при побудові ТСК кількість ЗММ може бути фіксованим або обрано з різними значеннями. Загальна кількість комбінацій ТСК визначається по формулі:

$$N_\text{p} = [ns - i(s-1)]!/i!\,(ns - is)!. \tag{10}$$

Розглянемо можливість побудови ТСК за допомогою СЗК. В табл. 1 представлено кодові слова, що отримані з використанням модулей $P_1 = 2$, $P_2 = 3$, $P_3 = 7$. За допомогою цих модулів визначимо загальну кількість ТСК $N_{\text{с}}$ [1]:

$$N_{\text{тск}} = P_1 \times P_2 \times P_3 = 2 \times 3 \times 7 = 42.$$

Визначимо, що сформовані кодові слова визначають кількість інтервалів Δ, які призначені для формування тривалості імпульсів згідно (8). Наприклад, тривалість трьох імпульсів під номером №22 табл. 1 будуть розраховані за допомогою мінімальної суми кодових слів (0, 1, 1) наступним чином:

$$t_{\text{с1}} = t_0 + \Delta \times 0;$$
$$t_{\text{с2}} = t_0 + \Delta \times 1;$$
$$t_{\text{с3}} = t_0 + \Delta \times 1.$$

Розрахуємо тривалість імпульсів для максимальної суми кодових слів (1, 2, 6) під № 41, табл. 1:

$$t_{\text{с1}} = t_0 + \Delta \times 1;$$
$$t_{\text{с2}} = t_0 + \Delta \times 2;$$
$$t_{\text{с3}} = t_0 + \Delta \times 6.$$

Знайдемо інтервал побудови ТСК $T_{\text{с}}$ з урахуванням максимальної суми кодових слів (1, 2, 6) за умови, що $s = 4$, тоді: $T_{\text{с}}(1,2\,,6) = t_0 + \Delta + t_0 + 2\Delta + t_0 + 6\Delta = 4\Delta + \Delta + 4\Delta + 2\Delta + 4\Delta + 6\Delta = 21\Delta = 5t_0 + \Delta$. Отриманий інтервал $T_{\text{с}}(1,2\,,6)$ складається з $5t_0$ та однієї Δ.

Для ТСК з кодовими словами (1, 2, 5) отримаємо: $T_{\text{с}}(1,2\,,5) = 20\Delta = 5t_0$. Для мінімальної суми кодових слів (0, 1, 1) отримуємо $T_{\text{с}}(0,1\,,1) = 14\Delta = 3t_0 + 2\Delta$. Бачимо, що часовий інтервал сформованих ТСК є нерівномірним. Для вирішення цієї проблеми та виконання умови (7) пропонується наступні три варіанти.

Перший варіант. До тривалості комбінації, яка складається з імпульсів максимальної суми кодових слів $T_{\text{с}}(1,2\,,6)$, потрібно додати додатковий захисний інтервал t_0, що забезпечить виконання умови (7). $T_{\text{сз1}}(1,2\,,6) = 5t_0 + \Delta + t_0 = 6t_0 + \Delta = 25\Delta$. Таким чином, отримуємо загальний часовий інтервал $T_{\text{сз1}} = 25\Delta$, призначений для формування всіх ТСК згідно табл. 1. Інтервал $T_{\text{сз}}$ складається з шести інтервалів Найквіста t_0 та однієї Δ, але умова (7) для всіх імпульсів ТСК виконується. При цьому є протиріччя, яке пов'язано з вибором цілого значення m кількості інтервалів Найквіста (9).

Другий варіант. Для отримання цілого значення m до $t_{\text{с3}} = t_0 + 6\Delta$ інтервалу $T_{\text{сз1}}(1{,}2{,}6)$ додати 3Δ, тобто: $T_{\text{сз2}}(1,2\,,6+3) = T_{\text{сз1}} + 3\Delta = 28\Delta = 7t_0$. Комбінація, що сформована на інтервалі $T_{\text{сз2}}(1,2\,,6+3)$ буде винятком, але в результаті отримуємо ціле значення m=7, що задовольняє умові (9).

Третій варіант. Реалізація цього варіанту передбачає виключення комбінації з кодовим словом (1, 2, 6) та додавання захисного інтервалу $t_0 = 4\Delta$ до комбінації, що формується за допомогою кодових слів (0, 2, 6), яка є другою за максимальною сумою. Це зменшить кількість комбінацій до $N_{\text{тск}}(2,3,7) = 41$ та забезпечить інтервал $T_{\text{сз3}}(0,2,6) = t_0 + t_0 + 2\Delta + t_0 + 6\Delta + t_0 = 6t_0 = 24\Delta$, тобто отримаємо ціле значення $m = 6$.

Таблиця 1

Кодові слова, що сформовані на основі модулів $P_1 = 2$, $P_2 = 3$, $P_3 = 7$

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
2	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
7	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0
№	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
2	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
7	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0

На рис. 1 надано приклад формування ТСК, що сформовані на основі кодових слів (0, 2, 6), (1, 1, 5) та (1, 2, 5). Бачимо, що всі імпульси $t_{\text{с1}}$, $t_{\text{с2}}$, $t_{\text{с3}}$ та $t_{\text{с4}}$ сигнальних конструкцій $X(0,2,6)$, $X(1,1,5)$ та $X(1,2,5)$ задовільнять умові (7), (8) і (9). Отримані ТСК мають кількість ЗММ $i = 3$.

Для порівняльного аналізу розглянемо позиційний завадостійкий код Хемінга з параметрами: $n = 7$ – загальна кількість біт; $k = 4$ –кількість інформаційних біт; $r = 3$ – кількість перевірочних біт; $d_0 = 3$ – мінімальна кодова відстань між дозволеними кодовими комбінаціями. Такий код має $N_{\text{доз рцк}} = 2^k = 16$ дозволених комбінацій та $N_{\text{ндоз рцк}} = 2^n - 2^k = 112$ недозволених комбінацій, кодову швидкість $\gamma_{\text{к}} = k/n = 4/7 = 0{,}57$ та виявляє до двох помилкових біт. Розглянуті таймерні сигнали мають $N_{\text{доз тск}}(2,3,7) = 41$

дозволену комбінацію, не потребують додаткових перевірочних біт та виявляють помилки. Загальна кількість ТСК $N_{\text{заг тск}} = 455 \gg N_{\text{заг рцк}} = 2^n = 128$ та формуються на меншому інтервалі часу, тобто $m = 6 < n = 7$.

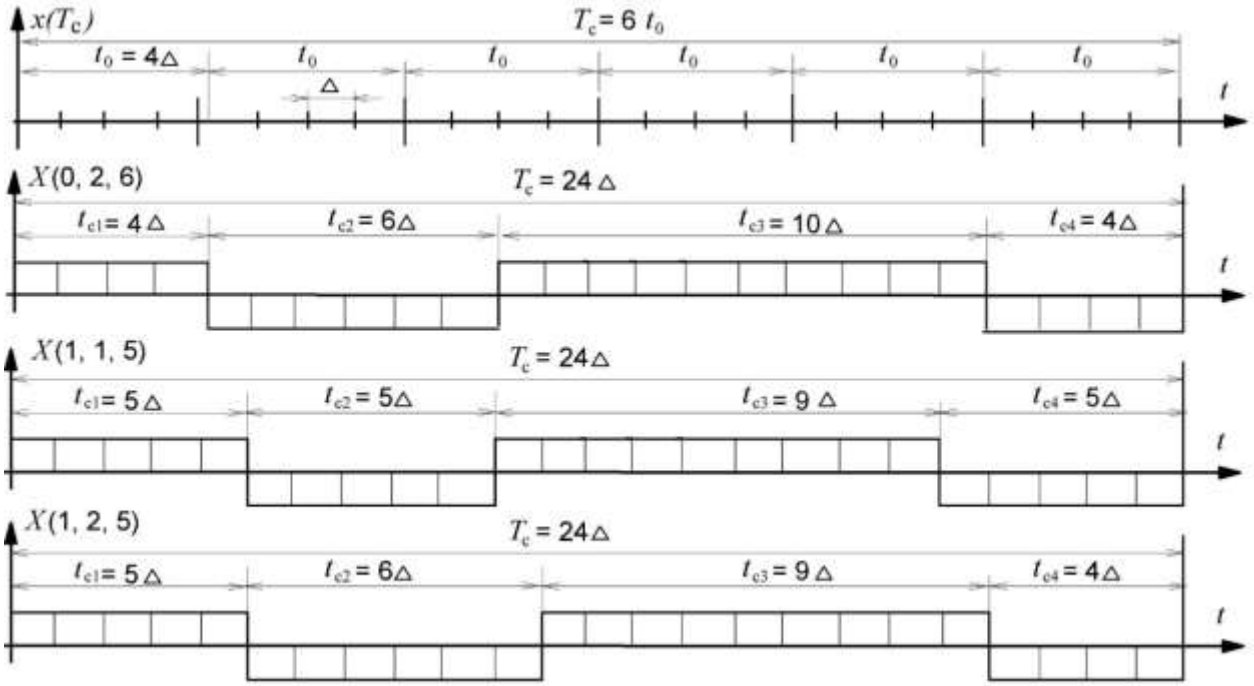

Рис. 1. Приклади формування ТСК за кодовими словами (0, 2, 6), (1, 1, 5) та (1, 2, 5)

Для оцінки захищеності сигнальних конструкцій визначимо структурну прихованість ТСК і розрядно-цифрового коду, яка визначається з урахуванням загального числа $N_{\text{р}}$ можливих комбінацій, які використовуються для передавання інформаційних символів:

$$S = \log_2 N_{\text{р}}. \tag{11}$$

Потенційну прихованість для ТСК оцінимо з урахуванням максимальної кількості комбінацій $S_{\text{п тск}} = \log_2 455 = 9$ дв. вим. Аналогічним чином оцінимо для коду Хемінга: $S_{\text{п рцк}} = \log_2 128 = 7$. Бачимо, що $S_{\text{п тск}} > S_{\text{п рцк}}$, що свідчить також про можливість таймерних сигналів забезпечувати функції захисту інформації від несанкціонованого доступу (НСД).

Більшу кількість комбінацій можна сформувати з використанням інших простих модулів, наприклад {3, 5, 7} або {2, 3, 5, 7, 11}. За допомогою цих модулів загальна кількість ТСК $N_{\text{тск}} = 3 \times 5 \times 7 = 105$ та $N_{\text{тск}} = 2 \times 3 \times 5 \times 7 \times 11 = 2310$.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШОГО РОЗВИТКУ У ДАНОМУ НАПРЯМІ

У роботі проаналізовано можливості використання СЗК для формування завадостійких ТСК для завдання захисту передаваних даних від НСД та помилок у каналі зв'язку. Таймерні сигнали, що сформовані на основі СЗК, набувають властивості завадостійкого коду, що дозволяє виявляти та виправляти спотворені комбінації. Показано, що ускладнення структури сигнальних конструкцій дозволяє забезпечувати певний рівень захисту даних від НСД, який оцінюється показником структурної прихованості.

Подальші дослідження передбачають розробку алгоритмів оптимального вибору модулів СЗК для синтезу ТСК під конкретні задачі захисту передаваних даних для систем зв'язку, що працюють в умовах РЕБ.

Література

1. Hordiichuk V., Snitsarenko P., Sarychev Y., Hrytsiuk V. War in cyberspace as a component of the Russian-Ukrainian hybrid war // Theoretical and applied aspects of the Russian-Ukrainian war: Hybrid aggression and national resilience / Koval M. (Ed.). – Kharkiv: Technology Center PC, 2023, pp. 183–208. – Режим доступу: DOI:10.15587/978-617-8360-00-9.

2. Захарченко, М. В. Модулі системи залишкових класів як інструмент інформаційної скритності / М.В.Захарченко, В.В. Гордійчук, О.Г. Данильчук // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем, 2018, № (16), 27–34. – Режим доступу: https://doi.org/10.46972/2076-1546.2019.16.03

3. Яцків В.В. Метод мережного кодування в системі залишкових класів / В.В. Яцків // Науковий вісник "Комп'ютерні системи та мережі" Національного університету «Львівська політехніка» Львів. – 2013. - № 773. – С.157-164. – Режим доступу: https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6704/26157-164.pdf

4. Menezes A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. – Boca Raton: CRC Press, 1997. – 810 p. – Режим доступу: https://doi.org/10.1201/9780429466335

5. Zaharchenko, M., Hadzhyiev, M., Salmanov, N. ., Golev, D., & Shvets, N. Інформаційні параметри кодових ансамблів, синтезованих на основі одного модуля // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2020, №3(7). С. 95-102. – Режим доступу: https://doi.org/10.28925/2663-4023.2020.7.95102.

6. Захарченко М.В., Гаджиев М.М., Салманов Н.С., Голев Д.В., Сєдов К.С. Ефективність кодування в системах залишкових класів. Наукові праці ОНАЗ ім. О.С. Попова, 2020, № 2. С. 25-30. – Режим доступу: DOI: https://doi.org/10.33243/2518-7139-2020-1-2-25-30

7. Захарченко М.В. Підвищення скритності передачі конфіденційної інформації на базі хаотичних сигналів та таймерних сигнальних конструкцій / М.В. Захарченко, В.В. Корчинський, Б.К. Радзімовський, В.И. Кільдішев // Східноєвропейський журнал передових технологій. 2012. – № 3/9 (57). – С. 45-49. https://doi.org/10.15587/1729-4061.2012.4168.

8. Корчинський В.В. Методи підвищення прихованості передавання інформації на основі розширення спектра таймерних сигналів / Корчинський В.В., Назаренко О.А., Степанов В.О., Аль-Файюми Халед // Науковий журнал «Інфокомунікаційні та комп'ютерні технології» – Київ, «Відкритий міжнародний університет розвитку людини «Україна». No 2 (02) 2022, - С.25-31. – Режим доступу: https://visn-icct.uu.edu.ua/index.php/icct/article/view/86.

9. Семенко А.І. Сучасні технології інфокомунікаційних та комп'ютерних мереж: монографія / А.І. Семенко, Ю.М. Бойко, О.М. Шпур, І. В. Стрелковська, В. В. Корчинський, Р. О. Яровий ; під заг. ред. А.І.Семенка. - Київ: Європейський університет, ФО-П Білецький Р.Г., 2024.- 557 с. ISBN 978-617-853-009-9. – Режим доступу: https://elar.khmnu.edu.ua/handle/123456789/17381.

10. Zakharchenko M., Korchynskii V., Kildishev V. Integrated methods of information security in telecommunication systems. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017), IEEE Xplore Digital Library. 11 – 15 September 2017. – V. 1. – pp. 78–81. URL: http://ieeexplore.ieee.org/document/8095366/.

References

1. Hordiichuk V., Snitsarenko P., Sarychev Y., Hrytsiuk V. War in cyberspace as a component of the Russian-Ukrainian hybrid war // Theoretical and applied aspects of the Russian-Ukrainian war: Hybrid aggression and national resilience / Koval M. (Ed.). – Kharkiv: Technology Center PC, 2023, pp. 183–208. – Режим доступу: DOI:10.15587/978-617-8360-00-9.

2. Zakharchenko, M. V. Moduli systemy zalyshkovykh klasiv yak instrument informatsiinoi skrytnosti / M.V.Zakharchenko, V.V. Hordiichuk, O.H. Danylchuk // Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system, 2018, № (16), 27–34. – Rezhym dostupu: https://doi.org/10.46972/2076-1546.2019.16.03

3. Yatskiv V.V. Metod merezhnoho koduvannia v systemi zalyshkovykh klasiv / V.V. Yatskiv // Naukovyi visnyk "Kompiuterni systemy ta merezhi" Natsionalnoho universytetu «Lvivska politekhnika» Lviv. – 2013. - № 773. – S.157-164. – Rezhym dostupu: https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6704/26157-164.pdf

4. Menezes A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. – Boca Raton: CRC Press, 1997. – 810 p. – Режим доступу: https://doi.org/10.1201/9780429466335

5. Zaharchenko, M., Hadzhyiev, M., Salmanov, N. ., Golev, D., & Shvets, N. Informatsiini parametry kodovykh ansambliv, syntezovanykh na osnovi odnoho modulia // Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika», 2020, №3(7). S. 95-102. – Rezhym dostupu: https://doi.org/10.28925/2663-4023.2020.7.95102.

6. Zakharchenko M.V., Hadzhyev M.M., Salmanov N.S., Holev D.V., Siedov K.S. Efektyvnist koduvannia v systemakh zalyshkovykh klasiv. Naukovi pratsi ONAZ im. O.S. Popova, 2020, № 2. S. 25-30. – Rezhym dostupu: DOI: https://doi.org/10.33243/2518-7139-2020-1-2-25-30

7. Zakharchenko M.V. Pidvyshchennia skrytnosti peredachi konfidentsiinoi informatsii na bazi khaotychnykh syhnaliv ta taimernykh syhnalnykh konstruktsii / M.V. Zakharchenko, V.V. Korchynskyi, B.K. Radzimovskyi, V.Y. Kildishev // Skhidnoievropeiskyi zhurnal peredovykh tekhnolohii. 2012. – № 3/9 (57). – S. 45-49. https://doi.org/10.15587/1729-4061.2012.4168.

8. Korchynskyi V.V. Metody pidvyshchennia prykhovanosti peredavannia informatsii na osnovi rozshyrennia spektra taimernykh syhnaliv / Korchynskyi V.V., Nazarenko O.A., Stepanov V.O., Al-Faiiumy Khaled // Naukovyi zhurnal «Infokomunikatsiini ta kompiuterni tekhnolohii» – Kyiv, «Vidkrytyi mizhnarodnyi universytet rozvytku liudyny «Ukraina». No 2 (02) 2022, S.25-31. – Rezhym dostupu: https://visn-icct.uu.edu.ua/index.php/icct/article/view/86.

9. Semenko A.I. Cuchasni tekhnolohii infokomunikatsiinykh ta kompiuternykh merezh: monohrafiia / A.I. Semenko, Yu.M. Boiko, O.M. Shpur, I. V. Strelkovska, V. V. Korchynskyi, R. O. Yarovyi ; pid zah. red. A.I.Semenka. - Kyiv: Yevropeiskyi universytet, FO-P Biletskyi R.H., 2024.- 557 s. ISBN 978-617-853-009-9. – Rezhym dostupu: https://elar.khmnu.edu.ua/handle/123456789/17381.

10. Zakharchenko M., Korchynskii V., Kildishev V. Integrated methods of information security in telecommunication systems. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017), IEEE Xplore Digital Library. 11 – 15 September 2017. – V. 1. – pp. 78–81. URL: http://ieeexplore.ieee.org/document/8095366/.