УДК 004.056.55
DOI: 10.31673/2409-7292.2025.031083

Лаптєв О.А., Стеценко В. О.

МЕТОД ПОБУДОВИ КРИПТОСИСТЕМИ НІДЕРРАЙТЕРА НА ОСНОВІ М-КОДІВ

У статті запропоновано метод підвищення крипостійкості криптосистеми Нідеррайтера шляхом використання М-кодів – алгеброгеометричних кодів, побудованих на еліптичних кривих. Обґрунтовано актуальність розробки математичного апарату для проектування захищених інформаційних мереж у умовах зростання кіберзагроз. Мета дослідження – розробка підходів до системного проектування криптосистем на основі структурних специфікацій. Розглянуто крипто-кодову конструкцію Нідеррайтера, стійкість якої базується на NP-повній задачі декодування випадкового лінійного коду. Запропоновано використання алгеброгеометричних кодів над GF(q), заснованих на еліптичних кривих (рід g=1), що забезпечує покращені комбінаторні та асимптотичні властивості кодів. Наведено математичний апарат побудови перевірочної матриці коду з використанням геометричних параметрів кривих. Показано, що такий підхід дозволяє збільшити кількість виправлених помилок і підвищити завадостійкість. Також описано алгоритм рівноважного кодування для формування вектора помилок. Запропонований метод дозволяє визначити мінімальну кількість модулів обробки, розподілити функції між ними та задати специфікації швидкодії, що значно скорочує час розробки систем захисту. Результати мають практичне значення для створення живучих інформаційних мереж, особливо в умовах інтенсивних кібератак, зокрема в період війни.

Ключові слова: захист інформації, кібербезпека, крипто-кодова система, кодування, кодограма, крипостійкість.

Вступ

Зростання складності впровадження захищених інформаційних мереж підкреслює актуальність наукового завдання. Впровадження сучасних інформаційних технологій у всі сфери суспільного життя неможливе без забезпечення високого рівня інформаційної безпеки, яка охоплює цілісність, конфіденційність та доступність даних. Зростання складності телекомунікаційних систем, масштабне використання цифрових технологій та збільшення обсягів переданої інформації значно підвищують ризик несанкціонованого доступу, що робить питання кібербезпеки надзвичайно актуальними. Особливо гостро ця проблема стоїть у контексті захищених інформаційних мереж, де потрібно забезпечити не лише конфіденційність передачі даних, а й їх живучість у разі інтенсивних кібератак. У сучасних умовах, зокрема в період військових дій, важливість стійких криптографічних систем значно зростає, оскільки інформаційні мережі стають пріоритетною ціллю для протидії. Тому актуальною науковою задачею є розробка методів та математичного апарату для побудови захищених інформаційних мереж із підвищеною крипостійкістю. У цьому контексті особливе місце посідають крипто-кодові системи, засновані на поєднанні криптографії та теорії кодування, зокрема криптосистеми Мак-Еліса та Нідеррайтера, стійкість яких базується на NP-повній задачі декодування випадкового лінійного коду. Однак класичні реалізації цих систем мають обмежену ефективність через великі розміри ключів та недостатню крипостійкість при використанні певних типів кодів. У роботі пропонується метод підвищення крипостійкості шляхом побудови криптосистеми Нідеррайтера на основі М-кодів – алгеброгеометричних кодів, зокрема побудованих на еліптичних кривих, що забезпечує покращені комбінаторні та асимптотичні властивості. Такий підхід дозволяє підвищити ефективність кодування, збільшити кількість виправлених помилок та скоротити час проектування систем захисту, що є критично важливим для швидкого розгортання захищених мереж у умовах підвищеної загрози.

Аналіз літературних джерел та формулювання проблеми.

Процес впровадження нових інформаційних технологій у всі сфери суспільного життя є неможливим без вирішення ключових питань інформаційної безпеки, яка охоплює різні, але взаємопов’язані аспекти [1, 2]. Масштабне використання обчислювальної техніки, телекомунікаційних систем і цифрових технологій, поряд зі зростанням обсягів оброблюваної інформації та розширенням кола користувачів, створює нові можливості для

несанкціонованого доступу до інформації. Це, своєю чергою, значно підвищує вразливість таких систем. У сучасних умовах, коли необхідно забезпечувати захист не лише державної чи військової інформації, але й промислової, комерційної та фінансової таємниць, питання захисту інформації загалом та в мережах зв'язку зокрема набувають особливої актуальності [3]. У контексті дослідження методів підвищення крипостійкості шляхом використання крипто-кодових систем на основі алгеброгеометричних кодів, проаналізовано сучасні наукові джерела за останні п'ять років, що відображають тенденції у розвитку криптографії з відкритим ключем, захисту даних у телекомунікаційних мережах та використання кодів з виправленням помилок. У роботі [6] аналізуються аспекти безпеки канального кодування в перспективних системах 6G. У документі підкреслюється важливість інтеграції криптографічних механізмів безпосередньо в канальне кодування, що відкриває шлях для розробки гібридних крипто-кодових систем, таких як системи Мак-Еліса та Нідеррайтера, особливо з використанням кодів із високою завадостійкістю, зокрема алгеброгеометричних. У статті [7] розглянуто апаратну реалізацію криптосистеми на основі генератора випадкових чисел із двома джерелами ентропії. Хоча робота фокусується на симетричних методах, вона підкреслює актуальність забезпечення фізичної безпеки ключів, що є важливим аспектом при реалізації асиметричних криптосистем, зокрема тих, що базуються на складних математичних структурах, як у випадку М-кодів. У дослідженні [9] запропоновано новий підхід до книжкового шифрування з використанням веб-сторінок як криптографічного ключа. Це демонструє тенденцію до пошуку нетрадиційних джерел ентропії та гнучких криптографічних моделей, що підтверджує актуальність розробки математично обґрунтованих, але адаптивних криптосистем, які можуть інтегрувати різноманітні математичні структури, зокрема геометричні. У роботі [10] розглянуто використання згорткових нейронних мереж для біометричної автентифікації. Хоча тематика відрізняється, важливим є акцент на комплексному захисті інформації, що поєднує криптографію, біометрію та штучний інтелект, що вказує на необхідність розробки криптосистем, інтегрованих у сучасні інформаційні архітектури. В джерелі [11] запропоновано проектування периферійних модулів на основі програмно-настроюваних процесорів, що дозволяє гнучко реалізовувати криптографічні алгоритми. Це підтверджує важливість розробки не лише теоретичних, а й практичних підходів до реалізації криптосистем, зокрема таких, що вимагають значних обчислювальних ресурсів, як криптосистеми на основі алгеброгеометричних кодів. У роботі [12] досліджуються алгоритми фільтрації спаму та виявлення спамерів у соціальних мережах. Хоча напрямок інший, це підкреслює загальну тенденцію до використання математичних та алгоритмічних методів для забезпечення кібербезпеки, що є спільною основою з криптографією на основі кодів.

Нарешті, у роботі [5] розглянуто інтелектуальну систему керування інформаційно-комунікаційними мережами, що дозволяє динамічно реагувати на загрози. Це підтверджує актуальність розробки не тільки стійких, а й живучих криптографічних систем, які можуть швидко розгортатися та адаптуватися, що є ключовим аргументом на користь запропонованого в статті методу структурного проектування.

Таким чином, аналіз сучасних джерел свідчить про зростаючий інтерес до інтегрованих, математично обґрунтованих і живучих систем захисту інформації, що підтверджує актуальність дослідження криптосистеми Нідеррайтера на основі М-кодів.

Мета роботи та цілі дослідження

Метою статті є підвищення крипостійкості та ефективності кодування інформації на основі обґрунтування методів та математичного апарату для побудови захищених інформаційних мереж.

Виклад основного матеріалу

Крипто-кодова конструкція Нідеррайтера вперше запропонована в [11]. Основні параметри крипто-кодової конструкції, яка формує несиметричну криптосистему: H –

перевірна матриця лінійного (*n, k, d*)-коду над *GF(q)* з поліноміальною складністю декодування. Матриці маскування (закритий (особистий) ключ): *X* – невироджена *r*×*n* матриця над *GF(q)*, *D* – діагональна матриця з ненульовими елементами на діагоналі, *P* – перестановна матриця розміру *n*×*n*. Відкритим (публічним) ключем є матриця $H_X = X \times H \times P \times D$. Інформаційна послідовність (криптограма, кодограма) S_X є вектором довжини $r = n - k$ та обчислюється за правилом:

$$S_X = e \cdot H_X^T, \tag{1}$$

де вектор *e* – вектор довжини *n* та ваги $\leq t$, який несе конфіденційну інформацію. Користувач (має особистий ключ) знаходить одне з q^k рішень виразу $S_X = c_X^* \cdot H_X^T$. Знайдене рішення – це кодове слово з помилками $c_X^* = i \cdot G_X + e$. Далі, як і у крипто-кодовій системі Мак-Еліса, користувач будує вектор $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$, та декодує отримане слово. Однак замість відновлення інформаційного слова *i'*, він обчислює кодове слово, а потім і вектор помилок $c' = i' \cdot G$, та за рахунок рівноважного кодування знаходить інформаційну послідовність.

Таким чином, стійкість крипто-кодовій конструкції Нідеррайтера також, як й крипто-кодовій конструкції Мак-Еліса базуються на NP-повної задачі – декодування випадкового кодового слова. Структурна схема протоколу використання крипто-кодової конструкції Нідеррайтера наведена на рис. 1. При передачі конфіденційної інформації користувач Б випадково, рівноймовірне, незалежно від інших абонентів формує особистий (закритий) ключ – матриці маскування *X*, *P*, *D* та перевірочну матрицю *H* блокового лінійного коду. Формує публічний (відкритий) ключ за правилом $H_X = X \times G \times H \times D$. Абонент А для відправлення інформаційної послідовності перетворює її у вектор помилки за допомогою рівноважного кодування.

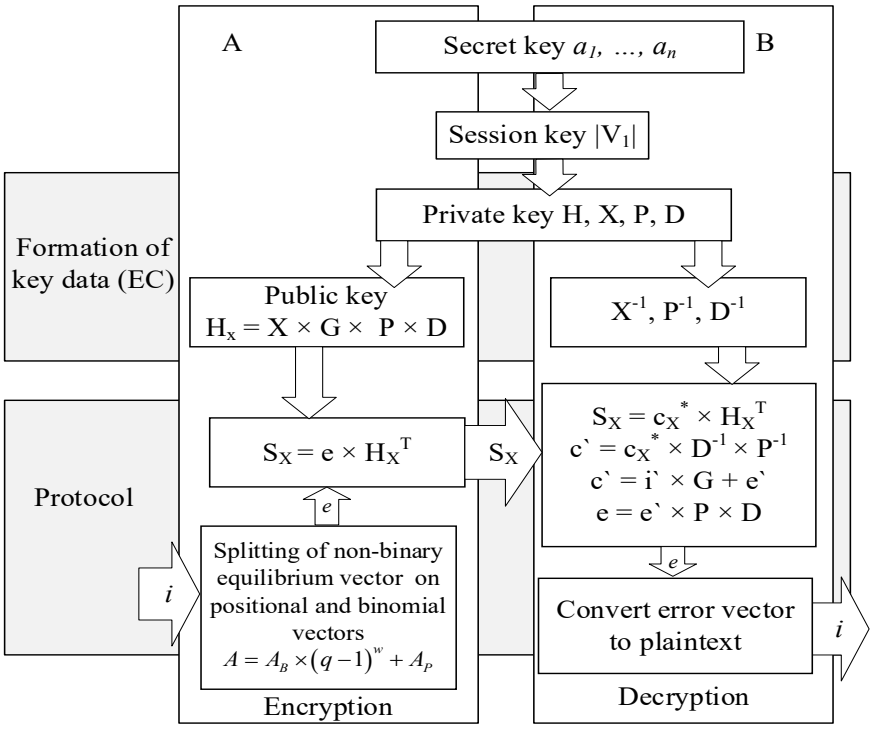

Рис. 1. Протокол обміну інформацією у крипто-кодової конструкції Нідеррайтера.

На рис. 2. наведений алгоритм рівноважного кодування. Її може сформувати будь-який користувач, який знає публічний (загальнодоступний) ключ. Таким чином, забезпечується

побудова криптограми. На приймальної стороні користувач Б розкодує криптограму (отримує інформаційну послідовність за рахунок використання алгоритму Берлекемпа-Месі).

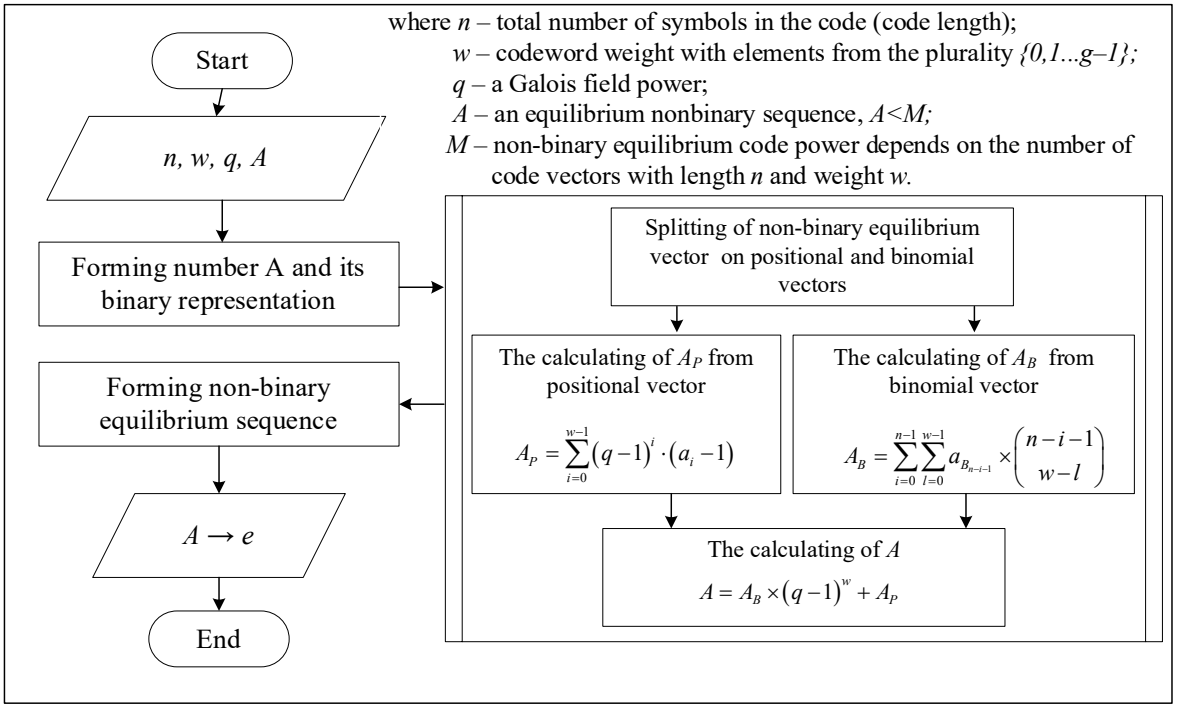

Рис. 2. Алгоритм рівноважного кодування

Розглянемо методи побудови m-кодів з хорошими комбінаторними властивостями на основі алгеброгеометричних кодів (кодів на основі синтезу методів побудови кодів теорії завадостійкого кодування та параметрами геометричних кривих третього роду – еліптичних кривих).

Методи алгеброгеометричного кодування забезпечують не тільки підвищення рівня стійкості крипто-кодових конструкцій як Мак-Еліса, так й Нідеррайтера, а також збільшення кількості виправлення помилок при збільшені (*n, k, d*)-параметрів лінійного блокового коду. В [12] доведено, що *m*-ічні алгебраїчні блокові коди, побудовані за алгебраїчними кривими (алгеброгеометричні коди) володіють хорошими асимптотичними властивостями.

Для побудови алгеброгеометричного лінійного блокового коду використовується кінцеве поле GF(q), в якому будується гладка проективна крива алгебри X – в проективному просторі P^n. Основні показники кривої: $g = g(X)$ – рід кривої, $X(GF(q))$ – множина її точок над кінцевим полем, $N = X(GF(q))$ – їх кількість. Якщо C – клас дивізорів на X ступеня $\alpha > g - 1$,то C визначає відображення $\varphi: X \to P^{k-1}$, де $k \geq \alpha - g + 1$. Набір $y_i = \varphi(x_i)$ задає код. Кількість точок у перетині $\varphi(X)$ з гіперплощиною дорівнює α визначається як, $n - d \leq \alpha$. Таким чином, конструкція дозволяє будувати коди з параметрами $k + d\ n - g + 1$, довжина n яких менша або дорівнює кількості точок на кривій X. При $2g < n$ алгеброгеометричний код має параметри (n, $\alpha - g + 1$, d), $d \geq n - \alpha$. Подвійний до нього код також є алгеброгеометричним і має параметри (n, $n - \alpha + g - 1$, $d^{\perp}$), $d^{\perp} \geq \alpha - 2g + 2$. X – гладка проективна крива алгебри в проективному просторі P^n – сукупність рішень однорідного неприводимого алгебраїчного рівняння ступеня $degX$ з коефіцієнтами з $GF(q)$. Тоді різноманіття, відповідні проективним гіперповерхням, заданим у P^n рівняннями F = 0, де F – однорідні одночлени ступеня $degF$. Алгеброгеометричний код по кривій X над $GF(q)$ – це лінійний код довжини $n \leq N$, який задається за правилом:

$$\sum_{i=0}^{k-1} i_j F_j(P_i) = c_i, \tag{2}$$

де $P_i(X_i, Y_i, Z_i)$ – проектні точки кривої X, X_i, Y_i, Z_i – рішення однорідного рівня алгебри, що задають криву X, $i = \overline{1,n}$; $F_j(P_i)$ – значення генераторних функцій у точках кривої.

Еліптичною кривою (*EC*) в афінному просторі A^2 над полем *GF(q)* визначемо гладку криву, яка задана рівнянням:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3}$$

або в P^2 задана однорідним рівнянням:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3, \tag{4}$$

де $a_i \in$ GF(q), рід кривої $g = 1$.

Алгеброгеометричний (n, k, d) код за еліптичною кривою (*EC*) над *GF(q)* будується з наступними параметрами: $\varphi: EC \to P^{k-1}$, $k + d \geq n$, $n \leq 2\sqrt{q} + q + 1$, $k \geq \alpha$, $d \geq n - \alpha$, $\alpha = 3 \cdot degF$, якщо $\varphi: X \to P^{k-1}$, де $k \geq \alpha$, характеристиками $k + d \geq n$, $d \geq n - \alpha$ [XXXXX].

Таким чином крипто-кодову система Мак-Еліса на основі *EC* визначається за правилом:

$$G^{EC} = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \dots & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}, \tag{5}$$

де $k \times n$, $k = \alpha$, $\alpha = 3 \cdot degF$.

Основні параметри несиметричної криптосистеми на основі крипто-кодової конструкції Мак-Еліса:

- відкритий (публічний) ключ – матриця $\mathrm{G}_{\mathrm{X}}^{\mathrm{EC}} = \mathrm{X} \cdot G^{EC} \cdot P \cdot D$;
- закритий (особистий) ключ – матриці маскування *X, P, D*.

Криптограма формується за правилом:

$$c_X^* = i \cdot G_X^{EC} + e. \tag{6}$$

Для побудови несиметричної криптосистеми на основі крипто-кодової конструкції Нідеррайтера на ЕС визначимо наступні параметри :

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0, \tag{7}$$

де $c_i \in GF(q)$, $d \geq \alpha - 2g + 2$, $\alpha = degX \cdot degF$.

Якщо: $H(c_0, c_1, ..., c_{n-1})^T = 0$, де H – перевірочна матриця коду розмірності $r \times n$, $r = n - k = d + g - 2$:

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \dots & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}. \tag{8}$$

Перевірочна матриця H^{EC} – *(n, k, d*-коду над *GF(q)* з *EC* має вид:

$$H^{EC} = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \dots & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}, \tag{9}$$

де $r \times n$, $r = \alpha$, $\alpha = 3 \cdot degF$.

Основні параметри несиметричної криптосистеми на основі крипто-кодової конструкції Нідеррайтера:

- відкритий (публічний) ключ – матриця $\mathrm{H}_{\mathrm{X}}^{\mathrm{EC}} = \mathrm{X} \cdot H^{EC} \cdot P \cdot D$;
- закритий (особистий) ключ – матриці маскування *X, P, D*.

Криптограма формується за правилом:

$$S_X = e \cdot \left(H_X^{EC} \right)^T . \quad (10)$$

Таким чином математичний апарат забезпечує побудову *m*-кодів з хорошими комбінаторними властивостями для крипто-кодових конструкцій Мак-Еліса та Нідеррайтера.

Висновки

У результаті проведеного дослідження розроблено науково обґрунтований метод підвищення крипостійкості та ефективності кодування в захищених інформаційних мережах шляхом побудови криптосистеми Нідеррайтера на основі М-кодів – алгеброгеометричних кодів, зокрема побудованих на еліптичних кривих.

Встановлено, що використання алгеброгеометричних кодів, заснованих на еліптичних кривих, дозволяє отримувати М-коди з покращеними комбінаторними та асимптотичними властивостями, що забезпечує підвищення стійкості криптосистеми до криптоаналітичних атак, зокрема завдяки складності задачі декодування випадкового лінійного коду (NP-повна задача).

Розроблено математичний апарат для побудови перевірочної матриці криптосистеми Нідеррайтера над скінченним полем GF(q) з використанням геометричних властивостей еліптичних кривих, що дозволяє формалізувати процес проектування криптосистеми та забезпечити її структурну цілісність.

Доведено, що запропонований підхід дозволяє підвищити кількість виправлених помилок при збільшенні параметрів (n, k, d) лінійного блокового коду, що особливо важливо для систем, що вимагають високої завадостійкості та безпечного кодування.

Таким чином, запропонований метод структурного проектування криптосистеми Нідеррайтера на основі М-кодів забезпечує комплексне вирішення задачі підвищення крипостійкості та ефективності кодування, що є актуальною задачею в умовах зростаючих загроз кібербезпеки, зокрема в період військових дій, коли стійкість і живучість інформаційних мереж є критично важливою.

Перелік посилань

1. Павлов І.М., Хорошко В.О. Проектування комплексних систем захисту інформації. К.: ВІТІ – ДУІКТ, 2011. 245 с.

2. Barabash O., Musienko A., Sobchuk V., Lukova-Chuiko N., Svynchuk O. Distribution of Values of Cantor Type Fractal Functions with Specified Restrictions. Chapter in Book “Contemporary Approaches and Methods in Fundamental Mathematics and Mechanics”. Editors Victor A. Sadovnichiy, Michael Z. Zgurovsky. Publisher Name: Springer, Cham, Switzerland AG 2021. P. 433-455. https://link.springer.com/book/10.1007/978-3-030-50302-4.

3. Barabash O.V., Dakhno N.B., Shevchenko H.V., Majsak T.V. Dynamic Models of Decision Support Systems for Controlling UAV by Two-Step Variational-Gradient Method. Proceedings of 2017 IEEE 4th International Conference “Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)”, October 17-19, 2017, Kyiv, Ukraine: National Aviation University, 2017. P. 108-111.

4. Лаптев О.А., Собчук В.В., Саланди И.П., Сачук Ю.В. Математична модель структури інформаційної сеті на основі нестаціонарної ієрархічної та стаціонарної гиперсети. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, Вип. 64, 2019. С. 124-132.

5. Lubov Berkman, Oleg Barabash, Olga Tkachenko , Andri Musienko, Oleksand Laptiev, Ivanna Salanda. The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347-3983. P.1920-1925.

6. Звіт ETSI Security Aspects of Channel Coding in 6G Systems (TR 103 756 V1.1.1). 2024.

7. Serhii Yevseiev, Khazail Rzayev, Oleksandr Laptiev, Ruslan Hasanov, Oleksandr Milov, Bahar Asgarova, Jale Camalova, Serhii Pohasii. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources. Eastern-European journal of enterprise technologies. Vol.5 №9 (119). 2022 P. 6–16. ISSN (print) 1729-3774. ISSN (on-line) 1729-4061. DOI: https://doi.org/10.15587/1729-4061.2022.265774.

© Лаптєв О.А., Стеценко В. О. (2025) Метод побудови криптосистеми нідеррайтера на основі М-кодів. Сучасний захист інформації, 3(63), 83–89.
https://doi.org/10.31673/2409-7292.2025.031083

8. Serhii Yevseiev, Khazail Rzayev, Oleksandr Laptiev, Ruslan Hasanov, Oleksandr Milov, Bahar Asgarova, Jale Camalova, Serhii Pohasii. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources. Eastern-European journal of enterprise technologies. Vol.5 №9 (119). 2022 P. 6–16. ISSN (print) 1729-3774. ISSN (on-line) 1729-4061. DOI: https://doi.org/10.15587/1729-4061.2022.265774.

9. F. K. Mammadov, "New approach to book cipher: web pages as a cryptographic key", Advanced Information Systems, vol. 7, no. 1, pp. 59–65, 2023, doi: https://doi.org/10.20998/2522-9052.2023.1.10.

10. S. Datsenko, and H. Kuchuk, "Biometric authentication utilizing convolutional neural networks", Advanced Information Systems, vol. 7, no. 2, pp. 87–91, 2023, doi: https://doi.org/10.20998/2522-9052.2023.2.12.

11. D. Salnikov, D. Karaman, and V. Krylova, "Highly reconfigurable soft-cpu based peripheral modules design", Advanced Information Systems, vol. 7, no. 2, pp. 92–97, 2023, doi: https://doi.org/10.20998/2522-9052.2023.2.13.

12. A. Podorozhniak, N. Liubchenko, V. Oliinyk, and V. Roh, "Research application of the spam filtering and spammer detection algorithms on social media and messengers ", Advanced Information Systems, vol. 7, no. 3, pp. 60-66, 2023, doi: https://doi.org/10.20998/2522-9052.2023.3.09.

Надійшла 30.06.2025