DOI: 10.18372/2225-5036.30.19244

ОЦІНКА ВЛАСТИВОСТЕЙ КРИПТО-КОДОВИХ КОНСТРУКЦІЙ НА LDPC-КОДАХ

Станіслав Мілевський[1], Ольга Король[2], Ольга Грищук[3], Тетяна Лаптєва[4], Сергій Євсеєв[5]

[1,2,5] Національний технічний університет "Харківський політехнічний інститут", Україна
[3]Національний університет оборони України, Україна
[4]Київський національний університет імені Тараса Шевченка, Україна

МІЛЕВСЬКИЙ Станіслав Валерійович, к.е.н., доцент
Рік та місце народження: 1979, Муром, Володимирська область.
Освіта: Харківський національний економічний університет, 2001.
Посада: доцент кафедри кібербезпеки Національний технічний університет "Харківський політехнічний інститут", Україна.
Наукові інтереси: захист інформації у соціокіберфізичних системах.
Публікації: більше 60 наукових публікацій, включаючи монографії, підручники, статті та патенти.
E-mail: milevskiysv@gmail.com.
Orcid ID: 0000-0001-5087-7036.

КОРОЛЬ Ольга Григорівна, к.т.н., доцент
Рік та місце народження: 1981 р., м. Джанкой, АР Крим
Освіта: Харківський національний економічний університет, 2005 р.
Посада: доцент кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна.
Наукові інтереси: захист інформації в соціокіберфізичних системах, механізми аутентифікації.
Публікації: понад 140 наукових публікацій, серед яких монографії, навчальні посібники, статті та патенти.
E-mail: korol.olha2016@gmail.com.
Orcid ID: 0000-0002-8733-9984.

ГРИЩУК Ольга Михайлівна
Рік та місце народження: 1984 рік, м. Житомир, Україна.
Освіта: Національний авіаційний університет, 2009 рік.
Посада: старший науковий співробітник науково-дослідної лабораторії управління інформаційною безпекою науково-дослідного відділу проблем розвитку та впровадження стратегічних комунікацій Інституту стратегічних комунікацій Національного університету оборони України.
Наукові інтереси: кібербезпека.
Публікації: понад 15 наукових публікацій.
E-mail: ol.hry@i.ua.
Orcid ID: 0000-0001-6957-4748.

ЛАПТЄВА Тетяна Олександрівна, аспірантка
Рік та місце народження: 1986, Київ, Україна.
Освіта: Національний авіаційний університет, Україна, 2010.
Посада: аспірантка, кафедри кібербезпеки та захисту інформації, факультету інформаційних технологій, Київського національного університету імені Тараса Шевченка.
Наукові інтереси: захист інформації, виявлення неправдивої інформації, інформаційне протиборство.
Публікації: понад 10 наукових публікацій.
E-mail: tetiana1986@ukr.net.
Orcid ID: 0000-0002-5223-9078.

ЄВСЕЄВ Сергій Петрович, д.т.н., професор
Рік та місце народження: 1969 р., м. Харцизьк Донецької області
Освіта: Харківський військовий університет, 2002 р.
Посада: професор, завідувач кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна.
Наукові інтереси: захист інформаційних ресурсів, постквантова криптографія, безпека в соціокіберфізичних системах.
Публікації: понад 300 наукових публікацій, серед яких монографії, навчальні посібники, статті та патенти.
E-mail: serhii.yevseiev@gmail.com.
Orcid ID: 0000-0003-1647-6444.

Анотація. *Зростання мобільних технологій та обчислювальних потужностей значно розширило діапазон цифрових послуг і фактично випередило розвиток комп'ютерної техніки. Це сприяє використанню мобільних і бездротових мереж у більшості напрямів смарт-технологій та підтримує подальше поєднання кіберпростору з мобільним Інтернетом. Однак, брак протоколів безпеки, що забезпечують конфіденційність та цілісність даних на ранніх етапах впровадження технологій LTE, створює умови для кіберзловмисників використовувати мобільні Інтернет-канали з метою проведення APT-атак. З розвитком і появою повноцінного квантового комп'ютера, який використовує алгоритми Шора та Гровера, можливе значне зниження стійкості криптосистем, побудованих на базі симетричної і асиметричної криптографії, включаючи криптографію на еліптичних кривих. Крім того, сучасні кіберзагрози демонструють ознаки синергії та гібридності, а їх поєднання із методами соціальної інженерії ускладнює впровадження ефективних превентивних заходів. У статті пропонуються постквантові криптосистеми на основі крипто-кодової схеми Мак-Еліса, яка використовує коди з низькою щільністю перевірок на парність (LDPC-коди). Цей підхід дозволяє легко інтегруватися у бездротові мережі, що відповідають стандартам IEEE 802.16 та IEEE 802.15.4, а також технологіям LTE, забезпечуючи належний рівень захисту від сучасних загроз.*

Ключові слова: *модифікована крипто-кодова конструкція Мак-Еліса, постквантовий період, коди з малою щільністю перевірок на парність.*

Постановка проблеми

Розвиток мобільних технологій та бездротових мереж визначив вектори створення принципово нових підходів до розширення спектру послуг на основі бездротових та мобільних мереж на основі технологій стандартів IEEE 802.16 та IEEE 802.15.4. Подальший розвиток мобільних технологій LTE дозволяє синтезувати технології Інтернет-речей, кіберфізичних систем з технологіями LTE, та формувати Mesh- та/або сенсорні мережі, розвивати смарт-технології та формувати соціокіберфізичні системи. Однак в умовах комплексування сучасних кіберзагроз із методами соціальної інженерії, можливості прояву синергізму та гібридності APT-атак (цільових атак) виникає необхідність розгляду безпеки у спектрі трьох складових: кібербезпеки (КБ), інформаційної безпеки (ІБ), безпеки інформації (БІ) [1]. Такий підхід забезпечує формування своєчасних превентивних заходів для забезпечення безпеки бізнес-процесів та формування контуру безпеки. Для формування послуг безпеки, як правило використовуються симетричний та несиметричний криптосистеми (стійкість перших ґрунтується на стійкості ключових послідовностей та S-boxів, других на теоретико-складних задачах (NP-повних задачах). Однак стрімкий розвиток квантових обчислень дозволяє суттєво знизити стійкість даних криптосистем на основі квантових алгоритмів Шора та Гровера [2-6], що потребує формування нових підходів до створення та/або модифікації відомих криптосистем – формування постквантової криптографії. На жаль, крім цього, аналіз ефективності механізмів забезпечення безпеки в LTE-технологіях практично не забезпечує мінімальний рівень безпеки [7-9], що значною мірою впливає на подальший розвиток цих технологій. Таким чином, питання забезпечення безпеки даного розвитку соціокіберфізичних систем, смарт-систем на основі постквантових алгоритмів є актуальним науково-технічним завданням.

Аналіз останніх досліджень і публікацій

[1-6] показав, що в умовах появи повномасштабного квантового комп'ютера на основі квантових алгоритмів Шора та Гровера ставиться під сумнів забезпечення необхідного рівня безпеки не тільки в об'єктах критичної інфраструктури, а й у кіберпросторі загалом. Тому з 2016 року спеціалістами НІСТ США проводиться конкурс на алгоритми постквантової криптографії, де на третьому етапі у групі несиметричних криптосистем лідирує крипто-кодова конструкція (ККК) Мак-Еліса на класичних кодах [10].

У роботі [19] наводиться алгоритм злому ККК Мак-Еліса на основі дробово-лінійних перетворень та властивості тричі транзитивності групи автоморфізмів узагальненого коду Ріда-Соломона. Суть якого зводиться до знаходження елементів матриці, що породжує, і зняття дії матриць маскування. Ортогональність матриць – що породжує та перевірочної дозволяє розглядати ефективність атаки і на ККК Нідеррайтера. Перспективним напрямом усунення виявлених закономірностей в [19] пропонується використовувати каскадні або алгеброгеометричні коди (АГК) – коди побудовані на основі алгебри теорії завадостійкого кодування та геометричних параметрах кривої, зокрема еліптичних кривих. У роботах [3–6] розглянуто моделі та практичні алгоритми реалізації ККК на алгеброгеометричних кодах. Однак в умовах розвитку соціо-кіберфізичних систем на основі консорціуму 3GPP [19] у мережах п'ятого покоління 5G New Radio (NR) як перешкодостійкий код використо-

вуватиметься LDPC – коди з низькою щільністю перевірок на парність. LDPC реалізовані в багатьох сучасних стандартах передачі даних, частотності IEEE 802.11n (Wi-Fi), IEEE 802.16e (WiMAX), IEEE 802.15.4 (ZigBee), цифровому телебаченні (DVBS2 (T2), DMB-T), а також системах зв'язку з ближнім та далеким космосом (CCSDS). Основною перевагою даних кодів є можливість забезпечити обробку інформації на сучасній елементній базі на швидкості до 1 Гбіт/с щодо сигнал/шум порядку 2 дБ і менше [18, 19].

Мета та постановка завдання

Таким чином, використання запропонованих рішень реалізації ККК на АГК, не дозволять забезпечити необхідну сумісність з кодами, що вже використовуються, а їх реалізації збільшить енергоємність даної реалізації, що в умовах застосування бездротових ліній зв'язку на основі LTE-технологій не бажано.

Виклад основного матеріалу дослідження

Для забезпечення безпеки технологій mesh-, сенсорних мереж із використанням стандартів бездротових каналів, які використовуються в соціокіберфізичних системах: мобільних технологій LTE, WiFi, Bluetooth необхідні нові підходи для забезпечення послуг безпеки. У разі появи квантового комп'ютера необхідно як використання постквантових криптоалгоритмів, а й новий підхід до забезпечення безпеки соціокіберфізичних систем. Такі алгоритми вимагають збільшення довжини ключових послідовностей до 512 біт для симетричних криптосистем, що забезпечує безпеку приблизно на 60 років, або використання постквантових асиметричних криптосистем (PQAS — post-quantum asymmetric cryptosystems).

В означених умовах пропонується використовувати структурні схеми крипто-кодових конструкцій (ССС) McEliece та Niederreiter на алгеброгеометричних кодах, які забезпечують захист від атаки Сідєльнікова та зниження енергоємності. Крім цього, вони інтегровано забезпечують виправлення помилок в інформаційній послідовності. Обидві ССС будуються за принципом використання теорії завадостійкого кодування і ортогональності матриць *G* – породжувальної матриці лінійного коду, і *H* – перевірочної матриці лінійного коду, рівноймовірно сформована джерелом ключів *k*×*k* матриця з елементами *GF(q)*; *q* – матриця, що породжує розмірністю *k*×*n* (ССС McEliece); *H* – перевірочна матриця розмірністю *r*×*n*. Крім цього, відмінною особливістю ССС Нідеррайтера є попереднє використання рівноважного кодування, що дозволяє забезпечити практично відносну швидкість кодування, що дорівнює одиниці. Нижче наведені співвідношення часу та ступеня секретності інформації (табл. 1).

Для формування математичної моделі методу забезпечення конфіденційності та автентичності у бездротових каналах скористаємось підходами [13, 16, 17].

Вихідними даними для математичних моделей ССС McEliece на LDPC-кодах є:

– множина відкритих текстів:

$$M = \left\{ M_1, M_{2,} ... M_{q^k} \right\},$$

де $M_i = \{I_0, I_{h_1}, .. I_{h_j}, I_{k\text{-}1}\}, \forall I_j \in GF(q)$, h_j – інформаційні символи, які дорівнюють нулю, $|h| = \frac{1}{2}k$, Тобто I_i=0, $\forall I_i \in h$. На основі алгоритму рівноважного кодування відкритий текст перетворюється на вектор помилки;

- множина закритих текстів (кодограм) $C = \{C_1, C_2, ..., C_{q^k}\}$, де $C_i = (c^*_{X_0}, c^*_{h_1}, ..., c^*_{h_j}, c^*_{X_{n-1}})$, $\forall c^*_{X_j} \in GF(q)$ – множина прямих відображень (на базі використання відкритого ключа – породжувальної/перевірочної матриці завадових кодів (error-correcting code – ECC) (алгеброгеометричних кодів: EC, MEC; LDPC; збиткових кодів):

$$(G_j^{U_j}, \forall j \in \{U_j\}, U_1 - EC, U_2 - MEC, U_3 - FC, U_1 - LDPC,)$$
$$H_j^{U_j}, \forall j \in \{U_j\}, U_1 - EC, U_2 - MEC, U_3 - FC, U_1 - LDPC,$$

$\phi = (\phi_1, \phi_2, ..., \phi_s)$, де $\phi_i : M \to C_{k-h_j}$, i=1, 2,…, s;

Таблиця 1

Співвідношення часу та ступеня секретності інформації

Ступінь секретності інформації	Час	Пропоновані коди для ССС
критична	до 1 року	*MEC*, збиткові коди
висока	до 1 місяця	*MEC*
середня	до 1 години	*EC*
низька	до 10 хвилин	*EC*
дуже низька	до 1 хвилини	LDPC

– множина зворотних відображень (на основі використання секретного (приватного) ключа – матриць маскування):

$$\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, ..., \phi_s^{-1}\},$$

де $\phi_i^{-1} : C_{k-h_j} \to M$, $i = 1, 2, ..., s$; - множина відкритих ключів, які параметризують прямі відображення (доступний ключ уповноваженого користувача):

$$KU_i = \{KU_1, KU_2, ..., KU_S\} = \{G_1^{U_1}, G_2^{U_2}, ..., G_S^{U_S}\},$$

де $G^{U_i}_{X_{a_i}}$ – матриця $n \times k$, що породжує замаскований під випадковий код. Матриця визначається з ортогональності матриць породжувальної та перевірочної;

- множина особистих (закритих) ключів користувачів:

$$KR = \left\{ \{X, P, D\}_1, ..., \{X, P, D\}_r \right\}, \qquad (1)$$

де X^i – невироджена, маскуюча, випадково рівноймовірно сформована джерелом ключів *k*×*k* матриця з елементами *GF(q)*; P^i – перестановна випадково рівноймовірно сформована джерелом ключів *n*×*n* матриця з елементами *GF(q)*; D^i – діагональна матриця *n*×*n*, сформована джерелом ключів з елементами *GF(q)*.

За рахунок того, що діагональна матриця дорівнює одиничній матриці, значення можна знехтувати, що дає зменшення ємності та складності обчислення.

Відкритий ключ формується шляхом перемноження матриць маскування на матриці, що породжує/перевірочну:

$$G_{X_{a_i}}^{U_i} = X^u \times G^{U_i} \times P^u, u \in \{1,2,...,s\};$$

У канал зв'язку надходить кодове слово: $C_j = M_i \times G_{X_{a_i}}^{U_i\ T} + e,$ де є додатковий сеансовий ключ кожної інформаційної посилки.

На приймальній стороні уповноважений користувач, який знає матриці маскування, використовує швидкий алгоритм розкодування:

$$M_i = f_u^{-1}\left(C_j^*, \{X, P, D\}_u\right). \quad (2)$$

Нульові інформаційні символи додає уповноважений користувач для відновлення відкритого тексту $C_j^* = C_j + C_{k-h_j}$, з відновленого закритого тексту C_j знімає дію секретних перестановної та діагональної матриць P^u та D^u:

$$C = C_j^* \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1}. \quad (3)$$

Розкодування отриманого вектору проводять за алгоритмом Берлекемпа-Мессі:

$$C = M_i \times \left(X^u\right)^T \times \left(G_{X_{a_i}}^{U_i}\right)^T + e \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1}, \quad (4)$$

тобто позбавляється від другого доданку і від співмножника $\left(G_{X_{a_i}}^{U_i}\right)^T$ у першому доданку у правій частині рівності, після чого знімає дію матриці маскування X^u. Для цього отриманий результат розкодування $M_i \times (X^u)^T$ слід помножити на $(X^u)^{-1}$: $(M_i \times (X^u))^T \times (X^u)^{-1} = M_i$. Отримане рішення – це відкритий текст M_i.

Далі уповноважений користувач, використовуючи матриці $\{X, P, D\}^u = \{X^u, P^u, D^u\}$ формує вектор: $\bar{c}^* = c_X^* \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1}$, таким чином демаскує кодову послідовність $c_{X_i}^*$.

Після підстановки отримаємо рівність:

$$\bar{c}^* = c_X^* \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1}. \quad (5)$$

Уповноважений користувач при формуванні вектору має можливість застосувати швидкий алгоритм завадостійкого декодування поліноміальної складності та сформувати таким чином вектор $\bar{c}^* = c_X^* \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1}$ та вектор $M_i^u = M_i \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1}$.

Для відновлення інформаційної рівноважної послідовності M_i достатньо знову помножити вектор M_i^u на матриці маскування P^u і D^u, у зворотній послідовності:

$$M_i = M_i^u \times P^u \times D^u. \quad (6)$$

Використання постквантових алгоритмів – ССС на LDPC дозволяє формувати криптосистеми над полем $GF(2^6)$, а при використанні та ущербних кодів, формувати гібридні криптосистеми на полі $GF(2^4)$, що дозволяє їх практичну реалізацію на ресурсообмежених чіпсетах. Проведені експериментальні дослідження показали, що застосування ССС у кіберфізичних системах на основі бездротових каналів потребує мобільного Інтернет-каналу (широкополосного каналу). Це обмеження формується на основі існуючої багатоконтурної моделі SCPS, де зазвичай система управління розгортається в хмарних технологіях.

Для реалізації HCCC McEliece на LDPC-кодах із заподіянням збитку скористаємося підходами, структурна схема передачі даних представлена (рис. 1) [12-15].

Математична модель HCCC McEliece використовує такі вихідні дані:

- множина інформаційних ресурсів $I = \left\{I_1, I_{2,}...I_{q^k}\right\}$, для всіх $I_j \in GF(q)$;

- множина криптоперетворень для формування кодового слова на матриці *LDPC*-коду, що породжує: $C=(C_1, C_2, \ldots, C_s)$, де $\phi_i : I \to C_{k-h_j}$, i = 1, 2, ..., s. де h_j – формує вектори ініціалізації (IV_1 – вектор ініціалізації, який визначає кількість та місця «виколювання» символів у кодовому слові, IV_2 – вектор ініціалізації, який визначає кількість та місця «до давлення» інформаційних символів у кодовому слові);

- множина криптоперетворень, які дозволяють отримати вихідний інформаційний ресурс:

$$\phi^{-1} = \{\phi_1^{-1}\phi_2^{-1}, ...\phi_s^{-1}\}, \quad (7)$$

де $\phi_i^{-1} : C_{k-h_j} \to I$;

- множина відкритих ключів:

$$KU_i = \left\{KU_1, KU_2, ..., KU_S\right\} = \\ = \left\{G_1^{LDPC}, G_2^{LDPC}, ..., G_S^{LDPC}\right\}, \quad (8)$$

де $G_{X_{a_i}}^{LDPC_i}$ – породжувальна матриця LDPC-коду.

Для формування ключа використовуємо:

$$G_{X_{a_i}}^{LDPCu} = X^u \times G^{LDPCu} \times P^u, \\ u \in \{1,2,...,s\}; \quad (9)$$

- множина особистих (закритих) ключів користувачів:

$$KR = \left\{KR_1, KR_2, ..., KR_r\right\} = \left\{X^i, P^i, D^i\right\}, \quad (10)$$

де матриці маскування: *Xi* – невироджена $k \times k$-матриця; *Pi* – перестановна $n \times n$-матриця; *Di* – діагональна $n \times n$-матриця.

Діагональна матриця LDPC-коду дорівнює одиничній матриці і може не використовуватися;

– множина збиткових текстів (C(x)i) – $CFT = \{CFT_1, ..., CFT_{q^k}\}$;

- множина збитків ($f(x)_i$ - прапор), $CHD = \{CHD_1, ..., CHD_{q^k}\}$;

– множина формування збиткового тексту та шкоди (на основі ключа алгоритму MV2) – $E = \{E_{K_{MV2}}^1, ..., \phi_{K_{MV2}}^S\}$, f(x)=n – |C(x)|, у випадку якщо |C(x)| > r, де r – це визначений параметр, $r \in_R Z_{q^m}$, $0 \langle r \langle n$;

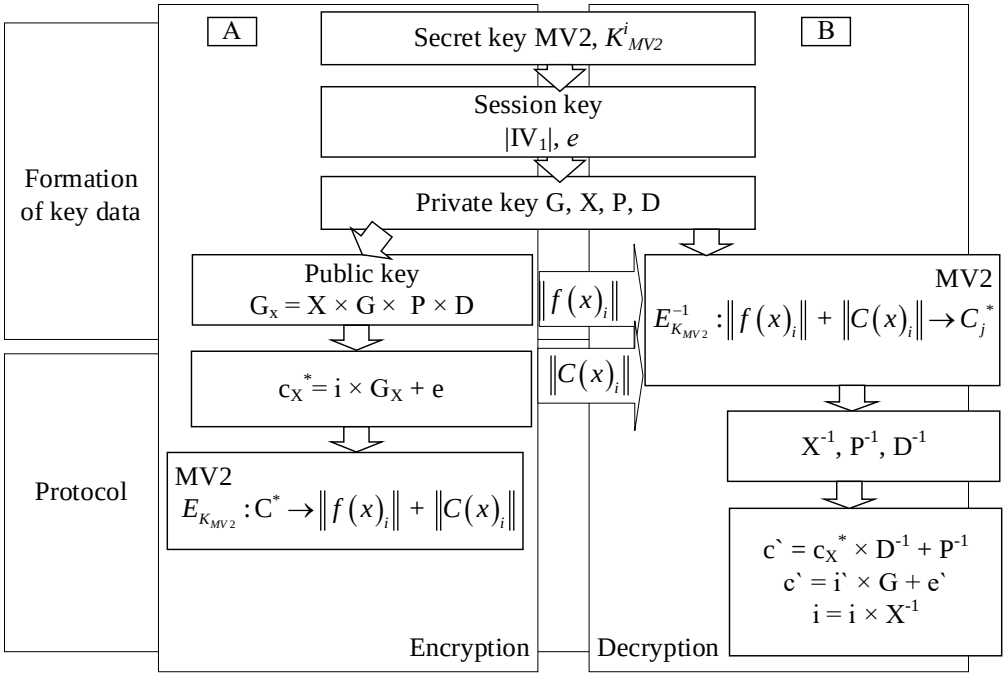

Рис. 1. Структурна схема гібридної ССС McEliece на LDPC-кодах із заподіянням збитку

– множина відображення MV2 $\rightarrow F_n^r$, що задає бієктивне відображення між множиною перестановок $\{S_1,...,S_{2^n}\}$ і множиною $\#F_n^r$, $\#F_n^r = \#\{(c, f)\} = 2^n!$;

– множина відображення неповноцінного тексту в інформаційний ресурс (на основі ключа – *Ki* MV2, і алгоритму MV2) – $E^{-1} = \{E^1_{K_{MV2}}{}^{-1}, ..., E^S_{K_{MV2}}{}^{-1}\}$, де $E^{-1}_{K_{MV2}} : \|f(x)_i\| + \|C(x)_i\| \rightarrow I.$

Відправник формує кодове слово: $C_j = M_i \times G^{LDPCu^T}_{X_{a_i}} + e,$ де є додатковий сеансовий ключ кожної інформаційної посилки.

До алгоритму MV2 надходить кодове слово $C_j = M_i \times G^{LDPCu^T}_{X_{a_i}} + e$ і перетворюється в алгоритмі MV2 у збитковий текст (залишок) та збиток (прапор):

$$E_{K_{MV2}} : C^* \rightarrow \|f(x)_i\| + \|C(x)_i\|. \quad (11)$$

У канал зв'язку надходить ‖f(x)i‖ і ‖ C(x)i‖ при цьому передача може проводитись і по одному, і по двох незалежних каналах.

На приймаючій стороні одержувач використовує правило завдання шкоди F_n^r, маскування, кількість та місця нульових інформаційних символів може розкодувати кодове слово та отримати інформаційне повідомлення:

$$E^{-1}_{K_{MV2}} : \|f(x)_i\| + \|C(x)_i\| \rightarrow C_j^*, \quad I_i = \phi_u^{-1}(C_j^*, \{X, P, D\}_u). \quad (12)$$

При використанні подовженого модифікованого LDPC-коду одержувач додає нульові інформаційні символи (по вектору ініціалізації V1), а також і «отримує» інформаційні символи (по вектору ініціалізації V2).

З $C_j^* = C_j + C_{k-h_j}$ знімається дія матриць маскування:

$$C = C_j^* \times (P^u)^{-1} = \left(I_i \times (G_X^{LDPCu})^T + e\right) \times (P^u)^{-1} = \left(I_i \times (X^u \times G^{LDPC} \times P^u)^T + e\right) \times$$
$$\times (P^u)^{-1} = I_i \times (X^u)^T \times (G^{LDPC})^T \times (P^u)^T \times (P^u)^{-1} + e \times (P^u)^{-1} = \quad (13)$$
$$= I_i \times (X^u)^T \times (G^{LDPC})^T + e \times (P^u)^{-1},$$

а потім розкодує отриманий вектор за алгоритмом Берлекемпа-Мессі [11, 13]:

$$C = I_i \times (X^u)^T \times (G^{LDPC})^T + e \times (D^u)^{-1} \times (P^u)^{-1}, \quad (14)$$

Отримуємо інформаційний ресурс:

$$\left(I_i \cdot (X^u)^T\right) \times (X^u)^{-1} = I_i. \quad (15)$$

Таким чином, представлені математичні моделі дозволяють використовувати ССС McEliece для забезпечення послуг конфіденційності цілісності та автентичності та практично реалізувати запропонований метод. Описані основні елементи пропонованого методу забезпечення основних послуг безпеки у соціокіберфізичних системах на основі бездротових каналів зв'язку. Основною відмінністю від відомих підходів є за збереження рівня пропускних можливостей бездротового каналу інтегровано забезпечити необхідний рівень захищеності (криптостійкості) каналу (криптостійкість на основі постквантових алгоритмів на рівні 10^{25}-10^{35} групових операцій), достовірності ($P_{пом}$ не нижче 10^{-9}-10^{-12}) [13].

Представлений математичний апарат дозволяє оцінити основні параметри ССС на LDPC-кодах із заподіянням збитку та на модифікованих кодах.

Укорочені *МЕС*	Подовжені *МЕС*
(n, k, d) параметри коду, який побудований через відображення виду $\varphi: X \rightarrow P^{k-1}$	
$n = 2\sqrt{q} + q + 1 - x$	$n = 2\sqrt{q} + q + 1 - x + x_1$
$k \geq \alpha - x,\ d \geq n - \alpha,\ \alpha = 3 \times degF$ $k + d \geq n$	$k \geq \alpha - x + x_1,\ d \geq n - \alpha,\ \alpha = 3 \times degF$
(n, k, d) параметри коду, який побудований через відображення виду $\varphi: X \rightarrow P^{r-1}$	
$n = 2\sqrt{q} + q + 1 - x$	$n = 2\sqrt{q} + q + 1 - x + x_1$
$k \geq n - \alpha,\ d \geq \alpha,$ $\alpha = 3 \times degF,\ k + d \geq n$	$k \geq n - \alpha,\ d \geq \alpha,\ \alpha = 3 \times degF$
розмірність секретного ключа	
$l_{K+} = x \times \left\lceil \log_2 \left(2\sqrt{q} + q + 1\right) \right\rceil$	$l_{K+} = (x - x_1) \times \log_2 \left(2\sqrt{q} + q + 1\right)$
розмірність секретного ключа	
$l_I = (\alpha - x) \times m$	$l_I = (\alpha - x + x_1) \times m$
розмірність криптограми	
$l_S = \left(2\sqrt{q} + q + 1 - x\right) \times m$	$l_S = \left(2\sqrt{q} + q + 1 - x + x_1\right) \times m$
відносна швидкість передачі	
$R = (\alpha - x) / \left(2\sqrt{q} + q + 1 - x\right)$	$R = (\alpha - x + x_1) / \left(2\sqrt{q} + q + 1 - x + x_1\right)$

Рис. 2. Основні параметри та властивості ССС McEliece на МЕС

Для дослідження властивостей ССС та НССС McEliece на МЕС та на LDPC-кодах та збиткових кодах наведені на рис. 2 та 3.

Основні параметри та властивості НССС McEliece на LDPC-кодах наведені на рис. 3.4.

Найважливішими показниками, які відображають можливість застосування ССС в різних компонентах соціокіберфізичних систем є складність формування кодограми (складність шифрування), складність розкодування (складність розшифрування) та складність декодування (складність зламу). В таблицях 2-4 наведені відповідні параметри для ССС на МЕС, НМЕС та ССС на LDPC для подовжених та скорочених кодів в залежності від потужності поля Галуа.

На рисунках 4-6 наведено графічну інтерпретацію отриманих результатів.

Таблиця 2

Складність формування кодограми для досліджуваних ССС в залежності від потужності поля Галуа та швидкості каналу передачі даних

GF^n	Тип ССС											
	1/2 sh LDPC	3/4 sh LDPC	1/2 leng LDPC	3/4 leng LDPC	0.5 leng MEC	0.75 leng MEC	0.5 sh MEC	0.75 sh MEC	0.5 leng HMEC	0.75 leng HMEC	0.5 sh HMEC	0.75 sh HMEC
3	44	43	42	39	242	603	817	968	643	780	923	998
4	73	73	69	65	760	980	2140	6282	905	1085	1563	5125
5	128	123	120	107	2241	6121	8706	11461	1863	2450	6137	8282
6	231	217	214	187	6348	9830	10722	60760	6273	7016	9183	10341
7	423	397	389	338	17092	61751	83000	210170	16582	15985	16563	16925
8	798	742	729	623	67016	105265	207422	605005	65278	65450	66137	68282
9	1528	1409	1391	1169	98765	510780	710920	1018079	95327	96037	97134	97841

Укорочені *LDPC*-коди	Подовжені *LDPC*-коди
Довжина відкритого тексту	
$l_I = l_z^c + l_z^f$	$l_I = \frac{k}{2} \times m + l_z^c + l_z^f$
Довжина кодограми	
$l_S = \left(2\sqrt{q} + q + 1 - k/2\right) \times m;$	$l_S = \left(2\sqrt{q} + q + 1 - k/2 + k/2\right) \times m.$
Довжина відкритого ключа	
$l_K = \frac{k}{2} \times \left(2\sqrt{q} + q + 1 - k/2\right) \times m;$	$l_K = \frac{k}{2} \times \left(2\sqrt{q} + q + 1 - k/2 + k/2\right) \times m.$
Довжина закритого ключа	
$l_{K_+} = \frac{k}{2}\left\lceil \log_2\left(2\sqrt{q} + q + 1\right)\right\rceil + \left\lvert F_u^v \right\rvert,$	$l_{K_+} = (k/2 - k/2)\left\lceil \log_2\left(2\sqrt{q} + q + 1\right)\right\rceil + \left\lvert F_u^v \right\rvert.$
Складність формування кодограми для систематичного кодування	
$O_K = (r+1) \times \left(2\sqrt{q} + q + 1 - k/2\right) + +O\left(\frac{1 - K_C^u}{K_f} \times L\right);$	$O_K = (r+1) \times \left(2\sqrt{q} + q + 1 - k/2 + k/2\right) + +O\left(\frac{1 - K_C^u}{K_f} \times L\right);$
Складність формування кодограми для несистематичного кодування	
$O_K = O_K = (k+1) \times (k+1) \times \times \left(2\sqrt{q} + q + 1 - k/2\right) + +O\left(\frac{1 - K_C^u}{K_f} \times L\right);$	$O_K = (k+1) \times \left(2\sqrt{q} + q + 1 - k/2 + k/2\right) + +O\left(\frac{1 - K_C^u}{K_f} \times L\right).$
Складність розкодування кодограми	
$O_{SK} = 2 \times \left(2\sqrt{q} + q + 1 - k/2\right)^2 + k^2/2 + +4t^2 + \left(t^2 + t - 2\right)^2/4;$	$O_{SK} = 2 \times \left(2\sqrt{q} + q + 1 - k/2 + k/2\right)^2 + +k^2 + 4t^2 + \left(t^2 + t - 2\right)^2/4.$
Складність процесу декодування	
$O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - k/2\right) \times r + +N_F \text{ або} \left(N_K\right),$	$O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - k/2 + k/2\right) \times \times r + N_F \text{ або} \left(N_K\right).$

Рис. 3. Основні параметри та властивості НССС McEliece на LDPC-кодах

Таблиця 3

Складність розкодування для досліджуваних ССС в залежності від потужності поля Галуа та швидкості каналу передачі даних

GF^n	Тип ССС											
	1/2 sh LDPC	3/4 sh LDPC	1/2 leng LDPC	3/4 leng LDPC	0.5 leng MEC	0.75 leng MEC	0.5 sh MEC	0.75 sh MEC	0.5 leng HMEC	0.75 leng HMEC	0.5 sh HMEC	0.75 sh HMEC
1	389	350	477	483	78	81	82	96	148	153	1568	1621
2	975	882	1277	1298	456	457	457	556	835	897	6112	9624
3	2883	2478	3888	4024	1024	1168	1280	5127	1240	1307	12283	14817
4	9223	7847	12896	13502	7672	8232	11028	23674	5224	11937	34673	225017
5	31265	26727	45255	47683	21073	42082	78634	277830	12348	25597	95088	1246572
6	111471	95031	164823	174963	103862	281472	760553	5220573	123548	127137	1316373	4383507

Таблиця 4

Складність декодування для досліджуваних ССС в залежності від потужності поля Галуа та швидкості каналу передачі даних

GF^n	Тип ССС											
	1/2 sh LDPC	3/4 sh LDPC	1/2 leng LDPC	3/4 leng LDPC	0.5 leng MEC	0.75 leng MEC	0.5 sh MEC	0.75 sh MEC	0.5 leng HMEC	0.75 leng HMEC	0.5 sh HMEC	0.75 sh HMEC
1	0,217	0,217	0,217	0,217	2,786	2,835	4,122	4,257	1,089	1,864	2,391	3,46
2	0,217	0,217	0,217	0,217	4,978	5,961	6,233	6,781	2,569	3,643	4,108	4,962
3	0,217	0,217	0,217	0,217	7,568	8,12	8,234	9,764	3,57	4,131	5,382	7,623
4	0,217	0,217	0,217	0,217	9,87	12,1	12,647	13,32	4,92	5,817	6,836	8,972
5	0,217	0,217	0,217	0,217	12,017	14,224	14,742	16,892	7,591	8,617	10,13	12,005

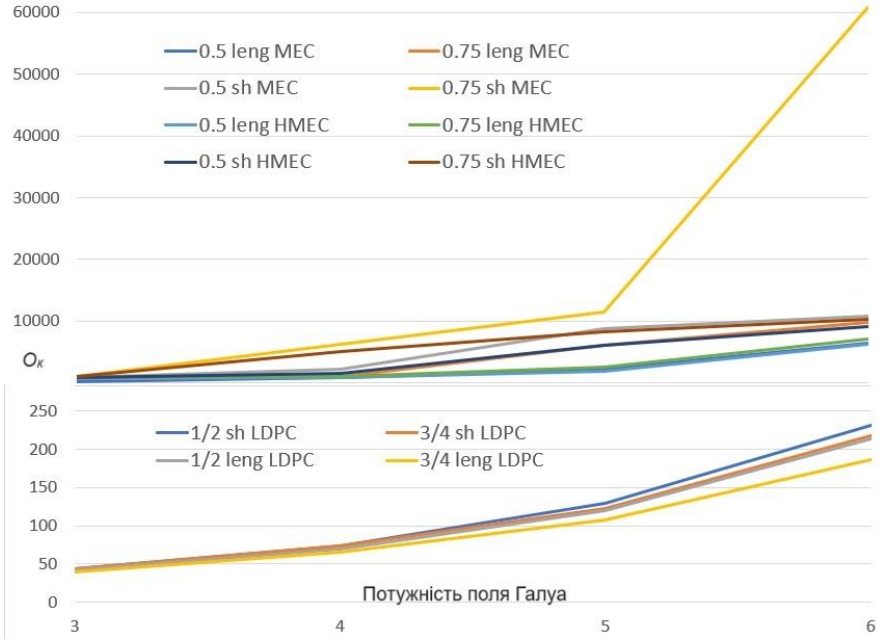

Рис. 4. Складність формування кодограми в залежності від потужності поля Галуа

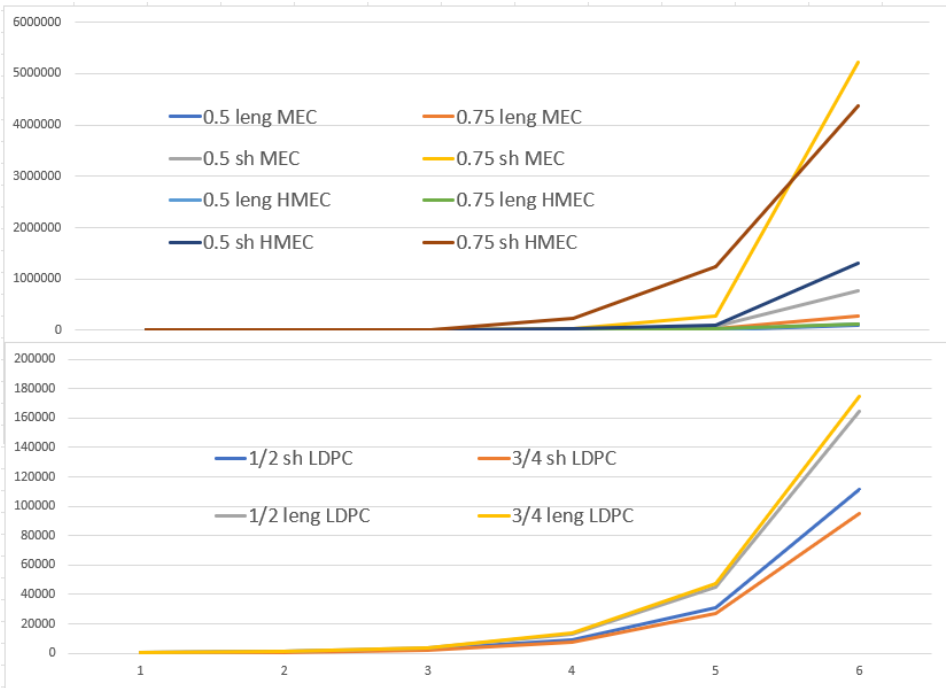

Рис. 5. Складність розкодування в залежності від потужності поля Галуа

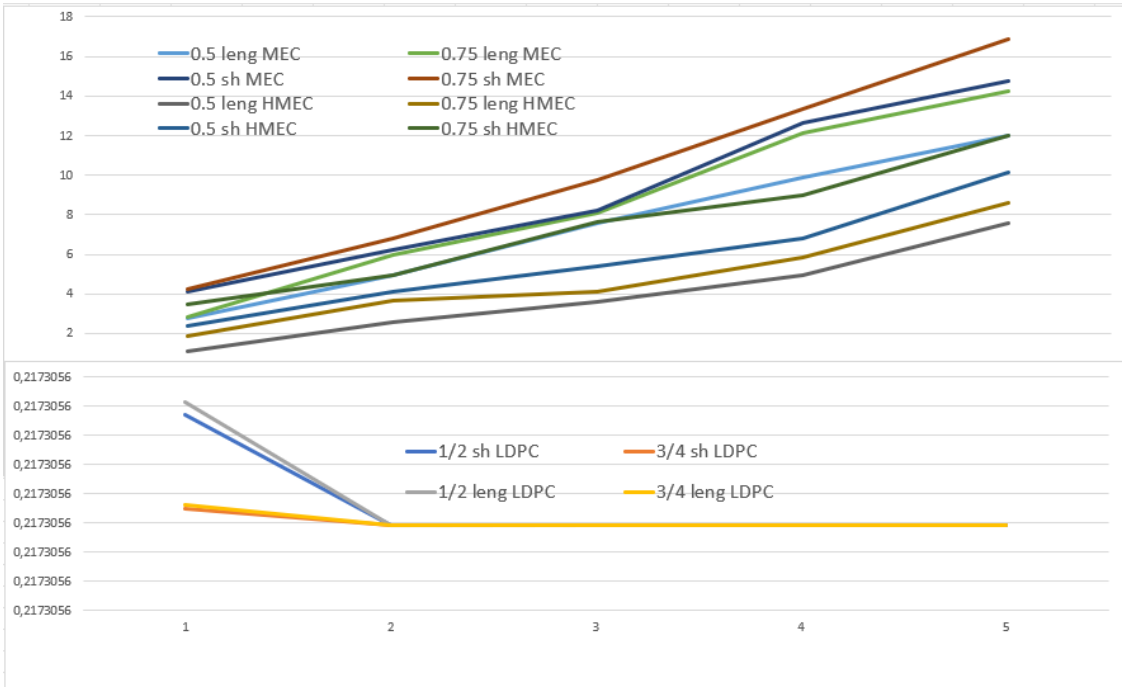

Рис. 6. Складність декодування (зламу) в залежності від потужності поля Галуа

Таблиця 5

Залежність швидкості програмної реалізації від кількості групових операцій (потужності поля)

CCC McEliece	*GF*(q)					
	2^5	2^6	2^7	2^8	2^9	2^{10}
EC	10018042	18048068	32847145	47489784	63215578	82467897
укорочені LDPC	10007947	17787431	28595014	44079433	61974253	79554764
подовжені LDPC	11156138	18561228	33210708	48297112	65171690	84051337

Отримані результати демонструють відносне зниження досліджуваних параметрів для ССС на LDPC-кодах у порівнянні з ССС на МЕС та НМЕС. Це дозволяє використовувати ССС на LDPC-кодах у соціокіберфізичних системах із пристроями з зниженими обчислювальними можливостями та одночасно забезпечити якісне виконання послуг конфіденційності цілісності та автентичності.

Результуюча табл. 5 показує, що кількість групових операцій програмної реалізації ССС залежно від потужності поля у 4,5 рази менша при використанні LDPC. Тож якщо реалізації ССС McEliece у полі $GF(2^{10})$ необхідно $82{,}5\times10^6$ групових операцій, то реалізація ССС на LDPC у полі $GF(2^6)$ вимагає 17,7 – $18{,}6\times10^6$ групових операцій.

У табл. 6 представлені результати досліджень ємнісної характеристики при програмної реалізації від потужності поля при використанні збиткових кіл та побудові гібридних крипто-кодових конструкцій (НССС).

Таблиця 6

Залежність швидкості програмної реалізації кодування від потужності поля
(визначено через кількість групових операцій)

CCC McEliece	*GF(q)*						
	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
укорочені МЕС	8293075	10007947	17787431	28595014	44079433	61974253	79554764
подовжені МЕС	8506422	11156138	18561228	33210708	48297112	65171690	84051337
НССС на подовжених LDPC	5612316	7900315	14892945	25565274	42279183	58963778	76564173
НССС на укорочених LDPC	5942627	7905257	14682411	25595014	42116327	58468143	75474764

При використанні НССС досягнуто суттєвого збільшення швидкодії систем (як мінімум у 20 разів за швидкістю формування криптограми), що дозволяє використовувати ресурсообмежені апаратні пристрої для криптографічного захисту інформації такими системами. Для проведення статистичних досліджень стійкості досліджуваних криптосистем використовувався пакет NIST STS 822 [13].

Результати досліджень представлені у табл. 7.

Аналіз табл. 6 показав, що для ССС на МЕС і для НССС зниження потужності поля Галуа до $GF(2^6)$ і $GF(2^4)$ відповідно, не вплинуло на статистичні характеристики таких ССС, і вони виявилися, як мінімум, не гіршими за традиційні ССС McEliece на $GF(2^{10})$. 100% тестів NIST пройшли усі криптосистеми, причому найкращий результат показала НССС на

укорочених LDPC: 155 із 189 тестів пройдено на рівні 0,99, що складає 82% від усієї кількості тестів. При цьому традиційна ССС McEliece на $GF(2^{10})$ показала результативність 149 тестів на рівні 0,99.

Таблиця 7

Результати досліджень статистичної безпеки

ССС McEliece	Тестування пройшли понад 99% послідовностей, кількість тестів	Тестування пройшли понад 96% послідовностей, кількість тестів	Тестування пройшли менше 96% послідовностей, кількість тестів
ЕС	149 (78,83%)	189 (100%)	0 (0%)
скорочені МЕС	151(79,89%)	189(100%)	0 (0%)
подовжені МЕС	152(80,42%)	189(100%)	0 (0%)
НССС на подовжених LDPC	153 (80,95%)	189 (100%)	0 (0%)
НССС на скорочених LDPC	155 (82%)	189 (100%)	0 (0%)

Висновки. Запропонований математичний апарат дозволяє не тільки отримати різні конструкції LDPC-кодів, а й формувати несиметричні крипто-кодові конструкції, що забезпечують можливість їх використання у постквантовий період.

Запропоновані постквантові алгоритми на основі крипто-кодових конструкцій McEliece забезпечують основні послуги безпеки у межах інфраструктри інтернет-сервісів соціокіберфізичних систем в постквантовий період (появи повномасштабного квантового комп'ютера). Для забезпечення послуг безпеки з урахуванням технологій які використовуються в стандартах бездротових каналів зв'язку, крипто-кодові конструкції побудовані на LDPC-кодах. Розроблені методи побудови гібридних крипто-кодових конструкцій дозволяють зменшити енергоємність криптоперетворень та придатні для забезпечення послуг безпеки в соціокіберфізичних системах.

Список літератури

[1]. Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника, "Основи кібербезпеки", Житомир : ЖНАЕУ, 636 с., 2016.

[2]. Report on Post-Quantum Cryptography // [Online], available: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[3]. A Comprehensive Survey of Prominent Cryptographic Aspects for Securing Communication in Post-Quantum IoT Networks // URL: https://www.sciencedirect.com/science/article/pii/S2542660520300159.

[4]. А. Кузнєцов, А. Пушкарьов, С. Кавун, В. Калашніков. (2016) Несиметричні криптосистеми на основі кодування алгебри: сучасний стан, існуючі протиріччя та перспективи практичного використання на пост-квантовий період. URL: https:// openarchive.nure.ua/handle/document/4642.

[5]. А.А. Кузнєцов, А.І. Пушкарьов, І.І. Сватовський, А.В. Шевцов (2016). Несиметричні криптосистеми на кодах алгебри для постквантового періоду URL: https: // periodicals.karazin.ua/cscs/article/download/7839/9850/.

[6]. О. Кузнецов, А. Пушкарьов, О. Шевцов, Т. Кузнецова (2016) Несиметричне криптографічне перетворення з використанням алгебраїчних блокових кодів URL: https://jrnl.nau.edu.ua/index. php/ZI /article/view/11088/14762.

[7]. Загрози безпеки ядра пакетної мережі 4G // URL: https: // www.ptsecurity.com /ru-ru/ research/ analytics/epc-2017/.

[8]. Уразливості протоколу Diameter у мережах 4G // URL: https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/.

[9]. Guide to LTE Security // URL:csrc.nist.gov /publications/drafts/80 187/sp800_187_draft.pdf.

[10]. H. Niederreiter, "Knapsack-Type Cryptosystems and Algebraic Coding Theory", Probl. Control and Inform. Theory, V.15, p. 19-34, 1986.

[11]. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. Kharkiv: PC TECHNOLOGY CENTER, 2022. 196 p.,

[12]. Pohasii Serhii, Yevseiev Serhii, Zhuchenko Oleksandr, Milov Oleksand, Lysechko Volodymyr, Kovalenko Oleksandr, Kostiak Maryna, Volkov Andrii, Lezik Aleksandr, Susukailo Vitalii. Development of crypto code structures on ldpc-codes. Eastern-European Journal of Enterprise Technologies. 2022. 2/9 (116). pp. 44-59.

[13]. Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. doi: http://doi.org/10.15587/978-617-7319-31-2.

[14]. Yevseiev S. and other Development of Niederreiter hybrid crypto-code structure on flawed codes. Eastern-European Journal of Enterprise Technologies, 1/9 (97). p. 27-37, 2019.

[15]. Yevseiev S., Korol O., Kots H., "Construction of hybrid security systems based on the crypto-code structures and flawed codes", Eastern-European Journal of Enterprise Technologies, 4/9(88), pp. 4-20, 2017.

[16]. Yevseiev S., Kots H., and Liekariev Y., (2016). "Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system", Eastern-European Journal of Enterprise Technologies, 6/4(84), pp. 11-23.

[17]. Yevseiev S., Rzayev, K., Korol, O., Imanova, Z. (2016). Development of McEliece modified asymmetric crypto-code system on elliptic truncated codes. Eastern-European Journal of Enterprise Technologies, 4(9-82), pp. 18-26.

[18]. QC-MDPC-McEliece: A public-key code-based encryption scheme based on quasi-cyclic moderate density parity check codes. URL: https://hal.archives-ouvertes.fr/hal-01095935.

[19]. 3GPP TS 38.212 V15.3.0. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; Multiplexing and channel coding (Release 15).

УДК 336.71:004.056

Milevskyi S., Korol O., Hryschuk O., Laptieva T., Yevseiev S. Crypto-code constructions on LDPC codes properties assessment

Abstract. *The growth of mobile technologies and computing power has significantly expanded the range of digital services and actually outpaced the development of computer technology. This promotes the use of mobile and wireless networks in most areas of smart technologies and supports the further combination of cyberspace with the mobile Internet. However, the lack of security protocols that ensure the confidentiality and integrity of data in the early stages of LTE technology implementation creates conditions for cybercriminals to use mobile Internet channels to conduct APT attacks. With the development and appearance of a full-fledged quantum computer that uses the Shor and Grover algorithms, a significant decrease in the stability of cryptosystems built on the basis of symmetric and asymmetric cryptography, including cryptography on elliptic curves, is possible. In addition, modern cyber threats show signs of synergy and hybridity, and their combination with social engineering methods makes it difficult to implement effective preventive measures. The paper proposes post-quantum cryptosystems based on the McAleese crypto-code scheme, which uses low density parity check codes (LDPC codes). This approach allows for easy integration into wireless networks that comply with IEEE 802.16 and IEEE 802.15.4 standards, as well as LTE technologies, providing an adequate level of protection against modern threats.*

Keywords: *modified McEliece crypto-code constructions, post-quantum era, codes with low density of parity checks.*

Мілевський Станіслав Валерійович, кандидат економічних наук**,** доцент кафедри кібербезпеки Національний технічний університет "Харківський політехнічний інститут", Україна.

Stanislav Milevskyi, candidate of economic sciences, associate professor of the cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Король Ольга Григорівна, кандидат технічних наук, доцент кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна.

Olha Korol, candidate of technical sciences, associate professor of the department of cyber security, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Грищук Ольга Михайлівна, старший науковий співробітник науково-дослідної лабораторії управління інформаційною безпекою науково-дослідного відділу проблем розвитку та впровадження стратегічних комунікацій Інституту стратегічних комунікацій Національного університету оборони України.

Olha Hryschuk, senior researcher of the research laboratory of information security management of the research department of problems of development and implementation of strategic communications of the Institute of Strategic Communications of the National University of Defense of Ukraine.

Лаптєва Тетяна Олександрівна, аспірантка, кафедри кібербезпеки та захисту інформації, факультету інформаційних технологій, Київського національного університету імені Тараса Шевченка.

Tetiana Laptieva, PhD student, Department of Cyber Security and Information Protection, Faculty of Information Technologies, Taras Shevchenko Kyiv National University.

Євсеєв Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна.

Serhii Yevseiev, Doctor of Technical Sciences, Professor, Head of the Department of Cyber Security, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Отримано *12 червня 2024 року,* затверджено редколегією *26 червня 2024 року*