УДК 004.056.523
DOI: 10.31673/2409-7292.2025.041209

Корольов Р. В., Сокол В. Є., Корченко А. О.

РОЗРОБКА МЕТОДУ АВТЕНТИФІКАЦІЇ НА ОСНОВІ МОДИФІКОВАНОЇ СХЕМИ MCELIECE ДЛЯ ЦИФРОВИХ РАДІОСТАНЦІЙ З ПОСТКВАНТОВОЮ СТІЙКІСТЮ

У сучасних транкових радіосистемах, таких як Project 25 (P25), TETRA чи DMR, забезпечення надійної автентифікації є ключовим для захисту від несанкціонованого доступу, імперсонації абонентських пристроїв та крадіжки радіоресурсів. Транкові системи, де канали динамічно виділяються для ефективного групового зв'язку, особливо вразливі до кіберзагроз, включаючи MITM-атаки, replay-атаки та клонування ідентифікаторів (Subscriber Unit ID). Наряду із цим зростає потреба у забезпеченні безпеки при віддаленому управлінні мережевою інфраструктурою та підтримці функцій OTAR (Over-The-Air Rekeying), що підвищує ризик компрометації ключів у разі використання традиційних методів автентифікації. Традиційні методи автентифікації, базовані на симетричних ключах (наприклад, AES у P25 Link Layer Authentication), забезпечують базовий рівень безпеки, але не стійкі до майбутніх загроз, таких як квантові обчислення, які можуть зламати класичну криптографію. Крім того, існуючі рішення часто обмежені апаратними ресурсами абонентських пристроїв. Це знижує ефективність комплексного захисту та гнучкість масштабування мережі. Метою дослідження є розробка методу автентифікації, що інтегрує теоретико-кодові схеми для підвищення криптостійкості в транкових мережах. Запропонований метод базується на модифікації challenge-response протоколу з використанням модифікованої теоретико-кодової схеми McEliece. Використання цього методу дозволяє поєднувати високу стійкість до атак із квантових комп’ютерів та оптимізоване використання обчислювальних ресурсів. Запропонована схема забезпечує безпеку, ґрунтуючись на NP-складній проблемі декодування синдрому, що робить метод стійким до атак на квантових комп'ютерах. Реалізація даного підходу дозволяє створити більш надійні транкові мережі нового покоління з підвищеною кіберстійкістю.

Ключові слова: транкові радіосистеми, автентифікація, теоретико-кодові схеми, post-quantum cryptography, challenge-response, P25, OTAR.

Введення

У наш час швидкий прогрес квантових технологій ставить під сумнів надійність класичних криптографічних методів. Алгоритми RSA (Rivest–Shamir–Adleman) та ECC (Elliptic Curve Cryptography), що спираються на важкі математичні проблеми (розкладання великих чисел на множники та знаходження дискретних логарифмів), виявляються незахищеними перед алгоритмом Шора, який може виконуватися на квантових обчислювальних пристроях [1]. Це створює ризики для механізмів перевірки ідентичності та доступу, які покладаються на електронні підписи та сертифікати.

Швидкий квантовий алгоритм факторизації (розкладу на множники цілого числа) важливий з трьох причин. По-перше, наявність такого алгоритму є відображенням того факту, що квантові комп’ютери по суті своїй є більш ефективними, ніж класичні. По-друге, задача факторизації є цікавою сама по собі, так що будь-який новий алгоритм для її вирішення, чи то класичний, чи то квантовий, представляє інтерес. По-третє, ефективний алгоритм факторизації може бути використаний для зламу криптосистеми RSA з відкритим ключем, яка широко використовується в сучасних інформаційних системах, зокрема, для кодування інформації у всесвітній мережі.

Стійкість асиметричних криптоалгоритмів ґрунтується на так званих односторонніх задачах, тобто на таких математичних задачах, коли пряма функція знаходиться значно швидше за обернену. Найвідомішим прикладом такої задачі є факторизація великих цілих чисел, тобто розкладання їх на прості множники. З математичної практики відомо, що задача розкладання великих цілих чисел на прості множники є проблемою надзвичайної обчислювальної складності. На цій задачі побудований криптоалгоритм RSA. Модуль криптоалгоритму утворюється множенням двох великих простих чисел. Цю операцію виконати не складно. А от обчислити приватний ключ, знаючи публічний, можна лише розклавши модуль на множники. При спробі виконати такі обчислення ми наштовхуємося на задачу надзвичайної обчислювальної складності.

Якщо квантовий алгоритм дозволить значно прискорити ці обчислення, асиметрична криптографія може припинити своє існування. Більше того, йдеться не тільки про RSA, а й про інші асиметричні алгоритми, які квантовий комп’ютер здатен зламати аналогічним чином.

Відмінністю алгоритму Шора порівняно з класичними алгоритмами факторизації є його ймовірнісний характер, оскільки задача факторизації зводиться до задачі знаходження періоду функції. Необхідно також спостерігати за квантовою пам’яттю, що теж призводить до випадкових результатів.

Значення алгоритму Шора полягає в тому, що з його допомогою, використовуючи квантовий комп'ютер з кількома сотнями логічних кубітів, стає можливим злам криптосистем з публічним ключем. Однією з найпопулярніших двоключових криптосистем є RSA. Алгоритм Шора, використовуючи можливості квантових комп'ютерів, здатен виконати факторизацію числа не просто за поліноміальний час, а й ненабагато повільніше за множення цілих чисел.

Постквантова криптографія (PQC) пропонує інноваційні рішення, зокрема ті, що ґрунтуються на принципах перешкодостійкого кодування, і є стійкими до квантових загроз. У цьому аспекті особливо актуальними є вдосконалені криптосистеми типу McEliece. На даний час рівень безпеки системи McEliece залишається на досить високому рівні, незважаючи на десятки задокументованих нападів протягом останніх десятиліть. Початкові параметри McEliece були розраховані на 64 біта, але систему легко модифікувати та зробити актуальною при різних ступенях розвитку комп'ютерної техніки, включаючи квантові комп'ютери.

Криптографічна стійкість системи заснована на двох складних обчислювальних завданнях: вичерпному пошуку по ключовому простору і декодуванню по максимуму правдоподібності. У цій статті розглядається створення способів автентифікації на базі цієї конструкції.

Постановка проблеми

Швидке вдосконалення квантових технологій робить алгоритми RSA (Rivest–Shamir–Adleman) та ECC (Elliptic Curve Cryptography) схильними до зламу. Алгоритм Шора [2], представлений 1994 р., дає змогу квантовим комп’ютерам розв’язувати проблеми, на яких базуються ці алгоритми, за поліноміальний час, тоді як класичні пристрої потребують експоненціальних витрат. Наприклад, злом RSA-2048, що на звичайному комп’ютері може тривати тисячоліття, на квантовому – лише кілька годин. Подібно, ECC стає вразливою через залежність від дискретного логарифму в еліптичних кривих.

Алгоритм Гровера посилює небезпеку, прискорюючи пошукові операції, що впливає на симетричні алгоритми шифрування та хешування, хоча головна загроза для асиметричних методів походить від Шора. Це ставить під удар світову інфраструктуру: банківські мережі, цифрові сертифікати, захищені канали зв’язку та пристрої Інтернету речей, де, за даними NIST, зростання кібератак може спричинити масштабні витоки інформації. Вразливість RSA та ECC перед квантовими атаками диктує необхідність швидкого переходу до постквантових альтернатив, які протистоять цим викликам.

Розробка постквантових механізмів автентифікації, стійких до алгоритмів Шора та Гровера, є вкрай актуальною. Криптосистеми McEliece, побудовані на теорії перешкодостійкого кодування, надають варіант, оскільки їхня міцність залежить від NP-складних завдань декодування, недоступних для квантових методів. Водночас вони потребують удосконалень для покращення продуктивності та подолання слабкостей, як-от складність відновлення породжувальної матриці G за відомою перевірочною матрицею H. Головне завдання – створення гнучких схем, що комбінують алгеброгеометричні коди з генераторами псевдовипадкових послідовностей, для гарантування захисту в умовах квантових ризиків, з урахуванням сумісності з поточною інфраструктурою.

Аналіз останніх досліджень та публікацій

Постквантова криптографія використовує алгоритми, які вважаються безпечними як для класичних, так і в майбутньому квантових атак. Алгоритми на основі решіток,

© Корольов Р. В., Сокол В. Є., Корченко А. О. (2025) Розробка методу автентифікації на основі модифікованої схеми McEliece для цифрових радіостанцій з постквантовою стійкістю. Сучасний захист інформації, 4(64), 90–96. https://doi.org/10.31673/2409-7292.2025.041209

перешкодостійких кодів та хеш-функцій були предметом інтенсивних досліджень Національного інституту стандартів і технологій (NIST) [3].

У 2025 р. алгоритм постквантової криптографії HQC (Hamming Quasi-Cyclic) був обраний як механізм інкапсуляції ключів (KEM-Key Encapsulating Mechanism) [4]. Даний алгоритм базується на квазі-циклічних кодах і призначений для захисту від квантових атак в майбутньому. Його складність зводиться до NP складної задачі декодування випадкового коду. У 2024 р. після публікації стандартів NIST FIPS 203, 204, 205 [5-7] міжнародна організація, яка займається розробкою та стандартизацією технічних протоколів і стандартів для Інтернету (IETF-Internet Engineering Task Force) формалізувала гібридні механізми постквантової криптографії для ключових протоколів TLS 1.3 та SSH [8, 9]. В останніх версіях OpenSSH (10.0+) впроваджено гібридний обмін ключами (KEX) з використанням ML-KEM768X255-19-SHA256. ML-KEM768X255-19-SHA256 представляє собою гібридний алгоритм обміну ключами, він поєднує постквантову схему ML-KEM з класичним ECDH на кривій X25519 та хеш функцію SHA-256 для забезпечення захисту від квантових загроз, таких як алгоритм Шора. Гібридні алгоритми повинні не лише підтримувати нові криптографічні примітиви, але й гарантувати зворотну сумісність.

Мета статті

Метою статті є розробка методу автентифікації на основі модифікованих теоретико-кодових схем McEliece з використанням перешкодостійких кодів.

Результати дослідження

В останні роки функції захисту на канальному рівні (LLS), включаючи автентифікацію канального рівня Link Layer Authentication (LLA) та шифрування канального рівня (LLE), викликають все більший інтерес у виробників та користувачів, які прагнуть посилити безпеку комунікацій.

LLA – це функціональність стандарту Project 25 (P25), призначена для автентифікації абонентських радіостанцій SU (Subscriber Units) у транкінгових радіосистемах. LLA є опціональною, але важливою стратегією для захисту систем місійно-критичного зв'язку від несанкціонованого доступу, крадіжки послуг, перешкоджання чи плутанини у комунікаціях. Вразливості включають моніторинг через сканери (якщо трафік не зашифрований), придбання обладнання онлайн, копіювання системних ключів або дублювання ID радіостанцій за допомогою піратського програмного забезпечення. LLA доповнює інші заходи безпеки, такі як ключі системи, бази даних реєстрації та обмеження програмування, та еволюціонує для протидії нових загроз. Саме тут постає питання застосування постквантових алгоритмів у спеціалізованих мережах, таких як транкінгові мережі стандарту Project25, котрі використовуються в службах громадської безпеки, поліції та рятувальних операціях.

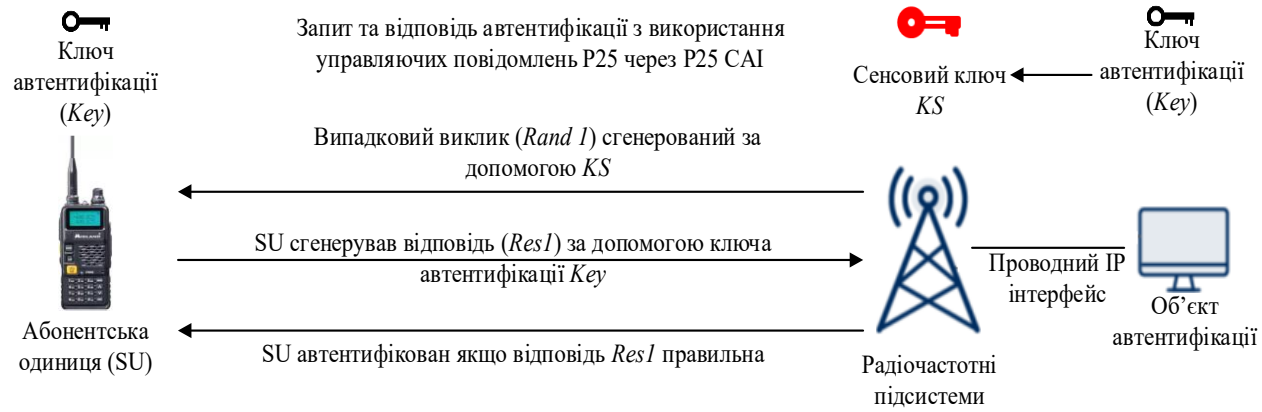

Рис. 1. Автентифікації канального рівня

Служби автентифікації обробляються засобом автентифікації. Залежно від продукту, який пропонує виробник системи, засобом автентифікації може бути локальний сервер або

© Корольов Р. В., Сокол В. Є., Корченко А. О. (2025) Розробка методу автентифікації на основі модифікованої схеми McEliece для цифрових радіостанцій з постквантовою стійкістю. Сучасний захист інформації, 4(64), 90–96. https://doi.org/10.31673/2409-7292.2025.041209

служба додатків, що працює на існуючому пристрої системної інфраструктури. Процес LLA базується на механізмі challenge-response (виклик-відповідь). Він відбувається переважно при початковій реєстрації, але може ініціюватися будь-якої миті через команди автентифікації.

Радіосистема P25 ініціює процес автентифікації, коли SU реєструється в системі. Це робиться шляхом надсилання запиту автентифікації на радіостанцію абонента через радіоінтерфейс. SU повертає відповідь на цей запит, який вимагає знання унікального 128-бітного ключа автентифікації за стандартом розширеного шифрування (AES), який програмується під час початкового налаштування SU. Потім радіосистема порівнює відповідь радіостанції абонента. Якщо вона правильна, автентифікація успішна, і радіостанція абонента вважається дійсною. Якщо автентифікація не вдається, радіостанції абонента відмовляється в доступі до радіосистеми (рис. 1).

Тобто процес автентифікації можна описати виконанням наступних кроків (табл. 1)

Таблиця 1

Процес LLA в транкових системах

Крок	Опис
Реєстрація SU	SU надсилає запит на реєстрацію (unit registration) на контрольний канал, вказуючи свій *ID*. Це відбувається при увімкненні, вході в нову зону або за запитом системи.
Виклик від системи	Автентифікаційний центр генерує випадкове значення (*Rand 1*) і надсилає його SU через Common Air Interface (CAI). У роумінгу виклик передається через Inter-RF Subsystem Interface (ISSI) між підсистемами.
Генерація відповіді	SU обчислює відповідь за допомогою унікального AES-128 ключа *Key* та надсилає її назад *Res1= AES_Encrypt(Rand 1, Key)*. Ключ *Key* не передається — використовується похідний сесійний ключ.
Перевірка відповіді	Система порівнює відповідь *Res 1* з очікуваною (обчисленою на основі збереженого ключа). Якщо збігається — доступ надано; інакше — відмовлено.

В якості основи для розробки методу автентифікації на крипто-кодовій конструкції McEliece обрана Link Layer Authentication [10].

Схематично запропонований метод автентифікації заснований на модифікованій крипто-кодовій конструкції McEliece представлено на рисунку 2.

Тобто запропонований процес автентифікації на модифікованій крипто-кодовій конструкції McEliece можна описати виконанням наступних кроків (табл. 2).

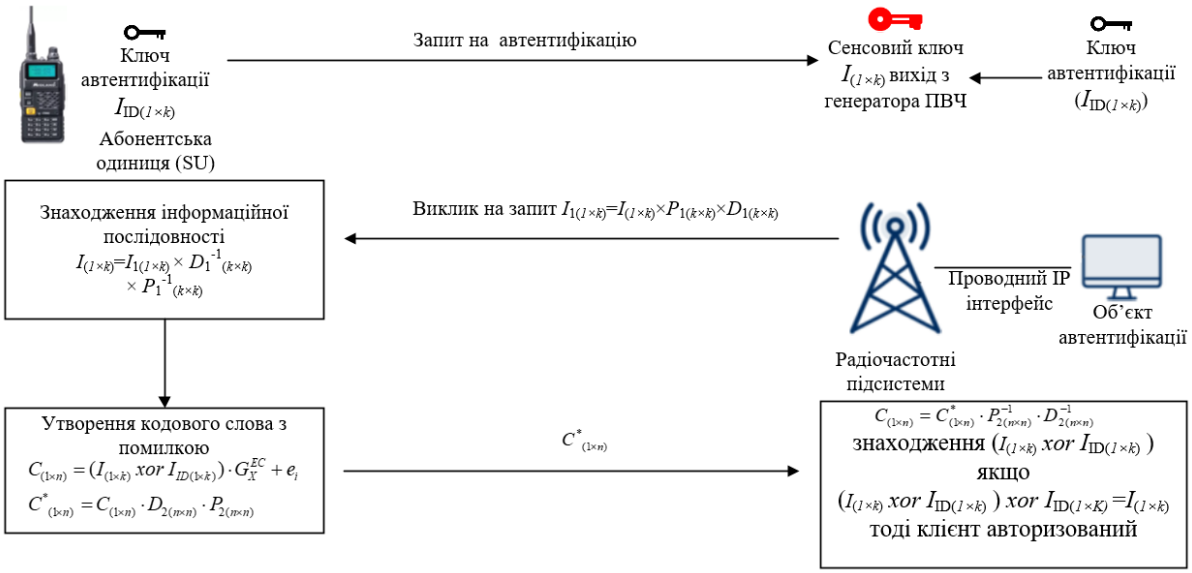

Рис. 2. Метод автентифікації заснований на модифікованій крипто-кодовій конструкції McEliece

© Корольов Р. В., Сокол В. Є., Корченко А. О. (2025) Розробка методу автентифікації на основі модифікованої схеми McEliece для цифрових радіостанцій з постквантовою стійкістю. Сучасний захист інформації, 4(64), 90–96. https://doi.org/10.31673/2409-7292.2025.041209

Таблиця 2

Процес автентифікації на модифікованій крипто-кодовій конструкції McEliece

Крок	Опис
Реєстрація SU	SU надсилає запит на реєстрацію (unit registration) на контрольний канал, вказуючи свій *ID*. Це відбувається при увімкненні, вході в нову зону або за запитом системи.
Виклик від системи	Автентифікаційний центр генерує випадкове значення $I_{1(1\times k)}=I_{(1\times k)}\times P_{1(k\times k)}\times D_{1(k\times k)}$ ($I_{(1\times k)}$ формується за рахунок використання генератора псевдовипадкових чисел) використовуючи секретні перестановочну та діагональну матриці ($P_{1(k\times k)}\times D_{1(k\times k)}$) і надсилає його SU через Common Air Interface (CAI).
Генерація відповіді	SU обчислює відповідь $C^{*}_{(1\times n)}$. $I_{(1\times k)}=I_{1(1\times k)}\times D_1^{-1}{}_{(k\times k)}\times P_1^{-1}{}_{(k\times k)}$ $C_{(1\times n)}=(I_{(1\times k)}\ xor\ I_{ID(1\times k)})\cdot G_X^{EC}+e_i$ $C^{*}_{(1\times n)}=C_{(1\times n)}\cdot D_{2(n\times n)}\cdot P_{2(n\times n)}$
Перевірка відповіді	$C_{(1\times n)}=C^{*}_{(1\times n)}\cdot P^{-1}_{2(n\times n)}\cdot D^{-1}_{2(n\times n)}$ Знаходження ($I_{(1\times k)}\ xor\ I_{\mathrm{ID}(1\times k)}$). Якщо ($I_{(1\times k)}\ xor\ I_{\mathrm{ID}(1\times k)}$) $xor\ I_{\mathrm{ID}(1\times K)}=I_{(1\times k)}$ то SU автентифікований.

Для формування інформаційної послідовності $I_{(1\times k)}$ для запропонованої схеми автентифікації на основі модифікованої крипто-кодової криптосистеми McEliece в статті пропонується використовувати генератори псевдовипадкових чисел на основі регістрів зсуву з лінійним зворотнім зв'язком. Інформаційна послідовність $I_{(1\times k)}$ та $I_{ID(1\times k)}$ представляє собою матрицю яка складається з одного рядка та *k* стовпців в яких знаходяться елементи поля $GF(2^m)$ в залежності від *(n,k,d)* параметрів коду який буде використовуватися в алгоритмі McEliece. Порядок формування інформаційної послідовності $I_{(1\times k)}$ представлено на рисунку 3.

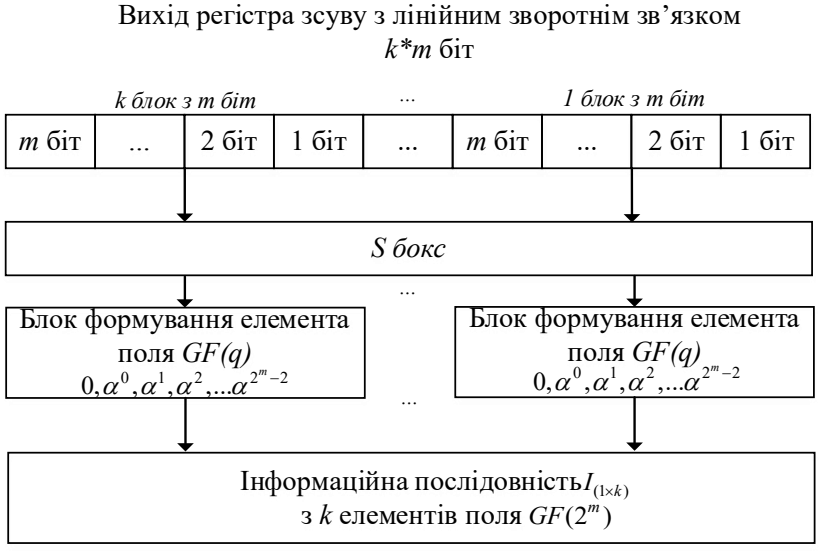

Рис. 3. Схема формування інформаційної послідовності $I_{(1\times k)}$

Схема формування інформаційної послідовності $I_{(1\times k)}$ працює наступним чином. За запитом формується інформаційна послідовність $I_{(1\times k)}$ з виходу генератора псевдовипадкових

чисел на основі регістрів зсуву з лінійним зворотнім зв’язком. Значення регістру зсуву з лінійним зворотнім зв'язком розбивається на блоки по *m* біт (*m* залежіть від параметрів *(n, k, d)* коду. Кількість блоків залежить від виправляючої здатності алгебраїчного *(n, k, d)* коду. Використання S-блоку вносить нелінійне перетворення в процес шифрування, що ускладнює криптоаналіз, зокрема лінійний та диференціальний та реалізує принцип "змішування", запропонований Шенноном, щоб приховати зв’язок між відкритим текстом, шифротекстом та ключем. Робота блока формування елемента поля в самому простому вигляді представлено в таблиці 3.

Далі над сформованою послідовністю $I_{(1\times k)}$ проводяться математичні операції додавання та множення згідно алгоритмів представлених на рисунку 2.

Таблиця 3

Приклад роботи блока формування елемента для поля $GF(2^4)$

Вхідні дані	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Вихідні дані	0	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}

Висновки

Запропоновано метод автентифікації на основі модифікованої крипто-кодової конструкції McEliece, що гарантує постквантову стійкість до атак, зокрема через маскування інформаційної послідовності за допомогою перестановочних та діагональних матриць. Запропоновано алгоритм генерації інформаційної послідовності, який застосовується в запропонованому методі автентифікації. Використання регістрів зсуву з лінійним зворотним зв'язком (LFSR) дозволяє формувати інформаційну послідовність з елементів розширеного поля Галуа, що надалі створює кодове слово для використання в запропонованому методі автентифікації. Запропонований метод, заснований на модифікованій криптосистемі McEliece демонструє стійкість до квантових атак (зокрема алгоритму Шора), на відміну від класичних RSA та ECC, і дозволяє інтегруватися в системи захисту інформації у транкінгових радіосистемах.

Статтю підготовлено в рамках проєкту 2025.06/0047 "Інформаційні технології криптографічного захисту й автентифікації даних для систем мобільного та супутникового зв’язку". Цей проєкт отримав фінансування від Національного фонду досліджень України.

Перелік посилань

1. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography [Електронний ресурс]. CRC Press. Режим доступу: https://cacr.uwaterloo.ca/hac/

2. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (pp. 124–134). IEEE.

3. National Institute of Standards and Technology. (2024). Post-quantum cryptography project [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography

4. Alagic, G., et al. (2025). Status report on the fourth round of the NIST post-quantum cryptography standardization process (NIST IR 8545) [Електронний ресурс]. National Institute of Standards and Technology. Режим доступу: https://csrc.nist.gov/pubs/ir/8545/final

5. National Institute of Standards and Technology. (2024). Module-lattice-based key-encapsulation mechanism standard (ML-KEM) (FIPS PUB 203) [Електронний ресурс]. U.S. Department of Commerce. Режим доступу: https://csrc.nist.gov/pubs/fips/203/final

6. National Institute of Standards and Technology. (2024). Module-lattice-based digital signature standard (ML-DSA) (FIPS PUB 204) [Електронний ресурс]. U.S. Department of Commerce. Режим доступу: https://csrc.nist.gov /pubs/fips/204/final

7. National Institute of Standards and Technology. (2024). Stateless hash-based digital signature standard (SLH-DSA) (FIPS PUB 205) [Електронний ресурс]. U.S. Department of Commerce. Режим доступу: https://csrc.nist.gov/ pubs/fips/205/final.

8. Stebila, D., Fluhrer, S., & Gueron, S. (2025). Hybrid key exchange in Transport Layer Security (TLS) 1.3 (RFC 9650) [Електронний ресурс]. Internet Engineering Task Force. Режим доступу: https://www.rfc-editor.org/rfc/rfc9650

9. M. B., Schinzel, J., Lange, T., & Bernstein, D. J. (2025). Hybrid post-quantum key exchange in Secure Shell (SSH) (RFC 9710) [Електронний ресурс]. Internet Engineering Task Force. Режим доступу: https://www.rfc-editor.org/rfc/rfc9710.

10. Cybersecurity and Infrastructure Security Agency. (2024). Link layer authentication and link layer encryption: Are you really secure? [Електронний ресурс]. Режим доступу: https://www.cisa.gov/sites/default/files/2024-09/24_0828_s-n_LLA_LLE_are_you_really_secure_2022_final_508C.pdf.

Надійшла 14.10.2025

УДК 004.85:330.322
DOI: 10.31673/2409-7292.2025.041210

Криворучко В. Ф., Садовенко В. С.

ІНТЕГРОВАНИЙ ПІДХІД ДО АНАЛІЗУ ІНВЕСТИЦІЙ У ЦИФРОВУ ІНФРАСТРУКТУРУ НА ОСНОВІ КЛАСТЕРИЗАЦІЇ ТА РЕГРЕСІЙНИХ МОДЕЛЕЙ

Стаття присвячена розробці інтегрованого підходу до аналізу інвестицій у цифрову інфраструктуру на основі поєднання алгоритмів кластеризації та методів регресійного моделювання. Актуальність дослідження зумовлена зростаючою роллю цифрової інфраструктури у забезпеченні економічної конкурентоспроможності регіонів та необхідністю оптимізації інвестиційних рішень в умовах обмежених ресурсів. У роботі використано алгоритми K-Means і DBSCAN для сегментації регіонів за показниками цифрової зрілості, рівнем IT-зайнятості, інтернет-покриття та доступності цифрових сервісів. Для кожного отриманого кластера побудовано окрему множинну лінійну регресійну модель, що дає змогу оцінити вплив ключових цифрових факторів на обсяг інвестицій. Якість моделей оцінено за метриками R^2, RMSE та MAE із застосуванням k-fold cross-validation. Інтеграція результатів кластеризації та регресійного аналізу дозволила сформувати матрицю аналітичної оцінки, яка порівнює фактичні та прогнозні інвестиції і визначає пріоритетні напрями інвестиційної політики. Запропонований підхід забезпечує підвищення обґрунтованості управлінських рішень, дозволяє виявляти ефективні та неефективні регіони, а також формувати рекомендації щодо оптимізації фінансування цифрової інфраструктури. Отримані результати можуть бути використані органами влади, аналітичними центрами та ІКТ-компаніями для підтримки стратегічного планування цифрового розвитку.

Ключові слова: цифрова інфраструктура; інвестиції; кластеризація; K-Means; DBSCAN; регресійний аналіз; цифрова економіка; машинне навчання.

Вступ

Цифрова трансформація стала одним із ключових драйверів економічного розвитку у XXI столітті. Розвиток цифрової інфраструктури (телекомунікаційних мереж, дата-центрів, хмарних сервісів, систем кібербезпеки) визначає конкурентоспроможність держави на глобальному ринку. Водночас ефективність інвестицій у цю сферу залишається неоднорідною, що зумовлює необхідність використання нових аналітичних інструментів для підтримки управлінських рішень.

Традиційні економетричні методи аналізу, зокрема класичні моделі регресії або кореляційного аналізу, не завжди здатні адекватно відобразити складні, нелінійні взаємозв’язки між показниками цифрового розвитку та обсягами інвестицій. Натомість алгоритми машинного навчання, особливо методи кластеризації та регресійного аналізу, відкривають можливість для глибшого виявлення закономірностей у багатовимірних економічних даних. Серед сучасних підходів до кластерного аналізу особливе місце посідають алгоритми K-Means і DBSCAN, які дозволяють групувати об’єкти за подібністю характеристик або виділяти аномальні спостереження у даних. Поєднання цих алгоритмів із методами множинної лінійної регресії створює основу для побудови комплексних моделей прогнозування та оптимізації інвестиційних рішень у сфері цифрової інфраструктури.

Актуальність дослідження зумовлена необхідністю підвищення ефективності державних і приватних інвестицій у цифровий сектор, особливо в умовах обмежених ресурсів та швидкої зміни технологічних пріоритетів. Водночас практична реалізація аналітичних підходів, що