функціональності систем аналізу цифрових слідів, що зробило запропоновану модель релевантною для сучасних Smart-кампусів.

Перелік посилань

1. Козубцова, Л., & Козубцов, І. (2024). Поняття і місце smart school в концепції інфраструктури SMART CITY. TTSIIT, 68.

2. Мужанова, Т. М. (2017). «Розумне місто» як інноваційна модель управління. «Економіка. Менеджмент. Бізнес» № 2 (20), 2017. 116-122.

3. Дзюндзюк, К. В. (2023). Публічне управління міським розвитком на засадах концепції розумного міста. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 281, публічне управління та адміністрування. Харківський національний університет імені В.Н. Каразіна, Харків, 2023.

4. Алексов, С. В., & Дідик, А. В. (2023). Перспективи впровадження системи «розумний дім» у заклади освіти. Трансформаційна економіка, (2 (02)), 5-9.

5. Чорненька, Ж. А., Грицюк, М. Я. І., & Бідучак, А. С. (2017). Впровадження SMART–освіти у вищих навчальних закладах. The Scientific Heritage, (11-2 (11)), 63-65.

6. Лахно, В., Волошин, С., Мамченко, С., Кулініч, О., & Касаткін, Д. (2024). Кластерний аналіз для дослідження цифрових слідів студентів закладів освіти. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 31-41.

7. Das, N. (2023). Digital education as an integral part of a smart and intelligent city: a short review. Digital learning based education: transcending physical barriers, 81-96.

8. Liang, H., Ganeshbabu, U., & Thorne, T. (2020). A dynamic Bayesian network approach for analysing topic-sentiment evolution. IEEE Access, 8, 54164-54174.

9. Peralta, A. F., Kertész, J., & Iñiguez, G. (2022). Opinion dynamics in social networks: From models to data. arXiv preprint arXiv:2201.01322.

10. Xu, H., Xu, M., Deng, X., & Wang, B. (2025). Sentiment Diffusion in Online Social Networks: A Survey from the Computational Perspective. ACM Computing Surveys.

11. Mujahid, Muhammad, et al. "Sentiment analysis and topic modeling on tweets about online education during COVID-19." Applied Sciences 11.18 (2021): 8438.

12. El Alaoui, I., Gahi, Y., Messoussi, R., Chaabi, Y., Todoskoff, A., & Kobi, A. (2018). A novel adaptable approach for sentiment analysis on big social data. Journal of Big Data, 5(1), 1-18.

13. Chakraborty, K., Bhatia, S., Bhattacharyya, S., Platos, J., Bag, R., & Hassanien, A. E. (2020). Sentiment Analysis of COVID-19 tweets by Deep Learning Classifiers-A study to show how popularity is affecting accuracy in social media. Applied Soft Computing, 97, 106754.

14. Zhou, Lili. Optimisation design of distance education resource recommendation system based on hierarchical linear model. International Journal of Continuing Engineering Education and Life Long Learning 32.6 (2022): 681-698.

15. Zhou, H., Jiang, S., & Liu, X. (2021). Regression analysis of intelligent education based on linear mixed effect model. Journal of Ambient Intelligence and Humanized Computing, 1-13.

Надійшла до редакції (Received): 20.01.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 004.056.55:004.272
DOI: 10.31673/2409-7292.2026.010544

Єлісєєва Г.С.

ПОСТКВАНТОВА КРИПТОГРАФІЯ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ

Постквантова криптографія є одним із ключових напрямів розвитку сучасних засобів захисту інформації у зв'язку з активним прогресом квантових технологій. Класичні криптографічні алгоритми, такі як RSA та ECC, стають вразливими через алгоритм Шора, що ставить під загрозу довгострокову безпеку інформаційних систем. У статті здійснено поглиблений огляд сучасного стану постквантових криптографічних алгоритмів на основі результатів відбору National Institute of Standards and Technology (NIST), а також проаналізовано підходи, запропоновані в останніх наукових публікаціях. Детально розглянуто характеристики алгоритмів Kyber, Dilithium, Falcon та SPHINCS+ – їхні параметри безпеки, продуктивність, криптостійкість, вимоги до апаратних

© Десятко А.М., Нікітенко Є.В., Гладких В.М. Аналіз цифрових слідів та IoT-поведінкових даних у Smart-кампусі. Сучасний захист інформації, 1(65), 31–38.
https://doi.org/10.31673/2409-7292.2026.010438

ресурсів і можливості застосування у практичних системах. Окрему увагу приділено питанням інтеграції постквантових алгоритмів у наявні криптографічні протоколи, зокрема у системи з відкритим ключем, інфраструктуру відкритих ключів та захищені канали зв'язку. Розглянуто ключові проблеми впровадження постквантової криптографії в інформаційних інфраструктурах, серед яких: збільшені розміри ключів і криптографічних параметрів, обчислювальні затримки, сумісність із наявними програмно-апаратними рішеннями та потреба у перегляді політик управління ключами. Окремо проаналізовано перспективи впровадження постквантових рішень в умовах України, а також запропоновано практичні рекомендації щодо поетапної міграції на такі алгоритми для державних та корпоративних систем з урахуванням вимог до довгострокової конфіденційності даних і захисту критичної інформаційної інфраструктури.

Ключові слова: постквантова криптографія, квантові атаки, NIST PQC, Kyber, Dilithium, Falcon, SPHINCS+, криптостійкість.

Вступ та формулювання проблеми

Стрімкий розвиток квантових технологій протягом останніх років створює суттєві виклики для сучасних криптографічних систем, що широко застосовуються у державних, військових та корпоративних інформаційних інфраструктурах. Класичні алгоритми з відкритим ключем, зокрема RSA, DSA та криптографія на еліптичних кривих, ґрунтуються на складності математичних задач факторизації та дискретного логарифмування, які можуть бути ефективно розв'язані квантовими комп'ютерами за допомогою алгоритму Шора. Це створює загрозу компрометації довгострокових криптографічних механізмів, що наразі забезпечують конфіденційність, автентифікацію та цілісність даних у більшості сучасних протоколів, і дослідники прогнозують необхідність переходу до квантово-стійких рішень задовго до появи масштабних квантових комп'ютерів [16].

У 2022-2024 роках Національний інститут стандартів і технологій США (NIST) завершив багаторічний відбір алгоритмів постквантової криптографії, що визначило глобальний напрям переходу до нових стандартів криптографічного захисту інформації. У зв'язку з цим питання впровадження постквантових алгоритмів, оцінювання їхньої стійкості, продуктивності та сумісності з існуючими інформаційними системами набувають особливої актуальності [5]. Цей перехід є критично важливим і для України, де функціонують значні за обсягом реєстрові, банківські, телекомунікаційні та державні платформи, що покладаються на класичні криптографічні механізми.

Постквантова криптографія розглядається як найбільш реалістичний шлях забезпечення криптостійкості в умовах появи квантових комп'ютерів промислового масштабу. На відміну від квантової криптографії, її впровадження можливе у наявні апаратні та програмні засоби без необхідності повної зміни інфраструктури, що робить її перспективним рішенням для національних та міжнародних інформаційних систем.

З огляду на зазначене, доцільним є всебічний аналіз сучасного стану постквантових криптографічних алгоритмів, визначення їх переваг, обмежень та готовності до практичного застосування. Це дозволить сформувати рекомендації щодо впровадження постквантових рішень у критично важливі інформаційні системи України.

Метою дослідження є аналіз сучасного стану розвитку постквантових криптографічних алгоритмів, які рекомендовані до стандартизації, та оцінювання їхньої придатності до впровадження у практичні інформаційні системи з урахуванням вимог довгострокової криптостійкості.

Для досягнення поставленої мети у роботі сформульовано такі завдання:

1. Проаналізувати загрози, що виникають для класичних криптографічних алгоритмів у разі появи квантових обчислювальних засобів промислового масштабу;

2. Розглянути основні напрями розвитку постквантової криптографії та алгоритми, відібрані в межах проєкту стандартизації NIST;

3. Виконати порівняльний аналіз характеристик базових постквантових алгоритмів (Kyber, Dilithium, Falcon, SPHINCS+) з точки зору рівня безпеки, продуктивності, розмірів криптографічних параметрів та вимог до ресурсів;

© Єлісєєва Г.С. Постквантова криптографія: сучасний стан та перспективи. Сучасний захист інформації, 1(65), 38–46. https://doi.org/10.31673/2409-7292.2026.010544

4. Оцінити особливості інтеграції постквантових алгоритмів у наявні криптографічні протоколи та інфраструктури відкритих ключів;

5. Визначити перспективи застосування постквантових криптографічних рішень у державних та корпоративних інформаційних системах України та сформулювати рекомендації щодо поетапної міграції до постквантових алгоритмів.

Аналіз літератури

Проблематика постквантової криптографії активно досліджується протягом останнього десятиліття, що зумовлено як теоретичним розвитком квантових обчислень, так і практичними ініціативами зі стандартизації нових криптографічних алгоритмів. У межах проєкту NIST Post-Quantum Cryptography Standardization було проведено багаторічний конкурс, у результаті якого відібрано та стандартизовано перші алгоритми, призначені для захисту від квантових атак, зокрема ML-KEM (на основі CRYSTALS-Kyber), ML-DSA (на основі CRYSTALS-Dilithium) та SLH-DSA (на основі SPHINCS+) [1, 2].

У науковій літературі з'явилася низка оглядових робіт, у яких систематизовано підходи до побудови постквантових алгоритмів. У роботах [3, 4, 5, 14] подано класифікацію основних сімейств постквантових схем (ґраткові, кодові, на ізогенії еліптичних кривих, мультиваріантні, хеш-підписні схеми), наведено статистику публікацій за останні роки, а також проаналізовано етапи конкурсу NIST, типові атаки та причини відсіву окремих кандидатів. Зазначені дослідження підкреслюють, що ґраткові схеми наразі є найбільш перспективним напрямом для масового впровадження завдяки поєднанню високого рівня безпеки та прийнятної продуктивності.

Окрему групу становлять праці, присвячені безпосередньо алгоритмам, рекомендованим до стандартизації. У роботах авторів CRYSTALS-Kyber запропоновано модульно-ґратковий механізм узгодження ключів, що ґрунтується на задачі Module-LWE та забезпечує різні рівні безпеки, еквівалентні класичним симетричним схемам AES-128/192/256 [6]. Аналогічно в роботі з описом CRYSTALS-Dilithium розроблено ґраткову схему електронного підпису на основі задачі Module-LWE/Module-SIS із акцентом на простоту реалізації та стійкість до широкого класу атак [7]. Для алгоритму SPHINCS+ проаналізовано властивості stateless-хеш-підписів, орієнтованих на підвищену надійність за рахунок більших розмірів підписів та ключів [3, 5, 18].

Важливий напрям досліджень стосується не лише криптографічних властивостей алгоритмів, а й питань їхньої практичної реалізації. У низці робіт запропоновано оптимізації реалізацій Kyber та Dilithium, зокрема використання спеціалізованих ґраткових кодів, що дозволяють зменшити ймовірність помилок дешифрування та комунікаційні витрати, забезпечуючи при цьому захист від побічних каналів [8]. Паралельно досліджуються особливості інтеграції постквантових схем у існуючі протоколи, такі як TLS, VPN-рішення та інфраструктури відкритих ключів, включаючи гібридні підходи, де класичні та постквантові алгоритми використовуються одночасно [3, 6, 9].

На рівні міжнародних організацій активно розробляються рекомендації щодо переходу до квантово-стійких рішень. У звітах ETSI Industry Specification Group з quantum-safe cryptography окреслено вимоги до алгоритмів, моделі загроз та загальні принципи побудови квантово-стійких протоколів [10]. Європейські та міжнародні ініціативи, такі як проєкти PQCrypto та консультативні документи Єврокомісії, зосереджуються на питаннях стандартизації, інтероперабельності та координації переходу до постквантової криптографії [5]. Окремі аналітичні звіти та рекомендації національних кібербезпекових центрів вказують орієнтовні часові горизонти для завершення міграції на постквантові алгоритми (до 2030-2035 років для критичної інфраструктури) [11, 12].

Разом з тим проведений аналіз показує, що значна частина робіт зосереджена або на теоретичних аспектах побудови постквантових схем, або на їх окремих програмно-апаратних реалізаціях. Питання комплексної оцінки готовності постквантових алгоритмів до впровадження в національні інформаційні системи, а також розроблення рекомендацій щодо

© Єлісєєва Г.С. Постквантова криптографія: сучасний стан та перспективи. Сучасний захист інформації, 1(65), 38–46. https://doi.org/10.31673/2409-7292.2026.010544

поетапної міграції з урахуванням особливостей українських реєстрових, фінансових та державних систем висвітлені недостатньо. Це зумовлює необхідність подальших досліджень, спрямованих на поєднання результатів міжнародної стандартизації з практичними вимогами захисту інформації в Україні.

Квантові загрози для класичних криптосистем

Поява квантових комп'ютерів здатних виконувати обчислення принципово іншого типу, ніж класичні процесори, створює критичні ризики для сучасних криптографічних алгоритмів з відкритим ключем. Більшість таких алгоритмів забезпечують свою стійкість завдяки складності задач факторизації великих чисел та обчисленню дискретного логарифма у мультиплікативних групах або на еліптичних кривих. Однак ці задачі можуть бути ефективно розв'язані на квантовому комп'ютері за допомогою алгоритму Шора [13].

Алгоритм Шора передбачає використання квантового паралелізму та квантового перетворення Фур'є для пошуку періодів функцій, що уможливлює розкладання великих чисел на прості множники за поліноміальний час. Це означає, що криптосистеми RSA, DSA, Diffie-Hellman та криптографія на еліптичних кривих (ECC) стають уразливими за умови наявності квантових обчислювальних засобів достатньої потужності [2; 3]. Такі системи традиційно вважаються базовими у більшості сучасних інформаційних протоколів – TLS, IPsec, SSH, електронному підписі та інфраструктурі відкритих ключів.

Іншим важливим квантовим алгоритмом, що впливає на стійкість криптографічних схем, є алгоритм Гровера. Він забезпечує квадратичне прискорення для задач повного перебору, у тому числі пошуку ключів у симетричних криптосистемах [15]. Попри те, що симетричні алгоритми, такі як AES та SHA-2, не руйнуються повністю, їхній ефективний рівень безпеки зменшується удвічі. Наприклад, AES-256 за наявності квантового комп'ютера забезпечує рівень безпеки, еквівалентний класичному AES-128. Це вимагає перегляду параметрів симетричних схем, подовження ключів та впровадження стійкіших функцій хешування.

Потенційні квантові загрози мають не лише теоретичний характер. У низці досліджень (NIST, ETSI, PQCrypto) зазначається, що поява квантових обчислювачів з кількома тисячами логічних кубітів зробить можливими атаки на RSA-2048 та ECC-256 у часових рамках, прийнятних для зловмисників [5, 6]. Особливо небезпечним є сценарій атаки «записуй зараз - розшифровуй потім» (store now - decrypt later), за якого перехоплені сьогодні зашифровані дані можуть бути розкриті в майбутньому після появи квантових засобів відповідної потужності [7]. Це становить критичний ризик для інформації з довготривалим строком конфіденційності - у тому числі персональних даних, державних реєстрів, медичних записів, фінансових транзакцій і військової інформації.

Таким чином, квантові загрози підривають фундаментальні припущення щодо складності задач, які покладено в основу класичних криптосистем. Розуміння цих загроз створює передумови для переходу до постквантових криптографічних алгоритмів, які ґрунтуються на задачах, що залишаються складними як для класичних, так і для квантових обчислювачів.

Огляд постквантових криптографічних алгоритмів NIST

У 2022-2024 роках Національний інститут стандартів і технологій США (NIST) завершив тривалий процес відбору криптографічних алгоритмів, призначених для заміни класичних схем з відкритим ключем у разі появи квантових обчислювальних засобів промислового масштабу. Результатом стало визначення першої групи стандартів постквантової криптографії – алгоритмів ML-KEM, ML-DSA та SLH-DSA, які ґрунтуються відповідно на схемах CRYSTALS-Kyber, CRYSTALS-Dilithium та SPHINCS+ [1, 2]. Усі три алгоритмічні сімейства забезпечують підвищений рівень криптостійкості та базуються на задачах, вважається складними як для класичних, так і для квантових комп'ютерів.

Алгоритм ML-KEM (CRYSTALS-Kyber)

ML-KEM є механізмом узгодження ключів на основі задачі Module-LWE, що забезпечує стійкість до квантових атак завдяки використанню поліноміальних ґраток. Алгоритм пропонує

© Єлісєєва Г.С. Постквантова криптографія: сучасний стан та перспективи. Сучасний захист інформації, 1(65), 38–46. https://doi.org/10.31673/2409-7292.2026.010544

три рівні безпеки – 512, 768 та 1024, які відповідають симетричним рівням AES-128/192/256 [3]. Основними перевагами Kyber є висока швидкість операцій та порівняно невеликі розміри ключів, що робить його придатним для широкого спектра застосувань, включаючи TLS, VPN, мобільні пристрої та IoT. Результати тестувань свідчать про стабільну ефективність алгоритму навіть на ресурсно-обмежених платформах [4].

Алгоритм ML-DSA (CRYSTALS-Dilithium)

ML-DSA – це схема цифрового підпису, що базується на задачах Module-LWE та Module-SIS. Однією з ключових переваг Dilithium є простота реалізації та високий рівень захисту від широкого класу атак, включно з атаками на побічні канали [5]. Алгоритм пропонує три рівні безпеки, де збалансовано співвідношення між швидкістю реалізації, розміром ключів та обсягом підпису. На відміну від Falcon, Dilithium є оптимізованим для програмних реалізацій і демонструє кращу стабільність параметрів при різних платформах [6].

Алгоритм Falcon

Схема Falcon базується на NTRU-решітках та використовує компактні цифрові підписи, які є одними з найменших серед постквантових алгоритмів [17]. Основною перевагою Falcon є дуже мала довжина підпису та порівняно невеликі ключі, що робить його перспективним для застосувань, де важлива економія пам'яті (смарт-картки, IoT, вбудовані системи). Водночас реалізація Falcon є значно складнішою порівняно з Dilithium: алгоритм потребує високоточного числового представлення, а його програмування та оптимізація є чутливими до побічних каналів та помилок реалізації, що детально проаналізовано в роботі [17].

Алгоритм SLH-DSA (SPHINCS+)

SPHINCS+ є хеш-орієнтованою схемою підпису, яка має унікальну властивість – статична (stateless) структура та повна незалежність від ґраткових задач [9]. Алгоритм забезпечує дуже високий рівень криптостійкості, проте має суттєвий недолік – великі розміри підписів (кілька десятків кілобайт) та ключів. Завдяки хеш-орієнтованому підходу SPHINCS+ розглядається як резервний варіант для систем, де потрібен максимальний рівень безпеки і менша увага приділяється швидкодії або комунікаційним витратам [10].

Порівняльний аналіз алгоритмів

Наведено узагальнені характеристики базових алгоритмів, рекомендованих NIST (табл. 1).

Таблиця 1

Порівняльний аналіз алгоритмів

Алгоритм	Клас задач	Тип	Рівні безпеки	Розмір відкритого ключа	Розмір підпису/ обміну	Продуктивність	Основні сильні сторони
ML-KEM (Kyber)	Module-LWE	KEM	512/768/ 1024	~800-1600 байт	~768-1536 байт	Висока	Швидкість, компактність
ML-DSA (Dilithium)	Module-LWE/SIS	Підпис	2/3/5	1-2 KB	~2-3 KB	Висока	Стабільність, простота
Falcon	NTRU-решітки	Підпис	1/5	~1 KB	~0.7 KB	Висока	Найменші підписи
SPHINCS+	Хеш-функції	Підпис	кілька варіантів	~16 KB	8-30 KB	Низька	Максимальна стійкість

Проблеми та виклики впровадження постквантових алгоритмів

Попри значний прогрес у стандартизації постквантових криптографічних алгоритмів, їх широке практичне впровадження супроводжується низкою технічних, організаційних та інфраструктурних викликів.

Особливості архітектури нових алгоритмів, збільшені криптографічні параметри, потреба у сумісності з наявними протоколами та відсутність єдиного підходу до міграції створюють значні бар'єри для їх масового використання [1. 2].

© Єлісєєва Г.С. Постквантова криптографія: сучасний стан та перспективи. Сучасний захист інформації, 1(65), 38–46. https://doi.org/10.31673/2409-7292.2026.010544

Збільшені розміри ключів та криптографічних параметрів

На відміну від класичних схем RSA чи ECC, постквантові алгоритми характеризуються значно більшими розмірами відкритих і закритих ключів, а також обсягами підписів та зашифрованих повідомлень.

Наприклад, у схемах Dilithium розмір підпису становить декілька кілобайт, що у 50-100 разів більше, ніж у класичних алгоритмів ECDSA [3]. У SPHINCS+ цей показник може сягати 20-30 кілобайт [4].

Такі параметри спричиняють підвищені вимоги до пропускної здатності каналів зв'язку, збільшення часу передавання даних та більші обсяги пам'яті.

Продуктивність та обчислювальні затрати

Хоча ґраткові алгоритми та механізми хеш-підписів можуть забезпечувати прийнятну швидкодію, у деяких сценаріях їх ефективність суттєво поступається класичним аналогам [5]. Обчислення перетворень NTT (Number Theoretic Transform) у ML-KEM та ML-DSA створюють додаткове навантаження на процесор, особливо на вбудованих або енергообмежених пристроях. SPHINCS+ демонструє значно нижчу продуктивність унаслідок великої кількості викликів хеш-функцій, що робить його проблемним для систем з високими вимогами до швидкості формування підписів.

Сумісність із наявними криптографічними протоколами

Більшість сучасних інформаційних систем побудована на класичних алгоритмах відкритого ключа. Інтеграція постквантових механізмів потребує перегляду протоколів TLS, SSH, IPsec, оновлення інфраструктури відкритих ключів (PKI), модифікації форматів сертифікатів і процедур керування ключами [6]. Особливо складною є реалізація гібридних схем, у яких одночасно використовуються класичні та постквантові алгоритми з метою забезпечення плавного переходу. Це збільшує складність реалізацій та створює додаткові ризики помилок.

Захист від атак на побічні канали

Багато PQC-алгоритмів характеризуються залежностями від обчислювальних операцій та арифметичних властивостей, що може зробити їх уразливими до атак типу timing, power analysis або cache-attacks [7]. У реальних умовах для забезпечення коректного рівня захисту необхідні додаткові заходи – маскування, випадковизація, нестандартні арифметичні оптимізації. Це ускладнює впровадження та підвищує вартість реалізацій.

Відсутність довгострокового досвіду застосування

Класичні криптографічні алгоритми використовуються понад три десятиліття, натомість постквантові схеми перебувають на етапі активної стандартизації та тестування. Їхня криптостійкість, хоча й підтверджена поточними дослідженнями, не має такого історичного підґрунтя, як RSA або ECC. Це створює певну невизначеність щодо потенційних нових типів атак, оптимізацій або математичних вразливостей, які можуть бути виявлені у майбутньому [8].

Проблеми міграції у великих інформаційних системах

Перехід до PQC у масштабних організаціях – банках, телеком-компаніях, державних реєстрах - потребує поетапного оновлення ключів, сертифікатів, серверного ПЗ, протоколів та клієнтських застосунків. Значна кількість систем використовує застарілі криптобібліотеки або апаратне прискорення, яке не підтримує PQC. Це створює ризик несумісності та може вимагати повної модернізації інфраструктури [6; 9].

Ризик атаки "записуй зараз – розшифровуй потім"

Цей тип атаки є одним із найбільш небезпечних у контексті появи квантових комп'ютерів. Зловмисники можуть перехоплювати класично зашифровані дані вже сьогодні, зберігати їх протягом тривалого часу та розшифрувати після появи відповідних квантових потужностей [10]. Це особливо критично для державної, військової, медичної та банківської інформації, строк конфіденційності якої може сягати десятиліть.

© Єлісєєва Г.С. Постквантова криптографія: сучасний стан та перспективи. Сучасний захист інформації, 1(65), 38–46. https://doi.org/10.31673/2409-7292.2026.010544

Перспективи впровадження постквантової криптографії в Україні

Впровадження постквантових криптографічних рішень в Україні є стратегічно важливим завданням, оскільки національні інформаційні системи зберігають значні обсяги даних довгострокової критичності, включно з персональною, фінансовою, військовою та державною інформацією. Сучасні криптографічні механізми, які базуються на RSA та ECC, у перспективі стають вразливими до квантових атак, що актуалізує необхідність переходу до алгоритмів, рекомендованих NIST, та їхнього послідовного впровадження в національну інфраструктуру захисту інформації [1, 5].

Одним із ключових напрямів є інтеграція постквантових алгоритмів у державні реєстри та критичні інформаційні системи. Оскільки такі системи обробляють дані з тривалим строком зберігання, вони є особливо чутливими до атаки типу «записуй зараз - розшифровуй потім» [7]. Поступовий перехід до алгоритмів ML-KEM та ML-DSA може забезпечити підвищення рівня захисту як на рівні передавання даних, так і на рівні автентифікації користувачів та сервісів.

Перспективним є також застосування постквантових рішень у фінансовому секторі України. Банківські системи широко використовують інфраструктури відкритих ключів, протоколи TLS та VPN, які потребують модернізації з урахуванням рекомендацій міжнародних організацій, зокрема ETSI та NIST [2]. Особливо актуальним є впровадження гібридних схем шифрування, які поєднують класичні та постквантові алгоритми та дають змогу зменшити ризики на перехідному етапі.

Для телекомунікаційних систем України важливою є можливість масштабного та ефективного розгортання PQC на різноманітних апаратних платформах - від серверного обладнання до IoT-пристроїв. Ґраткові алгоритми, такі як Kyber і Dilithium, вже демонструють достатню продуктивність на пристроях із обмеженими ресурсами, що створює передумови для їхнього застосування у мобільних мережах, державних сервісах та комунікаційних платформах.

Освітні, наукові та промислові установи України також мають потенціал для активного залучення до розробки та тестування практичних реалізацій постквантових алгоритмів. Упровадження відповідних курсів у закладах вищої освіти, підготовка фахівців у сфері криптографії та інформаційної безпеки, а також підтримка наукових досліджень сприятимуть формуванню національної експертизи у цій галузі.

Важливою умовою успішного впровадження постквантової криптографії є формування державної політики та нормативної бази, яка б визначала стандарти використання PQC-алгоритмів, вимоги до протоколів, сертифікації та управління ключами. Координація з європейськими ініціативами та дотримання міжнародних рекомендацій забезпечать сумісність національних рішень із глобальними системами безпеки.

Таким чином, Україна має всі передумови для поетапного переходу до постквантових криптографічних стандартів. З огляду на швидкий розвиток квантових технологій та важливість захисту критично важливих даних, впровадження алгоритмів ML-KEM, ML-DSA та SLH-DSA є не лише бажаним, а й необхідним у контексті забезпечення довгострокової інформаційної безпеки держави.

Висновки

У роботі було розглянуто основні загрози, пов’язані з розвитком квантових обчислювальних технологій, та проаналізовано перспективи переходу до постквантових криптографічних алгоритмів, рекомендованих NIST. Показано, що традиційні криптосистеми з відкритим ключем, зокрема RSA, Diffie-Hellman та криптографія на еліптичних кривих, втрачають стійкість у разі появи квантових комп’ютерів достатньої потужності. Алгоритми Шора та Гровера створюють реальні ризики для безпеки інформації, особливо тієї, що має тривалий строк конфіденційності.

Проаналізовано основні постквантові криптографічні алгоритми – ML-KEM (CRYSTALS-Kyber), ML-DSA (CRYSTALS-Dilithium), Falcon та SLH-DSA (SPHINCS+), які

© Єлісєєва Г.С. Постквантова криптографія: сучасний стан та перспективи. Сучасний захист інформації, 1(65), 38–46. https://doi.org/10.31673/2409-7292.2026.010544

становлять основу першої хвилі міжнародних криптографічних стандартів. Ці алгоритми ґрунтуються на математичних задачах, складність яких зберігається як для класичних, так і для квантових обчислювачів, що дає змогу забезпечити високий рівень захисту в умовах появи нових обчислювальних парадигм.

Розглянуті проблеми та виклики впровадження PQC демонструють, що перехід до нових алгоритмів є складним та багатокомпонентним процесом. Основними бар'єрами виступають великі розміри ключів і підписів, підвищені обчислювальні витрати, необхідність модернізації протоколів та інфраструктури, а також потреба у захисті від атак на побічні канали. Водночас проведені міжнародні дослідження засвідчують реалістичність впровадження PQC у практичні системи за умови поетапної та стандартизованої міграції.

Особливу увагу приділено перспективам впровадження постквантових алгоритмів в Україні. Встановлено, що національні інформаційні ресурси, державні реєстри, банківський сектор та телекомунікації мають високий рівень потреби у переході до алгоритмів ML-KEM та ML-DSA. Україна має усі передумови для адаптації міжнародних стандартів PQC та поступової інтеграції їх у національні системи захисту інформації.

Узагальнюючи, можна стверджувати, що впровадження постквантової криптографії є критично важливим напрямом розвитку сучасних систем інформаційної безпеки. Перехід до PQC повинен здійснюватися системно, з урахуванням міжнародних рекомендацій та національних потреб.

Результати проведеного дослідження можуть бути використані як методологічна основа для подальших робіт, спрямованих на модернізацію криптографічних протоколів, дослідження продуктивності PQC-алгоритмів та розробку вітчизняних рішень у сфері постквантової криптографії.

Перелік посилань

1. NIST. (n.d.). Post-Quantum Cryptography Standardization Project. https://csrc.nist.gov/projects/post-quantum-cryptography.

2. NIST. (2024). NIST releases first 3 finalized post-quantum encryption standards. https://www.nist.gov/news-events.

3. Dam, D. T., Mavroeidis, V., & Vishi, K. (2023). A survey of post-quantum cryptography: Start of a new quantum era. Cryptography, 7(3). https://doi.org/10.3390/cryptography7030040.

4. Kokare, Priyanka & Vora, Deepali & Patil, Shruti & Kotecha, Ketan & Khairnar, Vaishali & Choudhury, Tanupriya & Kulkarni, Ambarish. (2024). Post Quantum Cryptography: A survey of Past and Future. https://www.researchgate.net/publication/382398375_Post_Quantum_Cryptography_A_survey_of_Past_and_Future.

5. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. NIST IR 8105. https://doi.org/10.6028/NIST.IR.8105.

6. Bos, J. W., et al. (2017). CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM. https://pq-crystals.org/kyber/data/kyber-specification-round3.pdf.

7. Ducas, L., et al. (2018). CRYSTALS-Dilithium: Digital Signatures from Module Lattices. https://pq-crystals.org/dilithium/data/dilithium-specification-round3.pdf.

8. Pöppelmann, T., Oder, T., & Güneysu, T. (2015). High-Speed Ideal Lattice-Based Cryptography on 8-bit AVR Microcontrollers. IACR Cryptology ePrint Archive, Report 2015/382. https://eprint.iacr.org/2015/382.pdf.

9. Cloudflare. (2023). Post-Quantum Cryptography Support in TLS and Web Infrastructure. https://blog.cloudflare.com/tag/post-quantum-cryptography/.

10. ETSI. (2020). Quantum-Safe Cryptography – An Overview. https://www.etsi.org/technologies/quantum-safe-cryptography.

11. NCSC UK. (2020). Preparing for Quantum-Safe Cryptography. https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography.

12. Keyfactor & Ponemon Institute. (2023). State of Machine Identity Management Report. Keyfactor, Inc. https://www.keyfactor.com.

13. Shor, P. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science.

14. Bernstein, D., & Lange, T. (2017). Post-Quantum Cryptography. Springer. https://doi.org/10.1007/978-3-540-88702-7.

15. Grover, L. (1996). A fast quantum mechanical algorithm for database search. STOC '96. https://doi.org/10.1145/237814.237866.

16. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723.

© Єлісєєва Г.С. Постквантова криптографія: сучасний стан та перспективи. Сучасний захист інформації, 1(65), 38–46. https://doi.org/10.31673/2409-7292.2026.010544

17. Prest, T. (2020). Efficient implementation issues in Falcon. https://falcon-sign.info.
18. SPHINCS+ Team. (n.d.). SPHINCS+ Specification. https://sphincs.org/data/sphincs+-specification.pdf.

Надійшла до редакції (Received): 22.01.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 004.056:005.6
DOI: 10.31673/2409-7292.2026.010656

Іванченко Є.В., Ковальчук О.А.

АНАЛІЗ МЕТОДИК ТА СТАНДАРТІВ УПРАВЛІННЯ КІБЕРСТІЙКІСТЮ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Проведено комплексний аналіз сучасних міжнародних стандартів та прикладних методологій оцінювання кіберстійкості інформаційних ресурсів (ІР). Визначено, що теоретичним підґрунтям для побудови систем кіберстійкості виступають стандарти ISO/IEC 27001 (системи управління інформаційною безпекою), ISO/IEC 27031 (готовність ІКТ до забезпечення безперервності бізнесу) та спеціальні публікації NIST (Framework for Improving Critical Infrastructure Cybersecurity, SP 800-160), які формують системний підхід, інтегруючи превентивне управління безпекою, відновлення після інцидентів та принципи системної інженерії. Проведено порівняльний аналіз п’яти провідних фреймворків оцінювання: Cyber Resilience Review (CRR), Cyber Assessment Framework (CAF), Cyber Resilience Assessment Framework (C-RAF), Cyber Resilience Index (CRI) та IT Governance Framework. Для порівняння застосовано п’ять критеріїв: наявність числового (індексного) вираження стійкості, фокус оцінки (якісна зрілість чи кількісні показники), динаміка оцінювання (статичний аудит чи тестування), джерела даних та врахування їх адекватності. Виявлено розбіжності між існуючими підходами. Встановлено, що якісні моделі (CRR, CAF) зосереджені на оцінці зрілості процесів («паперова стійкість»), тоді як кількісні моделі (CRI) базуються на метриках часу (MTTD, MTTR), проте часто ігнорують організаційний контекст. Окремо відзначено досвід C-RAF щодо впровадження динамічного тестування (iCAST), який, однак, має вузькогалузеву специфіку. Ключовим результатом дослідження є виявлення критичної наукової прогалини – відсутності в існуючих моделях механізмів перевірки адекватності, повноти та достовірності вхідних даних. Обґрунтовано необхідність розробки механізму, що поєднав би кількісні архітектурні метрики з оцінкою зрілості процесів та коефіцієнтом адекватності вхідних даних.

Ключові слова: кібербезпека, кіберстійкість, кібератака, оцінювання кіберстійкості, NIST CSF, ISO 27001, C-RAF, адекватність даних, модель, метод, методологія, стандарт, інформаційна безпека, механізм оцінювання кіберстійкості.

Вступ

В умовах зростання інтенсивності та складності кібератак, традиційні підходи до інформаційної безпеки, орієнтовані виключно на запобігання інцидентам, стають недостатніми. Актуальним стає перехід до парадигми кіберстійкості (Cyber Resilience) – здатності інформаційного ресурсу (ІР) не лише протистояти загрозам, але й адаптуватися до них та швидко відновлювати функціонування після збоїв.

Теоретичною базою для цього є міжнародні стандарти, такі як ISO/IEC 27001 та NIST CSF, які визначають системний підхід до управління ризиками та безперервністю. Проте, на практиці виникає проблема об'єктивної оцінки реального рівня стійкості. Існуючі методології варіюються від опитувальників зрілості до складних технічних метрик, що ускладнює вибір універсального інструменту.

Мета та постановка задачі

Метою є аналіз існуючих методологій та стандартів управління кіберстійкістю, виявлення їхніх переваг та недоліків. Для досягнення поставленої мети необхідно провести порівняльний аналіз існуючих методологій оцінки кіберстійкості за такими критеріями, як джерела даних, фокус оцінки та наявність механізмів динамічного тестування.

© Єлісєєва Г.С. Постквантова криптографія: сучасний стан та перспективи. Сучасний захист інформації, 1(65), 38–46. https://doi.org/10.31673/2409-7292.2026.010544