DOI
УДК 004.056.55

А.І. Мишеніна [1],
e-mail: aliona.mishenina@gmail.com; orcid.org/0009-0000-4520-2202
І.В. Самойлов [1], канд. техн. наук,
e-mail: samoilov1966igor@gmail.com; orcid.org/0000-0002-8251-9257
А.С. Роскот [2],
e-mail: anastasiia.roskot@ccdcoe.org; orcid.org/0000-0002-8063-4104
М.М. Конотопець[1], канд. техн. наук,
e-mail: egorvetrovsky99@gmail.com; orcid.org/0000-0002-6963-1877
[1] Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут ім. Ігоря Сікорського»
Україна, 03056, Київ, вул. Верхньоключова, 4;
[2] Державний центр кіберзахисту Держспецзв'язку
Україна, 03110, Київ, вул. Солом'янська, 13

Багатокритеріальне оцінювання стандартів постквантового цифрового підпису

Обґрунтовано науково-методичні засади вибору оптимальних стандартів постквантового цифрового підпису в умовах критичної загрози компрометації класичних асиметричних криптосистем квантовими обчисленнями. Показано, що наявність різнорідних міжнародних та національного стандартів створює проблему невизначеності через відсутність єдиної методології їхнього об'єктивного порівняння.

З метою розв'язання цієї проблеми запропоновано комплексну дворівневу систему оціночних критеріїв, яка інтегрує безумовні фільтри криптографічної безпеки зі зваженими експлуатаційними характеристиками. Розроблений математичний апарат ґрунтується на застосуванні методу аналізу ієрархій, що забезпечує кількісне оцінювання технічних параметрів та формалізацію експертних суджень для розрахунку результуючого вектора пріоритетів. Проведено аналітичну оцінку ефективності стандартів, яка показує, що за прийнятих критеріїв, ваг і експертних оцінок для систем державного електронного документообігу та об'єктів критичної інформаційної інфраструктури України ДСТУ 9212:2023 отримує найбільший інтегральний пріоритет порівняно з міжнародними аналогами. Застосування розробленої математичної моделі дозволяє обґрунтовано врахувати ключові фактори прийняття рішень під час міграції на постквантову архітектуру, що сприяє зменшенню ризиків неправильного вибору алгоритму.

Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

К л ю ч о в і с л о в а: постквантова криптографія, цифровий підпис, стандарти постквантових цифрових підписів, багатокритеріальне оцінювання, вектор пріоритетів.

Постановка проблеми. Наразі фундамент глобальної інформаційної безпеки опинився під загрозою через стрімку еволюцію квантових обчислень. Компрометація алгоритмів цифрового підпису матиме миттєві наслідки в реальному часі. В умовах появи нових постквантових стандартів виникає науково-практична проблема їх об'єктивного вибору. Основна складність полягає у відсутності єдиної обґрунтованої системи критеріїв для оцінювання цих алгоритмів. Перехід до постквантової епохи зумовлює те, що архітектура постквантових алгоритмів (що ґрунтуються на решітках та геш-функціях) ставить принципово нові завдання: значне збільшення розмірів криптограм та потреба у виконанні специфічних математичних операцій. Це створює складну абстрактну задачу об'єктивного порівняння різнорідних математичних об'єктів для розбудови квантово-стійкої інфраструктури відкритих ключів.

Аналіз останніх досліджень та публікацій. У фундаментальних працях вітчизняних науковців [1] вже було закладено ефективний підхід до дворівневого оцінювання криптосистем. У ньому застосовувався метод аналізу ієрархій для порівняння стандартів на основі еліптичних кривих із чітким поділом параметрів на безумовні та умовні. Водночас критеріальний апарат, використаний у попередніх дослідженнях, виявився недостатнім для оцінювання сучасних постквантових алгоритмів. Зокрема, у методиці застосовувалися умовні критерії, орієнтовані на класичну криптографію: загальна часова та просторова складність реалізації, а також рівень стійкості до криптоаналітичних атак як умовний параметр. Включення «рівня захищеності» до умовних критеріїв у сучасних реаліях є недоцільним, оскільки будь-який постквантовий кандидат-фіналіст повинен мати абсолютну теоретичну стійкість до класичних атак за замовчуванням. Крім того, для класичних алгоритмів проблема компактності даних та апаратних обмежень не поставала настільки вагомо. Разом з тим, огляд сучасних публікацій свідчить про відсутність єдиного підходу до вибору параметрів для оцінювання постквантових алгоритмів. Так, у роботі [2] оцінювання проводиться через глибокий аналіз показників теоретичної стійкості, складності перетворень та наявності захисту від атак сторонніми каналами. З іншого боку, у роботі [3] порівняльна оцінка CRYSTALS-Dilithium, Falcon та SPHINCS+ здійснюється виключно за базовими експлуатаційними критеріями: розміром ключів і підпису, а також швидкістю генерації та верифікації; у роботі [4] зосереджуються на компромісах між швидкістю, розміром ключа та стійкістю, пропонуючи їх якісне порівняння.

Схожа вузькоспеціалізована спрямованість спостерігається і в сучасних міжнародних дослідженнях [5—8]. Західні науковці здебільшого оцінюють постквантову криптографію ізольовано, залежно від цільового середовища розгортання. Частина досліджень фокусується виключно на апаратних метриках: оцінці вимог до обсягу пам'яті (RAM/ROM), енергоспоживання та площі кристала при імплементації на FPGA/ASIC-архітектурах [9]. Інші публікації аналізуютьвиключно мережевий вплив алгоритмів, досліджуючи час виконання рукостискання, затримки передачі та втрату пакетів через аномально великі розміри постквантових сертифікатів [10].

Як видно з порівняльного аналізу (табл. 1), на відміну від базової методики [1], яка розроблялася для класичних асиметричних систем, запропонований варіант оцінювання з удосконаленою системою критеріїв кардинально переглядає статус критерію «рівень криптографічної стійкості». У класичній криптографії стійкість могла варіюватися і виступати умовним параметром. Для постквантових алгоритмів абсолютна стійкість до класичного та квантового криптоаналізу винесена на рівень безумовного фільтра. Крім того, архітектура PQC вимагає введення принципово нових експлуатаційних критеріїв: «апаратна універсальність» (через вимогу деяких стандартів, як от Falcon, до наявності модулів FPU, що відсутні в більшості мікроконтролерів) та «нормативна довіра» (що є критичним для легітимізації міграції державних систем у постквантову епоху). Просте додавання цих параметрів до моделі [1] є неможливим без руйнування її логічної структури та перерахунку всіх матриць попарних порівнянь.

Попри значний обсяг проведених досліджень, жодна з проаналізованих методик не пропонує комплексного оцінювання, яке б дозволило об'єктивно обрати оптимальний стандарт цифрового підпису для реального впровадження у державні інформаційні системи. Виникає критична необхідність у комплексній моделі, яка здатна збалансовано поєднати експлуатаційні параметри (компактність, обчислювальну ефективність, апаратну універсальність) із жорсткими нормативно-правовими вимогами.

Мета роботи полягає в удосконаленні системи критеріїв, які дозволять провести багатокритеріальне оцінювання постквантових стандартів цифрового підпису.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Розглянути особливості стандартів постквантового цифрового підпису та сформувати комплексну систему критеріїв для їх оцінювання.

2. Дослідити математичний апарат методу аналізу ієрархій.

3. Виконати багатокритеріальне оцінювання стандартів з використанням методу аналізу ієрархій та визначити їхній вектор пріоритетів для систем державного електронного документообігу та об'єктів критичної інформаційної інфраструктури України.

Таблиця 1. **Порівняльний аналіз методик оцінювання криптографічних алгоритмів**

Дослідження	Об'єкт оцінювання	Основні критерії вибору	Обмеження щодо застосування для PQC
Бондаренко М.Ф., Денисенко Б.І., Горбенко Ю.І. [1]	Класичні асиметричні криптосистеми, а саме стандарти електронного цифрового підпису на основі еліптичних кривих	Використовується метод аналізу ієрархій із поділом на безумовні та умовні параметри. Серед ключових умовних критеріїв — загальна часова та просторова складність реалізації алгоритму, а також рівень його стійкості до криптоаналітичних атак	Критерій «рівень захищеності» виступає в ролі умовного, тоді як для постквантових алгоритмів-фіналістів теоретична стійкість має бути абсолютною і розглядатися лише як безумовний фільтр Для класичних алгоритмів не поставала проблема компактності даних та жорстких апаратних обмежень. Відповідно, методика не враховує специфічних для PQC аномально великих розмірів криптограм та специфіки математичних перетворень
Горбенко І.Д., Качко О.Г., Потій О.В, Олексійчук А.М., Горбенко Ю.І. та ін. [2]	Постквантові алгоритми цифрового підпису (зокрема ті, що базуються на алгебраїчних решітках)	Глибокий аналіз показників теоретичної стійкості, складності математичних перетворень та наявності захисту від атак сторонніми (побічними) каналами	Дослідження сфокусовано переважно на математичній та криптографічній надійності алгоритмів. Воно не пропонує комплексної моделі, яка б поєднувала ці технічні показники з практичними експлуатаційними обмеженнями (компактність, апаратна універсальність) та нормативною довірою для впровадження в реальні державні системи
Лаврик І.В. [3], Фесенко А.О., Мирошніченко М.А. [4]	Алгоритми постквантового цифрового підпису (зокрема CRYSTALS-Dilithium, Falcon, SPHINCS+)	Базові експлуатаційні критерії (розмір ключів і підпису, швидкість генерації та верифікації), а також якісне порівняння компромісів між швидкістю, розміром ключа та стійкістю	Вузькоспеціалізована оцінка ізольованих технічних характеристик. Відсутня комплексна модель, яка б збалансовано поєднувала експлуатаційні параметри з жорсткими нормативно-правовими вимогами для реального впровадження у державні системи
Сучасні міжнародні дослідження [5—10]	Постквантова криптографія в ізольованих середовищах розгортання (апаратні FPGA/ASIC-архітектури або мережеві протоколи)	Суто апаратні метрики (вимоги до RAM/ROM, енергоспоживання, площа кристала) або виключно мережевий вплив алгоритмів (час виконання рукостискання, затримки передачі, втрата пакетів)	Оцінювання проводиться ізольовано, залежно від вузького цільового середовища. Не пропонується комплексного підходу, який би дозволив об'єктивно обрати оптимальний стандарт з урахуванням апаратної універсальності та національних регуляторних вимог (легітимності)

Закінчення таблиці

Дослідження	Об’єкт оцінювання	Основні критерії вибору	Обмеження щодо застосування для PQC
Запропонований варіант оцінювання з удосконаленою системою критеріїв	Провідні міжнародні (ML-DSA, Falcon, SLH-DSA) та національний (ДСТУ 9212:2023 «Вершина») стандарти постквантового цифрового підпису	Комплексна дворівнева система: безумовні критерії-фільтри (надійність математичної бази, відсутність слабких ключів, детермінованість часового профілю, легітимність) та зважені умовні характеристики (ефективність обчислень, компактність криптограм, нормативна довіра, апаратна універсальність, гнучкість параметрів). Математичний апарат — метод аналізу ієрархій (MAI) Т. Сааті	Запропонований варіант оцінки повністю адаптований до специфіки перехідного періоду на постквантову архітектуру. Він переводить криптографічну стійкість у статус обов’язкового безумовного фільтра, окремо враховує асиметрію продуктивності й жорсткі апаратні обмеження, а також інтегрує фактор нормативної довіри. Це дозволяє усунути невизначеність і знайти об’єктивний баланс між технічними параметрами та вимогами законодавства при впровадженні PQC у державні інформаційні системи

Виклад основного матеріалу дослідження. Вибір оптимального стандарту критично залежить від середовища його використання, оскільки алгоритми побудовані на різних математичних підходах і мають кардинально різні профілі продуктивності. Для проведення порівняльного аналізу було обрано чотири провідні стандарти постквантового цифрового підпису.

1. ДСТУ 9212:2023 «Вершина»: базується на математичному апараті алгебраїчних решіток із відхилами. Його важливою архітектурною відмінністю є глибока інтеграція з існуючою вітчизняною нормативною базою, зокрема використання стандартизованої геш-функції ДСТУ 7564:2014 «Купина». Це дозволяє мінімізувати залежність від іноземних стандартів гешування та забезпечує використання добре дослідженого вітчизняного примітиву, що відповідає вимогам до суверенітету національної системи захисту інформації [11].

Стійкість алгоритму, описаного в ДСТУ 9212:2023, базується на складності двох задач:

• Learning with Errors (LWE) — знаходження вектора s, якщо відома система рівнянь:

$$As + e \equiv b \bmod q,$$

де A — публічна матриця розміром $k \times l$ (наприклад, 256 × 256), s — вектор приватного ключа, e — вектор помилок (шум), b — вектор, що публічно відомий, q — модуль (зазвичай 8380417).

• Short Integer Solution (SIS) — пошук вектора z, для якого:

$$As \equiv 0 \bmod q,$$

де z має бути «коротким», тобто з координатами в малому діапазоні.

2. ML-DSA (FIPS 204): алгоритм на базі модулярних решіток, що використовує модифіковану схему перетворення Фіата-Шаміра з процедурою відбраковування. Ця інновація скасовує вектор підпису, якщо він перевищує допустимі межі або може розкрити фрагменти секретного ключа. Алгоритм не використовує складних арифметичних дій і оптимізований завдяки швидкому теоретико-числовому перетворенню, що робить його універсальним [12].

Стійкість алгоритму, описаного у FIPS 204, базується на складності двох алгебраїчних задач над кільцями поліномів:

• Module Learning With Errors — знаходження секретних векторів s_1 та s_2, якщо відома система рівнянь:

$$t = As_1 + s_2,$$

де A — публічна матриця поліномів розміром $k \times l$, s_1, s_2 — вектори приватного ключа з малими коефіцієнтами, t — публічно відомий вектор (відкритий ключ), q — модуль.

• Module Short Integer Solution — пошук ненульового вектора z, для якого:

$$As \equiv 0 \bmod q,$$

де z має бути «коротким», тобто його коефіцієнти знаходяться в дуже вузькому діапазоні.

3. Falcon (проєкт FIPS 206): використовує механізм гешування та підпису на базі класу решіток NTRU та використовує механізм «гешування-і-підпис» за схемою GPV. Він генерує надзвичайно короткий вектор підпису завдяки складній процедурі гауссівського семплювання. Проте це вимагає виконання швидкого перетворення Фур'є з числами з рухомою комою. На еталонних процесорних архітектурах (наприклад, x64 з модулем FPU) специфікація Falcon забезпечує детермінований час виконання. Однак, на пристроях з обмеженими ресурсами (смарт-картки без FPU) його безпечна реалізація з постійним часом є вкрай складною та ресурсомісткою, що суттєво обмежує апаратну універсальність алгоритму [13].

Стійкість алгоритму, описаного у проєкті FIPS 206, базується на складності розв'язання задачі пошуку найближчого вектора у решітках NTRU. Математично це зводиться до двох пов'язаних задач:

• NTRU — задача відновлення секретних коротких поліномів f та g за відомим відкритим ключем:

$$h = gf^{-1} \bmod q,$$

де h — відкритий ключ (поліном), f, g — короткі поліноми приватного ключа, що утворюють базис решітки, q — модуль (зазвичай 12289).

• Short Integer Solution (SIS) над решітками NTRU — пошук коротких поліномів s_1 та s_2, що є вектором підпису і задовольняють рівняння:

$$s_1 + s_2 h = c \bmod q,$$

де s_1, s_2 — вектор підпису з надзвичайно малою нормою, c — геш-значення від вхідного повідомлення (точка у багатовимірному просторі).

4. SLH-DSA (FIPS 205): алгоритм на основі геш-функцій, архітектура якого є схемою без збереження стану на базі багаторівневої ієрархії дерев Меркла. Він забезпечує максимально надійний профіль безпеки, покладаючись виключно на криптографічну надійність базової геш-функції (SHA-2 або SHAKE). Недоліком є необхідність додавання великої кількості проміжних геш-значень, що збільшує розмір криптограми до майже 50 кілобайт на найвищих рівнях безпеки, та значне уповільнення процесу підписання [14].

Стійкість алгоритму, описаного у FIPS 205, базується виключно на математичних властивостях геш-функцій (стійкість до колізій, стійкість до знаходження першого та другого прообразів). На відміну від алгоритмів на решітках, SLH-DSA не спирається на складні задачі на кшталт LWE або CVP. Замість цього використовуються три взаємопов'язані криптографічні механізми:

• Winternitz One-Time Signature (WOTS+) — схема одноразового підпису для зв'язування вузлів внутрішніх дерев Меркла;

• Forest of Random Subsets (FORS) — схема підпису на кілька разів (few-time signature), що застосовується безпосередньо для підписання самого гешу повідомлення;

• Hypertree — масивна багаторівнева ієрархія дерев Меркла, яка дозволяє об'єднати величезну кількість одноразових ключів в один загальний відкритий ключ.

Для об'єктивного порівняння основні характеристики алгоритмів зведено у табл. 2.

Для об'єктивного порівняння в табл. 2 для кожного стандарту обрано його найменший (стартовий) стандартизований набір параметрів, оскільки для систем державного документообігу критично важливою є мінімізація розмірів криптограм. Оскільки стандарт FIPS 204 не передбачає набору параметрів для 1-го рівня безпеки NIST, для ML-DSA використано найменший доступний варіант ML-DSA-44 (Рівень 2). Водночас для Falcon та SLH-DSA обрано їхні початкові стандартизовані набори, що відповідають Рівню 1.

Щодо національного стандарту ДСТУ 9212:2023, термін «Базовий рівень» є офіційною назвою набору параметрів згідно з текстом стандарту. За своєю криптографічною стійкістю цей набір забезпечує 128 біт безпеки, що дозволяє математично зіставити його з Рівнем 1 за класифікацією NIST (еквівалент стійкості алгоритму AES-128).

Швидкодія у таблиці 2 наведена у тисячах тактів процесора (кілоциклах, kcycles) для еталонних реалізацій на платформі архітектури x64 (типу Intel Haswell/AVX2) [15]. Для вітчизняного стандарту ДСТУ 9212:2023 наведено розрахункові (апроксимовані) показники швидкодії, зважаючи на його алгебраїчно-решіткову спорідненість з алгоритмом ML-DSA та використання геш-функції «Купина». Водночас слід прямо зазначити, що через відсутність результатів вимірювань на зіставній платформі, ці теоретичні оцінки не є рівноправними з експериментальними даними, наведеними для міжнародних алгоритмів, і використовуються в межах даного дослідження виключно як орієнтовні.

Усю сукупність оціночних критеріїв доцільно розділити на дві великі групи: безумовні (жорсткі фільтри) та умовні (зважені експлуатаційні характеристики).

Безумовні критерії визначають обов'язкові вимоги до алгоритмів. Невідповідність алгоритму хоча б одному з цих параметрів унеможливлює його подальший розгляд. До цієї групи віднесемо:

1. Надійність математичної бази (c_{u_1}). Алгоритм має ґрунтуватися на

досліджених математично складних задачах (наприклад, криптографії на решітках або криптографічних геш-функціях), які доведено є стійкими до

Таблиця 2. **Порівняльна характеристика алгоритмів постквантового цифрового підпису**

Назва алгоритму	Набір параметрів (Рівень безпеки NIST)	Розмір відкритого ключа (ВК)	Розмір приватного ключа (ПК)	Розмір підпису (П)	Швидкість підпису (кілоцикли, kcycles)	Швидкість перевірки (кілоцикли, kcycles)
ДСТУ 9212:2023 «Вершина»	Базовий рівень (Еквівалент рівень 1)	~1472 байти	~3504 байти	~2269 байтів	~1200	~400
ML-DSA (FIPS 204)	ML-DSA-44 (Рівень 2)	1312 байтів	2560 байтів	2420 байтів	1 081	327
Falcon (Проєкт FIPS 206)	Falcon-512 (Рівень 1)	897 байтів	1281 байт	666 байтів	388	82
SLH-DSA (FIPS 205)	SLH-DSA-SHA2-128s (Рівень 1)	32 байти	64 байти	7856 байтів	250 000	2 500

квантового криптоаналізу (алгоритмів Шора та Ґровера) та не мають відомих вразливостей субекспоненційного часу.

2. Відсутність слабких ключів (c_{u_2}). Ця вимога гарантує, що простір ключів алгоритму є однорідним і не містить математичних підмножин, генерування яких може призвести до критичного зниження заявленого рівня безпеки або спростити алгебраїчний криптоаналіз для зловмисника.

3. Теоретична детермінованість часового профілю (c_{u_3}). Алгоритм повинен мати архітектурну можливість базової реалізації з постійним часом виконання на еталонних обчислювальних платформах. Вплив специфічних апаратних обмежень на безпеку не є підставою для безумовної дискваліфікації, а оцінюється на другому рівні ієрархії через зважений критерій «Апаратна універсальність» (c_{c_4}).

4. Легітимність статусу та прозорість технічної документації (c_{u_4}). Алгоритм повинен мати статус затвердженого національного або міжнародного стандарту (наприклад, NIST FIPS, ДСТУ) чи перебувати на фінальному етапі офіційної стандартизації з відкритими та верифікованими специфікаціями.

До умовних критеріїв віднесемо критерії, за якими алгоритми, що успішно пройшли первинний відбір, порівнюються між собою для визначення оптимального балансу характеристик:

1. Ефективність обчислювальних витрат (c_{c_1}). Це комплексний критерій, що оцінює обчислювальну складність алгоритму: швидкість генерації ключової пари, швидкість формування підпису та швидкість його верифікації. Для постквантових стандартів цей критерій є особливо важливим через виражену асиметрію операцій (наприклад, швидка верифікація, але повільне підписування), що є критичним для високонавантажених серверних систем і центрів сертифікації ключів.

2. Компактність ключів та підпису (c_{c_2}). Характеризує сумарний обсяг даних, необхідних для криптографічного перетворення (розмір відкритого ключа, приватного ключа та самого цифрового підпису). Менший розмір зменшує навантаження на канали зв'язку та системи зберігання.

3. Нормативна довіра в Україні (c_{c_3}). Цей критерій визначає ступінь інтегрованості алгоритму в національне правове та технологічне поле. Встановлено, що ключовим фактором впливу на вибір у державному секторі України є саме цей критерій. Абсолютний пріоритет тут надається національним рішенням (ДСТУ).

Слід зазначити, що у запропонованому варіанті оцінювання з удосконаленою системою критеріїв вимога щодо наявності національного стан-

дарту свідомо не була віднесена до групи безумовних критеріїв-фільтрів. Попри те, що для систем державного електронного документообігу застосування сертифікованих вітчизняних рішень є пріоритетним, імплементація міжнародних норм не дозволяє повністю дискваліфікувати міжнародні стандарти на етапі попереднього відбору. Залишення «Нормативної довіри» як умовного критерію з високою вагою, а не жорсткого фільтра, забезпечує математичну гнучкість моделі. Це дозволяє не лише довести перевагу національного стандарту в умовах чинного законодавства, а й зберегти можливість адаптації рейтингу для комерційного або фінансового сектору (шляхом зміни ваг критеріїв без руйнування архітектури моделі).

4. Апаратна універсальність (c_{c_4}). Оцінює вимоги алгоритму до обсягу оперативної пам'яті та здатність функціонувати на пристроях з обмеженими ресурсами (смарт-картки, IoT-датчики). Важливою складовою критерію є незалежність від наявності специфічних математичних співпроцесорів, наприклад, модулів для роботи з рухомою комою (FPU), які відсутні у більшості мікроконтролерів.

5. Гнучкість параметрів (c_{c_5}). Здатність алгоритму масштабуватися та забезпечувати різні рівні криптографічної стійкості виключно шляхом зміни розмірності внутрішніх матриць чи параметрів гешування, без потреби у зміні базової математичної архітектури чи програмної логіки реалізації [1].

Для багатокритеріального оцінювання постквантових стандартів цифрового підпису будемо застосовувати метод аналізу ієрархій, розроблений Томасом Сааті [16, 17]. Цей математичний апарат дозволяє структурувати складну проблему прийняття рішень у вигляді ієрархії та виконати об'єктивне кількісне порівняння якісних показників алгоритмів.

Процес оцінювання базується на побудові матриць попарних порівнянь розмірності $n \times n$, де кожен елемент a_{ij} визначає ступінь переваги об'єкта *i* над об'єктом *j* за фундаментальною шкалою від 1 до 9, де 1 — рівноцінність об'єктів, а 9 — абсолютна перевага одного об'єкта над іншим (табл. 3).

Заповнення матриці відбувається за такими правилами [17]:

1. Якщо об'єкт *i* переважає об'єкт *j*, то клітинка a_{ij} отримує ціле число зі шкали (від 2 до 9), що відображає інтенсивність цієї переваги.

2. Згідно з аксіомою зворотної симетрії Сааті, об'єкт *j* при порівнянні з об'єктом *i* отримує обернене значення $a_{ij} = \frac{1}{a_{ij}}$.

3. Діагональні елементи матриці завжди дорівнюють 1, оскільки об'єкт є абсолютно рівноцінним самому собі.

Таблиця 3. **Фундаментальна шкала абсолютних чисел Т. Сааті**

Інтенсивність важливості	Визначення	Пояснення
1	Однакова важливість	Два об’єкти однаково сприяють досягненню мети
3	Помірна важливість	Досвід та судження незначно сприяють одному об’єкту над іншим
5	Суттєва важливість	Досвід та судження сильно сприяють одному об’єкту над іншим
7	Дуже сильна важливість	Об’єкт має дуже сильну перевагу, його домінування продемонстровано на практиці
9	Абсолютна важливість	Докази на користь одного об’єкта над іншим мають найвищий можливий порядок підтвердження
2, 4, 6, 8	Проміжні значення	Використовуються для компромісних оцінок, коли необхідно зробити вибір між двома сусідніми судженнями
Обернені величини	Зворотне порівняння	Якщо об’єкту *i* при порівнянні з об’єктом *j* присвоєно одне з вищезазначених чисел, то об’єкт *j* у порівнянні з *i* отримує обернене значення

Обчислення вектора локальних пріоритетів (вагових коефіцієнтів) ω_i здійснюється наближеним методом середнього геометричного за формулою

$$q_i = \sqrt[n]{\prod_{j=1}^{n} a_{ij}},$$

де q_i — середнє геометричне *i*-го рядка матриці.

Нормалізація отриманого вектора для приведення суми ваг до одиниці виконується як:

$$\omega_i = \frac{q_i}{\sum_{k=1}^{n} q_k},$$

де $\sum_{k=1}^{n} q_k$ — загальна сума середніх геометричних значень для всіх рядків матриці.

Критично важливим етапом методу аналізу ієрархій є перевірка несуперечливості експертних суджень. Для цього обчислюється максимальне власне значення матриці $\lambda_{\max}$. У строгому математичному поданні воно обчислюється безпосередньо як найбільший дійсний корінь її характеристичного полінома:

$$\det(\lambda I - A) = 0,$$

де I — одинична матриця відповідної розмірності; A — матриця попарних порівнянь.

$$\lambda_{\max} = \sum_{j=1}^{n}\left(\omega_j \sum_{i=1}^{n} a_{ij}\right),$$

де ω_j — j-й елемент нормалізованого вектора пріоритетів (ваговий коефіцієнт, що відповідає j-му стовпцю матриці).

На основі $\lambda_{\max}$ визначається індекс узгодженості (CI) та відношення узгодженості (CR):

$$CI = \frac{\lambda_{\max} - n}{n-1};\ \ CR = \frac{CI}{RI}100\%,$$

де RI — табличне значення випадкового індексу для матриці розмірності n.

Значення випадкового індексу для матриць різного порядку, розраховані Національною лабораторією Оук-Ридж (США) шляхом генерації великої кількості випадкових матриць, наведено нижче [17]:

Розмірність матриці (n)…	1	2	3	4	5	6	7	8	9	10	11	12
Випадковий індекс (RI)…	0	0	0,52	0,89	1,11	1,25	1,35	1,40	1,45	1,49	1,52	1,54

Згідно з методологією Сааті, матриця вважається логічно узгодженою, якщо показник $CR \le 10\%$.

Проведемо практичне використання методу аналізу ієрархій із запропонованою системою критеріїв для багатокритеріального оцінювання стандартів постквантового цифрового підпису.

Першим етапом є оцінка обраних кандидатів (ДСТУ 9212:2023, ML-DSA, SLH-DSA, Falcon) відносно безумовних критеріїв $(c_{u_1} - c_{u_4})$. У контексті побудови систем захисту інформації безумовні критерії виконують функцію жорсткого фільтра: їх невиконання хоча б за одним параметром означає «дискваліфікацію» алгоритму та його виключення з подальшого розгляду. Оцінювання на цьому етапі проводиться за бінарною логікою, де «1» означає повну відповідність вимогам, а «0» — невідповідність (табл. 4).

Аналіз табл. 4 показує, що всі досліджені алгоритми базуються на математично стійких постквантових задачах (теорія решіток та криптографічні геш-функції), не мають слабких ключів, захищені від атак по побічних каналах шляхом реалізації з постійним часом виконання, а також є стандартизованими на національному або міжнародному рівнях. Оскільки всі кандидати успішно пройшли перевірку, множина алгоритмів у повному складі допускається до наступного етапу — зваженого порівняння.

Оскільки офіційні специфікації NIST та ДСТУ для всіх обраних кандидатів передбачають наявність еталонних реалізацій, що математично виключають слабкі ключі та підтримують постійний час обчислень у базо-

вих середовищах, усі алгоритми отримують оцінку «1» за безумовними критеріями c_{u_2} та c_{u_3} (табл. 4).

Таблиця 4. **Результати оцінювання алгоритмів за безумовними критеріями**

Алгоритми	Критерії			
	c_{u_1}	c_{u_2}	c_{u_3}	c_{u_5}
ДСТУ 9212:2023	1	1	1	1
ML-DSA	1	1	1	1
SLH-DSA	1	1	1	1
Falcon	1	1	1	1

Слід зазначити, що отримання всіма чотирма досліджуваними алгоритмами максимальних оцінок в табл. 4 є закономірним, оскільки для аналізу були свідомо відібрані фіналісти міжнародних конкурсів та затверджені стандарти. Проте методологічно наявність безумовних фільтрів є критично необхідною для забезпечення безпеки системи. Головне призначення цього етапу оцінювання — діяти як запобіжник, що унеможливлює «компенсацію» фундаментальних вразливостей високими показниками швидкодії на етапі зваженого порівняння. У реальній практиці цей рівень ефективно відсіює невідповідні рішення. Наприклад, відомі постквантові алгоритми SIKE або Rainbow були б миттєво відхилені на цьому етапі за критерієм надійності математичної бази (c_{u_1}) через виявлені вразливості, а будь-які комерційні криптографічні розробки із закритим кодом були б відсіяні за критерієм легітимізації (c_{u_4}). Таким чином, ця таблиця гарантує, що до етапу пошуку експлуатаційних компромісів допускаються рішення з підтвердженим рівнем теоретичної надійності.

У задачі вибору криптографічного алгоритму умовні критерії мають різний ступінь важливості залежно від специфіки цільового застосування. Для визначення вагових коефіцієнтів за методом Т. Сааті було побудовано матрицю попарних порівнянь розмірності 5×5 для п’яти умовних критеріїв: ефективність (c_{c_1}), компактність (c_{c_2}), нормативна довіра (c_{c_3}), апаратна універсальність (c_{c_4}) та гнучкість параметрів (c_{c_5}). Матриця попарних порівнянь та результати обчислення вектора пріоритетів наведені у табл. 5.

Критично важливим етапом застосування методу аналізу ієрархій є формування вхідних даних. Для визначення значень елементів у матрицях попарних порівнянь (табл. 5—10) було сформовано експертну групу у складі 6 осіб. До неї увійшли автори цього дослідження, а також залучені наукові співробітники та фахівці-практики у сфері криптографічного захисту інформації з досвідом роботи в галузі понад 5 років.

Оцінювання критеріїв та алгоритмів здійснювалося за фундаментальною шкалою Т. Сааті. Для усунення суперечливих суджень та забезпе-

чення високої якості експертизи збір оцінок проводився шляхом колективного обговорення. Експерти аналізували кожен критерій, після чого шляхом відкритої фахової дискусії та ітеративного узгодження оцінок досягали повного консенсусу щодо інтенсивності переваги одного об'єкта над іншим.

Такий підхід дозволив сформувати єдині матриці попарних порівнянь без потреби математичного усереднення індивідуальних оцінок. Отримана внутрішня логічна узгодженість підсумкових матриць додатково підтверджує раціональність та узгодженість прийнятих експертною групою рішень.

У даному дослідженні оцінювання проводиться для вузько визначеного цільового сценарію: розгортання алгоритмів у системах державного сектору та на об'єктах критичної інфраструктури України. Згідно з вимогами законодавства, використання національних стандартизованих рішень, що пройшли державну експертизу, є обов'язковим. Саме тому при формуванні експертних оцінок (табл. 5) критерію «Нормативна довіра» (c_{c_3}) було надано найвищу інтенсивність важливості, що зумовило його домінуючу вагу у 0,3927. Таким чином, модель формалізує вибір оптимального алгоритму в умовах жорстких регуляторних обмежень, де технічні компроміси підпорядковуються легітимності впровадження.

Обчислення вектора пріоритетів виявило, що критерій c_{c_3} «Нормативна довіра» отримав найвищу питому вагу — 0,3927. Це обґрунтовується тим, що для систем державного сектору наявність офіційного національного стандарту є критичною вимогою. Друге місце за важливості розділили фундаментальні технічні критерії: ефективність (c_{c_1}) та компактність (c_{c_2}) з вагою 0,2130 кожен.

Для перевірки логічної узгодженості експертних суджень (табл. 5) було розраховано максимальне власне значення матриці $\lambda_{\max}$. Його об-

Таблиця 5. **Матриця попарних порівнянь та ваги умовних критеріїв**

Критерії	c_{c_1}	c_{c_2}	c_{c_3}	c_{c_4}	c_{c_5}	q_i	ω_i
c_{c_1}	1	1	1/2	3	2	1,2457	0,2130
c_{c_2}	1	1	1/2	3	2	1,2457	0,2130
c_{c_3}	2	2	1	4	4	2,2974	0,3927
c_{c_4}	1/3	1/3	1/4	1	2	0,5610	0,0959
c_{c_5}	1/2	1/2	1/4	1/2	1	0,5000	0,0855

числено безпосередньо як найбільший дійсний корінь характеристичного полінома матриці:

$$\det(\lambda I - A) = \left(\frac{\lambda^2}{2}\right)(2\lambda^3 - 10\lambda^2 - 7) = 0.$$

Найбільший дійсний корінь цього рівняння становить $\lambda_{\max} \approx 5{,}13285$.

Відповідно, індекс узгодженості становить:

$$CI = \frac{5{,}13285 - 5}{4} = 0{,}03321.$$

Відношення узгодженості становить:

$$CR = \frac{0{,}03321}{1{,}11} 100\ \% = 2{,}99\ \%.$$

Оскільки показник CR є значно меншим за гранично допустимі 10 %, матриця вважається ідеально узгодженою.

На фінальному етапі багатокритеріального оцінювання було проведено попарне порівняння чотирьох алгоритмів-кандидатів (ДСТУ 9212:2023, ML-DSA, SLH-DSA, Falcon) відносно кожного з п’яти умовних критеріїв

Таблиця 6. **Матриця попарних порівнянь критерію c_{c_1}**

Алгоритми	ДСТУ 9212:2023	ML-DSA	SLH-DSA	Falcon	q_i	ω_i
ДСТУ 9212:2023	1	1/2	5	3	1,6549	0,3100
ML-DSA	2	1	7	3	2,5457	0,4768
SLH-DSA	1/5	1/7	1	1/5	0,2749	0,0515
Falcon	1/3	1/3	5	1	0,8633	0,1617

Примітка: максимальне власне значення та відношення узгодженості обчислено безпосередньо через характеристичний поліном $CR = 4{,}82\ \%$.

Таблиця 7. **Матриця попарних порівнянь критерію c_{c_2}**

Алгоритми	ДСТУ 9212:2023	ML-DSA	SLH-DSA	Falcon	q_i	ω_i
ДСТУ 9212:2023	1	1	7	1/4	1,1502	0,1922
ML-DSA	1	1	7	1/4	1,1502	0,1922
SLH-DSA	1/7	1/7	1	1/9	0,2182	0,0365
Falcon	4	4	9	1	3,4641	0,5790

Примітка: максимальне власне значення та відношення узгодженості обчислено безпосередньо через характеристичний поліном $CR = 6{,}37\ \%$.

($c_{c_1} - c_{c_5}$). Для цього було побудовано п'ять локальних матриць розмірності 4×4, що надаються далі у вигляді таблиць (табл. 6—10).

Для кожної матриці обчислювався вектор локальних пріоритетів (ω_j) та перевірявся показник відношення узгодженості (*CR*). Для всіх п'яти побудованих матриць значення *CR* не перевищувало допустимий поріг у 10 %.

Зведені результати обчислення локальних пріоритетів (ω_j) алгоритмів за кожним критерієм формують матрицю рішень, яка наведена у табл. 11.

Для визначення найкращого постквантового алгоритму обчислюється результуючий вектор пріоритетів. Підсумковий пріоритет кожного алгоритму розраховується як сума добутків його локальних пріоритетів на відповідні ваги критеріїв.

У матричному вигляді рівняння для розрахунку результуючого вектора пріоритетів має такий вигляд:

$$\begin{pmatrix} 0,3100 & 0,1922 & 0,7013 & 0,3338 & 0,2010 \\ 0,4768 & 0,1922 & 0,1238 & 0,4712 & 0,2010 \\ 0,0515 & 0,0365 & 0,0510 & 0,1409 & 0,5205 \\ 0,1617 & 0,5790 & 0,1238 & 0,0533 & 0,0776 \end{pmatrix} \times$$

$$\times \begin{pmatrix} 0,2130 \\ 0,2130 \\ 0,3927 \\ 0,0959 \\ 0,0855 \end{pmatrix} = \begin{pmatrix} 0,4316 \\ 0,2536 \\ 0,0968 \\ 0,2181 \end{pmatrix},$$

де перша матриця — вектори локальних пріоритетів алгоритмів, другий вектор-стовпець — ваги умовних критеріїв (ω_j), а результуючий вектор — підсумкові оцінки кандидатів.

Значення результуючого вектора пріоритетів у відсотковому вираженні свідчать про таке: ДСТУ 9212:2023 (0,4316) — найкращий, ML-DSA (0,2536) — друге місце, Falcon (0,2181) — третє місце, SLH-DSA (0,0968) — четверте місце.

Аналіз альтернативного цільового сценарію. Для перевірки стійкості отриманого рішення та об'єктивності технічного порівняння було проведено аналіз чутливості моделі. Оскільки високий рейтинг алгоритму ДСТУ 9212:2023 зумовлений передусім вагою критерію легітимності, було змодельовано альтернативний сценарій застосування — для комерційного сектору, де критерій нормативної довіри (c_{c_3}) не є визначальним.

Таблиця 8. **Матриця попарних порівнянь критерію c_{c_3}**

Алгоритми	ДСТУ 9212:2023	ML-DSA	SLH-DSA	Falcon	q_i	ω_i
ДСТУ 9212:2023	1	7	9	7	4,5826	0,7013
ML-DSA	1/7	1	3	1	0,8091	0,1238
SLH-DSA	1/9	1/3	1	1/3	0,3333	0,0510
Falcon	1/7	1	3	1	0,8091	0,1238

Примітка: максимальне власне значення та відношення узгодженості обчислено безпосередньо через характеристичний поліном $CR = 4,02\,\%$.

Таблиця 9. **Матриця попарних порівнянь критерію c_{c_4}**

Алгоритми	ДСТУ 9212:2023	ML-DSA	SLH-DSA	Falcon	q_i	ω_i
ДСТУ 9212:2023	1	½	3	7	1,8001	0,3338
ML-DSA	2	1	3	7	2,5457	0,4721
SLH-DSA	1/3	1/3	1	3	0,7598	0,1409
Falcon	1/7	1/7	1/3	1	0,2872	0,0533

Примітка: максимальне власне значення та відношення узгодженості обчислено безпосередньо через характеристичний поліном $CR = 3,18\,\%$.

Таблиця 10. **Матриця попарних порівнянь критерію c_{c_5}**

Алгоритми	ДСТУ 9212:2023	ML-DSA	SLH-DSA	Falcon	q_i	ω_i
ДСТУ 9212:2023	1	1	1/3	3	1,0000	0,2010
ML-DSA	1	1	1/3	3	1,0000	0,2010
SLH-DSA	3	3	1	5	2,5900	0,5205
Falcon	1/3	1/3	1/5	1	0,3861	0,0776

Примітка: максимальне власне значення та відношення узгодженості обчислено безпосередньо через характеристичний поліном $CR = 1,73\,\%$.

Таблиця 11. **Зведена матриця локальних пріоритетів алгоритмів**

Алгоритми	Критерії				
	c_{c_1}	c_{c_2}	c_{c_3}	c_{c_4}	c_{c_5}
ДСТУ 9212:2023	0,3100	0,1922	0,7013	0,3338	0,2010
ML-DSA	0,4768	0,1922	0,1238	0,4721	0,2010
SLH-DSA	0,0515	0,0365	0,0510	0,1409	0,5205
Falcon	0,1617	0,5790	0,1238	0,0533	0,0776

Після виключення критерію (c_{c_3}) з матриці рішень (табл. 11) та нормування ваг решти суто технічних критеріїв (ефективність, компактність, апаратна універсальність, гнучкість), результуючий вектор пріоритетів набуває принципово іншого вигляду. У суто експлуатаційному середовищі лідерство переходить до міжнародного стандарту ML-DSA (0,3375). На другому місці опиняється Falcon (0,2791) завдяки компактності. Національний стандарт ДСТУ 9212:2023 займає третю позицію (0,2571), а SLH-DSA — четверту (0,1264) через великий розмір криптограм.

Цей аналіз показує, що за прийнятих критеріїв, ваг і експертних оцінок національний стандарт ДСТУ 9212:2023 отримує найбільший інтегральний пріоритет у розглянутому сценарії для державних та критичних інфраструктурних систем. Однак для приватного сектору або міжнародної взаємодії технічно виправданим є перехід на міжнародний стандарт ML-DSA.

Висновки

За результатами дослідження запропоновано удосконалену систему критеріїв, яка комплексно враховує специфічні особливості стандартів постквантового цифрового підпису: їхню математичну архітектуру, експлуатаційні характеристики та рівень легітимності. Завдяки використанню обраних критеріїв та методу аналізу ієрархій Т. Сааті було проведено багатокритеріальне оцінювання постквантових стандартів цифрового підпису для систем державного електронного документообігу та об’єктів критичної інформаційної інфраструктури України. Розрахунок результуючого вектора пріоритетів показав, що найбільш збалансованим рішенням є національний стандарт ДСТУ 9212:2023 із показником пріоритетності 43,16 %, який суттєво випередив міжнародні аналоги ML-DSA (25,36 %) та Falcon (21,81 %). Встановлено, що ключовим фактором впливу на вибір у державному секторі України є критерій «Нормативна довіра», питома вага якого склала 39,2 7%, що виявилося вагомішим за суто технічні показники швидкодії чи компактності.

Напрямом майбутніх досліджень є практичне дослідження ефективності обраних алгоритмів в умовах жорстких обмежень. Зокрема, моделювання виконання алгоритмів на апаратних носіях (смарт-картки, захищені токени), де є суворі обмеження щодо обсягу оперативної пам’яті, енергоспоживання та відсутності спеціалізованих апаратних співпроцесорів. Також доцільним є подальше масштабування розробленої моделі шляхом включення до порівняння наборів параметрів вищих рівнів безпеки за класифікацією NIST, із подальшим поглибленим аналізом чутливості критеріїв для різних сценаріїв застосування поза межами державного сектору.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бондаренко М.Ф., Денисенко Б.І., Горбенко Ю.І. Методика порівняння алгоритмів ЕЦП у групі точок еліптичної кривої. Прикладна радіоелектроніка. 2008. Т. 7, № 3. С. 256—262.
2. Basic principles and results of comparison of electronic signatures properties of the post-quantum period based on algebraic lattices / I. Gorbenko et al. Radiotekhnika. 2021. No. 2 (205). P. 5-21. URL: https://doi.org/10.30837/rt.2021.2.205.01 (date of access: 14.07.2026).
3. Лаврик І. Дослідження алгоритмів постквантового цифрового підпису. Вісник Хмельницького національного університету. Технічні науки. 2024. № 2 (333). С. 56—61. URL: https://doi.org/10.31891/2307-5732-2024-333-2-56 (дата звернення: 14.07.2026).
4. Fesenko A., Myroshnichenko M. Comparison of post-quantum standards in terms of implementation in classical electronic signature algorithms. Information systems and technologies security. 2024. P. 31—38. URL: https://doi.org/10.17721/ISTS.2024.7.31-38 (date of access: 14.07.2026).
5. Birgin B., Celiktas B. From Policy to Practice: A Sector-Agnostic Operational Framework for Post-Quantum Cryptography Transition. IEEE Access. 2026. Vol. 14. P. 33534—335551. URL: https://doi.org/10.1109/ACCESS.2026.3669437 (date of access: 14.07.2026).
6. Gbadebo M.O. Integrating Post-Quantum Cryptography and Advanced Encryption Standards to Safeguard Sensitive Financial Records from Emerging Cyber Threats. Asian Journal of Research in Computer Science. 2025. Vol. 18. P. 1—23. URL: https://doi.org/10.9734/ajrcos/2025/v18i4605 (date of access: 14.07.2026).
7. Quantum Security in Cyber Risk Analysis Through Fuzzy Analytic Hierarchy Process / A. Mahfooz et al. Journal of Information Security and Cybercrimes Research. 2024. Vol. 7. P. 143—155. URL: https://doi.org/10.26735/FWSL8668 (date of access: 14.07.2026).
8. Pandey A.K., Nadeem M. Quantum Software Security. International Journal of Research and Innovation in Social Science (IJRISS). 2026. Vol. 10. P. 6225—6240. URL: https://doi.org/10.47772/IJRISS (date of access: 14.07.2026).
9. High-Speed NTT Accelerator for CRYSTAL-Kyber and CRYSTAL-Dilithium / T.-H. Nguyen et al. IEEE Access. 2024. Vol. 12. P. 34918—34930. ISSN 2169-3536. URL: https://doi.org/10.1109/ACCESS.2024.3371581 (date of access: 14.07.2026).
10. Sikeridis D., Kampanakis P., Devetsikiotis M. Post-Quantum Authentication in TLS 1.3: A Performance Study. Network and Distributed System Security Symposium (NDSS). San Diego, 2020. URL: https://www.ndss-symposium.org/wp-content/uploads/2020/02/ 24203.pdf (date of access: 14.07.2026).
11. ДСТУ 9212:2023. Інформаційні технології. Криптографічний захист інформації. Алгоритм електронного підпису на алгебраїчних решітках із відхилами. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=102150 (дата звернення: 14.07.2026).
12. FIPS 204. Module-Lattice-Based Digital Signature Standard. National Institute of Standards and Technology, 2024. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf (date of access: 14.07.2026).
13. Perlner R. FIPS 206: FN-DSA (Falcon). National Institute of Standards and Technology, 2025. URL: https://csrc.nist.gov/csrc/media/presentations/2025/fips-206-fn-dsa-(falcon)/images-media/fips_206-perlner_2.1.pdf (date of access: 14.07.2026).
14. FIPS 205. Stateless Hash-Based Digital Signature Standard. National Institute of Standards and Technology, 2024. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf (date of access: 14.07.2026).

15. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process / G. Alagic et al. NIST Interagency/Internal Report (NISTIR) 8413. 2022. URL: https://doi.org/10.6028/NIST.IR.8413 (date of access: 14.07.2026).
16. Saaty T.L. The analytic hierarchy process: planning, priority setting, resource allocation. New York : McGraw-Hill, 1980. 287 p.
17. Практикум з теорії прийняття рішень / Л. Козубцова та ін. Київ : ВІТІ, 2025. С. 46—70. URL: https://mitit.mil.gov.ua/api/files/2278 (дата звернення: 14.07.2026).

Стаття надійшла 23.06.2026;
Прорецензована 31.07.2026

REFERENCES

1. Bondarenko, M.F., Denisenko, B.I., & Gorbenko, Yu.I. (2008). A method for comparing digital signature algorithms on a set of points on an elliptic curve. *Applied Radio Electronics, 7*(3), 256-262.
2. Gorbenko, I., Kachko, O., Potii, O., Oleksiychuk, A., Gorbenko, Y., Yesina, M., Stelnyk, I., & Ponomar, V. (2021). Basic principles and results of comparison of electronic signatures properties of the postquantum period based on algebraic lattices. *Radiotekhnika*, (205), 5-21. https://doi.org/10.30837/rt.2021.2.205.01
3. Lavryk, I. (2024). A study of post-quantum digital signature algorithms. *Bulletin of Khmelnytskyi National University. Technical Sciences*, (333), 56-61. https://doi.org/10.31891/2307-5732-2024-333-2-56
4. Fesenko, A., & Myroshnichenko, M. (2024). Comparison of post-quantum standards in terms of implementation in classical electronic signature algorithms. *Information Systems and Technologies Security*, 31–38. https://doi.org/10.17721/ISTS.2024.7.31-38
5. Birgin, B., & Celiktas, B. (2026). From policy to practice: A sector-agnostic operational framework for post-quantum cryptography transition. *IEEE Access, 14*, 33534-335551. https://doi.org/10.1109/ACCESS.2026.3669437
6. Gbadebo, M.O. (2025). Integrating post-quantum cryptography and advanced encryption standards to safeguard sensitive financial records from emerging cyber threats. *Asian Journal of Research in Computer Science, 18*, 1-23. https://doi.org/10.9734/ajrcos/2025/v18i4605
7. Ahmad, M., Fatima, E., Shukla, A., Bhusal, N., Khaliq, M., & Agrawal, A. (2024). Quantum security in cyber risk analysis through fuzzy analytic hierarchy process. *Journal of Information Security and Cybercrimes Research, 7*, 143-155. https://doi.org/10.26735/ FWSL8668
8. Pandey, A.K., & Nadeem, M. (2026). Quantum software security. *International Journal of Research and Innovation in Social* Science (IJRISS), 10, 6225-6240. https://doi.org/10.47772/ IJRISS
9. Nguyen, T.-H., Kieu-Do-Nguyen, B., Pham, C.-K., & Hoang, T.-T. (2024). High-speed NTT accelerator for CRYSTAL-Kyber and CRYSTAL-Dilithium. *IEEE Access, Vol. 12*, 34918-34930. https://doi.org/10.1109/ACCESS.2024.3371581
10. Sikeridis, D., Kampanakis, P., & Devetsikiotis, M. (2020). Post-quantum authentication in TLS 1.3: A performance study. In *Network and Distributed System Security Symposium (*NDSS). https://www.ndss-symposium.org/wp-content/uploads/2020/02/24203.pdf
11. Information technology. Cryptographic protection of information. Algorithm for electronic signatures based on algebraic lattices with deviations (DSTU 9212:2023). (2023). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=102150
12. National Institute of Standards and Technology. (2024). *Module-lattice-based digital signature standard* (FIPS 204). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

13. Perlner, R. (2025). *FIPS 206: FN-DSA (Falcon)*. National Institute of Standards and Technology. https://csrc.nist.gov/csrc/media/presentations/2025/fips-206-fn-dsa-(falcon)/images-media/fips_206-perlner_2.1.pdf
14. National Institute of Standards and Technology. (2024). *Stateless hash-based digital signature standard* (FIPS 205). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf
15. Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022). *Status report on the third round of the NIST post-quantum cryptography standardization process* (NISTIR 8413). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8413
16. Saaty, T.L. (1980). *The analytic hierarchy process: Planning, priority setting, resource allocation*. McGraw-Hill.
17. Kozubtsova, L.M., Beskrovnyi, O.I., Sukhomlynova, O.V., & Soloviova, T.V. (2025). *Practical guide to decision-making theory*. VITI. https://mitit.mil.gov.ua/api/files/2278

Article received 23.06.2026;
Reviewed 31.07.2026

A. Myshenina, I. Samoilov, A. Roskot, M. Konotopets

MULTI-CRITERIA EVALUATION OF POST-QUANTUM DIGITAL SIGNATURE STANDARDS

The scientific and methodological foundations for selecting optimal post-quantum digital signature standards are substantiated in the context of a critical threat of compromise to classical asymmetric cryptosystems posed by quantum computing. It is shown that the existence of diverse international and national standards creates a problem of uncertainty due to the lack of a unified methodology for their objective comparison.

To solve this problem, a comprehensive two-level system of evaluation criteria is proposed, which integrates unconditional cryptographic security filters with weighted operational characteristics. The developed mathematical framework is based on the application of the hierarchical analysis method, which enables the quantitative evaluation of technical parameters and the formalization of expert judgments to calculate the resulting priority vector. An analytical assessment of the standards' effectiveness was conducted, showing that, based on the adopted criteria, weights, and expert evaluations for Ukraine's state electronic document management systems and critical information infrastructure facilities, DSTU 9212:2023 receives the highest overall priority compared to its international counterparts. The application of the developed mathematical model allows for a well-founded consideration of key decision-making factors during migration to a post-quantum architecture, which helps reduce the risks of selecting the wrong algorithm.

K e y w o r d s: post-quantum cryptography, digital signature, post-quantum digital signature standards, multi-criteria evaluation, hierarchy analysis method, priority vector.

МИШЕНІНА Альона Ігорівна, курсант 5-го магістерського курсу Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського». Область наукових досліджень — постквантова криптографія, інформаційна безпека в інформаційно-комунікаційних системах, криптографічні протоколи, кібербезпека та управління ризиками.

САМОЙЛОВ Ігор Володимирович, канд. техн. наук, доцент, доцент Спеціальної кафедри №1 Інституту спеціального зв'язку та захисту інформації «Київський політехнічний інститут ім. Ігоря Сікорського». У 1988 р. закинчив Київське вище інженерне радіотехнічне училище протиповітряної оборони. Область наукових досліджень — криптографічний захист інформації.

РОСКОТ Анастасія Сергіївна, ст. фахівець в області захисту інформації Державного центру кіберзахисту (SCPS SSCIP), наук. співробітник з кібербезпеки Об'єднаного Центру передових технологій з кібероборони НАТО (CCDCOE). У 2021 р. закінчила Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського». Область наукових досліджень — кіберзахист, захист інформації, кіберстійкість, нарощування потенціалу в галузі кібербезпеки, міжнародне кіберспівробітництво, кібернавчання та застосування штучного інтелекту в кібербезпеці.

КОНОТОПЕЦЬ Микола Миколайович, канд. техн. наук, доцент, доцент Спеціальної кафедри №1 Інституту спеціального зв'язку та захисту інформації «Київський політехнічний інститут ім. Ігоря Сікорського». У 1994 р. закінчив Київський інститут Військово-повітряних сил; у 2004 р. — Національну академію оборони України. Область наукових досліджень — інформаційна безпека в інформаційно-комунікаційних системах.