УДК 004.056.55 DOI https://doi.org/10.35546/kntu2078-4481.2026.2.39

М. В. ОНАЙ
кандидат технічних наук, доцент,
доцент кафедри програмного забезпечення комп'ютерних систем
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0000-0002-4938-8355

Я. Ю. ЗГУРОВСЬКИЙ
аспірант кафедри програмного забезпечення комп'ютерних систем
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0009-0006-6087-1643

АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ МЕТОДІВ ТА АРХІТЕКТУРНЕ ПРОЄКТУВАННЯ ПРОГРАМНОЇ СИСТЕМИ ДЛЯ ОЦІНЮВАННЯ ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Ця робота присвячена вирішенню актуальної науково-практичної задачі, що полягає у розробленні алгоритмічного забезпечення методів та проєктуванні деяких компонентів архітектури програмної системи для оцінювання постквантових криптографічних алгоритмів.

Обґрунтовано, що стрімкий розвиток квантових обчислень та теоретична спроможність алгоритму Шора зламувати сучасні асиметричні алгоритми (RSA, ECC) за поліноміальний час створюють критичну загрозу для глобальної цифрової безпеки.

У роботі проаналізовано процес стандартизації постквантової криптографії (PQC), ініційований NIST США, та виокремлено ключові математичні підходи (ґратки, коди, хеш-функції), що лежать в основі нових стандартів FIPS 203, 204 та 205. Виявлено основну проблему переходу на PQC – різноманітність характеристик алгоритмів (розміри ключів, час виконання, використання пам'яті), що унеможливлює існування єдиного універсального рішення та створює проблему вибору для конкретних сценаріїв використання, таких як інтернет речей або високонавантажені серверні системи.

Метою дослідження є розроблення алгоритмічного забезпечення, яке включає математичну модель оцінювання та проєктування компонентів архітектури програмної системи для автоматизованого тестування PQC-алгоритмів у конкретних середовищах виконання.

У ході дослідження розроблено математичну модель багатокритеріального вибору, яка ґрунтується на методах лінійної та інверсної нормалізації метрик і адитивної згортки критеріїв. Модель дозволяє враховувати сукупність факторів: криптографічну стійкість, швидкодію операцій (генерація ключів, інкапсуляція, підпис), просторову ефективність, надійність (ймовірність помилки розшифрування) та стійкість до атак побічними каналами. Також, результатом роботи є компоненти модульної архітектури програмного забезпечення, представлені за допомогою UML-діаграм класів, послідовності та блок-схеми алгоритму. Описано функціонування ключових компонентів. Запропоновано підхід до адаптації оцінювання під специфічні прикладні сценарії шляхом налаштування вагових коефіцієнтів метрик.

Практична цінність результатів полягає у можливості ранжування криптографічних примітивів для вибору оптимального алгоритму, що відповідає обмеженням цільової апаратно-програмної платформи.

У подальшому рекомендується зосередити розвиток дослідження на програмній реалізації на основі запропонованих компонентів архітектури та апробацію на цільових сценаріях.

Ключові слова: *постквантова криптографія, алгоритми, NIST, криптографічна стійкість, інформаційна безпека, стандартизація, програмне забезпечення, інженерія програмного забезпечення, еліптична криптографія.*

M. V. ONAI
PhD, Associate Professor,
Associate Professor at the Department of Computer Systems Software
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
ORCID: 0000-0002-4938-8355

ISSN 2078-4481

YA. YU. ZGHUROVSKYI
Postgraduate Student at the Department of Computer Systems Software
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
ORCID: 0009-0006-6087-1643

ALGORITHMIC SUPPORT OF METHODS AND ARCHITECTURAL DESIGN OF A SOFTWARE SYSTEM FOR EVALUATING POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS

This paper is devoted to solving a pressing scientific and practical problem, which consists in developing algorithmic support for methods and designing certain architectural components of a software system for evaluating post-quantum cryptographic algorithms.

It is substantiated that the rapid development of quantum computing and the theoretical capability of Shor's algorithm to break modern asymmetric algorithms (RSA, ECC) in polynomial time pose a critical threat to global digital security.

The paper analyzes the post-quantum cryptography (PQC) standardization process initiated by the US NIST and highlights the key mathematical approaches (lattices, codes, hash functions) underlying the new FIPS 203, 204, and 205 standards.

The main problem of transitioning to PQC is identified – the diversity of algorithm characteristics (key sizes, execution time, memory usage), which precludes the existence of a single universal solution and creates a selection problem for specific use cases, such as the Internet of Things (IoT) or high-load server systems.

The aim of the study is to develop algorithmic support, which includes a mathematical evaluation model, and to design software architecture components for the automated testing of PQC algorithms in specific execution environments.

During the research, a mathematical model for multi-criteria selection was developed, based on the methods of linear and inverse metric normalization and the additive aggregation of criteria. The model allows taking into account a combination of factors: cryptographic strength, operation speed (key generation, encapsulation, signature), space efficiency, reliability (decryption failure probability), and resistance to side-channel attacks. Furthermore, the results of the work include components of a modular software architecture, represented using UML class and sequence diagrams, as well as an algorithm flowchart. The functioning of key components is described. An approach to adapting the evaluation to specific applied scenarios by tuning metric weight coefficients is proposed.

The practical value of the results lies in the ability to rank cryptographic primitives to select the optimal algorithm that meets the constraints of the target hardware and software platform.

For future work, it is recommended to focus the development of the research on software implementation based on the proposed architectural components and its validation in target scenarios.

Key words: *post-quantum cryptography, algorithms, NIST, cryptographic strength, information security, standardization, software, software engineering, elliptic curve cryptography.*

Постановка проблеми

Сучасна парадигма інформаційної безпеки, що забезпечує захист глобальної цифрової економіки, конфіденційності комунікацій та цілісності даних, ґрунтується на криптографії з відкритим ключем. Фундаментальною основою таких алгоритмів як RSA, Diffie-Hellman та криптографії на еліптичних кривих, є математична складність задач факторизації великих цілих чисел та дискретного логарифмування у скінченних полях або групах точок еліптичних кривих. Протягом десятиліть ці задачі вважалися нерозв'язними за прийнятний час для класичних архітектур фон Неймана. Однак розвиток квантових обчислювальних технологій докорінно змінює ландшафт загроз [1]. Алгоритм Шора, вперше запропонований Пітером Шором у 1994 році, теоретично довів здатність квантового комп'ютера розв'язувати задачі факторизації та дискретного логарифмування за поліноміальний час, що фактично нівелює захист переважної більшості сучасних асиметричних криптосистем [2]. Хоча створення повноцінного квантового комп'ютера, здатного оперувати тисячами логічних кубітів, необхідних для злому ключів актуальних довжин (наприклад, RSA-2048), залишається інженерним викликом, загроза є актуальною вже сьогодні через стратегію «збирай зараз, розшифровуй потім» (Harvest Now, Decrypt Later) [3]. Зловмисники можуть накопичувати зашифрований трафік сьогодні, щоб розшифрувати його в майбутньому, коли відповідні квантові потужності стануть доступними.

Відповіддю на цей виклик є перехід до постквантової криптографії (Post Quantum Cryptography – PQC) – класу криптографічних алгоритмів, які виконуються на класичних комп'ютерах, але базуються на математичних проблемах, що вважаються стійкими до атак як класичних, так і квантових супротивників (наприклад, задачі на ґратках, кодах, ізогеніях, багатовимірних поліномах).

Процес переходу на PQC ускладнюється безпрецедентною різноманітністю математичних підходів та суттєвими відмінностями у технічних характеристиках нових алгоритмів порівняно з класичними аналогами. PQC-алгоритми часто характеризуються значно більшими розмірами ключів або шифротекстів, варіативністю часу виконання, специфічними вимогами до пам'яті та вразливістю до атак побічними каналами (Side-Channel Attacks – SCA). Відсутність єдиного універсального алгоритму, який би перевершував інші за всіма параметрами, створює проблему вибору: для різних сценаріїв (IoT, VPN, блокчейн) оптимальними можуть бути абсолютно різні алгоритми [4].

Таким чином, актуальною науково-практичною задачею є розроблення уніфікованого алгоритмічного забезпечення та проєктування архітектури програмної системи для об'єктивного, комплексного оцінювання PQC-алгоритмів. Такий інструментарій повинен враховувати не лише теоретичну стійкість, а й практичні аспекти реалізації в конкретних апаратних та програмних середовищах, дозволяючи проводити порівняльний аналіз та ранжування алгоритмів.

Аналіз останніх досліджень і публікацій

Аналіз сучасного стану досліджень у галузі постквантової криптографії свідчить про інтенсивну роботу світової наукової спільноти над створенням, аналізом та стандартизацією нових криптографічних примітивів.

Ключовим рушієм у цій сфері є процес стандартизації, ініційований Національним інститутом стандартів і технологій США (NIST) у 2016 році [5]. Цей процес, на відміну від попередніх конкурсів (AES, SHA-3), спрямований на формування портфоліо алгоритмів для забезпечення криптографічної гнучкості (crypto-agility).

Процес пройшов через кілька етапів відбору, кожен з яких супроводжувався детальним криптоаналізом та оцінкою ефективності. У першому раунді [6] було розглянуто 69 кандидатів, що охоплювали широкий спектр математичних підходів (ґратки, коди, ізогенії, мультиваріативні рівняння, хеш-функції). Під час другого раунду в 2019 році [7] кількість кандидатів було зменшено до 26. Фокус змістився на детальний аналіз безпеки та продуктивності на різних архітектурах. Уже в третьому раунді (2020 рік) було визначено фіналістів та альтернативних кандидатів. Результатом цього раунду стало оголошення перших алгоритмів для стандартизації у липні 2022 року [8].

Кульмінацією цього багаторічного процесу стала публікація 13 серпня 2024 року перших трьох фінальних стандартів (FIPS), що знаменує початок ери практичного впровадження PQC [9]. Докладніше розглянемо кожен зі стандартів:

1. FIPS 203 (ML-KEM) – стандарт механізму інкапсуляції ключів, що ґрунтується на алгоритмі CRYSTALS-Kyber. Він використовує математичний апарат модульних ґраток (Module-Lattice) і призначений для захисту сесійних ключів. Його перевагами є висока швидкість роботи та відносно невеликі розміри ключів.
2. FIPS 204 (ML-DSA) – стандарт цифрового підпису, що ґрунтується на алгоритмі CRYSTALS-Dilithium. Також використовує модульні ґратки і є основним стандартом для автентифікації та забезпечення цілісності даних.
3. FIPS 205 (SLH-DSA) – стандарт цифрового підпису на основі хеш-функцій, що ґрунтується на алгоритмі SPHINCS+. Цей алгоритм слугує консервативною альтернативою ґратковим схемам, забезпечуючи захист, що ґрунтується виключно на стійкості хеш-функцій, хоча й ціною більшого розміру підпису та часу виконання.

Незважаючи на публікацію перших стандартів, NIST продовжує роботу над диверсифікацією криптографічного набору для зменшення ризиків, пов'язаних з потенційними вразливостями в математиці ґраток.

Під час четвертого раунду KEM у березні 2025 року було оголошено про вибір алгоритму HQC (Hamming Quasi-Cyclic) для стандартизації як додаткового механізму інкапсуляції ключів (KEM), що ґрунтується на теорії кодів. Алгоритм BIKE залишається у статусі кандидата для подальшого вивчення. Це забезпечує альтернативу ML-KEM на випадок виявлення алгебраїчних вразливостей у ґратках [10].

У жовтні 2024 року NIST оголосив 14 кандидатів, що пройшли до другого раунду процесу оцінювання додаткових схем підпису [11]. Серед них алгоритми на основі кодів (CROSS, LESS), багатовимірних поліномів (MAYO, UOV), ізогеній (SQIsign) та симетричних примітивів (FAEST). Метою є знаходження алгоритмів з короткими підписами або швидкою верифікацією для специфічних застосувань.

Також, аналіз інших публікацій показує, що існують значні прогалини у методології порівняльного оцінювання цих алгоритмів [12, 13], особливо для обмежених середовищ (IoT, вбудовані системи) [14]. Зокрема, дослідження [15- 17] фокусуються на окремих метриках чи середовищах, ігноруючи комплексний вплив на систему, надійність (ймовірність помилок розшифрування) та стійкість до атак побічними каналами.

Формулювання мети дослідження

Метою дослідження є розроблення алгоритмічного забезпечення для методів оцінювання постквантових криптографічних алгоритмів, що включає математичну модель інтегрального оцінювання, а також проєктування деяких компонентів архітектури програмної системи для автоматизованого тестування та оцінювання.

Викладення основного матеріалу дослідження

1. Математична модель

Для вирішення задачі багатокритеріального вибору оптимального алгоритму пропонується математична модель, яка формалізує процес оцінювання PQC-алгоритмів у конкретному середовищі виконання. Модель дозволяє отримати інтегральну оцінку, яка враховує суперечливі вимоги до безпеки, продуктивності та ресурсів.

Нехай маємо множину досліджуваних алгоритмів постквантової криптографії:

$$A = \{A_1, A_2, \ldots, A_n\}, \tag{1}$$

де n – скінченна кількість алгоритмів.

Для кожного алгоритму A_i виконується вимірювання ряду значень ключових характеристик $X_j(A_i)$, та нормалізацію виміряних значень $X_{j,norm}(A_i)$, де X – множина метрик:

$$X = \{X_1, X_2, \ldots, X_m\}, \quad (2)$$

де m – скінченна кількість метрик.

На основі аналізу та вимог NIST, визначено множину ключових метрик, які поділяються на кілька категорій, наприклад:

1. X_1 – криптографічна стійкість (бітова сила, рівні NIST), або кількісна міра стійкості алгоритму до відомих атак. Зазвичай вимірюється у "бітах безпеки" або відповідає категоріям безпеки NIST (рівні 1–5).
2. X_2 – швидкодія (час генерації ключа, інкапсуляції, декапсуляції), що характеризує швидкість виконання криптографічних примітивів. Ця метрика є критичною для систем реального часу. Вона може включати один або кілька показників з переліку: $t_{kg}(A_i)$ – час генерації пари ключів; $t_{enc/sign}(A_i)$ – час інкапсуляції (для KEM) або формування підпису (для DSA); $t_{dec/verify}(A_i)$ – час декапсуляції (для KEM) або перевірки підпису (для DSA).
3. X_3 – просторова ефективність (розмір ключів, шифротекстів, використання пам'яті).
4. X_4 – надійність, що характеризується ймовірністю помилки розшифрування (Decryption Failure Rate – DFR). На відміну від класичних алгоритмів, деякі PQC-схеми (зокрема на ґратках та кодах) мають ненульову ймовірність помилки, коли легітимний користувач не може відновити повідомлення. NIST вимагає DFR < 2^{-128}, але деякі реалізації можуть мати вищі показники.
5. X_5 – стійкість до атак побічними каналами, що характеризується оцінкою захищеності реалізації від атак за часом (timing attacks), енергоспоживанням (power analysis) та електромагнітним випромінюванням. Цей показник часто є якісним (рівень захисту) або кількісним (кількість слідів, необхідних для атаки).

Метрики мають різну розмірність (біти, мілісекунди, байти, ймовірності) та різний вектор оптимізації (для швидкості – "чим менше, тим краще", для стійкості – "чим більше, тим краще"). Для коректного згортання необхідно виконати процедуру нормалізації, що приводить усі значення до діапазону [0, 1]. Нехай $X_j(A_i)$ – виміряне абсолютне значення j-ої метрики для i-го алгоритму. $X_j^{\min}$ та $X_j^{\max}$ – відповідно мінімальне та максимальне значення цієї метрики серед усіх досліджуваних алгоритмів у вибірці A.

Для прямопропорційних метрик (де більше значення є кращим, наприклад, рівень безпеки, або рівень захисту від SCA) формула нормалізації має вигляд:

$$X_{j,\text{norm}}(A_i) = \frac{X_j(A_i) - X_j^{\min}}{X_j^{\max} - X_j^{\min}}. \quad (3)$$

Для обернено пропорційних (де менше значення є кращим, наприклад, час виконання, розмір ключів, DFR) метрик використовується інверсна нормалізація:

$$X_{j,\text{norm}}(A_i) = \frac{X_j^{\max} - X_j(A_i)}{X_j^{\max} - X_j^{\min}}. \quad (4)$$

Після нормалізації, кожна метрика $X_{j,norm}(A_i)$ набуває значення у діапазоні [0, 1].

Застосування лінійної нормалізації дозволяє зберегти відносні пропорції відмінностей між алгоритмами, що є важливим для об'єктивного ранжування.

Для отримання єдиної скалярної оцінки використовується метод адитивної згортки критеріїв з ваговими коефіцієнтами [18]. Це дозволяє гнучко адаптувати модель під конкретний сценарій використання, надаючи пріоритет найбільш критичним характеристикам. Це означає, що інтегральна оцінка $Q(A_i)$ розраховується як зважена сума нормалізованих показників з певними значеннями ваг w_j, які налаштовуються під конкретний сценарій використання і конфігурують пріоритети користувача або системи, що тестується:

$$Q(A_i) = \sum_{j=1}^{m} w_j \cdot X_{j,\text{norm}}(A_i), \quad (5)$$

де

$$\sum_{j=1}^{m} w_j = 1, \quad w_j \geq 0,$$

$i \in \{1,,2 \ldots, n\}$, n – скінченна кількість алгоритмів,

$j \in \{1,,2 \ldots, m\}$, m – скінченна кількість метрик.

Після отриманих оцінок здійснюється ранжування алгоритмів і відповідно серед множини вибраних алгоритмів обирається A^*, який є найбільш підходящим для використання у обраному середовищі з заданими параметрами:

$$A^* = \arg\max_{A_i \in A} Q(A_i). \quad (6)$$

Важливою перевагою запропонованої моделі є можливість налаштування вектору ваг $W = \{w_1, w_2, \ldots, w_m\}$ залежно від контексту застосування.

Розглянемо для прикладу декілька типових сценаріїв. Сценарій "IoT / вбудовані системи", де ресурси (пам'ять, енергія) та розмір ключів є критичними обмеженнями. Пріоритет надається метрикам просторової ефективності та енергоспоживання. Відповідно, ваги: w_{size}=0.4, w_{perf}=0.3, w_{sec}=0.1, w_{rel}=0.2. Сценарій "високонавантажений сервер / TLS Handshake", де критичною є затримка (latency) та пропускна здатність (throughput). Пріоритет це лише швидкість виконання. Розмір ключів менш важливий, якщо не викликає фрагментацію пакетів. Ваги: w_{perf}=0.5, w_{sec}=0.3, w_{size}=0.1, w_{rel}=0.1. Сценарій "довготривале зберігання даних", де продуктивність не є критичною. Головне – найвищий рівень безпеки та відсутність помилок. Пріоритетні метрики стійкість та надійність. Ваги: w_{sec}=0.6, w_{rel}=0.3, w_{size}=0.05, w_{perf}=0.05.

2. Архітектура програмної системи оцінювання

Для практичної реалізації запропонованої математичної моделі спроєктовано та розроблено певні аспекти архітектури програмного забезпечення для реалізації системи оцінювання. Проєктування виконано з використанням методів об'єктно-орієнтованого аналізу та проєктування, а специфікація компонентів – за допомогою уніфікованої мови моделювання UML.

Загальна архітектура програмної системи має ґрунтуватись на модульному принципі, що забезпечує гнучкість, розширюваність (можливість додавання нових алгоритмів без зміни ядра) та незалежність від конкретних реалізацій криптографічних бібліотек. Основні компоненти системи представлені на діаграмі класів (рис. 1), яка описує статичну структуру.

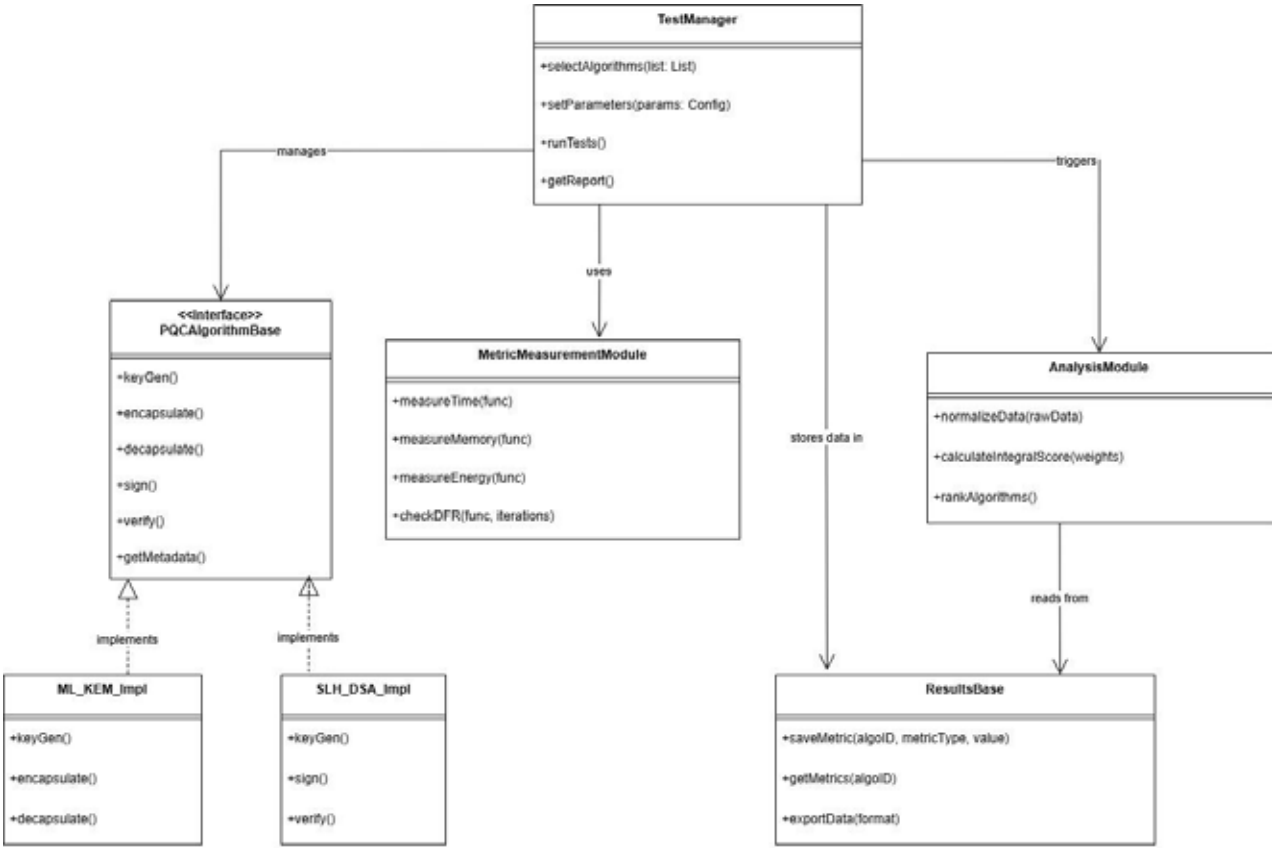

Рис. 1. Діаграма класів

Докладніше розглянемо основні компоненти системи:

– «Менеджер Тестування» – центральний контролер, що оркеструє процес тестування. Він відповідає за ініціалізацію, завантаження конфігурацій та управління потоком виконання.

– «База Алгоритмів PQC» – абстрактний інтерфейс та набір конкретних реалізацій для доступу до криптографічних функцій. Це дозволяє інтегрувати різні бібліотеки (liboqs, PQClean) через єдиний API.

– «Модуль Вимірювання Метрик» відповідає за профілювання виконання коду. Використовує апаратні лічильники (CPU cycles), системні виклики для моніторингу пам'яті та інтерфейси для зчитування енергоспоживання.

– «База Результатів» – сховище даних, де зберігаються необроблені результати вимірювань для забезпечення відтворюваності експериментів.

– «Модуль Аналізу» реалізує математичну модель. Виконує нормалізацію, зважування та ранжування алгоритмів.

Послідовність операцій алгоритму тестування описані за допомогою блок-схеми алгоритму (рис. 2). Динаміка взаємодії компонентів описана за допомогою діаграми послідовності (рис. 3). Зокрема, діаграма послідовності ілюструє часовий аспект виконання сценарію тестування: від вибору алгоритму користувачем до отримання аналітичного звіту.

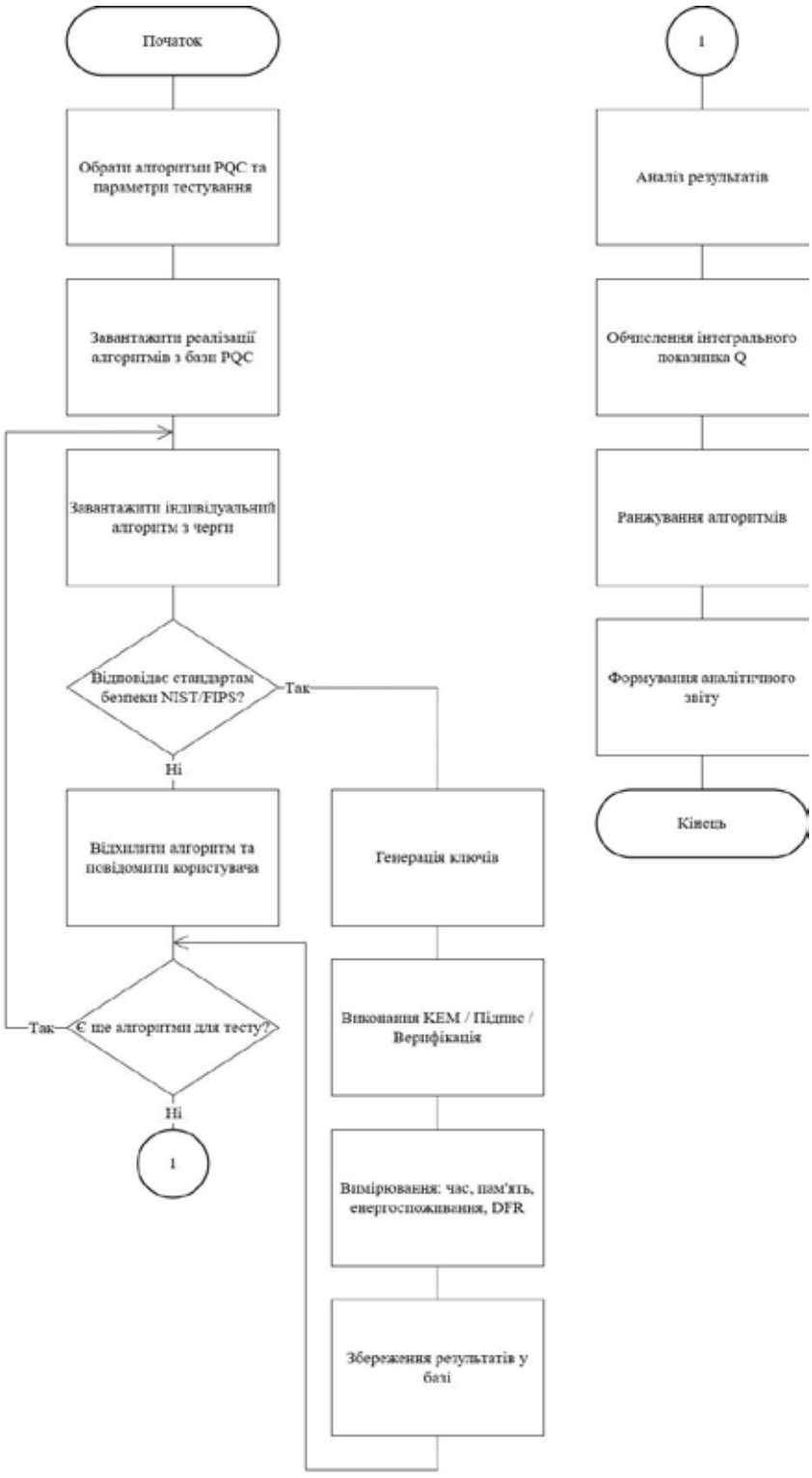

Рис. 2. Блок-схема алгоритму

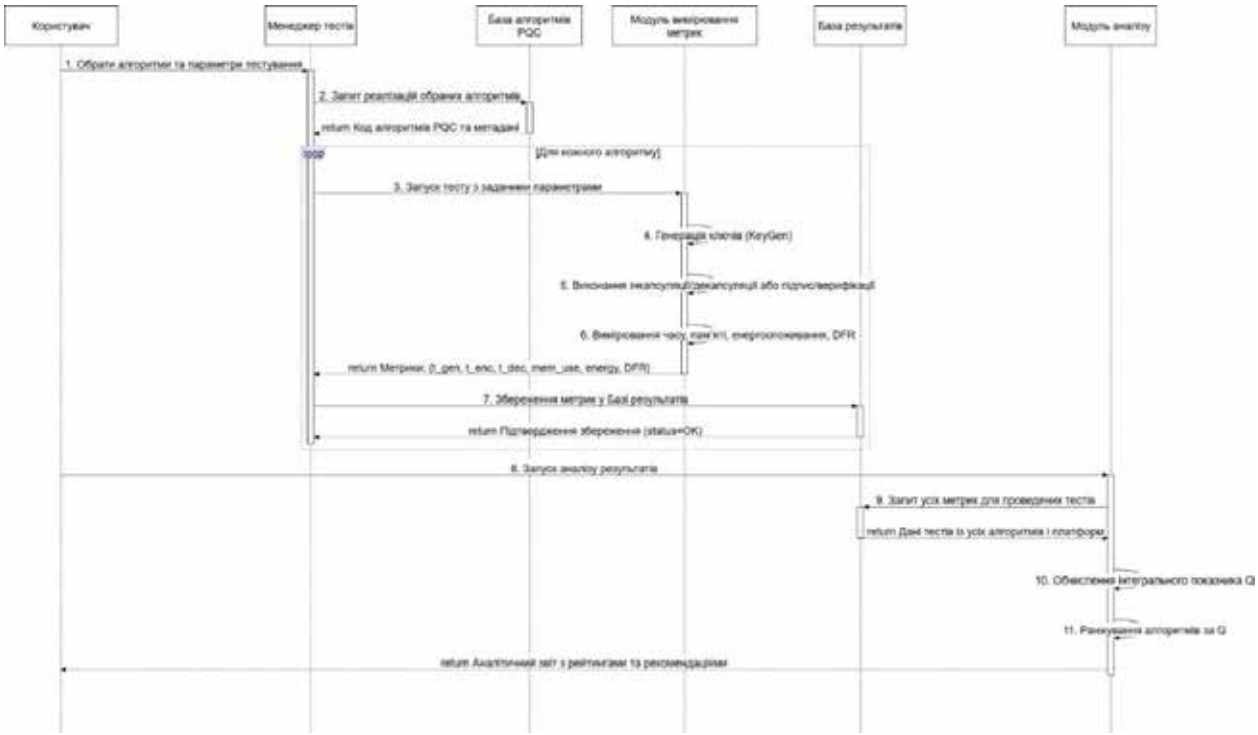

Рис. 3. Діаграма послідовності

Висновки

У роботі вирішено актуальну науково-практичну задачу розроблення алгоритмічного забезпечення та проєктування компонентів архітектури програмної системи для оцінювання постквантових криптографічних алгоритмів.

Проведений аналіз сучасного стану стандартизації NIST підтвердив, що перехід на PQC вимагає відмови від універсальних рішень (типу RSA) на користь спеціалізованих алгоритмів, оптимізованих під конкретні задачі (KEM, DSA) та умови використання. Виявлено, що різноманітність характеристик нових стандартів (FIPS 203, 204, 205) створює складну проблему вибору для інженерів безпеки.

Розроблено математичну модель інтегрального оцінювання, яка, на відміну від існуючих підходів, враховує не лише якийсь один аспект, а комплексну сукупність факторів: криптографічну стійкість, просторові витрати, надійність (DFR) та стійкість до побічних атак. Введення вагових коефіцієнтів дозволяє адаптувати модель до будь-якого сценарію використання.

Спроєктовано та описано аспекти архітектури програмного забезпечення для автоматизованого тестування, що включають статичну структуру основних компонентів та логіку взаємодії між ними. Використання формальних методів та UML-моделювання забезпечило структуризацію компонентів та логіки роботи спроєктованої архітектури програмної системи.

Подальший розвиток дослідження рекомендується зосередити на програмній реалізації на основі запропонованих компонентів архітектури, а також апробації для визначених цільових сценаріїв.

Список використаної літератури

1. What Is Post-Quantum Cryptography? *National Institute of Standards and Technology*. URL: https://www.nist.gov/cybersecurity/what-post-quantum-cryptography (date of access: 20.02.2026).

2. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994. P. 124–134. URL: https://doi.org/10.1109/SFCS.1994.365700 (date of access: 20.02.2026).

3. Barker W., Polk W., Souppaya M. Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms. *National Institute of Standards and Technology*. 2021. URL: https://doi.org/10.6028/NIST.CSWP.04282021 (date of access: 20.02.2026).

4. Post-Quantum Cryptography. *National Institute of Standards and Technology*. URL: https://csrc.nist.gov/projects/post-quantum-cryptography (date of access: 20.02.2026).

5. Chen L., Jordan S., Liu Y.-K., Moody D., Peralta R., Perlner R., Smith-Tone D. Report on Post-Quantum Cryptography. *National Institute of Standards and Technology*. 2016. URL: https://doi.org/10.6028/NIST.IR.8105 (date of access: 20.02.2026).

6. Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D., Liu Y.-K. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. *National Institute of Standards and Technology.* 2019. URL: https://doi.org/10.6028/NIST.IR.8240 (date of access: 20.02.2026).

7. Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Kelsey J., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D., Liu Y.-K. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. *National Institute of Standards and Technology.* 2020. URL: https://doi.org/10.6028/NIST.IR.8309 (date of access: 20.02.2026).

8. Alagic G., Apon D., Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D., Liu Y.-K. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. *National Institute of Standards and Technology*. 2022. URL: https://doi.org/10.6028/NIST.IR.8413-upd1 (date of access: 20.02.2026).

9. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. *National Institute of Standards and Technology.* URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (date of access: 20.02.2026).

10. Alagic G., Bros M., Ciadoux P., Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Liu Y.-K., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Silberg H., Smith-Tone D., Waller N. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. *National Institute of Standards and Technology.* 2025. URL: https://doi.org/10.6028/NIST.IR.8545 (date of access: 20.02.2026).

11. Alagic G., Bros M., Ciadoux P., Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Liu Y.-K., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Silberg H., Smith-Tone D., Waller N. Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. *National Institute of Standards and Technology.* 2024. URL: https://doi.org/10.6028/NIST.IR.8528 (date of access: 20.02.2026).

12. Raavi M., Wuthier S., Chandramouli P., Balytskyi Y., Zhou X., Chang S.-Y. Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms. *Applied Cryptography and Network Security.* 2021. P. 424–447. URL: https://doi.org/10.1007/978-3-030-78375-4_17 (date of access: 20.02.2026).

13. Demir E. D., Bilgin B., Onbasli M. C. Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms. *arXiv preprint.* 2025. URL: https://arxiv.org/abs/2503.12952 (date of access: 01.06.2025).

14. Vidaković M., Miličević K. Performance and Applicability of Post-Quantum Digital Signature Algorithms in Resource-Constrained Environments. *Algorithms.* 2023. Vol. 16, no. 11. P. 518. URL: https://doi.org/10.3390/a16110518 (date of access: 20.02.2026).

15. Chen A. C. H. The Performance Analysis of Post-Quantum Cryptography for Vehicular Communications. *Cryptology ePrint Archive.* 2022. URL: https://eprint.iacr.org/2022/1619 (date of access: 01.06.2025).

16. Abbasi M., Cardoso F., Váz P., Silva J., Martins P. A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments. *Cryptography.* 2025. Vol. 9, no. 2. P. 32. URL: https://doi.org/10.3390/cryptography9020032 (date of access: 20.02.2026).

17. Paquin C., Stebila D., Tamvada G. Benchmarking Post-Quantum Cryptography in TLS. *Microsoft Research.* 2020. URL: https://www.microsoft.com/en-us/research/publication/benchmarking-post-quantum-cryptography-in-tls/ (date of access: 20.02.2026).

18. Wątróbski J., Jankowski J., Ziemba P., Karczmarczyk A., Zioło M. Generalised framework for multi-criteria method selection. *Omega.* 2019. Vol. 86. P. 107–124. URL: https://doi.org/10.1016/j.omega.2018.07.004 (date of access: 20.02.2026).

References

1. National Institute of Standards and Technology. (2024, August 13). *What is post-quantum cryptography?* https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

2. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. https://doi.org/10.1109/SFCS.1994.365700

3. Barker, W., Polk, W., & Souppaya, M. (2021). *Getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms* (NIST CSWP 04282021). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04282021

4. National Institute of Standards and Technology. (2025, December 11). *Post-quantum cryptography*. https://csrc.nist.gov/projects/post-quantum-cryptography

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). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

6. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D., & Liu, Y.-K. (2019). *Status report on the first round of the NIST post-quantum cryptography*

standardization process (NIST IR 8240). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8240

7. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D., & Liu, Y.-K. (2020). *Status report on the second round of the NIST post-quantum cryptography standardization process* (NIST IR 8309). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8309

8. Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D., & Liu, Y.-K. (2022). *Status report on the third round of the NIST post-quantum cryptography standardization process* (NIST IR 8413-upd1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8413-upd1

9. National Institute of Standards and Technology. (2024, August 13). *NIST releases first 3 finalized post-quantum encryption standards*. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

10. Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Silberg, H., Smith-Tone, D., & Waller, N. (2025). *Status report on the fourth round of the NIST post-quantum cryptography standardization process* (NIST IR 8545). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8545

11. Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Silberg, H., Smith-Tone, D., & Waller, N. (2024). *Status report on the first round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process* (NIST IR 8528). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8528

12. Raavi, M., Wuthier, S., Chandramouli, P., Balytskyi, Y., Zhou, X., & Chang, S.-Y. (2021). Security comparisons and performance analyses of post-quantum signature algorithms. In K. Sako & N. O. Tippenhauer (Eds.), *Applied Cryptography and Network Security* (Vol. 12727, pp. 424–447). Springer, Cham. https://doi.org/10.1007/978-3-030-78375-4_17

13. Demir, E. D., Bilgin, B., & Onbasli, M. C. (2025). *Performance analysis and industry deployment of post-quantum cryptography algorithms*. arXiv. https://arxiv.org/abs/2503.12952

14. Vidaković, M., & Miličević, K. (2023). Performance and applicability of post-quantum digital signature algorithms in resource-constrained environments. *Algorithms, 16*(11), Article 518. https://doi.org/10.3390/a16110518

15. Chen, A. C. H. (2022). *The performance analysis of post-quantum cryptography for vehicular communications* (Cryptology ePrint Archive Paper 2022/1619). International Association for Cryptologic Research. https://eprint.iacr.org/2022/1619

16. Abbasi, M., Cardoso, F., Váz, P., Silva, J., & Martins, P. (2025). A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. *Cryptography, 9*(2), Article 32. https://doi.org/10.3390/cryptography9020032

17. Paquin, C., Stebila, D., & Tamvada, G. (2020, February 6). *Benchmarking post-quantum cryptography in TLS* (Microsoft Research Technical Report). Microsoft. https://www.microsoft.com/en-us/research/publication/benchmarking-post-quantum-cryptography-in-tls/

18. Wątróbski, J., Jankowski, J., Ziemba, P., Karczmarczyk, A., & Zioło, M. (2019). Generalised framework for multi-criteria method selection. *Omega, 86*, 107–124. https://doi.org/10.1016/j.omega.2018.07.004

Дата першого надходження статті до видання: 16.02.2026
Дата прийняття статті до друку після рецензування: 23.03.2026
Дата публікації (оприлюднення) статті: 07.05.2026