ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.30.19243

ПЕРЕХІД ДО ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ СИСТЕМ: ВИКЛИКИ, СТАНДАРТИЗАЦІЯ ТА ПЕРСПЕКТИВИ

Павло Воробець, Андрій Горпенюк, Іван Опірський

Національний університет «Львівська політехніка»

ВОРОБЕЦЬ Павло Андрійович, аспірант
Рік та місце народження: 1994 рік, м. Львів, Львівська обл., Україна.
Освіта: Національний університет «Львівська Політехніка», 2017 рік.
Посада: аспірант кафедри захисту інформації.
Наукові інтереси: криптографія, розвідка на основі відкритих джерел.
E-mail: pavlo.a.vorobets@lpnu.ua.
Orcid ID: 0009-0007-3870-829X.

ГОРПЕНЮК Андрій Ярославович, к.т.н., доцент
Рік та місце народження: 1969 рік, м. Львів, Львівська обл., Україна.
Освіта: Національний університет «Львівська Політехніка», 1994 рік.
Посада: доцент кафедри захисту інформації.
Наукові інтереси: криптографія, вимірювальна та обчислювальна техніка, системи захисту інформації.
E-mail: andrii.y.horpeniuk@lpnu.ua.
Orcid ID: 0000-0001-5821-2186.

ОПІРСЬКИЙ Іван Романович, д.т.н., проф.
Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: завідувач кафедри захисту інформації з 2023 рок.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання.
Публікації: більше 120 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

Анотація. *У цій статті здійснено детальний аналіз проблем та перспектив впровадження постквантових криптографічних алгоритмів, які стають дедалі актуальнішими у зв'язку з розвитком квантових обчислень. Розглянуто основні виклики, пов'язані зі стандартизацією постквантових алгоритмів, зокрема питання гнучкості алгоритмів, їхньої продуктивності, складності впровадження та невизначеності щодо появи квантових комп'ютерів, здатних зламувати сучасні криптосистеми. Окрему увагу приділено оцінці сучасного стану розвитку постквантових криптографічних стандартів, а також аналізу потенційних сценаріїв переходу до нових систем захисту інформації. Основну роль тут відіграє Національний інститут стандартів і технологій США (NIST). NIST здійснює ключову координацію та керівництво в процесі розробки стандартів постквантової криптографії, ініціювавши процес відкритого конкурсу для визначення найбільш перспективних криптографічних алгоритмів. Програма, запущена NIST, передбачає багаторічний процес оцінки, тестування та відбору алгоритмів, здатних забезпечити стійкість до атак з боку квантових комп'ютерів. У рамках цієї програми було розглянуто широкий спектр алгоритмів, які відрізняються підходами до шифрування, продуктивністю та ступенем безпеки. На основі проведеного дослідження запропоновано рекомендації щодо ефективного управління перехідним періодом від традиційних криптографічних систем до постквантових рішень, що мають забезпечити надійну безпеку даних в умовах нових технологічних викликів. Зокрема, пропонуються підходи до управління перехідним періодом, стратегії зниження ризиків, а також оцінки можливих загроз і шляхів їхньої мінімізації. У результаті стаття надає цінну основу для формування стратегії безпечної адаптації інформаційних систем у епоху квантових технологій.*

Ключові слова: *постквантова криптографія, квантові комп'ютери, процес стандартизації, NIST, постквантові криптографічні системи.*

Постановка проблеми

Концепція квантового комп'ютера – це не просто теорія. Квантові комп'ютери перетворюються з наукової фантастики на реальність, що має глибокі наслідки для багатьох сфер життя, зокрема для кібербезпеки. Квантові обчислення відкривають безмежні можливості для наукових відкриттів. Саме тому провідні наукові установи світу змагаються за те, щоб першими розкрити потенціал квантових комп'ютерів і зробити проривні відкриття в різних галузях знань. Завдяки цій технології час обчислень може скоротитися від років до годин або навіть хвилин. Потужність квантових обчислень принесе значну користь науковій спільноті. Однак це також створює значні загрози для кібербезпеки. Практично будь-який криптографічний алгоритм може бути атакований [1]. Згодом практичні квантові комп'ютери з мільйонами кубітів зможуть розшифрувати майже всі системи криптографії з відкритим ключем (табл. 1).

Аналіз останніх досліджень і публікацій

Сучасні криптографічні алгоритми є складними математичними конструкціями, які покликані забезпечити високий рівень безпеки даних. Але квантові комп'ютери мають потенціал зламати багато класичних криптографічних алгоритмів, які зараз широко використовуються. Традиційні криптографічні системи, такі як RSA та ECC, ґрунтуються на таких складних математичних задачах, як факторизація великих чисел або дискретне логарифмування, які важко вирішити за допомогою класичних комп'ютерів. Розв'язання цих задач для сучасних комп'ютерів займає неймовірно багато часу, що робить підбір ключів практично неможливим. Однак квантові комп'ютери можуть використовувати свої унікальні квантові властивості, такі як суперпозиція та заплутаність, щоб виконувати певні обчислення експоненціально швидше, ніж класичні комп'ютери [2-4].

Таблиця 1

Сучасний стан безпеки класичних криптосистем по відношенню до квантових комп'ютерів

Криптосистема	Статус
RSA	Ненадійний
DSA	Ненадійний
Diffie-Hellman key-exchange	Ненадійний
ECDSA, ECDH (Elliptic curve cryptography)	Ненадійний
DES, 3DES	Ненадійний
AES	Надійний при великому ключі
SHA-1	Ненадійний
SHA-2, SHA-3	Надійний при великому ключі
Chacha/Salsa20	Надійний при великому ключі
Blowfish, Twofish	Надійний при великому ключі

Вразливість класичної криптографії до квантових атак виникає через фундаментальні відмінності в обчислювальних можливостях квантових і класичних комп'ютерів. Квантові комп'ютери можуть виконувати певні математичні операції паралельно завдяки суперпозиції кубітів, що дозволяє їм вирішувати проблеми, які зайняли б у класичних комп'ютерів непрактичний час. Як наслідок, розробка та стандартизація постквантових криптографічних алгоритмів стала необхідною. Постквантова криптографія спрямована на створення криптографічних систем, які залишаться безпечними навіть за наявності потужних квантових комп'ютерів.

Мета та постановка завдання

З розвитком квантових обчислень постквантова криптографія набуває все більшої важливості. Проте процес стандартизації постквантових криптоалгоритмів стикається з багатьма викликами та проблемами. Серед них – гнучкість алгоритмів, невизначеність термінів появи квантових атак, відсутність зрілих алгоритмів, питання продуктивності, розмір ключів і пропускна здатність, сумісність та інтеграція, перехідний період, а також стандартизація від NIST. Крім того, необхідно враховувати потребу в адаптації існуючих систем і розробці нових захисних механізмів для забезпечення безпеки у майбутньому квантовому середовищі.

Виклад основного матеріалу дослідження

Проблеми постквантової криптографії

Останніми роками стрімкий розвиток квантових обчислень викликав зростання занепокоєння щодо безпеки традиційних криптографічних систем. Квантові комп'ютери мають потенціал значно прискорити обчислення, що дозволить розшифрувати багато з існуючих методів захисту інформації. Цей сценарій створює серйозну загрозу для конфіденційності, цілісності та автентичності інформації в різних сферах нашого життя.

Постквантова криптографія, також відома як квантово-стійка або квантово-безпечна криптографія, намагається вирішити ці проблеми безпеки, створюючи криптографічні алгоритми, які залишаються захищеними від атак як класичних, так і квантових комп'ютерів. Основною метою є розробка криптографічних методів, що базуються на математичних проблемах, які вважаються складними навіть для потужних квантових комп'ютерів [5, 17].

Потреба в постквантових криптографічних стандартах зростає. Хоча квантові комп'ютери, здатні зламати поточні криптографічні системи, все ще знаходяться в сфері теоретичних досліджень, загроза, яку вони становлять, вже зараз стимулює активний розвиток постквантової криптографії. Вчені та інженери працюють над створенням алгоритмів, які будуть стійкими до квантових атак, оскільки очікується, що в найближчі десятиліття квантові комп'ютери зможуть досягти рівня продуктивності, необхідного для зламування сучасних криптографічних систем. Дуже важливо заздалегідь підготуватися до неминучої появи більш потужних квантових комп'ютерів.

Недостатня випробовуваність алгоритмів

Постквантові криптографічні алгоритми мають бути достатньо гнучкими, щоб застосовуватися у різних сферах, від фінансових операцій до національної безпеки.

Багато постквантових криптографічних алгоритмів знаходяться на ранніх стадіях розробки і не пройшли достатньо тривалого тестування в реальних умовах. Відсутність тривалого досвіду використання цих алгоритмів викликає занепокоєння щодо їх безпеки та ефективності. Класичні криптографічні алгоритми пройшли роки криптоаналізу та експертної перевірки, що забезпечує високий рівень впевненості в їхній

безпеці. Навпаки, новизна постквантових алгоритмів означає, що їхня безпека може бути не так ретельно зрозуміла. Важливо піддати ці алгоритми ретельному аналізу, щоб переконатися в їх стійкості як до класичних, так і до квантових атак.

Відсутність тривалої історії використання в реальному світі залишає відкритою можливість непередбачених атак. На відміну від добре вивчених класичних алгоритмів, можуть існувати невивчені вразливості, якими хотітимуть скористатися зловмисники. Через їх відносну новизну та поточний процес стандартизації, постквантові криптографічні алгоритми можуть бути недоступні в комерційних продуктах і програмах. Це перешкоджає їх практичному розгортанню в поточному криптографічному ландшафті.

Також важливо мати детальну документацію та підтримку з боку розробників і спільноти. Це включає інструкції з впровадження, налаштування, оптимізації та вирішення проблем.

Однак квантові обчислення ще знаходяться в процесі розвитку, і нові відкриття в цій галузі можуть вплинути на ефективність існуючих постквантових алгоритмів. Це робить процес створення зрілих алгоритмів динамічним і потребує постійного оновлення та адаптації до нових викликів.

Відсутність зрілих алгоритмів означає, що ще потрібно багато роботи для того, щоб нові криптографічні рішення були надійними, ефективними та готовими до широкого впровадження. Це включає тривалі дослідження, тестування, впровадження в реальних умовах і активну співпрацю між дослідниками, розробниками та користувачами.

Невизначеність термінів

Точні терміни появи повноцінних квантових комп'ютерів залишаються невідомими, що ускладнює планування переходу на нові постквантові криптографічні алгоритми. Квантові обчислення перебувають у стадії активних досліджень і розробок. Хоча досягнуто значного прогресу, точні терміни досягнення квантової переваги залишаються невизначеними. Це ускладнює прогнозування, коли саме буде необхідний перехід на нові алгоритми.

Квантові комп'ютери використовують кубіти (квантові біти) замість традиційних бітів, що є основою їхньої потужності і суттєвої відмінності від класичних комп'ютерів. **Кубіт** або квантовий біт - це основна одиниця інформації в квантовому комп'ютері. У класичному комп'ютері біт може бути в одному з двох станів: 0 або 1. Кубіт, завдяки принципам квантової механіки, може бути одночасно в стані 0, в стані 1 або в будь-якому їхньому квантовому суперпозиційному стані. Основні принципи квантової механіки, на яких базується робота кубітів, включають наступні пункти.

Суперпозиція: кубіт може існувати в суперпозиції станів 0 і 1 одночасно. Це означає, що він може представляти набагато більше інформації, ніж класичний біт.

Заплутаність (ентанглмент): кубіти можуть бути заплутаними, тобто стан одного кубіта залежить від стану іншого, незалежно від відстані між ними. Це створює можливість для квантового паралелізму, що значно збільшує обчислювальну потужність квантових комп'ютерів.

Інтерференція: квантові стани можуть взаємодіяти один з одним, посилюючи або послаблюючи ймовірності певних результатів. Це використовується для керування обчисленнями і отримання бажаних результатів.

У квантовому комп'ютері кубіти використовуються для виконання квантових операцій (гейтів), які еквівалентні логічним операціям у класичному комп'ютері. Проте, завдяки суперпозиції і заплутаності, квантові комп'ютери можуть обробляти величезну кількість можливих станів одночасно. Одним з найбільш відомих квантових алгоритмів є алгоритм Шора, який може факторизувати великі числа експоненційно швидше, ніж найкращі класичні алгоритми. Це має значні наслідки для криптографії, зокрема для RSA-шифрування.

Перший квантовий комп’ютер з 1 кубітом був створений і представлений у 1998 році. Відтоді ми бачимо як кількість кубітів, представлених у квантовому комп’ютері, з часом зростає. Нижче (табл. 2) наведено основні часові рамки просування кубіта за роками на момент написання цієї статті на основі заяв різних виробників.

Таблиця 2

Збільшення кількості кубітів у комп’ютерах впродовж років

Рік	Кількість кубітів
2000	5- та 7-кубітний у комп’ютер
2006	12-кубітний у комп’ютер
2008	28-кубітний у комп’ютер
2012	84-кубітний у комп’ютер
2015	100-кубітний у комп’ютер
2017	200-кубітний у комп’ютер
2022	500-кубітний у комп’ютер
2024	1121-кубітний у комп’ютер

Важливо розуміти, що кількість кубітів не є єдиним визначальним фактором продуктивності чи обчислювальної потужності квантового комп’ютера [21]. Мати більше кубітів, безперечно, добре, але не всі кубіти однакові, і здатність квантових комп’ютерів вирішувати задачі визначається більшою кількістю змінних, ніж просто кількістю кубітів. Ось деякі з ключових аспектів, які впливають на продуктивність квантових комп'ютерів.

Когерентність: це час, протягом якого кубіт зберігає свою квантову інформацію. Кубіти з довшим часом когерентності можуть виконувати складніші обчислення без втрати інформації.

Фіделіті: це міра точності операцій на кубітах. Висока фіделіті означає меншу кількість помилок під час квантових операцій.

Шум: квантові системи дуже чутливі до зовнішнього шуму, який може порушити квантові стани. Системи з меншою кількістю шуму здатні виконувати надійніші обчислення.

Зв’язність кубітів: це здатність кубітів взаємодіяти один з одним. Більша зв’язність дозволяє виконувати складніші квантові операції.

Архітектура квантового процесора: різні архітектури можуть мати різні переваги в залежності від типу задач. Наприклад, деякі архітектури краще підходять для реалізації певних квантових алгоритмів.

Квантові алгоритми: продуктивність квантового комп’ютера також залежить від алгоритмів, які на

ньому виконуються. Деякі задачі можуть бути значно прискорені за допомогою квантових алгоритмів, тоді як інші можуть не отримати такої вигоди.

Оптимізація програмного забезпечення: як і в класичних комп'ютерах, ефективність квантового обчислення може значно покращитися завдяки оптимізації програмного забезпечення та компіляторів, які мінімізують кількість помилок та ресурсів, необхідних для виконання квантових програм.

Квантова корекція помилок: оскільки квантові системи дуже чутливі до помилок, здатність ефективно коригувати помилки є критично важливою. Це включає використання спеціальних квантових кодів та схем корекції помилок, які дозволяють зберігати точність обчислень [19, 20].

Отже, продуктивність квантового комп'ютера визначається не лише кількістю кубітів, але й багатьма іншими факторами, які впливають на його здатність виконувати обчислення ефективно та надійно.

Якщо підсумувати вище написане, то якість кубітів має вирішальне значення. Квантові комп'ютери дуже чутливі до шуму та помилок, тому підтримувати когерентність кубітів є складним завданням. Високоточні кубіти з великим часом когерентності необхідні для надійних квантових обчислень. Розташування та підключення кубітів у квантовому процесорі є над важливим завданням. Здатність ефективно виконувати багатокубітові операції та реалізувати коди квантової корекції помилок залежить від підключення кубітів. Квантові комп'ютери повинні використовувати методи виправлення помилок, щоб пом'якшити вплив квантових помилок, які природно виникають під час обчислень. Квантова корекція помилок вводить додаткові кубіти та обчислювальні витрати. Розробка ефективних квантових алгоритмів і програмного забезпечення, адаптованого до апаратного забезпечення, важлива для максимізації продуктивності квантових обчислень [8].

Квантові обчислення — це міждисциплінарна галузь, яка охоплює фізику, інформатику, матеріалознавство тощо, і вимагає значного прогресу в апаратному забезпеченні, програмному забезпеченні та алгоритмах для досягнення практичних квантових переваг у вирішенні складних проблем. Вже досягнуто значного прогресу, але він залишається у сфері досліджень та експериментів.

Перехідний період та процес стандартизації

Оскільки розробляються постквантові криптографічні стандарти, існує перехідний період, коли повинні співіснувати як традиційні, так і постквантові алгоритми. Ефективне керування цим переходом без шкоди для безпеки є серйозною проблемою. Національний інститут стандартів і технологій (NIST) очолює зусилля зі стандартизації постквантової криптографії. Однак цей процес займає багато часу, і існують різні алгоритми-кандидати, які слід розглянути, що ускладнює процес відбору та стандартизації.

Процес стандартизації постквантової криптографії (Post-Quantum Cryptography - PQC) NIST розпочався в грудні 2016 року, коли NIST опублікував публічний заклик подати постквантові криптографічні алгоритми з відкритим ключем. Вони визначили п'ять основних категорій постквантових криптографічних алгоритмів:

Алгебраїчні структури над ґратками (Lattice-Based Cryptography): використовує складність розв'язання проблем над ґратками (рис. 1). Ґратка (решітка) — це набір точок у багатовимірному просторі, які утворюють регулярну структуру, подібну до сітки. Вона включає алгоритми, що базуються на проблемах, таких як Shortest Vector Problem (SVP) і Learning With Errors (LWE). Криптографічні алгоритми на основі решітки видаються найбільш перспективними та квантово стійкими [6, 16].

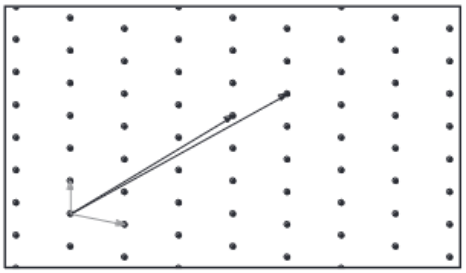

Рис. 1. Алгебраїчні структури над ґратками

Кодовані криптографічні системи (Code-Based Cryptography): базується на складності розв'язання проблем декодування лінійних кодів. Цей підхід є одним із найперспективніших для постквантової криптографії через його стійкість до квантових атак. Кодовані криптографічні системи використовують різні типи структурованих кодів, такі як лінійні коди, які мають математичну структуру, що дозволяє здійснювати операції кодування та декодування. Безпека цих систем ґрунтується на обчислювальній складності завдання декодування випадкових лінійних кодів [13]. Це завдання є NP-важким, що означає, що воно є надзвичайно складним для розв'язання, навіть з використанням квантових комп'ютерів. Оскільки завдання декодування випадкових лінійних кодів є обчислювально складним, ці системи вважаються стійкими до квантових атак, зокрема до атак на основі алгоритму Шора. Кодовані криптографічні системи не залежать від часу когерентності кубітів у квантових комп'ютерах, що робить їх стабільними і надійними.

Схеми на основі хеш-функцій (Hash-Based Cryptography): базуються на криптографічних хеш-функціях і зазвичай використовуються для створення підписів. Вони мають високий рівень безпеки, оскільки спираються на стійкість хеш-функцій до колізій. Багато схем на основі хеш-функцій використовують деревоподібні структури, для генерації та перевірки цифрових підписів. Алгоритми на основі хеш-функцій відносно прості в реалізації і не вимагають складних математичних структур або великих обчислювальних ресурсів.

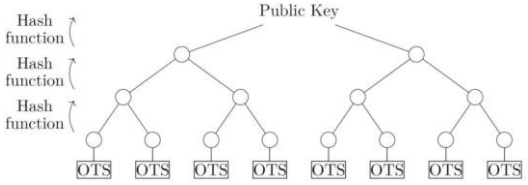

Рис. 2. Схеми на основі хеш-функцій

Многочлени над кінцевими полями (Multivariate Polynomial Cryptography): базуються на складності розв'язання систем многочленів над кінцевими полями. Вони включають алгоритми, які використовують

багатовимірні поліноміальні рівняння. Ці поліноми можуть бути визначені як над основним, так і над полем розширення в певних ситуаціях. Розв'язання таких систем є обчислювально складним завданням, особливо коли кількість змінних і ступінь поліномів збільшується. Системи багатовимірних поліноміальних рівнянь є складними для розв'язання навіть для квантових комп'ютерів, що робить ці алгоритми стійкими до квантових атак [7].

Криптографія на основі ізогеній (Isogeny-Based Cryptography): базується на математичній структурі еліптичних кривих та ізогеній між ними - проблемах суперсингулярної ізогенії або пошуку відображення ізогенії між двома суперсингулярними еліптичними кривими з однаковою кількістю точок. Цей підхід використовує складність певних задач, пов'язаних з ізогеніями, для створення криптографічних систем, що, як вважається, стійкі до атак як класичних, так і квантових комп'ютерів. Порівняно з іншими постквантовими криптографічними підходами, схеми на основі ізогеній часто мають відносно малі розміри ключів, що є перевагою з точки зору ефективності та зберігання. Але криптографічні операції на основі ізогеній можуть бути обчислювально складними, що може впливати на продуктивність. Ця криптосистема є відносно новою та не перевіреною, тому можуть бути непередбачені недоліки або слабкі місця, якими зловмисники можуть скористатися. Крім того, незважаючи на те, що криптографії на основі ізогенії потрібні лише невеликі розміри ключів, обчислювальна вартість створення ключа все ще досить висока, що може бути недоліком для систем з обмеженими ресурсами (рис. 3).

Ці категорії розглядаються як потенційні кандидати на квантово стійкі криптографічні стандарти. Загалом до кінця листопада 2017 року було подано 82 кандидати. У грудні 2017 року NIST оголосив, що 69 із цих кандидатів відповідали як вимогам до подання, так і мінімальним критеріям та були прийняті до першого раунду процесу стандартизації.

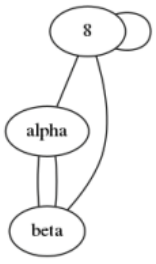

Рис. 3. Суперсингулярне відображення ізогенії

Після ретельного розгляду під час третього раунду процесу стандартизації NIST PQC, NIST визначив чотири кандидатські алгоритми для стандартизації. NIST рекомендує використовувати CRYSTALS-KYBER (обмін ключами) і CRYSTALS-Dilithium (цифрові підписи). Крім того, схеми підписів FALCON і SPHINCS+ також будуть стандартизовані. До четвертого раунду обрано також ще чотири алгоритми: BIKE, Classic McEliece, HQC і SIKE [10,11].

Після завершення процесу стандартизації нові алгоритми будуть впроваджені в реальні системи, замінюючи або доповнюючи існуючі криптографічні механізми. Це включає оновлення програмного забезпечення, апаратних засобів та інших компонентів інформаційної безпеки. Важливо бути в курсі прогресу стандартизації, оскільки криптографічні стандарти відіграють вирішальну роль у забезпеченні безпеки та стійкості цифрових комунікацій у постквантову еру. Стандартизація постквантової криптографії є складним і тривалим процесом, що вимагає співпраці між науковою спільнотою, індустрією та урядовими організаціями.

Оцінка продуктивності

Нові алгоритми мають бути достатньо ефективними, щоб не знижувати продуктивність систем. Це особливо важливо в контексті постквантової криптографії, де необхідно знайти баланс між високим рівнем безпеки та оптимальною продуктивністю.

Деякі постквантові криптографічні алгоритми потребують інтенсивних обчислень, що може призвести до меншої швидкості шифрування та дешифрування порівняно з традиційними криптоалгоритмами. Це додаткове навантаження на продуктивність може обмежити їх практичне застосування, особливо в середовищах з обмеженими ресурсами [9].

Ресурси, необхідні для створення та перевірки ключів, часто є значно більшими, ніж у класичній криптографії, навіть якщо квантово стійкий криптографічний алгоритм має менші розміри ключів. Через це конкурс NIST вимагає ретельного тестування продуктивності, і учасники докладають усіх зусиль, щоб пришвидшити свої алгоритми. Хоча очікується, що перехід на постквантовий алгоритм знизить загальну продуктивність навіть на найбільш потужних і найшвидших комп'ютерах і пристроях, NIST, вибере постквантовий стандарт, який має хороший компроміс між продуктивністю та безпекою.

Аналіз продуктивності алгоритмів виконується за допомогою проекту Open Quantum Safe (OQS). Це проект, який розробляє та створює прототипи квантово-стійких криптографічних алгоритмів. Проект OQS надає бібліотеку з відкритим кодом, яка реалізує кілька постквантових криптографічних алгоритмів. Бібліотека OQS має на меті сприяти дослідженню, розробці та інтеграції квантово-стійких алгоритмів у різні програми та системи.

Продуктивність постквантових алгоритмів може значно відрізнятися залежно від конкретного алгоритму, його реалізації та апаратного забезпечення, на якому він виконується. OQS також пропонує порівняльну інформацію для різних квантово-стійких алгоритмів, яка використовується в цій статті для порівняння поведінки під час виконання та використання пам'яті алгоритмами [23].

Поведінка алгоритмів під час виконання та дані про використання пам'яті збираються на основі виконання алгоритмів у Amazon Web Service (AWS) із моделлю ЦП Intel(R) Xeon(R) Platinum 8259CL, що працює на частоті 2,50 ГГц [12].

Аналіз продуктивності численних квантово-безпечних алгоритмів показує, що ці алгоритми зазвичай вимагають великої кількості циклів ЦП для своїх основних дій, таких як створення ключа, шифрування/дешифрування, обмін ключами, підписання та перевірка тощо [22].

Крім того, алгоритми вимагають дуже великих розмірів відкритого та закритого ключів. У порівнянні

з класичними криптографічними методами, ці підходи споживають багато пам'яті під час виконання. Вищий цикл процесора та використання пам'яті обмежені системами та пристроями інформаційно-комунікаційних технологій. Обмеження ресурсів можна певною мірою вирішити для таких систем, як ноутбук, настільний комп'ютер або сервер високого класу.

Однак це складна проблема для настільних пристроїв, таких як смартфони, сенсорні мережі, розумні мережі, IoT, розумні пристрої, розумні будинки тощо.

Таблиця 3

Оцінка продуктивності постквантових криптографічних алгоритмів

Алгоритм	Тип алгоритму	Продуктивність
CRYSTALS-KYBER	Алгебраїчні структури над ґратками	Загальна продуктивність CRYSTALS-KYBER у програмному, апаратному та гібридному налаштуваннях чудова.
CRYSTALS-Dilithium	Алгебраїчні структури над ґратками	Використовує псевдовипадковість, а методи скороченого зберігання покращують продуктивність. Схема не використовує арифметику з плаваючою комою, що є перевагою. Високоефективний і відносно простий у виконанні.
Falcon	Алгебраїчні структури над ґратками	Процес перевірки швидкий і вимагає низької пропускної здатності. Це найкращий вибір для деяких сценаріїв обмеженого протоколу.
SPHINCS+	Схеми на основі хеш-функцій	Генерація та перевірка ключів відбувається набагато швидше, ніж підписання.
BIKE	Кодовані криптографічні системи	Продуктивність BIKE підійде для більшості додатків, що підтверджено декількома апаратними тестами.
HQC	Кодовані криптографічні системи	Пропускна здатність HQC перевищує пропускну здатність BIKE, але для декапсуляції потрібна лише частка кілоциклів, необхідних BIKE. HQC є одним із двох найкращих альтернативних KEM. Загальна продуктивність HQC не є оптимальною, але все ж прийнятною.
Classic McEliece	Кодовані криптографічні системи	Має найменший зашифрований текст серед усіх кандидатів NIST PQC
SIKE	Криптографія на основі ізогеній	Продуктивність на вбудованих пристроях може бути проблемою через час для виконання інкапсуляції/декапсуляції одного ключа.

Важливо пам'ятати, що постквантові алгоритми все ще активно досліджуються та оптимізуються. Характеристики продуктивності цих алгоритмів можуть змінюватися з часом, оскільки дослідники виявляють більш ефективні реалізації та вдосконалюють свої проекти [14, 15]. Оцінюючи продуктивність постквантових алгоритмів, важливо враховувати такі фактори, як розмір ключа, швидкість шифрування та дешифрування, вимоги до пам'яті та цільова апаратна платформа.

Щоб досягти балансу між безпекою та ефективністю, залежно від вимог і обмежень конкретної програми часто робляться компроміси щодо продуктивності.

Таблиця 4

Порівняння довжини ключів постквантових криптографічних алгоритмів

Алгоритм	Тип алгоритму	Публічний ключ	Приватний ключ	Підпис
CRYSTALS-KYBER	Алгебраїчні структури над ґратками	1568 B	3168 B	
CRYSTALS-Dilithium	Алгебраїчні структури над ґратками	2592 B	4864 B	
Falcon	Алгебраїчні структури над ґратками	897 B / 1793 B	1281 B / 2305 B	666 B / 1280 B
SPHINCS+	Схеми на основі хеш-функцій	32 B	64 B	8 KB
BIKE	Кодовані криптографічні системи	5122 B	16494 B	
HQC	Кодовані криптографічні системи	7245 B	7258 B	
Classic McEliece	Кодовані криптографічні системи	1232 B	2464 B	
SIKE	Криптографія на основі ізогеній	564 B	48 B	

Розмір ключів та пропускна здатність

Постквантові криптографічні алгоритми вимагають більшого розміру ключів порівняно з класичними алгоритмами. Це може спричинити підвищення вимог до пропускної здатності для забезпечення безпечного зв'язку, а також може створити проблеми для пристроїв з обмеженими ресурсами. Додатково, такі вимоги можуть призвести до затримок в обробці інформації та зниження загальної ефективності системи [18].

Порівнюючи розміри ключів різних постквантових криптографічних алгоритмів, важливо розуміти, що ці алгоритми мають власні рівні безпеки та компроміси щодо продуктивності. Розмір ключа є одним із факторів, який може впливати на безпеку та ефективність криптографічної системи. Як правило, більші розміри ключів пропонують вищий рівень безпеки, але вони також можуть призвести до збільшення вимог до пам'яті та пропускної здатності.

У таблиці 4 наведено порівняння постквантових криптографічних алгоритмів і їх типових розмірів ключів (табл. 4).

Більші розміри ключів призводять до потреби в більшій пам'яті для зберігання ключів і збільшення використання пропускної здатності для передачі криптографічних даних. Це може бути проблематичним для пристроїв з обмеженими ресурсами, наприклад, пристроїв Інтернету речей (IoT) та мобільних пристроїв, де пам'ять і пропускна здатність є надзвичайно важливими. Більший розмір ключа може призвести до збільшення обчислювальних витрат під час операцій шифрування, дешифрування та генерації ключів. Це може уповільнити криптографічні процеси та вплинути на продуктивність системи, особливо на пристроях з обмеженою обчислювальною потужністю.

Існуючі системи та протоколи можуть бути не розроблені для роботи з постквантовими розмірами ключів, що може створити проблеми сумісності під час переходу на постквантові криптографічні рішення. Оновлення систем для підтримки більших розмірів ключів вимагатиме значних змін у апаратному та програмному забезпеченні, що може призвести до підвищення витрат і складності реалізації. Крім того, перехід на нові криптографічні стандарти може викликати затримки в обробці даних і потребуватиме додаткових ресурсів для забезпечення належної безпеки та продуктивності системи. Розробка ефективних і безпечних реалізацій для цих алгоритмів може бути складнішою порівняно з класичними криптографічними алгоритмами.

Сумісність та інтеграція

Забезпечення сумісності між старими і новими системами є складним завданням. Інфраструктура, яка підтримує класичні алгоритми, повинна бути оновлена для підтримки нових постквантових алгоритмів, що може вимагати значних інвестицій та ресурсів.

Поточну інфраструктуру будь-якої компанії потрібно буде значно оновити, щоб перейти до постквантової криптографії. Деякі з їхніх поточних ІТ-систем можуть стати повністю непридатними та потребуватимуть заміни. Може виникнути потреба переробити та змінити протокол, програмне забезпечення та алгоритми, які зараз використовуються. Загалом компанії зазнають значних бюджетних витрат і неминучої складності в результаті процесу інтеграції. Багато пристроїв, зокрема IoT та мобільні пристрої, мають обмежені ресурси. Впровадження нових алгоритмів може вимагати модернізації апаратного забезпечення для забезпечення достатньої обчислювальної потужності та пам'яті.

Існуючі програмні рішення, зокрема операційні системи, програми та протоколи, повинні бути оновлені або переписані для підтримки нових криптографічних стандартів. Це може включати зміну базового коду, тестування та перевірку сумісності.

Багато сучасних протоколів (наприклад, TLS, IPsec) були розроблені з використанням класичних криптографічних методів. Їхнє оновлення для підтримки постквантових алгоритмів потребуватиме внесення змін до існуючих стандартів і можливе створення нових [24]. Впровадження постквантових алгоритмів може вплинути на продуктивність системи через збільшення вимог до обчислювальних ресурсів. Це особливо важливо для систем, які мають суворі обмеження щодо затримки та швидкості обробки даних. Хоча постквантові алгоритми розроблені для протидії загрозам з боку квантових комп'ютерів, існують ризики, пов'язані з їхньою новизною та недостатнім тестуванням. Перехід до нових алгоритмів повинен супроводжуватися ретельною оцінкою безпеки та управління ризиками. Інтеграція нових алгоритмів потребуватиме значних фінансових вкладень для розробки, тестування, впровадження та підтримки нових рішень. Організації можуть зіткнутися з додатковими витратами на навчання персоналу та модернізацію інфраструктури.

Більшість перспективних алгоритмів постквантової криптографії стикаються зі складною проблемою масштабованості. Наприклад, один із основних методів створення квантово-безпечних алгоритмів, криптографія на основі решітки, добре масштабується, але забезпечує лише середню надійність. Отже можна сказати, що масштабованість і надійність можуть бути порушені, оскільки можна досягти будь-якого результату, але не обох одночасно.

Це означає, що у світі постквантової криптографії розробники протоколів повинні усвідомлювати можливість різних компромісів і вибирати системи, які відповідають їх сценарію застосування. Потрібно зважати, як часто надсилаються відкриті ключі щодо зашифрованих текстів або підписаних повідомлень і наскільки важлива швидкість обчислень відносно пропускної здатності. Вибір постквантового криптографічного алгоритму повинен ґрунтуватися на ретельному аналізі конкретних вимог і обмежень програми. Збалансування безпеки, ефективності та обмеження ресурсів є ключовим для успішної інтеграції постквантової криптографії в різні системи та протоколи. Оскільки сфера постквантової криптографії продовжує розвиватися, можуть з'явитися більш ефективні та оптимізовані алгоритми, що ще більше розширить можливості безпечних і практичних криптографічних рішень в еру квантових обчислень. Окрім технічних проблем, інтеграція постквантових алгоритмів потребуватиме значних фінансових та організаційних ресурсів. Компаніям і організаціям доведеться інвестувати в навчання персоналу, оновлення інфраструктури та підтримку нових систем, що може бути складним завданням в умовах обмежених бюджетів.Таким чином, успішна інтеграція постквантових криптографічних алгоритмів вимагатиме комплексного підходу, враховуючи як технічні, так і організаційні аспекти.

Майбутнє постквантових алгоритмів

Кібербезпека постквантових алгоритмів є ключовою характеристикою, яка додає значення їх роз-

витку та інтеграції в сучасні інформаційні системи. Фундаментальна концепція постквантової криптографії полягає в розробці алгоритмів, які залишаються стійкими до атак як класичних, так і квантових комп'ютерів.

Основною вимогою до постквантових алгоритмів є їх стійкість до атак потенційних квантових обчислювальних систем. Ці алгоритми розроблені, щоб залишатися безпечними навіть за наявності потужних квантових комп'ютерів. Постквантові алгоритми також повинні протистояти атакам з боку класичних обчислювальних систем. Це важливо, оскільки нові криптографічні алгоритми можуть бути вразливими до атак у перші роки після їх появи. Розробка постквантових алгоритмів повинна гарантувати, що вони не будуть вразливими до нових методів атак, у тому числі тих, які використовують квантові технології. Вони повинні пройти ретельну перевірку та аналіз безпеки, щоб переконатися в їх стійкості до різних типів атак і вразливостей. Постквантові алгоритми повинні бути готові до оновлень та адаптації, оскільки криптографічний ландшафт постійно розвивається, і з часом можуть з'явитися нові атаки та методи [25].

Кожна організація повинна вжити заходів перед початком ери квантових обчислень, що наступає. Застарілі та квантово нестійкі криптографічні методи повинні бути негайно замінені надійними альтернативами. Цей проактивний перехід до існуючої квантово-стійкої криптографії має бути головним пріоритетом, де це можливо. Актуальність цієї зміни полягає в потенційній вразливості поточних криптографічних систем до квантових атак. Застосовуючи квантово-стійку криптографію, організації можуть зміцнити свій захист і забезпечити довговічність безпеки своїх даних.

Очікується, що більшість ранніх квантових систем застосують гібридний підхід, використовуючи комбінацію як квантових, так і класичних алгоритмів. Ця гібридна модель буде розроблена для використання сильних сторін як квантових, так і класичних обчислень для створення більш надійних і ефективних рішень для різних систем. Гібридний підхід пропонує організаціям можливість використати новий потенціал квантових обчислень, зберігаючи при цьому сумісність із усталеною класичною інфраструктурою. Він також надасть поступовий перехід, оскільки квантові технології продовжують розвиватися та стають більш застосовними для ширшого використання. У міру розвитку та зрілості галузі квантових обчислень очікується, що інтеграція квантових і класичних технологій стане більш плавною та гнучкою, що призведе до реалізації більш потужних та ефективних квантових систем.

Квантово-стійка криптографія здатна суттєво зменшити ризики, пов'язані з квантовими атаками, але все ще залишається залежною від класичних обчислювальних методів, що робить її проміжним рішенням на шляху до повністю квантових технологій. Повністю квантові технології — це технології, які використовують квантові принципи на всіх рівнях своєї роботи. Це включає квантові комп'ютери, квантову криптографію та квантові мережі, де всі процеси і рішення базуються на властивостях квантової механіки. Такі технології здатні значно підвищити продуктивність обчислень і забезпечити рівень безпеки, який неможливо досягти з використанням класичних обчислювальних методів. Наприклад, квантова криптографія, як-от квантовий розподіл ключів (QKD), гарантує абсолютну безпеку передачі даних, оскільки будь-яка спроба перехоплення одразу буде виявлена через зміну квантових станів [26]. Повністю квантові рішення стосуються майбутнього стану, коли квантові обчислювальні технології будуть не тільки повністю розроблені, але й інтегровані в різні аспекти роботи інформаційних систем [27].

Отже, повністю квантові технології — це майбутнє інформаційної безпеки, де всі елементи систем будуть працювати на базі квантових принципів, забезпечуючи найвищий рівень захисту від будь-яких загроз, включаючи ті, які можуть виникнути з розвитком квантових обчислень.

Висновки. Квантові комп'ютери представляють собою революцію в обчислювальній техніці, здатну змінити фундаментальні підходи до вирішення складних завдань. Однак, з їхнім розвитком виникають нові загрози для традиційних криптографічних алгоритмів, які використовуються для захисту даних у сучасних інформаційних системах.

Для зламу поточних криптографічних алгоритмів за допомогою квантового комп'ютера справді потрібен масштабний квантовий комп'ютер із значною кількістю кубітів. Кількість кубітів, необхідних для зламу конкретних алгоритмів, залежить від рівня безпеки алгоритму та обраного методу квантової атаки. Проте експоненціальний ріст розвитку квантових комп'ютерних технологій показує, що шторм наближається дуже швидко. Квантово-стійка криптографія стає критично важливою для забезпечення безпеки в епоху квантових обчислень. Ці алгоритми розробляються з урахуванням потенційних можливостей квантових комп'ютерів і покликані зберегти безпеку даних, навіть коли класичні методи шифрування стануть вразливими. Дослідники та експерти галузі працюють разом, щоб розробити та перевірити ці алгоритми, та забезпечити їх безпеку і ефективність у реальних системах. Хоча терміни розгортання квантових комп'ютерів залишаються невизначеними, перехід на постквантові криптографічні алгоритми є розумним кроком для захисту нашої цифрової безпеки в епоху квантових обчислень.

Проте, у довгостроковій перспективі, повністю квантові рішення, включаючи квантову криптографію, можуть стати золотим стандартом захисту інформації. Використання квантових принципів для створення систем безпеки, що є невразливими до будь-яких атак, зробить квантові технології не лише інструментом для зламування існуючих шифрів, але й основою для створення нових, незламних криптографічних систем. Таким чином, майбутнє інформаційної безпеки залежить від розвитку та впровадження квантових технологій, які можуть забезпечити абсолютно новий рівень захисту та продуктивності. Постквантова криптографія вносить значні зміни в сферу криптографії та безпеки, але вона також відкриває нові можливості для забезпечення стійкості цифрової інфраструктури перед обличчям зростаючої загрози квантових комп'ютерів.

Список літератури

[1]. L.K. Grover. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the twenty-eighth annual ACM symposium on Theory of computing.

[2]. S. Yevseiev, O. Tsyhanenko, A. Gavrilova, V. Guzhva, O. Milov, V. Moskalenko, I. Opirskyy, O. Roma, B. Tomashevsky, O. Shmatko. (2019). Development of niederreiter hybrid crypto-code structure on flawed codes. Eastern-european journal of enterprise technologies. Information and controlling system 1, 9 (97), pp. 27-38. https://doi.org/10.15587/1729-4061.2019.156620.

[3]. A. Sahun, V. Khaidurov, V. Lakhno, I. Opirskyy, V. Chubaievskyi, O. Kryvoruchko., A. Desiatko. (2021). Devising a method for improving crypto resistance of the symmetric block cryptosystem RC5 using nonlinear shift functions. Eastern-European Journal of Enterprise Technologies, 5 (113), pp. 17–29. https://doi.org/10.15587/1729-4061.2021.240344.

[4]. I. Opirskyy, Y. Sovyn and O. Mykhailova. (2022). Heuristic Method of Finding Bitsliced-description of Derivative Cryptographic S-box," 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), pp. 104-109. https://doi.org/10.1109/TCSET55632.2022.9766883.

[5]. D.J. Bernstein, J. Buchmann, E. Dahmen. (2016). Code-based cryptography.

[6]. D.J. Bernstein. (2019). Visualizing size-security tradeoffs for lattice-based encryption. IACR Cryptol. ePrint Arch. pp. 655.

[7]. A. Casanova, J.C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, J. Ryckeghem. (2017). A great multivariate short signature. Submission to NIST.

[8]. R.A. Grimes. (2020). Cryptography Apocalypse.

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

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

[11]. G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta, R. Perlne, A. Robinson, D. Smith-Tone, Y.-K. Liu. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process. NIST Publications. https://doi.org/10.6028/NIST.IR.8413.

[12]. M. Kumar. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. Array, Volume 15, Article 100242. https://doi.org/10.1016/j.array.2022.100242.

[13]. M. Baldi, P. Santini, G. Cancellieri. (2017). Post-quantum cryptography based on codes: state of the art and open challenges. AEIT International Annual Conference. https: // doi.org / 10.23919 / aeit.2017.8240549.

[14]. P. Wallden, E. Kashefi. (2021). Cyber security in the quantum Era.

[15]. D. Bellizia, N. Mrabet, A. P. Fournaris, S. Pontié, F. Regazzoni; F.-X. Standaert, É. Tasso. (2021). Post-Quantum Cryptography: Challenges and Opportunities for Robust and Secure HW Design. IEEE International Symposium on Defect and fault tolerance in VLSI and Nanotechnology systems (DFT), pp. 1-6. https://doi.org/10.1109/DFT52944.2021.9568301.

[16]. R. Asif. (2021). Post-quantum cryptosystems for internet-of-Things: a Survey on lattice-based algorithms. IoT, 2 (1), pp. 71-91. https://doi.org/10.3390/iot2010005.

[17]. W. Buchanan, A. Woodward. (2016). Will quantum computers Be the end of public key encryption? Journal of Cyber Security Technology, 1 (1), pp. 1-22. https://doi.org/10.1080/23742917.2016.1226650.

[18]. L. Chen. (2017). Cryptography standards in quantum time: new wine in an Old Wineskin? IEEE Security & Privacy 15 (4), pp. 51-57. https://doi.org/10.1109/MSP.2017.3151339.

[19]. C. Bernhardt. (2019). Quantum Computing for Everyone. Cambridge, MA: MIT Press.

[20]. P. Hauke, H.G. Katzgraber, W. Lechner, H. Nishimori, W.D. Oliver. (2020). Perspectives of quantum annealing: Methods and implementations. Reports on Progress in Physics 83 (5), Article 054401.

[21]. A. Maitra, J. Samuel, S. Sinha. (2019). Likelihood Theory in a Quantum World: Tests with Quantum coins and computers. Pramana, J Phys 94, 57. https://doi.org/10.1007/s12043-020-1926-9.

[22]. M. Raavi1, S. Wuthier1, P. Chandramouli, Y. Balytskyi, X. Zhou1, and S.-Y. Chang1. (2021). Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms. ACNS 2021: Applied Cryptography and Network Security, pp. 424-447. https://doi.org/10.1007/978-3-030-78375-4_17.

[23]. U. Banerjee, S. Das, A.P. Chandrakasan. (2020). Accelerating post-quantum cryptography using an Energy-efficient TLS Crypto-Processor. 2020 IEEE International Symposium on Circuits and Systems. https://doi.org/10.1109/iscas45731.2020.9180550.

[24]. W. Barker, W. Polk, M. Souppaya. (2021). Getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms. NIST Cybersecurity White Paper. https: // doi.org / 10.6028/NIST.CSWP.04282021.

[25]. F. Borges, P.R. Reis, D. Pereira. (2020). A Comparison of security and its performance for key Agreements in post-quantum cryptography. IEEE Access, 8, pp. 142413-142422. https: // doi.org / 10.1109 /access.2020.3013250.

[26]. V. Pastushenko, D. Kronberg. (2023). Improving the Performance of Quantum Cryptography by Using the Encryption of the Error Correction Data. Entropy 25, Article 956. https://doi.org/10.3390/e25060956

[27]. C. Portmann, R. Renner. (2022). Security in quantum cryptography. Rev.Mod.Phys 94, Article 025008. https: // doi.org /10.1103/RevModPhys.94.025008.

УДК 004.056

Vorobets P., Horpenyuk A., Opirskyy I. Transition to post-quantum cryptography: challenges, standardization, and prospects

Abstract. *This article provides a detailed analysis of the problems and prospects of the implementation of post-quantum cryptographic algorithms, which are becoming more and more relevant in connection with the development of quantum computing. The main challenges related to the standardization of post-quantum algorithms are considered, in particular the issues of flexibility of algorithms, their performance, complexity of implementation and uncertainty regarding the appearance of quantum computers capable of breaking modern cryptosystems. Particular attention is paid to the assessment of the current state of development of post-quantum cryptographic standards, as well as to the analysis of potential scenarios of the transition to new information protection systems. The main role here is played by the US National Institute of Standards and Technology (NIST). NIST provides key coordination and leadership in the development of post-quantum cryptography standards, initiating an open competition process to identify the most promising cryptographic algorithms. The program launched by NIST involves a multi-year process of evaluating, testing and selecting algorithms capable of providing resistance to attacks by quantum computers. Within this program, a wide range of algorithms were considered, which differ in encryption approaches, performance and degree of security. On the basis of the conducted research, recommendations are proposed for the effective management of the transition period from traditional cryptographic systems to post-quantum solutions, which should ensure reliable data security in the face of new technological challenges. In particular, approaches to managing the transition period, risk reduction strategies, as well as assessment of possible threats and ways to minimize them are offered. As a result, the article provides a valuable basis for the formation of a strategy for the safe adaptation of information systems in the age of quantum technologies.*

Keywords: *post-quantum cryptography, quantum computers, standardization process, NIST, post-quantum cryptographic systems.*

Воробець Павло Андрійович, аспірант, кафедра захисту інформації, Національного університету «Львівська політехніка».

Pavlo Vorobets, PhD student, Department of Information Security, Lviv Polytechnic National University.

Горпенюк Андрій Ярославович, кандидат технічних наук, доцент, кафедра захисту інформації, Національного університету «Львівська політехніка».

Andriy Horpenyuk, doctor of Technical Sciences, assistant professor, Department of Information Security, Lviv Polytechnic National University.

Опірський Іван Романович, доктор технічних наук, професор, кафедра захисту інформації, Національного університету «Львівська політехніка».

Ivan Opirskyy, doctor of Technical Sciences, professor, Department of Information Security, Lviv Polytechnic National University.

Отримано *9 червня 2024 року*, затверджено редколегією *26 червня 2024 року*