DOI 10.15276/imms.v14.no3.183
УДК 004.04

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 3, pp. 183-190

КРИПТОГРАФІЯ ПІСЛЯ КВАНТОВОЇ ЕРИ: НОВІ ВИКЛИКИ ТА РІШЕННЯ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

А. С. Коляда[1], А. В. Павлишко[2], В. Ф. Літвінов[3]

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Emails: akolyada@gmail.com[1], pavlyshko.a.v@op.edu.ua[2], litvinov.v.f@op.edu.ua[3]

У сучасному світі, де квантові технології швидко розвиваються, традиційні криптографічні системи стикаються з серйозними викликами. Квантові обчислення здатні порушити основи сучасних криптографічних протоколів, таких як RSA і ECC, шляхом застосування алгоритмів, які можуть зламати ці системи за рекордно короткий час. Ця стаття присвячена аналізу впливу квантових технологій на криптографію, а також необхідності створення нових рішень для захисту інформації. Метою даного наукового дослідження є оцінка сучасного стану постквантової криптографії та виявлення нових підходів, які можуть забезпечити надійний захист інформації в умовах квантового прогресу. У роботі розглядаються такі напрямки, як криптографія на основі решіток, кодова криптографія, мультиваріантна криптографія та криптографія на основі хеш-функцій. Наукова і практична значущість цієї роботи полягає в тому, що вона допомагає зрозуміти виклики, які постають перед сучасною криптографією в умовах квантових обчислень, і пропонує можливі рішення для їх подолання. Методологія дослідження включає огляд літератури, аналіз існуючих криптографічних систем, а також оцінку їх стійкості до квантових атак. Основні результати роботи показують, що підходи на основі решіток та кодів мають високу стійкість до квантових атак і можуть бути використані для розробки нових криптографічних протоколів. Також було виявлено, що мультиваріантна криптографія, хоча і показує обіцяючи результати, потребує подальших досліджень для оптимізації продуктивності. Висновки дослідження підкреслюють важливість комплексного підходу до безпеки інформації в умовах квантового прогресу. Цінність проведеного дослідження полягає в його внеску у розвиток постквантової криптографії, оскільки воно не тільки визначає актуальні виклики, але й пропонує нові напрямки для майбутніх досліджень. Практичне значення підсумків роботи полягає в тому, що результати можуть бути використані для розробки безпечних інформаційних систем у контексті квантових загроз.

Ключові слова: постквантова криптографія, інформаційна безпека, криптографія на основі решіток, кодова криптографія, мультиваріантна криптографія, квантові комп'ютери, криптографічні протоколи.

Вступ. З розвитком квантових обчислень криптографія, яка є основою сучасної інформаційної безпеки, стикається з новими викликами. Сучасні криптографічні алгоритми, такі як RSA, DSA та алгоритми на основі еліптичних кривих, широко використовуються для захисту конфіденційних даних, онлайн-транзакцій та комунікацій в інтернеті. Вони забезпечують надійну безпеку завдяки складності факторизації великих чисел або вирішення дискретних логарифмів, що є обчислювально непосильними для класичних комп’ютерів. Проте з розвитком квантових обчислень постала загроза традиційним криптографічним методам, які вже кілька десятиліть використовуються для забезпечення інформаційної безпеки. Квантові комп'ютери використовують принципи квантової механіки, зокрема квантову суперпозицію та квантову заплутаність, завдяки яким вони можуть одночасно обробляти багато варіантів рішення задачі, що робить їх набагато швидшими для певних обчислювальних завдань, як, наприклад, факторизація великих чисел або пошук у великій базі даних. Потужність квантових комп'ютерів дозволяє зламати багато з існуючих криптосистем за допомогою алгоритмів Шора [1] та Гровера [2], що ставить

під загрозу безпеку величезних обсягів даних у різних сферах – від державних секретів до банківських транзакцій. Квантові комп’ютери здатні виконувати обчислення, які займають тисячоліття на класичних машинах, у рекордно короткі строки. Алгоритм Шора, зокрема, може ефективно факторизувати великі числа, що ставить під загрозу схеми шифрування на основі факторизації. Алгоритм Гровера зменшує час пошуку у великих просторах ключів, що ставить під сумнів стійкість багатьох симетричних шифрів. Ці відкриття вже підштовхнули криптографічну спільноту до пошуків нових рішень – криптографії після квантової ери (post-quantum cryptography), яка повинна забезпечити стійкість до атак квантових комп'ютерів.

Основна мета постквантової криптографії полягає у створенні нових криптографічних алгоритмів, які залишаться надійними навіть у світі квантових обчислень. Науковці та інженери активно працюють над різноманітними підходами, що базуються на складних математичних проблемах, які квантові комп’ютери не можуть вирішити ефективно. Ці методи пропонують нові схеми шифрування, цифрових підписів та аутентифікації, які мають витримувати атаки квантових комп’ютерів. Зокрема, криптографія на основі решіток демонструє значний потенціал завдяки своїй стійкості до відомих квантових атак. Вона використовує проблеми з лінійною алгеброю, такі як проблема найкоротшого вектора або навчання з похибками, які є складними не лише для класичних, але й для квантових обчислень. Інші підходи, такі як кодова криптографія та криптографія на основі хеш-функцій, також пропонують надійні рішення, але їх застосування наразі обмежене специфічними сферами або потребує великих обсягів даних для реалізації.

У цій статті ми розглянемо сучасні виклики, що постають перед криптографією в епоху квантових обчислень, а також проаналізуємо перспективні криптографічні методи, які можуть захистити інформаційну безпеку у майбутньому. Особливу увагу буде приділено оцінці ефективності нових підходів, можливим шляхам стандартизації та викликам їх впровадження у реальні системи. Таким чином, криптографія після квантової ери потребує глибокого переосмислення сучасних підходів до шифрування, щоб забезпечити надійний захист даних навіть в умовах потужних квантових загроз.

Огляд літератури. Квантові обчислення, хоча ще перебувають на ранніх стадіях свого розвитку, вже спровокували значні зміни в галузі криптографії та інформаційної безпеки. Відкриття алгоритмів Шора та Гровера стало каталізатором для досліджень у галузі постквантової криптографії, мета якої – створення стійких до квантових атак криптографічних систем. Останні дослідження в галузі криптографії свідчать про неминучий вплив квантових обчислень на безпеку цифрових комунікацій. У роботі Шора [1] запропоновано алгоритм, який дозволяє квантовим комп'ютерам ефективно факторизувати великі числа, що робить такі криптосистеми, як RSA та ECC, вразливими. Крім того, дослідження Гровера [2] показали, що квантові пошукові алгоритми можуть знизити ефективність стійких до атак алгоритмів симетричного шифрування, таких як AES, скорочуючи час необхідний для атаки грубою силою в квадратному ступені. Сучасна література охоплює різноманітні підходи до цієї проблеми, серед яких виділяються криптографія на основі решіток, кодова криптографія, мультиваріантні методи, хешована криптографія, кільцеві схеми та інші. За останні кілька років кілька наукових праць було присвячено дослідженню стійких до квантових обчислень алгоритмів. Наприклад, дослідження Чанга [3] та Янга [4] фокусуються на постквантовій криптографії, що базується на математичних проблемах, стійких до квантових атак. Зокрема, криптографія на основі решіток та схем кодування, таких як NTRU та Kyber, стали предметом пильної уваги вчених та інженерів. Кодова криптографія, започаткована ще в 1978 році Робертом МакЕлісом, стала одним із найстаріших підходів до постквантової криптографії. В основі цього методу лежить використання важкості декодування випадкових лінійних кодів, що вважається складною задачею навіть для квантових комп’ютерів. Однак, попри свою стійкість до

квантових атак, криптосистема McEliece має певні обмеження, зокрема пов'язані з великими розмірами ключів, що ускладнює її використання у реальних умовах. Робота Бернштейна, Ланге та Пітерса [5] досліджує слабкі місця цієї криптосистеми та пропонує шляхи їх усунення. Автори показали, що за допомогою збільшення розмірів ключів можна значно підвищити безпеку системи, але це також призводить до збільшення вимог до пам'яті та обчислювальних ресурсів. Попри ці проблеми, кодова криптографія залишається важливою частиною постквантової криптографії, і тривають активні дослідження щодо її оптимізації для зменшення обчислювальних ресурсів та покращення продуктивності. Загалом, література у галузі постквантової криптографії демонструє велику кількість досліджень, спрямованих на створення криптографічних систем, здатних витримати атаки квантових комп'ютерів. Незважаючи на різноманітність підходів, існує спільна мета – розробка алгоритмів, які забезпечать безпеку у майбутньому квантовому світі.

Мета роботи. Метою цієї роботи є всебічне дослідження криптографічних методів, здатних забезпечити інформаційну безпеку в умовах розвитку квантових обчислень, а також аналіз нових викликів, що постають перед сучасною криптографією у світлі квантових загроз. Особливу увагу приділено постквантовим алгоритмам, здатним витримати атаки квантових комп'ютерів, та їх практичним застосуванням. У роботі передбачається вивчення сучасного стану постквантової криптографії. Вже сьогодні пропонуються нові алгоритми для шифрування, цифрових підписів і аутентифікації, що мають стати основою для побудови стійких до квантових атак систем. Окрім теоретичних аспектів, метою є також оцінка ефективності запропонованих криптосистем, їх продуктивність і практичні можливості впровадження. Робота також спрямована на визначення ключових викликів, з якими стикається постквантова криптографія, таких як збільшення розмірів ключів, вимоги до пам'яті та обчислювальних ресурсів, що можуть обмежувати їх практичне застосування. На основі цього аналізу буде запропоновано шляхи вирішення цих проблем та перспективи стандартизації нових криптографічних алгоритмів для захисту даних у квантовій ері. Таким чином, мета роботи полягає в розробці теоретичної та практичної бази для побудови стійких до квантових атак криптографічних систем, здатних забезпечити надійний захист інформації у світі майбутнього квантового обчислення.

Основний розділ. Постквантова криптографія, що включає в себе розробку криптографічних схем, стійких до квантових комп'ютерів, є активною сферою досліджень, яка охоплює кілька підходів: криптографія на основі решіток, кодова криптографія, мультиваріантні методи, криптографія на основі хеш-функцій та інші перспективні напрями. Нижче детально розглянуті основні результати досліджень цих методів та їх практичне застосування.

Криптографія на основі решіток (Lattice-based cryptography) є одним із найбільш перспективних і досліджуваних напрямків постквантової криптографії. Цей підхід базується на складних математичних проблемах, які важко вирішити навіть для квантових комп'ютерів. Основною перевагою криптографії на основі решіток є її стійкість до відомих квантових атак, а також гнучкість, що дозволяє створювати різноманітні криптографічні схеми і має широкий спектр застосувань, зокрема для шифрування, цифрових підписів та схем аутентифікації. Проблема навчання з похибками (Learning with Errors, LWE), запропонована Одедом Регеєм [6], є однією з центральних концепцій у криптографії на основі решіток. Дослідження Регева стало фундаментом для створення багатьох сучасних криптосистем, що отримали популярність у наукових та інженерних спільнотах завдяки своїй теоретичній стійкості та потенційній ефективності. Цей підхід ґрунтується на припущенні, що задача вирішення системи лінійних рівнянь із випадковими похибками є складною для розв’язання навіть для квантових комп’ютерів. У класичному випадку задача вирішення таких систем є NP-складною, що робить її придатною для криптографічних

застосувань. LWE відкрив широкі можливості для створення криптографічних алгоритмів, таких як системи шифрування, стійкі до квантових атак. Крім того, на основі LWE було розроблено кілька схем цифрових підписів, що використовуються у сучасних криптографічних стандартах. Дослідження Регева стало фундаментом для створення багатьох сучасних криптосистем, що отримали популярність у наукових та інженерних спільнотах завдяки своїй теоретичній стійкості та потенційній ефективності. Однак ефективність реалізації LWE-заснованих систем залишається однією з основних проблем, оскільки такі системи часто вимагають значних обчислювальних ресурсів і великих розмірів ключів. Щоб покращити продуктивність криптосистем на основі решіток, у подальших дослідженнях було запропоновано модифікацію LWE – проблему навчання з похибками над кільцями (Ring-LWE). Основна ідея цієї модифікації полягає у заміні векторів на кільцеві елементи, що значно знижує обчислювальну складність криптографічних операцій. Дослідження в цьому напрямку, зокрема роботи Любасевського, Пейкерта і Регея [7], продемонстрували значне покращення ефективності без втрати безпеки, що робить Ring-LWE одним із провідних кандидатів для стандартизації постквантових криптосистем. Системи на основі Ring-LWE, такі як шифрування Kyber та схема підпису Dilithium, вже були рекомендовані [8] для стандартизації у рамках ініціативи NIST (National Institute of Standards and Technology) з постквантової криптографії. Ці системи забезпечують високу стійкість до квантових атак при відносно невеликих вимогах до обчислювальних ресурсів, що робить їх придатними для практичного використання у багатьох сферах, від мобільних пристроїв до хмарних сервісів. Дослідження в галузі криптографії на основі решіток продовжують розвиватися, наприклад, Кріс Пайкерт у своїй роботі [9] зробив огляд десятирічних досягнень у цій галузі. Він робить акцент на перспективних алгоритмах, особливо на схемах шифрування та цифрових підписів, що базуються на проблемі навчання з помилками (LWE). Огляд включає детальний аналіз сучасних підходів, таких як решіткові алгоритми, і надає напрямки для подальших досліджень у цій галузі. Робота Пайкерта стала корисним ресурсом для криптографів та дослідників, які шукають надійні методи захисту в умовах майбутніх загроз від квантових комп'ютерів. Крім LWE, існують інші важливі математичні проблеми, на яких базується криптографія на основі решіток, зокрема проблема найкоротшого вектора (Shortest Vector Problem, SVP) та проблема найближчого вектора (Closest Vector Problem, CVP). Ці задачі є надзвичайно складними як для класичних, так і для квантових комп’ютерів, що робить їх привабливими для криптографії. На основі цих задач розробляються криптографічні алгоритми, які пропонують стійкі до квантових атак рішення. Однак ці проблеми вимагають глибоких досліджень у галузі теоретичної інформатики, квантової теорії та обчислювальної математики. Прогрес у їх розв'язанні має безпосередній вплив на безпеку сучасної та майбутньої криптографії, особливо в контексті загроз з боку квантових комп'ютерів.

Кодова криптографія (Code-based cryptography). Кодова криптографія – це один із найстаріших підходів до постквантової криптографії, який ґрунтується на використанні важкості декодування випадкових лінійних кодів. Найвідоміша система в цій галузі – криптосистема McEliece, запропонована ще в 1978 році. Вона використовує коди Гоппа (Goppa codes) для забезпечення стійкості до атак. Основною перевагою криптосистеми McEliece є її стійкість до атак квантових комп’ютерів, зокрема до алгоритму Шора. Однак ключовою проблемою залишається надмірно великий розмір публічних і приватних ключів, що ускладнює її впровадження у багатьох сучасних системах. Попри це, McEliece залишається одним із найбільш вивчених і надійних підходів у постквантовій криптографії. Останні дослідження, зокрема робота Берштейн, Ланге та Петерс [5], зосереджені на оптимізації цієї криптосистеми для зменшення вимог до пам'яті та підвищення ефективності, що відкриває нові можливості для її використання у практичних застосуваннях. Крім класичних кодів Гоппа, у кодовій

криптографії досліджуються й інші коди, зокрема коди LDPC (Low-Density Parity-Check) та коди на основі полів Ріда-Соломона. Ці коди також можуть використовуватися для побудови стійких криптосистем, однак вони стикаються з подібними проблемами, що й криптосистема McEliece, зокрема великими розмірами ключів та значною складністю декодування. Подальші дослідження у цій галузі спрямовані на оптимізацію використання цих кодів для підвищення ефективності криптосистем та зменшення вимог до обчислювальних ресурсів.

Мультиваріантна криптографія (Multivariate cryptography) базується на використанні нелінійних систем рівнянь з багатьма змінними над кінцевими полями. Завдяки своїй математичній складності, цей підхід є одним із перспективних для створення стійких до квантових атак криптосистем. Джунь Дін та Бені Янг у своїй книзі [10] надали огляд основних алгоритмів, що використовуються у мультиваріантній криптографії. Одним із найвідоміших прикладів мультиваріантної криптографії є алгоритм UOV (Unbalanced Oil and Vinegar), який використовується для створення схем цифрових підписів. Він базується на вирішенні систем нелінійних рівнянь (зокрема квадратичних) у скінченному полі. UOV розвивається на основі ідеї попередньої схеми Oil and Vinegar, яка має дві групи змінних: "масляні" змінні (oil variables) і "оцтові" змінні (vinegar variables). В UOV кількість змінних оцту значно більша за кількість масляних, що робить систему асиметричною, звідси й назва "Unbalanced." Схема є стійкою до квантових атак і забезпечує високу продуктивність. Однак дослідження виявили, що UOV може бути вразливим до певних типів класичних атак, що підкреслює необхідність подальших досліджень у цьому напрямку. Rainbow – це ще одна мультиваріантна криптографічна схема підпису на основі квадратичних рівнянь, яка розвинута з моделі UOV. Rainbow розширює концепцію UOV шляхом додавання кількох шарів змінних, кожен з яких взаємодіє один з одним певним чином. Цей підхід робить систему складнішою для аналізу, оскільки при обчисленні підпису і перевірці враховуються кілька шарів змінних, що взаємодіють нелінійно. Алгоритм Rainbow був фіналістом в конкурсі NIST на стандартизацію постквантових криптографічних алгоритмів у категорії цифрових підписів і розглядається як можливе рішення для захисту інформації в епоху квантових обчислень.

Хешована криптографія (Hash-based cryptography) на основі хеш-функцій є ще однією перспективною галуззю постквантової криптографії. Вона є одним із найстаріших та найнадійніших підходів у криптографії і може забезпечити стійкість до атак квантових комп'ютерів. Важливим аспектом хешованої криптографії є те, що її безпека ґрунтується на надійності хеш-функцій до знаходження колізій, таких як SHA-256 чи SHA-3, що ускладнює злам систем за допомогою квантових обчислень. Ральф Меркл ще у 1989 році запропонував підхід до цифрових підписів, заснований на хешованих деревах, що отримали назву Merkle Trees Однак, однією з проблем є те, що цей метод може вимагати великих обсягів обчислювальних ресурсів та пам'яті для збереження відповідних дерев. У сучасних дослідженнях, таких як публікації Бернштейн, Хюльсінг та інших [11], було запропоновано вдосконалені методи хеш-шифрування, зокрема системи підписів SPHINCS+. Вона використовує кілька рівнів дерев Меркла для створення багаторазових підписів. В основі його підписів лежить схема підпису Лемпорта (Lamport OTS) або Winternitz OTS (WOTS), що використовує хеш-функції для обчислення підписів. SPHINCS+ також інтегрує алгоритм Hypertree для поліпшення ефективності та скорочення розміру підписів. Ці підписи не потребують збереження стану та є практичними для використання у реальних умовах, що робить їх потенційним стандартом у постквантовій криптографії. Також SPHINCS+ був одним із фіналістів конкурсу NIST з постквантової криптографії, що означає він вважається однією з перспективним рішенням для стандарту постквантової криптографії завдяки своїй універсальності, стійкості до квантових атак і здатності підписувати багаторазово.

Результати та обговорення. У результаті проведеного аналізу сучасного стану постквантової криптографії були виявлені кілька ключових напрямків, які можуть стати основою для забезпечення інформаційної безпеки в умовах квантової ери. Перш за все, успішність постквантових криптографічних систем у великій мірі залежить від їх математичної стійкості до квантових атак. Основні результати нашого дослідження зосереджені на наступних підходах.

1. Криптографія на основі решіток: Розробка систем, таких як LWE і Ring-LWE, показала, що алгоритми, основані на складних задачах решіток, демонструють високу стійкість до квантових атак і забезпечують конкурентоспроможну продуктивність. Системи, такі як Kyber і Dilithium, уже рекомендовані для стандартизації, що свідчить про їх перспективність для практичного використання.
2. Кодова криптографія: Проблеми, пов'язані з великими розмірами ключів у криптосистемах, таких як McEliece, були виявлені як основні обмеження для їх впровадження. Однак продовження досліджень щодо оптимізації кодових систем може призвести до створення більш ефективних схем, які зможуть конкурувати з іншими постквантовими підходами.
3. Мультиваріантна криптографія: Алгоритми UOV і Rainbow продемонстрували потенціал для розробки стійких до квантових атак систем цифрового підпису. Проте необхідно подальше дослідження щодо їх уразливостей та оптимізації для досягнення кращої продуктивності.
4. Криптографія на основі хеш-функцій: безпека ґрунтується на надійності хеш-функцій до знаходження колізій, що ускладнює злам систем за допомогою квантових обчислень. Розробка нових хеш-функцій, які б забезпечували вищу стійкість, є актуальним напрямком дослідження. Система SPHINCS+ була одним із фіналістів конкурсу NIST з постквантової криптографії, що свідчить про її перспективність.

Обрані напрями постквантової криптографії показують, що дослідники активно працюють над створенням безпечних алгоритмів, однак існує багато викликів, які потрібно подолати. По-перше, продуктивність нових систем залишається важливим питанням. Багато постквантових алгоритмів вимагають більших обчислювальних ресурсів і пам'яті в порівнянні з традиційними криптографічними методами. Це може стати перешкодою для їх впровадження в реальні системи, особливо в середовищах з обмеженими ресурсами, таких як мобільні пристрої та IoT (інтернет речей). По-друге, стандартизація нових криптографічних алгоритмів є критично важливою. Рекомендування NIST криптосистем на основі LWE та кодової криптографії вже свідчить про важливість консенсусу у виборі стійких алгоритмів для глобальної інформаційної інфраструктури. Однак, не всі алгоритми можуть відповідати вимогам безпеки та продуктивності, які ставляться до них. Третім важливим аспектом є необхідність детального аналізу безпеки нових алгоритмів у порівнянні з традиційними методами. Дослідження показують, що, хоча нові підходи демонструють обіцянки, їх реальна безпека ще потребує більшого тестування у практичних умовах. Окрім технічних аспектів, важливими є також питання впровадження нових криптографічних систем. Це включає не лише технічні, але й правові та етичні аспекти, пов'язані з використанням криптографії в різних сферах. Системи, які забезпечують вищий рівень безпеки, можуть стати об'єктом підвищеної уваги з боку держав і регуляторів, що може вплинути на їх впровадження.

Висновки. Загалом, результати даного дослідження підтверджують, що постквантова криптографія є важливим напрямком, що потребує подальших досліджень та розробок. Актуальні підходи, такі як криптографія на основі решіток, кодова криптографія та мультиваріантна криптографія, показали свою стійкість до квантових атак, але ще потрібно подолати ряд викликів, щоб забезпечити їх широке впровадження. Отже, існує

безліч викликів, які потрібно вирішити, щоб забезпечити ефективну інтеграцію нових криптографічних алгоритмів у практичні системи. Успіх у цій сфері вимагатиме колективних зусиль з боку дослідників, розробників, регуляторів та промисловості, щоб забезпечити безпечний інформаційний обмін у квантовій ері. Наступні кроки в цьому напрямку повинні включати оптимізацію алгоритмів, стандартизацію, а також проведення додаткових досліджень щодо їх безпеки в реальних умовах. Успіх постквантової криптографії матиме важливе значення для збереження інформаційної безпеки в умовах, коли квантові комп'ютери стануть звичайним явищем.

Список літератури

1. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring. *35th Annual ACM Symposium on Theory of Computing*. 1997. С. 124–134.p
2. Grover L. K. A fast quantum mechanical algorithm for database search. *28th Annual ACM Symposium on Theory of Computing.* 1996. С. 212–219.
3. Chang Y. Post-Quantum Cryptography: Lattice-Based Cryptographic Algorithms *Journal of Cryptographic Research*. 2020. V. 8. No. 4. P. 145–161.
4. Young S. The Future of Post-Quantum Cryptography: Algorithms and Challenges *Information Security Review*. 2021. V. 12, No. 2. P. 56–67.
5. Bernstein D. J., Lange T., Peters C. Attacking and defending the McEliece cryptosystem. *International Workshop on Post-Quantum Cryptography*. 2008. P. 31–46.
6. Regev O. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*. 2005. V. 56. No 6. P. 1–40.
7. Lyubashevsky V., Peikert C., Regev O. On ideal lattices and learning with errors over rings. *Journal of the ACM.* 2010. V. 60, No6. P. 1–35.
8. National Institute of Standards and Technology. NIST announces first four quantum-resistant cryptographic algorithms. 2022. URL: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.
9. Peikert C. A Decade of Lattice Cryptography. *Foundations and Trends in Theoretical Computer Science*. 2016. V. 10. No 4. P. 283–424.
10. Din J., Yang B. Multivariate Public Key Cryptography. *Journal of Cryptographic Engineering*. 2009. V. 1.No 1. P. 35–59.
11. Bernstein D. J., Hülsing A.. SPHINCS+: Practical Stateless Hash-Based Signatures. *ACM SIGSAC Conference on Computer and Communications Security.* 2019. P. 1–15.

CRYPTOGRAPHY AFTER THE QUANTUM ERA: NEW CHALLENGES AND SOLUTIONS FOR INFORMATION SECURITY

A. S. Koliada[1], A.V. Pavlyshko[2], V. F. Litvinov[3]

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: akolyada@gmail.com[1], pavlyshko.a.v@op.edu.ua[2], litvinov.v.f@op.edu.ua[3]

In today's world, where quantum technologies are rapidly evolving, traditional cryptographic systems face serious challenges. Quantum computing has the potential to undermine the foundations of modern cryptographic protocols, such as RSA and ECC, by utilizing algorithms that can break these systems in record time. This article is dedicated to analyzing the impact of quantum technologies on cryptography, as well as the necessity of creating new solutions for information protection. The aim of this research is to assess the current state of post-quantum cryptography and identify new approaches that can ensure reliable information security in the face of quantum advancements. The paper discusses areas such as lattice-based cryptography, code-based cryptography, multivariate cryptography, and hash-based cryptography. The scientific and practical significance of this work lies in its contribution to understanding the challenges faced by contemporary cryptography in the context of quantum computing, and it offers possible solutions to overcome these challenges. The research methodology includes a literature review, analysis of existing cryptographic systems, and evaluation of their resilience to quantum attacks. The main results of the study indicate that lattice-based and code-based approaches demonstrate high resilience to quantum attacks and can be utilized for developing new cryptographic protocols. Additionally, it was found that multivariate cryptography, while showing promising results, requires further research to optimize performance. The conclusions of the research emphasize the importance of a comprehensive approach to information security in the context of quantum progress. The value of this research lies in its contribution to the development of post-quantum cryptography, as it not only identifies current challenges but also proposes new directions for future research. The practical significance of the findings is that the results can be used to develop secure information systems in the context of quantum threats.

Keywords: post-quantum cryptography, information security, lattice-based cryptography, code-based cryptography, multivariate cryptography, quantum computers, cryptographic protocols.