Лахно Валерій Анатолійович
доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів та природокористування України
ORCID: https://orcid.org/0000-0001-9695-4543
E-mail: lva964@nubip.edu.ua

Касаткін Дмитро Юрійович
кандидат педагогічних наук, доцент, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів та природокористування України
ORCID: https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА СТРАТЕГІЇ АДАПТАЦІЇ В ПРОТИСТОЯННЯ КРИПТОВАЛЮТ ТА КВАНТОВИХ КОМП'ЮТЕРІВ

Анотація. *Стаття присвячена дослідженню стійкості криптовалютних систем (КВС) в умовах нових загроз, пов'язаних із розвитком квантових обчислень. Діяльність представлена диференціальна ігрова модель, що дозволяє формалізувати взаємодія КВС і квантових комп'ютерів (КК), і навіть аналізувати їх взаємовплив. Методологія дослідження ґрунтується на застосуванні диференціальної теорії ігор для моделювання динаміки розподілу ресурсів між сторонами та оцінки їх стратегій в умовах невизначеності та конкуренції. У ході моделювання були розглянуті різні сценарії протистояння між КВС та квантовими обчисленнями, що дозволило виявити ключові закономірності та фактори, які суттєво впливають на ефективність криптографічного захисту, а також обчислювальні можливості атакуючих з використанням КК. Особливу увагу приділено аналізу різних методів захисту цифрових активів за умов можливих квантових загроз. Результати дослідження можуть бути основою для розробки нових стандартів криптографічної безпеки та адаптивних стратегій захисту, які будуть ефективними в умовах швидкого зростання обчислювальних потужностей квантових технологій.*

Ключові слова: *квантові обчислення, криптовалюти, криптографічна стійкість, математичне моделювання, ресурси розподілу, квантові загрози, стратегії захисту.*

Вступ. Сучасні виклики в галузі інформаційної безпеки (далі ІБ), пов'язані з розвитком квантових обчислень, ставлять під загрозу стійкість криптографічних методів, що лежать в основі більшості цифрових систем, у тому числі криптовалют. Криптовалюти (далі КВ), згідно з [1], можуть стати особливо вразливими в умовах появи квантових комп'ютерів (далі КК), здатних виконувати обчислення, недоступні традиційним системам. Основна проблема полягає в тому, що квантові алгоритми, такі як алгоритм Шора [2, 3], можуть ефективно вирішувати задачі, на яких базуються асиметричні криптографічні схеми, наприклад, факторизацію цілих чисел і обчислення дискретного логарифму, що потенційно дозволить зловмисникам з використанням квантових обчислювальних потужностей обходити криптографічні. Виходячи з цього, дослідження в галузі моделювання взаємодії між КВ та КК є актуальним, оскільки воно дозволить спрогнозувати динаміку протистояння між технологіями захисту даних та загрозами, спричиненими розвитком квантових обчислень. І, зокрема, моделювання з використанням методів диференціальної теорії ігор надає унікальний інструмент для аналізу адаптивних стратегій сторін, які враховують обмеженість ресурсів та динамічну зміну параметрів системи. У таких моделях ресурси сторін можна класифікувати на кілька категорій, наприклад, для КВ це, перш за все, методи та засоби криптографічного захисту, що включають алгоритми шифрування, які є стійкими до атак. Сюди також входять ресурси, спрямовані на модернізацію криптографічних механізмів у відповідь нові загрози. Відповідно, для квантових обчислень ресурси включають обчислювальні потужності КК, а також інфраструктуру та дослідницькі зусилля, спрямовані на розвиток цієї технології.

Запропонована в роботі методика аналізу передбачає побудову математичної моделі, що описує взаємодію сторін, де КВ та КК виступають як гравці. Дана модель дозволяє формалізувати процеси розподілу ресурсів та прогнозувати результати протистояння з

урахуванням різних сценаріїв. Вважаємо, що такий підхід може відкрити нові можливості для вироблення стратегій адаптації та захисту, спрямованих на мінімізацію ризиків, пов'язаних із квантовими загрозами для КВ.

Таким чином, виходячи з вище сказаного, дослідження проблеми стійкості криптовалютних систем в умовах квантових обчислень не тільки має теоретичну значимість, а й має високу практичну цінність, оскільки результати подібного аналізу можуть бути в подальшому використані для розробки нових стандартів криптографічної безпеки, створення протоколів захисту цифрових активів і формування довгострокової стратегії .

Огляд попередніх досліджень. В умовах стрімкого розвитку квантових обчислень [4, 5] посилюється необхідність у дослідженні механізмів протидії загрозам, пов'язаним із використанням КК для атак на існуючі криптографічні системи [6, 7]. Квантові алгоритми, такі як алгоритм Шора [8] та алгоритм Гровера [9], надають значні переваги у вирішенні завдань факторизації та пошуку, що ставить під загрозу безпеку традиційних криптографічних алгоритмів, таких як RSA, ECC та AES.

З іншого боку, розробка постквантових алгоритмів [10] та модернізація криптографічних систем, як було показано у роботах [8, 9-12], забезпечують активну протидію цим загрозам. Проте, динаміка протистояння між засобами захисту та атакуючими технологіями вимагає ретельного математичного моделювання, щоб передбачити поведінку обох сторін у різних сценаріях. Тому нові дослідження у цьому напрямі є релевантними.

Метою дослідження є розробка математичної моделі взаємодії криптовалютних систем та квантових комп'ютерів на основі диференціальної теорії ігор для аналізу динаміки розподілу ресурсів сторін та формування ефективних стратегій адаптації криптографічних механізмів до квантових загроз. При цьому об'єктом дослідження є криптографічні та обчислювальні системи, що взаємодіють в умовах розвитку квантових обчислень, з акцентом на криптовалютні платформи як найбільш уразливі до атаки з боку квантових комп'ютерів. Предметом дослідження є механізми розподілу ресурсів між сторонами (криптовалютами та квантовими комп'ютерами) у динамічній взаємодії, включаючи адаптивні стратегії захисту криптографічних систем та збільшення обчислювальних потужностей.

Методологія дослідження заснована на застосуванні диференціальної теорії ігор [13, 14] для моделювання взаємодії двох сторін – криптовалютних систем та квантових комп'ютерів (КК). Диференціальні ігри як розділ теорії оптимального управління дозволяють описувати динамічні процеси, де стратегічна поведінка учасників визначається зміною параметрів системи в часі. Використання запропонованої у роботі системи диференціальних рівнянь для опису стану ресурсів сторін забезпечує можливість обліку таких чинників, як обмеженість ресурсів, їх цілеспрямований розподіл та часові характеристики адаптації. У рамках побудованої моделі криптовалютні системи та КК розглядаються як гравці, які мають протилежні цілі. Для КВ метою є максимізація рівня захисту за рахунок застосування стійких криптографічних алгоритмів та модернізації механізмів безпеки. Для КК, своєю чергою, метою є досягнення обчислювальних потужностей, достатніх успішного обходу криптографічних бар'єрів.

Діяльність процес взаємодії сторін описується з допомогою набору функцій управління, що характеризують витрати ресурсів відповідні стратегії. Динаміка зміни параметрів представлена як системи звичайних диференціальних рівнянь, де кожна змінна моделі відбиває рівень ресурсів боку (наприклад, рівень криптографічного захисту, модернізаційні ресурси КВ, квантові обчислювальні потужності та ресурси інфраструктури). Для визначення оптимальних стратегій застосовуються методи чисельного аналізу та програмування, що дозволяють вивчати еволюцію системи у різних сценаріях. Візуалізація результатів обчислювальних експериментів проводилася з використанням засобів кібернетичного моделювання, що дозволило інтерпретувати отримані залежності та виявляти ключові закономірності у протистоянні сторін.

Диференційна ігрова модель криптографічної стійкості до квантових загроз.

Для детального аналізу протистояння гравців необхідно розглянути ключові змінні, що описують активні засоби криптографічного захисту та квантових комп'ютерів, а також їх взаємний вплив.

Для криптовалют та квантових комп'ютерів визначимо змінні.

Для КВ:

Активні засоби КВ:

$z_1(t)-$ ефективність поточного криптографічного алгоритму;

$z_2(t)-$ ресурси модернізації (наприклад, перехід на постквантові алгоритми).

Активні засоби квантових комп'ютерів:

$z_3(t)-$ обчислювальна потужність квантового комп'ютера

$z_4(t)-$ ресурси підвищення обчислювальної потужності.

Активні засоби криптографічного захисту характеризують поточні та потенційні можливості систем криптографічного захисту у протидії загрозам, включаючи атаки квантових комп'ютерів. Вони описуються двома основними аспектами. Перший – це ефективність поточного криптографічного алгоритму. Ця змінна відбиває, наскільки стійкий існуючий криптографічний алгоритм атак, зокрема з використанням квантових обчислень. Наприклад, алгоритми RSA та ECC (еліптичні криві) демонструють високу стійкість до класичних атак, але вразливі для атак з використанням квантових комп'ютерів, таких як алгоритм Шора . Ефективність може бути виражена в бітах криптографічної стійкості, наприклад, 128-бітний AES вважається стійким до більшості атак, але його стійкість має бути переглянута в умовах квантової загрози. Якщо система використовує 256-бітний алгоритм AES для шифрування конфіденційних даних, ефективність алгоритму оцінюється за його здатністю запобігти атаки за заданий час при існуючих квантових обчислювальних потужностях. Другий аспект – це ресурси модернізації криптографічних алгоритмів. Дані ресурси включають витрати (тимчасові, обчислювальні, фінансові) на перехід до більш захищених криптографічних стандартів. Наприклад, впровадження постквантових алгоритмів, таких як алгоритми на основі ґрат (lattice-based cryptography), вимагатиме значних інвестицій у навчання фахівців, оновлення обладнання та модифікацію програмного забезпечення (ПЗ). Проілюструємо це невеликим прикладом. Скажімо, організація розглядає перехід на алгоритм CRYSTALS-Kyber, сертифікований NIST як постквантовий стандарт, це, відповідно, вимагатиме закупівлі нових апаратних модулів шифрування та оновлення протоколів зв'язку.

Аналогічна логіка міркувань справедлива й у активних коштів КК. Ці змінні описують можливості атакуючої сторони (наприклад, КК) здійснення обчислень, необхідні злому існуючих криптографічних алгоритмів. Тут також можна виділити два ключові аспекти. Перший аспект – це обчислювальна потужність КК. Ця змінна відображає поточний стан квантових обчислень, включаючи кількість кубитів та рівень їхньої когерентності. Таким чином, чим більше кубитів і вища їхня когерентність, тим більше можливостей для виконання складних обчислень, таких як факторизація великих чисел або пошук колізій у хеш-функціях. Наприклад, квантовий комп'ютер Google Sycamore з 53 кубитами в 2019 році досяг "квантової переваги", вирішивши завдання, недоступне для класичних комп'ютерів. Відповідно, КК із 1000 стабільними кубитами може провести факторизацію 2048-бітного ключа RSA за кілька годин, що неможливо для класичного комп'ютера в розумні терміни. Другий аспект – це ресурси підвищення обчислювальної потужності КК. Дані ресурси включають витрати на розробку потужніших КК, такі як фінансування досліджень, поліпшення технологій охолодження зниження рівня шуму, а також оптимізація квантових алгоритмів. Так, наприклад, створення кубитів на основі надпровідників вимагатиме значних матеріальних та енергетичних витрат. А інвестиції компанії у створення нового покоління кубітів дозволять підвищити обчислювальну потужність системи з 256 до 512 кубітів , що призведе до різкого збільшення можливостей атаки.

Тоді система диференціальних рівнянь виглядатиме так:

$$\dot{z}_1 = -p_{41} z_4 v_1 + c_1,$$
$$\dot{z}_2 = -p_{42} z_4 v_2 + c_2,$$
$$\dot{z}_3 = -p_{23} z_2 u_1 + c_3,$$
$$\dot{z}_4 = -p_{24} z_2 u_2 + c_4,$$

де p_{ij} – ефективність засобів однієї сторони проти іншої (для аналізованої моделі описує, наскільки успішно ресурси і стратегії однієї сторони (наприклад, криптовалютні системи або КК) можуть протидіяти зусиллям протилежної сторони. Для КК це може бути, наприклад, рівень стійкості криптографічних алгоритмів до злому з боку квантових комп'ютерів, який виражається через ймовірність успішного показу, що характеризує здатність їх алгоритмів та обчислювальних потужностей долати існуючі криптографічні захисту);

u_1, u_2, v_1, v_2 – частки ресурсів, що направляються на відповідні цілі (являють собою пропорції загального обсягу доступних ресурсів кожної зі сторін (наприклад, криптовалютних систем або КК, які виділяються для виконання конкретних завдань або стратегій у процесі їх взаємодії. Для криптовалют частки ресурсів можуть включати, зокрема, питомий обсяг, спрямований на підтримку поточних крипографів). також, ресурси, виділені на розробку і впровадження постквантових криптографічних стандартів, які зможуть протистояти атакам з боку КК. 1 (або 100%), оскільки ресурси обмежені, та їх розподіл між різними завданнями потребує оптимізації в рамках окремого завдання);

c_1, c_2, c_3, c_4 – можливості поповнення ресурсів (тобто здатність сторін збільшувати обсяг доступних ресурсів, необхідних для виконання їх стратегічних завдань. Дані ресурси можуть включати фінансові, технічні, обчислювальні або кадрові засоби, які забезпечують стійкість або розвиток сторін в умовах протистояння. Наприклад, для КВ можливості поповнення ресурсів відображають інвестиції в розробку нових криптографічних для інтеграції більш захищених протоколів, тощо. Для КК можливості поповнення ресурсів включають розвиток квантових технологій, таких як збільшення числа кубитів або підвищення їх когерентності, а також фінансування наукових досліджень для оптимізації квантових алгоритмів (наприклад, для прискорення роботи алгоритму Шора) тощо.

Тоді функцію виграшу сторін можна записати так.

Для криптовалют :

$$J_A = [z_1(T) - z_3(T)].$$

Мета криптовалют (КВ) – мінімізувати втрати своїх криптографічних засобів і максимізувати шкоду, нанесену обчислювальним засобам КК.

Для квантових комп'ютерів (КК):

$$J_B = [z_3(T) - z_1(T)].$$

Мета КК — максимізувати ефективність своїх обчислень та мінімізувати збитки від контрзаходів КВ.

Модель описує диференціальну гру з нульовою сумою, де динамічна взаємодія сторін та рівновага визначаються через оптимальні стратегії розподілу ресурсів. Зауважимо, що аналітичне рішення може бути недоступним, тому буде використано ітераційний процес для пошуку рівноважного стану, а алгоритм побудови може ґрунтуватися на принципі максимуму Л.С. Понтрягіна [14].

Результати дослідження та їх обговорення. Основне завдання обчислювального експерименту (ВЕ), результати якого показано на рис. 1, полягала в тому, щоб оцінити динамічну взаємодію сторін і відповісти на запитання: «Як криптовалюти адаптують свої захисні механізми у відповідь на атаки КК, і як КК посилюють свої обчислювальні потужності

для подолання цих захистів?». Крім того, необхідно в ході ВЕ визначити ключові залежності та виявити, які фактори, зокрема, ресурси модернізації криптографії або обчислювальні потужності КК) мають найбільший вплив на результат протистояння.

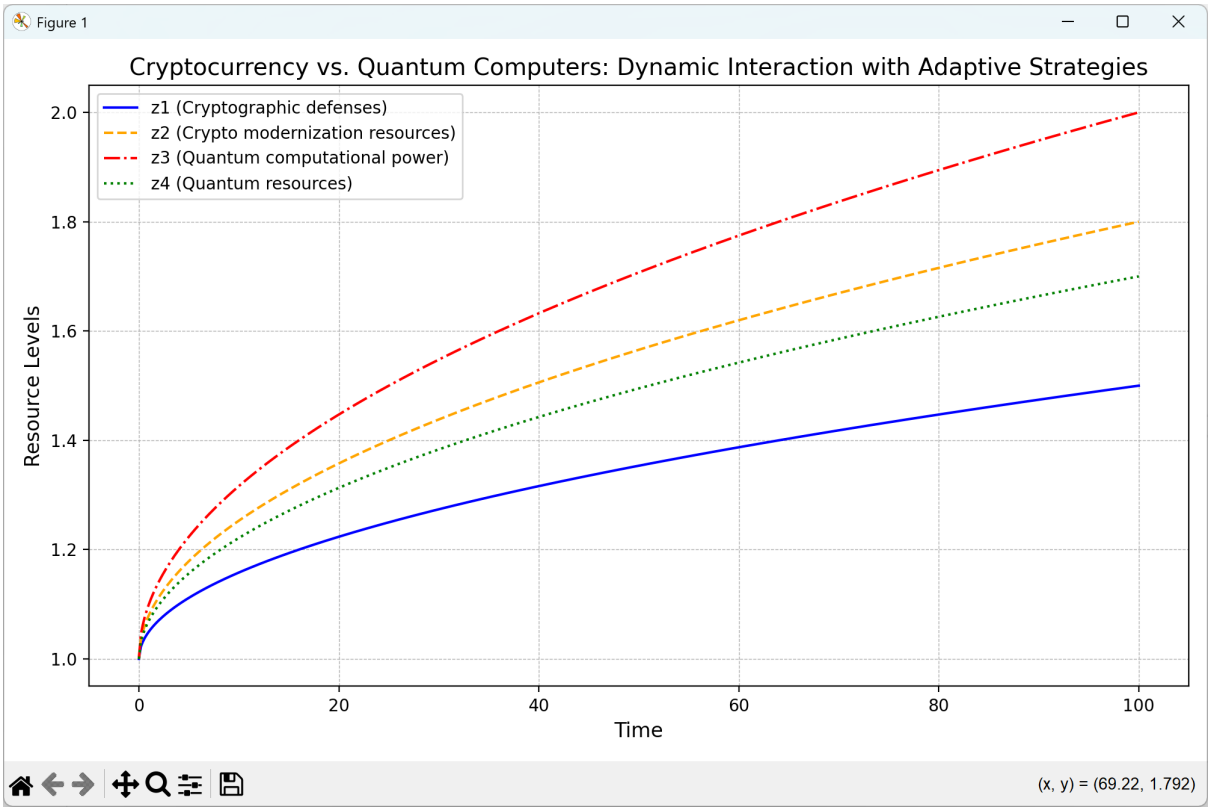

Рисунок 1 – Динаміка зміни ресурсів криптографічної системи та квантових обчислень в умовах протистояння

Експеримент включав завдання початкових значень змінних (наприклад, спочатку високий рівень криптографічного захисту $z_1(0)$та обчислювальних потужностей $z_3(0)$. Сценарії розподілу ресурсів, тобто тестування різних стратегій сторін, таких як максимальна концентрація ресурсів на одному напрямку, наприклад, КК повністю фокусується на збільшенні потужності, а КВ – на ефективності засобів однієї сторони проти іншої, що дозволяє оцінювати реальну загрозу та ступінь протидії.

Результати експерименту загалом дозволять зрозуміти динаміку взаємодії сторін, і визначити ключові чинники, які впливають на стійкість криптовалютних систем, що у подальших дослідженнях дасть змогу розробити конкретні практичні рекомендації щодо оптимального розподілу ресурсів та впровадження адаптивних стратегій захисту за умов квантових загроз для КВ.

Результати моделювання представлені рис. 1 як тимчасових залежностей рівнів ресурсів сторін, що у протистоянні, тобто, відповідно, криптовалютні технології і квантових обчислень. На графіках відображено зміни чотирьох ключових змінних: криптографічних захистів $z_1(t)$, ресурсів модернізації криптографії $z_2(t)$, обчислювальних потужностей квантових комп'ютерів $z_3(t)$ та їх ресурсів $z_4(t)$. Графік криптографічних захистів $z_1(t)$ показує, як рівень стійкості КВ змінюється під впливом атак із боку квантових комп'ютерів. На початкових етапах протистояння помітно зниження значень $z_1(t)$, що з активними діями боку квантових технологій, реалізують атакуючі стратегії із високим рівнем пріоритету. Однак наявність

ресурсів модернізації криптографії $z_2(t)$дозволяє компенсувати втрати, що призводить до стабілізації або навіть зростання $z_1(t)$ в більш пізні періоди.

Динаміка ресурсів модернізації $z_2(t)$ демонструє їхню критичну роль у протистоянні. На початкових етапах спостерігається поступове зниження $z_2(t)$ через перерозподіл коштів на відновлення та захист криптографічних систем. Однак заповнення ресурсів, описане в моделі, дозволяє підтримувати $z_2(t)$ на рівні, достатньому для ефективної стратегії, що протидіє.

Зміни обчислювальних потужностей квантових комп'ютерів $z_3(t)$відображають їхню високу початкову ефективність, яка поступово знижується під впливом атак з боку криптовалютної технології. Ця динаміка ілюструє ефективність адаптивних стратегій криптовалютного боку, вкладених у послаблення можливостей атакуючої сторони.

Ресурси квантових комп'ютерів $z_4(t)$ характеризуються аналогічною динамікою. Їхнє використання для атакуючих дій призводить до поступового виснаження, проте заповнення ресурсів дозволяє сторонам підтримувати активність протягом усього періоду моделювання.

Таким чином, отримані результати демонструють складну взаємодію сторін із змінним ступенем домінування залежно від застосовуваних стратегій та заповнення ресурсів , а також підтверджують, що адаптивні стратегії, що залежать від поточного стану системи, можуть значно вплинути на результат протистояння та забезпечити динамічну рівновагу між сторонами.

Висновки. Проведене дослідження продемонструвало, що розвиток квантових обчислень створює значні ризики для безпеки криптовалютних систем, оскільки квантові алгоритми, такі як алгоритм Шора можуть ефективно обходити існуючі криптографічні механізми. Запропонована в рамках роботи диференціальна ігрова модель показала, що динаміка протистояння між криптовалютами та квантовими комп'ютерами визначається стратегіями розподілу ресурсів сторін. Ключовим висновком є підтвердження ефективності адаптивних стратегій, які дозволять мінімізувати втрати криптографічної стійкості та уповільнити розвиток обчислювальних потужностей атакуючої сторони. Отримані в ході обчислювальних експериментів результати наголошують на необхідності впровадження постквантових криптографічних алгоритмів та модернізації інфраструктури для підвищення стійкості цифрових систем. А, крім того, запропонована методологія, на основі розвитку моделей, побудованих з використанням апарату диференціальних ігор, може бути використана для прогнозування довгострокових сценаріїв розвитку квантових загроз та вироблення превентивних заходів.

Список використаних джерел

1. Alexander Osipovich . (2024) A Looming Threat to Bitcoin: The Risk of a Quantum Hack. The Wall Street Journalhttps://www.wsj.com/tech/cybersecurity/a-looming-threat-to-bitcoin-the-risk-of-a-quantum-hack-24637e29?mod=mhp&utm_source=in_materials
2. Горбенка, І. Д., Кузнєцов , О. О., Потій , О. В., Горбенко, Ю. І., Ганзя , Р. С., & Пономар , В. А. (2016). Постквантова криптографія та механізми її реалізації . Радіотехніка , (186), 32-52.
3. Потій, О. В., Ісірова, К. В. (2017). Аналіз вимог та моделей безпеки для постквантової криптографії. Математичне та комп'ютерне моделювання . Серія : Технічні науки , 192-197.
4. Holmes, S., & Chen, L. (2021). Assessment of quantum threat to bitcoin and derived cryptocurrencies. Cryptology ePrint Archive.
5. Ostrianska , YV, Yesina , MV, & Gorbenko , ID (2022). Аналіз поглядів Європейського союзу на квантово- постквантові обмеження . Radiotechnika , (210), 87-98.

6. Denker , K., & Javaid , AY (2019). Quantum computing як threat to modern cryptography techniques. У ході міжнародної конференції з питань фармацевтичних наук (FCS) (pp. 3–8). The Steering Committee of World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

7. Khodaiemehr , H., Bagheri , K., & Feng, C. (2023). Navigation the quantum computing threat landscape for blockchains : A comprehensive survey. Authorea Preprints.

8. Raheman , F. (2024). Futureproofing Blockchain & Cryptocurrencies на основі Розвитку Vulnerabilities & Q-Day Threat with Quantum-Safe Ledger Technology (QLT). Journal of Computer and Communications, 12(7), 59 – 77.

9. Weinberg, AI, & Faccia , A. (2024). Quantum Algorithms: New Frontier в Financial Crime Prevention. arXiv preprint arXiv:2403.18322.

10. Gupta, KD, Nag, AK, Rahman, ML, Mahmud, MP, & Sadman , N. (2021). Використовуючи комп'ютерну комплексність для захисту криптоcurrency проти quantum threats: a review. IT Professional, 23 (5), 50 - 55.

11. Naik , A., Yeniaras , E., Hellstern , G., Prasad, G., & Vishwakarma , SKLP (2023). З portfolio optimization to quantum blockchain and security: Ha systematic review of quantum computing in finance. arXiv preprint arXiv:2307.01155.

12. Szatmáry , S. (2022, September). Quantum Computers—Security Threats and Solutions. У IFIP International Conference on Human Choice and Computers (pp. 431–441). Cham: Springer Nature Switzerland.

13. Pontryagin , LS (1965). On some differential games. Journal of Society for Industrial and Applied Mathematics, Series A: Control, 3(1), 49–52.

14. Pontryagin , LS (2018). Mathematical theory of optimal processes. Routledge. DOI https://doi.org/10.1201/9780203749319

Lakhno Valeriy
Doctor of Technical Sciences, Professor of the Department of Computer systems, networks and cybersecurity,
National University of Life and Environmental Sciences of Ukraine,
ORCID: https://orcid.org/0000-0001-9695-4543
E-mail: lva964@nubip.edu.ua

Kasatkin Dmytro
PhD, Associate Professor, Head of the Department of Computer systems, networks and cybersecurity,
National University of Life and Environmental Sciences of Ukraine
ORCID: https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

MATHEMATICAL MODELING AND ADAPTATION STRATEGIES IN THE CONFRONTATION BETWEEN CRYPTOCURRENCIES AND QUANTUM COMPUTERS

Abstract. *This article is dedicated to studying the resilience of cryptocurrency systems (CCS) under new threats associated with the development of quantum computing. A differential game model is introduced, allowing for the formalization of the interaction between CCS and quantum computers (QC), as well as the analysis of their mutual influence. The research methodology is based on the application of differential game theory to model the dynamics of resource allocation between the parties and to evaluate their strategies under conditions of uncertainty and competition. Various scenarios of confrontation between CCS and quantum computing were considered during the modeling process, which made it possible to identify key patterns and factors that significantly affect the effectiveness of cryptographic protection, as well as the computational capabilities of attackers utilizing QCs. Special attention is given to the analysis of different methods for protecting digital assets under potential quantum threats. The results of the study may serve as a foundation for developing new cryptographic security standards and adaptive protection strategies that will remain effective amid the rapid growth of quantum computing capabilities.*

Keywords*: quantum computing, cryptocurrencies, cryptographic resilience, mathematical modeling, resource allocation, quantum threats, protection strategies.*