

Сапожник Д.О.

Державний університет «Житомирська політехніка»

МЕТОДИ ТА НАПРЯМИ ЗАСТОСУВАННЯ КВАНТОВИХ КОМП'ЮТЕРІВ У КРИПТОГРАФІЇ ТА ЛОГІСТИЦІ

У статті проведено всебічний аналіз поточного стану та перспектив застосування квантових комп'ютерів у сферах криптографії та логістики. Завдяки використанню принципів квантової механіки, таких як суперпозиція та запутаність, квантові обчислення обіцяють революціонізувати підхід до вирішення складних обчислювальних задач, які є непідсильними для класичних систем. Це відкриває нові можливості для оптимізації, моделювання молекул та криптографії, що раніше вважалися нерозв'язними. У логістиці квантові алгоритми, зокрема *Quantum Approximate Optimization Algorithm* та квантовий відпал, демонструють значний потенціал для вирішення NP-складних задач, таких як маршрутизація транспортних засобів, планування виробництва, розподіл ресурсів та управління ланцюгами постачань. Вони дозволяють ефективніше досліджувати величезний простір рішень, симулювати складні системи та знаходити оптимальні або наближені до оптимальних розв'язки. У криптографії розвиток квантових комп'ютерів створює значну загрозу для існуючих криптографічних алгоритмів (наприклад, *RSA* та *Elliptic Curve Cryptography*) через потужність алгоритмів Шора та Гровера. Це підкреслює гостру необхідність у розробці та впровадженні постквантової криптографії, яка є стійкою до атак з використанням квантових комп'ютерів. Також активно досліджується квантова криптографія, що забезпечує незламні методи шифрування, ґрунтуючись на фізичних законах. Критично важливою є інтеграція безпеки в дизайн квантових мереж та систем Інтернету речей. Попри значний потенціал, реалізація повномасштабних квантових комп'ютерів стикається з серйозними технічними викликами, характерними для так званої «шумної» ери проміжних квантових пристроїв. Обмеження включають низьку точність, невелику кількість кубітів, чутливість до помилок, декогеренцію та проблеми масштабованості. Тому ключовим напрямком досліджень є розробка гібридних квантово-класичних підходів, які поєднують сильні сторони квантових процесорів для певних підзадач з ефективністю класичних алгоритмів оптимізації, прокладаючи шлях до практичної реалізації квантової переваги.

Ключові слова: квантові обчислення, квантові технології, криптографія, квантова криптографія, логістика, оптимізація, кубіти, суперпозиція, запутаність.

Постановка проблеми. Квантові комп'ютери, що використовують принципи квантової механіки для обробки інформації, обіцяють революціонізувати обчислювальні можливості, перевершуючи класичні системи у вирішенні певних складних задач [1]. Ця перевага випливає з їхньої здатності оперувати квантовими станами, що дозволяє паралельно обробляти великі обсяги даних та ефективно моделювати квантові системи [2]. На відміну від класичних комп'ютерів, які використовують біти, що можуть перебувати лише у стані 0 або 1, квантові комп'ютери застосовують кубіти, здатні одночасно існувати у суперпозиції обох станів [3]. Ця унікальна властивість, доповнена явищами запутаності, дозволяє квантовим комп'ютерам виконувати обчислення експоненційно швидше за класичні системи для певних типів завдань, таких як оптимізація, моделювання

молекул та криптографія [4]. Таким чином, розробка та впровадження квантових обчислювальних методів відкриває нові горизонти для вирішення задач, які раніше вважалися нерозв'язними або надто ресурсомісткими для класичних обчислювальних парадигм [5].

Аналіз досліджень і публікацій. Попри значний потенціал, створення повномасштабних квантових комп'ютерів стикається з серйозними технічними труднощами, такими як потреба в екстремально низьких температурах, вакуумі, високому енергоспоживанні та використанні дефіцитних ресурсів [6]. Однак, попри ці обмеження, розміри квантових комп'ютерів вже перевищують 100 кубітів, що свідчить про значний прогрес у порівнянні з класичними обчислювальними машинами [7]. Ця технологічна еволюція протягом останніх 25 років була рушійною силою для

глобальної наукової спільноти у напрямку розробки квантових технологій у більш значущих масштабах, дозволяючи перейти від доказів концепції до практичної реалізації [8]. Інтенсивні дослідження та експериментальні розробки в цій галузі сприяли безпрецедентному розширенню квантових технологій, включаючи як реалізації квантових комп'ютерів, так і квантових комунікацій [9]. Стрімкий перехід від фундаментальних наукових досліджень до формування самостійної технологічної галузі свідчить про зростаючий інтерес до квантових обчислень, який значною мірою зумовлений прогресом у розробці як апаратного, так і програмного забезпечення [10]. Зокрема, провідні технологічні компанії, такі як IBM, Google, Microsoft та Intel, активно інвестують у створення перших великомасштабних універсальних квантових комп'ютерів, що свідчить про значний інтерес до цієї галузі як з боку промисловості, так і з боку академічних кіл [11]. Ці зусилля спрямовані на демонстрацію квантової обчислювальної переваги, яка полягає у вирішенні завдань, що є недосяжними для найпотужніших класичних суперкомп'ютерів, підтверджуючи тим самим принципову неможливість ефективної імітації квантових систем класичними засобами [12]. Ця експоненційна складність симуляції квантових систем є ключовою причиною того, що квантові комп'ютери є ідеально придатними для моделювання квантово-механічних систем у різноманітних дисциплінах, таких як квантова хімія, логістика, ядерна фізика та криптографія [13]. Ці прориви відкривають шлях до розробки нових матеріалів з унікальними властивостями та глибшого розуміння фундаментальних процесів у природі. Крім того, швидкі темпи розвитку квантових технологій спричинили появу хмарних квантових обчислювальних сервісів, що знижує бар'єри для входу та дозволяє стартапам експериментувати з квантовими алгоритмами без необхідності володіти власним дорогим квантовим обладнанням [14]. Доступ до квантових ресурсів сприяє прискоренню досліджень та розширенню можливостей для розробки нових квантових алгоритмів та застосунків. Особливо це актуально в умовах, коли обмеження напівпровідникової технології, передбачені законом Мура, уповільнюють розвиток алгоритмів машинного навчання, які вимагають дедалі більших обчислювальних ресурсів для обробки інтенсивних наборів даних [15]. В даному контексті квантові комп'ютери пропонують нові підходи до обробки даних, які можуть подолати обмеження, використовуючи

властивості квантової механіки для прискорення складних обчислень та аналізу великих масивів інформації [16].

Дослідження показують, що квантові обчислення мають значний потенціал для вирішення складних задач оптимізації та підвищення ефективності у логістиці та управлінні ланцюгами постачань [17]. Традиційні методи оптимізації стикаються з труднощами через величезну кількість можливих рішень у таких задачах. Квантові алгоритми, зокрема Quantum Approximate Optimization Algorithm та квантовий відпал, розробляються для розв'язання складних проблем оптимізації в цих галузях, таких як маршрутизація транспортних засобів, планування виробництва та розподілу ресурсів [18].

Розробка квантових комп'ютерів створює значну загрозу для існуючих криптографічних алгоритмів, що лежать в основі безпеки цифрових комунікацій [19]. Алгоритми, такі як алгоритм Шора для факторизації великих чисел та алгоритм Гровера для пошуку в неструктурованих базах даних, можуть ефективно зламати широко використовувані асиметричні (наприклад, RSA, ECC) та симетричні криптографічні схеми [20]. Ця загроза призвела до активного розвитку постквантової криптографії, яка спрямована на створення криптографічних систем, стійких як до класичних, так і до квантових атак [21].

Метою статті є проведення комплексного аналізу поточного стану та перспектив застосування квантових комп'ютерів у криптографії та логістиці, визначення їхнього потенціалу для трансформації цих галузей, а також аналіз поточних викликів та обмежень, які стримують їхнє широкомасштабне впровадження.

Виклад основного матеріалу. Квантова криптографія, зокрема, обіцяє незламні методи шифрування, що ґрунтуються на законах квантової механіки, унеможливаючи перехоплення даних без виявлення [22]. Ця галузь активно досліджується, оскільки поточні криптографічні системи, що покладаються на складні математичні задачі, можуть стати вразливими (рис. 1) перед обличчям зростаючої обчислювальної потужності квантових комп'ютерів [23]. Зокрема, алгоритми Шора та Гровера становлять значну загрозу для чинних асиметричних та симетричних криптографічних схем, вимагаючи розробки постквантових криптографічних рішень. Ці алгоритми здатні ефективно розкладати великі числа на прості множники та прискорювати пошук у неструктурованих базах даних, що робить вразливими широко викорис-

товувані протоколи, такі як RSA та Elliptic Curve Cryptography [24].

З огляду на це, існує гостра потреба в розробці та впровадженні нових криптографічних стандартів, стійких до атак із використанням квантових комп'ютерів, що є одним з ключових напрямків досліджень у сфері квантової безпеки. Ця загроза підсилила необхідність створення постквантової криптографії, яка розробляє криптосистеми, стійкі як до класичних, так і до квантових атак. Розглядаються також гібридні стратегії, що інтегрують квантову та постквантову криптографію для забезпечення надійного захисту даних у різноманітних обчислювальних середовищах. Критично важливою є інтеграція безпеки в дизайн квантових мереж з самого початку, оскільки класичні системи зв'язку, що використовуються для їх функціонування, також вразливі до кібератак [25]. Цей ризик поширюється на системи Інтернету речей, які, хоч і є надзвичайно корисними, проте схильні до серйозних загроз безпеці, таких як витік даних, атаки по сторонніх каналах та проблеми автентифікації даних [26]. Особливе занепокоєння викликають кіберфізичні системи, які, попри їхню гнучкість, є вразливими до обчислювальних та мережевих атак, що підкреслює необхідність посилення досліджень у сфері кіберфізичної безпеки у квантову еру [27].

Оптимізація та логістика є критично важливими сферами для багатьох галузей промисловості, де навіть незначні покращення ефективності можуть призвести до значної економії ресурсів та часу. Багато задач у цих галузях є NP-складними, що робить їх вирішення для великих масштабів практично неможливим за допомогою класичних комп'ютерів. Квантові комп'ютери пропонують нові підходи до розв'язання цих складних задач [28]. Ключові напрямки застосування квантових

технологій включають комбінаторну оптимізацію, де задача комівояжера, задача маршрутизації транспортних засобів та задача пакування, є прикладами комбінаторної оптимізації. Зв'язок квантових алгоритмів з задачами логістики можна побачити на рисунку 2.

Ці проблеми є складними через величезний простір рішень, який класичним методом важко досліджувати через нестачу обчислювальної потужності та архітектури. Квантові алгоритми, такі як Quantum Approximate Optimization Algorithm (QAOA) [29] та квантовий відпал [30], демонструють потенціал для пошуку кращих або наближених до оптимальних рішень для цих задач швидше, ніж класичні методи для певних типів проблем [28]. Дослідження показують, що QAOA може бути використаний для розв'язання VRP [31] та TSP [29]. Також вивчаються квантові нейронні мережі для логістичних застосувань [32]. Іншим важливим напрямком є оптимізація ланцюгів постачань, що включає оптимізацію інвентаризації, планування виробництва, розподілу ресурсів та управління ризиками [33]. Квантові алгоритми можуть допомогти моделювати та оптимізувати складні, динамічні системи ланцюгів постачань, враховуючи велику кількість змінних та невизначеностей. Дослідники застосовують QAOA для оптимізації виробництва та ланцюгів постачань, прагнучи підвищити продуктивність, знизити витрати та покращити якість продукції [33]. Квантові та класичні алгоритми відпалу також досліджуються для логістики ланцюгів постачань [34]. Розподіл ресурсів та розклад також є ключовими, адже задачі планування, такі як розподіл співробітників, машин або часу, можуть бути надзвичайно складними [35]. Квантові методи можуть запропонувати ефективніші рішення для таких задач за допомогою принципу суперпозиції який



Рис. 1. Виклики, які ставлять квантові технології для криптографії

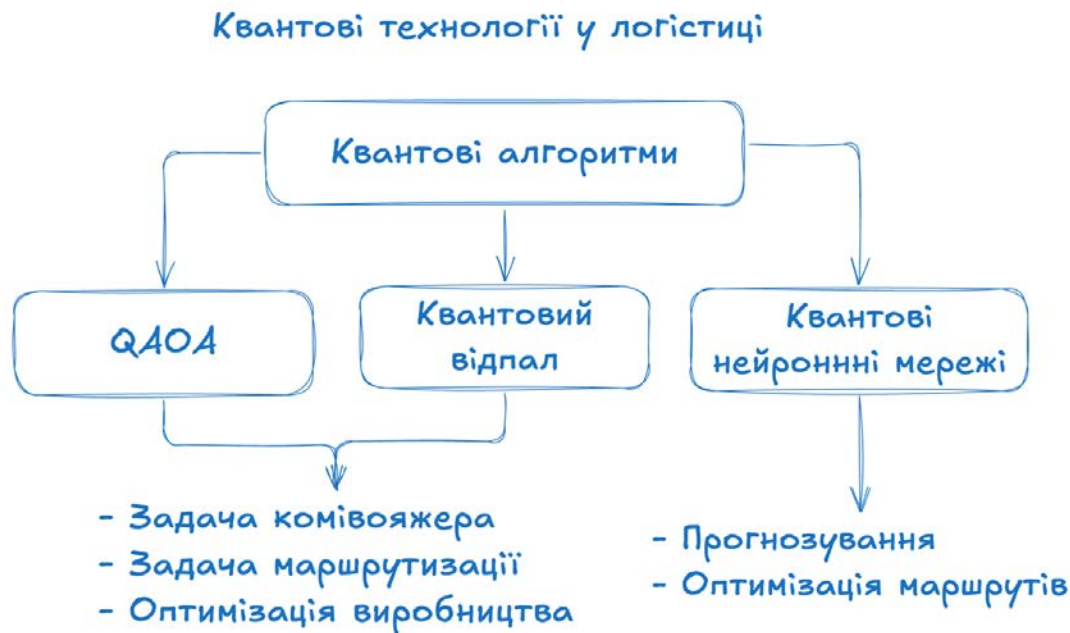


Рис. 2. Застосування квантових технологій у логістиці

лежить в основі квантових обчислень. Наприклад, досліджується квантова готовність для планування автоматизованих керованих транспортних засобів як задача цехового планування [36]. Симуляція та моделювання є ще одним напрямком, де квантові комп'ютери можуть бути використані для симуляції складних систем, таких як транспортні мережі або потоки товарів, дозволяючи компаніям тестувати різні сценарії та оптимізувати свої операції без ризику реальних втрат [37]. В умовах обмежень ери (NISQ – Noisy Intermediate-Scale Quantum), розв'язання задач реального масштабу виключно за допомогою квантових алгоритмів є мало ймовірним. Натомість гібридні класично-квантові підходи мають потенціал для досягнення ефективних результатів на значно більших екземплярах проблем. Ці підходи поєднують сильні сторони квантових процесорів для певних підзадач з класичними алгоритмами оптимізації.

Висновки. Квантові обчислення, використовуючи принципи суперпозиції та запутаності, представляють собою трансформаційну технологію, що здатна вирішувати обчислювальні задачі, які недосяжні для класичних систем. Ця робота підкреслює їхній значний потенціал у двох критично важливих сферах: логістиці та криптографії. У логістиці квантові алгоритми пропонують ефективні рішення для складних задач оптимізації, таких як маршрутизація транспортних засо-

бів, планування виробництва та управління ланцюгами постачань, забезпечуючи підвищення ефективності та значну економію ресурсів. Водночас у сфері криптографії розвиток квантових комп'ютерів створює пряму загрозу для існуючих криптографічних протоколів через потужність алгоритмів Шора та Гровера. Це зумовлює невідкладну потребу в розробці та впровадженні постквантової криптографії, а також подальшому дослідженні квантової криптографії для забезпечення надійного захисту даних у майбутньому.

Незважаючи на ці багатообіцяючі перспективи, широкомасштабне впровадження повноцінних квантових комп'ютерів стикається з суттєвими технічними викликами, характерними для так званої «шумної» ери (NISQ) пристроїв. Ці обмеження включають низьку точність гейтів, обмежену кількість кубітів, високу чутливість до помилок, декогеренцію та проблеми масштабованості. У зв'язку з цим, гібридні квантово-класичні підходи, що ефективно поєднують сильні сторони квантових процесорів для специфічних підзадач з можливостями класичних алгоритмів оптимізації, визнані ключовим напрямком досліджень. Вони прокладають шлях до практичної реалізації квантової переваги, долаючи поточні обмеження апаратного забезпечення та прискорюючи впровадження квантових технологій у реальні застосунки.

Список літератури:

1. Huang H.-L., Xu X., Guo C., Tian G., Wei S., Sun X., Bao, W.-S., Long G. Near-Term Quantum Computing Techniques: Variational Quantum Algorithms, Error Mitigation, Circuit Compilation, Benchmarking and Classical Simulation. *arXiv* (Cornell University). 2022. DOI: 10.48550/arxiv.2211.08737.
2. Daribayev B., Mukhanbet A., Azatbekuly N., Imankulov T. A Quantum Approach for Exploring the Numerical Results of the Heat Equation. *Algorithms*, 17 (8), 327 p. 2024. DOI: 10.3390/a17080327.
3. Сапожник Д. О. Аналіз можливостей мови програмування Q# шляхом реалізації програми для генерації випадкових чисел. *Технічна Інженерія*, С. 240. 2024. DOI: 10.26642/ten-2024-1(93)-240-245.
4. Greiner F., Müller, R., Bitzenbauer P., Ubben M. S., Weber K.-A. Future quantum workforce: Competences, requirements, and forecasts. *Physical Review Physics Education Research*. 19 (1). 2023. DOI: 10.1103/physrevphyseducres.19.010137.
5. Ajagekar A., Humble T. S., You F. Quantum computing based hybrid solution strategies for large-scale discrete-continuous optimization problems. *Computers & Chemical Engineering*, 132. 2019. DOI: 10.1016/j.compchemeng.2019.106630.
6. Arora N., Kumar P. Sustainable Quantum Computing: Opportunities and Challenges of Benchmarking Carbon in the Quantum Computing Lifecycle. *arXiv*. 2024. DOI: 10.48550/ARXIV.2408.05679.
7. Ngo A. P., Thomas C., Nguyen H. T., Eroglu, A., Oikonomou K. Evaluate Quantum Combinatorial Optimization for Distribution Network Reconfiguration. *North American Power Symposium (NAPS)*, 1. 2022. DOI: 10.1109/naps56150.2022.10012259.
8. Britt K. A., Mohiyaddin F. A., Humble T. S. Quantum Accelerators for High-Performance Computing Systems. 2017 IEEE *International Conference on Rebooting Computing (ICRC)*. 2017. DOI: 10.1109/icrc.2017.8123664.
9. Mugel S., Abad M., Bermejo M., Sánchez, J., Lizaso E., Orús R. Hybrid quantum investment optimization with minimal holding period. *Scientific Reports*, 11 (1). 2021. DOI: 10.1038/s41598-021-98297-x.
10. Gill S. S., Cetinkaya O., Marrone S., Combarro E. F., Claudino D., Haunschild D., Schlote L., Wu H., Ottaviani C., Liu, X., Machupalli S. P., Kaur K., Arora P., Liu, J., Shamshad S., Farouk A., Song H., Uhlig S., Ramamohanarao K. Quantum Computing: Vision and Challenges. *arXiv* (Cornell University). 2024. DOI: 10.48550/arxiv.2403.02240.
11. Gill S. S., Kumar A., Singh, H., Singh M., Kaur K., Usman M., Buyya R. Quantum Computing: A Taxonomy, Systematic Review and Future Directions. *arXiv* (Cornell University). 2020. DOI: 10.48550/arxiv.2010.15559.
12. Deshpande A., Mehta A., Vincent T., Quesada N., Hinsche M., Ioannou M., Madsen L. S., Lavoie J., Qi H., Eisert J., Hangleiter D., Fefferman B., Dhand I. Quantum computational advantage via high-dimensional Gaussian boson sampling. *Science Advances*, 8 (1). 2022. DOI: 10.1126/sciadv.abi7894.
13. Martonosi M., Roetteler M. Next Steps in Quantum Computing: Computer Science's Role. *arXiv* (Cornell University). 2019. DOI: 10.48550/arxiv.1903.10541.
14. Gill S. S., Buyya R. Transforming Research with Quantum Computing. *Journal of Economy and Technology*. 2024. DOI: 10.1016/j.ject.2024.07.001.
15. Stein S. A., L'Abbate R., Mu W., Liu Y., Baheri B., Mao, Y., Guan Q., Li A., Fang B. A Hybrid System for Learning Classical Data in Quantum States. 2021 IEEE *International Performance, Computing, and Communications Conference (IPCCC)*. 2021 DOI: 10.1109/ipccc51483.2021.9679430
16. Srivastava N., Belekhar G., Shahakar N., Babu H. The Potential of Quantum Techniques for Stock Price Prediction. 2023 IEEE *International Conference on Recent Advances in Systems Science and Engineering (RASSE)*. 2023. DOI: 10.1109/rasse60029.2023.10363533.
17. Hwang M.-L. T., Collin W.-L., Wang-xu L. S. Quantum computing and supply chain optimization: addressing complexity and efficiency challenges. *International Journal of Enterprise Modelling*, 15 (3), 148 p. 2021. DOI: 10.35335/emod.v15i3.49.
18. Sapozhnyk D. Quantum Approximate Optimization Algorithm for the Max-Cut Problem : JavaScript Programming Language Implementation. *International Conference on Applied Innovations in IT (ICAIIIT)*. 2024. DOI: 10.25673/118110.
19. Emmanni P. S. The Impact of Quantum Computing on Cybersecurity. *Journal of Mathematical & Computer Applications*, 2 (2). 2023. DOI: 10.47363/jmca/2023(2)140.
20. Dam D.-T., Tran T.-H., Hoang V., Pham C., Hoang T.-T. A Survey of Post-Quantum Cryptography: Start of a New Race. *Cryptography*, 7 (3), 40 p. 2023. DOI: 10.3390/cryptography7030040.
21. Oladimeji S., Egon A., Brooklyn P. The Impact of Quantum Computing on Post-Quantum Cryptography: Standardization And Migration Strategies. *SSRN Electronic Journal*. 2024. DOI: 10.2139/ssrn.4904933.
22. Kim H., Jeng M. J., Smith K. N. Toward Human-Quantum Computer Interaction: Interface Techniques for Usable Quantum Computing. *arXiv*. 2025. DOI: 10.48550/ARXIV.2502.00202.
23. Bagirovs E., Provodin G., Sipola, T., Hautamäki J. Applications of Post-quantum Cryptography. *arXiv* (Cornell University). 2024. DOI: 10.34190/eccws.23.1.2247.
24. Mavroeidis V., Vishi K., Mateusz D., Jøsang A. The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications*, 9 (3). 2018. DOI: 10.14569/ijacsa.2018.090354.

25. Peters N. A., Alshowkan M., Chapman J. C., Pooser R. C., Rao N. S. V., Newell R. Long-term cybersecurity applications enabled by quantum networks. *arXiv (Cornell University)*. 2023. DOI: 10.48550/arxiv.2304.14479.
26. Bhatt A. P., Sharma A. Quantum Cryptography for Internet of Things Security. *Journal of Electronic Science and Technology*, 17 (3), 213 p. 2019. DOI: 10.11989/jest.1674-862x.90523016.
27. Barbeau M., García-Alfaro J. Cyber-physical defense in the quantum Era. *Scientific Reports*, 12 (1). 2022. DOI: 10.1038/s41598-022-05690-1.
28. Au-Yeung R., Chancellor N., Halffmann P. NP-hard but no longer hard to solve? Using quantum computing to tackle optimization problems. *Frontiers in Quantum Science and Technology*, 2. 2023. DOI: 10.3389/frqst.2023.1128576.
29. Qian W., Basili R., Eshaghian-Wilner M. M., Khokhar A., Luecke G. R., Vary J. P. Comparative Study of Variations in Quantum Approximate Optimization Algorithms for the Traveling Salesman Problem. *Entropy*, 25 (8), 1238 p. 2023. DOI: 10.3390/e25081238.
30. Phillipson F. Quantum Computing in Logistics and Supply Chain Management an Overview. *arXiv*. 2024. DOI: 10.48550/ARXIV.2402.17520.
31. Azfar T., Ke R., Raisuddin O. M., Holguin-Veras J. Quantum-Assisted Vehicle Routing: Realizing QAOA-based Approach on Gate-Based Quantum Computer. *arXiv*. 2025. DOI: 10.48550/ARXIV.2505.01614.
32. Correll R., Weinberg S. J., Sanches F. de O., Ide T., Suzuki T. Quantum Neural Networks for a Supply Chain Logistics Application. *Advanced Quantum Technologies*, 6 (7). 2023. DOI: 10.1002/qute.202200183.
33. Chen W. J., Marcus G. S., Leesburg D. Quantum computing for manufacturing and supply chain optimization: enhancing efficiency, reducing costs, and improving product quality. *International Journal of Enterprise Modelling*, 15 (3), 130 p. 2021. DOI: 10.35335/emod.v15i3.48.
34. Weinberg S. J., Sanches F., Ide T., Kamiya K., Correll R. Supply chain logistics with quantum and classical annealing algorithms. *Scientific Reports*, 13 (1). 2023. DOI: 10.1038/s41598-023-31765-8.
35. Osaba E., Delgado I. P., Ali A. M., Rodríguez P. R. H., Leceta A. M. F. D., RIVAS L. C. Quantum computing in industrial environments: where do we stand and where are we headed? *Dyna*, 100 (3), 267 p. 2025. DOI: 10.52152/d11380.
36. Śmiechrzalski T., Paweł Ł., Gardas B., Puchała Z., Koniorczyk M., Domino K. Quantum readiness for scheduling of Automatic Guided Vehicles (AGVs) as job-shop problem. *arXiv (Cornell University)*. 2023. DOI: 10.48550/arxiv.2309.03088.
37. Phillipson F. Quantum Computing in Logistics and Supply Chain Management an Overview. *arXiv (Cornell University)*. 2024. DOI: 10.48550/arxiv.2402.17520.

Sapozhnyk D.O. METHODS AND AREAS OF APPLICATION OF QUANTUM COMPUTERS IN CRYPTOGRAPHY AND LOGISTICS

This article provides a comprehensive analysis of the current state and prospects of applying quantum computers in the fields of cryptography and logistics. Leveraging quantum mechanical principles such as superposition and entanglement, quantum computing promises to revolutionize the approach to solving complex computational problems that are intractable for classical systems. This opens up new possibilities for optimization, molecular modeling, and cryptography, previously considered unsolvable. In logistics, quantum algorithms, particularly the Quantum Approximate Optimization Algorithm and quantum annealing, demonstrate significant potential for solving NP-hard problems, such as vehicle routing, production planning, resource allocation, and supply chain management. They enable more efficient exploration of vast solution spaces, simulation of complex systems, and finding optimal or near-optimal solutions. In cryptography, the development of quantum computers poses a significant threat to existing cryptographic algorithms (e.g., RSA and Elliptic Curve Cryptography) due to the power of Shor's and Grover's algorithms. This underscores the urgent need for the development and implementation of post-quantum cryptography, which is resilient to attacks using quantum computers. Quantum cryptography, which provides unbreakable encryption methods based on physical laws, is also actively being researched. The integration of security into the design of quantum networks and Internet of Things systems is critically important. Despite their significant potential, the realization of full-scale quantum computers faces serious technical challenges characteristic of the "noisy" era of noisy intermediate-scale quantum devices. Limitations include low gate fidelity, a small number of qubits, susceptibility to errors, decoherence, and scalability issues. Therefore, a key direction of research is the development of hybrid quantum-classical approaches that combine the strengths of quantum processors for specific sub-problems with the efficiency of classical optimization algorithms, paving the way for the practical realization of quantum advantage. The article analyzes these challenges and limitations that hinder the widespread adoption of quantum technologies in these fields.

Key words: quantum computing, quantum technologies, cryptography, quantum cryptography, logistics, optimization, qubits, superposition, entanglement.

Дата надходження статті: 19.09.2025

Дата прийняття статті: 01.10.2025

Опубліковано: 16.12.2025