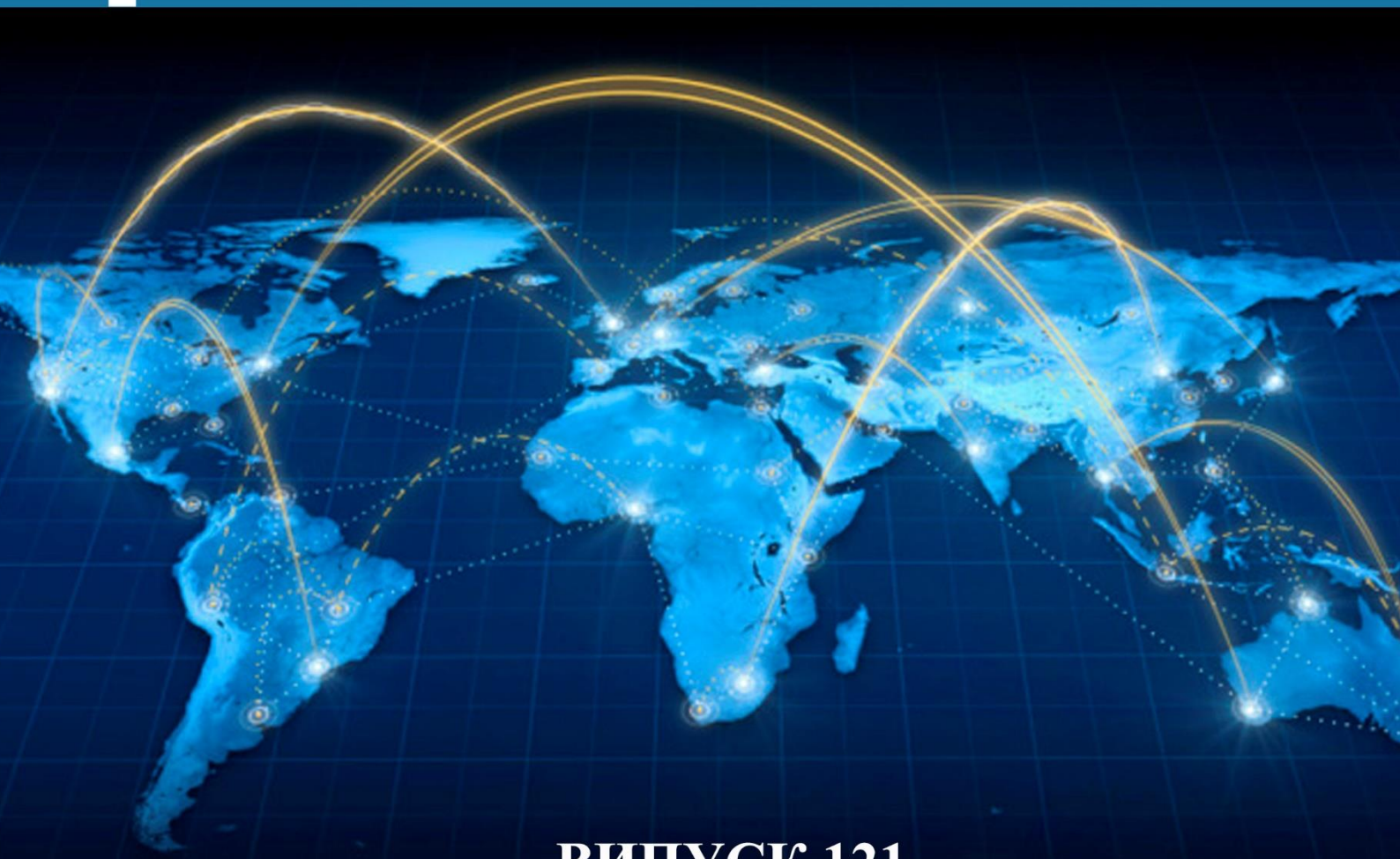
МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА
ІНТЕРНЕТ-КОНФЕРЕНЦІЯ

«ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НАУКИ І ОСВІТИ В УМОВАХ ГЛОБАЛІЗАЦІЇ»



ВИПУСК 121

30 вересня 2025 р.

м. Переяслав

УНІВЕРСИТЕТ ГРИГОРІЯ СКОВОРОДИ
В ПЕРЕЯСЛАВІ

Рада молодих учених університету

Матеріали
Міжнародної науково-практичної інтернет-конференції
«ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НАУКИ І ОСВІТИ В УМОВАХ ГЛОБАЛІЗАЦІЇ»
30 вересня 2025 року
Вип. 121

Збірник наукових праць

Переяслав – 2025

УДК 001+37(100)
ББК 72.4+74(0)
Т 33

Матеріали Міжнародної науково-практичної інтернет-конференції «Тенденції та перспективи розвитку науки і освіти в умовах глобалізації»: Зб. наук. праць. Переяслав, 2025. Вип. 121. 222 с.

Збірник матеріалів конференції вміщує результати наукових досліджень наукових співробітників, викладачів вищих навчальних закладів, докторантів, аспірантів, студентів з актуальних проблем гуманітарних, природничих і технічних наук

Відповідальність за грамотність, автентичність цитат, достовірність фактів і посилань несуть автори публікацій

The practical checklist is short. Stick to a clear baseline (BM25 for search; simple popularity plus item similarity for recommendations). Add one improvement at a time and measure carefully. Use a small, stable set of metrics: nDCG@k and latency for search; CTR, reach, and diversity for recommendations. Control costs with compression (PQ), caching, and smart packet sizes; first choose FAISS settings that fit your latency budget, then gradually increase the level of reproduction [3, pp. 1–3]. Prefer a two-stage design so that a fast first pass protects tail latency and a second pass focuses on quality [1, pp. 191–195]. Document assumptions and data filters (language, time frame, security rules) to ensure that results are reproducible [5, pp. 1–4]. Finally, record data update and retraining schedules (e.g., daily reindexing, weekly retraining) to keep the system from becoming obsolete [6, pp. 352–360; 3, pp. 1–3; 1, pp. 195–197].

Conclusion. Modern IR and RS are based on a small set of ideas that work okay together: fast first pass, stronger second pass, and efficient vector index. BM25 is a reliable start; dense search and ColBERT add semantic power; two-stage recommendation systems scale in production. With careful evaluation and simple operating rules, these systems can be implemented by small teams and student projects [5, pp. 1–4; 6, pp. 333–340; 1, pp. 191–195]. In practice, the winning recipe is a hybrid: BM25 for retrieval, a dense search engine for semantic matches, and a precise re-ranker for the best results, as well as candidate generation and pair ranking on the recommendation side [4, pp. 39–41; 1, pp. 191–195].

REFERENCES

1. Covington P., Adams J., Sargin E. Deep Neural Networks for YouTube Recommendations. In: RecSys ’16. ACM, 2016. PP. 191–198.

2. He X., Liao L., Zhang H., Nie L., Hu X., Chua T.-S. Neural Collaborative Filtering. In: WWW ’17. ACM, 2017. PP. 173–182.

3. Johnson J., Douze M., Jégou H. Billion-Scale Similarity Search with GPUs. arXiv:1702.08734, 2017. 25 p.

4. Khattab O., Zaharia M. ColBERT: Efficient and Effective Passage Search via Contextualized Late Interaction over BERT. In: SIGIR 2020. PP. 39–48.

5. Manning C. D., Raghavan P., Schütze H. Introduction to Information Retrieval. Cambridge University Press, 2008. 482 p. (Online edition: Stanford NLP).

6. Robertson S., Zaragoza H. The Probabilistic Relevance Framework: BM25 and Beyond. Foundations and Trends in Information Retrieval. 2009. Vol. 3(4). PP. 333–389.

УДК 004.94

Artemii Muzychenko, Maryna Vyshnevska
(Kyiv, Ukraine)

THE RISE OF QUANTUM COMPUTING: OPPORTUNITIES AND RISKS

This article provides a comprehensive analysis of the phenomenon of quantum computing as a technology capable of fundamentally changing science, the economy, and the global security system. It examines the fundamental principles of quantum computers, such as superposition and entanglement, and analyzes their potential capabilities in the fields of medicine, materials science, and artificial intelligence.

Keywords: *quantum computing, qubit, superposition, quantum advantage, cryptography, Shor's algorithm, post-quantum cryptography, cybersecurity.*

У статті проводиться комплексний аналіз феномену квантових обчислень як технології, що здатна кардинально змінити науку, економіку та систему глобальної безпеки. Розглядаються фундаментальні принципи роботи квантових комп'ютерів, такі як суперпозиція та заплутаність, а також аналізуються їхні потенційні можливості у сферах медицини, матеріалознавства та штучного інтелекту.

Ключові слова: *квантові обчислення, кубіт, суперпозиція, квантова перевага, криптографія, алгоритм Шора, постквантова криптографія, кібербезпека.*

The world is on the cusp of a new technological revolution, driven by the power of quantum computing. "Quantum computing is emerging as a groundbreaking force, promising to redefine the boundaries of technology and business" [3, p. 585]. Unlike classical computers, which operate using bits (0 or 1), quantum machines use qubits, which, thanks to the principles of quantum mechanics, can exist in countless states simultaneously. This fundamental difference opens the door to solving problems of exponential complexity that will forever remain beyond the reach of today's most powerful supercomputers.

The development of quantum technologies promises breakthroughs in fields as diverse as new drug discovery, the creation of innovative materials, the optimization of global logistics networks, and the enhancement of artificial intelligence models. Tech giants like Google, IBM, and Microsoft, along with numerous startups and research institutes, are investing billions of dollars in this race, striving to be the first to achieve "quantum advantage" – the point at which a quantum computer can perform a task that is practically impossible for a classical one.

However, like any powerful technology, quantum computing carries significant risks. The most discussed threat is its ability to break modern cryptographic algorithms that form the foundation of our global digital infrastructure's security – from banking transactions to secure government communications. The purpose of this article is to provide a comprehensive analysis of both the immense opportunities and the serious threats associated with the development of quantum computers, as well as to review the current challenges on the path to their full-scale implementation.

Fundamentals of Quantum Computing. To understand the potential of quantum computers, it is necessary to consider their fundamental principles, which are radically different from classical logic. "Quantum computer operates on the principles of quantum mechanics and utilizes the properties of quantum (microscopic) particles, i.e., superposition and entanglement, to perform computation" [6, p. 6662].

1. The Qubit and Superposition. A classical bit can be either a 0 or a 1. "The difference between qubits and bits is that a qubit can be in a state other than 0 or 1, or we can say in a superposition of 0 and 1" [1, p. 64]. This can be imagined as a spinning coin in the air before it lands on "heads" or "tails." While it's spinning, it is both at the same time. The ability of qubits to exist in multiple states allows a quantum computer to process vast arrays of information in parallel. The number of possible states grows exponentially with each new qubit added. Thus, a system of N qubits can simultaneously represent 2N values. While in superposition, a qubit's state is a probability wave. Only upon measurement does this wave "collapse" into one of the definite classical states (0 or 1), a phenomenon known as the measurement problem.

2. Quantum Entanglement. "Quantum computers exploit principles of quantum mechanics, such as superposition and entanglement, to represent data and perform operations on them" [5, p. 2529]. This is one of the most astonishing phenomena of quantum mechanics, which Albert Einstein called "spooky action at a distance." Two or more qubits can become "entangled," meaning their states become interdependent, regardless of the distance between them. If you measure the state of one entangled qubit, the state of the other is instantly known. This property allows for the creation of complex correlations between qubits, which is key to executing powerful quantum algorithms. Entanglement is a crucial resource that enables quantum computers to achieve computational speedups impossible in the classical world.

These two principles allow quantum computers to perform computations in a fundamentally different way. They operate not with classical logic gates like AND and OR, but with quantum gates that manipulate the probability states of qubits. Instead of sequentially going through options, as a classical computer does, a quantum computer explores a vast computational space of all possible variants at once, giving it a colossal advantage in solving certain types of problems.

Opportunities. The potential impact of quantum computing is difficult to overstate. It is capable of revolutionizing many areas.

- Medicine and Pharmaceuticals. Developing new drugs is an incredibly complex process that requires modeling the behavior of molecules. Classical computers are unable to accurately simulate complex molecular structures, such as proteins or enzymes. Quantum computers will be able to model molecular interactions at the quantum level, which will allow for the creation of new, more effective drugs and personalized treatments for diseases like cancer or Alzheimer's in record time. This could drastically reduce the time and cost of drug discovery.
- Materials Science. The creation of new materials with desired properties (for example, superconductors that work at room temperature or more efficient catalysts for industry) also requires precise modeling. Quantum simulations will enable the development of materials that seem fantastical today, leading to breakthroughs in energy, electronics, and construction. This includes designing more efficient batteries for electric vehicles or developing new catalysts to make industrial processes like fertilizer production less energy-intensive.
- Finance. The financial sector stands to gain enormous benefits from quantum computing. "Financial institutions tackle a wide array of computationally challenging problems on a daily basis" [2, p. 451]. Quantum algorithms can solve complex optimization problems, such as optimizing investment portfolios, calculating risks, and developing more accurate models for predicting market fluctuations. For example, the Monte Carlo simulation, used extensively in finance for risk assessment, could be performed quadratically faster on a quantum computer.
- Artificial Intelligence and Machine Learning. Quantum computing can significantly accelerate machine learning processes. "It is reported that quantum computing can help artificial intelligence in many ways, such as processing huge complex datasets and evolving algorithms to allow better learning, reasoning, and understanding" [4, p. 203]. Quantum algorithms are capable of processing large datasets faster and identifying complex patterns that are inaccessible to classical algorithms. This specialized field, known as Quantum Machine Learning (QML), opens up new possibilities for the development of more sophisticated and powerful artificial intelligence.
- Climate Change Modeling. Simulating the Earth's climate is one of the most challenging computational tasks due to the vast number of variables involved. Quantum computers could model climate systems with unprecedented accuracy, leading to better predictions of the effects of global warming and helping to develop more effective strategies for mitigation, such as designing new molecules for efficient carbon capture.

Risks. The biggest and most immediate risk associated with quantum computers lies in the field of cryptography. Modern internet security is largely based on asymmetric encryption systems, such as RSA, whose reliability is based on the difficulty of factoring large numbers for classical computers.

In 1994, mathematician Peter Shor developed Shor's algorithm, a quantum algorithm that can find the prime factors of large numbers exponentially faster than any known classical algorithm. A powerful quantum computer capable of executing this algorithm could break most modern encryption systems in a matter of hours or even minutes.

The consequences of this would be catastrophic:

- Banking and financial transactions would become vulnerable.
- State and military secrets, encrypted with current methods, could be exposed.
- Digital signatures and security certificates, which verify the authenticity of websites and software, would lose their reliability.
- Blockchain-based technologies, including cryptocurrencies, could be compromised.

A particularly insidious danger is the "harvest now, decrypt later" attack. Adversaries can record and store currently encrypted data from governments and corporations. While this data is secure today, it can be held indefinitely until a sufficiently powerful quantum computer is built, at which point it will all be decrypted. This means that data considered secure today is already at risk.

Recognizing this threat, the global scientific community is actively working on the development of post-quantum cryptography (PQC) – new encryption algorithms that will be resistant to attacks from both classical and quantum computers. The U.S. National Institute of Standards and Technology (NIST) is already in the process of standardizing such algorithms. The transition to new cryptographic standards will be one of the biggest challenges for the global IT infrastructure in the coming decades.

Current Challenges and Future Prospects. Despite significant progress, the road to creating a full-scale, fault-tolerant quantum computer remains long and difficult. The main obstacles include:

- Quantum Decoherence. Qubits are extremely sensitive to their external environment. Any "noise" – vibrations, temperature fluctuations, electromagnetic fields – can destroy their fragile quantum state in fractions of a second. Maintaining coherence for a sufficient amount of time to perform computations is the primary technological challenge. To combat this, most current quantum computers must be housed in highly controlled environments, often cooled to temperatures colder than deep space (near absolute zero) and shielded from all external interference.
- Error Correction. Due to decoherence, quantum computations are prone to errors at a much higher rate than classical computers. Developing effective codes for quantum error correction requires a significant number of additional physical qubits to create a single logical, stable qubit. It's estimated that thousands of physical qubits might be needed to create one reliable logical qubit.
- Scalability. Building systems with thousands, and eventually millions, of high-quality qubits is an extremely complex engineering task. Researchers are exploring various physical platforms for creating qubits, including superconducting circuits, trapped ions, photonic particles, and silicon quantum dots, each with its own set of advantages and scaling challenges.

To date, existing quantum processors have from several dozen to a few hundred qubits. They are still "noisy" and limited in their capabilities (the so-called NISQ – Noisy Intermediate-Scale Quantum era). However, progress in this field is accelerating. Achieving quantum advantage for solving commercially significant problems is expected within the next 5-10 years.

Conclusion. Quantum computing is a technology with dual potential. On one hand, it promises incredible breakthroughs capable of changing the world for the better – from conquering diseases to creating new materials and solving global optimization problems. On the other hand, it poses an unprecedented threat to the foundations of digital security upon which modern society rests.

The future depends on how quickly and effectively humanity can prepare for this new era. This requires coordinated efforts from scientists, engineers, businesses, and governments. It is necessary not only to continue fundamental research and engineering, but also to actively begin the transition to new, quantum-resistant cryptographic standards.

REFERENCES

1. Bhat H. A., Khanday F. A., Kaushik B. K., Bashir F., Shah K. A. Quantum Computing: Fundamentals, Implementations and Applications. *IEEE Open Journal of Nanotechnology*. 2022. Vol. 3. PP. 61-77.

2. Herman D. et al. Quantum Computing for Finance. *Nature Reviews Physics*. 2023. Vol. 5. PP. 450-465.

3. How M. L., Cheah S. M. Business Renaissance: Opportunities and Challenges at the Dawn of the Quantum Computing Era. *Businesses*. 2023. Vol. 3. PP. 585-605.

4. Rawat B., Mehra N., Bist A. S., Yusup M., Sanjaya Y. P. A. Quantum Computing and AI: Impacts & Possibilities. *ADI Journal on Recent Innovation*. 2022. Vol. 3. PP. 202-207.

5. Rietsche R., Dremel C., Bosch S., Steinacker L., Meckel M., Leimeister J. M. Quantum Computing. *Electronic Markets*. 2022. Vol. 32. PP. 2525-2536.

6. Sood S. K. Quantum Computing Review: A Decade of Research. *IEEE Transactions on Engineering Management*. 2023. Vol. 71. PP. 6662-6676.