Computing, Telecommunication and Control, 2025, Vol. 18, No. 2, Pp. 56–73.
Информатика, телекоммуникации и управление. 2025. Том 18, № 2. С. 56–73.

Research article
DOI: https://doi.org/10.18721/JCSTCS.18205
UDC 004.03

CONCEPT OF ENSURING THE RESILIENCE OF OPERATION OF NATIONAL DIGITAL PLATFORMS AND BLOCKCHAIN ECOSYSTEMS UNDER THE NEW QUANTUM THREAT TO SECURITY

V.Yu. Skiba[1] ✉, *S.A. Petrenko*[1], *K.O. Gnidko*[1], *A.S. Petrenko*[2]

[1] Sirius University of Science and Technology, Federal Territory "Sirius", Krasnodar Krai, Russian Federation;

[2] St. Petersburg Electrotechnical University, St. Petersburg, Russian Federation

✉ vskiba69@mail.ru

Abstract. The obtained results in the field of quantum informatics clearly demonstrate the high technological potential of quantum technologies. A cryptanalytically relevant or significant quantum computer can threaten the operation of various systems, including national blockchain ecosystems and platforms in the Russian Federation. In this situation, a concept of ensuring the resilience of the operation of national digital platforms and blockchain ecosystems under the new quantum security threat is needed, the provisions of which are substantiated in this article. The concept contains a justification for the relevance of the problem and strategic goals of ensuring quantum resilience, national interests in the field of quantum information technologies, the presence of quantum threats to the operation of digital platforms and blockchain ecosystems, methods, means and priority measures to ensure the quantum resilience of national digital platforms and blockchain ecosystems. The main directions of further research of the group "Technologies for countering previously unknown quantum cyber threats" of the Scientific Center for Information Technology and Artificial Intelligence of the Sirius University of Science and Technology, aimed at implementing the proposed concept, are also considered.

Keywords: information security, quantum information technology, quantum security threat, quantum resilience, technological safety, operational safety, verifiable safety

Acknowledgements: The project "Technologies for countering previously unknown quantum cyber threats" was selected for support within the framework of event 2.3 of the state program of the federal territory Sirius "Scientific and technological development of the federal territory Sirius" (application registration No. FCS-2024-2.3-VY-1160-5744, leading scientist – Petrenko S.A., PhD).

Citation: Skiba V.Yu., Petrenko S.A., Gnidko K.O., Petrenko A.S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security. Computing, Telecommunications and Control, 2025, Vol. 18, No. 2, Pp. 56–73. DOI: 10.18721/JCSTCS.18205

Научная статья
DOI: https://doi.org/10.18721/JCSTCS.18205
УДК 004.03

КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ НАЦИОНАЛЬНЫХ ЦИФРОВЫХ ПЛАТФОРМ И БЛОКЧЕЙН-ЭКОСИСТЕМ В УСЛОВИЯХ НОВОЙ КВАНТОВОЙ УГРОЗЫ БЕЗОПАСНОСТИ

В.Ю. Скиба[1] ✉, *С.А. Петренко*[1], *К.О. Гнидко*[1], *А.С. Петренко*[2]

[1] Научно-технологический университет «Сириус», федеральная территория «Сириус», Краснодарский край, Российская Федерация;

[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина), Санкт-Петербург, Российская Федерация

✉ vskiba69@mail.ru

Аннотация. Полученные результаты в области квантовой информатики наглядно показывают высокий технологический потенциал квантовых технологий. Криптоаналитически релевантный или значимый квантовый компьютер может поставить под угрозу функционирование различных систем, в том числе национальных блокчейн-экосистем и платформ в Российской Федерации. В этой ситуации необходима концепция обеспечения устойчивости функционирования национальных цифровых платформ и блокчейн-экосистем в условиях новой квантовой угрозы безопасности, положения которой обоснованы в данной статье. Концепция содержит обоснование актуальности проблемы и стратегических целей обеспечения квантовой устойчивости, национальных интересов в сфере квантовых информационных технологий, наличия квантовых угроз для функционирования цифровых платформ и блокчейн-экосистем, методов, средств и первоочередных мероприятий обеспечения квантовой устойчивости национальных цифровых платформ и блокчейн-экосистем. Также рассматриваются основные направления дальнейших исследований группы «Технологии противодействия ранее неизвестным квантовым киберугрозам» НЦ ИТ и ИИ Научно-технологического университета «Сириус», направленные на реализацию предложенной концепции.

Ключевые слова: информационная безопасность, квантовая информационная технология, квантовая угроза безопасности, квантовая устойчивость, технологическая безопасность, эксплуатационная безопасность, верифицируемая безопасность

Финансирование: Проект «Технологии противодействия ранее неизвестным квантовым киберугрозам» был отобран для поддержки в рамках мероприятия 2.3 государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории “Сириус”» (регистрационный номер заявки ФТС-2024-2.3-VY-1160-5744, ведущий ученый – д.т.н. Петренко С.А.).

Для цитирования: Skiba V.Yu., Petrenko S.A., Gnidko K.O., Petrenko A.S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security // Computing, Telecommunications and Control. 2025. Т. 18, № 2. С. 56–73. DOI: 10.18721/JCSTCS.18205

Introduction

With the advent of the first cryptocurrency platform Bitcoin in 2009, the implementation of blockchain technology began as a special case of building distributed ledger systems [1, 2]. With the advent of the Ethereum platform, it became possible to save records in a ledger created by the user, develop smart contracts to describe the business logic of any transactions without intermediaries [2]. These capabilities made it possible to store all the necessary information (from the conclusion of a contract to

the successful closure of a transaction, subsequent warranty service and compliance with the rights to the intellectual property used) in distributed ledgers in the format of smart contracts, and were developed numerous concepts for creating digital information and logistics platforms to control all regulatory operations [3, 4]. As noted in [3, 4], the implementation of such digital information and logistics platforms allows reducing the risks of logistics errors, unifying document flow, visualizing in real time the processes of movement of goods and the status of customs documents.

All this has led to the rapid development of blockchain technologies (Enterprise Ethereum Alliance, Waves Enterprise, Hyperledger Fabric, Corda Enterprise, Bitfury Exonum, Blockchain Industrial Alliance, Exonum, Nodes Plus, Microsoft Azure Blockchain, Masterchain 2.0 etc.) both in terms of the emergence of new blockchain platforms for various purposes, and in terms of the development of the decentralized financial sector, which de facto is a system of various protocols and applications built on blockchain technology and operating on the basis of smart contracts.

There is a steady growth in the implementation of blockchain technologies in the creation of digital platforms in various areas and industries of the Russian Federation. The National Technology Initiative website[1] lists a number of developed and implemented projects, such as Cryptoveche (remote voting system), Edemes (database for identifying and monitoring the movement of cultural property), InsurDoc (management of intellectual property rights), Trevo (control of cargo and goods transportation), DSMS (decentralized exchange of financial messages) and a number of other projects. Web3 Tech company offers a range of products operating on its own blockchain platform called Confident. Among the products offered, based on the Confident platform, is the software and hardware complex for working with digital assets, Digital Treasury.

Using similar approaches, the Bank of Russia "Digital Ruble" platform and the Russian Export Center's information system "My Export" digital platform (state information system "Single Window") are evolving, and the National digital transport and logistics platform (NDTLP) is being created [4, 5].

Simultaneously with this, the issue of the security of using blockchain technologies is constantly being raised. First of all, these issues are related to the security and reliability of storing and using data placed in systems using blockchain technologies (blockchain ecosystems). An analysis of publications shows that researchers, as a rule, focus their attention on one or more interrelated aspects that pose a potential threat to the operation of the blockchain ecosystem.

The development of quantum computing poses a threat to existing cryptographic mechanisms used in digital platforms and blockchain ecosystems (DPiBE), creating risks to transaction security and threatening the integrity and immutability of data in distributed ledger systems.

The results obtained in the field of quantum technologies and quantum information technologies clearly demonstrate the high technological potential of quantum technologies for solving a number of problems, much more efficiently than any modern "traditional" computer [2, 4–7].

A cryptoanalytically relevant or significant quantum computer may threaten the resilience of various systems [4, 8, 9], including critical information infrastructure facilities of the Russian Federation, national DPiBE.

Ensuring the resilience of DPiBE to attacks by intruders (or malicious actors) using a quantum computer (or, in other words, their quantum resilience) is one of the pressing scientific and technical problems of the digital economy of the Russian Federation.

In this situation, the Concept is needed to ensure the resilience of the operation of national DPiBE under of a new threat to quantum security (the Concept), which should contain, according to the opinion of the authors of this article, at least the following provisions based on the systematization of the results obtained in more than 30 other our own papers:

- national interests and strategic goals of the Russian Federation;

[1] Natsional'naia tekhnoløgicheskaia initsiativa (NTI) [National Technology Initiative (NTI)], Available: https://nti2035.ru/ (Accessed 13.03.2025)

- current state of development of quantum technologies and quantum information technologies;
- main quantum threats to DPiBE and the ways of ensuring their quantum resilience.

Prerequisites for conducting research in the sphere of quantum resilience of national DPiBE

Despite numerous doubts about the feasibility of using blockchain technologies in the early years of their development, today there is a stable growth and development of these technologies, as well as their implementation in various digital platforms in almost all areas and sectors of the digital economy of the Russian Federation. At the same time, questions arise about ensuring the security of information in DPiBE.

The global information space, DPiBE are simultaneously used, on the one hand, to expand access of individuals and legal entities to information, digital services and financial instruments and to increase the efficiency of the digital economy (data economy), and, on the other hand, by criminal structures, international terrorist organizations and states pursuing an unfriendly policy towards the Russian Federation, to disrupt the functionality of these facilities and create centers of social tension [4, 8–12].

Conducting cyber operations against transportation infrastructure, power grids, dams, chemical plants, nuclear power plants and other critical infrastructure, DPiBE is technically possible. Such operations could have large-scale consequences, causing significant damage and/or leading to a large number of casualties among the civilian population [4, 8–10, 12].

As DPiBE develop, they acquire new and increasingly emergent system properties: controllability, self-organization, adaptability, cybersecurity, technological security, operational security, verifiable security and cyber resilience (including quantum resilience). Each of these properties is the subject of research, and each subsequent property makes sense only if the previous one is present.

Cyber resilience of a DPiBE is understood as the ability of a DPiBE, operating according to a certain set of algorithms, to achieve the goals and objectives of operation in the face of growing security threats.

Summarizing the results of the authors' research (for example, [4, 8, 9, 13]), the following conclusions can currently be drawn:

- in the context of the growth of classical and quantum cyberattacks by intruders, ensuring cyber resilience is becoming much more difficult;
- of particular concern are the so-called new type of quantum threats – quantum attacks or attacks using a quantum computer;
- most cryptographic primitives used in modern information systems (including hash functions, digital signatures, asymmetric cryptographic algorithms and related protocols) are not resistant to quantum attacks;
- in order to hack the crypto-primitives used, a number of well-known quantum algorithms can be successfully and effectively applied, in particular, Shor's algorithm [14, 15] for factorization and discrete logarithm and Grover's algorithm for accelerating the attack on the hash function [16].

This creates risks to transaction security and threatens the integrity and immutability of data in distributed ledger systems.

Accordingly, the quantum resilience of DPiBE is the ability of these systems to achieve the goal of functioning under the conditions of attacks by intruders using a quantum computer.

A bibliometric analysis of scientific literature on quantum technologies for the period from 1990 to 2020 showed [7]: the dynamism of the development of the field, a high degree of concentration of research and international scientific relations, as well as the participation of not only universities and academic organizations, but also large corporations (especially from Japan) and military research structures (primarily from the USA). At the same time, the Russian Federation is characterized by:

- high concentration of research in metropolitan areas and their significant internationalization;
- leading contribution of the Russian Academy of Sciences (RAS), which ranks sixth among scientific organizations in the world in the number of publications in the field of quantum technologies for the analyzed period [6]);

• growing role of universities in the development of the scientific base of quantum technologies and quantum information technologies;

• still weak involvement of the Russian commercial sector in research.

Since 2020, the number of scientific publications on the results of research in the field of quantum technologies and quantum information technologies has been growing exponentially, including due to work on ensuring information security in connection with the emergence of new quantum threats.

The situation in the field of quantum computing is characterized by a kind of "technological race" between leading companies [4]. There are dozens of organizations in the world attracting significant investments to create quantum computers[2].

In the Russian Federation, scientific research and engineering surveys are also being conducted to create the first domestic quantum computers. Well-known Russian mathematicians have made significant contributions to this field of knowledge, for example, employees of the Steklov Mathematical Institute of RAS: head of the Department of Mathematical Physics, PhD, corresponding member of the RAS I.V. Volovich and head of the Department of Probability Theory and Mathematical Statistics, laureate of the Claude E. Shannon Award for outstanding achievements in information theory, PhD, academician of the RAS A.S. Holevo [17, 18]. And scientists from the Russian Quantum Center and P.N. Lebedev Physical Institute of RAS, for example, have developed a prototype of a quantum computer on ytterbium ions[3]. Quantum processors with 2–10 qubits and quantum simulators with 10–20 qubits have been developed, and the first domestic quantum processors with 50–100 qubits are expected to appear by the end of 2025.

Despite the fact that the era of noisy intermediate-scale quantum (NISQ) devices is currently ongoing, quantum information science as a whole is already a new, rapidly developing branch of science associated with the use of quantum systems to implement fundamentally new methods of transmitting messages, computing and technologies (quantum communication channels, quantum cryptography, quantum computer) [9, 17–21].

Periodically, there are reports of achieving "quantum supremacy"[4], that is, the creation of a quantum computer capable of solving problems significantly more efficiently than any modern "traditional" computer (modern von Neumann supercomputers are also considered "traditional" tools in this approach) or even impossible to solve using "traditional" computing tools [4, 22]. Soon, quantum computers will reach sufficient maturity and will be able to "hack" most cryptographic primitives used in blockchain ecosystems [4, 23, 24].

These results have allowed experts to predict that quantum information technologies capable of cracking Bitcoin cryptographic algorithms could be created in 2027, and the RSA cryptographic algorithm in 2031 [25]. The British regulator (National Cyber Security Centre, NCSC) in its 2020 recommendations predicts the emergence of a cryptographically significant quantum computer in 2030[5].

It should be taken into account that most forecasts are based on open data, and in the conditions of geopolitical confrontation, there is a possibility that real successes in creating a working quantum computer are confidential information. It is possible to determine the real situation only after identifying facts of compromise of a significant array of data or facts of disruption of the functioning of any systems (not necessarily DPiBE) as a result of the use of quantum computers by an intruder, including in conjunction with "traditional" computers.

[2] Quantum computing start-up secures €10m investment – National Technology, Available: nationaltechnology.co.uk (Accessed 13.03.2025); PsiQuantum Closes $450 Million Funding Round to Build the World's First Commercially Viable Quantum Computer — PsiQuantum, Available: https://www.psiquantum.com/news-import/psiquantum-closes-450-million-funding-round-to-build-the-worlds-first-commercially-viable-quantum-computer (Accessed 13.03.2025)

[3] Sozdan prototip kvantovogo komp'iutera na ionakh itterbia [A prototype of a quantum computer on ytterbium ions has been created], Available: https://strana-rosatom.ru/2022/02/25/sozdan-prototip-kvantovogo-kompjute/ (Accessed 13.03.2025)

[4] Here the question of "price vs quality" arises: how much more expensive is such a quantum component of a computing system than a traditional one, capable of doing the same work, albeit over a longer period of time?

[5] Preparing for Quantum-Safe Cryptography, Available: https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography (Accessed 13.03.2025)

Thus, developments in the field of creating quantum computers and developing quantum information technologies with quantum computing algorithms create more and more preconditions for their use by potential intruders (or malicious actors) to disrupt the operation of DPiBE.

Scenario and methods for ensuring quantum resilience of DPiBE

In [4, 8], it has already been noted that a number of technological countries around the world have already begun to prepare to counteract future quantum threats.

The US presidential administration has issued several directives[6] on preparing the state and business for future quantum cyberattacks, and has also instructed the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the Cybersecurity and Infrastructure Security Agency (CISA) to take all necessary measures to protect the critical infrastructure of the US and its NATO allies from a quantum threat within one year. There is no information on what has been done.

In [4, 13], it is substantiated that due to the current lack of a unified scientific, methodological and technical basis for the development of quantum resilience DPiBE in the Russian Federation, the creation of such systems is a long-term task. At the same time, it is necessary to develop a new technology to counter quantum security threats. Without solving this fundamental scientific problem, it is impossible to talk about achieving the goals of the national program "Data Economy"[7].

In this regard, in the fall of 2024, a research group "Technologies for countering previously unknown quantum cyber threats" was formed at the Scientific Center for Information Technology and Artificial Intelligence of the Sirius University of Science and Technology.

The main goal of creating the research group is to create a promising world-class technology to ensure quantum resilience of the leading national DPiBE of the digital economy of the Russian Federation, which, unlike known technologies, will prevent significant or catastrophic consequences in the face of previously unknown cyberattacks by intruders using a quantum computer.

Based on the results obtained in [4, 23, 24], when developing the Concept, it is necessary to take into account two main scenarios for the development of quantum information technologies:

1. Use of quantum computing tools in the infrastructure of DPiBE for information processing and/or protection. Obviously, in this case, quantum computing tools and quantum calculations will be used together with "traditional" computing tools and information protection;

2. Use of quantum computing tools to solve individual local computationally intensive problems. At the same time, the formation of "hostile" information impacts is realized using quantum computing tools.

The absence of serial production of basic elements of quantum computing tools ("quantum chips"), as well as the selected basic physical platform for the creation and production, at least in small batches, of quantum processors (or computers) determines the second scenario as a priority.

The results of an analysis of various platforms (using which work is being carried out to create quantum computers, emulate quantum computing, and develop quantum information processing technologies) and quantum threats to various DPiBE (for example, performed in [2, 4, 8, 9]) allow us to draw a number of conclusions:

- development of quantum computing threatens the existing cryptographic mechanisms used in DPiBE;
- achievements of IBM, as well as a number of other high-tech manufacturers of quantum computers, convincingly demonstrate the realism of the implementation of quantum threats in the near future. The emergence of a relevant quantum computer capable of cracking traditional cryptographic algorithms is expected in the period 2026–2030;

[6] Memorandum on Preparing for Post-Quantum Cryptography, Available: https://www.dhs.gov/publication/memorandum-preparing-post-quantum-cryptography (Accessed 13.03.2025); National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, Available: Preparing Secrets for a Post-Quantum World—National Security Memorandum 10 – EveryCRSReport.com (Accessed 13.03.2025)

[7] The national program "Data Economy" has been implemented in the Russian Federation since 2025 and replaces the project "Digital Economy of the Russian Federation", which was completed in 2024.

• main problematic issues of ensuring quantum resilience include the insufficient level of readiness for the growth of quantum cyberattacks by intruders and the growth in the number and complexity of DPiBE structures, as well as the difficulty of identifying quantitative patterns that allow us to study the cyber stability of DPiBE in the face of classical and quantum cyberattacks by malicious actors.

Ignorance or ignoring the above-mentioned problematic issues leads to a decrease in the efficiency of DPiBE.

The Concept also needs to take into account that the use of classical approaches (for example, methods of mathematical statistics and experimental design and analytical verification methods) considered in [4] to identify the indicated patterns is impractical due to the presence of contradictions associated with the specifics of specific models of system behavior in the presence of quantum and classical attacks by an intruder.

The Concept must provide for the use of methods for ensuring verified security, when technological and operational security is ensured using one mathematical apparatus of specification and verification both at the stage of system creation and adaptive information security management using a reference model with anticipatory forecasting. Such methods were proposed in [26], but require development in the interests of ensuring quantum resilience of national DPiBE.

It seems advisable to identify three main directions in the Concept for solving the scientific problem of ensuring the quantum resilience of national DPiBE, which, in accordance with [4, 8, 9, 23, 24], have already been developed to one degree or another.

The research group for countering previously unknown quantum cyber threats has completed the development of three new post-quantum algorithms for electronic digital signatures based on the mathematical apparatus of finite non-commutative associative algebras (FNAA). Effective algorithms for solving this problem on classical and quantum computers are currently unknown [27].

Similar works are also known in this area, aimed at creating:

• the post-quantum electronic signature "Rosehip"[8] [28], the cryptographic resistance of which is based on the computationally complex mathematical problem of decoding a random linear code;

• the "Forsythia" protocol for generating a common key using the supersingular elliptic curve isogeny apparatus[9] [29].

This direction is relatively "young" and poorly studied, which requires work on optimizing the performance of post-quantum algorithms and proving their cryptographic resistance in the conditions of using of quantum computers by an intruder. In the spring of 2023, for example, the Royal Swedish Institute of Technology discovered a vulnerability in the CRYSTALS-Kyber post-quantum algorithm, one of the finalists of the famous NIST competition [30].

The use of quantum cryptographic algorithms with mathematically proven cryptographic resistance is the second direction of ensuring quantum resilience of the national DPiBE. This direction should also include the use of quantum data transfer protocols, quantum key distribution protocols, quantum random number generators etc. At the same time, it is necessary to take into account the high probability of the presence of undeclared capabilities and software backdoors in a large number of emerging open and commercial libraries for developers of digital platforms (SDK) implementing new cryptographic schemes.

The third direction of ensuring quantum resilience of the national DPiBE is the creation of a full-fledged quantum infrastructure, which provides for the software and hardware implementation of a fully quantum model of protected information systems. It should be emphasized that this direction is a distant and possibly unachievable prospect in general.

[8] The package of documents on the post-quantum electronic signature "Rosehip" was presented to the Technical Committee for Standardization "Cryptographic Protection of Information" of Rosstandart (TC26) in June 2022.

[9] Developed within the framework of the activities of the working subgroup on isogenies of supersingular elliptic curves of Working Group 2.5 "Post-quantum cryptographic mechanisms" of TC26.

The following section of this article sets out the main provisions of the Concept developed by members of the above-mentioned research group at the first stage of the project by generalizing, systematizing and comprehensively rethinking the results obtained earlier. Given that this section is essentially a draft regulatory legal act, references to the sources used in its writing are not provided.

Proposals for the main provisions of the Concept

The Concept, based on the analysis of the current state of ensuring information security of national DPiBE of the Russian Federation and the development of quantum technologies and quantum information technologies, defines the goals, objectives and key problems of ensuring quantum stability of national DPiBE.

The purpose of the Concept development is to identify the main approaches to achieving the goal of functioning DPiBE of the Russian Federation in the face of attacks by intruders (or malicious actors) using a quantum computer (that is, the quantum resilience of national DPiBE) to ensure global technological competitiveness and technological sovereignty of the Russian Federation in the field of quantum technologies, quantum communications, quantum computing and quantum information technologies.

The Concept should become an integral part of the Concept for Ensuring Information Security of the Russian Federation.

General provisions

The Concept serves as a methodological basis for the development of a set of regulatory and organizational and methodological documents regulating activities in the field of ensuring the quantum resilience of the national DPiBE, as well as for developing proposals to improve scientific, technical and organizational support for the quantum resilience of the national DPiBE, as well as training personnel in this area.

For the purposes of this Concept, the following concepts are used:

• blockchain (or distributed ledger) – a continuous sequential chain of blocks (linked list) built according to certain rules, containing some information;

• blockchain ecosystem – a network of all participants in a blockchain network, who share business processes and business goals;

• quantum computing – a type of computing that uses quantum mechanical phenomena, such as superposition and entanglement to perform operations on data;

• quantum information technology – a technology that provides for the implementation of quantum algorithms using quantum computing, quantum communications or other quantum technologies;

• quantum communication – technology of encoding and transmitting data in quantum states of photons;

• quantum key distribution – procedure of generating and distributing secret keys, implemented using quantum cryptographic protocols and quantum communication channels;

• quantum technology – technology for creating computing systems based on new principles (quantum effects) that allows us to radically change the ways, in which large amounts of information are transmitted and processed;

• quantum resilience – ability to achieve the goal of operation under of attacks by intruders (or malicious actors) using a quantum computer;

• digital platform – online services and/or software products that allow user interaction and transactions, provide access to content, services, or products, and provide user-friendliness for various functions.

Importance of ensuring the quantum resilience of the national DPiBE

Ensuring the resilience and security of critical infrastructure facilities and services for the transmission, processing and storage of large amounts of data in the face of the growth of both classical and previously unknown (and, consequently, poorly studied) security threats is one of the five key objectives of the "Information Security" project in accordance with the requirements of the passport of the national

program “Data Economy”. Special attention is paid to assessing the level of security of government information systems (GIS).

National DPiBE are generally GIS and are becoming an increasingly important element of the digital economy of the Russian Federation.

The urgency of the problem of ensuring the quantum resilience in fractionally of national DPiBE as GIS is due to:

• the contradiction between the emergence of a new type of information security threat (quantum threats) and the inability of known technologies (models, methods and means) for ensuring information security and cyber resilience to detect, neutralize and prevent such threats;

• the need to increase requirements for ensuring information security and cyber resilience of the critical information infrastructure of the Russian Federation, including national DPiBE;

• the growth in the number of national DPiBE, the increasing complexity of their structures and functioning processes.

National interests in the sphere of quantum technologies and quantum information technologies

The development of the field of quantum technologies and quantum information technologies is one of the tasks aimed at achieving the goal of scientific and technological development of the Russian Federation in accordance with the National Security Strategy[10].

National interests in the field of quantum technologies and quantum information technologies are reflected in the following documents:

• Strategy for scientific and technological development of the Russian Federation[11] (subparagraph “d” of paragraph 21 and subparagraphs “a” – "c" of paragraph 24);

• Priority areas of scientific and technological development (paragraph 4) and the List of the most important science-intensive technologies (paragraph 12)[12];

• List of instructions following the meeting with scientists and the plenary session of the Forum of Future Technologies “Computing and Communications. Quantum World” (regarding the development of quantum technologies and the creation of a university in the field of quantum technologies for the purpose of implementing educational programs for studying advanced developments in this area and involving the participation of schoolchildren)[13];

• Concept for regulating the quantum communications industry in the Russian Federation until 2030[14].

On February 6, 2024, the Federation Council Committee on Defense and Security reviewed and took control of the issue of ensuring information security using quantum technologies as part of the national project to form a data economy.

Strategic goals of ensuring quantum resilience of national DPiBE

The strategic goals of ensuring the quantum resilience of national DPiBE are as follows:

• *Ensuring the quantum sovereignty of the Russian Federation*. The development of quantum technologies and quantum information technologies in the world increases the number of new external risks and threats to the country’s digital sovereignty. The emergence of quantum computers, as well as the high degree of development of quantum computing and AI technologies, create risks and threats of compromising existing methods of data protection. It is necessary to ensure the creation

[10] Approved by the decree of the President of the Russian Federation dated July 2, 2021 No. 400 “On the National Security Strategy of the Russian Federation” (http://publication.pravo.gov.ru/document/0001202107030001)

[11] Approved by the decree of the President of the Russian Federation dated February 28, 2024 No. 145 “On the Strategy for Scientific and Technological Development of the Russian Federation” (http://publication.pravo.gov.ru/document/0001202402280003)

[12] Approved by Decree of the President of the Russian Federation dated June 18, 2024 No. 529 “On approval of priority areas of scientific and technological development and a list of the most important science-intensive technologies” (http://publication.pravo.gov.ru/document/0001202406180018)

[13] Approved by the President of the Russian Federation on September 3, 2023 No. Pr-1734 (https://digitalcryptography.ru/news/novosti-otrasli/vladimir-putin-dal-porucheniya-po-razvitiyu-kvantovykh-tekhnologiy/)

[14] Approved by the Order of the Government of the Russian Federation dated July 11, 2023 No. 1856-r “On approval of the Concept for regulating the quantum communications industry in the Russian Federation until 2030” (http://publication.pravo.gov.ru/document/0001202307170029)

and development of domestic quantum information technologies that ensure the quantum resilience of national DPiBE.

• *Creating modern and effective domestic systems for protecting information from quantum threats*. Government agencies, industrial enterprises, scientific and expert communities are working in many directions to create systems capable of countering new quantum threats to information security. It is necessary to ensure the development of a complex of domestic trusted computing equipment using quantum technologies and quantum information technologies and certified information security tools, including cryptographic ones, that ensure effective counteraction to quantum threats.

• *Implementing and integrating quantum and post-quantum cryptography, including methods of quantum communication and quantum key distribution, into key DPiBE in various areas of the digital economy of the Russian Federation*.

• *Providing guarantees to Russian individuals and legal entities to ensure the security of their information processed on national DPiBE*. It is necessary to ensure the attractiveness and competitiveness of using national DPiBE in comparison with foreign DPiBE.

• *Developing the export potential of national DPiBE*. It is necessary to provide proof of the quantum resilience of national DPiBE, recognized by the international community, which will expand the customer base or the number of implementations among states friendly to the Russian Federation.

The current state of ensuring quantum resilience of national DPiBE

In the era of NISQ devices, the components of a quantum computer that can be implemented in practice are imperfect in terms of accuracy and highly susceptible to interference and errors. However, using these components in combination with classical computers and fifth-generation supercomputers will soon allow a malicious actor to achieve significant overall computing acceleration when solving multidimensional optimization and information security problems.

The general situation is that there is no technology for mass production of quantum chips and even a physical platform for quantum computers has not been selected. In parallel, work is underway to create quantum computers based on more than 10 platforms, the main ones being: superconductors, ions, neutral atoms and photons.

The first (on superconductors) are developed by IBM, Google, Rigetti, Intel, Alibaba. The advantages of these platforms include: good scalability, stability over time and relative ease of management. The disadvantages are: need to use ultra-low temperatures and low coherence.

The second (on ions) are being improved by Honeywell, IonQ, AQT. These platforms are characterized by better stability and accuracy of operations. The disadvantage is considered to be the technological limitation of the maximum size of the quantum register.

The third (on neutral atoms) are being improved by Pasqal, Harvard University and the University of Paris-Saclay. Platforms of this type allow for good scaling. At the same time, they are distinguished by the high complexity of managing quantum systems.

The fourth (on photons) are created by Xanadu, Quix, Psi Quantum etc. These platforms are compact in size, operate at room temperatures and are relatively easy to interface with fiber-optic communication lines. However, it is more difficult to implement logical circuits in such platforms due to the weak interaction of photons.

In the Russian Federation, scientific research and engineering studies are also being conducted to create the first domestic quantum computers.

Cooperation and consortia are being formed on the basis of domestic competence centers in the field of quantum technologies, quantum information technologies and quantum communications[15].

[15] The cooperation includes scientific divisions of the Russian Academy of Sciences (Institute of Automation and Electronics SB RAS, SB RAS, IPF RAS and its branch IMF RAS), the Center for Quantum Technologies of Lomonosov Moscow State University, Sirius University of Science and Technology, Bauman Moscow State Technical University, MIET, MIAN., FIAN, PTIAN, ISAN, Russian Quantum Center, FSUE VNIIA named after N.L. Dukhov, ITF named after L.D. Landau, ITF named after A.V. Rzhanov, ISP named after P.L. Kapitsy, ISSP, KNRTU-KAI, KHFTI, KFU, Moscow State Pedagogical University, MIPT, MISiS, NSTU, Skoltech, ITMO University, Ioffe Institute of Physics and Technology and others.

By the end of 2025, the first domestic quantum processors with 50–100 qubits are expected to appear.

At the same time, the results of the analysis of the current state of information security in national DPiBE are showing that the level of quantum resilience currently does not meet the vital needs of individuals, society and the state.

The current conditions of the country's political and social and economic development are exacerbating contradictions between the needs of society to expand the free exchange of information and the introduction of digital, including financial, tools and the need to maintain certain restrictions on the dissemination of information and ensure the sustainability of digital tools.

The main factors of the presence of quantum threats to national DPiBE are:

- insufficient cybersecurity and cyber resilience of DPiBE in the context of the growth of classical and quantum cyberattacks by intruders;
- the growing number of structures of national digital platforms and the growing complexity of the behavior of blockchain ecosystems;
- difficulty in identifying quantitative patterns that allow to study the cyber resilience of national DPiBE in the context of classical and quantum cyberattacks by intruders;
- inconsistency of the actual parameters of the operating of national DPiBE in functional specifications;
- overvaluation of the capabilities of modern methods and means of information protection, reliability and fault tolerance of blockchain.

The lack of effective mechanisms for regulating the quantum resilience of national DPiBE leads to many negative consequences.

Insufficient security of GIS, which are digital platforms or blockchain ecosystems, leads to the loss of important political, scientific, technical, economic or commercial information, including information on foreign economic activity, transport and logistics or other activities important for ensuring the security of the state.

The lack of protection of citizens' rights to information, manipulation of information in GIS, cause an inadequate response from the population and in some cases can lead to political or social instability in society or the state.

The lag of domestic information technologies (including quantum technologies and quantum information technologies) forces operators of national DPiBE to purchase untrusted and unprotected imported computing equipment and software, including blockchain technologies. As a result, the likelihood of unauthorized access to databases and data banks increases, both as a result of classical attacks and especially using quantum threats. The country's dependence on foreign manufacturers of computer equipment, software and information products also increases.

This state of affairs in the field of ensuring quantum resilience of national DPiBE requires solving the following key tasks:

1. Development of scientific and practical foundations of quantum technologies, quantum computing, quantum information technologies and ensuring quantum resilience, corresponding to the world's advanced levels of scientific and technological development, the current geopolitical situation and the conditions of political and social and economic development of the Russian Federation.

2. Improvement of the legislative and regulatory framework for ensuring information security in terms of ensuring cybersecurity and quantum resilience of national DPiBE.

3. Development of modern methods and software and hardware that provide a comprehensive solution to the problems of quantum resilience of national DPiBE.

4. Development of criteria and methods for assessing the quantum resilience of national DPiBE, as well as assessing the effectiveness of systems and means of ensuring the security of national DPiBE.

5. Development of a set of interconnected training programs in the field of quantum information technologies and ensuring quantum resilience of national DPiBE, including additional professional training and/or advanced training.

The quantum threats to the functioning (threats to quantum resilience) of national DPiBE

Sources of threats to the quantum resilience of national DPiBE can be divided into external and internal. The external sources include:

- unfriendly policies of foreign states in the field of global information monitoring, dissemination of information and new information technologies, including quantum technologies and quantum information technologies;
- activities of foreign intelligence services, special services, political and economic structures directed against the interests of the Russian Federation using quantum technologies and quantum information technologies;
- criminal actions of international groups, formations and individuals using quantum technologies and quantum information technologies.

The internal threats to the quantum resilience of national DPiBE are:

- illegal activities of political and economic structures in the field of using national DPiBE;
- violations of established regulations for the collection, processing and transmission of information in national DPiBE;
- intentional actions and unintentional errors of personnel of national DPiBE;
- disruption of technical means and software failures in national DPiBE.

The ways of influencing national DPiBE with the aim of violating quantum resilience are divided into informational, software and mathematical and physical.

The informational methods for violating the quantum resilience of national DPiBE include:

- intrusions of the targeting and timeliness of information exchange, illegal collection and use of information in national DPiBE using quantum technologies and/or quantum information technologies;
- unauthorized access to information resources of national DPiBE using quantum technologies and/or quantum information technologies;
- manipulation of information (disinformation, concealment or distortion of information) from national DPiBE using quantum technologies and/or quantum information technologies;
- illegal copying of data from national DPiBE using quantum technologies and/or quantum information technologies;
- destruction of information processing technology in national DPiBE using quantum technologies and/or quantum information technologies.

Software and mathematical methods for violating the quantum resilience of national DPiBE include:

- introduction of malware and viruses into national DPiBE using quantum technologies and/or quantum information technologies;
- installing software and hardware bugs into national DPiBE using quantum technologies and/or quantum information technologies;
- destruction or modification of data into national DPiBE using quantum technologies and/or quantum information technologies;
- defeat or destruction of information processing and communication facilities in national DPiBE using quantum technologies and/or quantum information technologies;
- destruction, disruption or theft of machine or other originals of information carriers;
- theft from national DPiBE using quantum technologies and/or quantum information technologies of software and/or hardware keys, means of cryptographic information protection;
- application of quantum information technologies and quantum algorithms for cryptographic analysis of information obtained from DPiBE;
- supply of components "infected" with the use of quantum technologies and/or quantum information technologies for use into national DPiBE.

As a result of the impact of quantum threats on national DPiBE, serious damage may be caused to the vital interests of the Russian Federation in political, economic, defense and other areas of state activity, and social and economic damage may be caused to society and individuals.

Methods and means of ensuring quantum resilience of national DPiBE

In order to prevent, counteract and neutralize quantum threats to national DPiBE, it is necessary to comprehensively apply legal, software and hardware, organizational and technical methods to ensure the quantum resilience of national DPiBE.

Legal methods for ensuring the quantum resilience of national DPiBE include the development of a set of regulatory legal acts, guidelines and regulatory and methodological documents on information protection in information systems and the use of quantum technologies and quantum information technologies. Considering the problems and risks associated with the use of quantum technologies and quantum information technologies, it is necessary to form in the field a new quantum legislation [31].

Software and hardware methods for ensuring the quantum resilience of national DPiBE include preventing leakage of processed information by eliminating unauthorized access to it, preventing special impacts that cause destruction, annihilation, distortion of information or failures in the operation of information technology, identifying embedded software or hardware errors, eliminating the interception of information by technical means, using cryptographic means of protecting information during transmission via communication channels, including using quantum key distribution and post-quantum cryptographic algorithms.

Organizational and economic methods for ensuring quantum resilience of national DPiBE include the formation and maintenance of systems for protecting confidential information in DPiBE using quantum information technologies, certification of these systems according to information security requirements, licensing of activities in the field of information security, standardization of methods and means of protecting information in DPiBE using quantum information technologies, control over the actions of personnel in protected DPiBE using intelligent methods (including quantum) and means.

An important place among these methods of ensuring the quantum resilience of the national DPiBE is occupied by motivation, economic incentives and psychological support for the activities of personnel involved in ensuring the quantum resilience of DPiBE, including the use of methods of multi-level filtering of potentially dangerous information and psychological influences [32].

Priority measures to ensure quantum resilience of national DPiBE

Priority measures to ensure quantum resilience of national DPiBE should include:

- development of forms, methods and means of implementing methods for ensuring quantum resilience of national DPiBE;
- preparation of decisions of executive authorities and documents that consolidate the main provisions of state policy to ensure the quantum resilience of national DPiBE;
- creation of a regulatory framework for implementing methods for ensuring quantum resilience of national DPiBE, including determining the sequence and procedure for developing legislative and regulatory legal acts, as well as mechanisms for the practical implementation of the adopted legislation;
- analysis of technical and economic parameters of domestic and foreign software and hardware for ensuring information security, including with the use of quantum information technologies and quantum key distribution, and the selection of promising areas for the development of domestic quantum technologies;
- formation of a scientific and technical program for the improvement and development of methods and means for ensuring quantum resilience of national DPiBE, providing for their use in national information and telecommunication networks and systems, taking into account the entry of the Russian Federation into global information networks and systems;
- creation of a certification system for domestic information technology tools for compliance with the requirements for ensuring quantum resilience;

• improving the organizational structure of the information security system of the Russian Federation in part of coordinating and regulating activities to ensure the security of the use of quantum information technologies and ensuring the quantum stability of DPiBE;

• development of a system of economic and statistical indicators characterizing the efficiency of DPiBE in the presence of quantum threats;

• determination of the real needs for specialists in ensuring the quantum resilience of national DPiBE, organization of a system for the selection, training and retraining of personnel.

Organizational framework for ensuring the resilience of national DPiBE

The results of the analysis of the state of quantum resilience of national DPiBE indicate the need to reform the existing organization of information security as a whole with the aim of integrating it into the information security system of the Russian Federation.

The organizational structure for ensuring quantum resilience of DPiBE of the Russian Federation consists of:

• state authorities and administration bodies of the Russian Federation and constituent entities of the Russian Federation solving problems within their competence;

• state and interdepartmental commissions and councils specializing in the development and implementation of digital platforms, blockchain ecosystems, quantum communications, quantum technologies, as well as ensuring quantum resilience and information security;

• research, design and engineering organizations involved in the development and implementation of digital platforms, blockchain ecosystems, quantum communications, quantum technologies, as well as ensuring quantum resilience and information security;

• operators of national DPiBE;

• educational institutions that train and retrain personnel for the development and implementation of digital platforms, blockchain ecosystems, quantum communications, quantum technologies, as well as ensuring quantum resilience and information security[16].

Main research areas within the project "Technologies for countering previously unknown quantum cyber threats"

The research group at the Sirius University of Science and Technology has already conducted and obtained the following results within the framework of the project "Technologies for countering previously unknown quantum cyber threats":

1. Conceptual model of quantum security threats for DPiBE of the Russian Federation has been developed based on the addition and development of the well-known Methodology for assessing security threats by FSTEC of Russia and the Matrix of tactics and techniques of cyberattacks – MITRE Enterprise ATT&CK Matrix [33].

2. Based on the Kalman filter and the catastrophe theory of R.K. Thomas and V.I. Arnold, the mathematical model of the functioning of national DPiBE under the conditions of attacks by intruders using a quantum computer has been developed.

Currently, the common types of attacks on blockchain include, for example, [1, 34, 35]:

• 51% attack (a malicious actor controls more than 50% of the network's processing power, allowing to manipulate the blockchain, potentially enabling double-spending or reversing transactions);

• Eclipse attack (a malicious actor attacks a single node of the blockchain network, creating an artificial false area around it, intercepting and replacing messages);

• Sybil attack (a malicious actor tries to capture and use a certain number of nodes of the blockchain network at once to generate incorrect data);

• Finney attack and Race attack (double-spending of funds in the blockchain system, if a miner accepts an unconfirmed transaction in the network);

[16] Currently, training and retraining in quantum stability of personnel related to ensuring quantum stability is carried out at the Sirius University of Science and Technology.

• Dust attack (formation of similar addresses in the network with the transfer of a small amount of money to the recipient's account in the hope that the next time the recipient will confuse the addresses and send the transfer to the wrong account);

• Denial of service (a malicious actor sends a large number of identical requests to a node of the blockchain network, DDoS);

• Cyberattacks on blockchain crypto primitives performed using quantum computers (quantum attacks).

3. Requirements have been developed for the system architecture, tools for ensuring quantum stability of national DPiBE using the cores of Enterprise Ethereum Alliance, Waves Enterprise, Hyperledger Fabric, Corda Enterprise, Masterchain, Microsoft Azure Blockchain in the context of a new quantum security threat.

The main areas of further research by the above-mentioned research group are:

• development of methods and models for ensuring verified security of national DPiBE in the context of a new quantum security threat;

• development of methods and algorithms for analyzing the resilience of national DPiBE in the context of a new quantum security threat based on modification of quantum algorithms (Shor, Grover, etc.);

• development of a methodology for solving problems of analyzing the quantum resilience of national DPiBE;

• development of methods and algorithms for parametric synthesis of quantum-resilience national DPiBE based on the theory of multi-criteria optimization in the context of a new quantum security threat;

• development of a methodology for solving problems of synthesizing technologies and programs for ensuring quantum resilience of national DPiBE;

• creation and development of the complex of logical and dynamic models to ensure the quantum resilience of national DPiBE;

• development of a software architecture for solving problems of analyzing (assessing) the resilience of national DPiBE under of a new quantum security threat;

• creation and debugging of a prototype of the software package for solving the problems of analysis (assessment) of the resilience of the operating of national DPiBE under of a new quantum security threat;

• detailing of contents and features of the implementation of the main stages of solving the problems of technology synthesis and comprehensive planning for ensuring quantum resilience of national DPiBE;

• defining the composition and structure of a possible analytical and simulation software package for synthesizing technology for ensuring quantum resilience of national DPiBE;

• detailing of composition and structure of mathematical and software support for solving the problems of analysis and synthesis of technologies and comprehensive plans for ensuring quantum resilience of national DPiBE;

• development of methods based on the integration of methods for ensuring verified security and the development of Agile and Waterfal approaches for designing quantum-resilience national DPiBE (Q-VSAWD);

• development based on the addition and development of methods of verified security and methodology of continuous development of digital platforms, taking into account security requirements, methodology for creating quantum-resilience national DPiBE (Q-DevSecOps);

• development of a software architecture for solving the problems of synthesizing quantum-resilience national DPiBE under of a new quantum security threat using methods of verified security and a methodology for continuous development taking into account security requirements;

• creation and debugging of a prototype of a software package for solving the problems of synthesizing quantum-resilience national DPiBE under of a new quantum security threat using methods of verified security and a methodology for continuous development taking into account security requirements.

This is not an exhaustive list of planned research aimed at implementing the proposed Concept.

Conclusion

The results obtained in the field of quantum informatics clearly demonstrate the high technological potential of quantum technologies. A cryptanalytically relevant or significant quantum computer can threaten the operating of various systems, including the functioning of national DPiBE in the Russian Federation.

The DPiBE of the Russian Federation do not have the required resilience of target operating under of attacks by intruders using quantum computers.

This article proposes and formulates the main provisions of the relevant Concept for ensuring the resilience of national DPiBE under a new quantum security threat. After discussion, coordination and approval, the Concept should become an integral part of the Information Security Concept of the Russian Federation.

In developing the Concept, were summarized, systematized and comprehensively rethought the results obtained in the works well-known works of Russian scientists on quantum information technologies and the results obtained in the works of the authors of this article and other members of the group "Technologies for countering previously unknown quantum cyber threats" of the Scientific Center for Information Technology and Artificial Intelligence of the Sirius University of Science and Technology.

This article also reviewed the main directions of further research of the above-mentioned group, aimed at implementing the proposed Concept.

REFERENCES

1. **Ishchukova E.A., Panasenko S.P., Romanenko K.S., Salmanov V.D.** *Kriptograficheskie osnovy blokchein-tekhnologii* [*Cryptographic foundations of blockchain technologies*]. Moscow: Izdatel'stvo «DMK Press», 2022. 301 p.

2. **Petrenko A.S.** *Kvantovo-ustoichivyi blokchein. Kak obespechit' bezopasnost' blokchein-ekosistem i platform v usloviiakh atak s ispol'zovaniem kvantovogo komp'iutera* [*Quantum-resilience blockchain: How to ensure the security of blockchain ecosystems and platforms in the face of attacks using a quantum computer*]. St. Petersburg: Piter, 2023. 320 p.

3. **Zaborovsky V.S., Lei Zhang, Skiba V.Yu., Strekalov S.V.** Digital information and logistic platform for operational management of foreign trade activities of high-tech product suppliers. *St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunications and Control Systems*, 2018, Vol. 11, No. 4, Pp. 7–20. DOI: 10.18721/JCSTCS.11401

4. **Skiba V.Yu., Petrenko S.A., Murzina A.A., Popova K.R.** New types of threats and assessment of quantum stability of information systems in the field of foreign trade activity. *Computing, Telecommunications and Control*, 2024, Vol. 17, No. 4, Pp. 16–34. DOI: 10.18721/JCSTCS.17402

5. **Petrenko S.A., Petrenko A.S., Ozhiganova M.I.** Concept of ensuring the cyber resilience of the Bank of Russia digital ruble platform in the face of growing security threats. *Zaŝita informacii. Inside*, 2024, Vol. 119, No. 5, Pp. 6–13.

6. **Terekhov A.I.** On the Development of the Scientific Base of Quantum Technologies. *Economics of Science*, 2022, Vol. 8, No. 1, Pp. 58–72. DOI: 10.22394/2410-132X-2022-8-1-58-72

7. **Terekhov A.I.** Bibliometric Analysis of Academic Literature on Quantum Information Processing. *Photonics*, 2024, Vol. 18, No. 4, Pp. 296–312. DOI: 10.22184/1993-7296.FRos.2024.18.4.296.312

8. **Skiba V.Yu., Petrenko S.A., Murzina A.A., Popova K.R.** Evaluation of quantum stability of information systems of customs authorities of the Russian Federation in present-day conditions. *Vestnic of Russian Customs Academy*, 2024, Vol. 69, No. 4, Pp. 32–45.

9. **Stupin D.D., Petrenko A.S., Petrenko S.A.** Razvitie tekhnologii kvantovykh vychislenii i sviazannye s nim ugrozy dlia kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii [Development of quantum

computing technologies and associated threats to the critical information infrastructure of the Russian Federation]. *XVI Vserossiiskaia Mul'tikonferentsiia po Problemam Upravleniia* (*MKPU-2023*) [*XVI All-Russian Multi-Conference on Management Problems* (*MCMP-2023*)], 2023, Pp. 168–172.

10. **Kazarin O.V., Skiba V.Yu., Sharyapov R.A.** Novye raznovidnosti ugroz mezhdunarodnoi informatsionnoi bezopasnosti [New types of threats to international information security]. *RSUH/RGGU BULLETIN "Information Science. Information Security. Mathematics" Series*, 2016, Vol. 3, No. 1, Pp. 54–72.

11. **Konyavsky V.A., Ross G.V., Sychev A.M., Skiba V.U.** Information protection in systems of critical information infrastructures. *Journal of the Balkan Tribological Association*, 2021, Vol. 27, No. 4, Pp. 479–496.

12. **Skiba V.Yu., Turgiev E.Z., Lisov D.N., Salokina (Polyakova) N.A., Sergeev V.S.** Proaktivnaia bezopasnost' kvantovykh AIS [Proactive Security of Quantum Automated Information Systems]. *VIII International Conference "The 2024 Symposium on Cybersecurity of the Digital Economy – CDE'24"*, 2025, Pp. 71–77.

13. **Petrenko S.A., Petrenko A.S.** O protivodeistvii ranee neizvestnym kvantovym kiberugrozam [On countering previously unknown quantum cyber threats]. *VII International Conference "The 2023 Symposium on Cybersecurity of the Digital Economy – CDE'23"*, 2024, Pp. 13–23.

14. **Shor P.W.** Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 1997, Vol. 26, No. 5, Pp. 1484–1509. DOI: 10.1137/S0097539795293172

15. **Shor P.W.** Algorithms for quantum computation: discrete logarithms and factoring. Proceedings *35th Annual Symposium on Foundations of Computer Science*, 1994, Pp. 124–134. DOI: 10.1109/SFCS.1994.365700

16. **Simon D.R.** On the power of quantum computation. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, Pp. 116–123. DOI: 10.1109/SFCS.1994.365701

17. **Holevo A.S.** *Vvedenie v kvantovuiu teoriiu informatsii* [*Introduction to Quantum Information Theory*]. Moscow: MTsNMO, 2002. 128 p.

18. **Holevo A.S.** *Veroiatnostnye i statisticheskie aspekty kvantovoi teorii* [*Probabilistic and statistical aspects of quantum theory*]. Moscow: MTsNMO; NMU, 2020. 364 p.

19. **Bogdanov Y.I., Valiev K.A., Kokin A.A.** Quantum computers: achievements, implementation difficulties, and prospects. *Microelectronics*, 2011, Vol. 40, No. 4, Pp. 243–255. DOI: 10.1134/S1063739711040032

20. **Nielsen M.A., Chang I.L.** *Quantum Computation and Quantum Information: 10th Anniversary ed*. Cambridge: Cambridge University Press, 2011. 702 p.

21. **Bennett C.H., Shor P.W.** Quantum information theory. *IEEE Transactions on Information Theory*, 1998, Vol. 44, No. 6, Pp. 2724–2742. DOI: 10.1109/18.720553

22. **Arute F., Arya K., Babbush R. et al.** Quantum supremacy using a programmable superconducting processor. *Nature*, 2019, Vol. 574, Pp. 505–510. DOI: 10.1038/s41586-019-1666-5

23. **Petrenko S.A., Petrenko A.S., Kostyukov A.D.** Countermeasures technologies previously unknown quantum cyber threats. *Zaŝita informacii. Inside*, 2024, Vol. 118, No. 4, Pp. 66–76.

24. **Petrenko A.S., Petrenko S.A.** Quantum resilience estimation method blockchain. *Cybersecurity Issues*, 2022, Vol. 49, No. 3, Pp. 2–22. DOI: 10.21681/2311-3456-2022-3-2-22

25. **Mosca M.** Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 2018, Vol. 16, No. 5, Pp. 38–41. DOI: 10.1109/MSP.2018.3761723

26. **Skiba V.Yu.** *Ob"ektno-funktsional'naia verifikatsiia informatsionnoi bezopasnosti raspredelennykh avtomatizirovannykh informatsionnykh sistem tamozhennykh organov. Diss. doktora tekhn. nauk* [*Object-functional verification of information security of distributed automated information systems of customs authorities. Doctor of Technical Sciences diss.*]. St. Petersburg, 2009. 365 p.

27. **Moldovyan N.A., Petrenko A.S.** Algebraic signature algorithms with two hidden groups. *Cybersecurity Issues*, 2024, Vol. 64, No. 6, Pp. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107

28. **Vysotskaya V.V., Chizhov I.V.** The security of the code-based signature scheme based on the Stern identification protocol. *Applied Discrete Mathematics*, 2022, Vol. 57, Pp. 67–90. DOI: 10.17223/20710410/57/5

29. **Vasyutina A.P., Klyucharev P.G.** Optimization of a post-quantum cryptographic protocol based on isogeny of supersingular elliptic curves. *Bezopasnye Informatsionnye Tekhnologii* [*Secure Information Technologies*], 2023, Pp. 40–43.

30. **Wang R., Dubrova E.** A shared key recovery attack on a masked implementation of CRYSTALS-kyber's encapsulation algorithm. In: *Foundations and Practice of Security. FPS 2023* (eds. M. Mosbah, F. Sèdes, N. Tawbi, T. Ahmed, N. Boulahia-Cuppens, J. Garcia-Alfaro), 2024, Vol. 14551, Pp. 424–439. DOI: 10.1007/978-3-031-57537-2_26

31. **Gromova E.A., Petrenko S.A.** Quantum law: The beginning. *Journal of Digital Technologies and Law*, 2023, Vol. 1, No. 1, Pp. 62–88. DOI: 10.21202/jdtl.2023.3

32. **Gnidko K.O., Sadreev K.R., Lisov D.N.** Kontseptsiia povysheniia ustoichivosti avtomatizirovannoi sistemy k novym ugrozam tipa otkaz v obsluzhivanii cheloveka [The concept of increasing the resilience of an automated system to new threats such as denial of human service]. *VII International Conference "The 2023 Symposium on Cybersecurity of the Digital Economy – CDE'23"*, 2024, Pp. 71–74.

33. **Petrenko S.A., Balyabin A.A.** A model of quantum threats to information security for national blockchain ecosystems and platforms. *Cybersecurity Issues*, 2025, Vol. 65, No. 1, Pp. 7–17. DOI: 10.21681/2311-3456-2025-1-7-17

34. **Saha B., Hasan M.M., Anjum N., Tahora S., Siddika A., Shahriar H.** Protecting the decentralized future: An exploration of common blockchain attacks and their countermeasures. *arXiv:2306.11884*, 2023. DOI: 10.48550/arXiv.2306.11884

35. **Guru A., Mohanta B.K., Mohapatra H., Al-Turjman F., Altrjman C., Yadav A.** A survey on consensus protocols and attacks on blockchain technology. *Applied Sciences*, 2023, Vol. 13, No 4, Art. no. 2604. DOI: 10.3390/app13042604

INFORMATION ABOUT AUTHORS / СВЕДЕНИЯ ОБ АВТОРАХ

Skiba Vladimir Yu.
Скиба Владимир Юрьевич
E-mail: vskiba69@mail.ru
ORCID: https://orcid.org/0000-0002-9805-7800

Petrenko Sergei A.
Петренко Сергей Анатольевич
E-mail: petrenko.sa@talantiuspeh.ru
ORCID: https://orcid.org/0000-0003-0644-1731

Gnidko Konstantin O.
Гнидко Константин Олегович
E-mail: gnidko.ko@talantiuspeh.ru
ORCID: https://orcid.org/0000-0002-8605-8865

Petrenko Alexei S.
Петренко Алексей Сергеевич
E-mail: a.petrenko1999@rambler.ru
ORCID: https://orcid.org/0000-0002-9954-4643

Submitted: 20.03.2025; Approved: 12.05.2025; Accepted: 30.05.2025.
Поступила: 20.03.2025; Одобрена: 12.05.2025; Принята: 30.05.2025.