

EMERGING TECHNOLOGIES AND LAW

Article



DOI: 10.17803/2713-0533.2025.4.34.781-800

Development of Legal and Normative-Technical Regulation of Quantum Communications

Alexey V. Minbaleev,¹ Kirill S. Evsikov,^{1, 2} Sergey V. Solovkin¹

¹ *Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation*

² *Tula State University, Tula, Russian Federation*



Corresponding Author — Alexey V. Minbaleev

© A.V. Minbaleev, K.S. Evsikov, S.V. Solovkin, 2025

Abstract: In 2023, the Russian Federation adopted the Concept for the Regulation of the Quantum Communications Industry until 2030. The authors of this article participated in its development. The document emphasizes the necessity of improving both legal and normative-technical regulatory frameworks for activities in this field. The development of an effective legal regulatory system for the quantum communications industry should be preceded by the establishment of a coherent system of technical regulation specific to the quantum sector. From a legal standpoint, key directions for the potential development of the quantum communications industry have been identified. To a large extent, further progress in this area will depend on the determination of a number of technological development trajectories within the sector. The study shows that the system of domestic standards in quantum communications is contradictory and mutually exclusive. Although several standards have been adopted in recent years, their coverage demonstrates the lack of a coordinated standardization plan to meet the priority needs of the industry. The standards for the quantum internet

of things adopted in 2023 have not yet found their end users, and the backbone quantum communication lines created and functioning in our country remain without relevant standards. The analysis of foreign experience shows similar problems in other countries and a lack of unambiguous recommendations from international standardization bodies. This has made it possible to justify the need to adopt a roadmap for the standardization of quantum communications and additional domestic standards for quantum communication trunk lines. The article highlights the importance of the participation of domestic experts in the work of international standardization bodies on developing technical documents in the quantum communications field.

Keywords: quantum technologies; quantum communications; quantum cryptography; post-quantum cryptography; quantum networking; quantum key distribution; quantum law; regulatory framework for the quantum communications sector; standardization of quantum communications

Acknowledgments: The research was funded by the Russian Science Foundation (project No. 24-18-00950 “Problems and Prospects of Regulation of Quantum Communications in a Data Economy”).

Cite as: Minbaleev, A.V., Evsikov, K.S. and Solovkin, S.V., (2025). Development of Legal and Normative-Technical Regulation of Quantum Communications. *Kutafin Law Review*, 12(4), pp. 781–800, doi: 10.17803/2713-0533.2025.4.34.781-800

Contents

I. Introduction	782
II. General Theoretical Issues of Legal Regulation and Normative-Technical Regulation of Quantum Communications	785
III. Legal Regulation of Quantum Communications	788
IV. Normative-Technical Regulation of Quantum Communications	793
V. Conclusion	795
References	798

I. Introduction

In 2023, the Government of the Russian Federation approved the Concept for the Regulation of the Quantum Communications Industry in the Russian Federation until 2030 (Order No. 1856-r dated

11 July 2023; hereinafter referred to as the “Concept”). A roadmap for its implementation has been developed. It includes measures for drafting and coordinating over 50 regulatory projects, including the establishment of state standards.

The authors of this article were involved in the development of the draft Concept and contributed to establishing the theoretical and legal foundation for creating an effective legal framework for the emerging technology. Some of the conceptual approaches were previously published by the authors and are accessible to readers; however, some of these approaches have not yet been presented to the wider public (Minbaleev et al., 2024, pp. 13–52; Polyakova et al. 2022, pp. 106–111). As a result, misunderstandings in legal interpretation and law enforcement have begun to emerge, which may undermine the effectiveness of legal mechanisms aimed at fostering the development of the quantum communications sector. To counter this trend, the authors conduct regular analysis of regulatory practices in Russia and abroad, enabling them to provide recommendations to regulatory bodies for improving current approaches.

This article is devoted to the analysis of approaches to the normative-technical regulation of quantum communications that is currently being implemented at the national level in many countries, as well as at the international level through several international organizations. This work has already begun in Russia as well; to date, several methodological recommendations from the technical committees,¹ as well as several preliminary national standards, have been adopted. It is important to note that national legislation permits the classification of data protection standards as restricted-access information that is not published or made available to the general public. This imposes limitations on research in this field, as well as on the publication of its results. Such technical requirements cannot be taken into account during the publicly available research process, acknowledged as existing requirements, or disclosed. This article fully complies with this restriction, and the analysis is

¹ First of all, the Technical Committee of the Federal Agency for Technical Regulation and Metrology (Rosstandart) 194 “Cyber-physical systems” (TC 194) and Technical Committee of the Federal Agency for Technical Regulation and Metrology (Rosstandart) 26 “Cryptographic Protection of Information” (TC 26).

conducted exclusively on the basis of publicly accessible standards in the field of quantum communications.

Regarding the use of classified standards in the field of quantum communications that are being developed not only in the Russian Federation but also in other countries, it should be noted that the very existence of restricted-access standards serves to mitigate certain risks associated with large-scale attacks on cryptographic data protection systems. However, in the context of an emerging quantum communications market, such standards do not allow consumers to form an informed opinion about the quality of the equipment. In practice, quantum cryptographic devices become a “black box” standardized by an authorized body according to undisclosed criteria for end users. Under these conditions, a fundamental issue arises regarding the assessment of the quality of equipment provided by different manufacturers. If the operational schemes of two types of equipment are not disclosed, yet both are certified for use in the field of data protection, then, from the perspective of rational economic behavior, they are perceived as functionally equivalent. Consequently, consumers are inclined to choose the least expensive option.

This pitfall becomes particularly acute for organizations procuring equipment through competitive tenders, where price becomes the primary criterion in selecting a supplier. As a result, a legal framework is inadvertently created that undermines the manufacturer’s incentive to improve equipment quality. In the long term, this may lead to a decrease in investments in research and development. Therefore, we recommend embedding compensatory mechanisms into the legal framework governing the cryptographic market in general, and the quantum communications market in particular.

To prevent similar issues in the field of technical regulation of quantum communications, we have conducted an analysis of existing domestic and international standards. This analysis has enabled us to identify several key challenges and propose measures for their proactive mitigation.

II. General Theoretical Issues of Legal Regulation and Normative-Technical Regulation of Quantum Communications

In this article, we proceed from the actual social relations currently existing in the field of quantum communications that define several types of the technological usage: for the transmission of various types of information and for the transmission of information used for generating cryptographic keys. Both options have significant commercial potential, but the global market is effectively developing only for goods, works, and services related to the transmission of encryption keys within quantum communications. This necessitates two actions on the part of the State:

- to establish an effective system of legal and technical regulation for quantum communications as a type of data protection technology,
- to ensure, within the legal and technical regulatory framework for quantum communications, the possibility of applying certain rules to govern the transmission of quantum information unrelated to cryptography.

This can be achieved through the creation of a legal regime that establishes general rules for the transmission of quantum information, as well as the rights and obligations of parties in social relations when encryption keys are transmitted via quantum communication channels. It is important to recognize that quantum communication is a unified technology that has simultaneously been subject to legal regulation under both telecommunications law and cryptography law. Consequently, quantum communication equipment qualifies as both telecommunications equipment and cryptographic equipment, thereby requiring compliance with the legal frameworks governing both telecommunications and cryptography. This constitutes a hybrid legal regime.

In Russian law, the legal regime governing quantum communications is constructed as a harmonious combination of rules regulating the rights and obligations of legal subjects in the processes of quantum networking and quantum cryptography. It is important to note that this approach has been agreed upon by the working groups and incorporated into official documents, including the Concept. The purpose of this

classification is to extract the portion of quantum communications that we designate as quantum networking from the realm of non-public legal and technical regulation. This allows for the formation of an open system of legal norms and technical standards for quantum communications equipment without violating the overall legal framework established for cryptography in the Russian Federation.

However, during the implementation of the Concept, an additional issue arose that requires systematization within the framework of legal and technical regulation. The institution of quantum cryptography that received a significant impetus due to preparations for the Q-Day (the “Q-Day” refers to the moment when quantum computers can break today’s public-key cryptography) was mistakenly interpreted in domestic law. This is primarily related to the use of terminology by the professional community that varies across different countries, as well as the absence of a prominent international classification. In response, in 2024, we proposed a classification system for types of cryptography resistant to quantum computing as part of the development of a legal regulatory framework. This classification includes quantum cryptography resistant to quantum computing, classical cryptography resistant to quantum computing, and new cryptographic algorithms resistant to quantum computing.

The classification we have proposed clearly establishes the following fundamental principles that should be incorporated into the Concept for preparation for the Q-Day:

- quantum computing will render a significant number of encryption methods currently in use ineffective;
- cryptographic evolution will occur globally, involving a transition to encryption methods resistant to quantum computing;
- the transition to new encryption algorithms and new types of quantum cryptography carries significant risks associated with misjudgments regarding the capabilities of quantum computers and modern quantum decryption algorithms.

From this, a basic sequence can be derived for government authorities to follow when transitioning to quantum-resistant cryptography:

- identifying encryption methods that are potentially resistant to quantum computing,

- identifying encryption methods that are reliably not resistant to quantum computing,
- transitioning to classical cryptography resistant to quantum computing and quantum cryptography resistant to quantum computing in all cases where it is technically and economically feasible,
- adopting new cryptographic algorithms resistant to quantum computing based on existing research findings, with the mandatory implementation of cryptographic agility technologies.²

An alternative approach to preparing for the Q-Day may lead to increased costs in ensuring information security. In this context, we refer to the expenses companies currently incur when replacing cryptographic algorithms, as well as the additional costs they may incur for subsequent replacements of cryptographic equipment if critical vulnerabilities in new quantum-resistant encryption algorithms are discovered.

In this regard, there are only two conservative strategies:

- transitioning to classical cryptographic methods resistant to quantum computing,
- transitioning to quantum key distribution.

It is important to remember that quantum key distribution is a component of classical cryptography based on symmetric encryption. Currently, within this technology, the cryptographic key is transmitted by a “special courier” on a physical medium. As is evident from this scheme, the transmission of the cryptographic key is currently not vulnerable to decryption by a quantum computer. Therefore, in our view, it is a conceptual error to include, in the official documents of certain public authorities, the transition to quantum key distribution as a method of preparing for the Q-Day.

Quantum key distribution should be regarded as an element of digital transformation. Functions previously performed manually, such as generating and transmitting encryption keys from one point to another, will now occur automatically. As with other cases of digital transformation, this will increase operational speed and eliminate the risk of accidental or intentional human error. It is widely recognized

² By cryptographic agility, we mean the capability of software and hardware to transition to a new encryption algorithm with minimal economic and technological losses, without the need for a complete replacement of software and equipment.

that a significant number of information security breaches within companies result from the behavior of trusted personnel. Thus, the use of frequently and randomly changing quantum keys, transmitted without human involvement, not only relieves personnel of the key delivery task but also significantly enhances the level of information security (Minbaleev and Evsikov, 2023; Reutov and Tayduganov, 2022, pp. 66–67).

Undoubtedly, such digital transformation has different value for companies. Therefore, the primary stakeholders interested in implementing quantum key distribution technologies should be the following actors:

- legal entities managing a significant number of high-risk sources, including mechanisms operated remotely or driven by artificial intelligence technologies (for example, railway companies, airlines, automotive transport companies, etc.),
- legal entities managing substantial volumes of confidential information received from various sources, such as data centers,
- legal entities managing critical infrastructure facilities.

It appears appropriate to define the list of these entities at the regulatory level based on several factors. Quantum communications constitute a costly technology that requires the establishment of infrastructure. The most effective existing model for building quantum communication networks today is a scheme in which backbone quantum communication lines are connected to a metropolitan line arranged in a star topology. For the economically justified allocation of resources during infrastructure development, it is necessary to identify priority users who will be granted access to the backbone quantum communication lines.

III. Legal Regulation of Quantum Communications

The Concept defines nine sector-wide and five sector-specific regulatory directions for the quantum communications industry. The sector-wide directions include the following:

- development and clarification of terms and definitions for the quantum communications industry,

-
- advancement of legal mechanisms for integrating quantum communications into existing communication networks,
 - advancement of legal mechanisms for the use of quantum communications in information security,
 - legal liability within the quantum communications industry,
 - development of regulatory legal acts pertaining to the quantum communications industry at the international level,
 - improvement of the system of technical regulation and conformity assessment in the quantum communications industry,
 - provision of support for domestic manufacturers in the quantum communications industry,
 - ensuring the development of the quantum communications industry in the face of hostile actions against the Russian Federation, Russian companies, and citizens,
 - other regulatory directions within the quantum communications industry.

The sector-specific directions identified by the Concept include the following:

- legislation of the Russian Federation on state (municipal) administration,
- legislation of the Russian Federation on transport security,
- legislation of the Russian Federation in the field of industrial safety,
- legislation of the Russian Federation on space activities,
- other sector-specific directions for improving the application of quantum communications technologies.

The implementation of these directions involves the development and adoption of more than 50 regulatory legal acts. Below, we review the main ones currently under development.

When providing access to quantum communications for a wide range of users, a regulatory issue arises concerning the relationship between the service provider and the consumer. To regulate these relations, it is permissible either to conclude a contract or to establish service provision rules issued by a governmental authority. It appears that the choice between these approaches should be based on an assessment of infrastructure investments. If services are provided via

a quantum communication network established using funds from a commercial company, the State should not interfere in its commercial activities by imposing binding rules on legal entities. However, when infrastructure development is fully or partially financed by budgetary funds, it is advisable to define state rules for the provision of quantum communication services. The same approach should apply if private networks are connected to state backbone quantum communication lines. In this context, the authors of this article have developed a draft of the Rules for the Provision of Quantum Communication Services, which is proposed for adoption at the level of Russian Railways, the operator of the most extensive quantum communication network. It is deemed appropriate that after testing and connecting urban quantum communication networks to the company's network, these rules should be adopted at the level of the Russian Government. Currently, several service provision rules exist in the telecommunications sector. By 2030, the adoption of the Rules for the Provision of Quantum Communication Services is planned.

Measures to support quantum communications equipment manufacturers should be taken. The authors have prepared a draft amendment to the existing product classifiers by type of economic activity (OK (All-Russian Classifier) 034-2014, KPES (Classification of European Union Products) 2008), in force at the federal level since 1 January 2024, pursuant to Rosstandart Order No. 1477-st dated 27 November 2023.

This amendment has enabled changes to current procurement legislation that is based on this classifier. The next step involves amending procurement legislation applicable to public authorities to limit the purchase of these types of products from foreign manufacturers. To this end, a draft amendment to regulatory legal acts has been developed to establish a mechanism for assessing equipment based on whether it is produced within the territory of the Russian Federation or not. It is considered that domestic quantum communications equipment should contain domestically sourced components. This approach, in addition to ensuring technological sovereignty, is expected to secure a market for domestic equipment, thereby serving as a form of support for domestic manufacturers.

In the Russian Federation, several special economic zones and technology parks conducting research in the field of quantum communications have been established. For example, by Decree of the Government of the Russian Federation No. 2133 dated 30 November 2021, the Innovative Scientific and Technological Center “Quantum Valley” was created. Many participants in the quantum communications sector have registered in these zones, enabling them to receive tax incentives and other forms of government support.

Measures to support research in the field of quantum communications have to be taken. In this area, the List of Directives No. Pr-1734 dated 3 September 2023, approved by the President of the Russian Federation, was adopted. It stipulates that the Government of the Russian Federation must ensure the approval of a national project for the development of the data economy until 2030 that includes, among other things, measures for data security using quantum encryption technology. To this end, the Government is required to provide tools for comprehensive support for quantum communications development that will, *inter alia*, ensure the uninterrupted operation of research teams and laboratories in the field. Additionally, according to the List of Directives, the Government of the Russian Federation should consider the following issues:

- simplifying the procedure for accessing state support funds for scientific research conducted under the guidance of leading scientists in Russian higher education institutions, research organizations, and state scientific centers of the Russian Federation, as well as improving control over the expenditure of these funds;

- creating conditions for attracting domestic and foreign scientists and qualified specialists in quantum technologies, including the development of quantum sensors, quantum computing, and communications (hereinafter referred to as “quantum technologies”), to the Russian Federation, including easing visa procedures, obtaining residence permits and Russian citizenship, streamlining the processing of documents necessary for migration registration and employment authorization, and developing mechanisms for individual material support and social and household arrangements for such persons and their family members;

- establishing a university focused on quantum technologies to implement educational programs on advanced developments in this area, including programs engaging schoolchildren in the educational process;

- expanding cooperation in quantum technologies with countries in the BRICS intergovernmental association (Brazil, Russia, India, China, South Africa), including joint funding of projects in this field;

- increasing opportunities for exchanging up-to-date scientific information on future technologies, including quantum technologies, by creating international scientific journals and organizing conferences;

- instituting awards for outstanding scientific discoveries and achievements in future technologies, including quantum technologies, as well as scholarships for young scientists in the field of quantum technologies.

The National Project “Data Economy and Digital Transformation of the State,” for the period up to 2030, is a comprehensive document that includes support measures for various technologies, including quantum technologies. Additionally, in the field of quantum communications support, Presidential Decree No. 529 dated 18 June 2024, “On the Approval of Priority Directions for Scientific and Technological Development and the List of Key Science-Intensive Technologies,” is currently in force. This document approves priority directions for scientific and technological development and enumerates key science-intensive technologies. Among others, it includes the following item: “12. Technologies for Secure Quantum Data Transmission Systems.” This document is crucial for the research sector, as it defines areas eligible for grant funding from the Russian Federation’s budgets.

One should also mention other directions of legal regulation in the quantum communications industry. On 3 September 2023, the President of the Russian Federation approved the List of Directives (Pr-1734) following a meeting with scientists and the plenary session of the Future Technologies Forum. Among other provisions, the document highlights the need to increase the maximum amount of grants provided by the Government of the Russian Federation for scientific research projects headed by leading foreign scientists, and conducted in Russian higher

education institutions, research organizations, and state scientific centers, to 250 million rubles.

The Russian Ministry of Labor has approved a number of professional standards for specialists in the field of quantum communications. Among these, the Ministry's Orders have approved professional standards, including "Specialist in Research and Development in Quantum Communications," "Specialist in Installation and Technical Operation of Quantum Networks," and "Specialist in the Development of Manufacturing Technology for Quantum Electronics and Photonics Devices."

It is important to note that the further development of an effective legal and regulatory system for the quantum communications industry should be preceded by the establishment of a normative-technical regulatory system for the quantum domain. From a legal perspective, key vectors for the potential development of the quantum communications industry have been identified. To a significant extent, further steps in this direction will depend on the definition of several technological development trajectories within this industry.

IV. Normative-Technical Regulation of Quantum Communications

According to Section 1 of the Concept, the initial stage of establishing a regulatory framework for quantum communications requires amending the normative-technical base to incorporate terms already used in strategic planning documents, as well as to define their interrelationships and correlations. Section 6 of the Concept specifies that technical regulation of the quantum communications industry should be based on national standards that define requirements in the following spheres: quantum communication networks, equipment, software, the application of quantum communication technologies in existing communication lines, the testing of quantum communication networks, equipment, and software.

To maintain a high level of information security and protect the quantum communication market, a certification system for equipment, including individual components, is proposed (Dobrobaba, 2024,

pp. 110–112; Nikolskaya, 2024; Ruzhitskaya et al., 2021, pp. 840–845). To harmonize certification requirements and reduce unnecessary administrative barriers, it is essential to implement unified requirements that eliminate the need for manufacturers to obtain multiple certifications for a single piece of equipment from different state bodies or authorized organizations. For the reliability, accuracy, security, and interoperability of quantum communication solutions, it is necessary to standardize normative-technical requirements in this area, considering existing international standards, the experience of other countries, and the current development level of domestic technologies. Furthermore, effective regulatory oversight of cryptographic information security systems in the banking sector requires the participation of the Central Bank of the Russian Federation.

At the time of this writing, the government has not fully achieved any of these objectives, except for the development of a terminology system. It cannot be claimed that the government has completely neglected the standardization of quantum communications. Currently, the following publicly accessible technical documents are in effect:

- Methodological recommendations of the Technical Committee of the Federal Agency for Technical Regulation and Metrology (Rosstandart) 26 “Cryptographic Protection of Information” (TC 26),
- Preliminary National Standards in Quantum Communications issued by the Federal Agency for Technical Regulation and Metrology,
- Preliminary National Standards in the Field of Quantum Internet issued by the Federal Agency for Technical Regulation and Metrology.

The analysis of these standards suggests that all of them are first-generation technical documents designed for a short-term period, after which decisions will be made regarding their approval or modification. Although this approach to standardization is widely accepted, it carries risks for economic entities that invest significant resources in developing the national quantum communications infrastructure. In Russia at present, such entities include two key stakeholders:

- Russian Railways, which has already built and is using a backbone quantum communications network (Ivanov, 2021),
- a consortium of domestic universities that has established an inter-university quantum communication network (Ovsyannikov and Shabanov, 2023).

These networks interact with each other, yet both entities have already invested considerable resources in developing the network architecture and purchasing equipment. If the aforementioned preliminary national standards are amended, there is a risk that the operation of these networks could become difficult or even impossible. Such an outcome must be avoided. It is crucial to prioritize the development of long-term technical acts in quantum communications. This raises the question of the priority areas for standardization in quantum communications. From a technological resource perspective, the most significant technology would be the transmission of quantum keys via satellites (Duplinsky et al., 2023, pp. 104–105). However, the satellite component is currently absent from Russia's quantum communication networks that makes it unfeasible to prioritize this sector for the standardization of quantum technologies.

V. Conclusion

Therefore, we conclude that the initial regulatory steps for quantum communications should comprise the following fields of activities:

- defining the system of legal regimes applicable to quantum communications,
- establishing an internal classification of quantum communication components,
- determining the objectives for the deployment and use of quantum communications,
- identifying priority entities to be granted access to quantum communication infrastructure.

As part of this study, it has been established that the regulatory framework for the development of quantum communications can be structured through three main approaches.

Development of a framework of official documents issued by executive public authorities, including interpretive legal acts, enforcement acts, and advisory instruments such as methodological guidelines. The main advantages of this approach include the ability to issue official documents promptly and regulatory flexibility that makes it possible to address specific life cases arising in the quantum

communications sector. However, this approach also entails several drawbacks, namely:

- public officials may be reluctant to express a clear position on certain legal enforcement matters, due to concerns that such positions could later be deemed incorrect;

- official interpretive acts lack the status of regulatory legal acts in the sense that they cannot be directly cited in court proceedings. As a result, in the event of a legal dispute, there is a risk that a judicial authority might depart from the position of the executive body and reach a different decision in the specific case.

Amendment of existing regulatory legal acts governing the creation and use of quantum communications. This option is considered the most preferable, as it allows for the development of a regulatory framework tailored to the needs of the industry. However, this approach presents several challenges, including the following problems:

- a complex coordination process for the text of the regulatory legal act that may lead to significant changes to its substance, thereby reducing the effectiveness — or even nullifying — the initial legislative initiative,

- a prolonged approval procedure for draft regulatory legal acts.

Establishment of an experimental legal regime in the field of digital innovation. The authors of this article highlight the possibility of excluding quantum communication lines from the general regulatory framework governing communications, information security, and cryptography. At various conferences, roundtables, and strategic sessions, representatives from the industry and public authorities have expressed support for this regulatory approach. Nevertheless, as of today, no legal entity in the Russian Federation has agreed to act as the initiator of an experimental legal regime in the digital innovation sphere. A likely subjective barrier to this approach is the perception of the technology as one that ensures a higher information security level. Consequently, exempting it from certain general rules in the areas of telecommunications or cryptography may adversely affect consumer perception, potentially fostering distrust in the technology, particularly during its initial deployment stage.

The further development of an effective legal and regulatory system for the quantum communications industry should be preceded by the establishment of a normative and technical regulatory framework for the quantum domain. From a legal perspective, the key directions for the potential development of the quantum communications industry have been outlined. To a significant extent, future steps in this direction will depend on the determination of specific technological development trajectories within the industry.

Russia has developed six preliminary national standards in quantum communications. However, only two remain relevant due to the specific needs of the national quantum communications industry and quantum cryptography sector. The quantum Internet of Things standards adopted in 2023 have not yet found practical application (Minbaleev and Evsikov, 2024), while existing backbone quantum communication lines in Russia continue to operate without applicable standards. A plan is currently underway to establish a strategy for developing quantum communications standards, taking into account the most effective practices worldwide.

The analysis reveals a significant gap between the number of domestic standards and those developed internationally, where many aspects of quantum communications have already been standardized (Chen, 2023; Gromova and Petrenko, 2023; Gulyamov, 2023; Kuleshov, 2023; Naumov and Stankovsky, 2019; van Deventer et al., 2022). However, despite this international lead, notable deficiencies remain in the standardization of the following issues:

- materials used in the development of quantum technologies,
- infrastructure for quantum networks, including network management systems,
- quantum equipment.

Russia has not yet initiated standardization efforts in these areas, which represents a critical gap that could adversely impact the sector. Given the existence of Russia's backbone quantum communication line for Russian Railways and the Inter-University Quantum Communication Network, both of which involved substantial infrastructure investments, the adoption of national or international standards that fail to take into account the technologies and advancements of domestic quantum

equipment manufacturers could harm the industry. Therefore, the authors stress the urgent need to adopt new national standards that will protect both quantum network operators and quantum communication service users. A more strategic approach is required, with priorities aligned to current industry needs rather than speculative future developments. Furthermore, the authors highlight the necessity for the active participation of Russian specialists in the development of international standards for quantum communication networks.

References

Chen, Y., (2023). Quantum Algorithms for Lattice Problems. *Cryptology ePrint Archive*, report No. 555. Available at: <https://eprint.iacr.org/2024/555> [Accessed 14.10.2024].

Duplinsky, A.V., Khmelev, A.V., Merzlinkin, V.E., Pismenyuk, L.V., Bakhshaliev, R.M., Tikhonova, K.A., Nesterov, I.S., Kurochkin, V.L. and Kurochkin, Yu.V., (2023). Scalable Satellite Network for Quantum Key Distribution Based on CubeSats. *Tomsk State University Journal of Control and Computer Science*, 63, pp. 103–110, doi: 10.17223/19988605/63/12. (In Russ.).

Gromova, E.A. and Petrenko, S.A., (2023). Quantum law: The beginning. *Journal of Digital Technologies and Law*, 1(1), pp. 62–88, doi: 10.21202/jdtl.2023.1. (In Russ.).

Gulyamov, S., (2023). Quantum Law: Navigating the Legal Challenges and Opportunities in the Age of Quantum Technologies. *Uzbek Journal of Law and Digital Policy*. 1(1), pp. 1–11, doi: 10.59022/ujldp.54.

Dobrobaba, M.B., (2024). Ensuring information security as a component of the model of legal regulation of quantum communications. *Courier of Kutafin Moscow State Law University (MSAL)*, 10, pp. 108–116, doi: 10.17803/2311-5998.2024.122.10.108-116. (In Russ.).

Ivanov, A., (2021). Russia Launches Its First Regional Backbone Quantum Network. *Pervaya milya*, 3(95), pp. 22–23, doi: 10.22184/2070-8963.2021.95.3.22.23. (In Russ.).

Kuleshov, D.A., (2023). The global approaches to the regulation of quantum communication. *Digital Law Journal*, 4(4), pp. 54–72, doi: 10.38044/2686-9136-2023-4-4-4.

Minbaleev, A., Zenin, S. and Evsikov, K., (2024). Prospects for Legal Regulation of Quantum Communication. *BRICS Law Journal*, 11(2), pp. 11–54, doi: 10.21684/2412-2343-2024-11-2-11-54.

Minbaleev, A.V. and Evsikov, K.S., (2024). Regulation of Atmospheric Optical Quantum Communication Links. *E3S Web Conf*, 541, VI International Scientific Forum on Computer and Energy Sciences (WFCES 2024), doi: 10.1051/e3sconf/202454102001.

Minbaleev, A.V. and Evsikov, K.S., (2023). Regulation of Quantum Communications in the “Smart City” Information System. *E3S Web Conf*, 419, doi: 10.1051/e3sconf/202341901006.

Naumov, V.B. and Stankovsky, G.V., (2019). Legal aspects of quantum Communications: New Horizons. *Probely v rossijskom zakonodatel'stve*, 4, pp. 235–239. (In Russ.).

Nikolskaya, K.Y., (2024). Cybersecurity and quantum technologies: risks and threats. *Digital technologies and Law*. Kazan: Publishing House “Cognition,” 2024, pp. 30–33. (In Russ.).

Ovsyannikov, A.P. and Shabanov, B.M., (2023). On the Interuniversity Quantum Network Project. *Programmnye produkty i sistemy*, 36(4), pp. 695–702, doi: 10.15827/0236-235X.142.695-702. (In Russ.).

Polyakova, T.A., Minbaleev, A.V. and Naumov, V.B., (2022). Legal Regulation of Quantum Communications in Russia and in the World. *Gosudarstvo i pravo*, 5, pp. 104–114, doi: 10.31857/S102694520019763-0. (In Russ.).

Reutov, A.A. and Tayduganov, A.S., (2022). QKD and Phase Modulator Imperfections. *St. Petersburg Polytechnic University Journal. Physics and Mathematics*, 15(3.2), pp. 65–68, doi: 10.18721/JPM.153.212.

Ruzhitskaya, D.D., Zhluktova, I.V., Petrov, M.A., Zaitsev, K.A., Acheva, P.P., Zunikov, N.A., Shilko, A.V., Aktas, D., Jollinger, F., Trefilov, D.O., Ponosova, A.A., Kamynin, V.A. and Makarov, V.V., (2021). Creation of Vulnerabilities in Quantum Key Distribution Systems Due to Pulsed Laser Attacks. *Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics*, 21(6), pp. 837–847, doi: 10.17586/2226-1494-2021-21-6-837-847. (In Russ.).

van Deventer, O., Spethmann, N., Loeffler, M. et al., (2022). Towards European Standards for Quantum Technologies. *EPJ Quantum Technology*, 9, 33, doi: 10.1140/epjqt/s40507-022-00150-1.

Information about the Authors

Alexey V. Minbaleev, Dr. Sci. (Law), Professor, Head of Information Law and Digital Technologies Department, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

alexmin@bk.ru (Corresponding Author)

ORCID: 0000-0001-5995-1802

Kirill S. Evsikov, Cand. Sci. (Law), Associate Professor, Associate Professor, Department of Information Law and Digital Technologies, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation; Head of the Department of State and Administrative Law, Tula State University, Tula, Russian Federation

aid-ltd@yandex.ru

ORCID: 0000-0002-4593-0063

Sergey V. Solovkin, Cand. Sci. (Law), Lecturer, Department of Information Law and Digital Technologies, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

svsolovkin@msal.ru

ORCID: 0000-0002-3708-1137

Received 07.06.2025

Revised 23.06.2025

Accepted 02.07.2025