http://dx.doi.org/10.18623/rvd.v23.6345

THE EVOLUTION OF LAW CONCEPT OF INFORMATION: FROM PHILOSOPHICAL ABSTRACTION TO QUANTUM INFORMATION AND CRYPTOGRAPHY IN THE CONTEXT OF GROWING CYBER THREATS AND THE TRANSITION TO POST-QUANTUM SECURITY METHOD

A EVOLUÇÃO DO CONCEITO JURÍDICO DE INFORMAÇÃO: DA ABSTRAÇÃO FILOSÓFICA À INFORMAÇÃO QUÂNTICA E À CRIPTOGRAFIA NO CONTEXTO DAS CRESCENTES AMEAÇAS CIBERNÉTICAS E DA TRANSIÇÃO PARA O MÉTODO DE SEGURANÇA PÓS-QUÂNTICA

Article received on: 1/2/2026
Article accepted on: 4/1/2026

Sergey Polyakov*
*Novosibirsk State Technical University, Novosibirsk, Russia
Orcid: https://orcid.org/0000-0003-0159-9484
s.a.polyakov@inbox.ru

Liliya Smeshkova*
*Novosibirsk State Technical University, Novosibirsk, Russia
Orcid: https://orcid.org/0009-0006-8992-5537
l.v.smeshkova@mail.ru

Vyacheslav Lapin**
**HSE University, Moscow, Russia
Orcid: https://orcid.org/0000-0003-1539-1211
lapin78@mail.ru

Anna Solomatina***
***Moscow University of the Ministry of Internal Affairs of Russia named by V.Ya. Kikot, Moscow, Russia
Orcid: https://orcid.org/0009-0009-4965-544X
ansolomatina@mymail.academy

Alexey Konstantinov****
****Russian University of Transport, Moscow, Russia
Orcid: https://orcid.org/0009-0007-6890-9498
a.konstantinov@mymail.academy

Elmir Alimamedov*****
*****Financial University under the Government of the Russian Federation, Moscow, Russia
Orcid: https://orcid.org/0000-0003-2477-3166
alimamedov.e.n@mail.ru

The authors declare that there is no conflict of interest

Abstract
The article examines the significant transformation of the concept of information and its impact on modern security technologies. Until the middle of the 20th century, the concept of information was considered as a philosophical category related to the transfer of knowledge and meaning. With the advent of Claude Shannon's communication theory, information was reinterpreted as a measurable and transferable quantity, which opened up new horizons for the

Resumo
O artigo examina a transformação significativa do conceito de informação e seu impacto nas modernas tecnologias de segurança. Até meados do século XX, o conceito de informação era considerado uma categoria filosófica relacionada à transferência de conhecimento e significado. Com o advento da teoria da comunicação de Claude Shannon, a informação foi reinterpretada como uma quantidade mensurável e transferível, o que abriu novos

development of fields such as coding theory and cybernetics. The introduction of the bit as a unit of information measurement allowed for a more accurate analysis of data transmission processes. Landauer and Bennett's research has shown that information has a physical nature, closely related to energy and entropy. In recent decades, the concept of information has begun to play an important role in quantum theory, which has given rise to such areas as quantum information and quantum cryptography. In the face of increasing cybersecurity threats, quantum cryptography can become a reliable basis for protecting critical information systems. Existing post-quantum algorithms, although they have larger keys, can serve as a substitute for traditional security systems. The development of new standards and the transition to post-quantum security methods are becoming important steps to ensure data security in the near future. Quantum cryptography offers not only adaptation to new challenges, but also a fundamentally new level of security previously inaccessible to classical cryptographic systems, which makes it a key element for data protection in the future. Conclusion. The presented work demonstrates the evolution of the concept of information from a philosophical abstraction to a practical and measurable entity in the field of computer science, physics and cryptography. The article highlights the importance of quantum cryptography as a means of protection against future threats in the field of cybersecurity, offering both a theoretical and practical basis for protecting critical information. Taking into account the further development of quantum information science, its impact on data security and protection will have a significant impact on the formation of future cybersecurity strategies in various industries.

Keywords: Shannon Theory. Entropy. Quantum Entanglement. The Physical Nature of Information. Artificial Intelligence. Big Data Theory.

horizontes para o desenvolvimento de campos como a teoria da codificação e a cibernética. A introdução do bit como uma unidade de medida de informação permitiu uma análise mais precisa dos processos de transmissão de dados. A pesquisa de Landauer e Bennett mostrou que a informação tem uma natureza física, intimamente relacionada à energia e à entropia. Nas últimas décadas, o conceito de informação começou a desempenhar um papel importante na teoria quântica, que deu origem a áreas como informação quântica e criptografia quântica. Diante das crescentes ameaças à segurança cibernética, a criptografia quântica pode se tornar uma base confiável para proteger os sistemas de informações essenciais. Os algoritmos pós-quânticos existentes, embora tenham chaves maiores, podem servir como substitutos dos sistemas de segurança tradicionais. O desenvolvimento de novos padrões e a transição para métodos de segurança pós-quânticos estão se tornando etapas importantes para garantir a segurança dos dados em um futuro próximo. A criptografia quântica oferece não apenas a adaptação a novos desafios, mas também um nível de segurança fundamentalmente novo, antes inacessível aos sistemas criptográficos clássicos, o que a torna um elemento fundamental para a proteção de dados no futuro. Conclusão. O trabalho apresentado demonstra a evolução do conceito de informação de uma abstração filosófica para uma entidade prática e mensurável no campo da ciência da computação, da física e da criptografia. O artigo destaca a importância da criptografia quântica como um meio de proteção contra futuras ameaças no campo da segurança cibernética, oferecendo uma base teórica e prática para a proteção de informações críticas. Levando em conta o desenvolvimento futuro da ciência da informação quântica, seu impacto na segurança e proteção de dados terá um impacto significativo na formação de futuras estratégias de segurança cibernética em vários setores.

Palavras-chave: *Teoria de Shannon. Entropia. Emaranhamento Quântico. A Natureza Física da Informação. Inteligência Artificial. Teoria de Big Data.*

1 INTRODUCTION

For centuries, the concept of information has remained one of the most complex and ambiguous categories at the intersection of philosophy, science and practice. Initially, information was perceived as something intangible, associated with the transfer of knowledge, meanings and their interpretations. Philosophers, starting with Aristotle and ending with modern thinkers, have reflected on its role in understanding the world and shaping human consciousness. However, with the development of science and technology, information has ceased to be an abstract idea, becoming a concrete and measurable category that has become the basis of modern communications, technology, and even physical processes.

The most important stage in understanding information was the work of Claude Shannon, who in the middle of the 20th century laid the foundations of information theory by linking it with entropy and introducing the bit as a unit of measurement. This discovery not only changed the scientific landscape, but also became the starting point for the development of fields such as coding theory, cybernetics, and computer science. Later, the research of Rolf Landauer and Charles Bennett proved that information is not just an abstraction, but a physical phenomenon closely related to energy and entropy.

Today, information occupies a central place in the scientific picture of the world, becoming a key element in a wide variety of fields — from biology and physics to quantum mechanics and artificial intelligence. In the era of digital transformation, information is not just transmitted and stored — it is actively transformed into new knowledge, insights and strategic decisions. However, the rapid development of technologies such as blockchain, quantum computing, and artificial intelligence poses new challenges to society related to data protection, regulation of information processes, and ethical responsibility for decisions made by autonomous systems.

This article examines the evolution of the concept of information, its role in modern science and technology, as well as the prospects for the development of quantum cryptography and other innovative methods of data protection. Special attention is paid to Russian developments in the field of quantum technologies and their importance for ensuring information security in the context of global challenges. The article also analyzes

the legal and ethical aspects of the use of information in the era of digitalization, suggesting ways to adapt legislation to new realities.

2 MATERIALS AND METHODS

The main purpose of the article is to trace the conceptual evolution of information from philosophical roots to quantum cryptography, analyzing its significance for modern cybersecurity and post—quantum transitions.

The authors are tasked with studying the relationship between philosophical theories and technological advances, assessing the vulnerability of classical cryptography to quantum threats, and developing a legal approach to understanding post-quantum cryptographic solutions and their impact on society. It is planned to conduct an interdisciplinary review of the literature on philosophy, physics, computer science, cryptography, information security and law from the perspective of retrospective and comparative research methods. Identification of forecast scenarios and their analysis will allow modeling the consequences of delayed post-quantum implementation of national security risks.

Expert assessment methods will allow a comprehensive study of the evolution of information, contextualizing its philosophical roots in the context of urgent cybersecurity issues and the legal regulation of these processes related to the achievements of quantum physics.

3 RESULTS ANALYSIS

For centuries, the concept of “information” has remained ephemeral and largely philosophical: it has been viewed as something intangible, associated with the transfer of knowledge, meanings and meanings. Philosophers immersed themselves in the analysis of its role in human perception, consciousness and interpretation, which gave the term a subjective and multi-layered character. This approach prevailed until the middle of the 20th century, when Claude Shannon, with his revolutionary work, transformed “information” from a philosophical abstraction into a rigorous and measurable scientific category. His work not only laid the foundations of communication theory, but also

changed the very perception of information, making it a key concept of modern science and technology (Shannon, 1963).

Shannon showed that information and entropy are interrelated and both are related to energy and introduced a unit of information, the “bit”, which allowed us to assess the degree of uncertainty or entropy in transmitted messages. This key innovation allowed us to consider information as a fundamental category along with energy and matter. Claude Shannon's work “Mathematical Theory of Communication” (1948) redefined information as a measure of uncertainty elimination, laying the foundations of coding theory. It became possible to describe the processes of information transmission in technical and physical systems, which created the basis for fields such as coding theory, cybernetics, and computer science.

Seth Lloyd, continuing the development of Shannon's ideas, emphasized the relationship between information and physical systems. According to him, the essence of information lies in the ability of one physical system (for example, numbers, letters, or words) to represent another physical system. This statement strengthens the concept of information, linking it with the material world and emphasizing its universal role in describing nature (Lloyd, 2013).

After Shannon, the concept of information began to be considered not only in the context of communications, but also as an important characteristic of physical systems. The breakthrough was made by the research of Rolf Landauer and Charles Bennett, who proved that information is a physical phenomenon related to entropy. The Landauer principle (“erasing a bit increases the entropy of the system”) was experimentally confirmed in 2012 in the experiments of Eric Lutz's group (University of Aix-Marseille), where the measurement of heat release during data deletion showed compliance with theoretical predictions (Bérut *et al*., 2012). This brought to the fore the concept of the physical nature of information, which is currently the subject of active research.

Today, information occupies a central place in the scientific picture of the world, becoming a key concept in a wide variety of fields of knowledge — from biology to physics and quantum mechanics. In the broadest sense, information is information about the world and the processes taking place in it, which can be perceived and interpreted by both humans and specialized devices. This definition, recorded in authoritative sources, emphasizes the universality and fundamental nature of information as a phenomenon that

underlies our understanding of reality and interaction with it (Ozhegov & Shvedova, 2010, p. 221; Vaulina *et al*., 2014).

In a rapidly changing digital world, information is becoming the basis for innovative transformations, influencing technological and social processes. In the era of artificial intelligence and blockchain, information is not just recorded and transmitted — it is actively transformed into new knowledge and insights, which raises fundamental questions about the nature and role of information in modern systems, as well as about the norms of its regulation.

In Russian legislation, information is understood as: "information (messages, data), regardless of the form of their presentation", covering both digital data and any other form of information, as reflected in paragraph 1 of Article 2 of Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and information protection" (State Duma of the Federal Assembly of the Russian Federation, 2006).

Due to the avalanche-like development of new technologies, including artificial intelligence technologies, a positive example of adapting legislation to the challenges of digitalization of our society is the introduction in 2021 of amendments to the aforementioned Law No. 149-FZ "On Information" regulating the use of artificial intelligence.

It should be noted that this modification is partially borrowed from the concept of the European GDPR (General Data Protection Regulation), in which lawmakers grouped information by levels of criticality, which allows differentiating its protection measures (European Union, 2016.

It seems possible to learn from the positive experience of the United States, similar principles of transparency of data processing are enshrined in the California Consumer Privacy Act (CCPA) (California Legislative Information, 2018), a California law that entered into force on January 1, 2020, aimed at protecting residents' personal information from misuse. The CCPA grants consumers the rights to information about the collection, use, disclosure and sale of their data, the ability to request the deletion of data, refuse to sell it, and guarantees equal treatment and data portability. Companies are required to notify consumers about working with their personal information, and fines are provided for violations: up to $2,500 for unintentional and up to $7,500 for intentional.

With the development of neural networks and machine learning, information is becoming a key resource powering analytical and predictive models. Artificial intelligence (AI) doesn't just process data - it generates a new quality of information, converting it into strategic insights. This raises the question: can information created by an AI system based on processed data be considered new knowledge? What will be the ethical and legal norms governing this knowledge in the future? Who is responsible for the AI's decision or action/inaction?

Legal regulation is also necessary in this context of the use of AI. It is important to decide which place the law should assign to information created by artificial intelligence, and how this relates to the protection of intellectual property, as well as the rights to privacy and confidentiality.

Responsibility for AI solutions remains an urgent and widely discussed issue. This is because AI, especially in high-risk areas such as autonomous transportation, medicine, or finance, is capable of making decisions that can lead to serious consequences, including harm to life, health, or property. One of the most striking examples illustrating this problem was the traffic accident involving a Tesla self-driving car in 2022, which attracted widespread attention from the public and the legal community.

In the case of an accident involving a Tesla self-driving car in 2022 In the United States, the court blamed the manufacturer, Tesla. This decision became an important precedent for the United States, as for the first time in the history of judicial practice, responsibility for an accident involving an autonomous vehicle was assigned to the company rather than the driver, and it became an important example that highlighted the need for further development of legal and ethical standards in the field of AI use, especially from the point of view of autonomous systems where the cost of error can be extremely high.

In terms of blockchain technology, information takes on another dimension: it becomes transparent, immutable, and distributed.

The report of the World Economic Forum (WEF) defined blockchain technology or distributed ledger technology (DLT) as a technological protocol that allows:

1. Ensure transparency and immutability of data through cryptographic encryption and a chain of blocks linked by hash functions.

2. Eliminate the need for centralized intermediaries (banks, notaries, regulators) due to a decentralized architecture.
3. Guarantee security and trust between network participants through consensus algorithms (Proof of Work, Proof of Stake, etc.) (World Economic Forum, 2015).

After analyzing these features of the technology, it is possible to summarize that the blockchain is making changes to traditional concepts of privacy and information protection. Since traditional legal provisions are not always adapted to the dynamics of distributed systems, there is a need to create new rules that take into account promising areas of development of blockchain technologies.

It also requires a revision of regulatory and legal norms related to information processes, such as data management, storage and protection, since traditional data protection tools do not always adequately cope with the new challenges of distributed networks, since the expansion of the concept of information in legal norms should take into account not only current, but also promising areas of development of data application. technologies related to its dynamic nature and use in the era of the present and future development of the digital society.

Nevertheless, the emergence of quantum computers poses an even more significant challenge to cybersecurity. Quantum computers using Shor's algorithm[1] are capable of solving multiplier problems in polynomial time, which makes traditional cryptographic protection methods vulnerable. For example, hacking RSA-2048 by a classical computer will take billions of years, whereas a quantum computer with 4,099 qubits (according to IBM estimates) will be able to complete this task in a matter of hours. This poses a threat to the security of banking transactions, government communications, and even blockchain networks, underscoring the need to rethink and update information security standards in the light of new technological realities (NIST, 2022).

This leads to the need to develop new data protection methods that will be resistant to attacks using quantum computing. In particular, quantum cryptography, based on the principles of quantum mechanics, offers solutions that ensure the absolute security of data transmission.

[1] Shor's algorithm is a quantum algorithm that allows efficient factorization of large numbers, which compromises classical cryptographic systems such as RSA.

Quantum mechanics continues to fundamentally change our view of the nature of reality, offering new opportunities for information processing and transmission. One of the key concepts of this field was the idea of quantum information.

Quantum information is information represented as states of a quantum system, and photons are used to transmit it. The main systems for transmitting quantum information are quantum optical systems.

As noted by E.Ya Kilin (1999),

> a new field of physics — quantum information — arose at the intersection of quantum mechanics, optics, information theory and programming, discrete mathematics, laser physics and spectroscopy and includes issues of quantum computing, quantum computers, quantum teleportation and quantum cryptography, problems of decoherence and spectroscopy of single molecules and impurity centers. Some new results have been reported in this rapidly developing field of research. (p. 507).

Quantum entanglement is a quantum mechanical phenomenon in which the quantum states of two or more objects turn out to be interdependent. For example, it is possible to obtain a pair of photons in an entangled state, and then if, when measuring the spin of the first particle, its helicity turns out to be positive, then the helicity of the second always turns out to be negative, and vice versa (Mironov, 2018).

Quantum entanglement, described in the EPR (Einstein-Podolsky-Rosen) paradox, became the basis for state teleportation technologies. Although Einstein called entanglement a "terrible long-range effect" (specifically emphasizing his criticism), this effect has been confirmed by numerous experiments. Research has demonstrated that entanglement is not an anomaly, but a fundamental physical property that can be used for practical purposes such as quantum communications, encryption, and computing.

One of the most promising areas is quantum cryptography, which provides the highest level of data protection due to the Heisenberg uncertainty principle and the property of quantum entanglement.

The Heisenberg uncertainty principle states that it is impossible to simultaneously accurately measure certain parameters of a particle (for example, its position and momentum) without disturbing its state. In the context of quantum cryptography, this means that any attempt to intercept data will “destroy” the original quantum state and

make changes that will immediately become noticeable to the sender and recipient. This makes the data resistant to imperceptible substitution or theft.

As the researchers note, "at the moment, there are already post-quantum systems that are not inferior in speed and ease of use to classical cryptographic protection systems (for example, RSA)[2]. The only drawback of such systems is the large size of the public key, which can be explained by their cryptographic strength in the post-quantum world. Therefore, it is already worthwhile to study data encryption algorithms and replace classical systems with them" (Kudryashov & Fionov, 2022, p. 114).

For example, quantum cryptography, such as the BB84 protocol, uses the laws of quantum mechanics to protect information. According to the Wikipedia online encyclopedia, BB84 is the first quantum key distribution protocol proposed in 1984 by Charles Bennett and Gilles Brassard, which uses four quantum states of a two-level system to encode information, forming two conjugate bases. Information carriers are 2-level systems called qubits (quantum bits) (Vikipediya, n.d.).

Unlike classical encryption methods, quantum encryption ensures that information interception will be detected, since any interference with a quantum system changes its state, which undoubtedly makes quantum cryptography a potentially more secure alternative to traditional methods. In the context of increasing threats to cybersecurity, such as crime in the field of information and telecommunication technologies (Pushkarev *et al*., 2019a, 2019b, 2020, 2021; Rastoropov *et al*., 2024), espionage, disruption of critical infrastructures quantum cryptography can become a reliable foundation for protecting critical information systems and a key element for data protection in the future.

Advances in the transmission of entangled photons pave the way for the creation of global quantum communication networks that can replace or complement existing information systems. A quantum network will provide an unprecedented level of data security due to the principle that any interference with a quantum system leaves

[2] RSA is an asymmetric cryptosystem used to encrypt and sign messages. RSA got its name from the first letters of the surnames of its founders Rivest, Shamir and Adelman. RSA uses a public and a private key. The public key is used to encrypt the data, and the private key is used to decrypt it. In addition, the private key is used to sign messages, and the public key is used to verify the signature.

unavoidable traces. This property is particularly attractive for areas such as finance, government security, and medical data.

A breakthrough in this field occurred in 2017 thanks to the Chinese Mo-Tzu satellite, the world's first satellite for quantum experiments. During the experiment, a record was set: the transmission of entangled photons between a satellite and two ground stations at a distance of 1,200 kilometers. Communication between Earth and the Chinese Mo-Tzu satellite was secured using quantum key distribution. This was a truly revolutionary achievement for quantum communication and demonstrated the scalability of such technologies. Such a significant distance was previously unattainable, since terrestrial experiments were limited to tens of kilometers due to transmission losses through the atmosphere and fiber-optic cables (Liao *et al*., 2017).

Experiments like the launch of the Mo-Tzu satellite demonstrate that quantum physics is gradually ceasing to be a field of exclusively fundamental science, moving into the field of practical technology. Quantum mechanics and its applications open up perspectives that can change the world as much as classical computers and the Internet once did.

It follows from the above that quantum cryptography is a promising direction in ensuring information security, capable not only of adapting to threats, but also of preventing them at a level previously inaccessible to classical cryptographic systems.:

1. Detection of interception attempts. Any interference or observation of the transmitted quantum particles changes their state. In this way, the sender and recipient can instantly detect an attempt to intercept data.
2. Resistance to quantum computers. Quantum cryptography does not depend on the complexity of mathematical problems based on classical methods, and therefore is resistant to the threats of quantum computing.
3. Absolute security. Unlike classical methods, which are “difficult but possible” to crack, quantum cryptography offers a fundamentally inaccessible communication channel based on physical laws.

1. One of the most obvious applications of quantum cryptography is the financial industry. In the context of global digitalization of banking services, transaction protection is becoming an important task. Modern encryption systems based on

classical algorithms can become very effective, but theoretically vulnerable to the threat of hacking using quantum computers.

As noted above, quantum cryptography, thanks to its principles, allows you to create communication channels where data interception cannot be carried out without detection. Thus, it is possible to ensure that banking operations and financial transactions are protected at a very serious level. In addition, protecting customers' personal data using quantum methods will make it impossible to leak them even in the event of an attack by intruders, ensuring trust in financial institutions.

2. Quantum cryptography will ensure the security of government institutions. The encryption of strategically important information, as well as ensuring the safety of data transmitted between government agencies, is of paramount importance for national security. The interaction between intelligence services, diplomatic missions, and other government agencies requires strong encryption, especially given the growing threats of espionage and cyber attacks.
3. Using quantum cryptography technologies will be useful in the medical field, where patient data such as personal information, medical history, and diagnostic test results require special protection. Any loss of them may entail not only significant reputational damage, but also a threat to the confidentiality and legitimate rights of patients. Clinics and laboratories can use quantum keys to securely exchange diagnostic results or treatment referrals, eliminating the possibility of unauthorized access. In addition, with the development of telemedicine, the use of highly secure communication channels is becoming an integral part of modern healthcare infrastructure.

Research in the field of quantum computing and cryptography is actively underway in Russia. For example, at the National Research Technological University "MISIS" and the Russian Quantum Center (RCC) There are already developments in the field of quantum cryptography, which allows you to protect transmitted data from interception. The developers have introduced a quantum key distribution protocol compatible with fiber-optic networks with a range of up to 250 km (The Beacon of Russian Achievements, 2019). Professor K.E. Rumyantsev (MISiS) emphasizes: “Our goal is to create hybrid systems that combine quantum and classical methods for a smooth transition”, and, supporting the development of quantum technologies in the country, they

state: “Quantum cryptography provides solutions that can guarantee data security in the face of quantum attacks. We are working to ensure that Russia does not lag behind in this important area” (Rumyantsev & Plyonkin, 2015, p.p. 135).

4 CONCLUSIONS

The conducted scientific research is an in-depth analysis of the evolution of the concept of information, its role in science, technology and legislation, as well as the prospects for the development of quantum technologies and their impact on modern society. Based on the presented material, the following conclusions can be drawn::

1. The concept of information has gone from a philosophical abstraction to a strict scientific category thanks to the work of Claude Shannon, who introduced the bit as a unit of information measurement and associated it with entropy.
2. Information began to be considered as a fundamental category along with energy and matter, which opened up new horizons for research in physics, biology, quantum mechanics and other sciences.

With the development of artificial intelligence, blockchain, and big data, information has become a key resource that transforms into new knowledge and insights.

Questions arise about the legal regulation of information created by AI, as well as about the ethical and legal responsibility for decisions made by autonomous systems.

Russian legislation defines information as "information regardless of the form of its presentation," which creates a universal regulatory framework, but also creates gaps in law enforcement, especially in matters of personal data protection and cybersecurity.

Quantum cryptography, based on the principles of quantum mechanics, offers absolute data transmission security due to the phenomena of quantum entanglement and the Heisenberg uncertainty principle.

Russian developments in the field of quantum cryptography, such as quantum key distribution protocols, demonstrate a high level of data protection and compatibility with modern networks.

Quantum computers capable of breaking traditional cryptographic algorithms pose a threat to modern security systems.

The development of post-quantum algorithms and the transition to quantum cryptography are becoming necessary steps to protect data in the future.

Quantum entanglement and quantum teleportation open up new possibilities for creating global quantum communication networks that provide an unprecedented level of security.

In the end, it should be concluded that information, having gone from a philosophical abstraction to a fundamental scientific category, has become a key element of the modern world. Its physical nature, its connection to energy and entropy, as well as its role in artificial intelligence, blockchain, and quantum computing technologies make it a central focus of research and regulation. With the rapid development of technology, it is necessary not only to improve legislation, but also to develop new methods of data protection, such as quantum cryptography, to ensure the security and stability of information systems in the future. By actively participating in these processes, Russia demonstrates significant potential for leadership in the field of quantum technologies and information security.

REFERENCES

Bérut, A., Arakelyan, A., Petrosyan, A., Ciliberto, S., Dillenschneider, R., & Lutz, E. (2012). Experimental verification of Landauer's principle linking information and thermodynamics. *Nature*, *483*(7388), 187–189. https://doi.org/10.1038/nature10872

California Legislative Information. (2018). *California Consumer Privacy Act of June 28, 2018*. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L 119/1, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Kilin, S. Ya. (1999). Quantum information [Kvantovaya informatsiya]. *Uspekhi fizicheskikh nauk*, *169*(5), 507–527. https://doi.org/10.3367/ufnr.0169.199905b.0507

Kudryashov, V. E., & Fionov, A. N. (2022). Problem of stability of modern cryptosystems against the background of the emergence of quantum computers

[Problema ustoychivosti sovremennykh kriptosistem na fone poyavleniya kvantovykh komp'yuterov]. *Interekspo Geo-Sibir'*, (6), 109–115. https://doi.org/10.33764/2618-981X-2022-6-109-115

Liao, S.-K., Cai, W. Q., Liu, W. Y., Zhang, L., Li, Y., Ren, J. G., Yin, J., Shen, Q., Cao, Y., Li, Z. P., Li, F. Z., Chen, X. W., Sun, L. H., Jia, J. J., Wu, J. C., Jiang, X. J., Wang, J. F., Huang, Y. M., Wang, Q., Zhou, Y. L., Deng, L., Xi, T., Ma, L., Hu, T., Zhang, Q., Chen, Y. A., Liu, N. L., Wang, X. B., Zhu, Z. C., Lu, C. Y., Shu, R., Peng, C. Z., Wang, J. Y., & Pan, J. W. (2017). Satellite-to-ground quantum key distribution. *Nature, 549*(7670), 43–47. https://doi.org/10.1038/nature23655

Lloyd, S. (2013). *Programming the universe: A quantum computer and the future of science*. Alpina Non-Fiction.

Mironov, A. A. (2018). The birth of quantum Internet [Zarozhdeniye kvantovogo interneta]. *Vestnik sovremennykh issledovaniy*, *11.7*(26), 492–493.

NIST. (2022). *Post-quantum cryptography standardization*. https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization

Ozhegov, S. I., & Shvedova, N. Yu. (2010). *Explanatory dictionary of the Russian language*. Temp.

Pushkarev, V. V., Boziev, T. O., Esina, A. S., Zhamkova, O. E., & Chasovnikova, O. E. (2020). Criminal prosecution for crimes committed in the banking industry. *Laplage em Revista, 6*(Extra-C), 244–248.

Pushkarev, V. V., Fadeev, P. V., Khmelev, S. A., Van Tien, N., Trishkina, E. A., & Tsviliy-Buklanova, A. A. (2019a). Crimes in the Military-Industrial Complex (MIC). *International Journal of Recent Technology and Engineering*, *8*(3), 7950–7952. https://doi.org/10.35940/ijrte.C6635.098319

Pushkarev, V. V., Gaevoy, A., Skachko, A. V., Kolchurin, A., & Lozovsky, D. N. (2019b). Criminal prosecution and qualification of cybercrime in the digital economy. *Journal of Advanced Research in Dynamical and Control Systems*, *11*(8), 2563–2566.

Pushkarev, V. V., Poselskaya, L. N., Skachko, A. V., Tarasov, A. V., & Mutalieva, L. S. (2021). Criminal prosecution of persons who have committed crimes in the banking sector. *Cuestiones Políticas*, *39*(69), 395–406. https://doi.org/10.46398/cuestpol.3969.25

Rastoropov, S., Pushkarev, V., Fadeev, P., Grimalskaya, S., & Chikovani, M. (2024). Legal relations arising between an investigator and a legal entity that has suffered from a crime in the criminal process of the Russian Federation. *Relações Internacionais no Mundo Atual*, *1*(43), 367–376.

Rumyantsev, K. E., & Plyonkin, A. P. (2015). Security of the synchronization mode of quantum keys distribution system [Bezopasnost' rezhima sinkhronizatsii sistemy

kvantovogo raspredeleniya klyuchey]. *Izvestiya SFEDU. Engineering Sciences*, *5*(166), 135–153.

Shannon, C. (1963). *Works on information theory and cybernetics [Raboty po teorii informatsii i kibernetike]*. Izd-vo inostrannoy literatury.

State Duma of the Federal Assembly of the Russian Federation. (2006). *Federal Law of July 27, 2006, No. 149-FZ "On information, information technologies, and information protection" [Federal'nyy zakon ot 27.07.2006 No. 149-FZ "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii"]*. http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264

The Beacon of Russian Achievements. (2019). *Developing quantum cryptography methods [Sozdanie metodov kvantovoy kriptografii]*. https://bra.mikluho-maclay.ru/shifrovanie/

Vaulina, E. Yu., Sklyarevskaya, G. N., Tkacheva, I. O., & Fiveyskaya, E. A. (Eds.). (2014). *Explanatory dictionary of key terms of the Russian language [Tolkovyy slovar' klyuchevykh slov russkogo yazyka]*. Saint Petersburg State University, Faculty of Philology.

Vikipediya. (n.d.). *BB84*. Retrieved February 9, 2025, from https://ru.wikipedia.org/wiki/BB84

World Economic Forum. (2015). *Deep shift – Technology tipping points and societal impact: Survey report*. https://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf