SECURITY OF ELECTRONIC HEALTH RECORDS: FEDERATED BLOCKCHAIN AND POST-QUANTUM CRYPTOGRAPHY

Kostrov SA ✉, Potapov MP

Yaroslavl State Medical University, Yaroslavl, Russia

The article presents a review on the potential of the distributed ledger technology (DLT), particularly federated blockchain, that can be used to create a secure, transparent and patient-managed ecosystem of medical data. The hybrid architecture reviewed uses the blockchain to store immutable metadata and hashes, and manage large amounts of data (for example, diagnostic images) on external cloud storage, which ensures the integrity of data without network overloading. The key aspect of the research is to analyze long-term threats posed by quantum computing that makes current cryptographic standards vulnerable. It is stressed that adoption of post-quantum cryptography (PQC) is required to ensure future security of medical data. An analysis was carried out to compare the leading global (CRYSTALS-Dilithium, Falcon) and Russian (Hypericum, Shipovnik) post-quantum cryptography algorithms.

Keywords: blockchain, post-quantum cryptography, electronic health record, distributed ledger, federated computing, bioethics

Author contribution: Potapov MP — research planning, analysis, editing; Kostrov SA — data collection, analysis and interpretation, preparing a draft manuscript.

✉ **Correspondence should be addressed:** Sergey A. Kostrov
Revolutsionnaya St., 5, Yaroslavl, 150000, Russia; kosea@ysmu.ru

Received: 13.08.2025 **Accepted:** 18.10.2025 **Published online:** 03.11.2025

DOI: 10.24075/medet.2025.019

БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ ЗАПИСЕЙ: ФЕДЕРАТИВНЫЙ БЛОКЧЕЙН И ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ

С. А. Костров ✉, М. П. Потапов

Ярославский государственный медицинский университет, Ярославль, Россия

Статья посвящена анализу потенциала технологии распределенного реестра, в частности федеративного блокчейна, как основы для создания защищенной, прозрачной и управляемой пациентом экосистемы медицинских данных. Рассмотрена гибридная архитектура, при которой блокчейн используется для хранения неизменяемых метаданных и хешей, а объемные файлы (например, диагностические изображения) размещаются во внешних децентрализованных хранилищах, что гарантирует целостность данных без перегрузки сети. Ключевым аспектом исследования является анализ долгосрочных угроз, связанных с развитием квантовых компьютеров, которые ставят под угрозу существующие криптографические стандарты. Подчеркивается необходимость перехода на постквантовую криптографию для обеспечения будущей безопасности медицинских данных. Проведен сравнительный анализ ведущих мировых (CRYSTALS-Dilithium, Falcon) и перспективных отечественных («Гиперикум», «Шиповник») квантово-устойчивых алгоритмов криптографии.

Ключевые слова: блокчейн, постквантовая криптография, электронная медицинская запись, распределенный реестр, федеративные вычисления, биоэтика

Вклад авторов: М. П. Потапов — планирование исследования, анализ, редактирование; С. А. Костров — сбор, анализ, интерпретация данных, подготовка черновика рукописи.

✉ **Для корреспонденции:** Сергей Александрович Костров
Ул. Революцилнная, д. 5, г. Ярославль, 150000, Россия; kosea@ysmu.ru

Статья поступила: 13.08.2025 **Статья принята к печати:** 18.10.2025 **Опубликована онлайн:** 03.11.2025

DOI: 10.24075/medet.2025.019

In the digital age of healthcare, storage and management of electronic health records deserve equal attention both from a technical and bioethical perspective. The issue is pressing due to the exponential growth of healthcare data generated during diagnostics and treatment, including telemedical consultations and wearable technologies. Medical images, genomics and molecular research form the core of them. According to the World Health Organization, healthcare data will reach one-third of global medical data in zettabytes [1]. It increases the risk of leakage and unauthorized access. Thus, in developed countries, healthcare is considered a critical information infrastructure. In 2025, global economic losses from cyber incidents are estimated to reach 10 billion dollars [2, 3].

Patients value not only high-quality and complete healthcare information but also information security, ethical privacy standards, and control over their data. Traditional centralized data storage in medical information systems poses significant risks due to single points of failure.

Blockchain technologies that ensure decentralization, cryptographic protection and flexible safety partly controlled by an individual hold significant promise in line with AI, quantum computations and enhanced cryptography.

The aim of the publication is to introduce the distributed ledger technology used to store health records to the medical community while addressing the issues of enhancing information security and confidentiality through cryptographic algorithms.

MATERIALS AND METHODS

This article articulated an approach for searching in the leading Russian and foreign bibliographic resources such as eLibrary and PubMed, using specialized platforms to analyze scientific publications including Semantic Scholar, Consensus и Elicit, performing critical analysis, and selecting relevant sources. To be included, publications needed to match the topic of the study, be published between 2018 and 2025, and have both full-text Russian and English versions available. The relevance of sources was initially assessed through abstracts by checking if they focused on the topic of using blockchain technology in the healthcare sector.

A group of experts checked the final manuscript for accuracy. OpenAI ChatGPT-4.1 and Google Gemini 2.5 were used for summarization and grammar correction.

RESULTS AND DISCUSSION

Individuals may erroneously believe that blockchain is a synonym for cryptocurrency though it is just the underlying technology. The technology has made it possible for records to be unchangeable, controllable, accessible and protected no matter if it is used in economics, logistics, management or medicine.

Unlike the traditional centralized systems, which data are controlled by medical institutions, blockchain allows patients to manage their health records with greater autonomy [4].

Users hold a private cryptology key that helps them do the following:

- determine the conditions for data use through smart contracts;
- track all transactions due to blockchain immutability;
- withdraw approvals at any time.

The main property of the blockchain is immutability, as once data are recorded, they cannot be changed or deleted [4].

Blockchains used for storing health records are classified into public, private, and federated (consortium) blockchains based on DLT types. A public blockchain is a decentralized, open network that can be joined by any participant [5]. A private system managed by a single organization is well-suited for tasks that require centralized management and accelerated consensus. On the one part, it can speed up transactions, optimize clinical information flows, and implement policies of access, audit and compliance control at a greater rate. On the other part, private blockchains can suffer from disadvantages such as centralization risks, risks of failure and misuse, and challenges in scaling across institutions and regions [6].

Federated blockchains, also known as consortium or permissioned blockchains, are networks with restricted access, that can be controlled by a predetermined group of participants (medical organizations, laboratories and regulatory bodies), thus maintaining a balance between decentralization and access control. Federated blockchains enable integration of multiple medical institutions into a unified system and provide for the secure exchange of health records.

Also, federated blockchains help process transactions at a higher speed and ensure a greater flow capacity as validating nodes are limited in number and can be controlled. In public networks, the speed is lower as consensus of a greater number of unknown participants is required [5].

Electronic health records can be stored using technological platforms such as Hyperledger Fabric. They combine smart contracts, attribute-based access control (ABAC) and IPFS-based distributed data storage (file system) [7].

In Russia, Masterchain by FinTech Association, the first certified platform, which uses Russian means of cryptographic protection of information, is being actively implemented into the banking sphere. In 2021, Russia launched a blockchain operator for its distributed ledger system. Net processed information is legally significant here. It has been used by the Federal Tax Service of Russia to store computer-readable powers of attorney since 2023 [8].

Public blockchains such as Bitcoin, Ethereum, etc. cannot be directly implemented in healthcare. They are used to store hash functions and references to encrypted data partially solving the issue of confidentiality [7].

Transparency of public blockchains is a valuable advantage for financial and logistic applications. In medicine, however, it is rather a disadvantage. Placing encrypted data on an open network can be considered a form of data leakage because the data, when saved, can be decrypted in future using methods that are currently unavailable [7, 9]. For instance, widely applied ECDSA cryptographic methods based on elliptic curves, which are highly protected in traditional systems, can be broken with Shor's algorithm capable to reclaim the private key using the public key on a quantum computer in polynomial time [10].

A large-scale quantum computer capable of running Shor's algorithm with a sufficient number of qubits (around 2000) and low level of errors will compromise safety mechanisms. Healthcare systems require long-term digital safety. Active scientific and technological developments are transitioning to post-quantum cryptography, key distribution schemes and novel consensus protocols that do not depend on mathematical tasks vulnerable to Shor's algorithms [10].

First and foremost, post-quantum algorithms are based on lattices (lattice-based cryptography), and their security is guaranteed by the difficulty of mathematical problems associated with these lattices (for example, the Shortest Vector Problem (SVP) and the Learning with Errors (LWE) problem), which allow only exponential attacks, even on a quantum computer. Typical algorithms can include as follows [11, 12]:

- NTRUEncrypt is one of the first and most famous systems;
- CRYSTALS-Dilithium is a modern lightweight digital signature scheme recommended by the National Institute of Standards and Technology of the USA (NIST) in 2024 and proposed to replace ECDSA as the main standard. It demonstrates an optimal balance between the speed of key generation, signing, verification, and keys and signatures of "moderate" size [12];
- Falcon is recommended by NIST as an additional signature scheme for special cases where maximum compactness of signatures and keys is desired, as well as for applications that prioritize high signature verification speed [11].

In addition to lattice cryptography, solutions based on isogeny-based cryptography and the morphism of a path between two different elliptic curves, are of particular interest. SIKE (Supersingular Isogeny Key Encapsulation) was a well-known post-quantum cryptography algorithm based on isogenies, which also participated in the post-quantum standardization competition announced by NIST. However, the algorithm was cracked in 2022. Currently, other algorithms (SQISign — Short Quaternion and Isogeny Signature, CSIDH — Commutative Supersingular Isogeny Diffie-Hellman, etc.) are at the level of academic research and cannot be widely applied in practice [13].

Kyber is an advanced post-quantum encryption algorithm selected by the US National Institute of Standards and Technology (NIST) as the main standard for key encapsulation (KEM) mechanisms in the era of quantum computing [12].

Unfortunately, domestic developments are still significantly behind world standards. National standard systems, including GOST 34.10-2012 and GOST 34.10-2018, are also based on elliptic curve operations and are vulnerable to quantum

Table. Comparison of post-quantum cryptographic algorithms

Specification	Hypericum	Shipovnik	Falcon	CRYSTALS-Dilithium
Developer	QApp (Russia)	Kryptonite (Russia)	International group	International group
Cryptographic basis	Hash functions (SPHINCS+)	Coding theory (Stern based protocol)	NTRU grids	Grids (LWE)
Computed task	Hash functions Streebog GOST	Decoding an accidental linear code	Searching for short vectors in NTRU-grid	Ring learning with errors
Public key (bytes)	64	512	897 (Falcon-512) 1793 (Falcon-1024)	1,312 (Dilithium2) 1,952 (Dilithium3) 2,592 (Dilithium5)
Signature size (bytes)	18,292–58,460	~ 600,000	752 (Falcon-512) 1462 (Falcon-1024)	2,420 (Dilithium2) 3,293 (Dilithium3) 4,595 (Dilithium5)
Performance	Relatively slow signature and verification	Rapid generation of keys and signature verification	Slow generation of keys with rapid verification of signature	Rapid generation of keys and signature verification
Patterns	Very large size of signature, slow functioning	Long process of signature creation	Most compact signatures, high productivity and difficult implementation	Balanced features, simple implementation, good productivity

cryptanalysis. Academic research and development of domestic post-quantum algorithms are still underway [14–17]:

Hypericum is an algorithm of digital signature developed by QApp in line with Technical Committee 26 of Rosstandard. To implement SPHINCS+ postquantum digital signature scheme, the works on using the Russian standardized Streebog hash function are in progress [17].

Shipovnik is an algorithm developed by Kryptonite, which is based on the complex task of an accidental linear code decoding. At present, effective algorithms that allow standard or quantum computers to solve some types of problems are unknown. In theory, they cannot be created even using computers of tomorrow with millions operating qubits. However, a large signature size is impractical for blockchain use.

The Oblepikha algorithm presented during the RusCrypto'2025 conference is also of interest. It is based on the theory of grids (LIP task) and uses the decreasing signature size while preserving a high level of stability.

Hypericum and Shipovnik can be classified as future state cryptographic standards in Russia with open implementations in the C language, including many hosted on GitHub: https://github.com/QAPP-tech/shipovnik_tc26 and https://github.com/QAPP-tech/hypericum_tc26 (table).

Apart from encryption, permissioned systems used in healthcare enable flexible access control. Hybrid models that combine role-based and attributive-based access controls (RBAC and ABAC) and multitiered systems of access control are used in practice.

Role-based access control (RBAC) is used by patients to assign various roles (doctor, nurse, researcher) with respective access levels [18].

Attribute-based access control (ABAC) enables to create more flexible access policies based on numerous attributes such as time frames, geographic location, data types and purpose of use.

Technological solutions are based on multitiered architectures where a user interface intuitively integrates management of approvals and review of medical data. The level of smart contracts provides a seamless way to execute business logic including issue, change and withdrawal of consents, as well as monitoring of all operations.

Every transaction such as appointment entry, prescriptions, test results, medical reports and discharge summaries can be recorded within the chain of blocks creating an indisputable and chronologically adjusted audit trail. However, blockchains cannot store large files. Attempts to include diagnostic images (MRI scans, CT scans, etc.) or other large data in the blockchain will result in an exponential growth of registry size, decrease of network productivity and unreasonably high transaction expenses [19].

In a typical blockchain scenario, blockchain uses hashes and meta-data that make transactions immutable and transparent, whereas large medical files are placed in decentralized file systems (IPFS). It warrants that the data are highly accessible and integral. If a file in a blockchain-based repository is altered even by a single byte, its cryptographic hash will change, which will break the link to subsequent blocks in the chain, immediately revealing the tampering to anyone inspecting the ledger [5, 19].

The public key of a patient functions both as an address or network ID that can be freely shareable with others (medical institutions or insurance companies) to obtain access to the data. However, any transaction, including approval for review or change in health records, should be signed using a respective private key [18].

Despite the advantages, the system makes a patient liable. The loss of a private key is critical. In totally decentralized (public) blockchain systems, such a loss means a complete and permanent loss of access to medical health records and their control. The protocols restoring personalities and keys can be implemented in the federative blockchain. A consortium can act as a trusted arbiter. Thus, if patients lose the key, their personality can be verified and a new key can be provided to access the records. It is common to use multi-signature schemes when signatures of several parties are required to restore the access.

Digital literacy should be continuously improved, as many doctors and patients can't manage keys effectively and are still unaware of how blockchain works. Low awareness leads to digital inequality and makes new solutions less available for individuals, countries and regions.

CONCLUSIONS

A distributed ledger technology, particularly federated blockchain (consortium), represents a perspective solution that can dramatically increase the level of data protection, ensure their integrity and allow patients to control their data. A balance between a complete decentralization of public networks and centralized control of public systems is required. Managing the consortium of authorized members (medical organizations, laboratories, insurance companies, state regulators) corresponds to the structure of healthcare system and enables high speed of transactions and flow capacity. Hybrid storage in decentralized file-based systems and use of blockchain to store hashes and metadata ensure integrity without overloading the network.

Russian developments such as the Masterchain platform have already displayed the technology potential, its legal significance in the banking sphere and perspectives of use in healthcare and adjacent fields.

The existing cryptographic standards including GOST are vulnerable to quantum cryptoanalysis. Thus, shifting to post-quantum cryptography is both a key perspective and a challenge. To create truly protected medical systems of the future, quantum-resistant algorithms, such as globally used CRYSTALS-Dilithium and Falcon, and Russian-based Hypericum and Shipovnik, should be developed and standardized. A wide-ranging application requires improved legislation in the field of data protection, updated GOSTs, and certification of cryptographic data protection tools.

Successful implementation of the technologies depends on how technical, social and organizational tasks can be solved, primarily on improved digital literacy of physicians and patients. Blockchain advantages cannot be implemented completely and digital risks are impossible to avoid when the principles of blockchain operation and responsible management of cryptographic keys are failed to be understood.

References

1. Meeting Abstracts from the 5th National Big Data Health Science Conference. BMC Proceedings. 2024; 18(9). DOI: 10.1186/s12919-024-00292-3.
2. Broklyn, Peter and Shad, Ralph and Egon, Axel, The Evolving Thread Landscape Pf Ai-Powered Cyberattacks: A Multi-Faceted Approach to Defense and Mitigate. July 18, 2024. DOI: 10.2139/ssrn.4904878.
3. Dirksen S and Korah J. "GUARD: Graph-based Unknown Attack Recognition and Detection,"2024 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 2024; 1–6. DOI: 10.1109/WIFS61860.2024.10810721.
4. Porsdam Mann S, Savulescu J, Ravaud P, & Benchoufi M. Blockchain, consent and prosent for medical research. Journal of medical ethics, 2020; 47(4): 244–250. Advance online publication. DOI: 10.1136/medethics-2019-105963
5. Litvin AA, Korenev SV, Knyazeva EG, Litvin V. The Possibilities of Blockchain Technology in Medicine (Review). Modern Technologies in Medicine. 2019; 11(4): 191–199. DOI: 10.17691/stm2019.11.4.21. — EDN FKRPUE.
6. Esmaeilzadeh P. Benefits and concerns associated with blockchain-based health information exchange (HIE): a qualitative study from physicians' perspectives. BMC medical informatics and decision making, 2022; 22(1): 80. DOI: 10.1186/s12911-022-01815-8.
7. Hasnain M, et al. The Hyperledger fabric as a Blockchain framework preserves the security of electronic health records. Frontiers in Public Health. 2023; 11. DOI: 10.3389/fpubh.2023.1272787.
8. Andrianova NG. Osnovnyye napravleniya ispol'zovaniya tekhnologiy v finansovoy sfere. Agrarnoye i zemel'noye pravo. 2024; 4 (232): 109–111. DOI: 10.47643/1815-1329_2024_4_109109-111. Russian.
9. Liu C, Xiang F, Sun Z. Multiauthority Attribute-Based Access Control for Supply Chain Information Sharing in Blockchain. Security and Communication Networks. 2022; 1. DOI: 10.1155/2022/8497628.
10. Huang Y, et al. Choosing Coordinate Forms for Solving ECDLP Using Shor's Algorithm. arXiv preprint arXiv:2502.12441. 2025.
11. Dam D -T, Nguyen T -H, Tran T -H, Le D -H, Hoang T -T and Pham C -K. "High-Efficiency Multi-Standard Polynomial Multiplication Accelerator on RISC-V SoC for Post-Quantum Cryptography", in IEEE Access. 2024; 12: 195015–195031. DOI: 10.1109/ACCESS.2024.3520592.
12. Li' A, Li Z, Tang J and Lu Y. "KDA: Kyber and Dilithium Accelerator for CRYSTALS Suite of Post-Quantum Cryptography in Hybrid Multipath Delay Commutator Pipelined Architecture". 2024 IEEE Asian Solid-State Circuits Conference (A-SSCC). Hiroshima. Japan. 2024; 1–3. DOI: 10.1109/A-SSCC60305.2024.10848993.
13. Castryck W, Decru T. (2023). An Efficient Key Recovery Attack on SIDH. In: Hazay C, Stam M. (eds) Advances in Cryptology — EUROCRYPT 2023. EUROCRYPT 2023. Lecture Notes in Computer Science. 2023; 14008. Springer, Cham. DOI: 10.1007/978-3-031-30589-4_15.
14. Komarova A, Korobeynikov A. Combined authentication schemes with increasing level of resistance and methods for improving the security of electronic signature schemes: Kombinirovannye skhemy autentifikacii s povyshennym urovnem stojkosti i metody povysheniya bezopasnosti skhem elektronnoj. Podpisi. Proceedings of the 12th International Conference on Security of Information and Networks. 2019; 1–8.
15. Nazarenko AP, Dmitriyev Ye V. Sovremennoye sostoyaniye postkvantovoy kriptografii v Rossii i za rubezhom. Sistemy sinkhronizatsii, formirovaniya i obrabotki signalov. 2021; 12(6): 77–83. EDN FNKIVP. Russian.
16. Urban NA, Mel'nikova Ye A. Primeneniye algoritmov na reshotkakh v postkvantovoy kriptografii. Sovremennyye informatsionnyye tekhnologii i IT-obrazovaniye. 2024; 20(1): 27–33. DOI: 10.25559/SITITO.020.202401.27-33. EDN BNHDRO. Russian.
17. Kiktenko EO, et al. SPHINCS + digital signature scheme with GOST hash functions. arXiv. 2019. DOI: 10.1063/5.0011441.
18. Guo H, et al. Access control for electronic health records with hybrid blockchain-edge architecture. 2019 IEEE international conference on blockchain (Blockchain). IEEE. 2019; 44–51. DOI: 10.48550/arXiv.1906.01188.
19. Rajasekharan A and Koshy R. "EMRChain: Electronic Medical Records Management System using Blockchain". 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) Pune. India. 2024; 1–6. DOI: 10.1109/ICBDS61829.2024.10837244.

Литература

1. Meeting Abstracts from the 5th National Big Data Health Science Conference. BMC Proceedings. 2024; 18(9). DOI: 10.1186/s12919-024-00292-3.
2. Broklyn, Peter and Shad, Ralph and Egon, Axel, The Evolving Thread Landscape Pf Ai-Powered Cyberattacks: A Multi-Faceted Approach to Defense and Mitigate. July 18, 2024. DOI: 10.2139/ssrn.4904878.
3. Dirksen S and Korah J. "GUARD: Graph-based Unknown Attack Recognition and Detection,"2024 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 2024; 1–6. DOI: 10.1109/WIFS61860.2024.10810721.
4. Porsdam Mann S, Savulescu J, Ravaud P, & Benchoufi M. Blockchain, consent and prosent for medical

research. Journal of medical ethics, 2020; 47(4): 244–250. Advance online publication. DOI: 10.1136/medethics-2019-105963.

5. Litvin AA, Korenev SV, Knyazeva EG, Litvin V. The Possibilities of Blockchain Technology in Medicine (Review). Modern Technologies in Medicine. 2019; 11(4): 191–199. DOI: 10.17691/stm2019.11.4.21. — EDN FKRPUE.
6. Esmaeilzadeh P. Benefits and concerns associated with blockchain-based health information exchange (HIE): a qualitative study from physicians' perspectives. BMC medical informatics and decision making, 2022; 22(1): 80. DOI: 10.1186/s12911-022-01815-8.
7. Hasnain M, et al. The Hyperledger fabric as a Blockchain framework preserves the security of electronic health records. Frontiers in Public Health. 2023; 11. DOI: 10.3389/fpubh.2023.1272787.
8. Андрианова Н. Г. Основные направления использования технологии блокчейн в финансовой сфере. Аграрное и земельное право. 2024; 4 (232): 109–111. DOI: 10.47643/1815-1329_2024_4_109.
9. Liu C, Xiang F, Sun Z. Multiauthority Attribute-Based Access Control for Supply Chain Information Sharing in Blockchain. Security and Communication Networks. 2022; 1. DOI: 10.1155/2022/8497628.
10. Huang Y, et al. Choosing Coordinate Forms for Solving ECDLP Using Shor's Algorithm. arXiv preprint arXiv:2502.12441. 2025.
11. Dam D -T, Nguyen T -H, Tran T -H, Le D -H, Hoang T -T and Pham C -K. "High-Efficiency Multi-Standard Polynomial Multiplication Accelerator on RISC-V SoC for Post-Quantum Cryptography," in IEEE Access. 2024; 12: 195015–195031, DOI: 10.1109/ACCESS.2024.3520592.
12. Li' A, Li Z, Tang J and Lu Y. "KDA: Kyber and Dilithium Accelerator for CRYSTALS Suite of Post-Quantum Cryptography in Hybrid Multipath Delay Commutator Pipelined Architecture". 2024 IEEE Asian Solid-State Circuits Conference (A-SSCC). Hiroshima. Japan. 2024; 1–3. DOI: 10.1109/A-SSCC60305.2024.10848993.
13. Castryck W, Decru T. (2023). An Efficient Key Recovery Attack on SIDH. In: Hazay C, Stam M. (eds) Advances in Cryptology — EUROCRYPT 2023. EUROCRYPT 2023. Lecture Notes in Computer Science. 2023; 14008. Springer, Cham. DOI: 10.1007/978-3-031-30589-4_15.
14. Komarova A, Korobeynikov A. Combined authentication schemes with increasing level of resistance and methods for improving the security of electronic signature schemes: Kombinirovannye skhemy autentifikacii s povyshennym urovnem stojkosti i metody povysheniya bezopasnosti skhem elektronnoj. Podpisi. Proceedings of the 12th International Conference on Security of Information and Networks. 2019; 1–8.
15. Назаренко, А. П., Дмитриев Е. В. Современное состояние постквантовой криптографии в России и за рубежом. Системы синхронизации, формирования и обработки сигналов. 2021; 12(6): 77–83. EDN FNKIVP.
16. Урбан Н. А., Мельникова Е. А. Применение алгоритмов на решётках в постквантовой криптографии. Современные информационные технологии и ИТ-образование. 2024; 20(1): 27–33. DOI: 10.25559/SITITO.020.202401.27-33. EDN BNHDRO.
17. Kiktenko EO, et al. SPHINCS + digital signature scheme with GOST hash functions. arXiv. 2019. DOI: 10.1063/5.0011441.
18. Guo H, et al. Access control for electronic health records with hybrid blockchain-edge architecture. 2019 IEEE international conference on blockchain (Blockchain). IEEE. 2019; 44–51. DOI: 10.48550/arXiv.1906.01188.
19. Rajasekharan A and Koshy R. "EMRChain: Electronic Medical Records Management System using Blockchain". 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) Pune. India. 2024; 1–6. DOI: 10.1109/ICBDS61829.2024.10837244.