INFORMATION SECURITY IN HEALTHCARE: MODERN THREATS AND PROTECTION METHODS

Sokolova OV[1] ✉, Zheltkevich OV[1], Kalabekova SV[2]

[1] Yaroslavl State Medical University, Yaroslavl, Russia

[2] North Caucasus State Academy, Cherkessk, Russia

The paper analyzes information security issues in Russian healthcare in the context of digital transformation. Digitalization of the healthcare sector, including integration of information systems of medical and pharmaceutical organizations with the Uniform State Health Information System (EGISZ), improves the quality of medicines and healthcare provided to the population. Meanwhile, the risk of patient personal data leakage and computer attacks on healthcare organizational information systems is increasing. The purpose of the study is to develop an integrated approach to information security in medical and pharmaceutical organizations. The research uses content analysis, logical and structural analysis of scientific papers and regulatory legal acts in the field of information technology in healthcare. The authors identify the stages of information security regulation from protecting medical secrets to categorizing critical information infrastructure and using domestic software. The classification of security threats to digital systems is provided based on the location of the threat source depending on whether they originate outside or inside the organization's network perimeter. The directions and evaluation criteria for improving information security are provided based on modern methods and technologies of information protection, including technical means of protection, legal mechanisms, as well as organizational and managerial methods.

Keywords: healthcare, information security, medical personal data, computer attacks, information protection, EGISZ, critical information infrastructure, medical and pharmaceutical workers

✉ **Correspondence should be addressed:** Olga V. Sokolova
Revolutsionnaya Str., 5, Yaroslavl, 150014, Russia; sova293@yandex.ru

Received: 10.04.2026 **Accepted:** 15.04.2026 **Published online:** 27.04.2026

DOI: 10.24075/medet.2026.009

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЗДРАВООХРАНЕНИИ: СОВРЕМЕННЫЕ УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ

О. В. Соколова[1] ✉, О. В. Желткевич[1], С. В. Калабекова[2]

[1] Ярославский государственный медицинский университет, Ярославль, Россия

[2] Северо-Кавказская государственная академия, Черкесск, Россия

Статья посвящена анализу проблем информационной безопасности в здравоохранении России в условиях цифровой трансформации. Цифровизация сферы здравоохранения, включая интеграцию информационных систем медицинских и фармацевтических организаций с ЕГИСЗ, повышает качество оказания медицинской и лекарственной помощи населению. При этом увеличиваются риски утечек персональных данных пациентов и угрозы компьютерных атак на информационные системы организаций. Цель исследования — формирование комплексного подхода к обеспечению информационной безопасности в медицинских и фармацевтических организациях. В ходе исследования использованы контент-анализ, логический и структурный анализ научных трудов и нормативно-правовых актов в области применения информационных технологий в здравоохранении. Авторами выделены этапы регулирования информационной безопасности от защиты врачебной тайны к категорированию критической информационной инфраструктуры и применению отечественного программного обеспечения. Приведена классификация угроз безопасности цифровых систем по расположению источника угроз относительно организации по внешним и внутренним критериям. Предложены направления и критерии оценки для повышения информационной безопасности на основе современных методов и технологий защиты информации, включая технические средства защиты, юридические механизмы, а также организационно-управленческие методы.

Ключевые слова: здравоохранение, информационная безопасность, компьютерные атаки, защита информации, ЕГИСЗ, медицинские персональные данные, критическая информационная инфраструктура, медицинские и фармацевтические организации

✉ **Для корреспонденции:** Ольга Вячеславовна Соколова
ул. Революционная, д. 5, г. Ярославль, 150014, Россия; sova293@yandex.ru

Статья поступила: 10.04.2026 **Статья принята к печати:** 15.04.2026 **Опубликована онлайн:** 27.04.2026

DOI: 10.24075/medet.2026.009

Digitalization and informatization of the healthcare system, implemented within the information society development strategy and the national Healthcare project, are associated with the introduction and use of information systems in medical and pharmaceutical organizations to provide high-quality medical and medicinal care. Information systems designed to automate business processes include a set of information, software, technical, and organizational tools [1, 2]. At the same time, information systems store data from financial, economic, administrative and organizational facets; medical information about patients; research and monitoring results, etc. The use of information systems makes it possible to reduce errors when filling out accounting documents, provide quick access to large volumes of medical information, etc. [3].

The possibility of integrating information systems of medical and pharmaceutical organizations with the Unified

State Information System in the Field of Healthcare (USISZ) is worth mentioning, as one of its tasks is to provide information support for state regulation in the field of healthcare. EGISZ includes information about data from the federal electronic registry, electronic patient medical records (EHRs), electronic medical documents, etc. The EGISZ information also includes federal registers. The Federal Register of Medical Workers (FRMR) is a centralized database that contains information about all medical and pharmaceutical workers in Russia. The Federal Register of Medical Organizations (FRMO) contains information about the structure, business profiles, addresses and equipment of each medical institution. The subsystems of the EGISZ are represented by a specialized patient registry for individual diseases and/or conditions, a registry of medicines for medical use, as well as an information and analytical subsystem for monitoring and control in the field of drug procurement [4].

Consequently, the integrated digital healthcare environment contains up-to-date information on technical, medicinal, and human resources in healthcare and personal health-related data of patients. However, as practice shows, digital transformation is accompanied by an increase in risks, with information security threats now occupying a leading position. Therefore, it is necessary to ensure security of information systems for protection of personal data of patients and specialists by developing ways to protect data and equipment from computer attacks [5–8].

Thus, the relevance of the topic is determined by several factors. First, medical data belongs to a special category of personal data. Its leakage is regarded as a violation of the patient's right to medical confidentiality. Second, medical and pharmaceutical organizations are recognized as subjects of critical information infrastructure (CII) with increased requirements for information protection. Third, the significant increase in computer attacks on the healthcare sector confirms its high vulnerability (in the first half of 2025, their number increased by 24% compared to the same period in 2024). Fourth, the level of digital literacy of medical and pharmaceutical workers and training in information security is often insufficient.

The abovementioned facts have determined the purpose of this work consisting in the formation of an integrated approach to information security in medical and pharmaceutical organizations.

Achieving this goal included solving consecutive tasks.

1. Analysis of the stages of development of information security in the healthcare sector.
2. Identification and structuring of information security threats in healthcare.
3. Conducting an analysis of modern information security methods and technologies.
4. Development of recommendations and proposals for ensuring information security in medical and pharmaceutical organizations.

MATERIALS AND METHODS

The research was based on both Russian and foreign scientific publications on the use of information technology while providing medical and medicinal care. Regulatory legal acts in the field of digital transformation of healthcare were studied. In the research process, the logical method, the structural method, and method of content analysis were used.

RESULTS AND DISCUSSION

Based on the analysis of Russian regulatory documents, it is shown that both medical and pharmaceutical information are considered part of the "information constituting a medical secret" (Articles 13, Articles 20 of Federal Law No. 323-FZ) [9] and "special categories of personal data" (Article 10 of Federal Law No. 152-FZ) [10]. This dual legal status determines a special treatment regime to process information. Collection, storage and transfer of such data require the consent of the subject or a lawful basis.

The formation of the legal framework for information security in Russian healthcare is a gradual process. The main focus is primarily on medical secrecy and protection of personal data in accordance with Federal Law No. 152-FZ [10]. In 2017, Federal Law No. 187-FZ was adopted. It changed approaches to information protection. Thus, medical information systems (MIS) and pharmaceutical systems (PS) are classified as objects of critical information infrastructure (CII), which entailed the obligation to categorize them [11]. As part of meeting the requirements of the law on CII, medical and medicinal care providers are required to categorize not only information systems, but also automated process control systems (automated process control systems), which include medical equipment. It is also necessary to create departmental monitoring centers and use certified protective equipment.

In 2021, amendments to Decree of the President of the Russian Federation No. 250 [12] came into force, instructing the heads of CII organizations to create structural information security units. This requirement applies to organizations at the federal, regional, and municipal levels.

In 2022, the Government of the Russian Federation has defined the tasks of the Unified State Healthcare System (USISZ), its structure, procedures and deadlines for providing information, participants in information interaction, the procedure for protecting information contained in the unified system, as well as requirements for software and hardware. The next important step was to tighten the requirements for using foreign software. Since 2025, CII subjects have not been allowed to use foreign-made information protection tools [13].

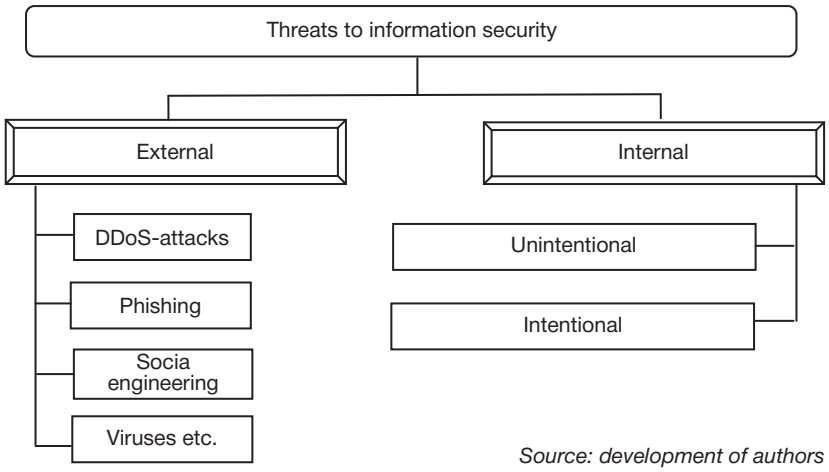
Thus, issues of information security protection in healthcare are being addressed at the state level.

The analysis of the identified risks of healthcare digitalization within the framework of digital information security has shown that the most likely threat is the loss of personal patient data and computer attacks on the digital databases of medical and pharmaceutical organizations [14–17].

It has been established that threats to the security of digital systems are classified according to various criteria. Therefore, to make the further study possible, a tailored classification of information security (IS) threats is essential for medical and pharmaceutical organizations. As threats come not only from outside, but also from within the organization, we have presented a classification based on the source's location relative to the organization (Fig.).

External threats are manifested through targeted computer attacks. Malware is used to infect systems and block access to data; DDoS attacks on telemedicine services make it difficult for the information systems of the Ministry of Defense and the Federal District to function; phishing and social engineering, in the form of letters sent on behalf of the heads of the organization asking for a password, aim at obtaining confidential information from users. Outdated IT systems are also classified by us as external threats because they are vulnerable and can be used by intruders to gain unauthorized access.

Internal threats to information security are classified by source into unintentional and intentional actions of the organization's



Source: development of authors

Fig. Classification of information security threats in healthcare by the source of occurrence

employees. The threats included in the first group are related to the loss of a USB flash drive containing databases; sending confidential information from a personal email to messengers; using simple passwords for authentication. Intentional actions may be accompanied by the sale of patient data to competitors, copying of information before dismissal, violations of regulations for information systems, etc.

Thus, understanding specific threats to information security contributes to the formation of comprehensive protection against risks.

The theoretical foundations of information security in medical and pharmaceutical organizations involve the use of various methods and technologies, including technical means of protection, legal mechanisms, as well as organizational and managerial methods.

Technical protection measures include intrusion detection and blocking systems, hardware and software solutions (DLP systems) against data leaks, antivirus software and firewalls. Cryptographic methods (data encryption algorithms and electronic digital signature) are used to ensure data security. Data access control is provided by an authentication system that uses passwords, certificates, and biometric data.

The transition to domestic software in Russia, mandated by law, serves both strategic political goals and critical practical needs. The products of Russian developers are not inferior to their foreign counterparts in terms of functionality, and in a number of aspects (integration with government monitoring systems, adaptation to the specifics of Russian legislation) surpass them [13].

Compliance with the requirements in the field of processing, storing and transferring personal data in healthcare is regulated by a set of regulatory legal acts, whereas legal enforcement mechanisms provide for liability for violations of information security rules in the form of compensation for damage caused to the patient and payment of a fine in accordance with art. 13.11 of the Administrative Code of the Russian Federation.

Technical means and legal mechanisms for information protection will be effective only if they are integrated into the system of organizational and managerial tools that are used to achieve the goals and objectives of the organization.

Based on the results of the study, we have proposed an approach to ensuring information security in healthcare for provision of high-quality medical and medicinal care, consisting of the main directions and criteria for assessing information security.

One of the directions is categorization of CII objects in accordance with the legislation. Depending on the requirements for protective equipment, an object is assigned the first, the second or the third category of significance. Medical and pharmaceutical organizations are included in the register of significant CII facilities [11].

The next direction involves creating a system for responding to the incidents associated with an unauthorized access to information. It is about development of a standard operating procedure (SOP) outlining mandatory actions for detecting hacking or information leakage incidents. This helps you understand who makes the decision to shut down the system, who interacts with law enforcement agencies, and who notifies patients. Regular exercises (for example, phishing simulations) are crucial for practicing these actions.

Continuous staff training is a significant step in ensuring information security. The basics of information security should be studied already at the training stage of university students and followed by advanced training within the system of continuing professional education.

The proposed criteria for assessing information security for medical and pharmaceutical organizations include:

1) regular antivirus software updates;
2) the presence of a structural unit responsible for information security, the presence of an approved SOP in this area;
3) the proportion of employees who received information security training;
4) the absence of recorded violations in the field of information security.

CONCLUSIONS

It has been found out during the study that regulation of information security in healthcare has evolved through successive stages that reflect a systematic strengthening of government requirements for information protection. There exist external and internal threats to the information security of medical and pharmaceutical organizations. Three complementary groups including technical, legal, as well as organizational and management ones were set up following analysis of information protection methods, while the use of each separate group does not provide a sufficient level of protection. To improve information security in medical and pharmaceutical organizations, it is proposed to use an integrated approach containing the main directions and evaluation criteria.

References

1. Sokolova OV, Isaeva IYu, Kulikova OA, Alekseeva KS, Kuznetsova EA. Application of digital tools in a medical organization for optimization of drug provision. Cardiovascular Therapy and Prevention. 2024; 23 (S6): 150–151. Russian.
2. Sokolova OV, Kulikova OA, Alekseeva KS., Isaeva IYu. The Importance of Information Systems in the Activities of a Pharmacy Organization. Issues of Drug Quality Assurance. 2025; 1 (47): 54–58. DOI 10.34907/JPQAI.2025.63.82.008. Russian.
3. Shandora N. I. Information Security in the Healthcare Sector. In the collection: Proceedings of the 6th International Scientific and Practical Conference dedicated to the 25th Anniversary of the Faculty of Economics at BSU: Trends in Economic Development in the 21st Century, February 28–29, 2024. Minsk. 2024; 529–531.
4. Decree of the Government of the Russian Federation No. 140 dated February 9, 2022. "On the Unified State Healthcare System" (together with the "Regulations on the Unified State Healthcare Information System"). Russian.
5. Platonova NI, Ustilentsev KA, Ustilentseva TA. Information Security in the Healthcare Sector: Challenges and Development Prospects. 2022; 33 (2): 124–136. DOI 10.20410/2073-7815-2022-33-2-124-136. Russian.
6. Udaltsov KR. Cybersecurity in Healthcare: Strategies for Protecting Medical Data and Equipment. International Journal of Information Technology and Energy Efficiency. 2024; 9 (5): 18–22. Russian.
7. CODE RED 2026 Current Cyber Threats to Russian Organizations. Available from URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id1 (accessed: 27.03.2026). Russian.
8. Less than 25% of medical organizations in the Russian Federation are equipped with means of protection against internal information threats. Available from URL: https://medvestnik.ru/content/news/sredstvami-zashity-ot-vnutrennih-informacionnyh-ugroz-osnasheny-menshe-25-medorganizacii-rf.html (accessed: 27.03.2026). Russian.
9. Federal Law No. 323-FZ dated November 21, 2011. "On the Fundamentals of Public Health Care in the Russian Federation". Russian.
10. Federal Law No. 152-FZ dated July 27, 2006. "On Personal Data".
11. Federal Law No. 187-FZ dated July 26, 2017. "On the Security of the Critical Information Infrastructure of the Russian Federation". Russian.
12. Presidential Decree No. 250 dated May 1, 2022. "On Additional Measures to Ensure the Information Security of the Russian Federation." Russian.
13. Kochergina MO, Chugunova SA. The Role of Medical Software in the Digitalization of Healthcare. In the collection: New Technologies in the Educational Process and Production: Materials of the XXIII Scientific and Technical Conference with International Participation. Ryazan. April 16–18, 2025; 347–350. Russian.
14. Solovyov NV. Digital Security in Medicine: Challenges and Threats of Digital Transformation. In the collection: Materials of the International Scientific and Practical Conference. Volgograd. November 20, 2025; 40–44. Russian.
15. Lapina MA., Maksimova EA, Lapin VG, Boykov NS. Analytical review of methods for designing security systems in telemedicine systems. Proceedings of ISP RAS. 2024; 5. Available from URL: https://cyberleninka.ru/article/n/analiticheskiy-obzor-metodov-proektirovaniya-sistem-bezopasnosti-v-telemeditsinskih-sistemah (accessed: 27.03.2026). Russian.
16. Dubovskov MV, Fot Yu D. Information Security in the Healthcare Sector. In the collection: Current Issues in Ensuring Comprehensive Security: Proceedings of the National Scientific and Practical Conference with International Participation Dedicated to the 35th Anniversary of the Russian Ministry of Emergency Situations and the 95th Anniversary of the Orenburg State Agrarian University. Orenburg. May 23, 2025; 1041–1044. Russian.
17. Code of Administrative Offenses of the Russian Federation dated 30.12.2001 No. 195-FZ. Russian.

Литература

1. Соколова О. В., Исаева И. Ю., Куликова О. А., Алексеева К. С., Кузнецова Е. А. Применение цифровых инструментов в медицинской организации для оптимизации лекарственного обеспечения. Кардиоваскулярная терапия и профилактика. 2024; 23 (S6): 150–151.
2. Соколова О. В., Куликова О. А., Алексеева К. С., Исаева И. Ю. Значимость информационных систем в деятельности аптечной организации. Вопросы обеспечения качества лекарственных средств. 2025; 1 (47): 54–58. DOI 10.34907/JPQAI.2025.63.82.008.
3. Шандора Н. И. Информационная безопасность в сфере здравоохранения. В сборнике: Материалы VI Международной научно-практической конференции, посвященной 25-летию экономического факультета БГУ: Тенденции экономического развития в XXI веке. Минск. 2024; (1): 529–531.
4. Постановление Правительства РФ от 09.02.2022 № 140 «О единой государственной системе в сфере здравоохранения» (вместе с «Положением о единой государственной информационной системе в сфере здравоохранения»).
5. Платонова Н. И., Устиленцев К. А., Устиленцева Т. А. Информационная безопасность в сфере здравоохранения: проблемы и перспективы развития. 2022; 33 (2): 124–136. DOI 10.20410/2073-7815-2022-33-2-124-136.
6. Удальцов К. Р. Кибербезопасность в здравоохранении: стратегии защиты медицинских данных и оборудования. Международный журнал информационных технологий и энергоэффективности. 2024; 9 (5): 18–22.
7. CODE RED 2026 Актуальные киберугрозы российских организаций. Режим доступа: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id1 (дата обращения: 27.03.2026).
8. Средствами защиты от внутренних информационных угроз оснащены меньше 25% медорганизаций РФ. Режим доступа: https://medvestnik.ru/content/news/sredstvami-zashity-ot-vnutrennih-informacionnyh-ugroz-osnasheny-menshe-25-medorganizacii-rf.html (дата обращения: 27.03.2026).
9. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».
10. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
11. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
12. Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
13. Кочергина М. О., Чугунова С. А. Роль медицинского программного обеспечения в цифровизации здравоохранения. В сборнике: Новые технологии в учебном процессе и производств: Материалы XXIII научно-технической конференции с международным участием, 16–18 апреля 2025 г. Рязань. 2025; 1: 347–350.
14. Соловьев Н. В. Цифровая безопасность в медицине: вызовы и угрозы цифровой трансформации. В сборнике: Материалы международной научно-практической конференции. 20 ноября 2025 г. Волгоград. 2025; 1: 40–44.
15. Лапина М. А., Максимова Е. А., Лапин В. Г., Бойков Н. С. Аналитический обзор методов проектирования систем

безопасности в телемедицинских системах. Труды ИСП РАН. 2024;5. Режим доступа: https://cyberleninka.ru/article/n/analiticheskiy-obzor-metodov-proektirovaniya-sistem-bezopasnosti-v-telemeditsinskih-sistemah (дата обращения: 27.03.2026).

16. Дубовсков М. В., Фот Ю. Д. Информационная безопасность в сфере здравоохранения. В сборнике: Актуальные вопросы обеспечения комплексной безопасности: Материалы национальной научно-практической конференции с международным участием, посвященной 35-летию МЧС России и 95-летию Оренбургского ГАУ. 23 мая 2025 г. Оренбург. 2025; 1: 1041–1044.
17. Кодекс Российской Федерации об административных нарушениях от 30.12.2001 № 195-ФЗ.