DOI 10.34132/pard2026.31.05

Отримано: 17 серпня 2025
Змінено: 09 вересня 2025
Прийнято: 23 грудня 2025
Опубліковано:
31 березня 2026

Received: 17 august 2025
Revised: 09 september 2025
Accepted: 23 december 2025
Published:
31 March 2026

Zhao Zhenyi

FEATURES OF INFORMATION SECURITY IN THE HEALTHCARE SECTOR

The article examines the role of information security in healthcare in the context of active digitalization of medical processes. It is shown that the introduction of electronic medical records, telemedicine and automated management systems not only improves the quality of medical services, the efficiency of institutions and the availability of medical care, but also creates new risks of leakage, modification or distortion of sensitive information, which requires special attention to cyber protection and standardization of information processes.

The features of medical information, which are characterized by high confidentiality, accuracy and criticality for the life and health of patients, are revealed. The need for proper data protection is emphasized to prevent errors in diagnosis, improper treatment, violation of ethical standards and loss of patients' trust in medical institutions. Special attention is paid to the protection of personal data and ensuring the integrity of medical records in the digital environment.

The main directions of information security organization in medical institutions are considered: multi-level authentication, access control, backup, data encryption and personal data protection. Key threats to medical information systems are identified – cyberattacks, phishing, malware, technical failures

and the human factor, which require a comprehensive approach to risk management and integration of technological, organizational and regulatory measures. Based on the analysis, practical recommendations for increasing the level of information security are formulated: improving data protection policies, using modern encryption technologies and secure information storage, constant monitoring of system operation, creating internal incident response protocols, implementing multi-level user authentication and regular training of personnel on cybersecurity. Implementation of these measures ensures stable, reliable and secure operation of medical information systems, increases the efficiency of medical institutions and strengthens patients' trust in modern digital healthcare.

Keywords: *information, information security, healthcare, digitalization, cyberattack*

General statement of the problem. In today's conditions of rapid development of information technologies, global digitalization and intensive informatization of society, the issue of ensuring information security is becoming one of the key priorities of national policy. The protection of information resources, personal data and all participants in information relations is gaining particular importance against the backdrop of the constant growth of data volumes circulating in the digital environment, as well as the active implementation of electronic services in various spheres of the economy, education, medicine and public administration. Reliable and secure functioning of the information space is not only a technical challenge, but also an important element of national security, social stability and economic development of the state.

The decisive role in ensuring information security is played by the state, which forms and implements a set of legal, organizational and institutional measures aimed at protecting information systems, digital networks and users from unauthorized access, data leakage, cyberattacks and other threats. This includes the development of legislative norms, security standards, the creation of specialized bodies and centers for

 DOI 10.34132/pard2026.31.05

cyber protection, as well as systems for monitoring and responding to information incidents [14; 16].

This problem is especially relevant in the field of healthcare, where the confidentiality of medical data, the protection of electronic medical records, ensuring the continuity and reliability of information systems are critically necessary for patient safety and the effectiveness of medical care. Information security in the medical sector, therefore, is not only a technical task, but also a strategic direction of state policy that determines the reliability and effectiveness of medical institutions, contributes to the protection of citizens' rights and ensures the stability of the national infrastructure in the context of digital transformation.

Taking into account these aspects allows the state to form an integrated system of information protection that covers legal, organizational, technical and educational components, providing a comprehensive approach to the security of the information environment and increasing the level of trust of citizens in digital services and state institutions.

Analysis of recent research and publications. The complexity of this issue requires an interdisciplinary approach, since information security encompasses legal, ethical, socio-psychological, communicative and technological aspects. An important role in the formation of modern approaches to the regulation of information security in the healthcare sector is played by the research of Ukrainian scientists – O. Mintser, Yu. Voronenko, L. Babintseva, M. Banchuk, V. Krasnov, V. Martsenyuk, S. Denysenko, O. Azarkhov, I. Shupyatsky, V. Yakobchuk, O. Ivanyuk, V. Krut and others. Their works are devoted to ensuring effective medical activity, protecting patients' personal data, adhering to ethical principles and improving state regulation of information security in the medical industry.

Formulation of the purpose of the article (task statement). The purpose of the article is to substantiate the features of information security in the healthcare sector.

Presentation of the main material of the study. The safe operation of information systems in the healthcare sector and related medical institutions is possible only with a comprehensive and systematic approach to information security management. This approach involves the integration of organizational, technical, programmatic, legal

and educational measures that together ensure reliable protection of information resources (Fig. 1). Its effectiveness depends on the coordinated interaction of all stakeholders, including government agencies, the administration of medical institutions, IT departments and personnel who directly work with medical information.

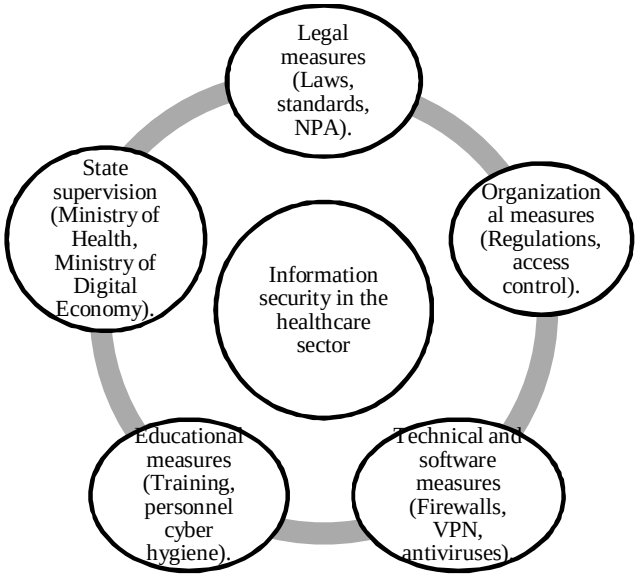

Fig. 1. A comprehensive approach to information security in medicine
Source: compiled by the author

Modern areas of cybersecurity in the healthcare sector cover several key aspects:

– Protecting data integrity – ensuring that medical information is not subject to unauthorized changes, loss or distortion, which is critical for the correct diagnosis and treatment of patients.

– Ensuring confidentiality – controlling access to information in such a way that only authorized persons have the right to view and use medical data, which allows you to protect patients' personal data and meet legal requirements.

 DOI 10.34132/pard2026.31.05

– Maintaining the availability of systems and data – ensuring the uninterrupted operation of medical IT systems even after technical failures, software errors or cyberattacks, which is critically important for the continuous provision of medical services and rapid response to emergencies [7].

The implementation of these areas involves the implementation of comprehensive measures, such as modernization of IT infrastructure, the use of modern systems for protection against cyberattacks, ongoing training of personnel, the development and application of regulatory documents and security standards, as well as regular monitoring and auditing of information systems. Such an integrated approach allows not only to minimize the risks of data leakage or loss, but also to increase citizens' trust in digital medical services and ensure the stability of the entire healthcare system.

Medical data is classified as particularly sensitive information, as it contains personal and confidential information that is subject to medical confidentiality. Reliable protection of such data is critically important, as its unauthorized disclosure can harm both the patient himself – violating his right to confidentiality and security – and the medical institution, which can lead to legal, financial and reputational losses.

A feature of medical information is that the patient has the right to independently control its disclosure, determine what information can be transferred to third parties, and also provide consent for data processing only to specific specialists. In addition, medical data requires operational processing and quick access for doctors, nurses and other authorized specialists in the process of providing medical services. These requirements significantly increase the risks of unauthorized access and abuse, since even temporary failures or insufficient level of protection of information systems can lead to critical consequences for the patient and the safe functioning of the medical institution.

Therefore, protecting medical data requires a comprehensive approach that combines technical encryption, access control, user activity monitoring, legal mechanisms, and staff training in confidentiality and information security. Only the integrated application of these measures can minimize the risks of data leakage, loss, or corruption and ensure the reliability and security of modern medical information systems.

It is worth emphasizing the important role of the state in the processes of digitalization of the healthcare sector, since it is it that forms the appropriate regulatory framework, establishes data protection standards, monitors compliance with established legal norms and coordinates the work of participants involved in medical data. In Ukraine, these functions are carried out by the State Service for Special Communications, the Ministry of Health and the Ministry of Digital Affairs, which develop requirements for medical IT systems, support the development of eHealth and regulate the secure operation of state registries [9]. The state should also ensure the training of specialists in medical cybersecurity, create cyber incident response centers and increase the level of information culture of medical workers. Examples of cyber attacks on hospitals in the world confirm that effective protection is possible only at the state level. Therefore, the implementation of a comprehensive approach to security in the healthcare sector should maximally combine legislative regulation, modern technologies and personnel training. It is this approach that will provide the optimal combination of legislative regulation, modern technologies and personnel training. Such systematic work will ensure reliable protection of medical data, stable functioning of information systems and patient safety. However, it is worth emphasizing the presence of another problem in the formation of a generally accepted approach to information security in the healthcare sector, namely the heterogeneity of the digital infrastructure of medical institutions. Today, most of them have different levels of technical support, using incompatible systems and programs that differ in scale, activity profile and form of ownership, which significantly complicates the implementation of centralized security standards.

Additional complexity in ensuring information security in the healthcare sector is created by the varying levels of staff training in working with digital technologies. In many healthcare institutions, specialists do not have sufficient knowledge and skills in the field of cybersecurity, which significantly increases the risk of human error, accidental disclosure of confidential data or violations of security procedures. Small hospitals and outpatient clinics often lack IT departments capable of responding promptly to information incidents,

 DOI 10.34132/pard2026.31.05

which makes these institutions particularly vulnerable to cyberattacks and technical failures.

The most common information security breaches in healthcare institutions include:

– Breach of confidentiality – leakage of personal data due to hacker attacks, social engineering or staff negligence;

– Unauthorized access to databases – access by persons without appropriate rights to medical information;

– Data loss – due to damage to media, server failures or incorrect backups;

– Information corruption – incorrect or altered information that can affect diagnosis, treatment planning, and clinical decisions;

– System outage – inability to access electronic medical records, which complicates the provision of medical care in critical situations;

– System malfunction – failure due to viruses, malware, or errors during updates [4].

These problems emphasize the need for a systemic approach to cybersecurity in medicine, which includes not only technical and software measures, but also staff training, the creation of clear regulations and incident response protocols, as well as constant auditing and monitoring of information systems. Only the comprehensive implementation of such measures allows minimizing risks and ensuring the reliability, security, and continuity of medical IT systems.

A striking example of the consequences of insufficiently protected medical IT systems was the WannaCry cyberattack in the United Kingdom in 2017. During this attack, the work of many hospitals was practically paralyzed: access to electronic medical records was lost, medical services were suspended, and staff were forced to switch to manual documentation. This case clearly demonstrated the global vulnerability of medical information systems and showed that even highly developed government institutions can suffer serious consequences from cyberattacks if comprehensive data protection and the continuity of critical systems are not ensured [13].

In this context, the state plays a decisive role, forming a unified cybersecurity policy for medical institutions and coordinating its

implementation at the national level. The state initiates the development of unified standards for the protection of information systems, the creation of centralized backup systems, certification of medical platforms and monitoring compliance with security requirements [1].

In Ukraine, cybersecurity issues are regulated on the basis of the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine» and a number of by-laws relating to the protection of personal data and critical infrastructure. This activity is coordinated by the Ministry of Health, the Ministry of Digital Transformation and the State Service for Special Communications and Information Protection, which provide methodological support to medical institutions, conduct regular checks of the state of information security, as well as train personnel on cyber hygiene and data protection [11].

Such a state approach allows for the creation of a unified cyber defense system that combines regulatory, organizational, and technical measures, increasing the resilience of medical institutions to cyberattacks, minimizing the risks of data leakage, and ensuring the continuous and secure functioning of medical IT systems.

To effectively ensure information security in the healthcare sector, a comprehensive approach is needed that combines technical, organizational, legal and educational measures, as well as provides for effective coordination at the state level. The following are the main areas and recommendations for protecting medical information systems:

1. Physical security:

– control of access to server rooms and rooms with medical equipment;

– video surveillance and electronic perimeter control;

– restriction of access by unauthorized persons;

– keeping a log of personnel accesses.

These measures help prevent theft of information carriers, unauthorized connection of devices and interference with equipment operation.

2. Network security:

– use of firewalls, intrusion detection and prevention systems (IDS/IPS), virtual private networks (VPN);

 DOI 10.34132/pard2026.31.05

– regular software updates;

– network segmentation to separate patient data and administrative information.

This ensures that systems continue to function smoothly even in the event of a cyberattack or unauthorized access attempts.

3. Password management and authentication:

– A policy of using complex, unique and regularly changed passwords across all key systems and applications;

– Implementing two-factor authentication (2FA) for access to eHealth systems and employee accounts.

4. Access control:

– Applying the principle of least necessary access for employees;

– Profiling users by roles and responsibilities;

– Using one-time access scripts or authorized remote intervention when necessary.

5. Personal responsibility and training:

– Continuously educating staff on cyber hygiene and digital literacy;

– Conducting training, cyberattack simulations, and briefings on secure data handling;

– Establishing non-disclosure agreements to ensure accountability for each employee [5; 12].

The comprehensive implementation of these measures allows to increase the level of protection of medical information systems, minimize the risks of data leakage or distortion, ensure the continuous operation of the digital infrastructure of medical institutions and create conditions for the safe provision of medical services (Table 1).

The state plays a key role in ensuring the consistency and unity of approaches to the implementation of information security recommendations in the healthcare sector. It forms and implements regulatory acts and standards, carries out security audits of medical information systems and finances projects to modernize digital infrastructure. For example, the Ministry of Health of Ukraine, together with the Ministry of Digital Transformation and the State Service for Special Communications and Information Protection, are implementing

cyber security standards in the eHealth system, which ensures the secure exchange of medical data between hospitals, pharmacies and state registries [6].

Table 1

Key aspects of medical data protection

Aspect (CIA Triad)	Description in the medical field	Risks of violation
Confidentiality	Description in the medical field Risks of violation Confidentiality Access to data (medical confidentiality) only to authorized persons.	Leakage of diagnoses, personal data, lawsuits.
Integrity	Protection of data from unauthorized modification or deletion.	Errors in diagnosis due to distortion of medical history.
Availability	Uninterrupted operation of the MIS and access to cards in 24/7 mode.	Paralysis of hospital work (as in the WannaCry attack).

Source: compiled by the author

This approach allows creating a unified cyber security system that combines legal, organizational and technical measures, increases the resilience of medical institutions to cyber attacks and reduces the risks of loss or compromise of confidential patient data, ensuring the continuous and secure functioning of the digital medical infrastructure.

Informatization of the healthcare sector is closely related to the implementation of medical information systems (MIS), which automate the work of medical and preventive institutions through a comprehensive combination of information, organizational, software and technical means. MIS covers a wide range of data, including financial, administrative and organizational information, electronic medical records of patients, results of laboratory and instrumental studies, as well as tools for monitoring the condition of patients and treatment processes.

 DOI 10.34132/pard2026.31.05

The main goals of implementing MIS are to improve the quality of medical care, minimize errors in documentation, ensure quick and convenient access to large volumes of data, as well as reliable protection of patients' personal data (Fig. 2). The implementation of such systems contributes to the optimization of management processes in medical institutions, increase the efficiency of staff work and create conditions for the safe and controlled exchange of medical information between different departments and healthcare institutions [10].

During the implementation of medical information systems (MIS), numerous risks arise that can negatively affect their security, reliability and efficiency of functioning. The main risk factors include:

– the use of common operating systems (OS) and database management systems (DBMS), which makes the system vulnerable to known vulnerabilities and cyberattacks;

– users working in open or insufficiently protected network segments, which increases the likelihood of unauthorized access;

– access to MIS via the Internet, in particular when providing telemedicine services, which creates additional entry points for potential attacks;

– administration of MIS in a shared IT infrastructure, which complicates the control and isolation of critical data;

– threats from malicious software (viruses, Trojans, encryptors) and loss or compromise of access keys [8].

Taking these risks into account at the MIS implementation stage is critically important to ensure the security of medical data, the reliability of information systems and patient safety, as well as to minimize the potential consequences of technical failures or cyber incidents.

State support plays a key role in minimizing risks during the implementation and operation of medical information systems (MIS) (Table 2). It is implemented through a set of measures that include establishing uniform standards for protecting information systems, financing modern secure IT solutions, monitoring compliance with cybersecurity requirements, as well as training and advanced training of medical informatics specialists.

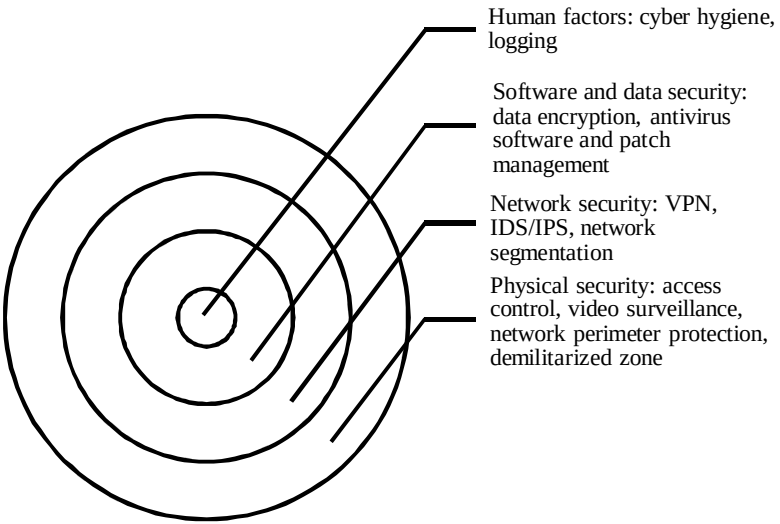

Fig. 2. Medical information system protection levels
Source: compiled by the author

Table 2

Medical Information System (MIS)

Protection Levels	Protection Level	Tools Goal
Physical	ACS, video surveillance	Preventing equipment theft
Logical (Network)	Firewall, VPN, segmentation	Protection from hacker attacks
Software	RBAC, 2FA, Encryption	Protecting the confidentiality of records
Organizational	Training, audits, backups	Minimizing the «human factor»

Source: compiled by the author

DOI 10.34132/pard2026.31.05

Thanks to such state support, a reliable and secure information environment is formed that provides comprehensive protection of patients' personal data, reduces the likelihood of cyberattacks and accidental loss of information, and also guarantees uninterrupted and efficient operation of MIS. In addition, centralized state measures contribute to the unification of rules and procedures in various medical institutions, increase the level of responsibility of staff for observing cyber hygiene, and create the basis for the further development of the digital infrastructure of healthcare in the conditions of rapid informatization and global cyber threats.

To ensure reliable protection of medical information systems (MIS), it is recommended to implement a layered approach to security, which combines technical and organizational measures and allows to minimize the risks of unauthorized access, the impact of malicious software and violation of data integrity.

The main measures of such protection include:

– implementation of strong passwords and strict user account management policies;

– creation of demilitarized zones (DMZ) and network perimeter protection to limit external access;

– use of firewalls to isolate the local network from the Internet;

– restriction of Internet access where possible and appropriate;

– implementation of intrusion detection and prevention systems (IDS/IPS);

– regular analysis of network traffic and event logs for timely detection of potential threats [2].

Layered protection allows to implement the principle of multi-layered security, when the absence or breach of one level does not lead to complete compromise of the system. This approach is critically important for healthcare institutions where ensuring the confidentiality, integrity, and availability of patient data is of paramount importance.

Antivirus software is not a universal means of information security due to a number of limitations. These include: a possible decrease in system performance, false positives and accidental quarantine of clinical data, as well as the potential vulnerability of the antivirus software itself to attacks. In addition, the effectiveness of such protection depends on regular updates of signature databases and software components.

State support minimizes these risks by establishing unified protection standards, financing secure IT solutions, monitoring compliance with cybersecurity, and training medical informatics specialists. This ensures a reliable information environment, protection of patients' personal data, and uninterrupted operation of MIS (Table 3).

Table 3

Problems of digitalization of medicine and the role of the state

Identified problem	Consequences	The role of the state in solving
Infrastructure heterogeneity	Incompatibility of systems, complexity of updates.	Implementation of unified standards and certification of MIS.
Low cyber literacy	Human errors, password leakage.	Training programs, certification of specialists.
Lack of IT departments	Slow response to incidents.	Creation of centralized threat monitoring centers.
Threats of malicious software	Data loss, service shutdown.	Financing of licensed software and development of security regulations.

Source: compiled by the author

Government support is critically important and necessary to ensure the reliable functioning of medical information systems (MIS) and minimize cyber risks. It includes the following key areas:

– Development and implementation of cybersecurity standards for MIS, which unifies the requirements for protecting information systems in all medical institutions;

– Financing licensed software and timely updates, which guarantees the relevance of protection tools and their effectiveness;

– Monitoring compliance with security requirements, including regular audits and inspections of medical institutions;

– Training and certification of medical informatics and cybersecurity specialists, which ensures competent management of

 DOI 10.34132/pard2026.31.05

information systems and an appropriate level of cyber hygiene of personnel;

– Creation of centralized threat monitoring and incident response services, which allows for the prompt detection of potential attacks and minimizing the consequences of cyber incidents [3].

The implementation of these state measures forms a comprehensive cyber defense system, increases the resilience of medical institutions to cyberattacks and technical failures, ensures secure data exchange between various units and healthcare institutions, and guarantees the protection of patients' personal data.

By implementing comprehensive information security measures that integrate technical, organizational, legal, and educational tools, the healthcare sector as a whole, as well as individual medical institutions, can effectively ensure comprehensive protection of patients' personal data. This includes ensuring the integrity, confidentiality, and availability of medical information, preventing cyberattacks, malware, and other threats to information security, and maintaining the smooth and stable operation of medical information systems (MIS).

The implementation of such measures allows not only to reduce the risks of data leakage or corruption, but also to increase the efficiency of management and clinical processes in medical institutions. As a result, timely access to the necessary information is ensured for specialists, staff work is optimized, and administrative errors are reduced. In addition, reliable information protection significantly increases the level of patient trust in medical institutions and healthcare systems as a whole, which is critically important in today's digital environment, where the volume and significance of medical data is constantly growing.

Conclusions. Thus, in modern conditions of operation of medical equipment and information technologies, the characteristics and functional capabilities of medical information systems (MIS) are constantly changing not only under the influence of technical progress, but also due to the constant updating of the regulatory framework, standards and recommendations in the field of healthcare. This creates a need for regular review of all information security measures and policies, a comprehensive internal and external assessment of the state of data

protection, as well as timely implementation of technological updates, patches, software improvements and equipment modernization.

A critically important element of an effective information security system is proper training of personnel and their active participation in information protection processes. The competence of employees, their awareness of possible cyber threats and a deep understanding of the principles of cyber hygiene directly affect the real level of data protection, the stability and reliability of the functioning of the MIS, as well as the continuity of medical services. Lack of trained personnel or insufficient level of their awareness can significantly increase the risks of information leakage or compromise, even with the presence of modern technical protection tools.

Only an integrated combination of modern technologies, updated regulatory and legal requirements, centralized control procedures and a high level of professional staff is able to ensure stable, reliable and secure operation of the digital infrastructure of healthcare institutions. Such an approach not only guarantees the protection of patients' personal data and maintains the continuity of medical services, but also contributes to improving the quality of medical care, optimizing clinical and administrative processes and strengthening patients' trust in the healthcare system in the conditions of rapid informatization and the growth of global cyber threats.

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СФЕРІ ОХОРОНИ ЗДОРОВ›Я

У статті досліджено роль інформаційної безпеки в охороні здоров'я в умовах активної цифровізації медичних процесів. Показано, що впровадження електронних медичних карток, телемедицини та автоматизованих систем управління підвищує не лише якість надання медичних послуг, ефективність роботи закладів і доступність медичної допомоги, але й створює нові ризики витоку, модифікації або спотворення чутливої інформації, що потребує особливої уваги до кіберзахисту та стандартизації інформаційних процесів.

 DOI 10.34132/pard2026.31.05

Розкрито особливості медичної інформації, яка характеризується високою конфіденційністю, точністю та критичністю для життя і здоров'я пацієнтів. Наголошено на необхідності належного захисту даних для запобігання помилкам у діагностиці, неправильному лікуванню, порушенню етичних стандартів та втраті довіри пацієнтів до медичних установ. Особлива увага приділяється захисту персональних даних і забезпеченню цілісності медичних записів у цифровому середовищі.

Розглянуто основні напрями організації інформаційної безпеки в медичних закладах: багаторівнева аутентифікація, контроль доступу, резервне копіювання, шифрування даних та захист персональних даних. Визначено ключові загрози для медичних інформаційних систем – кібератаки, фішинг, шкідливе програмне забезпечення, технічні збої та людський фактор, які вимагають комплексного підходу до управління ризиками та інтеграції технологічних, організаційних і нормативних заходів.

На основі проведеного аналізу сформульовано практичні рекомендації щодо підвищення рівня інформаційної безпеки: удосконалення політики захисту даних, застосування сучасних технологій шифрування та безпечного зберігання інформації, постійний моніторинг роботи систем, створення внутрішніх протоколів реагування на інциденти, впровадження багаторівневої автентифікації користувачів та регулярне навчання персоналу з питань кібербезпеки. Виконання цих заходів забезпечує стабільну, надійну та безпечну роботу медичних інформаційних систем, підвищує ефективність функціонування медичних закладів і зміцнює довіру пацієнтів до сучасної цифрової охорони здоров'я.

Ключові слова: *інформація, інформаційна безпека, сфера охорони здоров'я, цифровізація, кібератака*

References

1. Hromadska, N., Andriiash, V. (2020). Efektyvnist pryiniattia derzhavno-upravlinskykh rishen: osoblyvosti vykorystannia politychnoho analizu [The effectiveness of state management decision-making: features of

the use of political analysis]. *Publichne upravlinnia ta rehionalnyi rozvytok.* № 8. Retrieved from https://doi.org/10.34132/PARD2020.08.05 [in Ukrainian].

2. Hulchak, Yu. P. (2020). Zakhyst informatsiinykh resursiv medychnykh informatsiinykh system [Protection of information resources of medical information systems]. Informatsiini tekhnolohii: nauka, tekhnika, tekhnolohiia, osvita, zdorovia : tezy dop. KhXVIII mizhnar. nauk.-prakt. konf. MicroCAD-2020, (Kharkiv, 28-30 zhovt. 2020 r.) : u 5 ch. / za red. prof. Sokola Ye. I. Kharkiv : NTU «KhPI». Ch. 2. Retrieved from https://dspace.vnmu.edu.ua/123456789/5033 [in Ukrainian].

3. Dolbnieva, D. V., Honcharuk, S.M. (2016). Neobkhidnist ta osnovni napriamky vdoskonalennia poriadku formuvannia ta vykorystannia resursnoho potentsialu okhorony zdorovia v Ukraini [The need and main directions for improving the procedure for the formation and use of health care resource potential in Ukraine]. *Problemy ekonomiky*. № 3. Retrieved from http://nbuv.gov.ua/UJRN/Pekon_2016_3_7. [in Ukrainian].

4. Kiberbezpeka v medytsyni: chomu likarni staly uliublenoiu mishenniu khakeriv (2025). [Cybersecurity in medicine: why hospitals have become a favorite target of hackers] Retrieved from https://datami.ee/ua/blog/cybersecurity-in-healthcare/ [in Ukrainian].

5. Kobrusieva, Ye. A. (2025). Informatsiina bezpeka elektronnykh system okhorony zdorovia: teoretychni ta praktychni aspekty [Information security of electronic health care systems: theoretical and practical aspects]. *Yurydychnyi naukovyi elektronnyi zhurnal.* № 1. Retrieved from https://doi.org/10.32782/2524-0374/2025-1/69 [in Ukrainian].

6. Kupershtein, L.M., Yasinska, Ya.O. (2025). Doslidzhennia polityky informatsiinoi bezpeky u rozrizi normatyvnoi dokumentatsii [Research on information security policy in the context of regulatory documentation]. Retrieved from https://doi.org/10.31891/2219-9365-2021-68-2-4 [in Ukrainian].

7. Liashuk, A. (2023). Zahrozy i vyklyky dlia systemy kiberbezpeky informatsiinykh system ta reiestriv sfery okhorony zdorovia [Hreats and challenges for the cybersecurity system of information systems and registries in the healthcare sector]. *Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia.* № 6. Retrieved from https://doi.org/10.31470/2786-6246-2023-6-113-121 [in Ukrainian].

8. Mintser, O. P., Voronenko Yu. V., Babintseva, L. Yu., Banchuk, M. V., Krasnov, V. V., Martseniuk, V. P., Denysenko, S. V., Azarkhov, O. Yu., Shupiatskyi, I. M. (2012). Kontseptsiia informatyzatsii okhorony zdorovia Ukrainy [Concept of healthcare informatization in Ukraine]. *Medychna*

informatyka ta inzheneriia. № 3. Retrieved from http://nbuv.gov.ua/UJRN/Mii_2012_3_3 [in Ukrainian].

9. Mintsyfra ta Derzhspetszviazku vdoskonaliuiut sferu informatyzatsii (2025). [The Ministry of Digital and the State Service for Special Communications Improve the Sphere of Informatization]. Retrieved from https://thedigital.gov.ua/news/technologies/mintsifra-ta-derzhspetszvyazku-vdoskonalyuyut-sferu-informatizatsii [in Ukrainian].

10. Nazirova, T. O., Kostenko, O. B. (2017). Ohliad modelei rozvytku eHealth ta naiavnykh medychnykh informatsiinykh system. Problemy stvorennia yedynoho medyko-informatsiinoho prostoru [Review of eHealth Development Models and Existing Medical Information Systems. Problems of Creating a Unified Medical Information Space]. *Naukovyi visnyk NLTU Ukrainy*. Vyp. 27(10). Retrieved from https://doi.org/10.15421/40271027 [in Ukrainian].

11. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 05.10.2017 № 2163-VIII [On the Basic Principles of Ensuring Cybersecurity in Ukraine: Law of Ukraine] Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

12. Iakobchuk, V., Ivaniuk, O., Krut, V. (2024). Upravlinnia informatsiinymy tekhnolohiiamy v sferi okhorony zdorovia v umovakh voiennoho stanu [Management of Information Technologies in the Sphere of Healthcare under Martial Law]. *Ekonomichnyi prostir.* № 195. Retrieved from https://doi.org/10.30838/EP.195.193-200 [in Ukrainian].

13. Wanna Cry: zapytannia i vidpovidi pro hlobalnu kiberataku (2024). [WannaCry: Questions and Answers about the Global Cyberattack]. Retrieved from https://www.dw.com/uk/wannacry-%D0%B7%D0%B0%D0%BF%D0/a-38830357 [in Ukrainian].

14. Natalia Dragomyretska, Yuliana Palagnyuk, Victoria Andriyash, Iryna Matvieienko, Dmytro Samofalov (2022). The introduction of modern technologies in public administration in the context of globalization. *International journal of computer science and network security.* vol. 22. no. 2. pp. 334-340 https://doi.org/10.22937/IJCSNS.2022.22.2.42 [in English].

15. Budzin, V., Shtyrov, O. (2023). Administratyvno-pravovi ta instytutsiini aspekty kontroliu ta nahliadu v realizatsii derzhavnoi polityky okhorony zdorovia na suchasnomu etapi transformatsii. [Administrative-legal and institutional aspects of control and supervision in the implementation of the state policy of health protection at the current stage of transformations]. *Publichne upravlinnia i administruvannia v Ukraini. Vyp. 38.* Retrieved from: https://doi.org/10.32782/ pma2663-5240-2023.38.7 [in Ukrainian].

16. Myroslav Kryshtanovych, Viktoria Andriyash, Hanna Bondar, Yuriy Kushnir, Kateryna Ozarko (2022). Public Administration Mechanisms for Ensuring Cybersecurity in Modern Conditions of Socio-Economic Development. *International journal of computer science and network security*. vol. 22. no. 3. pp. 606-610 https://doi.org/10.22937/IJCSNS.2022.22.3.79 [in English].

Відомості про автора / Information about the Author

Чжао Чженьї, аспірант кафедри публічного управління та адміністрування, юридичного факультету Чорноморського національного університету імені Петра Могили, м. Миколаїв, Україна. orcid: https://orcid.org/0009-0006-7030-2479

Zhao Zhenyi, PhD Student at the Department of Public Management and Administration, Faculty of Law, Petro Mohyla Black Sea National University, Mykolaiv, Ukraine. orcid: https://orcid.org/0009-0006-7030-2479

Zhao Zhenyi, (2026). Features of information security in the healthcare sector. Public Administration and Regional Development, 31, 109-128. https://doi.org/10.34132/pard2026.31.05