TSARKA SCIENCE

Volume 1 (2026)
Issue 1

ANALYSIS AND FORECASTING OF INFORMATION SECURITY THREATS IN MEDICAL SYSTEMS

I. Uvaliyeva[1]*, A. Zeken[2]

[1]D. Serikbayev East Kazakhstan Technical University, Oskemen, Kazakhstan

[2]D. Serikbayev East Kazakhstan Technical University, Oskemen, Kazakhstan

*Corresponding author: indirauvalieva@gmail.com.

Abstract

This article comprehensively examines the issues of analyzing and predicting dangerous situations in medical systems. Currently, the rapid development of digitalization and information technologies in healthcare organizations poses new challenges to security. The close interrelationship of cyber threats, human factors, organizational management, and regulatory aspects requires a comprehensive assessment and prediction of risks in medical systems. The authors considered the classification of threats, their causes and consequences, as well as methods for managing threats. Based on international and domestic research, the possibilities of predicting threats using machine learning and big data were analyzed. The current situation in the healthcare sector in Kazakhstan was compared with international experience, and effective ways to manage threats at the national level were proposed. The need for transcultural adaptation of tools for assessing safety culture was also noted. As a result, integrated approaches to risk management in medical systems have a positive impact on patient safety and organizational stability. The conclusion provides specific recommendations for reducing risks and increasing patient safety in healthcare.

Keywords: *Medical systems, risk analysis, cybersecurity, human factors, management, data privacy, modelling, probability, healthcare, risk prediction.*

1. Introduction

Currently, the rapid development of medical systems and the digitization of healthcare have become pressing areas of research on a global scale. The increasing complexity of information technologies in the medical field necessitates a comprehensive approach to protecting patient data, enhancing the efficiency and safety of medical processes, and addressing organizational management aspects [1]. Researchers pay

special attention to the potential risks of cybersecurity threats and human factors in healthcare systems, as any error or vulnerability can directly impact patients' lives and health.

Analyzing and forecasting risks related to the development of information technologies in medical organizations is fundamental to ensuring the stability and security of healthcare systems. According to recent studies, cybersecurity incidents and organizational errors in healthcare institutions have resulted in significant financial and moral losses. The World Health Organization (WHO) reports a steady increase in the number of cyberattacks in the medical sector each year, highlighting the importance of thoroughly studying healthcare systems and improving integrated protective measures. Over the last few years, the proliferation of medical information systems that process large volumes of data (Big Data) and the growing prevalence of Internet of Medical Things (IoMT) devices connected to networks have contributed to increased risks [2]. Healthcare organizations in Kazakhstan have also been affected by this trend, creating a growing need for strategic management of medical system security.

The aim of the study is to provide a comprehensive analysis of threats to medical systems and to propose scientifically based measures to predict these threats.

2. Material and research methods

Over the past decade, cybersecurity in healthcare has become an intensively studied field. For example, Nifakos S., Chandramouli K., Nikolaou C. K., Papachristou P., Koch S., Panaousis E., and Bonacina S. [1] demonstrated the significant influence of human factors on organizational cybersecurity in their systematic review. They identified poorly designed training programs, non-compliance with data security protocols, and social engineering attacks as key contributors to vulnerabilities. Darwish A., Hassanien A. E., Elhoseny M., Sangaiah A. K., and Muhammad K. [2] analyzed the integration of Internet of Things (IoT) and cloud computing technologies in healthcare, emphasizing both their innovative potential and the risks they introduce. While connected device systems have streamlined hospital infrastructure, they have also increased the likelihood of data breaches.

In Kazakhstan, studies have highlighted shortcomings in the protection of automated healthcare systems. Alimzhanova Zh. M. and Baiyuzakova A. K. [3] identified insufficient safeguards in these systems and emphasized the necessity for robust cybersecurity measures. Similarly, Askar A. J. [4] pointed out that aligning cybersecurity with information management practices ensures the seamless functioning of healthcare institutions.

Kalibekov A. T. [5] discussed strategies for the development of Kazakhstan's healthcare sector, underscoring the critical role of organizational management. Podrecca M., Culot G., Nassimbeni G., and Sartor M. [6] demonstrated that implementing in-

ternational standards like ISO/IEC 27001 enhances both operational efficiency and financial performance. Additionally, Elizabeth M. J., Jobin J., and Dona J. [7] proposed a fog-based security model to strengthen the protection of electronic medical records (EMRs) and elevate system-wide security.

Edemekong P. F., Annamaraju P., and Haydel M. J. [8] emphasized the need for legislative measures similar to HIPAA regulations in countries outside the United States, advocating for their role in minimizing legal risks associated with data breaches. Russian researchers Sotskova S. I. and Emelyanov A. A. [9] suggested adapting enterprise-level risk analysis methods for use in medical organizations to ensure sustainable development.

Further studies by Uspanova K. T., Oshakbayev T. Zh., Kamaliev M. A., Kadyrmanov N. M., Sabanbayev Z. A., and Iksanov R. I. [10] described the successful implementation of mobile medical complexes in military healthcare units, noting that challenges such as insufficient staffing and inadequate training increase overall risks. Rao A., Carreón N., Lysecky R., and Rozenblit J. [11] proposed probabilistic risk assessment models for cyber-physical medical systems, emphasizing the importance of continuous staff training, internal audits, and motivational programs to mitigate human error. Dorgushayeva A. K., Dovgal V. A., Kozlova N. Sh., and Kozlov R. S. [12] explored the use of machine learning technologies for real-time risk detection and prevention, ensuring rapid responses to critical incidents. Igoshina N. A., Sotskova S. I., and Kalashnikova I. V. [13] proposed a comprehensive methodology for assessing the quality of services in rehabilitation centers, contributing to the development of a risk management culture in the healthcare sector.

Calhoun B. C., Kiel J. M., and Morgan A. A. [14] examined legal risks associated with non-compliance with HIPAA regulations and proposed strategies to minimize these risks. Within the framework of Kazakhstan's national project «Healthy Nation» [15, 16], particular attention is paid to improving the accessibility and quality of medical care. However, these documents lack dedicated sections addressing comprehensive information security. Ito Sh., Kanako S., Kigawa M., Fujita Sh., and Hasagawa T. [17] analyzed tools for assessing patient safety culture (HSOPS), showing that combining governmental support with organizational culture significantly reduces risks. Jalali M. S., Razak S., Gordon W., Perakslis E., and Madnick S. [18] conducted a bibliometric analysis of medical cybersecurity literature, highlighting the rapid growth of this field and emphasizing the critical importance of protecting data collected via Big Data, telemedicine, and wearable devices.

The classification of risks in medical systems is presented in Figure 1.

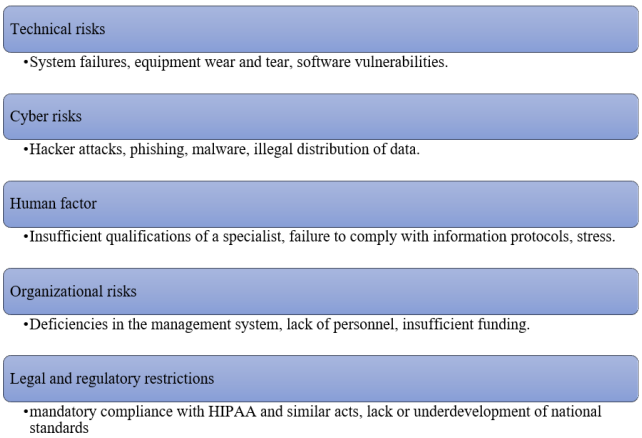

Figure 1. The classification of risks in medical systems

Most of these risks are interdependent and therefore cannot be solved by a single technical method. At the same time, the human factor, culture within the organization, and legislative support are becoming the main factors determining the stability of any organization.

This study used a comprehensive methodological framework to analyze risks in healthcare systems and propose effective management strategies. A comparative analysis was conducted to identify similarities and differences between global and Kazakhstani studies on risk management in healthcare systems. This analysis focused on:

- Methodologies applied in foreign and local studies.
- Adaptability of international practices, such as ISO/IEC 27001 and HIPAA, to the healthcare context of Kazakhstan [19].
- Identification of approaches suitable for implementation in domestic healthcare organizations.

This step identified the specific challenges faced by the healthcare sector in Kazakhstan and served as a basis for developing targeted recommendations. Various analytical methods were used to assess and predict risks, including:

- Failure Mode and Effect Analysis (FMEA): used to identify potential vulnerabilities and assess their impact on operational processes.
- Markov Chains: used to model changes in system states over time, helping to predict long-term reliability.
- Monte Carlo simulation: used to analyze complex scenarios and estimate risk probability in multivariable systems.
- Machine learning models: classifiers and neural networks were implemented to

process large data sets and improve the accuracy of risk predictions.

All research activities followed ethical standards to ensure the confidentiality of patient and institutional data.

3. The results and discussion

According to the World Health Organization (WHO) 2024 data, the number of threats to healthcare facilities has increased significantly in recent years. These threats include cyberattacks, information system vulnerabilities, human error, natural disasters, and changing regulatory requirements. The research findings indicate that the majority of threats in medical systems are associated with cyberattacks. Phishing and ransomware attacks have a direct impact on data security within organizations, potentially leading to financial losses and reputational damage. Insider threats should be mitigated through strengthened internal monitoring and by enhancing employees' proficiency in information security. To minimize software vulnerabilities, it is essential to regularly update systems, implement patches in a timely manner, and utilize modern antivirus solutions. Furthermore, continuous employee training and the development of a strong cybersecurity culture enhance an organization's ability to withstand cyber threats.

In Table 1, the highest probability is associated with human error and phishing, as medical personnel often fail to adhere to information protocols or are susceptible to external manipulation. Consequently, the likelihood of data loss increases, leading to reputational damage for the organization. Although insider threats have a lower probability, their impact is significant due to the extensive access that internal personnel often possess. The analysis of the main threats to medical systems revealed that network attacks, human factor influence, software vulnerabilities, phishing attacks and insider threats have the highest risk. Although network attacks (DDoS, hacker attacks) have a medium probability, their impact is high, as they directly affect the availability of data and the operation of the system [20].

Table 1. Classification of major threats in medical systems and their probability and impact

Threat Type	Cause	Probability	Impact	Control Mechanism	Primary Risk
1	2	3	4	5	6
Network Attacks	Hacking, DDoS	Medium	High	Firewall, IPS, network monitoring	Data access compromise
Human Error	Employee mistakes	High	Medium	Regular training, internal audits	System errors
Software Vulnerabilities	Lack of system updates	Medium	High	Antivirus, patch management	Susceptibility to attacks

Table 2. Continued

1	2	3	4	5	6
Phishing and Social Engineering	Deception to obtain sensitive data	High	High	Employee training, anti-phishing systems	Theft of confidential data
Insider Threat	Deliberate actions by insiders	Low	Very High	Access policies, monitoring	Data breaches

Human error is one of the most common factors, which leads to system failures and violations of security protocols. Software vulnerabilities arise from the untimely introduction of updates, which increases the likelihood of attacks. Phishing and social engineering-based attacks are very common, their probability is high and can lead to data theft. Insider threats are rare, but their impact is very high, since deliberate actions by internal employees can lead to complete destruction or theft of medical data. To prevent these threats, it is necessary to strengthen system security, train employees and tighten security protocols.

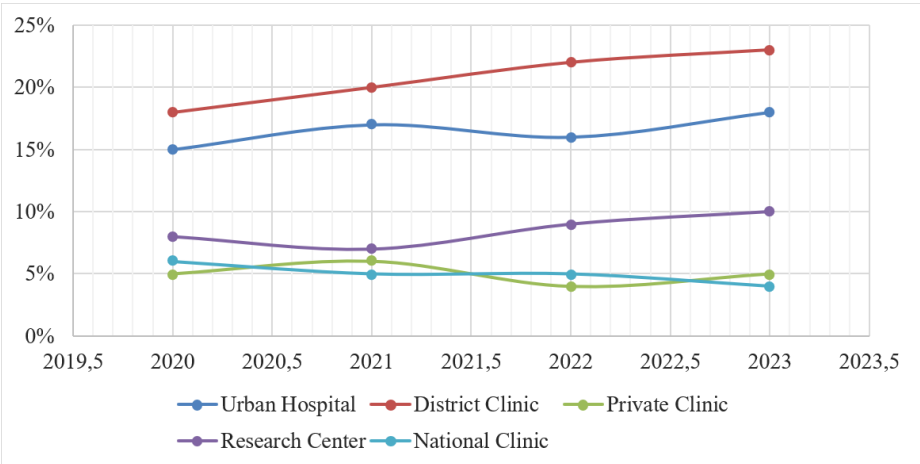

Figure 2. Percentage of Incidents Caused by «Human Error» (2020–2023)

Table 2 shows the distribution of the main threats to the healthcare system by probability and impact and highlights the most important vulnerabilities that require urgent attention and mitigation strategies. The Failure Mode and Effects Analysis (FMEA) method allows for the early identification of potential threats and their causes, but it is constrained by predefined probabilities and lacks complete accuracy in forecasting. The Markov Chain method enables tracking changes in the state of a system over time, but processing large datasets presents challenges. This method

is particularly effective in analyzing the reliability of medical equipment. The Monte Carlo method can simulate complex scenarios, but its calculations require significant computational resources. This approach is used for multi-scenario analysis. Artificial Neural Networks (ANNs) process large datasets and are capable of self-learning, yet they are difficult to configure. This method is widely applied in medical diagnostics and image recognition. Machine Learning (ML) offers fast computational capabilities and can handle various data streams, but achieving high efficiency requires a large dataset [21]. All these methods should be applied comprehensively for the analysis and forecasting of threats in medical systems.

Table 2. Comparative analysis of threat forecasting methods

Method Name	Advantages	Limitations	Application Area	Real-Time Capability	Model Complexity	Efficiency Level
FMEA	Early identification of root causes	Limited to probabilities	Operational processes	Medium	Low	High
Markov Chain	Tracks state changes over time	Difficult to process large data	Equipment reliability	High	Medium	Medium
Monte Carlo	Models' complex scenarios	Requires extensive computation	Multi-scenario analysis	Low	High	High
Neural Networks	Processes large datasets, self-learning	Challenging to configure	Diagnostics, image recognition	Medium	Very High	Medium
Machine Learning	Fast calculations, versatile	Requires sufficient data	Data stream monitoring	Medium	Medium	High

According to the data in Figure 3, the level of incidents due to employee errors is especially noticeable in urban hospitals and district clinics. This situation is caused by the fact that employees do not pay enough attention to confidentiality and information protocols. In addition, deception by external factors (giving passwords to outsiders, inadvertently opening phishing emails) is common. To reduce such errors, it is important to systematically train and increase information security literacy [22].

Figure 3 shows that phishing attacks are at a consistently high rate. Ransomware attacks are also on the rise, reaching 31% in 2023.

These figures underscore the need for healthcare organizations to improve their internal defense protocols. While the incidence of Insider Actions is relatively low, the consequences can be significant [23].

The research clearly showed the growing trend of the main threats in medical organizations. First, it was found that the human factor is more likely and has become the main source of danger (Figure 1). Here, staff training and information culture are of great importance. Secondly, the fact that phishing attacks prevail over other types of attacks (Figure 2) requires constant improvement of information security protocols and internal authorization mechanisms. Methods such as FMEA and Markov Chain allow for early identification of risks when assessing the reliability of operational processes and equipment.

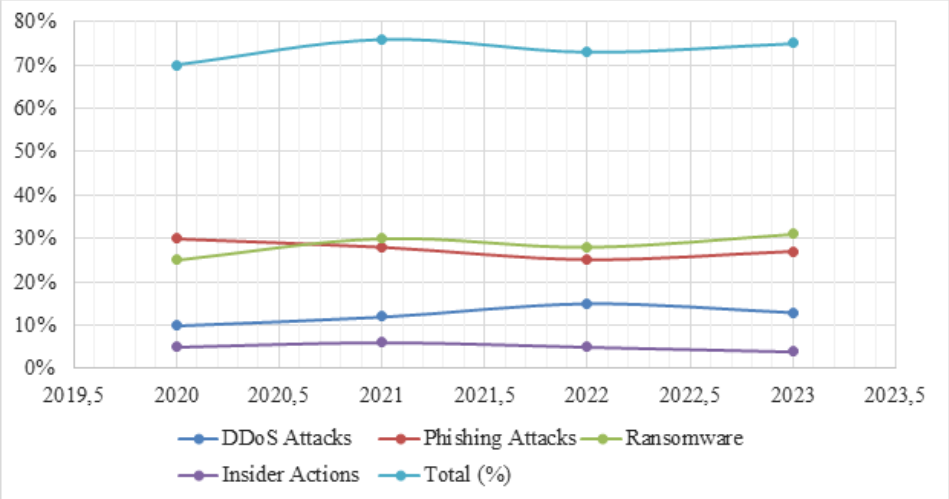

Figure 3. Types and Frequency of Cyberattacks (2020–2023)

However, the Monte Carlo model has limitations in real-time analysis, since it requires massive calculations based on several scenarios. Neural Networks and Machine Learning methods are considered indispensable tools for working with large amounts of data, but highly qualified specialists are required for their harmonious and effective configuration. Thanks to new technologies, IoMT (Internet of Medical Things) devices significantly improve the quality of medical care. However, the connection of such devices to the network multiplies the flow of information, which in turn is likely to lead to an increase in cyber threats. Therefore, there is a need to develop a comprehensive security strategy that includes both internal and external threats. Among the organizational measures, it is important to conduct regular training for employees, check the level of readiness through simulated attacks, and systematically conduct internal audits. At the same time, it is necessary to improve specific norms and rules that ensure the confidentiality of medical data from a legislative. In the Kazakhstani context, all cyber risk management systems for national

healthcare organizations should be regulated on a single platform, which will create a uniform approach to data exchange and threat prediction.

Within the framework of these measures, particular attention must be given to statistical modeling and Big Data analysis methods to ensure the stability of the information ecosystem. This approach enables the identification of previously unknown cyberattack patterns while simultaneously strengthening organizational preparedness at a strategic level. The analysis and forecasting of threats in medical organizations require a multifaceted and integrated approach: managing the human factor, monitoring new technologies, improving standards and regulations, and reinforcing the internal security culture of organizations. Only through the synergy of these efforts can the resilience of medical systems and the safety of patients be ensured.

4. Conclusion

In conclusion, the analysis and forecasting of threats in medical systems play a crucial role in modern healthcare. The findings of the conducted research indicate that the primary threats include network attacks, human factor vulnerabilities, software weaknesses, phishing attacks, and insider threats. Each of these threats directly impacts the stability of medical organizations, the confidentiality and integrity of data, and, most importantly, patient safety.

During the identification of effective methods for forecasting and managing risks, various mathematical models and machine learning technologies were applied. Machine learning models, such as classifiers and neural networks, were implemented to process large volumes of data and improve the accuracy of threat prediction. These methods help reduce the load on medical information systems and enable the early detection of potential attacks and vulnerabilities.

Based on the research conducted, the following recommendations are proposed to enhance the forecasting and management of threats in medical systems:

• Strengthening Information Security Protocols – To mitigate network attacks and cyber threats, the adoption of international standards such as ISO/IEC 27001 is necessary. This measure will enhance the protection of medical organizations' information systems.

• Employee Training and Promotion of an Information Security Culture – To reduce risks associated with the human factor, regular training sessions should be organized, and effective countermeasures against phishing attacks should be implemented.

• Integration of Machine Learning and Artificial Intelligence – The incorporation of machine learning models based on neural networks and classifiers in medical systems will improve the ability to detect threats in advance. This will enhance prediction accuracy and increase the reliability of information systems.

• Regular Software Updates – To minimize vulnerabilities, timely system updates and patch management are critical. This approach ensures the stable operation of the system and significantly reduces the likelihood of hacker attacks.

• Enhancing Access Control Policies – To prevent insider threats, it is essential to establish precise access levels within medical information systems, improve monitoring mechanisms, and implement advanced encryption methods for data protection.

To summarize, an integrated approach is necessary for effective threat management in medical systems. The implementation of machine learning technologies, the enhancement of cybersecurity protocols, and the improvement of employees' information security skills will significantly strengthen the security and reliability of medical organizations. These strategies will contribute to the protection of patients' personal data, the improvement of medical service quality, and the overall stability of healthcare information systems.

Financing. This research has been/was/is funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP19679525).

Conflict of interest: The authors declare that there is no conflict of interest.

References

1. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, 21(15), 5119. https://www.mdpi.com/1424-8220/21/15/5119
2. Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., & Muhammad, K. (2019). The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. Journal of Ambient Intelligence and Humanized Computing, 10, 4151-4166. https://link.springer.com/article/10.1007/s12652-017-0659-1
3. Alimzhanova ZH. M., Bayuzakova A. K. Problemy obespecheniya bezopasnosti avtomatizirovannykh sistem //Vestnik Universiteta Shakarima. Seriya tekhnicheskiye nauki. – 2023. – T. 1. – №. 4 (12). – S. 31-39. https://tech.vestnik.shakarim.kz/jour/article/-view/521
4. Askar, A. J. (2019). Healthcare management system and cybersecurity. International Journal of Recent Technology and Engineering, 237-248.
5. Kalibekov, A. T. (2022). Upravleniye razvitiyem sistemoy zdravookhraneniya v respublike Kazakhstan: sovremennoye sostoyaniye i perspektivy. Nauchnyye

issledovaniya: problemy i perspektivy v kontekste global'nykh vyzovov (37-41). https://elibrary.ru/item.asp?id=49591797

6. Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. Computers in Industry, 142, 103744. https://www.sciencedirect.com/science/article/pii/S0166361522001415
7. Elizabeth, M. J., Jobin, J., & Dona, J. (2019). A fog based security model for electronic medical records in the cloud database. International Journal of Innovative Technology and Exploring Engineering, 8 n.7, pp. 2552-2560
8. Edemekong P. F., Annamaraju P., Haydel M. J. Health insurance portability and accountability act. The American University in Cairo – 2018. https://europepmc.org/books/nbk500019
9. Sotskova S.I., Yemel'yanov A.A. Analiz predprinimatel'skikh riskov kak instrument obespecheniya ustoychivogo razvitiya khozyaystvuyushchego sub"yekta. Problemy razvitiya predpriyatiy: teoriya i praktika. 2018. № 3. S. 156-159. https://elibrary.ru/item.asp?id=36548001
10. Uspanova, K. T., Oshakbayev T. Dzh., Kamaliyev M. A., Kadyrmanov N. M., Sabanbayev Z. A., Iksanov R. YA. (2024). Opyt i praktika: vnedreniye mobil'nykh meditsinskikh kompleksov v voinskikh chastyakh Vooruzhennykh Sil Respubliki Kazakhstan. Medicine, Science and Education, (4), 58-75.
11. Rao, A., Carreón, N., Lysecky, R., & Rozenblit, J. (2017). Probabilistic threat detection for risk management in cyber-physical medical systems. IEEE Software, 35(1), 38-43. https://ieeexplore.ieee.org/abstract/document/8239935/
12. Dorgushaova, A. K., Dovgal', V. A., Kozlova, N. SH., & Kozlov, R. S. (2024). Obzor ispol'zovaniya tekhnologiy mashinnogo obucheniya v obespechenii informatsionnoy bezopasnosti dannykh: nastoyashcheye i budushcheye. Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Yestestvenno-matematicheskiye i tekhnicheskiye nauki, (1 (336)), 51-59.
13. Igoshina N.A.., Sotskova S.I., Kalashnikova I.V.Metodika kompleksnoy integral'noy otsenki kachestva uslug reabilitatsionnykh meditsinskikh tsentrov. Ekonomika i predprinimatel'stvo. 2023. № 5 (154). S. 1180-1184. Doi: 10.34925/eip.2023.154.5.236 https://elibrary.ru/item.asp?id=54073539
14. Calhoun B. C., Kiel J. M., Morgan A. A. Health insurance portability and accountability act violations by physician assistant students: applying laws to clinical vignettes. The Journal of Physician Assistant Education. – 2018. – T. 29. – №. 3. – C. 154-157. https://journals.lww.com/jpae/fulltext/2018/09000/Health_Insurance_Portability_and_Accountability.5.aspx
15. Ob utverzhdenii Natsional'nogo Proyekta «Kachestvennoye i dostupnoye zdra-

vookhraneniye dlya kazhdogo grazhdanina “Zdorovaya Natsiya”: utv. 12 oktyabrya 2021 goda, № 725. IPS «adílet» 2021, oktyabr’ – URL: https://adilet.zan.kz/rus/docs/P2100000725

16. Ob utverzhdenii Natsional’nogo Proyekta «Kachestvennoye i dostupnoye zdravookhraneniye dlya kazhdogo grazhdanina “Zdorovaya Natsiya”: utv. 12 oktyabrya 2021 goda, № 725. IPS «a dílet» 2021, oktyabr’ – 16. https://adilet.zan.kz/rus/docs/P2100000725
17. Ito S. et al. Development and applicability of hospital survey on patient safety culture (HSOPS) in Japan. BMC health services research. – 2011. – T. 11. – C. 1-7. URL: https://doi.org/10.1186/1472-6963-11-28 2019.
18. Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. Health care and cybersecurity: bibliometric analysis of the literature. Journal of medical Internet research. – 2019. – T. 21. – №. 2. – C. e12644. https://www.jmir.org/2019/2/e12644/
19. Ewoh P., Vartiainen T. Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. Journal of medical internet research. – 2024. – T. 26. – C. e46904.
20. Gasanova, Z. B., Dement’yeva, M. O., & Martynova, A. M. (2024). Primeneniye it-innovatsiy v sisteme zdravookhraneniya v usloviyakh tsifrovoy sredy. Redaktsionnaya kollegiya, 93 - 99.
21. Ishutina N. A., Andriyevskaya I. A., Prikhod’ko N. G. Novyy podkhod k otsenke reproduktivnykh poter’ pervogo trimestra beremennosti. Acta Biomedica Scientifica. – 2021. – T. 6. – №. 3. – S. 43-52.
22. Dias, F. M., Martens, M. L., Monken, S. F. de P., Silva, L. F., & Santibanez-Gonzalez, E. D. R. (2021, Jan./Apr.). Risk management focusing on the best practices of data security systems for healthcare. International Journal of Innovation - IJI, São Paulo, 9(1), 45-78. https://doi.org/10.5585/iji.v9i1.18246.
23. Koppel, R., & Kuziemsky, C. (2019). Healthcare data are remarkably vulnerable to hacking: Connected healthcare delivery increases the risks. Studies in Health Technology and Informatics, 218-222. doi:10.3233/978-1-61499-951-5-218

Information about authors

Uvaliyeva Indira Makhmutovna - PhD, D. Serikbayev East Kazakhstan Technical University.
e-mail: indirauvalieva@gmail.com
ORCID: 0000-0002-2117-5390

Zeken Alma Ayankyzy – Master of Computer Science, D. Serikbayev East Kazakhstan Technical University.
e-mail: alma_zeken@mail.ru
ORCID: 0009-0007-0015-0032