DOI: 10.51634/2307-5201_2025_3_66
УДК 342.7
МРНТИ 10.15.59

FINDINGS FROM A STUDY ON CYBERSECURITY IN THE HEALTHCARE SECTOR OF KAZAKHSTAN: RECOMMENDATIONS FOR STRENGTHENING LEGAL AND CYBER POLICY

ZH. TEMIRBEKOV, PhD in Jurisprudence, Teaching Professor, Maqsut Narikbayev University (Astana, Republic of Kazakhstan), e-mail: zh_temirbekov@kazguu.kz

The *relevance* of the study lies in the fact that as digital technologies are more and more integrated into the healthcare sector of Kazakhstan, the risk of cyberattacks targeting patient data and threatening the realization of the right to health increases. The *subject* of the study is the cybersecurity of healthcare organizations in Kazakhstan. The *purpose* of this study is to examine the level of cyber awareness and preparedness for cyber threats among workers in the healthcare sector. The study's *novelty* lies in the fact that it is original due to its comprehensive approach, including an online survey of 14,372 healthcare workers. Based on the findings, the article presents proposals for the improvement of legal regulation and cyber policy in the field of cybersecurity in the healthcare sector of Kazakhstan.

Keywords: healthcare sector, cybersecurity, cyber threats, cyber awareness, cyber hygiene, Kazakhstan, cybersecurity policy, right to health

Introduction

Cybersecurity breaches can undermine patient trust, disrupt healthcare systems, and thus put human lives at risk [1]. Owing to its cybersecurity vulnerabilities, including the specific ways personnel use data, the healthcare sector could be considered a soft target [2]. For example, openness and information sharing in healthcare are essential [3]. This is the reason that health information systems in nearly every hospital department store protected health information and personally identifiable information. All healthcare providers utilize e-prescribing software, electronic health records, remote patient monitoring, laboratory information systems, and dietitian information systems (including physicians, nurses, pharmacists, technicians, and physical therapists) [4]. Because of this, there is a greater chance that the confidentiality or integrity of healthcare data will be compromised.

The UN General Assembly is concerned that gaps in states' access to and use of information technologies can diminish their social and economic prosperity. With special concern, it highlights the needs of less developed countries regarding cybersecurity best practices and training [5]. The World Health Organization's (WHO) strategic objectives are to strengthen governance for digital health at the national and global levels while supporting the capacity and skill-building of countries in adopting, innovating, and scaling up digital health technologies [6].

Cybersecurity skills are the armamentarium that healthcare professionals need to use to protect sensitive patient data and the integrity of healthcare systems. According to the European Network of Cybersecurity Centers and Competence Hub for Innovation and Operations (ECHO) Cyber-Skills Framework, promoting a systematic process of developing cybersecurity competencies and targeting the healthcare sector with unique vulnerabilities amid the dynamic cyber environment is important [7]. However, although considerable efforts have been made to define the content of core informatics competencies in recent years, less attention has been focused on assessing the practical informatics competencies and skills of healthcare workers [8].

In Kazakhstan, the governmental "Digital Kazakhstan" program sets the main direction for developing a uniform digital contour and introducing innovative technologies, including those in healthcare information systems. The implementation of these technologies has improved the quality of medical services [9]. Currently, 31 medical information systems and 14 laboratory information systems are in the Kazakhstani healthcare sector [10].

The legal framework supporting this digital transformation is outlined in the Code of the Republic of Kazakhstan, "On Public Health and Healthcare System," which stipulates developing and operating electronic information resources and systems in healthcare and ensures their accessibility for physical and legal entities [11]. In addition, integrating healthcare information systems into clinical practice is among the major focuses of the "Concept of digital transformation, development of the information and communication technology industry and cybersecurity for 2023–2029" [12].

According to the Information and Communication Technologies Development Index 2024, Kazakhstan has a high level of development of information and communication technologies [13]. However, in the area of cybersecurity, despite Kazakhstan's efforts to create a comprehensive cybersecurity legal framework that is more advanced than some of its Central Asian neighbors [14], the country is faced with such serious risks as low legal literacy of its citizens, ICT managers and staff on information protection issues, and violation by state and nonstate informatization institutions and ICT service users of established requirements, technical standards and norms of collection, processing, storage, and transfer of information in electronic form [15]. As some experts note, the level of awareness of cyber risks in the Kazakhstani healthcare sector is mixed, with some players shifting responsibility to developers of medical information systems, whereas others are not paying enough attention to information security issues [16]. According to a few research articles related to the cybersecurity sphere of Kazakhstan, there is no clear trajectory for the strategic plan for cybersecurity in the country; only the main directions are outlined without an assessment of their implementation [17]. Bringing the regulatory framework into line with international experience, using modern technologies, developing human resources, and strengthening international cooperation are still the most important strategic steps that Kazakhstan must take in cybersecurity [18].

Additionally, by developing partnerships, the healthcare industry can strengthen its defenses against evolving cyber risks, ensuring the continued delivery of high-quality healthcare and protecting global public health [19]. In addition, the WHO has emphasized that recent developments addressing the emerging needs of the digital health workforce in Kazakhstan have emphasized that education and training are needed to ensure safety and effectiveness in the use of new technologies [20]. Furthermore, the use of artificial intelligence and big data technologies in Kazakhstan requires appropriate legal regulation, as the development of digital technologies in healthcare is rapidly progressing, creating both new opportunities and legal gaps [21].

In light of the above, an evaluation is important for determining progress and new directions for cybersecurity in the healthcare sector. The present study is the first attempt to assess cybersecurity levels in the Kazakhstani healthcare sector. To analyze the study findings comparatively, a literature review was conducted to evaluate cybersecurity issues in the healthcare sector in the USA, Canada, Australia, and several European countries.

Materials and methods

This study involved diverse healthcare professionals from various regions and organizations across Kazakhstan. According to the survey results, 14,372 healthcare workers participated, including 3352 doctors, 9333 nurses, and 1687 administrative personnel.

The participants were selected from state organizations, private organizations, and research institutes, reflecting the composition of Kazakhstan's healthcare system. The demographic distribution included a wide range of ages and professional experiences, from less than five years to over thirty years, ensuring a comprehensive analysis of perspectives across different career stages. The recruitment strategy aimed to achieve a representative sample of the healthcare workforce in Kazakhstan to provide insights into their cybersecurity practices and perceptions. The survey included professionals from all major urban and rural areas, including Astana, Almaty, and Shymkent. This geographical and institutional diversity

is critical to understanding the sector's varied cybersecurity challenges and needs. The inclusion criteria were to involve healthcare professionals actively engaged in their respective fields and directly or indirectly interacting with the IT infrastructure as part of their daily activities.

Instrument

The questionnaire was developed on the basis of the literature on the cybersecurity practices of healthcare workers. The questionnaire was divided into several sections, covering demographics and professional background, IT infrastructure and cybersecurity awareness, cybersecurity practices and training, perceptions and attitudes toward cybersecurity, policy, and cooperation.

Procedure

The final version of the questionnaire was distributed electronically via Microsoft Forms, ensuring a user-friendly experience for participants. Given that it is generally difficult to collect answers from healthcare workers due to the nature of their work, the author was provided with the Ministry of Health of Kazakhstan's support in distributing the questionnaire among healthcare organizations. The surveys were conducted from March 2024 to July 2024. There was no time limit for completing the questionnaire, and participants were not reimbursed or offered any other incentive.

Ethical considerations

Ethical considerations were prioritized throughout the data collection process. The survey was anonymous, and no personally identifiable information was collected. The participants were informed of the study's purpose, and their informed consent was obtained before they began the survey. They were also informed that their participation was voluntary and that they could withdraw from the survey without any consequences. All survey data were securely stored to maintain confidentiality. Fundamental rights, such as the right to privacy, were guaranteed, and relevant country laws were safeguarded.

Data Analysis

The data analysis was conducted via Jamovi (version 2.3.28.0), a statistical software package based on R, to ensure a rigorous and systematic approach. Descriptive statistics were used to summarize and describe the basic features of the dataset. Cross-tabulation was performed to examine relationships between different categorical variables. Pearson's correlation was used to assess the strength of the associations between variables. ANOVA tests with Post Hoc (Tukey) analyses were conducted to compare the means across relevant multiple groups.

Results

The overwhelming majority of participants (95.8%) were employed in public healthcare institutions, reflecting the dominant role of state-run facilities in Kazakhstan's healthcare system, and only a small number were from private organizations (3.6%) and research institutes (0.6%). One critical factor affecting cybersecurity is Internet access. According to the survey, 93.4% of the respondents reported having Internet access at their workplace, whereas 6.6% did not. Moreover, on average, 3.5% of healthcare workers from all three types of organizations indicated that their organizations experienced cyberattacks. Among them, approximately 3% were nurses, 3.5% were doctors, and 5% were administrative personnel.

Confidence in cybersecurity protection

The results revealed that approximately 30% of respondents of each type of organization had trouble answering or acknowledging that their organization does not have internal policies requiring personnel to inform management or IT staff about significant performance issues with their PC. Moreover, only 50% of the participants indicated that their organization has enough IT personnel. Furthermore, among the respondents, only 30% agreed or fully agreed with the statement that their computers are well protected

against hacker attacks. That said, the ANOVA test reveals no significant differences (p from 0.476 to 575)[1] in the level of cyber protection confidence between healthcare workers of state organizations, research institutes, and private organizations. The results above are illustrated in Figure 1.

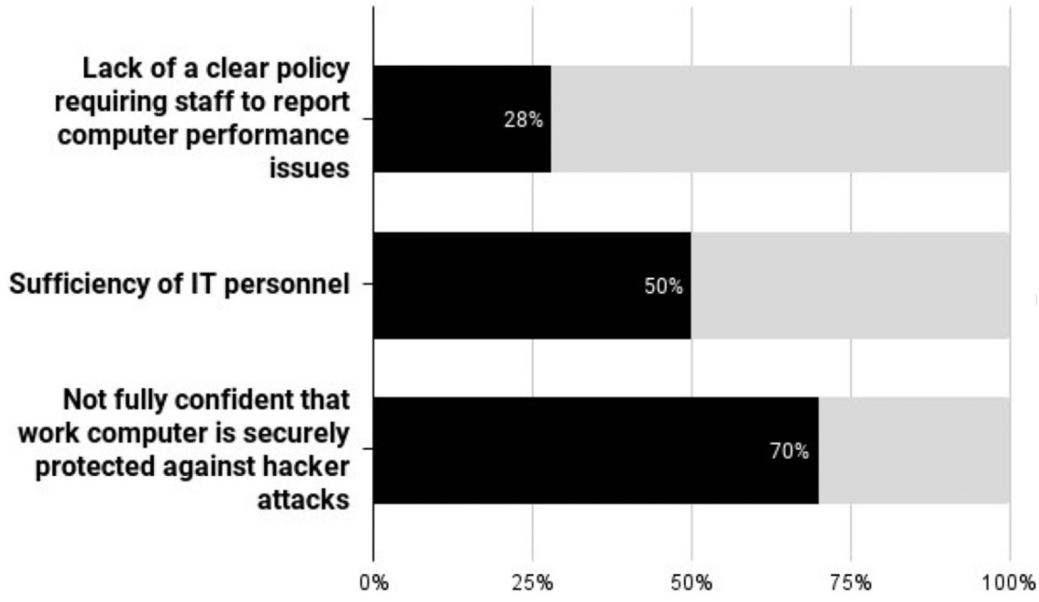

Figure 1. Some cybersecurity-related challenges in the national healthcare sector

Training on cybersecurity

The survey revealed a lack of cybersecurity-related training across all types of organizations. More than 53% of the respondents answered that their institution does not conduct cyber-related training (Figure 2). However, 28% of the respondents from private organizations answered that their organization conducts cybersecurity training at least once a year, 25% of the respondents from research institutes, and 24% of the respondents from state organizations answered the same way. Moreover, a positive ($r = 0.095$, $p < 0.001$) correlation was found between training frequency and the level of cyber threat awareness. Additionally, the results indicated that the level of confidence of healthcare sector workers that their computer is well protected against hacker attacks is strongly positively correlated with training frequency ($r = 0.358$, $p < 0.001$) and positively correlated with the level of awareness of cyber threats ($r = 0.212$, $p < 0.001$).

[1]Normality test not computed due to large sample size (>5000). Levene's test for homogeneity of variances has found no significant violation of variance homogeneity.

Figure 2. Frequency of cybersecurity training in all types of organizations

Cybersecurity awareness level

The survey revealed that more than one-third of the respondents from each type of organization do not have sufficient information about cyber threats. For example, 31% of workers in research institutes, 36% of staff in private organizations, and 39% of healthcare professionals in state organizations answered that they are not aware or are not sure about the types of dangers posed by malicious software (viruses, trojans, worms) and DoS attacks. With respect to professional roles, approximately 59% of nurses, 65% of doctors, and 67% of administrative personnel answered that they are aware of cyber-related threats.

The Pearson correlation matrix reveals a statistically significant ($p = 0.001$) but weak ($r = 0.027$) positive correlation between awareness of cyber threats and years of experience. However, ANOVA[2] and Post Hoc (Tukey) tests demonstrate that notable differences exist in the mean levels of awareness of cyber threats across the three organizational types. Private organizations' workers are significantly more aware of cyber threats than state institutions are ($p = 0.002$).

Additionally, the state-backed transnational malicious cyber operations (the cyber-attack against Estonia in 2007 [22], WannaCry 2017 [23], NotPetya 2017 [24]) are the most dangerous for the national healthcare sector; thus, it is interesting to analyze the opinions of healthcare professionals on this matter. According to the results, on average, 22% of all respondents agreed that state and private healthcare organizations may be targets for state-backed transnational malicious cyber operations. Furthermore, 40% of the respondents believe that Kazakhstan needs to cooperate with other countries in terms of cybersecurity to protect domestic healthcare organizations from hacker attacks. The results also revealed that most respondents (63%) agreed or strongly agreed that the country needs to develop and adopt a special law to protect the healthcare sector's security from hacker attacks. However, only 39% of therespondents supported the statement that restrictions on Internet use in the workplace are justified if they protect work computers from hacker attacks.

[2]Normality test not computed due to large sample size (>5000). Levene's test for homogeneity of variances has found no significant violation of variance homogeneity.

Discussion

This study provides important insights into cybersecurity in the Kazakhstani healthcare sector. Its findings highlight considerable challenges and opportunities for enhancing the sector's cybersecurity level.

The relatively low percentage of healthcare workers reporting the sufficiency of IT staff (50%) reflects a serious lack of IT resources. However, the result is better than the average global indicator. For example, research by the CDW Corporation revealed that fully staffed IT security teams reported only 14% of health IT leaders; the majority noted occasional or severe understaffing [25]. Recent research by the Australian Digital Health Agency (ADHA) also identified notable IT staff shortages in the healthcare sector [26]. A healthcare IT staff shortage reduces support for information systems and patching updates (Cartwright, 2023), negatively affecting cybersecurity. Owing to the insufficient cybersecurity level, cybercriminals have made the healthcare industry one of the best options to target [27]. The understaffing issue is further compounded by the small proportion of the survey respondents (3.5%), indicating that their organizations had experienced cyberattacks, which may suggest underreporting or a lack of awareness regarding cybersecurity incidents. In comparison, in the United States (US), for example, the American Medical Association (AMA) reported that over 77% of physicians experienced a form of cyberattack in less than three months of the year 2024 [28].

Research by KPMG conducted in the United Kingdom (UK) has shown that there is growing concern over the level of cybersecurity knowledge among healthcare staff, with many not understanding the risks associated with different types of cyber threats, such as viruses and Trojans [29]. Another study conducted among healthcare organizations in the European Union highlighted healthcare workers' lack of awareness of cybersecurity [30]. Furthermore, some recent studies have reported a decline in cybersecurity awareness programs in healthcare systems worldwide [31]. The present study's results also revealed an alarming level of cybersecurity awareness among healthcare professionals. For example, a substantial portion of respondents – ranging from 31% in research institutes to 39% in state organizations – reported limited or no knowledge of malicious software threats such as viruses, Trojans, or DoS attacks. That said, a poor understanding of the cyber threat landscape increases a healthcare organization's vulnerability to cyberattacks [32]. For example, a ransomware attack can be prevented if PC users are aware of this cyberattack method and can recognize it [33].

Thus, low levels of cyber threat awareness underscore the urgent need for targeted cybersecurity education and training programs. Notably, the positive correlation between training frequency and both awareness and confidence in cybersecurity protection suggests that regular training could significantly improve the readiness of healthcare personnel to address cyber threats. The 2024 report by the World Economic Forum reflects that, on a global scale, disparities in cyber resilience are increasing, particularly magnifying the difference between large and small organizations, which often correlates with private versus state-run organizations [34]. The present study revealed that private organization personnel exhibit higher awareness levels than state organization workers do. One of the reasons may be that, according to experts, healthcare organizations, especially public organizations, often operate on very constrained budgets and a general shortage of IT staff [35]. However, some authors have suggested that employees within the private sector tend to have more risky information system behavior and lower information security awareness than their colleagues in the public sector do [36].

One of the most pressing challenges identified in this study is the lack of cybersecurity training. The survey indicated that over half of the respondents answered that no cybersecurity-related training occurs in their organizations. This inadequacy may contribute to the observed lack of confidence, with only one-third of respondents agreeing that their work computers are well protected against hackers. While cybersecurity training can be an effective component in any successful healthcare cybersecurity program [37], studies show that such an issue is a common problem worldwide. For example, surveys conducted in 2020 in Poland [38] and 2019 in Finland [39] and Canada [40] have shown that healthcare workers lack sufficient training in cybersecurity. According to some studies in the U.S., many healthcare organizations are unprepared to address the reality of cyber threats. As some experts noted, the overwhelming nature of the problem is causing healthcare executives to look the other way and adopt an "if it ain't broke, don't fix it" attitude [41]. Therefore, establishing standardized, mandatory training programs across all healthcare organizations is globally important to mitigate this issue and build a more secure healthcare IT infrastructure.

Furthermore, the absence of clear internal cybersecurity policies requiring staff to report IT issues, such as system lags or failures, compounds the problem. A lack of awareness among staff about organizational IT policies and compliance requirements can create a greater risk of security breaches [40]. As the survey demonstrated, approximately one-third of the respondents either did not know about or could not confirm the existence of internal cybersecurity policies. The absence of internal cybersecurity policies may be connected with the situation in which, according to a survey, healthcare organizations are experiencing a critical shortage of IT personnel, highlighting the urgent need for qualified cybersecurity professionals in the healthcare sector, which is also a global issue [42]. Nevertheless, effective incident reporting mechanisms are essential for minimizing the risk of data breaches and ensuring timely responses to potential cyber threats. According to research conducted in 2022 in Greece, Romania, and Portugal's healthcare sectors, 76% of non-ICT staff responded that following hospital safety policies would help them perform better [43].

The global nature of cybersecurity threats to healthcare organizations requires international cooperation [44], and the United Nations highlights its need [45,46]. For example, the Commonwealth Telecommunications Organization has set up a knowledge-sharing program on the use of artificial intelligence in healthcare cybersecurity involving 40 member states [44]. With almost half of the survey respondents supporting Kazakhstan's collaboration with other nations on cybersecurity and more than half of the participants advocating for a dedicated cybersecurity law for the healthcare sector, there is a clear signal for appropriate proactive governmental actions in these directions. These measures could include developing cross-border information and knowledge sharing and adopting practices, such as international cooperation through threat intelligence sharing, joint research, and the development of security standards to help countries and companies better counter cyberattacks [47]. The examination of legal practices of the US Health Insurance Portability and Accountability Act (HIPAA), the Australian My Health Records Act, and the Indian Digital Information Security in Healthcare Act (DISHA), which are facilitating the cybersecurity level of the healthcare sector due to their administrative, physical, and technical safeguards in protecting HIS, is particularly interesting.

Conclusions

In addition to the remarkable development of the country's digital healthcare infrastructure, there are still conspicuous gaps in cybersecurity across healthcare organizations, especially concerning cybersecurity awareness and training.

As a cybersecurity culture is the set of attitudes, behaviors, knowledge, and awareness that an organization's personnel should demonstrate [48], practical steps toward enhancing cybersecurity resilience in the healthcare sector must include establishing regular, sector-wide training programs tailored to the needs of healthcare professionals. Such programs may significantly improve awareness and reduce an organization's cyberattack vulnerability. Second, it is crucial to develop internal policies that mandate incident reporting and ensure sufficient IT staffing levels to address cybersecurity concerns proactively. Third, specific cybersecurity laws for the healthcare sector should be elaborated upon and enacted, and international cooperation should be fostered to leverage best practices and share resources.

Limitations

The study's cross-sectional design limits its use. Future research should consider longitudinal studies to evaluate the effectiveness of interventions and explore in-depth qualitative assessments to uncover the organizational and cultural factors affecting cybersecurity practices in the healthcare sector. The reliance on self-reported data may also introduce biases, as participants might underreport or overreport their knowledge and experiences.

Acknowledgments

The author would like to thank all the anonymous healthcare professionals who voluntarily completed the questionnaire during their busy schedules and the Ministry of Health of Kazakhstan for supporting the distribution of the questionnaire among healthcare organizations.

Ж.Р. Темірбеков, PhD in Jurisprudence, LLM in International Law, Teaching Professor Maqsut Narikbayev University (Астана қ., Қазақстан Республикасы): Қазақстанның денсаулық сақтау саласындағы киберқауіпсіздік жөніндегі зерттеу нәтижелері: құқықтық реттеуді және киберсаясатты жетілдіруге арналған кейбір ұсыныстар.

Зерттеудің *өзектілігі,* цифрлық технологиялардың Қазақстанның денсаулық сақтау секторына барған сайын еніп келе жатқандықтан, пациенттердің деректеріне бағытталған және денсаулық құқығын жүзеге асыруға қауіп төндіретін кибершабуылдар қаупінің артуымен байланысты. Зерттеу *пәні* – Қазақстандағы денсаулық сақтау ұйымдарының киберқауіпсіздігі. Зерттеудің *мақсаты* – Қазақстандағы денсаулық сақтау қызметкерлерінің киберқауіптерге дайындығы мен кибер хабардарлық деңгейлерін зерделеу. Жұмыстың жаңалығы оның 14 372 медицина қызметкері арасында жүргізілген онлайн сауалнаманы қоса алғанда, комплексті тәсіліне байланысты түпнұсқалығында. Мақалада, зерттеудің нәтижелері негізінде, Қазақстанның денсаулық сақтау секторындағы киберқауіпсіздік саласындағы құқықтық реттеу мен киберсаясатты жетілдіру бойынша ұсыныстар тұжырымдалған.

Түйінді сөздер: денсаулық сақтау секторы, киберқауіпсіздік, киберқауіптер, кибер хабардар болу, кибергигиена, Қазақстан, киберқауіпсіздік саясаты, денсаулыққа құқық.

Ж.Р. Темирбеков, PhD in Jurisprudence, LLM in International Law, Teaching Professor Maqsut Narikbayev University (г. Астана, Республика Казахстан): Результаты исследования кибербезопасности в сфере здравоохранения Казахстана: некоторые рекомендации по совершенствованию правового регулирования и киберполитики.

Актуальность исследования заключается в том, что по мере того, как цифровые технологии все больше проникают в сферу здравоохранения Казахстана, возрастает риск кибератак, нацеленных на данные пациентов и создающих угрозу реализации права на здоровье. *Предметом* исследования является кибербезопасность организаций здравоохранения Казахстана. *Целью* данного исследования является изучение уровня кибер-осведомленности и готовности к кибер-угрозам среди работников сферы здравоохранения Казахстана. *Новизна* исследования заключается в том, что оно является оригинальным благодаря своему комплексному подходу, включающему онлайн опрос 14 372 работников здравоохранения. В статье, по результатам исследования, представлены предложения по совершенствованию правового регулирования и киберполитики в сфере кибербезопасности сектора здравоохранения Казахстана.

Ключевые слова: сектор здравоохранения, кибербезопасность, киберугрозы, кибер-осведомленность, кибергигиена, Казахстан, политика кибербезопасности, право на здоровье.

References:

1. Sharma P., Habibi Lashkari A., Parizadeh M. Understanding Cybersecurity Management in Healthcare: Challenges, Strategies and Trends. Cham: Springer Nature Switzerland, 2024. 1 p.

2. Thamer N., Alubady R. A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research // 2021 1st Babylon International Conference on Information Technology and Science (BICITS). Babil, Iraq: IEEE, 2021. P. 210–216.

3. Bhosale K., Nenova M., Iliev G. A study of cyber attacks: In the healthcare sector // 2021 Sixth Junior Conference on Lighting (Lighting). IEEE, 2021. P. 1–6.

4. Argaw S. et al. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks // British Medical Journal (medical informatics and decision making). London: BioMed Central, 2020. Vol. 20, № 1. P. 1–146.

5. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures: A/C.2/64/L.8. 2009.

6. Global Strategy on Digital Health 2020-2025. 1st ed. Geneva: World Health Organization, 2021. 1 p.

7. EMK. ECHO Cyberskills Framework – ECHO Network. URL: https://echonetwork.eu/echo-cyberskills-framework/ (09.01.2025).

8. Blažun Vošner H., Železnik D., Kokol P. Bibliometric analysis of the International Medical Informatics Association official journals // Informatics for Health and Social Care. 2019. Vol. 44, № 4. P. 405–421.

9. Digital Kazakhstan. URL: https://www.gov.kz/memleket/entities/mdai/activities/14764?lang=ru (09.01.2025).

10. The list of MIS that meet the requirements for working in the GOBMP and SMS system. URL: https://betaegov.kz/memleket/entities/dsm/documents/details/196758 (09.01.2025).

11. On Public Health and Healthcare System. URL: https://adilet.zan.kz/eng/docs/K2000000360 (10.01.2025).

12. Concept of digital transformation, development of the information and communication technology industry and cybersecurity for 2023–2029. URL: https://adilet.zan.kz/rus/docs/P2300000269 (10.01.2025).

13. ICT Development Index 2024 // ITU. URL: https://www.itu.int/hub/publication/d-ind-ict_mdd-2024-3/ (09.01.2025).

14. Nussipova A. et al. PandemIc, hoaxes and InformatIon securIty of Kazakhstan // Journal of Information Policy. Pennsylvania State University Press, 2023. Vol. 13. P. 140–158.

15. Cybersecurity concept ("Kazakhstan Cyber Shield"). URL: https://adilet.zan.kz/rus/docs/P1700000407 (10.01.2025).

16. Cybersecurity of Medical Data: Real Threats and Innovative Solutions [Electronic resource] // Information system PARAGRAPH. URL: https://online.zakon.kz/Document/?doc_id=38536156 (19.01.2025).

17. Isabayeva S. Ensuring cybersecurity of Kazakhstan in the context of global digitalization. Astana: Academy of Public Administration under the President of the Republic of Kazakhstan, 2020.

18. Tlepbergenov S. et al. Improvement of Critical Objects of the Information and Communication Infrastructure of the Republic of Kazakhstan // In The World Of Science and Education. Общественный фонд «Исследовательский центр «Endless Light in Science», 2024. № 15 December TH. P. 77–81.

19. Temirbekov Z. Global Health Security in the Age of Transnational Malicious Cyber Operations: A Taxonomic Analysis of Non-State and State-Backed Cyber Threats // Law and state. 2024. № 2. P. 6–17.

20. Addressing the growing needs of Kazakhstan's digital health workforce. URL: https://www.who.int/europe/news-room/20-10-2023-addressing-the-growing-needs-of-kazakhstan-s-digital-health-workforce (10.01.2025).

21. Rustemova G., Baiseitova A. Legal Risks of Digital Medicine: Issues and Opinions // Legalitas. 2024. Vol. 2, № 2. P. 63–70.

22. Traynor I. Russia accused of unleashing cyberwar to disable Estonia // The Guardian. 2007.

23. Investigation: WannaCry cyber attack and the NHS. UK National Audit Office, 2017.

24. Greenberg A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History // Wired.

25. CDW Research Report: Shortages Impact Healthcare Cybersecurity Strategies // CDW. URL: https://healthtechmagazine.net/article/2024/06/new-cdw-research-report-shortages-impact-healthcare-cybersecurity-strategies (14.01.2025).

26. Annual report (2023-2024) // Australian Digital Health Agency. URL: https://www.digitalhealth.gov.au/about-us/annual-reports (14.01.2025).

27. Vikash S. Exploring Challenges Faced by Information Technology Security Managers in Implementing Risk Management Framework to Protect Protected Health Information and Personally Identifiable Information. Northcentral University, 2022.

28. Physicians struggle to keep practices afloat after Change cyberattack (2024 survey) // American Medical Association. URL: https://www.ama-assn.org/press-center/press-releases/physicians-struggle-keep-practices-afloat-after-change-cyberattack (14.01.2025).

29. Cybersecurity considerations 2024 // KPMG. URL: https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2024.html (14.01.2025).

30. Argyridou E. et al. Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study // J Med Internet Res. 2023. Vol. 25. P. e41294.

31. Ewoh P., Vartiainen T. Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review // J Med Internet Res. 2024. Vol. 26. P. e46904.

32. Bris A., Asri W. State of Cybersecurity & Cyber Threats in Healthcare Organizations. Essec Business School, 2016. P. 1–13.

33. Carreiro A., Silva C., Antunes M. The use of gamification on cybersecurity awareness of healthcare professionals // Procedia Computer Science. 2024. Vol. 239. P. 526–533.

34. Global Cybersecurity Outlook 2024 // World Economic Forum. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2024/ (15.01.2025).

35. Beltempo E. Implementation of the ECHO Cyber-Skills Framework in the CyberSecPro Project: Enhancing Cybersecurity Capabilities in healthcare fi=AMK-opinnäytetyö|sv=YH-examensarbete|en=Bachelor's thesis|. 2024. URL: http://www.theseus.fi/handle/10024/869217 (09.01.2025).

36. Solic K., Velki T., Galba T. Empirical study on ICT system's users' risky behavior and security awareness // 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Opatija, Croatia: IEEE, 2015. P. 1356–1359.

37. Conrad M. Standardizing Cybersecurity Training in the Healthcare Industry Using Qualitative Nominal Group Technique. University of Phoenix, 2021.

38. Hyla T., Fabisiak L. Measuring Cyber Security Awareness within Groups of Medical Professionals in Poland // Proceedings of the 53rd Hawaii International Conference on System Sciences. 2020.

39. Haukilehto T., Hautamäki J. Survey of Cyber Security Awareness in Health, Social Services and Regional Government in South Ostrobothnia, Finland // Internet of Things, Smart Spaces, and Next Generation Networks and Systems / ed. Galinina O. et al. Cham: Springer International Publishing, 2019. Vol. 11660. P. 455–466.

40. Arain A., Tarraf R., Ahmad A. Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization // Journal of Multidisciplinary Healthcare. 2019. Vol. Volume 12. P. 73–81.

41. Abraham C., Chatterjee D., Sims R. Muddling through cybersecurity: Insights from the U.S. healthcare industry // Business Horizons. 2019. Vol. 62, № 4. P. 539–548.

42. Rahim J. et al. Cybersecurity Threats in Healthcare IT: Challenges, Risks, and Mitigation Strategies // Journal of Artificial Intelligence General science. 2024. Vol. 6, № 1. P. 438–462.

43. Gioulekas F. et al. A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures // Healthcare. 2022. Vol. 10, № 2. P. 327.

44. Gala M. The Role of AI in Shaping Global Healthcare Cybersecurity Policies // International Journal for Multidisciplinary Research. 2024. Vol. 6, № 5. P. 1–14.

45. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: A/76/135. 2021.

46. Final Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security: A/78/265. 2023.

47. Lysenko S. et al. Global cybersecurity: Harmonising international standards and cooperation // Multidiscip. Rev. 2024. Vol. 7. P. 2024spe021.

48. Yeng K., Yang B., Snekkenes A. Framework for Healthcare Security Practice Analysis, Modeling and Incentivization // 2019 IEEE International Conference on Big Data (Big Data). Los Angeles, CA, USA: IEEE, 2019. P. 3242–3251.

Для цитирования и библиографии: Temirbekov Zh. Findings from a Study on Cybersecurity in the Healthcare Sector of Kazakhstan: Recommendations for Strengthening Legal and Cyber Policy // Право и государство. № 3(108), 2025. – С. 66-75. DOI: 10.51634/2307-5201_2025_3_66

Материал поступил в редакцию 10.04.2025