Valeology: International Journal of Medical Anthropology and Bioethics
(ISSN 2995-4924) VOLUME 03 ISSUE 1, 2025

CYBERSECURITY ISSUES AND METHODS OF PROTECTING INFORMATION SYSTEMS IN MEDICINE

NEMATOV NIZOM ISMATULLAYEVICH
Assistant of Samarkand State Medical University

NORBOYEVA SEVINCH NORBEK QIZI
Student of Samarkand State Medical University

Abstract:

Cybersecurity issues are one of the most pressing issues in the field of information technology today, and this issue is becoming even more important in the medical field. The confidentiality and integrity of medical data are important for maintaining patient privacy, protecting against adverse events, and ensuring effective data flow management. This article examines the current issues of information security in the medical field, in particular, threats leading to data corruption, malicious programs, data transmission disruptions, and problems related to the human factor.

The article also describes modern methods of protecting information systems used in medicine, including cryptographic protection tools, authentication and authorization technologies, network monitoring systems, and recommendations for developing security policies. The results of this study serve as an important scientific and practical basis for ensuring security in the development of medical information systems.

Keywords: cybersecurity, medical information systems, data protection, information security, medical data.

Introduction

Introduction: Today, information technologies are deeply integrated into various spheres of society, including medicine. In the medical field, information systems allow storing personal information of patients, automating diagnostic and treatment processes, as well as organizing remote medical services. At the same time, the widespread use of these systems makes them vulnerable to cybersecurity threats. Risks such as breaches of medical data, unauthorized access, theft or loss of data negatively affect not only the interests of patients, but also the efficiency of the overall healthcare system.

Cybersecurity is a critical factor in making medical information systems reliable and secure. In particular, ensuring the confidentiality of patients' medical data and preventing misuse of this data is crucial. This requires the implementation of modern security technologies, rapid response to new threats, and the development of effective protection strategies.

Result: This study examined current issues related to cybersecurity of information systems in the medical field and methods for their protection. The results showed the following:

The increasing number of cyberattacks on medical information systems was analyzed. Among the main threats, factors such as malware, human error, data corruption, and system failures were identified, which negatively affect the efficiency of medical institutions.

Cryptographic technologies, multi-factor authentication systems, real-time monitoring, backup management, and security policy formulation have been proposed as important solutions for protecting medical data. These approaches help ensure the security of systems and effectively combat cyberattacks.

The use of technologies based on artificial intelligence and machine learning has been proven to be effective in identifying threats in advance. With the help of such technologies, medical institutions will be able to detect and prevent cyberattacks in real time.

It was emphasized that it is important to formulate a security policy in medical institutions, regularly train employees on cybersecurity, and conduct regular audits of systems. At the same time, the introduction of security measures that comply with international standards will help strengthen information systems.

Discussion: Given the increasing relevance of cybersecurity issues in the medical sector, a number of problems are observed in this area. Since medical information systems are often designed to store sensitive and personal data, they are becoming one of the main targets for cyberattacks. Among the threats are malicious programs (viruses, ransomware), data theft, and unauthorized access to systems, internal human factors, and interruptions in data transmission. In particular, ransomware attacks can disrupt the activities of medical organizations and reduce the quality of services provided to patients.

In the modern world, new technologies and electronic services have become an integral part of our daily lives. Given that society is becoming more and more dependent on information and communication technologies every day, the protection and use of these technologies is becoming a crucial and very important topic for national interests. Today, a prerequisite for the development of the information society is cybersecurity, which can be ensured by an almost endless list of security measures, from technical to legislative, and by solving them. Cybersecurity issues range from the level of information security on a separate computer to the level of creating a single cybersecurity system as an integral part of the information and national security of each state. Therefore, in order to ensure cybersecurity for each organization, employees engaged in this field are being attracted, and a series of seminars and training courses are being organized to constantly familiarize employees with cybersecurity knowledge.

Cybersecurity is currently one of the emerging concepts, and there are various definitions given to it. In particular, the CSEC2017 Joint Task Force defines cybersecurity as follows: cybersecurity is a computationally based field of knowledge that integrates technology, people, information, and processes to ensure that operations are performed correctly in the presence of attackers. It includes the creation, implementation, analysis, and testing of secure computer systems. Cybersecurity is an integrated field of knowledge of education and includes legal aspects, policy, human factors, ethics, and risk management. Cisco, an organization operating in the field of networks, defines cybersecurity as follows: Cybersecurity is the practice of protecting systems, networks, and

applications from digital attacks. These cyberattacks are usually aimed at controlling, replacing, or destroying confidential information; extorting money from users; and disrupting normal operations. Nowadays, the implementation of effective cybersecurity measures is becoming increasingly difficult in practice due to the number and types of devices and the increasing capabilities of attackers compared to humans. There are different approaches to defining the fundamental terms of cybersecurity. In particular, some experts have defined cybersecurity terms as follows: Confidentiality is the state of information or its carrier in such a way that unauthorized access or copying is prevented. Confidentiality deals with protecting information from unauthorized "reading". Confidentiality is especially important for banks in the banking system. Risk is the potential benefit or loss, and in general, risk arises when the probability of an event occurring is added to any situation. ISO defines risk as "the effect of uncertainty on objectives". Information security is the state of information according to which accidental or intentional unauthorized access to information or its unauthorized use is not allowed. Or, the level of information protection that ensures the preservation of characteristics such as confidentiality, integrity, and usability when processing information using technical means.

During the discussion, it became clear that many of the existing cybersecurity problems are related to the difficulties of medical organizations in implementing modern security technologies. For example, many medical institutions use outdated software or have insufficiently developed security policies. In addition, the lack of sufficient knowledge and skills of medical staff in cybersecurity is also an important factor.

A number of effective methods are proposed to eliminate these problems:

Application of cryptographic technologies – ensuring the confidentiality of data by encrypting it.

Multi-factor authentication systems are used to ensure that only authorized users have access to systems.

Real-time monitoring systems – detect and respond quickly to any unusual activity occurring on networks.

Training and education programs for healthcare workers are essential to reduce human error.

Creating and managing backups – ensuring data recovery in the event of system failures.

At the same time, solutions to the problems should cover not only technological, but also legal and managerial aspects. It is important to further strengthen the information security policies of medical institutions and bring them into line with international standards.

Conclusion: While the widespread implementation of information systems in medicine has increased efficiency in managing patient data, they have also created new cybersecurity threats. This study identified the main vulnerabilities of medical information systems and examined modern approaches and technologies aimed at eliminating cybersecurity problems.

The results showed that:

The increasing number of cyberattacks in the healthcare sector makes ensuring the confidentiality, integrity, and availability of data a critical task.

Inadequate implementation of security policies and technologies in medical facilities increases the vulnerability of systems.

Modern protection methods – cryptography, multi-factor authentication, real-time monitoring, and backups – help significantly increase the security of medical systems.

Artificial intelligence and machine learning technologies have emerged as effective tools in the early detection of cybersecurity threats.

In conclusion, effective protection of information systems in medicine requires the introduction of modern technologies, regular training of staff, and improvement of security policies. The results of this study are of great importance in developing practical measures and strategies aimed at strengthening information security in medical institutions.

In the future, it is necessary to continue research on this topic, in particular, in the direction of applying new security technologies and analyzing international experience. This will create broad opportunities for making medical information systems more efficient and secure.

References:

1. Nabiyeva, S. S., Rustamov, A. A., Malikov, M. R., & Ne'matov, N. I. (2020). Concept of medical information. European Journal of Molecular and Clinical Medicine, 7(7), 602-609.
2. Malikov, M. R., Rustamov, A. A., & Ne'matov, N. I. (2020). STRATEGIES FOR DEVELOPMENT OF MEDICAL INFORMATION SYSTEMS. Theoretical & Applied Science, (9), 388-392.
3. Berdiyevna, A. S., & Olimjonovna, T. F. (2022). INNOVATIVE APPROACHES IN THE EDUCATION SYSTEM TO INCREASE YOUTH PARTICIPATION. Web of Scientist: International Scientific Research Journal, 3(3), 674-677.
4. Esirgapovich, K. A. (2022). THE EASIEST RECOMMENDATIONS FOR CREATING A WEBSITE. Galaxy International Interdisciplinary Research Journal, 10(2), 758-761.
5. Toxirova, F. O., Malikov, M. R., Abdullayeva, S. B., Ne'matov, N. I., & Rustamov, A. A. (2021). Reflective Approach In Organization Of Pedagogical Processes. European Journal of Molecular & Clinical Medicine, 7(03), 2020.
6. Ne'matov, N., & Rustamov, T. (2022). SANATORIYLAR ISHINI AVTOMATLASHTIRISH: BRON XIZMATI VA UNING STRUKTURASI. Eurasian Journal of Academic Research, 2(11), 763-766.
7. Ne'matov, N., & Ne'matova, N. (2022). OLIY TA'LIM TIZIMI TALABALARIGA O'ZBEK TILINI O'QITISHDA AXBOROT TEXNOLOGIYALARINING O'RNI. Академические исследования в современной науке, 1(19), 37-38.
8. OB Akhmedov, AS Djalilov, NI Nematov, AA Rustamov // Directions Of Standardization In Medical Informatics // Emergent: Journal of Educational Discoveries and Lifelong Learning (EJEDL), 2(2), 1-4 p. 2021
9. Ne'matov, N., & Isroilov, J. (2022). TIBBIY VEB SAYTLAR YARATISH YUTUQ VA KAMCHILIKLARI. Zamonaviy dunyoda innovatsion tadqiqotlar: Nazariya va amaliyot, 1(25), 162-164.
10. Ne'matov, NI. (2022). TIBBIY VEB SAYTLAR YARATISH SAMARADORLIGI. Academic Research in Educational Sciences (ARES) 3 (2), 118-124
11. Ismatullayevich, N. N. (2023). The role of educational websites in the development of student's higher education systems. Eurasian Journal of Research, Development and Innovation, 17, 17-20.
12. Ismatullayevich N. N., Ilxomovna M. Z. Automation of Sanatorium Work: Reservation Service and its Structure //Miasto Przyszłości. – 2022. – T. 29. – C. 65-67.
13. Ne'matov, N., & Sobirova, K. (2024). THE ROLE OF WEBSITES IN IMPROVING THE WORK OF MEDICAL INSTITUTIONS. Modern Science and Research, 3(2), 530-532.

14. Ismatullayevich, N. N. (2024). Medical Higher Education Institutions in Medicine and Science Lessons from the Use of Information Technology in the Organization of the Laboratory of Multimedia Tools. *American Journal of Biomedicine and Pharmacy*, *1*(6), 16-20.
15. Ne'matov, N., & Yarmahammadov, U. (2023). USE OF MULTIMEDIA IN ORGANIZING PRACTICAL LESSONS IN INFORMATION TECHNOLOGY IN INSTITUTIONS OF HIGHER EDUCATION. *Modern Science and Research*, *2*(4), 693-697.
16. MALIKOV, M. R., & NE'MATOV, N. I. (2022). Visual structure of health websites: the need to develop a comprehensive design guide. *THEORETICAL & APPLIED SCIENCE Учредители: Теоретическая и прикладная наука,(3)*, 805-810.