**Iryna Parfonova**

Candidate of Economic Sciences (PhD),

Associate Professor of the Department of Social Medicine, Organization and Management in Healthcare

Kharkiv National Medical University.

ORCID ID https://orcid.org/0000-0002-7049-4312

**Oleksandra Zinchenko**

PhD Student at the Department of Political Science of School of Philosophy

V.N. Karazin Kharkiv National University

ORCID ID <https://orcid.org/0000-0003-1623-957X>

**IMPLEMENTATION OF EU EHEALTH CYBERSECURITY STANDARDS IN UKRAINE**

In the contemporary world, digital technologies have become an integral part of all aspects of our lives, and the healthcare sector is no exception. The implementation of the electronic healthcare system (hereinafter referred to as eHealth) in Ukraine marks a revolutionary development in the healthcare sector, which provides an opportunity to optimize medical services significantly.

Overall, the draft Concept for the Electronic Healthcare System Development was developed more than 5 years ago [1], with the participation of the Ministry of Health of Ukraine, the NHSU and the State Enterprise «Electronic Health». The concept was adopted with a shift in the focus of eHealth reform towards digital transformation projects at the end of 2020. The implementation of this concept was divided into 2 stages (until 2022 and until 2025) [2]. While the first stage was mainly focused on creating a legislative framework, healthcare facilities informatization, and transition to electronic documentation. The second stage raised the issue of cybersecurity and envisages the implementation of security standards, cyberthreats monitoring, digital competencies development and secure environment creation for the eHealth system.

In our opinion, this addition is quite apt, as in today's world, cybersecurity is becoming a crucial aspect of the functioning of any sector, especially such a sensitive one as the healthcare system, and the key problem is the underestimation of the cybersecurity importance. Frequently, healthcare institutions invest heavily in technical equipment and digital services, but pay insufficient attention to cybersecurity. In this regard, it is particularly important to implement a comprehensive approach, a kind of «eHealth Cybersecurity Vector» that includes both technical and organizational aspects. This means that every healthcare facility should have a clear cyberdefense strategy that includes regular software updates, multi – stage security systems, staff training and independent audits.

The healthcare sector is one of the main targets for cyberattacks due to the large amount of sensitive information that healthcare institutions process. This includes patients' personal data, medical records, diagnostic test results, and even financial information. According to global trends, medical institutions are at the top of the list of those most vulnerable to attacks. In most cases, attackers exploit known vulnerabilities, such as outdated technology, weak passwords, or insufficient cyber hygiene. This suggests that the problem is often not so much the complexity of the attacks as the lack of preparedness of the healthcare sector for modern threats. Therefore, based on the peculiarities of this problem, we consider it appropriate to propose our own «Vector for ensuring eHealth cybersecurity».

Among the key components, we believe that, first of all, it is necessary to perform a risk and vulnerability assessment to identify critical threats and develop strategies to minimize them. We emphasize the necessity of European security standards integration, which as expected, contribute to the long – term sustainability of the system and its compliance with international requirements. In addition, we prioritise the introduction of cyber education for healthcare professionals to raise their awareness of current cyber threats. Finally, international cooperation and knowledge exchange with leading countries will allow the implementation of the best cybersecurity practices. Ukraine will be able to integrate the experience of EU countries in implementing cybersecurity standards, conduct joint research and apply pilot projects e.g., the international coalitions or partnerships creation would allow the exchange of best practices and the introduction of innovative technologies. In this regard, it is worth mentioning initiatives that promote Ukraine's integration into the European cyberspace, ensuring high resilience to the current threats.

Thus, ensuring cybersecurity in the healthcare sector requires a systematical approach that includes technical, organizational and social aspects. Merely comprehensive solutions taking into account the needs of both healthcare facilities and citizens can guarantee the resilience of the eHealth system to the challenges of the digital age. European standards integration, cybersecurity national competencies development, staff training and active citizens` involvement to the digital services usage are key elements of this Vector.

To sum up, it is important to emphasize that Ukraine has all the capabilities to create a safe and efficient eHealth system that will meet modern challenges. However, it requires not only technical support, but also political intention to change, as only through joint efforts can the appropriate level of security and trust in digital healthcare be achieved.

**References**

1. Some issues of the electronic healthcare system: Decree of the Cabinet of Ministers of Ukraine of 18 July 2018. of Ministers of Ukraine of 25.04.2018 No. 411: as of 4 July. 2024 URL: https://zakon.rada.gov.ua/laws/show/411-2018-п#Text (accessed 03.01.2025).
2. МОЗ. Концепція розбудови електронної охорони здоров’я в Україні. 2024. URL: https://moz.gov.ua/uk/koncepciya-rozbudovi-elektronnoyi-ohoroni-zdorov-ya-ukrayini (дата звернення: 03.01.2025).