DOI: https://doi.org/10.30525/2256-0742/2025-11-1-95-103

CYBER RISK MANAGEMENT IN THE BUSINESS STRATEGIES OF HEALTHCARE INSTITUTIONS AND COMPLIANCE WITH DIGITAL PATIENTS' RIGHTS: EU EXPERIENCE AND PROPOSALS FOR UKRAINE IN WARTIME*

Oleh Zaiarnyi[1]

Abstract. The article examines the issues of cyber risk management in the business strategies of healthcare institutions operating in the European Union, in order to ensure the digital protection of patients and reduce potential negative economic losses. The *relevance* of the study stems from the rapid development of digital technologies in the healthcare sector and the increasing incidence of cyber threats that compromise the confidentiality of patient data, disrupt the operations of healthcare institutions and pose significant economic risks. The *purpose* of the article is to study the existing approaches to cyber risk management in the business strategies of healthcare institutions in order to reduce economic losses and ensure compliance with patients' digital rights, and on this basis to formulate proposals for improving the legislation of Ukraine and medical practice, taking into account the challenges of war. The *research methods* employed encompass the dialectical method, analysis and synthesis techniques to examine the interrelationships between cyber threats and patients' digital rights, statistical analysis to evaluate the prevalence of cyber threats within the European Union, modelling to formulate recommendations, and a comparative legal approach to identify common and distinct approaches in the European Union and Ukrainian legislation concerning the regulation of cyber security in healthcare facilities. The study's primary *findings* indicate that the most prevalent cyber threats within the digital healthcare sector encompass phishing attacks, malware, disruptions to artificial intelligence algorithms, and insider threats. The European Union has adopted contemporary methodologies in the realm of cyber security, underpinned by the principles of secure design of information systems and data protection in accordance with the rule of secure processing. At the same time, as proved in the article, it is necessary to improve the legislation of Ukraine, in particular by introducing provisions on the processing of medical data in accordance with the principles of the GDPR, strengthening the influence of international ISO standards on the business strategies of healthcare institutions for managing cyber risks and overcoming the consequences of their manifestation. A number of recommendations for Ukraine are proposed, namely ensuring cyber hygiene of medical personnel, integrating data encryption and cyber incident response plans, using artificial intelligence technologies to monitor risks, and adapting European experience to Ukrainian realities. The *conclusions* emphasise the necessity of implementing the most effective European practices in the realm of cyber risk management within the business strategy of medical institutions in Ukraine. This approach is expected to enhance the level of cyber security, mitigate the risks of violating patients' digital rights, and ensure the economic sustainability of healthcare facilities in the context of the ongoing war against Ukraine.

Keywords: business strategy of a healthcare institution, challenges of the war against Ukraine, European Union, economic security, healthcare institution, cyber risks, Patient Digital Rights.

JEL Classification: I11, L21, M10, H56, P16, F15, F55, E66, H12, I18, K24, M15, K32

* This article was prepared within the framework of the Verkhovna Rada of Ukraine's Named Scholarship for Young Scientists – Doctors of Science in 2024.

[1] Taras Shevchenko National University of Kyiv, Ukraine
E-mail: olehzaiarnyi@knu.ua
ORCID: https://orcid.org/0000-0003-4549-7201

1. Introduction

The digital healthcare industry is undergoing rapid transformation, facilitating patients' access to essential medical information and contemporary, cutting-edge medical services.

Digital healthcare is predicated on the collection, storage and dissemination of patient data, which may encompass sensitive information such as medical history, identification data and financial information. In the event of this information falling into the wrong hands, there is the potential for significant consequences for patients, including identity theft and financial fraud. Furthermore, a data breach can also have substantial legal and economic ramifications for healthcare facilities.

In July 2024, the European Cyber security Agency published an Analytical Report entitled "ENISA Threat Landscape: Health Sector (January 2021 to March 2023)". As stated in this document, the most prevalent cyber threats affecting healthcare institutions within the European Union (henceforth referred to as the EU) between January 2021 and May 2023 were data breaches (43%), disruptions to health services (22%), and the impact on patients due to the disclosure of confidential information (ENISA, 2023). It is evident that the manifestation of these and other cyber risks in the healthcare field is intended to compromise the security of medical data exchanges, resulting in its unauthorised disclosure or transfer to third parties. Primarily, these risks are directed towards the digital rights of patients and the financial and economic activities of healthcare institutions. In this regard, a significant problem that must be comprehensively addressed is the improvement of existing approaches in the EU and the Member States to forming business strategies of healthcare institutions based on modern methods of cyber risk management and ensuring the digital rights of patients.

The purpose of the article is to study the existing approaches to cyber risk management in the business strategies of healthcare institutions to reduce economic losses and ensure compliance with patients' digital rights, formulate proposals on this basis to improve the legislation of Ukraine and medical practice, taking into account the challenges of war.

The problem delineated in the article's purpose encompasses a combination of tasks that necessitate legislative, law enforcement, and doctrinal solutions. In particular, these include the need for doctrinal justification of causal relationships between cyber threats and violations of patients' digital rights, research of cyber risk management tools in the sense of a component of the business strategies of healthcare institutions, and the mechanism for complying with patients' digital rights; development of unified approaches to the formation of business strategies of healthcare institutions based on the integration of modern methods of detecting and stopping cyber threats, minimising the negative consequences of their manifestation, based on the best experiences of EU Member States; development of recommendations to improve the existing business strategies of healthcare institutions in terms of cyber risk management and compliance with patients' digital rights, based on the active application of international technical standards for cyber security ISO and cyber incident response plans.

Legislative and scientific support in solving these and other tasks is also important for the relevant areas of public life in Ukraine. In addition to Ukraine's European integration obligations and the orientation of its society towards the deep integration of European values in all spheres of public life, the healthcare sector in Ukraine is under the influence of significant systemic cyber threats.

The study used both general and specific scientific methods. For example, the dialectical method and the method of analysis and synthesis were used to identify common links between healthcare organisations' business strategies and cyber risk management tools in order to determine the best approaches to reducing healthcare organisations' economic losses and ensuring compliance with patients' digital rights. The statistical method was used to analyse statistical indicators of cyber risks in the activities of healthcare institutions registered in the EU, in order to assess the degree of impact of specific cyber threats on the digital rights of patients and the economic security of healthcare institutions. The modelling methodology was used to develop recommendations for the development of best practices for cyber risk management in the activities of healthcare institutions in the EU, based on the implementation of innovative cyber risk mitigation methods and international technical standard provisions in their business strategies. The comparative legal method allowed to identify common and different approaches of the EU and Ukrainian legislation in ensuring the cyber security policy of health care institutions and, on this basis, to formulate specific recommendations for improving the legislation of Ukraine in this area of legal regulation.

The objectives defined in this article determine the logic of the structure of the study. It provides for the definition of the concept and the analysis of the main groups of cyber risks observed in the activities of healthcare institutions in the EU, from the point of view of their economic consequences and their impact on the respect of patients' digital rights. Another component of the study is to analyse the cause-and-effect relationships between the manifestation of cyber threats and the effectiveness of healthcare organisations' business strategies in minimising negative economic consequences and respecting patients' digital rights. The study further

explores the legislative approaches of EU and Ukrainian law on cyber risk management policy in the medical field, taking into account the challenges posed by armed conflict. On this basis, a set of fundamental measures for cyber risk management is proposed, with the aim of integrating these into the business strategies of healthcare institutions in Ukraine. These measures are designed to counteract the negative consequences of cyber threats and ensure compliance with patients' digital rights, taking into account the challenges posed by armed conflict.

The theoretical basis of the study is as follows: the issues raised in this article have been the subject of research by many scientists and practitioners, who have analysed various aspects of ensuring cyber security in healthcare institutions.

In this paper, Schmittner C., Veledar O., Faschang T., Macher G., & Brenner E. (in a comparative legal context) analyse the EU Cyber Resilience Act (CRA), the aim of which is to increase cyber security and trust in the digital economy. Significant emphasis was placed on the impact of EU Directive 2022/2555 on the improvement of a system of measures to counter modern cyber threats, particularly in the field of healthcare. The authors highlight the achievements made by the EU in updating its cyber security legislation (Schmittner, 2024).

The article by Ksibi S., Jaidi F., & Bouhoula A. provides an analysis of the opportunities and challenges associated with the application of the Internet of Medical Things (IoMT) in the healthcare field. Scientists in their work explore the issues of security and cyber risk management in IoMT systems, proposing a business model for assessing and managing risks in these environments (Ksibi, 2023).

In their article, Almashaqbeh G., & Jansen conducted a comprehensive study of e-health systems (e-Healthcare) and related security issues, using the example of the medical Internet of Things. The researchers analyse existing methods for assessing cyber risks and propose a new model for improving trust and risk management in e-healthcare environments. The article also proposes a draft of an innovative model for managing cyber risks in healthcare institutions providing electronic healthcare services, especially in cross-border environments (Almashaqbeh, 2022).

Niemiec M., Pappalardo S. M., Bozhilova M., Stoianov N., Dziech A., & Stiller B. in their article propose a multi-level model of cyber risk management in different areas of public relations, especially in the e-health sector. The researchers recommend that the development of specific business strategies for cyber risk management should start with the most typical threats to individual critical infrastructure facilities and take into account the economic activities of healthcare institutions. In addition, the authors suggest paying special attention to threats such as data breaches, disruption of information exchange and the use of malware when developing cyber risk management approaches (Niemiec et al., 2022).

Another publication explores the ethical issues associated with the implementation of medical chatbots based on natural language processing. In this publication, the researchers place particular emphasis on patient privacy and the cyber security of medical information exchanges. The researchers emphasise the need to introduce special regulatory norms aimed at regulating the procedures for using chatbots based on language models in the practice of healthcare institutions (Kumar et al., 2022).

2. The Concept and Main Cyber Risks in the Activities of Healthcare Institutions

The fundamental concept, the accurate comprehension of which is contingent upon the efficacy of the business strategy in ensuring a healthcare institution's cyber security, is "cyber risk".

The accuracy of its definition and the identification of the main economic and legal characteristics of this concept allow not only to prevent in time the transformation of cyber risks into potential cyber threats, but also to find the causal relationship between the manifestation of cyber incidents and the facts of violation of patients' digital rights.

The main sources of EU cyber security legislation (EU Regulation 2019/881, 2019; EU Directive 2022/2555, 2022) do not currently contain a universal definition of cyber security threats. In a manner analogous to EU legislation, the Law of Ukraine "On the Basic Principles of Cyber security Assurance of Ukraine" (The Law of Ukraine "On the Basic Principles of Cyber security in Ukraine", 2017) does not contain a definition of the concept of "cyber risk", nor does it specify actions or activities. This ambiguity enables a generic interpretation of the concept, encompassing all forms of cyber threats and incidents (Semenchenko et al., 2020).

A systematic analysis of the EU legislation on cyber security (EU Regulation No. 2019/881; EU Directive No. 2022/2555) and certain provisions of the legislation of Ukraine on cyber security (Law of Ukraine No. 2163-VIII) allows to define the concept of "cyber risks" as potential threats, vulnerabilities and consequences that may arise as a result of the use of information and communication technologies, in particular in the event of unauthorised access, violation of the integrity, confidentiality or availability of data and systems.

The analytical report of the European Cyber security Agency "ENISA Threat Landscape: Health Sector (January 2021 to March 2023)" lists the following main groups of cyber threats to the EU e-Health sector,

which directly developed from the main types of cyber risks previously identified in the practice of medical organisations in the EU Member States:

Phishing attacks are attempts to trick people or organisations into providing sensitive information, such as login credentials or financial information, through fraudulent emails or websites. In the context of digital healthcare, phishing attacks can target healthcare professionals, employees or patients.

Ransomware attacks are a form of cyber-crime in which hackers encrypt data on a computer or network, rendering it inaccessible to the user. The hacker then demands a ransom in exchange for the decryption key. In the field of digital healthcare, the consequences of ransomware attacks can be severe, as they can prevent healthcare professionals from accessing patient data, which can result in delays in the delivery of care.

Malware, including viruses and spyware, has the potential to facilitate unauthorised access to sensitive information, such as login credentials and patient data.

Insider threats are threats that come from within the organisation, such as employees or contractors. Insider threats can include deliberate or careless disclosure of confidential information by employees of healthcare organisations, or data theft (ENISA, 2024).

Concurrently, the substantial augmentation in the implementation of innovative technologies, including artificial intelligence within the digital health sector, has precipitated the emergence of novel cyber risks that exert a deleterious effect on the assurance of digital rights for patients.

The report of the European Cyber security Agency on the risks of cyber threats in the use of artificial intelligence in the digital health sector, published in 2023, identifies, in addition to the cyber threats mentioned above, a separate group of specific cyber threats, the manifestation of which accompanies the use of artificial intelligence in the provision of medical services. Among these threats, the report identifies breaches of artificial intelligence algorithms as a result of cyber-attacks or other forms of unauthorised interference; opacity of machine learning algorithms or loss of control over decision-making processes by artificial intelligence; breaches of the integrity or unreliability of data used to train intelligent systems; internal interference in the operation of intelligent systems by medical professionals or third parties (*Cyber security and privacy in AI – Medical imaging, 2023).*

A generalisation of the content of the main types of cyber risks that accompany medical practice in the EU Member States shows that one of their obvious manifestations is the violation or significant restriction of patients' digital rights proclaimed in primary acts of EU law. In particular, the focus is on rights related to the processing of personal medical data, patients' rights of access to medical information, and the right to an adequate level of information security, especially in the digital health sector.

3. Justifying the Connection Between Cyber Risks and Patients' Digital Rights

In the field of legal literature, the properties of digital rights of citizens are indicative of their implementation in the virtual space, direct connection with the means of information processing, in particular, methods of ensuring the confidentiality of information about personal and family life, the need for electronic identification of a person or verification of digital documents, and the existence of additional cyber risks in the implementation of this category of rights (Pleskach et al., 2020).

In this study, an examination will be undertaken of the digital rights of patients, as influenced by the inherent existence of the individual and a state-guaranteed measure of possible (i.e., permitted) behaviour in the virtual sphere. The focus will be on the collection, storage, and dissemination of information about medical services; the disposal of personal medical data; the assurance of personal cyber security; and the fulfilment of other legitimate needs in the domain of digital healthcare.

The delineation of patients' digital rights in this manner signifies that their observance necessitates the passive or active comportment of healthcare institutions and public administration bodies in the health sector, with the aim of refraining from violating regulatory prohibitions or deliberately creating obstacles that impede patients' satisfaction of their needs.

Consequently, the necessity to uphold the digital rights of patients gives rise to a model of behaviour defined by law or contract for healthcare institutions, medical professionals, digital health service providers, and other authorised entities.

The primary acts of EU law that define the legal boundaries of such behaviour, namely the EU General Regulation 2016/679 on the protection of natural persons with regard to the automatic processing of personal data and repealing Directive 1995/46 (hereinafter referred to as GDPR) (EU Regulation 2016/679, 2016), EU Regulation 2019/881 (EU Regulation 2019/881, 2019) and EU Directive 2022/2555 (EU Directive 2022/2555, 2022), are based on the principles of "data protection by default and secure design".

This approach to the formation of lawful behaviour in the digital health sector can be explained by the fact that the GDPR classifies data on the mental and physical health of individuals as personal data, Article 4 (15) of the above-mentioned act of EU law. The processing of this category of personal data

is classified by the GDPR, according to the rules of Article 9 of the Regulation, as actions that may pose a particular risk to patients' rights. Accordingly, the processing of such data is permitted solely on the basis of the patient's voluntary and informed consent, specifically for the establishment of a clinical diagnosis, the administration of treatment, or the prevention of a disease, or for the purpose of medical research. This consent must be in accordance with the principles of confidentiality and the rights of the patient. Specifically, the patient's right to be informed about the purpose, methods, and means of data processing must be acknowledged, as must their right to be forgotten, the security of their data, its portability, the right to withdraw consent, and the right to object to further processing of medical data.

In the context of the secure design of medical information systems intended for the processing of patients' personal data, Article 25 of the GDPR stipulates that developers of such systems must incorporate data protection mechanisms into the system's design during the development phase. In particular, the minimisation of data collection, the encryption of patient data intended for automated processing and the pseudonymisation of personal data; the standard protection of medical personal data in accordance with Article 25 of the GDPR stipulates that all settings must be aimed at maximising the protection of patient data. For example, medical information systems must, by default, restrict access to data by third parties who are prohibited by law from accessing such data; patients' personal data must not be accessible to third parties without the patient's consent, Article 6(1)(a) (EU Regulation 2016/679, 2016).

In turn, Regulation (EU) 2019/881 introduces mandatory certification for IT products, services and processes, including medical information systems. This will ensure compliance with the security standards necessary to protect sensitive patient data, Article 54 of the aforementioned EU Regulation (EU Regulation 2019/881, 2019).

These and other EU laws provide a comprehensive legal framework for the proper respect of patients' digital rights in EU Member States.

Based on the approach to the mechanism for regulating patients' digital rights established in EU legislation, the following criteria can be distinguished for assessing the state of compliance with the mechanism for managing cyber risks in the digital health sector:

1. Any identification or authentication of patients, as well as the verification of their documents, may only be carried out for legal reasons and for a predetermined purpose.

2. The regulatory establishment of prohibitions on the creation and use of digital services aimed at restricting the digital rights of patients or their access to their own medical data entails the emergence of obligations for authorised medical organisations or bodies to carry out any actions related to the use of these services.

3. Digital health services, in particular the means of storing and transmitting medical data, should be protected at a level that minimises the risks of unwarranted intrusion into patients' private lives and reduces the risks of negative impact on them.

4. Every patient should be adequately informed about the operation of intelligent data processing systems or the provision of public services in the field of digital health that are used or may be applied to them.

5. Developers, suppliers and operators of IT solutions for digital health should refrain from using inaccurate or illegally collected data. They should also avoid providing compromised IT products or solutions that could lead to unjustified restriction of patients' digital rights or to the manifestation of cyber risks in the health sector.

6. Medical organisations and public administration bodies of the digital health sector are obliged to refrain from cases of unauthorised collection or automated processing of information about patients, in order to prevent cases of unreasonable ignorance of the facts of their prohibition of further processing of confidential medical data.

The proposed criteria for assessing the state of compliance with patients' digital rights are based on the approaches proclaimed in the primary sources of EU law to ensure the cyber security of medical information systems according to the principles of secure design and adequate protection of medical data by default. The legalisation of such an approach to ensuring the cyber security of medical organisations in EU legislation leads to the emergence of obligations for their heads and authorised management bodies to implement innovative methods of cyber risk management at all stages of the functioning of medical information systems.

This makes it possible to link regulatory requirements for ensuring patients' digital rights with cyber risk management methods in the practice of healthcare institutions. In this respect, cyber risk management methods are integrated into the general mechanism of guaranteeing patients' digital rights, and compliance with these rights in the activities of specific organisations can be considered an indicator of the effectiveness of the business strategy of healthcare institutions.

The development of an approach to ensuring the cyber security of healthcare institutions, based on a combination of general and special regulation of relevant public relations, as well as the legislation of Ukraine, simultaneously omits certain aspects of the problems raised in this work from legal regulation.

In particular, this concerns the right of certain patients to ensure the confidentiality of their personal data. This encompasses a range of rights, including the right to be forgotten, the right to secure processing of personal data, the right to be informed about the use of intelligent systems for processing personal data, and the right to the portability of personal data. In addition, in the provisions of the Laws of Ukraine "On the Basic Principles of Cyber security in Ukraine" (The Law of Ukraine "On the Basic Principles of Cyber security in Ukraine", 2017), "On Personal Data Protection" (The Law of Ukraine "On Personal Data Protection", 2010), "On Information Protection in Information Communication Systems" (The Law of Ukraine "On Information Protection in Information Communication Systems", 1994) and other laws, the issue of applying the principles of ensuring cyber security of medical information systems according to the principles of secure design and data protection is regulated by default compared to acts EU law to a sufficient extent.

Despite the existence of some discrepancies in the legislative support for the mechanism for the formation of business strategies of healthcare institutions, the fulfilment of Ukraine's European integration obligations necessitates the acceleration of the implementation of the experience of the EU Member States in ensuring the digital rights of patients based on the use of innovative methods of ensuring cyber security.

4. Analysis of Modern Approaches to Countering Cyber Threats in the EU and Their Implementation in the Practice of Ukrainian Healthcare Institutions in the Context of the Challenges of War

In the scientific literature, the problem of determining the system of cyber risk management tools is traditionally approached by taking into account the peculiarities of the functioning of specific sectors of the national economy (Kruse et al., 2017).

At the same time, there is a widespread view among cyber security gap researchers that the system of cyber risk management tools should not only be consistent with their possible economic, legal and organisational consequences, but also be based on generally binding technical requirements of a regulatory nature (Semenchenko et al., 2020, p. 284; Schmittner et al., 2024). Firstly, it is important to note that the subject under discussion pertains to international ISO standards, which delineate the optimal methodologies for the management of cyber risks within the context of the activities of healthcare institutions.

A systematic analysis of ISO standards in the healthcare sector enables to identify the following groups of cyber risk management measures that can be aimed at respecting patients' digital rights and reducing the negative property consequences of cyber threats:

– Cyber hygiene in the work of medical personnel. Employees should be trained in cyber security best practices, such as how to recognise phishing attempts and how to properly handle confidential information, the disclosure of which could lead to a violation of patients' digital rights or damage to the property of medical organisations due to additional risks caused by hostilities.

– Network security. Firewalls and other security measures should be incorporated into the business strategies of healthcare facilities to protect the network and prevent unauthorised access to the information resources of these organisations, taking into account the systemic risks associated with hybrid warfare against Ukraine.

– Encryption. Sensitive information, such as patient data, should be encrypted both in transit and at rest in databases to protect against data leakage.

– Regular security audits and penetration testing of healthcare information systems. Regular security audits and penetration testing should be part of the business strategy of healthcare organisations to identify and address vulnerabilities in healthcare systems.

– Developing and integrating cyber incident response plans into the business strategies of healthcare organisations, particularly as a result of the manifestation of war against Ukraine. The modern business strategy of every healthcare institution must include a plan for rapid and effective response to any security incidents that may occur in the practice of healthcare institutions and subsequently cause negative property or reputational consequences.

– Adherence to international and national technical standards. Healthcare institutions must comply with international and national standards that define the requirements for cyber security policies in the design and use of medical information systems to increase the effectiveness of their business strategies and meet the digital rights of patients in their operations.

– Cyber risk management in all supply chains of medical equipment or software. In order to reduce cyber risks and ensure respect for the digital rights of patients, particularly those most vulnerable to the consequences of war (military personnel, children, internally displaced persons), when implementing information and communication technologies in the practice of medical organisations, such organisations should implement a set of legal, organisational and technical measures aimed at preventing negative property consequences at each stage of the supply of medical equipment and technologies, including the selection, testing, purchase and adaptation of appropriate means, the introduction of special technical

means designed to prevent the processing of personal data of certain groups of patients who are more vulnerable to the consequences of war.

– Remote Access Cyber security. With the growth of telemedicine and remote working, it is important to ensure secure remote access to the healthcare organisation's network and data. This can include the implementation of two-factor authentication, VPNs and monitoring of remote access activity by healthcare professionals and patients on local healthcare information networks.

– Security of connected medical devices. In the context of the war against Ukraine and the significant war risks for many EU Member States, ensuring the security of connected medical devices is critical to protect the integrity of patient data and device functionality. This can include implementing secure software development practices, regular software updates and network segmentation.

– Use of artificial intelligence technologies for cyber risk management. In order to increase the effectiveness of the business strategies of medical organisations in countering cyber risks and respecting patients' digital rights, the implementation of certain groups of tasks can be entrusted to intelligent agents and management decision support systems. The use of artificial intelligence for the implementation of these tasks can be carried out, among others, in such areas as identification and economic assessment of cyber risks, formation of recommendations on tactical measures to respond to such risks, development of recommendations for improving the business strategies of medical organisations to reduce the risks of economic losses from possible manifestations of cyber threats and violations of patients' digital rights.

Regarding the last recommendation, it should be emphasised that the integration of artificial intelligence into the business strategies of healthcare organisations is possible if this technology is used legally.

Legal doctrine has developed separate evaluation criteria for assessing the degree of integration of artificial intelligence into the activities of medical organisations: normative, legal and factual. The essence of the first of these criteria is the need for the mandatory existence of national legislation on which the use of artificial intelligence in medical practice can be based. The legal criterion is manifested in the need for medical organisations to establish in the terms of contracts, local laws, business strategies specific conditions for the use of artificial intelligence in the provision of medical services, the principles of maintaining the confidentiality of patient data and respect for their digital rights in medical practice. The actual criterion is found in the existence of a case in medical practice, in the presence of which the use of artificial intelligence is justified and does not create greater risks for the patient than those that could exist without the use of the appropriate technology (Zayarnyi, 2019).

Taken together, the above-mentioned criteria for assessing the degree of legality of the use of artificial intelligence have found their consolidation and detailed regulation in the provisions of the Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act, 2024).

In terms of content, these measures cover all stages of healthcare organisations' business strategies for cyber risk management, including the secure design of medical information systems and the protection of patient data in accordance with the principles of safe use. They can be both legal and organisational in nature. However, according to their purpose and application objectives, these measures aim to respect the digital rights of patients and to prevent or reduce the property losses of healthcare organisations from the possible manifestation of cyber threats.

5. Conclusions

The study of cyber risk management in the business strategies of healthcare institutions, in the context of overcoming negative economic consequences and respecting the digital rights of patients in the EU, allows the following main conclusions to be formulated for Ukraine, taking into account the challenges of the war.

1. In the EU and Member States, the main groups of cyber risks associated with the activities of healthcare institutions are theft of confidential patient data and financial information, phishing attacks on medical information systems, or loss of access by healthcare workers to their automated workstations.

2. EU legislation imposes obligations on healthcare institutions to base their business strategies on the implementation of rules for the secure design of medical information systems and to ensure reliable protection of patient data based on its lawful use. Implementing this approach at the level of primary acts of EU law means integrating cyber risk management tools into all stages of healthcare institutions' business strategies and policies to protect patients' rights.

3. Compared to the primary acts of EU law, the legislation of Ukraine does not sufficiently regulate public relations on cyber risk management as a component of business strategies of healthcare institutions, taking into account the challenges of war. It is this author's opinion that in order to eliminate this problem, the Law of Ukraine "On the Basic Principles of Cyber security in Ukraine" should introduce a rule on the need to ensure the mandatory cyber security of critical infrastructure facilities, in particular

healthcare institutions, based on the implementation of the principles of safe design and protection of medical data according to the rule of safe processing. It is also important to introduce a norm in Ukraine on forming a single database of cyber incidents in Ukraine with a breakdown by sectors of the national economy. At the same time, the Law of Ukraine "Fundamentals of the Legislation of Ukraine on Health Care" considers it relevant to make additions, according to which the electronic processing of medical data of military personnel, prisoners of war and journalists in the course of war reporting can be carried out only if the collection of personal data is minimised, automatic digital identifiers are introduced for the processing of personal data of these categories of patients, and the period of storage of such data is limited to the period of treatment and rehabilitation of patients.

4. In order to optimise the costs of healthcare institutions in dealing with the consequences of cyber threats and violation of patients' digital rights, both EU Member States and Ukraine see the expansion of the scope of application of artificial intelligence technologies. The main areas of application of this technology can be, among other things, the testing of medical information systems to identify cyber risks, the optimisation of business strategies for cyber risk management, the development of proposals for improving the privacy of medical data of certain categories of patients, etc. In order to form a solid legal basis for implementation in Ukraine it is necessary to adopt the Law of Ukraine "On the Basic Principles of the Development and Application of Artificial Intelligence in Ukraine", which implements the provisions of the EU AI Act.

5. In order to avoid the emergence of additional risks associated with the introduction of artificial intelligence into the business strategies of healthcare institutions, it is important for the latter to be guided by the criteria for assessing the degree of lawful use of this technology developed by legal doctrine and enshrined in the EU AI Act.

6. As a systematic analysis of scientific sources, EU legislation and the provisions of international ISO standards has shown, among the main cyber risk management tools to be implemented in the business strategy of healthcare institutions, it is necessary to highlight the cyber hygiene of medical staff, supply chain management of medical equipment and digital content, encryption of medical data, means to counter phishing attacks and spamming, and artificial intelligence tools. In order to ensure a systematic approach to the implementation of these tools in the business strategy of healthcare organisations, it is important to comply with international cyber security standards, primarily those of the International Committee for Standardisation.

7. Ensuring the uniformity of approaches to the legislation of Ukraine and the EU in observing the digital rights of patients necessitates the processing of medical data in accordance with the rights of patients to free, informed consent for the processing of their personal data, the establishment of conditions for the exercise of the right to portability of medical data, the right to withdraw consent or the right to be forgotten in medical information systems. To this end, it is imperative for healthcare institutions to develop their own health data privacy policies and to integrate these policies into their overall business strategies.

References:

Almashaqbeh, G., & Jansen, N. (2022). A Comprehensive Study of Security and Cyber-Security Risk Management in e-Healthcare Environments. Mobile Networks and Applications.

Directive (EU) 2022/2555 on measures for a high common level of cyber security in the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

European Parliament and Council (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 March 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act). Available at: http://data.europa.eu/eli/reg/2024/1689/oj

European Union Agency for Cyber security (ENISA) (2023). Cyber security and privacy in AI – Medical imaging diagnosis. European Union Agency for Cyber security. Available at: https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis

European Union Agency for Cyber security (ENISA) (2023). ENISA Threat Landscape: Health Sector (January 2021 to March 2023). European Union Agency for Cyber security. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-health-sector

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cyber security in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, Vol. 25(1), p. 1–10. DOI: https://doi.org/10.3233/THC-161263

Ksibi, S., Jaidi, F., & Bouhoula, A. (2023). IoMT Applications Perspectives: From Opportunities and Security Challenges to Cyber-Risk Management. In Decision Making and Security Risk Management for IoT Environments (pp. 21–37). Springer.

Kumar, N., & Tripathi, R. (2022). Healthcare Chatbots with NLP and Cyber security: Safeguarding Patient Rights and Privacy. Paper presented at the 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud).

Niemiec, M., Pappalardo, S. M., Bozhilova, M., Stoianov, N., Dziech, A., & Stiller, B. (2022). Multi-sector Risk Management Framework for Analysis Cyber security Challenges and Opportunities. In Multimedia Communications, Services and Security (pp. 49–65). Springer.

Pleskach, M., Zaiarnyi, O., & Pleskach, V. (2020). Respect for Information Rights of a Person as a Condition for Cyber security of Smart Cities Residents. *10th International Conference on Advanced Computer Information Technologies (ACIT),* 759–764. Available at: https://ieeexplore.ieee.org/document/9208977

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on the European Union Agency for Cyber security (ENISA) and on information and communications technology cyber security certification and repealing Regulation (EU) No 526/2013 (Cyber security Act). Available at: https://zakon.rada.gov.ua/laws/show/984_024-19#Text

Schmittner, C., Veledar, O., Faschang, T., Macher, G., & Brenner, E. (2024). Fostering Cyber Resilience in Europe: An In-Depth Exploration of the Cyber Resilience Act. In Systems, Software and Services Process Improvement (pp. 390–404). Springer.

Semenchenko, A., Pleskach, V., Zaiarnyi, O., & Pleskach, M. (2020). Cyber security and cyber protection: The current state of public administration in Ukraine. In Proceedings of the 12th International Scientific and Practical Conference of Programming (UkrPROG 2020) (pp. 280–289), September 15–16, 2020, Kyiv, Ukraine. CEUR Workshop Proceedings. Available at: https://ceur-ws.org/Vol-2866/ceur_276_283_pleskach.pdf

The Law of Ukraine "On Personal Data Protection" of June 1, 2010, No. 2297-VI. Available at: https://zakon.rada.gov.ua/laws/show/2297-17

The Law of Ukraine "On Information Protection in Information Communication Systems" of July 5, 1994, No. 80/94-BP. Available at: https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

The Law of Ukraine “On the Basic Principles of Cyber security in Ukraine” of October 5, 2017, No. 2147-VIII. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text

Zaiarnyi, O. A. (2019). Assessment criteria for the lawfulness of artificial intelligence technologies application in health care. *Wiadomości Lekarskie*, 72(12, Pt. II), 2568–2572. Available at: https://www.researchgate.net/publication/339723357_Assessment_criteria_for_the_lawfulness_of_artificial_intelligence_technologies_application_in_health_care

Received on: 10th of January, 2025
Accepted on: 21th of February, 2025
Published on: 13th of March, 2025