UDC 351.86:004.056:614(048.8)(477) https://doi.org/10.26641/2307-0404.2024.4.319402

I. Parfonova [1],
O. Zinchenko [2]

CYBERSECURITY ENHANCEMENT IN THE FIELD OF EHEALTH SYSTEM DEVELOPMENT IN UKRAINE (REVIEW)

Kharkiv National Medical University [1]
Nauky ave., 4, Kharkiv, 61000, Ukraine
e-mail: Managerhnmi@proton.me
V.N. Karazin Kharkiv National University [2]
Svobody area, 4, Kharkiv, 61022, Ukraine
[*]e-mail: alekca.98@ukr.net
Харківський національний медичний університет [1]
пр. Науки, 4, Харків, 61000, Україна
Харківський національний університет імені В.Н. Каразіна [2]
майдан Свободи, 4, Харків, 61022, Україна

***Цитування:** Медичні перспективи. 2024. Т. 29, № 4. С. 247-256*
***Cited:** Medicni perspektivi. 2024;29(4):247-256*

Key words: *confidential information, cyberattacks, cybersecurity, eHealth system, European legal sources*
Ключові слова: *конфіденційна інформація, кібератаки, кібербезпека, електронна система охорони здоров'я, європейські правові джерела*

Abstract. Cybersecurity enhancement in the field of eHealth system development in Ukraine. Parfonova I., Zinchenko O. *Today, more than ever, cybersecurity issues are crucial in all industries and sectors, yet healthcare remains the most vulnerable. This work aims to analyze the state of cybersecurity in the most successful European countries and to outline the main steps for strengthening cybersecurity in Ukraine's electronic healthcare system. A review of literature on electronic healthcare and cybersecurity in Europe and Ukraine was conducted using Web of Science, SCOPUS, Google Scholar, and legislative databases from each of the analyzed European countries, covering a total of 49 sources from 2020 to 2024. The search was conducted using scientific terms such as "eHealth system", "cyberattack", "cybersecurity", "medical information systems", "EU4 Health", "electronic healthcare", "digital healthcare services", "Ministry of Health", "confidential information", "legislative framework". A total of 83 sources were initially selected and reviewed. After systematizing the gathered information, 55 of the most relevant sources were retained. Exclusion criteria included publications that did not align with the purpose of this review. The methods used included bibliographic, analytical, and forecasting. The analytical method was applied to compare Ukraine's approach to ensuring cybersecurity in electronic healthcare with those of countries such as Estonia, Germany, France, and the United Kingdom, allowing the identification of key differences and potential improvements for Ukraine's system. Additionally, the forecasting method was used to assess future initiatives and plans in eHealth cybersecurity that should be implemented to further develop Ukraine's protective systems. First, a clear concept of "cybersecurity of electronic healthcare" was formulated, identifying its key components. Second, the establishment of a regulatory framework was proposed to detail the aspects of cybersecurity in electronic healthcare, including guidelines and methods for supporting and improving protection systems in medical institutions. It is recommended to incorporate these provisions into the laws "On Cybersecurity" and "Fundamentals of Ukrainian Legislation on Healthcare" to enhance the effectiveness of cybersecurity measures in healthcare. Thirdly, we analyze the effectiveness of the most common cybersecurity tools and provide recommendations for their use in Ukraine: introducing regular backups for all medical systems, setting up firewalls, centralized IDS/IPS systems, mandatory data encryption, enhanced VPN authentication, automated threat monitoring systems, and engaging experts to ensure comprehensive cybersecurity of medical institutions. This will help to preserve significant amounts of confidential information and ensure the possibility of recovering lost data. The need to adapt the best European practices to the special conditions in Ukraine to work confidently in the face of potential and real threats was emphasized, which will allow timely response to new challenges and ensure cybersecurity.*

Реферат. Посилення кібербезпеки у сфері розвитку системи електронної охорони здоров'я в Україні. Парфьонова І., Зінченко О. *Сьогодні, як ніколи, стають актуальними питання кібербезпеки в усіх галузях та сферах, але найбільш вразливою є охорона здоров'я. Метою цієї роботи було проаналізувати стан кібербезпеки в найуспішніших країнах Європи і сформулювати основні кроки для посилення кібербезпеки в електронній системі охорони здоров'я України. Огляд літературних джерел з питань електронної охорони здоров'я та кібербезпеки в Європі та Україні проводився за допомогою Web of Science, SCOPUS, Google Scholar, а також*

законодавчих баз кожної з описаних Європейських держав загальною кількістю 49 джерел за період з 2020 року до 2024 року. Пошуки проводилися з використанням таких наукових термінів: «eHealth», «кібератака», «кібербезпека», «медичні інформаційні системи», «EU4 Health», «електронна охорона здоров'я», «цифрові медичні послуги», «МОЗ», «конфіденційна інформація», «законодавча база». Усього при первинному аналізі було відібрано та опрацьовано 83 джерела літератури. Після систематизації відібраної інформації залишилось 55 найбільш релевантних джерел. Критеріями виключення були публікації, які не відповідали меті цього огляду. Використані методи: бібліографічний, аналітичний та метод прогнозування. Аналітичний метод був застосований для порівняння підходів України до забезпечення кібербезпеки електронної охорони здоров'я з підходами таких країн, як Естонія, Німеччина, Франція та Сполучене Королівство. Це дозволило виявити ключові відмінності та можливості до вдосконалення української системи. Крім того, метод прогнозування був використаний для оцінки майбутніх ініціатив та планів у сфері кібербезпеки електронної охорони здоров'я, що мають бути впроваджені для подальшого розвитку системи захисту в Україні. По-перше, була сформульована чітка концепція «кібербезпеки електронної охорони здоров'я» з визначенням її основних компонентів. По-друге, запропоновано створення нормативно-правової бази, яка детально буде регламентувати аспекти кібербезпеки електронної охорони здоров'я, правила та методи підтримки й вдосконалення систем захисту в медичних установах. Ці положення рекомендовано включити до законів «Про кібербезпеку» та «Основи законодавства України про охорону здоров'я», що дозволить підвищити ефективність заходів з кібербезпеки в охороні здоров'я. По-третє, проведено аналіз ефективності найпоширеніших інструментів кібербезпеки та надані рекомендації щодо їхнього застосування в Україні: запровадження регулярного створення резервних копій для всіх медичних систем, налаштування міжмережевих екранів, централізованих систем IDS/IPS, обов'язкового шифрування даних, посиленої автентифікації VPN, автоматизованих систем моніторингу загроз та залучення експертів для забезпечення комплексного кіберзахисту медичних установ. Це сприятиме збереженню значних обсягів конфіденційної інформації та забезпечить можливість відновлення втрачених даних. Наголошено на потребі адаптування найкращих європейських практик до особливих умов в Україні для впевненої роботи в умовах потенційних і реальних загроз, що дасть змогу своєчасно реагувати на нові виклики та забезпечувати кібербезпеку.

Nowadays, technologies are rapidly developing and influencing many aspects of our lives. People today cannot imagine their lives without the Internet, which is explained by the using various service convenience. However high technologies used in various spheres provoke ease of strikes through the global network, this demands for the reliability of data storage, speed and economy of data transmission, minimization of risks of their loss and confidentiality violation etc...

Cybersecurity of the eHealth system has become an important issue. The electronic healthcare development has undergone a rapid transition to digital transformation. Issues related to the functioning of electronic healthcare are predominantly discussed by experts such as O.A. Muzika-Stefanchuk with co-authors, elucidated legal aspects of providing public administrative services in the healthcare sector in the article "Public administrative services in healthcare" [1]; I.V. Venediktova's article "Public services in the medical sphere" examined the specifics of providing public services in the medical field [2]; O.M. Shevchuk and co-authors clarified the peculiarities of legal regulation of providing medical services in the article "Aspects of legal regulation of the provision of medical services" [3], A. Velikanov in the article "Content of public electronic services in healthcare" [4] explored the essence and content of providing public electronic services in healthcare in the context of the development of administrative law science and public administration theory, etc. Analysis of domestic and foreign works on the research topic indicates that the issue of implementing electronic healthcare has been attracting the attention of scholars for many years. For instance, N.O. Vasyuk, A. Genova, D.O. Homon, H.V. Mulyar, V. Tuziyn, and many others studied some aspects of this topic. Today healthcare organizations possess large volumes of confidential data and critically important medical information, such as medical histories, test results, diagnoses and treatments, as well as information about insurance, payment details, electronic medical records, and medical equipment that is managed and serviced using network technologies. Lately it can be observed that computerized hospital equipment is becoming increasingly vulnerable to cyberattacks. The cyberattacks can damage equipment for monitoring, treatment, and patient support, sometimes leading devices to be temporarily disabled, which can significantly affect the treatment, cause significant harm to patients' lives and health, and in some situations even lead to fatalities.

On this basis, the purpose of the article was to analyze the state of cybersecurity in the most successful European countries and to formulate the main steps to strengthen cybersecurity in the Ukrainian eHealth system.

MATERIALS AND METHODS OF RESEARCH

The comprehensive analysis of eHealth systems and cybersecurity issues presented in this article is supported by a number of methods. The review of literature on cybersecurity in electronic healthcare

was conducted using a variety of academic and regulatory resources to gain a comprehensive understanding of contemporary approaches and challenges in this field, taking into account the experiences of European countries and Ukraine.

The tools for gathering sources included the scientific databases Web of Science Core Collection (https://www.webofscience.com/wos/woscc/basicsearch), Scopus (https://www.scopus.com) and Google Scholar (https://scholar.google.com.ua), along with legislative databases providing access to regulatory documents from various European states. A total of 49 selected sources were analyzed, encompassing materials published from 2009 to 2024. No. restrictions were placed on publication date or language, allowing for the inclusion of a broad range of available materials.

To efficiently filter relevant literature, specialized search terms were employed, covering key aspects of electronic healthcare and cybersecurity, such as “eHealth”, “cyberattack”, “cybersecurity”, “medical information systems”, “EU4 Health”, “electronic healthcare”, “digital healthcare services”, “Ministry of Health”. During the initial selection phase, 83 sources were identified, from which, after systematization and assessment for alignment with the review's objectives, 55 of the most relevant sources were retained for analysis. An essential criterion in this selection process was the alignment of each material with the specific goals of the review, leading to the exclusion of publications that did not meet the defined criteria and focus of the study.

However, the issue of implementing eHealth in wartime, as well as ensuring cybersecurity of eHealth in Ukraine, has hardly been studied by scholars, which underlines the relevance and practical significance of this work. The research method used was to analyze peer-reviewed articles published over the past decade that focus on the intersection of technology, healthcare and cybersecurity. This method of analysis allows conducting a thorough study of existing research in the field, identifying trends, gaps and emerging topics. In addition, Ukraine's approach to eHealth cybersecurity was benchmarked against that of other European countries such as Estonia, the United Kingdom, Germany and France. This method helps to identify best practices, potential solutions and areas for improvement in different health systems. By comparing approaches, the article aims to highlight the unique challenges Ukraine faces and potential lessons learnt from other countries. For these purposes electronic legal bases of all the mentioned countries were used.

Based on the results of this article, a foresight approach was applied, namely, future initiatives and plans to improve cybersecurity measures of the eHealth system in Ukraine. This forward-looking approach helps to identify potential solutions and areas for future research. By exploring the proposed policies and methods, the article contributes to the development of effective strategies for improving cybersecurity in healthcare systems. Together, these methods provide a comprehensive analysis of the complex relationship between technological advances, healthcare delivery, and cybersecurity issues, especially in the current situation in Ukraine.

The research was conducted in accordance with the principles of bioethics set out in “Universal Declaration on Bioethics and Human Rights” (UNESCO) and was approved by the Bioethics Commission of the Kharkiv National Medical University (dated Nov. 11, 2024).

RESULTS AND DISCUSSION

According to Article 3 of the “Fundamentals of the Legislation of Ukraine on Healthcare”, an electronic healthcare is an information and communication system that facilitates the automation of medical service accounting and management of healthcare information, including medical information, through the creation, hosting, publication, and exchange of information, data, and documents electronically. This system includes a central database and electronic medical information systems, between which automated information exchange is ensured via an open application-programming interface (API) [5].

The European Commission prioritizes digital healthcare within the single digital market, supported by EU legislation on medical devices, data protection, and digital identity. Rapidly adopted eHealth strategies in the EU, along with the “European Health Strategy 2020” and WHO-aligned “Health 2020”, promote innovation to address public health challenges and improve population health. [6]. Achieving the outlined goals accelerates the resolution of key challenges in electronic healthcare. Strategic innovations streamline processes at all levels, introducing tools like electronic prescriptions, medical histories, online forms, and digital medical records, simplifying treatment procedures. By 2025, 25 EU countries will gradually implement these eHealth services.

The EU4 Health program, launched during the COVID-19 pandemic for 2021-2027, addresses healthcare system vulnerabilities exposed by the crisis. It focuses on strengthening response capabilities and creating more resilient and accessible healthcare systems. Ukraine participates in this program as an associated country under the “Agreement between Ukraine and the European Union on the participation of Ukraine in the EU4 Health program”. As part of this, Ukraine makes annual

financial contributions proportional to the Union's budget allocations for the program [7].

A significant milestone was reached at the seventy-second session of the WHO Regional Committee for Europe in Tel Aviv in 2022 with the adoption of the Regional Action Plan for Digital Health for 2023-2030. This plan outlines four strategic priorities to advance digital transformation in healthcare, including establishing standards, developing technical guidance, and enhancing countries' capacity for effective strategic leadership in digital healthcare transformation [8]. The regional plan is also based on the Global Strategy on Digital Health for 2020-2025, the Thirteenth General Programme of Work for 2019-2025, and the European Work Programme for 2020-2025 [9].

In recent years, Ukraine has undergone significant digital transformations in healthcare, with legislation recognizing eHealth as fundamental to the sector's development. The 2016 Health Care Financing Reform Concept introduced the "money follows the patient" [10] principle via an electronic system. In June 2017, primary care facilities in Kyiv, Cherkasy, and Dnipro joined eHealth in its pilot phase [11]. By February 2018, intellectual property rights for the system were transferred to the Ministry of Health, which now oversees its development through the State Enterprise "Electronic Health" [12], established in December 2017.

State Enterprise Electronic Health serves as the primary developer of Ukraine's eHealth technical infrastructure. The system includes a central medical data component managed by SE eHealth, alongside medical information systems. The Ministry of Health oversees eHealth implementation through regulatory measures, while the National Health Service of Ukraine (NHSU) reimburses medical institutions for the services they provide [13, 14]. In 2019, Ukraine expanded eHealth with pharmacy registration under the NHSU reimbursement program. By 2020, electronic and paper referrals coexisted due to partial adoption of the system. Cybersecurity experts, including a "Big Four", ensured system reliability through comprehensive audits during development [15].

On April 1, 2020, a new stage of healthcare reform began, impacting secondary healthcare. During the "DigitalMed 2020" sessions in October 2020 [16, 17], Denis Tsvaig, president of the National Cybersecurity Association, warned of the risks in electronic systems, highlighting that critical devices could be remotely disabled. He stressed the need for a state-level cybersecurity strategy with clear protocols to prevent and address cyberattacks. These concerns are valid, as rapid automation in healthcare has often sidelined cybersecurity, increasing vulnerabilities. On December 28, the Cabinet of Ministers of Ukraine approved the Concept for the Development of the Electronic Healthcare System. The implementation of the Concept is envisaged for the period until 2025 and involves addressing existing problems and challenges by ensuring the implementation of comprehensive measures in the following directions: regulatory support for the development of the electronic healthcare system; organization, management, and technical support for the development of the electronic healthcare system; resource provision; ensuring the quality, safety, and accessibility of the electronic healthcare system [18]. Throughout 2023, Ukraine successfully implemented a number of innovative digital projects in the field of electronic healthcare (electronic prescriptions, reimbursement program, COVID certificates, electronic record of rehabilitation interventions, electronic inventory management system for medicines and medical products "e-Stock", "MedData" system expansion, digitization of military medical commissions, telemedicine development [19]. So, we can generalize that Ukraine has developed a healthcare electronic monitoring system in a fairly short time and under difficult conditions of martial law. Considering the advanced state of this sector in many EU countries, Ukraine is striving to take all possible measures to improve this system, bring it to a high level of operation, and learn from the experience of leading European countries not only in organizing electronic healthcare systems but also in addressing one of the urgent problems hindering the successful operation of the system, namely its cybersecurity.

Estonia's electronic healthcare project, launched in 2008 [20], began with online patient data access and later expanded to include digital prescriptions, referrals, and medical history tracking. Patients and doctors benefit from seamless access to medical records, improving care and reducing state costs. Estonia's innovative approach has made it a global leader in eHealth.

The United Kingdom exemplifies the complexity of constructing a healthcare system, with each of its four countries operating its own healthcare service, all funded by the National Health Service (NHS) [21]. Despite their independence, these services collaborate closely to ensure uniform care quality for all citizens. In Wales, the NHS is accountable to the Welsh Assembly Government, a decentralized administration with powers derived from the UK Parliament. In 2010, the NHS in Wales launched a program to develop new methods, tools, and technologies to improve medical services. Its eHealth strategy for 2016-2026 [22] focuses on delivering excellent healthcare services. In Scotland [23], the NHS is overseen by the Scottish Government and operates

under its own electronic healthcare strategy, managed by the Scottish Department of Health. The first health and social care data strategy, published in February 2023, outlines plans to optimize data use for service development and provision. Northern Ireland combines healthcare and social care under the jurisdiction of the Department of Health, Social Services, and Public Safety within the Northern Ireland Executive. It has its own eHealth strategy, complemented by the Digital Health Strategy for 2022-2026 and a Cybersecurity Strategy for Healthcare and Social Services for 2022-2026. These strategies focus on innovative products, enhanced security management, and new structures to strengthen cybersecurity [24, 25].

In Germany, in the light of rapid technological advancements the IT Security Act has been adopted. The BSI (Federal Office for Information Security) develops standards and recommendations for cybersecurity. In collaboration with healthcare, it provides guidance and supports the development of secure information systems [26]. The GDPR (General Data Protection Regulation) ensures the protection of personal data, including medical information, and requires medical institutions to implement appropriate security measures for processing such data [27].

France's Dossier Medical Partagé (DMP) system, launched in 2004 to enhance patient care and coordination among medical professionals, faced significant challenges. By 2008 and 2013, government reviews highlighted its shortcomings, leading to a reorientation of the program. To address these issues, the National Agency for the Security of Information Systems (ANS) introduced two key frameworks in 2012: a general security policy for healthcare information systems to establish security standards and a compatibility framework for technical and semantic interoperability [28, 29]. These measures aimed to strengthen the DMP and improve digital healthcare infrastructure. In June 2023, ANS launched the Priority Research and Infrastructure Program for Digital Healthcare (PEPR) to position France as a leader in digital health innovation. The 2023-2027 Digital Healthcare Roadmap, introduced in May 2023, fosters collaboration among government agencies, healthcare professionals, companies, and citizens to advance France's digital health initiatives [30].

Therefore, the example of France is of great significance for Ukraine, as the creation of an electronic healthcare system is one of Ukraine's main state priorities.

Cybersecurity is essential in healthcare digitization, as cyberattacks increasingly jeopardize operations, patient data, and lives. Dependency on digital systems has exposed vulnerabilities, with ransomware posing significant threats. The WannaCry ransomware attack on May 12, 2017 [31], became the largest cyberattack in the UK, severely disrupting the National Health Service (NHS). Though not the primary target, it affected 603 primary care facilities and 8% of GP practices, compromising critical systems like clinical information access and test results. Third-party services, such as DocMan42 [32], which manages clinical data flow, were also impacted. This incident highlighted the NHS's susceptibility to ransomware and the urgent need for stronger cybersecurity defenses. Another significant attack occurred in 2020 when Germany's University Hospital of Düsseldorf experienced a ransomware attack that infiltrated 30 hospital servers. This incident caused system failures, forcing the hospital to redirect emergency patients to other facilities. The attack, linked to the Ryuk ransomware [33, 34, 35], led to severe operational disruptions and indirectly contributed to the death of a woman when emergency care was delayed. This tragic event highlighted the potentially fatal consequences of cyberattacks on healthcare systems, which are becoming increasingly common as hospitals are often targeted due to their reliance on uninterrupted access to patient data and computer systems. In May 2021, Ireland's Health Service Executive (HSE) faced a devastating ransomware attack [36], described as the most significant cyberattack on the Irish state. Around 40 hospitals were affected, requiring weeks to restore electronic systems. The attack disrupted operations and highlighted vulnerabilities in healthcare infrastructure, underscoring the need for preparedness and coordinated response strategies to mitigate such risks.

France, too, faced a wave of cyberattacks during the COVID-19 pandemic, which created fertile ground for cybercriminals targeting overstretched healthcare systems. In February 2021, 500,000 medical records stolen from laboratories in Brittany and Normandy were put up for sale, exposing sensitive patient data [37]. Hospitals in France also suffered direct attacks on their IT systems, causing operational disruptions. For instance, a hospital near Paris had to suspend emergency admissions due to a cyberattack targeting its infrastructure. Similarly, Villefranche-sur-Saône Hospital Hospital experienced a cyberattack [38] that forced the redirection of emergency patients to other facilities until operations could be restored. In 2022, hospitals in France reported 730 cyber incidents [39], highlighting the scale and frequency of such attacks. The most notable was the Corbeil-Essonne Hospital attack by the Lockbit 3.0 hacker group [40,41], which resulted in a massive data breach of over 11 gigabytes of sensitive information, later distributed on the dark web. This breach

included personal and medical data, demonstrating the high stakes of cyberattacks in healthcare.

Healthcare systems across Europe remain highly vulnerable to cyber threats, with hospitals often targeted by ransomware due to their critical operations and urgent need to restore services. Despite existing countermeasures, threats to medical infrastructure persist, as demonstrated by cases in the UK, Germany, Ireland, and France. These incidents underscore the urgent need for robust cybersecurity strategies to protect healthcare systems and safeguard lives. Strengthening security frameworks, fostering international cooperation, and implementing proactive measures are essential to mitigate these risks effectively. European healthcare systems remain vulnerable to cyber threats, with hospitals frequently targeted by ransomware due to their critical operations. Incidents in the UK, Germany, Ireland, and France underscore the urgent need for robust cybersecurity strategies to protect systems and save lives. Strengthening security frameworks, international cooperation, and proactive measures is essential to mitigate these risks.

In Ukraine, the full-scale war has sharply escalated cyberattacks on critical infrastructure, including healthcare. The eHealth system remains inadequately protected, with cybercriminals attempting to destabilize its operations and exploit personal medical data. However, the war and the forced displacement of millions of people have become a catalyst for the development of innovative cybersecurity solutions for the healthcare industry.

In response to the new threats, Ukraine has launched a number of measures aimed at improving cybersecurity in the healthcare sector, including eHealth. The Ministry of Health of Ukraine (MOH) issued an Order dated 15 June 2022 “On the Establishment of the Working Group on the Development and Implementation of the Concept of Strategic Directions for the Development of Cybersecurity in the Field of Electronic Healthcare” [42]. This body was established to develop strategic solutions to improve cybersecurity in the healthcare sector. Thus, the development of strategic decisions by this body will allow not only to respond to current challenges, but also to proactively prevent future cyber incidents, which is critical in today's realities. In addition, the Ministry of Health has developed a plan to restore medical infrastructure after the war [43]. This plan envisages not only the restoration of destroyed medical facilities, but also the improvement of accessibility and quality of medical services for Ukrainian citizens.

Describing the practice tools for combating cyberthreats, firewalls are considered to be one of the main means of protection against cyberattacks [44], providing protection against unauthorised access to internal networks. However, their effectiveness can be low if they are not properly configured and updated. In Ukraine, these systems are mainly used in the commercial sector, while medical institutions often ignore them due to lack of funding. It is important to note that the problem of funding needs to be addressed at the state level. Supporting medical institutions in implementing and maintaining cybersecurity systems is an investment in protecting the nation's health.

Intrusion detection and prevention systems (IDS/IPS) [45] are critical for real-time anomaly detection and are widely used in European state healthcare platforms, ensuring centralized threat management. Countries like the UK and Estonia have successfully integrated these mechanisms, but Ukraine lacks a centralized IDS/IPS for its state healthcare platforms. This gap poses significant risks, especially during wartime, as cyberattacks could disrupt medical care and endanger lives. Addressing this requires amending Ukraine’s eHealth cybersecurity strategy to include IDS/IPS implementation, allocating funding, engaging experts, and strengthening data protection through virtual private networks (VPNs). These measures are vital for safeguarding healthcare and citizen safety [46]. These networks encrypt data, which is especially important for medical institutions where confidential patient data is transmitted. However, European experience shows that weak passwords and lack of updates can lead to security breaches. In Ukraine, VPN implementation requires strict authentication requirements and regular checks. Data encryption [47] is one of the most effective ways to protect confidential information. However, it requires careful management of cryptographic keys, and their loss can lead to irreversible data loss. Encryption is only partially used in Ukrainian medical institutions, which increases the risk of information leaks. Therefore, state regulations should be developed to require mandatory encryption of medical records.

However, technical protections are not sufficient. The human factor is one of the biggest vulnerabilities. Insufficient training of medical staff is often the cause of successful cyberattacks. In Europe, there are mandatory training programs for healthcare professionals that raise their awareness of cyber threats. In Ukraine, such programs are just beginning to be developed, which creates significant cybersecurity risks. In addition, the legal regulation of cybersecurity in healthcare facilities is important. The Law of Ukraine “On Personal Data Protection” [48] establishes general provisions on confidentiality, but does not take into account the specifics of medical information. The

Law "On the Basic Principles of Cybersecurity in Ukraine" [49] such as The Law of Ukraine "On Protection of Personal Data: [50] The Law of Ukraine "On State Secrets" [51], The Law of Ukraine "On Information" [52] also don`t detail the cyber protection of medical institutions, which is a significant gap in the legislative control mechanism. In the EU, there are NIS2 and GDPR directives that create clear rules for data protection, including a significant focus on eHealth. This year, the European Union Agency for Cybersecurity (ENISA) is organising the 9th eHealth Cybersecurity Conference [53], which confirms the urgency of this issue. Currently, Ukraine has serious problems with responding to cyberattacks, usually detected only after the damage has already been done. This underscores the need to introduce automated monitoring systems to detect threats at an early stage. International organizations like USAID play a key role in enhancing Ukraine's healthcare cybersecurity. From March 2023 to September 2024, USAID [54, 55] collaborates with the government to improve healthcare quality, equip professionals, and expand digital expertise. To address cybersecurity risks, Ukraine must adopt European practices, strengthen legal frameworks, and ensure comprehensive staff training, building a secure and resilient eHealth system.

CONCLUSIONS

Healthcare cybersecurity is one of the most important aspects of ensuring national cybersecurity. Understanding the significance of these threats and implementing robust protection measures, as well as fostering awareness of cyber threats, healthcare organizations can safeguard patient data and ensure the continuity of quality care. We believe that a step-by-step mechanism for enhancing cybersecurity in electronic healthcare should be developed, including the following steps:

1. Explanation of the essence of the concept of "cybersecurity of eHealth" and its components. We consider the following working definition acceptable: "Cybersecurity of eHealth is ensuring the organization of timely, accessible, and quality medical services while using cyberspace, which is guaranteed by fulfilling specific requirements such as safeguarding life-critical information and patient data (medical histories, test results, diagnoses, and treatment plans), proper functioning of medical systems and equipment, maintaining security and continuity of operations in emergency situations, and adherence to rules that include necessary protection methods against external and internal cyber threats".
2. Development of a law that explain the features of cybersecurity of eHealth, rules and methods for ensuring, maintaining and improving the work of protection systems. These proposals can also be included in one of the laws regulating the security of the state, as well as especially be highlighted in certain provisions of the laws of Ukraine "On Cybersecurity" and "Fundamentals of Ukrainian legislation on Healthcare".
3. Enhancing cybersecurity in medical institutions requires regular firewall updates and the implementation of intrusion detection and prevention systems (IDS/IPS) at the state medical platform level to improve centralized control. Ensuring mandatory encryption of medical data and stricter VPN authentication protocols is critical to safeguarding confidential information. Additionally, the state cybersecurity strategy should be updated to include these measures, while automated monitoring systems must be introduced to detect threats early. The involvement of leading cybersecurity specialists is essential to create a robust, comprehensive framework for protecting eHealth systems against evolving threats.
4. Utilization of cutting-edge global expertise: All personnel involved in the healthcare system must undergo training for confident and uninterrupted operation in the event of potential or actual threats. They should familiarize themselves with examples of attacks and global response methodologies.

Contributors:

Parfonova I. – writing – original draft, methodology, supervision;

Zinchenko O. – writing an original draft, conceptualization, investigation;

Funding. This research received no external funding.

Conflict of interests. The authors declare no conflict of interest.

REFERENCES

1. Muzyka-Stefanchuk OA, Otradnova OO, Danchenko TV, Muzyka LA, Savenkova VH. Public administrative services in health care. Zaporozhye Medical Journal. 2020;22(2):261-6.
doi: https://doi.org/10.14739/2310-1210.2020.2.200634

2. Venediktova A. Public services in the medical sphere. Medical Law [Internet]. 2009 [cited 2024 Oct 03];3:7-14. Available from: http://medicallaw.org.ua/fileadmin/user_upload/pdf/3_-_1_-_Venediktova.PDF

3. Shevchuk I. Aspects of legalregulation of the provision of medical services. Amazonia Investiga. 2020;9(27):357-66.
doi: https://doi.org/10.34069/AI/2020.27.03.39

4. Velikanov A. [The content of public electronic services in the field of health care]. Entrepreneurship,

Economy and Law. 2020 Dec;12:137-42. Ukrainian. doi: https://doi.org/10.32849/2663-5313/2020.12.23

5. [Fundamentals of the Legislation of Ukraine on Healthcare. Law of Ukraine N 2801-XII 1992 Nov 19]. [Internet]. 1992 [cited 2024 Oct 03]. Ukrainian. Available from: https://zakon.rada.gov.ua/laws/show/2801-12#Text

6. [What is electronic health care?]. Department of health protection of Ternopil region administration [Internet]. [cited 2024 Jan 18]. Ukrainian. Available from: https://uozter.gov.ua/ua/681-reestr-zakladiv-oblasti-e-servisi

7. EU4Health Program 2021-2027 – a Vision for a Healthier European Union. n.d. Public Health [Internet]. 2021 [cited 2024 Jan 26]. Available from: https://health.ec.europa.eu/funding/eu4health-programme-2021-2027-vision-healthier-european-union_en

8. The Seventy-second session of the European Regional Committee: Tel Aviv, 12-14 September 2022: Regional action plan in the field of digital health for the WHO European Region 2023-2030. Globethics [Internet]. 2022 Jul 28 [cited 2024 Jan 18]. Available from: https://repository.globethics.net/handle/20.500.12424/4184161?locale-attribute=en

9. Global strategy on digital health 2020-2025. Geneva: World Health Organization; 2021.

10. Ustinov N. [Electronic health care system open for registration of doctors and patients]. Ukrainian medical journal Chasopys [Internet]. 2017 Sep 21 [cited 2024 Jan 24]. Ukrainian. Available from: https://www.umj.com.ua/article/114387/elektronna-sistema-ohoroni-zdorov-ya-vidkrita-dlya-reyestratsiyi-likariv-i-patsiyentiv

11. [The first medical institutions joined the pilot of the eHealth system. 2017. Ministry of Health of Ukraine]. [Internet]. 2017 Jun 20 [cited 2024 Jan 24]. Ukrainian. Available from: https://web.archive.org/web/20210910003045/https://moz.gov.ua/article/news/pershi-medichni-zakladi-doluchilisja-do-pilotu-systems-ehealth

12. [The project office handed over the eHealth system to the Ministry of Health. 2018. Ministry of Health of Ukraine]. [Internet]. 2018 Jun 6 [cited 2024 Jan 24]. Ukrainian. Available from: https://web.archive.org/web/20180305062948/https://www.ehealth-ukraine.org/news/proektnij-ofis-peredav-moz-sistemu-ehealth-58

13. Electronic health: what does the eHealth system in Ukraine consist of. Ukrainian Medical Journal [Internet]. 2018 Oct 18 [cited 2024 Jan 26]. Available from: https://umj.com.ua/uk/novyna-131430-elektonne-zdorov-ya-z-chogo-skladayetsya-sistema-ehealth-v-ukrayini

14. [Hospitals can now register in the electronic health care system]. ukrinform.ua [Internet]. 2020 Aug 8 [cited 2024 Jan 24]. Ukrainian. Available from: https://web.archive.org/web/20200808032636/https://www.ukrinform.ua/rubric-society/2810529-likarni-vze-mozut-reestruvatisa-v-elektronnij-sistemi-ohoroni-zdorova.html

15. Goncharova K. Deputy suprun told how the eHealth system is protected from cyber attacks. Media Sapiens [Internet]. 2019 July 31 [cited 2024 Jan 24]. Available from: https://web.archive.org/web/20190731114238/https://ms.detector.media/web/cybersecurity/zastupnik_suprun_rozpoviv_yak_sistemu_ehealth_zakhischayut_vid_kiberatak/

16. [Digital Med 2020: challenges and development of eHealth in Ukraine]. Pharmacy Online [Internet]. 2020 Oct 19 [cited 2024 Jan 24]. Ukrainian. Available from: https://www.apteka.ua/article/568312

17. [The Cabinet of Ministers approved the Concept of the development of the electronic health care system]. ukrinform.ua [Internet]. 2020 Dec 28 [cited 2024 Jan 24]. Ukrainian. Available from: https://www.ukrinform.ua/rubric-society/3162532-kab-min-zatverdiv-koncepciu-rozvitku-elektronnoi-sistemi-ohoroni-zdorova.html

18. [On the approval of the concept of the development of electronic health care. Order Cabinet of Ministers of Ukraine from 2020 Dec 28, No. 1671]. [Internet]. 2020 [cited 2024 Jan 24]. Ukrainian. Available from: https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80#Text

19. Ustinov OV. [Digitalization of health care: results of the year and plans for the future]. Ukrainian Medical Journal [Internet]. 2023 Dec 21 [cited 2024 Jan 26]. Ukrainian. Available from: https://www.umj.com.ua/uk/novyna-249615-tsifrovizatsiya-ohoroni-zdorov-ya-pidsumki-roku-ta-plani-na-future

20. Kütt A. Estonia and Sweden to join forces to drive innovation in Healthcare. Invest in Estonia [Internet]. 2023 [cited 2024 Jan 26]. Available from: https://investinestonia.com/estonia-and-sweden-to-join-forces-to-drive-innovation-in-healthcare

21. Whitehouse D, Giest S, Dumortier J, Artmann J. Country Brief: Wales. [Internet]. eHealth Strategies: European Commission; 2010 [cited 2024 Jan 26]. Available from: https://ehealth-strategies.eu/database/documents/-Wales_CountryBrief_eHStrategies.pdf

22. NSW government. eHealthstrategy for NSW Health 2016-2026: A digitally enabled and integrated health system delivering patient-centred health experiences and quality health outcomes. NSW Government; 2016.

23. The Scottish Government. Health and social care: Data strategy [Internet]. 2023 Feb 23 [cited 2024 Jan 26]. Available from: https://www.gov.scot/publications/data-strategy-health-social-care-2

24. [Health and Social Care Northern Ireland 2022-2030, Digital Strategy]. [Internet]. 2022 Jul 11 [cited 2024 Nov 1]. Nothern Ireland. Available from: https://www.health-ni.gov.uk/sites/default/files/publications/health/doh-hscni-digital-strategy-final.pdf

25. Department of Health. Cyber Security Strategy. HSC Northern Ireland 2022-2026. E-book. [Internet]. 2022 [cited 2024 Nov 1]. Available from: https://niopa.qub.ac.uk/bitstream/NIOPA/15413/1/doh-cyber-strategy-2022_0.pdf

26. Second act to increase the security of information technology systems (IT Security Act 2.0) [Internet]. Bonn: Bundesamtes für Sicherheit in der Informationstechnik; 2021 [cited 2024 Jan 26]. German. Available from:

https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html#:~:text=Der%20Bundesrat%20hat%20das%20GesetzApril%2020 2021%20verabschiedet

27. Kiteworks. What is GDPR? Protection of data and personal rights. Kiteworksyour private content network [Internet]. 2023 Feb 8 [cited 2024 Jan 26]. Available from: https://www.kiteworks.com/de/risiko-compliance-glossar/dsgvo/#:~:text=Die%20General%20Data%20Protection%20Regulation%20(GDPR)%20ist%20ein%20umfassendes%20Datenschutz,ihre%20pers%C3%B6nlichen%20Daten%20zu%20geben

28. [EHealth Expertise in France – Expertise. French Healthcare]. French Healthcare [Internet]. 2023 Sep 15 [cited 2024 Jan 26]. French. Available from: https://frenchhealthcare.fr/expertises/eHealth/

29. [Cross-border electronic health services]. Public Health [Internet]. 2024 Jan 9 [cited 2024 Jan 18]. French. Available from:https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_fr

30. Atella V. Challenges and Opportunities for the French Health System. E-book. 31st ed. [Internet]. Fondazione Farmafactoring; 2020 [cited 2024 Jan 18]. Available from: https://www.bff.com/documents/2155734/-2177835/FarmafactoringFoundation-ResearchPapers-03_2020-FR.pdf/bb0b1d74-5e0b-9806-561b-74cfa2809a31

31. Collier R. NHS ransomware attack spreads worldwide. CMAJ. 2017 Jun 5;189(22):786-7. doi: https://doi.org/10.1503/cmaj.1095434

32. Palmer D. Ransomware: How the NHS learned the lessons of wannacry to protect hospitals from attack. ZDNET [Internet]. 2021 May 13 [cited 2024 Jan 26]. Available from: https://www.zdnet.com/article/ransomware-how-the-nhs-learned-the-lessons-of-wannacry-to-protect-hospitals-from-attack/

33. Smart W. Lessons learned review of the wannacryransomware cyber attack [Internet]. London: gov.uk; 2018 [cited 2024 Jan 26]. Available from: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

34. Eddy M, Perlroth N. Cyberattack suspected in German woman's death. The New York Times [Internet]. 2020 [cited 2024 Jan 26]. Available from: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

35. Nath B. Woman died after a ransomware attack Encrypted hospital services. Techdator (blog) [Internet]. 2022 Dec 26 [cited 2024 Jan 26]. Available from: https://techdatoral.pages.dev/posts/woman-died-after-a-ransomware-attack-encrypted-hospital-services

36. Arishti Info Labs. Ransomware Attack on Irish Healthcare System – Arishti Info Labs. Medium [Internet]. 2022 March 5 [cited 2024 Feb 6]. Available from: https://arishti.medium.com/ransomware-attack-on-irish-healthcare-system-82b973b7abb4

37. Kerkour T. [Cyberattacks against healthcare establishments doubled in 2021]. Le Figaro [Internet]. 2022 Feb 15 [cited 2024 Feb 5]. French. Available from: https://www.lefigaro.fr/secteur/high-tech/les-cyberattaques-contre-les-etablissements-de-sante-ont-double-en-2021-20220215

38. Afp, Le Parisien Avec. [Cyberattack at Dax hospital: very gradual recovery, no ransom paid]. leparisien.fr. [Internet]. 2021 Feb 12 [cited 2024 Feb 5]. French. Available from: https://www.leparisien.fr/faits-divers/cyberattaque-a-lhopital-de-dax-reprise-tres-progressive-aucune-rancon-payee-11-02-2021-KICTQBN3D5GNNJS6GRFAVZMCKU.php

39. Versailles hospital victim of cyberattack. Les Echos [Internet]. 2022 Dec 5 [cited 2024 Feb 5]. Available from: https://www.lesechos.fr/pme-regions/ile-de-france/lhopital-de-versailles-victime-dune-cyberattaque-1885808#:~:text=L'%C3%A9tablissement%20hospitalier%20de%20%20Versailles%2C%20dans%20les%20Yvelines%2C%20est,le%20coup%20de%20cette%20cyberattaque

40. leparisien.fr [Internet]. [Victim of a computer attack, the Villefranche-sur-Saône hospital is forced to cancel operations]. Paris: Le Parisien; 2021 Feb 16 [cited 2024 Feb 6]. French. Available from: https://www.leparisien.fr/faits-divers/

41. portail-ie.fr [Internet]. [Portail De L'IE: A look back at major cyberattacks in France in 2022: what resolutions for 2023 April 17]. 2023 [cited 2024 Feb 5]. French. Available from: https://www.portail-ie.fr/univers/

42. [On the establishment of a Working Group on the development and implementation of the Concept of strategic directions for the development of cybersecurity in the field of electronic healthcare. Order 2022 Jun 15 No. 1034]. [Internet]. 2022 Jun 15 [cited 2024 May 11]. Ukrainian. Available from: https://zakon.rada.gov.ua/rada/show/v1034282-22#Text

43. [Ministry of Health of Ukraine. Plan for the restoration of the health care system of Ukraine from the consequences of the war for 2022-2032]. Dataset. Government portal [Internet]. 2022 [cited 2024 May 11]. Ukrainian. Available from: https://moz.gov.ua/uploads/ckeditor/News/21-07-2022-Draft-Ukraine%20HC%20System%20Recovery%20Plan-2022-2032_UKR.pdf

44. Serafini G. Cips Legal. Firewall e Sistemi IAM. SGSI e conformità NIS2. [Internet]. Cips Legal; 2024 Oct 18 [cited 2024 Oct 5]. Available from: https://www.cipslegal.it/nis2/atti-documenti-nis2/firewall-e-sistemi-iam-sgsi-e-conformita-nis2/

45. Cybersecurity Exchange. IDS vs. [Internet]. IPS: Key Difference and Similarities Best for Cybersecurity; 2023 Dec 15 [cited 2024 Nov 22]. Available from: https://www.eccouncil.org/cybersecurity-exchange/network-security/ids-and-ips-differences/

46. Compliancy Group. VPN in Healthcare. Healthcare Data Protection [Internet]. Compliancy Group; 2023 [cited 2024 Nov 22]. Available from: https://compliancy-group.com/using-vpn-for-healthcare-data-protection/

47. Efficient medical information retrieval in encrypted Electronic Health Records [Internet]. PubMed. 2012 [cited 2024 Nov 22]. Available from: https://pubmed.ncbi.nlm.nih.gov/22874185/

48. [On information protection in information and communication systems. The law of Ukraine 1994 No. 80/94-VR]. [Internet]. 1994 [cited 2024 Feb 6]. Ukrainian. Available from: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

49. [On the Basic Principles of Cybersecurity in Ukraine. The law of Ukraine 2017 No. 2163-VIII]. [Internet]. 2017 [cited 2024 May 30]. Ukrainian. Available from: https://zakon.rada.gov.ua/laws/show/2163-19?lang=en#Text

50. [On the protection of personal data. The law of Ukraine 2010 No. 2297-VI]. [Internet]. 2010 [cited 2024 Feb 6]. Ukrainian. Available from: https://zakon.rada.gov.ua/laws/show/2297-17#Text

51. [About state secrets. The law of Ukraine 2024 No. 3855-XII]. [Internet]. 2024 [cited 2024 Feb 6]. Ukrainian. Available from: https://zakon.rada.gov.ua/laws/show/3855-12#Text

52. [On information 2657-XII. Official web portal of the Parliament of Ukraine. Verkhovna Rada of Ukraine]. [Internet]. 1992 [cited 2024 Feb 6]. Ukrainian. Available from: https://zakon.rada.gov.ua/laws/show/2657-12#Text

53. Prioritising eHealth cybersecurity against emerging challenges. ENISA [Internet]. 2024 [cited 2024 Nov 10]. Available from: https://www.enisa.europa.eu/news/prioritising-ehealth-cybersecurity-against-emerging-challenges

54. Country development cooperation strategy 2019-2024: USAID country development cooperation strategy for Ukraine (2019-2024). Agency for International Development. USAID [Internet]. 2024 [cited 2024 Feb 6]. Available from: https://www.usaid.gov/sites/default/files/2022-05/Ukraine_USAID_CDCS_2019-2024_Public_EN_12.pdf

55. [USAID project “Health care reform support”]. Brovary City Council [Internet]. 2023 Dec 27 [cited 2024 Feb 6]. Ukrainian. Available from: https://brovary-rada.gov.ua/news/proiekt-usaid-pidtrymka-reformy-okhorony-zdorovia

Стаття надійшла до редакції 22.10.2024;
затверджена до публікації 09.12.2024