UDC 004.056
DOI https://doi.org/10.32689/maup.it.2025.2.31

Maksym CHEREMNOV
Postgraduate Student at the Department of Computer Engineering and Innovative Technologies,
International Humanitarian University,
cheremnovmaksym@gmail.com
***ORCID:** 0009-0006-4936-4747*

TRANSFORMATION OF INTERNATIONAL CYBERSECURITY STANDARDS AS A RESPONSE TO TECHNOLOGICAL AND GEOPOLITICAL CHALLENGES

Abstract. *The article is aimed at analyzing the transformation of international cybersecurity standards (ISO/IEC 27001, NIST Cybersecurity Framework, GDPR) as a response to technological (AI, IoT, 5G) and geopolitical challenges (state-sponsored cyberattacks, regulatory fragmentation).*

The study aims *to identify key areas of evolution of standards, assess their adaptation to current threats, and suggest ways to improve global cyber resilience through cross-sectoral cooperation.*

The study is based on the analysis of verified data from reputable sources, including IBM Security Cost of a Data Breach 2024, ENISA 2023, Verizon DBIR 2024, Microsoft Threat Intelligence Report 2023, as well as official documents of international organizations (EU, NIST, ISO). A systematic approach was used to assess technological, geopolitical and regulatory factors affecting cybersecurity standards. A comparative analysis of standards (ISO/IEC 27001:2022, NIST CSF 2.0, GDPR, NIS2) allowed us to identify their updates and limitations. Additionally, cross-sectoral cooperation initiatives such as the Cybersecurity Tech Accord and the ENISA MeliCERTes platform were analyzed to assess their role in the implementation of standards.

The article offers a comprehensive analysis of the transformation of cybersecurity standards with a focus on their adaptation to new technological threats (AI, IoT) and geopolitical realities (state-sponsored attacks). The novelty lies in the consideration of cross-sectoral cooperation as a key mechanism for implementing standards, which has not been sufficiently covered in the literature. The study also systematizes standard updates (e.g., the "Govern" feature in NIST CSF 2.0, the integration of DevSecOps in ISO/IEC 27001:2022) and assesses their impact on global harmonization, highlighting the barriers associated with regulatory fragmentation.

The transformation of international cybersecurity standards is necessary to counter modern threats. Updates to ISO/IEC 27001:2022 and NIST CSF 2.0 address risks from AI, IoT, and supply chains, while GDPR and NIS2 strengthen data protection and incident response. However, political differences, such as between Western and Chinese standards (GB/T), complicate global harmonization. The human factor, which accounts for 68% of data breaches, calls for increased cyber literacy. Cross-sectoral cooperation, such as the ENISA and CISA initiatives, is critical to the practical implementation of standards. In the future, cyber resilience will depend on flexible standards, coordination between states, the private sector and international organizations, and investment in education and technology.

Key words: *cybersecurity, international standards, AI, IoT, geopolitical challenges, ISO/IEC 27001, NIST.*

Максим ЧЕРЕМНОВ. ТРАНСФОРМАЦІЯ МІЖНАРОДНИХ СТАНДАРТІВ КІБЕРБЕЗПЕКИ ЯК ВІДПОВІДЬ НА ТЕХНОЛОГІЧНІ ТА ГЕОПОЛІТИЧНІ ВИКЛИКИ

Анотація. *Стаття спрямована на аналіз можливості та доцільності змін в міжнародних стандартах кібербезпеки (ISO/IEC 27001, NIST Cybersecurity Framework, GDPR) з огляду на технологічні (ШІ, IoT, 5G) та геополітичні чинники.*

Мета роботи. *полягає у визначенні ключових напрямів еволюції стандартів, оцінки рівня їхньої адаптації до сучасних загроз і формування пропозицій щодо підвищення глобальної кіберстійкості через міжсекторальну співпрацю.*

Методологія. *В дослідженні використано системний підхід до оцінки технологічних, геополітичних і регуляторних факторів, що впливають на стандарти кібербезпеки. Проведено порівняльний аналіз стандартів ISO/IEC 27001:2022, NIST CSF 2.0, GDPR, NIS2, який дозволив виявити їхні обмеження в контексті змін зовнішнього середовища.*

Наукова новизна *полягає, насамперед, у фокусуванні дослідження на міжсекторальній співпраці як ключового механізму реалізації стандартів, що раніше висвітлювалося недостатньо. В цьому контексті проаналізовано ініціативи міжсекторальної співпраці, такі як Cybersecurity Tech Accord і ENISA MeliCERTes, для оцінки їхньої ролі в можливій трансформації наявних стандартів. Визначено, що останні оновлення ISO/IEC 27001:2022 і NIST CSF 2.0 враховують ризики від ШІ, IoT і ланцюгів постачання, тоді як GDPR і NIS2 посилюють захист даних і реагування на інциденти. Проте політичні розбіжності, зокрема між західними та китайськими стандартами (GB/T), ускладнюють глобальну гармонізацію. Паралельно із цим визначено, що людський фактор, що спричиняє 68% витоків даних, вимагає посилення кіберграмотності.*

Висновки. *За підсумками дослідження зроблено висновок, що у майбутньому глобальна кіберстійкість залежатиме від гнучкості стандартів та ефективної координації між державами, приватним сектором і міжнародними організаціями за умови належних інвестицій у освіту й технології.*

Ключові слова: *кібербезпека, міжнародні стандарти, ШІ, IoT, геополітичні виклики, ISO/IEC 27001, NIST.*

Problem statement. In the modern world, cyberspace has become an environment for economic, social and political activities. At the same time, the rapid development of technologies, including artificial intelligence, the Internet of Things and 5G, as well as the growth of cyberattacks (primarily strategic ones, as an element of military and geopolitical confrontations), create new challenges for cybersecurity. Therefore, existing international standards, such as ISO/IEC 27001, NIST Cybersecurity Framework, and GDPR, need to be transformed to effectively respond to these challenges. The key problems are insufficient adaptation of standards to technological innovations, regulatory fragmentation, and geopolitical barriers that complicate global harmonization and reduce cyber resilience.

Analysis of recent research and publications. A number of scientific works are devoted to research on standardization in the context of ensuring effective cyber defense. Thus, S. Arsila, N. Pritam, S. Kepple [1] in their report on the investigation of data leaks drew attention to the need to revise approaches to risk assessment. The model for assessing risk management processes proposed by B. Barafor, A. L. Mesquida, A. Mas [2] is based on the ISO 31000 standard and integrates it into the context of multiple standards, which promotes an integrated approach to cybersecurity. At the same time, M. Edwards [7] emphasized the importance of updating the ISO 27001:2022 standard, in particular Annex A 5.23, which regulates the security of cloud services. Tanvir [20] notes that reliable communication frameworks for IoT play a critical role in ensuring data security in networks with a large number of connected devices. In addition, the GB/T 22239-2019 standard [9] establishes basic requirements for classified cybersecurity protection, which is relevant, in particular, for Asian countries.

Regarding the coverage of geopolitical factors, A. Venkat [21] emphasized that geopolitical conflicts are increasingly becoming a catalyst for cyberattacks, which prompts the creation of international initiatives such as the Cooperative Cyber Defense Cooperation [12]. K. Siglik and J. Gehring [5] propose a multilateral approach to ensuring peace in cyberspace, emphasizing the need for cooperation between states, the private sector, and international organizations. In this context, the NIS 2 Directive [15] and Regulation (EU) 2019/881 [17] set higher standards for the protection of critical infrastructure and cybersecurity certification in the EU. Increased cyber threats, including ransomware, also affect standards. S. Morgan [14] predicts that global losses from ransomware will reach $57 billion in 2025, which emphasizes the need to strengthen incident response standards such as ISO/IEC 27035-1:2023 [11]. A. Ribeiro [19] in the ENISA 2024 report points to the growth of attacks on availability and data, which requires the adaptation of standards to new challenges. IBM's 2024 report [6] confirms that data breaches remain one of the most costly problems for organizations, prompting the implementation of standards such as ISO 27001:2022 [10].

At the legislative level, cybersecurity standards are also evolving. L. Y. Chang [4] analyzes the Budapest Convention as a basis for combating cybercrime, which is especially relevant for Asian countries. In turn, the California Personal Data Protection Act of 2018 [3] establishes new requirements for data processing, affecting global standards. I. Relekar [18] notes that the updated NIST Cybersecurity Framework 2.0 helps organizations adapt to new threats through a flexible approach to risk management.

D. Parsons [16] emphasizes the growth of attacks on industrial control systems, which requires strengthening the standards for protecting critical infrastructure. Microsoft's 2023 report [13] emphasizes the need to integrate artificial intelligence into cybersecurity standards to counter sophisticated attacks.

A. Folorunso, W. Mohammed, I. Wada, B. Samuel [8] prove that the implementation of ISO standards significantly increases the level of cybersecurity of organizations, providing a structured approach to information security.

The purpose of the article is to analyze the transformation of international cybersecurity standards (ISO/IEC 27001, NIST Cybersecurity Framework, GDPR) in response to technological (AI, IoT, 5G) and geopolitical (state-sponsored cyberattacks, regulatory fragmentation) challenges, as well as to identify key areas for their adaptation, assess the role of cross-sectoral cooperation, and develop recommendations for improving global cyber resilience.

Summary of the main material. Cyberspace is a key element of the modern world, where technological innovations and geopolitical tensions pose complex security challenges. The growth of cyberattacks, the proliferation of artificial intelligence (AI), the Internet of Things (IoT), 5G networks, and state-sponsored cyber operations require the adaptation of international cybersecurity standards. This transformation is aimed at responding to new threats, harmonizing regulatory requirements, and taking into account political realities.

Technological advances are radically changing the nature of cyber threats. The IBM Security Cost of a Data Breach 2024 report reports that the average global cost of a data breach reached USD 4.88 million, which is 10% more than in 2023. Phishing (16% of cases) and the use of stolen credentials (15%) remain the main causes of leaks. Artificial intelligence is opening up new opportunities for attacks, such as automated phishing campaigns and deepfakes, which make them more difficult to detect [6]. Statista predicts that by the end of 2025, the number of IoT devices will reach 75.44 billion, which creates additional vulnerabilities due to weak security and protocol heterogeneity [20]. In response, ISO/IEC 27001:2022 has been updated to include requirements for risk management in cloud, AI, and IoT. The standard emphasizes the integration of cybersecurity into software

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

development processes through DevSecOps and continuous risk monitoring to adapt to rapidly changing technologies [10; 7].

The fact that modern cyber threats are caused mainly by geopolitical challenges is confirmed by the fact that most cyber attacks on critical infrastructure in the EU showed signs of state support, in particular from Russia, China and North Korea [21]. The Microsoft Threat Intelligence Report 2023 indicates that Russia is responsible for 58% of state-sponsored attacks in the world. This prompts the development of standards that take into account political aspects [13]. The EU Cybersecurity Act of 2019 established a framework for the certification of products and services, promoting the unification of requirements in the EU [17]. However, global harmonization is complicated by differences between the approaches of the United States (NIST), China (GB/T standards) and other countries. For example, Chinese standards GB/T 22239 provide for data localization, which contradicts Western principles [9].

Regulatory changes are an important driver of transformation (Tab. 1). For example, the GDPR, introduced in 2018, set a global standard for data protection, influencing legislation, including the California Consumer Protection Act (CCPA) [10]. In 2023, the European Commission proposed the NIS2 Directive, which covers the energy, transport, healthcare, and digital services sectors, strengthening the requirements for incident response. ENISA estimates that NIS2 will affect 160 thousand organizations in the EU, which is twice as many as the previous NIS Directive [15]. The NIST Cybersecurity Framework 2.0, published in February 2024, introduces the "Govern" function for strategic cybersecurity management and recommendations for protecting supply chains and countering AI attacks [18].

Table 1

Key cybersecurity standards and frameworks

Standard	Organization	Year of update	Main changes
ISO/IEC 27001	ISO/IEC	2022	Integration of DevSecOps, AI risk management, cloud technologies, and IoT
NIST CSF 2.0	NIST	2024	Implementation of the "Govern" function, supply chain protection, countering AI attacks
GDPR	EU	2018	Establishment of global data protection standards, fines up to 4% of annual turnover
EU Cybersecurity Act	EU	2019	Certification of cybersecurity products, services, and processes
NIS2	EU	2023 (offer)	Expansion into new sectors, strengthening incident response requirements

Джерело: складено за даними [10; 17; 18]

It is the flexibility of standards that can be considered a key component for an effective response to challenges. NIST CSF 2.0 uses a modular approach, allowing organizations to adapt the framework to their needs [18]. ISO/IEC 27001:2022 supports integration with other standards, such as ISO 31000 (risk management), which facilitates implementation in different jurisdictions [2].

The main priority is to prepare for cyber incidents. For example, Cybersecurity Ventures noted that in 2021, ransomware attacks occurred every 11 seconds, causing $20 billion in losses, which in turn will lead to attacks every second in 2031 [14]. ISO/IEC 27035:2023 provides guidance on coordination between organizations and government agencies during incidents [11]. The MITRE ATT&CK framework, which includes more than 200 attack techniques, is used to model threats. According to the SANS Institute, in 2023, 45% of organizations in the United States used MITRE ATT&CK to test systems [16].

It is also important to note that the human factor poses the greatest risks. The Verizon DBIR 2024 report indicates that 68% of data breaches are due to human error, including unintentional disclosure (43%) and weak passwords (25%) [1]. ISO/IEC 27002:2022 includes recommendations for two-factor authentication and staff training.

In general, effective cyber risk management requires a comprehensive approach that combines technological, organizational and human aspects, and takes into account geopolitical factors. To systematize the relationships between these elements and relevant standards, we have developed the diagram shown in (Fig. 1), which illustrates the integration of technological, geopolitical challenges and cybersecurity standards in a single conceptual model.

International cybersecurity standards continue to evolve to meet new realities. Updates to ISO/IEC 27001:2022 and NIST CSF 2.0 demonstrate progress in countering AI attacks, protecting IoT and supply chains [8]. GDPR and NIS2 set high standards for data protection and incident response, influencing global practices. However, regulatory fragmentation and political differences, especially between the West and China, make

harmonization difficult. Investments in cyber literacy and coordination between states and organizations are critical to improving global cyber resilience.

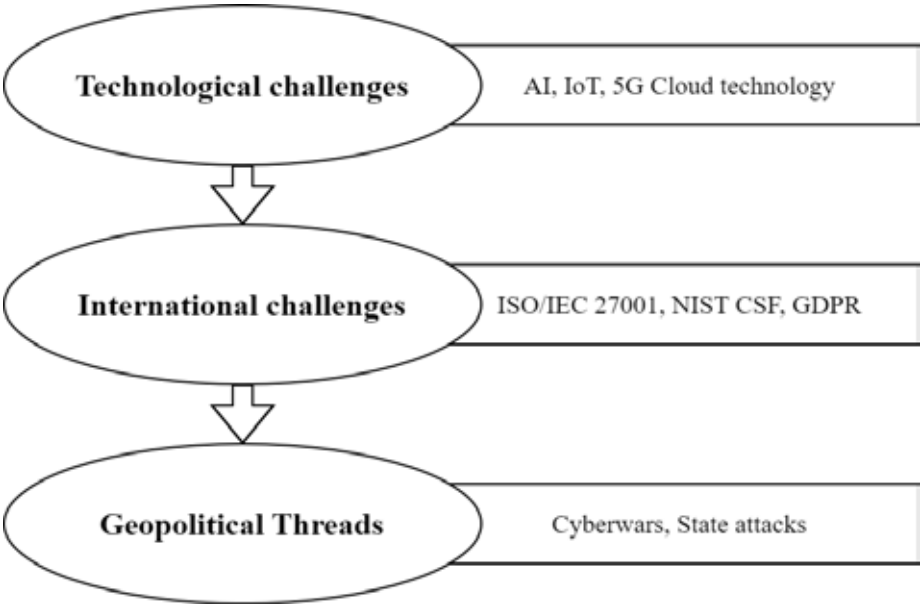

Fig. 1. Transformation of cybersecurity standards

Effective transformation of international cybersecurity standards is impossible without close cooperation between the public and private sectors, as well as international organizations. Most organizations around the world consider cross-sectoral partnerships to be critical to countering cyber threats. For example, the Cybersecurity Tech Accord initiative, signed by more than 150 technology companies, including Microsoft and Cisco, aims to jointly develop secure products and share information about threats [5]. Within the EU, ENISA coordinates with national authorities to facilitate the exchange of incident data through the MeliCERTes platform. In 2023, this platform processed more than 10,000 cyber incident reports, which is 25% more than in 2022, according to ENISA [19].

In addition, international organizations such as the ITU (International Telecommunication Union) and the OECD play a key role in harmonizing standards. For example, in 2023, the ITU published the X.1205 guidelines, which clarify approaches to cybersecurity in the IoT, facilitating their integration with ISO/IEC 27001. The OECD, in turn, updated its digital security guidelines in 2024, emphasizing the need for a global framework for managing risks in supply chains. However, cooperation is complicated by geopolitical barriers. For example, China's refusal to participate in international initiatives such as the Budapest Convention on Cybercrime limits global information sharing on cyber threats. According to Interpol, in 2023, only 40% of member countries regularly exchanged data on cyber incidents, which emphasizes the need for greater coordination [7].

Practical implications of cross-sectoral cooperation include the creation of joint cyber threat response centers. For example, in the United States, CISA (the Cybersecurity and Infrastructure Security Agency) launched the Joint Cyber Defense Collaborative in 2023, which brings together government, the private sector, and international partners to counter ransomware attacks [12]. In Europe, a similar role is played by the European Cyber Crisis Liaison Organization Network (CyCLONe), created under NIS2. These initiatives demonstrate that the transformation of standards must be accompanied by practical mechanisms for their implementation, including joint training, technology sharing, and policy harmonization.

To increase the effectiveness of international cybersecurity standards, a global harmonization framework based on cooperation through platforms such as the International Telecommunication Union should be developed to facilitate the harmonization of requirements across jurisdictions. Strengthening cyber literacy programs by introducing regular trainings for organizational staff is important, as only 30% of companies in the EU, according to ENISA 2023, conduct them systematically. Establishing international cyber threat response centers, following the example of CISA's Joint Cyber Defense Collaborative, will allow for the rapid exchange of information about incidents and coordination between states and the private sector [12]. The integration of artificial intelligence into cybersecurity standards, in particular to automate threat detection and analysis, is necessary to counter sophisticated attacks such as deepfake or automated phishing. Implementation of these measures requires joint efforts of governments, technology companies and international organizations to ensure the resilience of cyberspace in the face of modern challenges.

Conclusion. The transformation of international cybersecurity standards is a necessary response to technological innovation, geopolitical tensions, and growing cyber threats. Updates to ISO/IEC 27001:2022, NIST CSF 2.0, and proposals such as NIS2 are adapting regulatory frameworks to the challenges of AI, IoT, and state-sponsored attacks, while the GDPR remains the global benchmark for data protection. However, regulatory fragmentation and policy differences, particularly between Western and Chinese approaches, complicate harmonization. The human factor that causes most data breaches underscores the importance of cyber literacy.

Cross-sectoral and international cooperation, such as the Cybersecurity Tech Accord and ENISA platforms, is critical to implementing standards and building cyber resilience. Going forward, success will depend on flexible standards, increased coordination between governments, the private sector and international organizations, and investments in technology and education to ensure the resilience of global cyberspace.

Bibliography:

1. Arcila C., Pritam N., Kepple S. Data Breach Investigations Report: Vulnerability exploitation boom threatens cybersecurity. *Verizon*, 2024. URL: https://www.verizon.com/about/news/2024-data-breach-investigations-report-vulnerability-exploitation-boom (Accessed at: 15.05.2025).

2. Barafort B., Mesquida A. L., Mas A. Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context. *Computer Standards & Interfaces*, 2018. № 60. С. 57–66.

3. California Consumer Privacy Act of 2018. *California Legislative Information – Website*. URL: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (Accessed at: 11.05.2025).

4. Chang L. Y. Legislative frameworks against cybercrime: The Budapest convention and Asia. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020. PP. 327–343.

5. Ciglic K., Hering J. A multi-stakeholder foundation for peace in cyberspace. *Journal of Cyber Policy*, 2021. № 6(3). PP. 360–374.

6. Cost of a Data Breach Report 2024. *IBM – Website*. URL: https://www.ibm.com/reports/data-breach (Accessed at: 03.05.2025).

7. Edwards M. ISO 27001:2022 Annex A 5.23 – Information Security for Use of Cloud Services. *ISMS.online*, 2025. URL: https://www.isms.online/iso-27001/annex-a/5-23-information-security-use-of-cloud-services-2022/ (Accessed at: 03.05.2025).

8. Folorunso A., Mohammed V., Wada I., Samuel B. The impact of ISO security standards on enhancing cybersecurity posture in organizations. W*orld Journal of Advanced Research and Reviews*, 2024. № 24(1). PP. 2582–2595.

9. GB/T 22239-2019 Information security technology–Baseline for classified protection of cybersecurity (English Version). *Code of China*, 2019. URL: https://www.codeofchina.com/standard/GBT22239-2019.html (Accessed at: 11.05.2025).

10. ISO 27001:2022 Controls: Annex A list. *Scrut Automationm*, 2025. URL: https://www.scrut.io/iso-27001/iso-27001-controls/ (Accessed at: 03.05.2025).

11. ISO/IEC 27035-1:2023. *ISO – Website*, 2023. URL: https://www.iso.org/ru/standard/78973.html (Accessed at: 15.05.2025).

12. Joint Cyber Defense Collaborative. *CISA – Website*. URL: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative (Accessed at: 19.05.2025).

13. Microsoft Digital Defense Report. Microsoft Threat Intelligence, 2023. 131 p.

14. Morgan S. Global Ransomware Damage Costs Predicted To Hit $57B Annually In 2025*. Elastio*, 2025. URL: https://elastio.com/research-report/2025-ransomware-report (Accessed at: 11.05.2025).

15. NIS 2 strengthens cybersecurity across the EU by setting higher standards for essential services. *ENISA – Website.* URL: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2?utm_source=chatgpt.com#contentList (Accessed at: 11.05.2025).

16. Parsons D. Sans Survey Ics 2023. *SCRIBD*, 2023. 19 p. URL: https://ru.scribd.com/document/678301429/Sans-Survey-Ics-2023 (Accessed at: 15.05.2025).

17. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). 2019. PP. 15–69.

18. Relekar I. NIST Cybersecurity Framework 2.0. *ACA,* 2024. URL: https://www.acaglobal.com/industry-insights/nist-cybersecurity-framework-20/ (Accessed at: 11.05.2025).

19. Ribeiro A. ENISA Threat Landscape 2024 identifies availability, ransomware, data attacks as key cybersecurity threats. *Industrial Cyber*, 2024. URL: https://industrialcyber.co/reports/enisa-threat-landscape-2024-identifies-availability-ransomware-data-attacks-as-key-cybersecurity-threats/ (Accessed at: 15.05.2025).

20. Tanweer A. A Reliable Communication Framework and Its Use in Internet of Things (IoT). *ResearchGate,* 2018. № 3. URL: https://www.researchgate.net/publication/325645304_A_Reliable_Communication_Framework_and_Its_Use_in_Internet_of_Things_IoT (Accessed at: 03.05.2025).

21. Venkat A. Geopolitics plays major role in cyberattacks, says EU cybersecurity agency. *CSO,* 2022. URL: https://www.csoonline.com/article/573999/geopolitics-plays-major-role-in-cyberattacks-says-eu-cybersecurity-agency.html (Accessed at: 03.05.2025).

Дата надходження статті: 02.06.2025
Дата прийняття статті: 30.06.2025
Опубліковано: 23.09.2025