Alina Liubyma, Head of the Department of Entrepreneurship and Information Technologies,
The Kyiv Applying College of Tourism and Hospitality
Kyiv, Ukraine

Andrii Panibratov, Lecturer
The Kyiv Applying College of Tourism and Hospitality
Kyiv, Ukraine

DOI: https://doi.org/10.30525/978-9934-26-633-1-41

REGULATORY ASPECTS OF CYBERSECURITY IN UKRAINE AND THE EU IN THE CONTEXT OF DIGITALIZATION

In today's conditions of globalization, digital transformation, and integration processes, the issue of cybersecurity has acquired particular strategic importance. The rapid development of technologies is accompanied by an increase in the number and complexity of cyber threats that affect the economy, government activities, and national security of the country.

From a public administration perspective, it is necessary to consider the boundlessness of cyberspace and the distributed responsibility of all participants in this process. After all, various levels and sectors are involved in ensuring cybersecurity – international chains of interaction, sectoral infrastructure, private business, IT companies and cybersecurity specialists, and so on.

Under such conditions, it is particularly important to clearly delineate the functions of government agencies, defining their powers in the field of standardization, certification, control, regulation, as well as to ensure effective legal support and a high-quality legislative base [1].

In view of this, the need arose to implement international standards that can compliment or even outright replace current ISO 27001 standart, particularly the EU NIS2 directive. They are designed to ensure uniform rules for information protection in the global cyberspace, coordinating them with national interests, economic conditions, and social challenges of each individual country [2].

The development of the digital economy opens up new opportunities – rapid access to international markets, provision of government electronic services, access to online financing. However, this simultaneously leads to an increase in cyber risks, which, due to the characteristics of cyberspace itself, can quickly turn into real threats. The need to form requirements for an appropriate level of cyber protection emerged simultaneously with the emergence of cyberspace itself. Corresponding regulatory acts and documents were developed by various organizations according to their own approaches, which created diversity in the regulatory system.

From a technical point of view, the foundation of information security remains three principles – confidentiality, integrity, and data availability. However, in modern conditions this is no longer sufficient, as there remains a significant legal and regulatory gap between the level of cyber threats, available technological protection capabilities, and the effectiveness of public administration.

In Ukraine, the market-oriented ISO/IEC 27001 standard is currently in effect – an internationally recognized voluntary ISMS standard adopted by the ISO and IEC organizations. Its implementation occurs on the initiative of the organization itself, with the possibility of independently selecting control measures based on the risk assessment defined in the standard [3].

In contrast, the EU has legislatively introduced a system of cybersecurity requirements, compliance with which is possible only through a combination of the ISO/IEC 27001 standard and the NIS2 directive as a complex [3-5].

NIS2 Directive should not be seen simply as a standart. It isa complex of provisions that primarily concern large and medium-sized enterprises (with more than 50 employees or annual turnover over €10 million). NIS2 directive demands that such organizations must implement comprehensive cyber risk management measures, timely report serious incidents (for example, preliminary notification – within 24 hours, full report – within 72 hours), and ensure personal responsibility of management for the state of cybersecurity [3; 6].

Below are listed the main differences between these two acts, which determine the difference in approaches to cybersecurity in Ukraine and the countries of the European Union [8]:

1) Legal obligation and personal responsibility of management, which involves strict compliance with requirements with specific sanctions for violations. This creates equal conditions for organizations in critical sectors and raises cybersecurity to the level of a strategic management priority [9].

2) Enhanced incident reporting procedure - establishes clear time frames for notifying about cyber incidents, which contributes to the creation of a unified database and ensures rapid and coordinated response to cyber threats [8–10].

Table 1

Comparative Characteristics of ISO 27001 Standard and NIS2 Directive

	ISO 27001	NIS2
Document type	International standart	European directive (regulatory and mandatory for organizations to comply with)
Goal	Determination of requirements for cybersecurity system	Improvement of security level for critical industry sectors
Sphere of usage	Any organization, regardless of size	Industrial and commercial clients/producers with 50+ workers
Control mechanism	Certificational audit	Monitoring from governing bodies
Field	Managing inner threats	Compliance with government regulations
Result of implementation	Certificate ISO 27001	Compliance with EU laws, security improvement

3) Supply chain security and sectoral requirements – puts forward increased requirements for assessing the reliability of suppliers and obliges organizations to bear direct responsibility for risks associated with third parties. This approach allows identifying and eliminating vulnerabilities that could potentially cause cyber incidents within entire sectors [3–4].

For effective implementation of a multi-level cyber defense system, the state must ensure:

– clear "rules of the game", enshrined in legislation, with the implementation of international standards, transparent response and control procedures, as well as flexible mechanisms for adapting to new risks;

– a developed institutional base – bodies controlling compliance with standards, certification systems, registration and licensing of entities, as well as platforms for public discussions and a system for training cybersecurity specialists in the public sector.

The responsibility of business in this process consists of:

– building trust in government institutions, undergoing licensing, certification, and audit procedures;

– implementing technical cyber defense mechanisms for self-protection and consumer protection – database encryption, password hashing, two-factor authentication, limiting the number of login attempts, etc.

At the same time, users are expected to have a high level of digital competence and adherence to cyber hygiene principles, which is the foundation of digital culture.

Despite having its own official cybersecurity requirements, one of the key directions for Ukraine should be updating the legal and regulatory base in accordance with the NIS2 directive. After all, the voluntary nature of ISO/IEC 27001 no longer meets modern challenges, and protection methods created back in the 2010s are outdated. The implementation of NIS2 has become an important step in developing management approaches, but in addition to critical infrastructure, the state, private, and scientific sectors require attention. And the main innovation should be the "Govern" function, which will emphasize that effective management in the field of cybersecurity begins not so much with technologies, but with responsible management, leadership, and strategic planning. By analyzing the experience of implementing the NIS2 directive in the countries of the European Union, Ukraine has the opportunity to take into account both the positive results and the difficulties faced by EU member states – and thus become one step closer to European integration.

References:

1. National Security and Defense Council of Ukraine. (2021). Cybersecurity Strategy of Ukraine for 2021-2025. Presidential Decree No. 447/2021 of August 26, 2021. Available at: https://rnbo.gov.ua
2. DSTU ISO/IEC 27001:2023. Information security, cybersecurity and privacy protection. Information security management systems. Requirements (ISO/IEC 27001:2022, IDT). Order No. 210 of August 17, 2023. Available at: https://zakon.rada.gov.ua/rada/show/v0223774-23#Text
3. ISO/IEC 27001:2022. Geneva: ISO, 2022. Available at: https://www.iso.org/standard/27001
4. NIS2 Directive: securing network and information systems. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive?utm.com
5. EU Digital Europe Programme. Available at: https://digital-strategy.ec.europa.eu/en/activities/digital-programme
6. European External Action Service. (2025, October 16). 4th EU-Ukraine Cyber Dialogue. Available at: https://eeas.europa.eu
7. Data Governance Act (EU) 2022. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868
8. Official Journal of the European Union. (2022). Directive (EU) 2022/2555 (NIS2 Directive). L 333, 27.12.2022. Available at: https://eur-lex.europa.eu
9. ENISA. Cybersecurity for SMEs Report 2024. Available at: https://www.enisa.europa.eu
10. Law of Ukraine “On the Basic Principles of Ensuring Cybersecurity in Ukraine”. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text