Regulation of CyberSecurity of Ukraine's Critical Infrastructure: Legal Aspects and Standards of Sustainable Protection

*Iaroslav Petrunenko**

Received: 29.03.2022
Accepted: 06.08.2022
Published: 25.08.2022

Abstract
This article addresses the regulatory and legal frameworks for protecting critical infrastructure facilities and civilian objects during armed conflicts, which is a key aspect of national stability and the survival of the state in the face of hybrid threats. The purpose of the study is to analyze the regulation of cybersecurity in relation to the country's critical infrastructure to ensure sustainable protection. The study employs comparative analysis of foreign cybersecurity regulations, such as NIST and ISO standards, and examines their adaptation to the conditions in Ukraine. Additionally, the study utilizes financial analysis methods, including assessments of budgetary expenditures on cybersecurity in Ukraine, as well as international aid and grants. The research established that thousands of infrastructure facilities, including networks for water, heat, gas, and electricity supply, as well as water and drainage systems, have been damaged or destroyed during the hostilities. Social and cultural infrastructure, such as schools, kindergartens, healthcare facilities, and cultural and historical monuments, have also been affected. The study highlights the key problems and obstacles within the existing cybersecurity legislation and examines international cybersecurity standards for their adaptation to the Ukrainian context. It also analyzes the coordination among various state institutions, including the Security Service of Ukraine (SBU), the State Service of Special Communications, and the Ministry of Digital Transformation. The results indicate an urgent need to improve the regulatory and legal framework for cybersecurity, enhance coordination between state bodies and the private sector, and integrate international experience and standards.

Keywords: legislation, normative acts, cyber protection standards, risks, security management.

INTRODUCTION

Critical infrastructure includes such systems, or their parts, which are extremely important for the state, including medicine, energy, economy, national defense and security. The cybersecurity of a critical infrastructure facility is ensured by the implementation of a comprehensive information protection system or an information protection system with confirmed compliance. An important aspect is that the cybersecurity of the critical infrastructure object is an integral part of the work related to the creation and operation of the critical information infrastructure object. Cyber security measures are planned and implemented at all stages of the critical information infrastructure object's life cycle. Given the importance of cybersecurity in today's world, critical infrastructure facilities are a particular target for cyber criminals and cyber threats. At the national level, such facilities include sectors critical to the functioning of society, such as energy systems, health care facilities, transportation systems, and telecommunications networks. Attacks on such systems can lead to disruption of business

Iaroslav Petrunenko
Doctor of Law, Professor, Department of Administrative and Economic Law, Odessa I.I. Mechnikov National University, Ukraine, petrunenko@yahoo.com, https://orcid.org/0000-0002-1186-730X, ResearcherID: B-8162-2019, Scopus Author ID: 57210814263

operations, loss of confidential data, and sometimes even threats to human life, which will have serious consequences in the future. As technology continues to evolve and the number of cyber threats increases, protecting critical infrastructure becomes a critical task. Over the past few years, Ukraine has faced several cyber attacks that have caused significant damage to its infrastructure and raised concerns about the country's preparedness, especially in relation to hybrid warfare launched by the Russian Federation. While the technical readiness and competence of cybersecurity personnel play an important role, they must be complemented by legislation that addresses cybersecurity needs. Currently, Ukraine has made significant progress in creating a legal framework for cybersecurity . In 2016, the CyberSecurity Strategy of Ukraine was adopted, which outlines the priorities and directions of cybersecurity and is an important structural element of the formation of a cybersecurity policy that meets world standards. In order to implement the Cyber Security Strategy, the Verkhovna Rada adopted the Law on CyberSecurity - the main legislative act that establishes the legal foundations of the cybersecurity system. The Law on Cyber Security defines the foundations of the cybersecurity system, including key national actors in the field of cybersecurity and their roles, as well as the coordination of activities in the field of cybersecurity. It also outlines critical infrastructure protection and serves as a starting point for further critical infrastructure regulation. This document also reviews draft regulations that have been proposed to further regulate the protection of critical infrastructure (Verkhovna Rada of Ukraine, 2021).

In the conditions of a full-scale war between Russia and Ukraine, the protection of critical infrastructure remains one of the key priorities of our state. In the current environment, cyber warfare is also taking place, which significantly increases the risks to infrastructure. The state of security of these objects is closely related to national security. Therefore, the enemy's numerous and targeted cyber attacks are primarily aimed at undermining the foundations of Ukraine's national security, in particular by causing damage to state information resources and internal objects of critical infrastructure.

The main focus of the research will be on the analysis of the effectiveness of the legislation in the field of critical infrastructure protection, as well as on the assessment of its compliance with international standards. Particular attention will be paid to specifying aspects that affect the effectiveness of legal regulation and identifying problem areas that need improvement.

Research problem

An important aspect of this study is a detailed analysis of the regulatory framework in the field of cybersecurity. In addition to the technical aspects, cybersecurity functions within the framework of the legal field. The Law "On the Basic Principles of Ensuring Cyber Security of Ukraine", adopted in 2017, is currently in force in Ukraine.However, despite the fact that this legislation is in force, the legal framework needs further improvement, regular updating and adaptation to international experience.

An important aspect of this study is the analysis of international standards such as ISO/IEC 27001 and the NIST Cyber Security Framework, which are essential for the effective protection of information systems. It also includes an assessment of current threats to critical infrastructure, taking into account the technical and organizational aspects of countering cyber attacks. It is important to identify the main challenges faced by critical infrastructure facilities and formulate recommendations for improving their protection.

Research directions are aimed at identifying controversial issues in current regulatory and legal documents of cybersecurity and provide recommendations for their settlement with the help of international experience and standards.

The **purpose** of the article is a comprehensive analysis of the current state and regulation of cybersecurity of Ukraine's critical infrastructure, as well as an assessment of the existing legal framework, in particular the Law of Ukraine "On the Basics of Ensuring cybersecurity of Ukraine". This document contains a detailed review and study of compliance with national legislation and international standards such as ISO/IEC 27001 and the NIST Cyber Security Framework. The main goal is to highlight the main shortcomings and problems of the current regulation of critical infrastructure, analyze the main threats and evaluate the measures aimed at their elimination.

Research Focus

The analysis of the normative and legal framework of Ukraine, which regulates the issue of cybersecurity , is the main goal of this study. How the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" guarantees the protection of critical infrastructure, in particular by checking the actual penetration and implementation of legal norms, international standards such as ISO/IEC 27001 and NIST Cybersecurity Framework, Conducting a comparative analysis with Ukrainian legislation. In order to conduct this comparison, it was necessary to evaluate how well international standards have been incorporated into national norms, identify any disparities and gaps, and examine how well the principles and requirements of international standards align with the current legislation of Ukraine.

Identification of the legal regulatory issue through evaluation of the efficacy of the application of legislative standards, considering the opinions of cybersecurity specialists and the examination of the inadequate safeguarding of vital infrastructure.

The degree of information system protection, the promptness of incident reaction, adherence to international regulations, and the evaluation of the actual impact on the safeguarding of vital infrastructure are among the performance metrics that are utilized for comparison.

Research questions

1. What are the main shortcomings of the current legislation of Ukraine in the field of cybersecurity of critical infrastructure?
2. How does Ukrainian cybersecurity legislation compare with international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework?
3. What specific changes and improvements are necessary to improve the effectiveness of Ukrainian legislation in the field of cybersecurity ?

LITERATURE REVIEW

The modern scientific space contains a lot of literature on cyberspace issues, from its essence, development forecasts to the analysis of certain cyber defence systems. To study the issue of cybersecurity of Ukraine's critical infrastructure with a focus on legal aspects, the works of contemporary Ukrainian researchers who are directly involved in the discourse and foreign researchers whose works have become the basis for analysing foreign experience and studying cyber defence systems were used.

Cybersecurity issues can be self-contained. For example, Alcaraz and Zedalli (2015) and Banerjee, Basu, and Sen (2018) highlight the changing demands and challenges of critical infrastructure protection in the 21st century and the best protection measures for them. Modernity also requires modern solutions, Brown, Saville, and Vargo (2017) argue. Their study emphasizes the importance of resiliency indicators and management processes to maintain infrastructure stability in the face of disruption. It discussed the broader cybersecurity challenges in the critical infrastructure sector (Dawson et al., 2011).

A separate issue is the introduction of cyber defence systems and the challenges to this. Integration of various cybersecurity standards is a recurring theme. This provides important practical information that can be used to predict the consequences of such implementation or to decide not to do so. In their study, Anttil et al. (2012) analyzed the integration of ISO/IEC 27001, highlighting the complexity of information security management in organizations. Similarly, Alcaraz and Lopez (2012) examine the requirements for critical facilities management systems and point out the need for a robust management system to effectively manage the security of critical infrastructure. The practical challenges to implementing these systems are addressed by Almuhammadi and Alsaleh (2017), who discuss the application of the NIST Cybersecurity Framework in the context of information security maturity models. They are complemented by Gordon, Loeb, and Zhou (2020), who advocate the inclusion of cost-benefit analysis in cybersecurity practice to improve decision-making. In one way or another, these papers complement each other, as they emphasise different aspects of this issue.

A separate issue is the introduction of cybersecurity systems and challenges. The integration of different cybersecurity standards

is a constant topic. This provides important practical information that can be used to predict the consequences of such implementation or to decide not to do so. In their study, Anttil et al. (2012) analyzed the integration of ISO/IEC 27001, highlighting the complexity of information security management in organizations. Similarly, Alcaraz and López (2012) examine the requirements for critical facilities management systems and point out the need for robust management systems to effectively manage the security of critical infrastructure. Regarding the practical challenges of implementing these systems, Almuhammadi and Alsaleh (2017) discuss the application of the NIST cybersecurity framework in the context of the information security maturity model. Gordon, Leb, and Zhou (2020) also advocate incorporating cost-benefit analysis into cybersecurity practices to improve decision making. In one way or another, these works complement each other, as they emphasize different aspects of this issue.

A separate issue in the paper is legal laws and regulations. In the proposed work, the works of Ukrainian authors are used more because of the existence of a unified legal framework. Bakalinska and Bakalynskyi (2019) analyze the legal framework for cybersecurity in Ukraine, emphasizing the need for a robust legal framework to support effective cybersecurity measures.

METHODS

The research employs a descriptive approach, which enables a clear understanding of the characteristics, trends, and relationships existing in the real world. The methodology in the field of cybersecurity regulation for critical infrastructure in Ukraine integrates both qualitative and quantitative approaches, providing a comprehensive analysis of legal aspects and protection standards. A systematic literature review (SLR) was conducted to gain an in-depth understanding of the existing legal frameworks and regulatory approaches, allowing for a broad analysis of relevant scientific works and legal documents.

The bibliometric analysis conducted included: (i) performance analysis, which described the main characteristics of the sample and identified the most influential documents and authors in the field of critical infrastructure cybersecurity; (ii) co-authorship analysis; (iii) co-citation analysis, which helped identify the most cited documents and standards; and (iv) keyword analysis, which revealed the major research topics within the selected sample.

This systematic literature review methodology enabled the identification of key legal and regulatory gaps in Ukraine's approach to critical infrastructure cybersecurity. Additionally, it facilitated the proposal of directions for further improvement of the national legislative framework and its harmonization with international standards.

For a detailed analysis of the compliance of Ukrainian legislation on critical infrastructure cybersecurity with international standards, such as ISO/IEC 27001 and the NIST Cybersecurity Framework, a set of comparison criteria and assessment methods was developed. These criteria encompass various aspects of the legal framework, technical requirements, and mechanisms for the implementation and monitoring of standards at the national level.

Sample and participants

The initial phase of the research involved conducting a comprehensive review of literature and legislative acts pertaining to Ukraine's cybersecurity regulations for critical infrastructure. Through a series of brainstorming sessions, the most relevant keyword combinations were selected to define the primary focus of the study. The Web of Science (WoS), a leading research platform, was employed to perform a keyword search related to cybersecurity law and critical infrastructure protection. The brainstorming aimed to identify the most precise keyword combinations reflecting key aspects of the topic, such as " cybersecurity ," "international standards," and "critical infrastructure."

Articles published between 2014 and 2022 were considered, as this period marked the most significant cyber attacks on Ukraine and the introduction of key legislative acts in this domain. The search yielded 789 sources, including scientific articles, legislative acts, and official reports on critical infrastructure protection and cybersecurity in Ukraine. These sources were subsequently selected for further analysis.

Instruments and Procedures

To analyze the compliance of Ukrainian legislation with international cybersecurity standards, WoS bibliometric analysis tools were used, which made it possible to specify the choice of sources. To increase the scientific quality of the sample, only peer-reviewed English-language publications, as well as legal acts available in open databases of Ukraine, were included. Conference papers and book chapters that did not pass rigorous peer review were excluded from the analysis.Further refinement of the sample included filtering submissions by WoS categories such as cybersecurity, law, information technology, critical infrastructure protection, and interdisciplinary research. The final selection of documents is based on works covering legal aspects and international aspects, such as ISO/IEC 27001 and the NIST Cybersecurity Framework, as well as their implementation in national legislation. Therefore, 50 sources that were already used directly in the research were chosen.

RESULTS

Cybersecurity is a vast and complex phenomenon that protects information systems, networks and data from unlawful access. 'The concept of 'cyberspace' was first used in the Okinawa Charter on the Global Information Society (Okinawa Charter on the Global Information Society) and the Convention on Cybercrime of 23.11.2001 (Convention on Cybercrime).' (Tkachenko et al., 2018, 77). 'According to the ISO/IEC 27032:2012 standard, cybersecurity is the preservation of the integrity, confidentiality and availability of information circulating in a cybersystem (i.e. information that enters a cybersystem, is accumulated and stored for further processing) in order to ensure the stability and continuity of the cybersystem's management functions in relation to the relevant management objects (Horbachenko, 2020, 183). The main goal is to ensure data security and integrity. Due to the process of globalisation and technologisation, cybersecurity has a significant impact on the economy, social sphere and security of citizens. Cybersecurity performs several functions at once. The first is the basic function. It is protection against cyberattacks (prevention, detection and counteraction to attempts to gain access to the system by unauthorised people). The second is monitoring the activity of threats and analysing their detection data. The third is strategy development. The fourth is risk management. 'The cybersecurity system consists of several elements, the coordination of which within an organisation is crucial to the success of the entire cybersecurity programme. These elements include the following: application security; data security; critical infrastructure security; network and operational security; cloud security; disaster recovery planning, and with it, business continuity; physical security; and end-user training.' (Sopilko, 2021, 111). But we should not forget that this problem is a common and international one, as cyberspace is vast (Orlov et al., 2013). It is important to realise that the quality and effectiveness of this area has implications for national security in general. Cyberattacks can complicate or even paralyse the work of state institutions, steal confidential (private) data, etc. Or, on the contrary, they can have minor but unpleasant consequences. For example, 'In cyberspace, such undesirable consequences include the classic well-known computer viruses that every citizen has encountered, in addition to the so-called "network worms" and "Trojan horses". All of these types of so-called network attacks, which have their own specifics and have a negative impact on the actual capability, are a form of danger in which it is difficult to identify the subject of influence and apply sanctions to it as a mechanism to protect the system. In modern Ukraine, there is no example of identifying and punishing subjects of influence within the framework of national law' (Zavgorodnya, 2021, 35). In general, it can be described as illegal interference with information technology. Considering the consequences for the economy, these are financial losses, decreased pace and productivity, increased costs Romanosky (2016) for system recovery after attacks and adaptation (Alcaraz, 2021; Alcaraz, 2015). If we take the private sphere for analysis, it is 'publicity' and loss of privacy due to theft of personal data, passwords, fraud, theft of money, etc. The last important area is critical infrastructure. Its issues include problems with the supply of electricity and water, the rapid provision of medical services, or the possibility

of providing them at all, etc.

Critical infrastructure is a set of facilities, systems, and networks that are essential to national security, economic stability, public health and safety. Simply put, these are the facilities that ensure people's lives. 'In particular, critical infrastructures can be seen as central elements in a widespread network of risk' (Pescaroli et al., 2016). These include: energy and transport systems, water supply networks, communications companies, financial institutions, healthcare facilities, etc. (Banerjee et al., 2018), (Kattel et al., 2020), (Brown et al., 2017; Kitagawa et al., 2016). That is why the protection of critical infrastructure is and should be one of the main issues of national security. 'As the arteries of modern cities, critical infrastructures are the cornerstones of resilient cities because their incapacitation or destruction will exert debilitating impacts on security, economy, public health or safety, environment, or any combination of these factors' (Liu et al., 2020). Ukrainian researcher Biryukov et al. (2012), studying the issue of critical infrastructure security, based on the work of Ted Lewis (2006), identifies the main challenges: knowledge of critical infrastructure in itself is important. The interdependence of government agencies, the public and private sectors, subject to the economic factor. The issue of data accumulation and implementation. Pluralism of relations within all critical infrastructure agents.

In addition, we would like to emphasise that there are 'cloud infrastructures' (Semenemko et al., 2019). 'Over the past few years, cloud computing has become the main direction of development of the modern IT industry. The use of the cloud can significantly improve the flexibility and scalability of an enterprise's IT infrastructure' Semenemko et al. (2019), which in turn has an impact on critical infrastructure, as it also has applications for customer communication, maintenance and service delivery. The concept of the Internet of Things should be added to this. 'The Internet of Things is the technological concept of connecting devices around the world to the Internet in order to control them remotely.' (Filinovych, 2020, 123; Gunduz et al., 2020).

If we take into account Ukraine's experience with critical infrastructure problems and challenges, we will see an insufficient level of protection against cyberattacks, outdated technical infrastructure, limited financial resources and insufficient understanding of risks by company management. One of the main challenges for the country is the dissemination and adaptation of international cybersecurity standards to the Ukrainian discourse. Over the past 10 years, Ukraine has experienced several major attacks. Western Ukraine, December 2015. Hackers knocked out the power supply system. June 2017 - the Petya virus. A large-scale cyber attack that paralysed the work of many public and private institutions. As a result, there were large financial losses, disruptions in work, or its termination. The reason was the lack of appropriate software provision, relevant units and state strategy, developed and aimed at the protection of both the citizen and the state. This case, like similar ones, once again showed the key role of the cyber front in the context of the Russian invasion of Ukraine (Saenko et.al., 2021). During 2020-2022, there were several notable cases in Ukraine that demonstrate jurisdictional conflicts and problems with limited funding in the field of cybersecurity. In 2021, problems arose regarding the coordination of efforts between the State Service for Special Communications and Information Protection of Ukraine (SSI), the Ministry of Digital Transformation, and the Security Service of Ukraine. Each of these bodies has certain functions in the field of cybersecurity, but no clear division of powers has been established. This led to situations where government agencies acted uncoordinated during cyber attacks, affecting the speed and effectiveness of the response. One example is the cyber attacks on government information systems in December 2021, when coordination between departments was not operational enough (Zavgorodnya, 2021).

In 2022, it became clear that the lack of a clear definition of who is responsible for protecting critical infrastructure leads to coordination problems. For example, a cyber attack on the energy sector in April 2022 caused a debate between the SSSZI and the SBU about who should respond to these threats and provide protection, which delayed the response to the threat.

After a large-scale cyber attack on state websites and banks in January 2022, it became known that a significant number of Ukrainian state structures do not have sufficient funding for the

implementation of modern means of cyber protection. According to reports, only a fraction of mission-critical institutions had updated protections, while most were vulnerable due to a lack of adequate cybersecurity funding. This is stated in analyst reports regarding Ukraine's low level of preparedness for complex cyber attacks. Despite the international support that came in the form of technical assistance from the EU and the USA in 2021-2022, Ukrainian state bodies still experienced significant financial difficulties. Budgetary spending on cybersecurity remains low due to the general economic crisis and military spending, which has forced government agencies to depend on foreign aid. For example, assistance within the framework of the USAID project "Cybersecurity of Ukraine's Critical Infrastructure" in 2021 only partially covered the needs for modernization of systems (Zhydovtseva, 2022).

These examples demonstrate that jurisdictional conflicts between government agencies and insufficient funding remain serious obstacles to effective protection of Ukraine's critical infrastructure.

The legal aspect of cybersecurity of Ukraine is based on the law "On the Basic Principles of Ensuring Cyber Security of Ukraine" (Law of Ukraine No. 45, 2017), which defines the key norms and principles of state policy in the field of cybersecurity . This law lays the legal and organizational foundations for the creation and implementation of cybersecurity initiatives, regulates information protection and defines procedures for public and private organizations. An important role in this process is played by the Cabinet of Ministers of Ukraine (implements state policy in the field of cybersecurity), the Security Service of Ukraine (coordinates and investigates cybercrimes), the National Police (focuses on cybersecurity violations) and CERT-UA (Computer Emergency Response Team of Ukraine, which monitors cyber threats).

The key components of comparing and evaluating the effectiveness of Ukrainian legislation are its compliance with international cybersecurity standards, in particular ISO/IEC 27001 and the NIST Cybersecurity Framework. For this study, an analysis of the legislative acts of Ukraine was carried out in the context of their compliance with the specified standards. In particular, attention was focused on the following aspects:

The ISO/IEC 27001 standard is a globally recognized standard that provides clear requirements for information security management systems (ISMS). Its main objective is to ensure the confidentiality, integrity and availability of information assets through the systematic management of risks related to information security. In the context of Ukraine, the study on the implementation of ISO/IEC 27001 is based on a detailed analysis of national legal acts related to information security and risk management.

In Ukrainian legislative acts, such as the Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine" and other normative acts, the main principles of information security are established, which coincide with the requirements of ISO/IEC 27001. For example, the principles of information protection, which include ensuring its confidentiality, integrity and availability, are consistent with the main provisions of this international standard.

Confidentiality refers to the prevention of unauthorized access to information, which is reflected in Ukrainian laws through requirements for the protection of state and commercial secrets. It was analyzed how the requirements regarding the use of encryption technologies, access control, as well as the role of state bodies, in particular the Security Service of Ukraine (SBU) and the State Service for Special Communications and Information Protection of Ukraine (SSIS) in ensuring the confidentiality of information assets, are implemented in practice. An example is the implementation of SBU and DBR encryption standards at state-owned enterprises and institutions, which takes place within the framework of the Law "On the Protection of Information and Information and Telecommunication Systems" and corresponds to international regulations and standards, namely AES (Advanced Encryption Standard) for the protection of confidential data.

Integrity refers to maintaining the accuracy and completeness of data, which is also a key aspect of the standard. Ukrainian legislation regulates these issues through requirements for auditing systems, monitoring and data verification in public and private organizations. It is also important to regulate measures to detect and eliminate cases of falsification or alteration of information.

The procedure for assessing compliance with ISO/IEC 27001 national laws included an analysis of ISMS implementation mechanisms in public institutions and the private sector. It was determined that Ukrainian enterprises are beginning to apply complex approaches to information security management, but the process of implementing systems remains at the stage of formation and needs improvement. In part, this is due to insufficient awareness of the private sector with international standards and the lack of unified approaches to their implementation.

In addition, it is important to note that in order to comply with ISO/IEC 27001 standards, Ukrainian enterprises must create integrated risk management systems. This includes both the identification of potential threats to information assets and the development of response plans for possible incidents. At the same time, it was analyzed how government bodies, such as CERT-UA, help in maintaining national security through the implementation of tools for monitoring cyber threats and responding to incidents.

An important tool that manages cybersecurity risks is the NIST Cybersecurity Framework (NIST CSF). This document brings together internationally recognized standards, tools and practices for organizations to prevent and manage cybersecurity risks. Having conducted a study of Ukrainian legislation to assess its compliance with NIST principles and requirements, CSF has shown both positive aspects and shortcomings that require further improvement.

One central aspect of the NIST CSF is the risk management process, which encompasses the identification, analysis, assessment, and mitigation of cyber threats. In Ukrainian legislation, such issues are regulated through laws related to cybersecurity and information protection, in particular the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine" (2017). It outlines general requirements for risk identification and threat response, but lacks detailed mechanisms for implementing systematic risk management consistent with NIST standards.

The NIST CSF emphasizes a comprehensive approach to risk management, including continuous monitoring and updating strategies based on changing threats. In this context, Ukraine has begun implementing elements of a risk management system through CERT-UA (Ukraine's Computer Emergency Response Team), which helps monitor cyber threats. However, in order to achieve full compliance with NIST standards, it is necessary to improve risk management processes at the level of both government agencies and private organizations, ensuring the integration of cyber risks into the overall risk management strategy.

Protecting critical infrastructures is a key element in the NIST CSF that ensures organizations' cyber resilience and business continuity. In Ukrainian legislation, in particular, in the Law "On the Basic Principles of Ensuring Cyber Security of Ukraine", responsibility for the protection of critical infrastructures is defined, with an emphasis on energy, transport, the financial sector and communications (Verkhovna Rada of Ukraine, 2016). Although these aspects are generally consistent with the NIST CSF, there are significant challenges in their practical implementation, especially in relation to the interaction between the private and public sectors.

The NIST CSF also emphasizes the importance of collaboration between various actors in the cybersecurity space, including government agencies, private companies, and international partners. It is important for Ukraine to develop this cooperation through public-private partnership, involvement of international experts and integration into European and global cybersecurity structures. A positive example is Ukraine's cooperation with NATO through the NATO Cyber Security Trust Fund, which helps to improve means of protecting critical infrastructures.

Monitoring and timely response to cyber threats is another important element of the NIST CSF. In this direction, Ukraine already has certain achievements, in particular, the creation of situation centers on the basis of the SBU and the State Service for Special Communications and Information Protection of Ukraine, which are engaged in tracking and responding to cyber attacks. However, the analysis of Ukrainian approaches shows that there are still problems with the integration of international best practices at the level of monitoring and response to incidents.

Table 1. Name Comparison of cybersecurity systems

Aspect	ISO/IEC 27001	CIS Controls	NIST Cybersecurity Framework
Purpose	To establish, implement, maintain, and continually improve an information security management system (ISMS)	To provide a set of best practices for securing IT systems	To provide a policy framework for managing cybersecurity risks
Structure	14 clauses with requirements for establishing an ISMS	18 controls grouped into 3 categories: Basic, Foundational, Organizational	Five core functions: Identify, Protect, Detect, Respond, Recover
Focus	Comprehensive information security management	Practical, actionable security measures and controls	Risk management and alignment with business objectives

Adaptation of the proposed international standards (ISO/IEC 27001, NIST Cybersecurity Framework and CIS Controls) in Ukraine is an important step towards improving the level of cybersecurity of critical infrastructure. At the moment, Ukraine has already started the process of integrating international standards, which in turn is reflected in the legal sector (adoption of the necessary laws and regulations). However, the current legislation still has certain shortcomings.

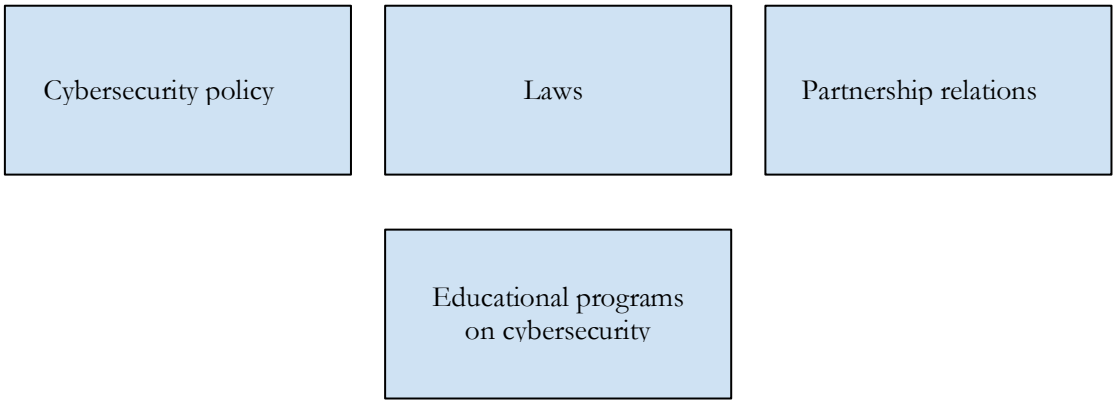

Figure 2. Shows Ukraine's actions in dealing with cybersecurity since 2019

Ukraine is in the early stages of developing a national system for ensuring the security of critical infrastructure. When examining foreign experience in this context, it is crucial to recognize that mechanically transferring even the most advanced practices without due consideration of Ukraine's current specifics and realities can undermine efforts in this area, compromise initiatives, and significantly hinder progress within the country.

Although Ukraine is not an EU member and is therefore not legally bound by the NIS Directive, the directive serves as a valuable guideline for best practices. Some provisions have been voluntarily incorporated into Ukrainian legislation, while others remain unresolved. A draft law has been registered in the Verkhovna Rada of Ukraine that aims to harmonize Ukrainian legislation with European Union law, including the NIS Directive. The State Service for Special Communication and Information Protection is working to

incorporate NIS Directive requirements into its legislative initiatives. However, representatives acknowledge that international assistance will be crucial in developing comprehensive cybersecurity laws that meet the standards of the NIS Directive (Horbachenko, 2020).

The Budapest Convention on Cybercrime is the only legally binding regional document on the issue. As a signatory, Ukraine has incorporated its key provisions into national legislation. However, for the effective implementation of the full scope of the Budapest Convention, the Criminal Procedure Code of Ukraine requires more detailed definitions concerning cybersecurity terms. According to Ukraine's Cybersecurity Strategy, approved by Presidential Decree No. 447 on August 26, 2021, ensuring cybersecurity is a top priority within the national security system (Zavgorodnya, 2021).

Weaknesses in the existing cybersecurity regulations in Ukraine arise from the lack of a comprehensive legal framework and the presence of numerous gaps and ambiguities in legislation. Ukrainian legislation lacks clear definitions of critical terms such as "user of services," "data on the movement of information," and "electronic evidence." Additionally, important aspects such as the urgent preservation of data are not adequately regulated, complicating the implementation of the Budapest Convention and international cooperation in combatting cybercrime. The Cybersecurity Law introduces new terms that are not always aligned with other legal acts, leading to legal confusion.

The absence of a special law on critical infrastructure protection highlights the lack of a unified national system for protecting critical infrastructure(Cabinet of Ministers of Ukraine, 2019). Existing regulatory rules are insufficient, with no clear criteria for identifying critical infrastructure objects or procedures for their certification and categorization, rendering certain provisions of the Cybersecurity Law merely declarative. The inadequacy of information security audit rules further complicates the situation. Despite the Cybersecurity Law mandating the creation of such rules for critical infrastructure objects, the deadlines have passed without their adoption. Another issue is the duplication of responsibilities among various bodies involved in cybersecurity, such as the Ministry of Defense, the Security Service of Ukraine (SBU), and the National Police (National Police of Ukraine, 2015). This leads to legal uncertainty and overlapping functions. Moreover, there is a lack of clear security requirements for critical infrastructure operators and digital service providers. While the Cybersecurity Law requires reporting cyber incidents, it lacks specific requirements and procedures for critical infrastructure operators. The incomplete implementation of the NIS Directive leaves certain aspects unaddressed.

In addition, there is no long-term strategic cybersecurity plan. Although the National Cybersecurity Strategy was adopted in 2016, the absence of an updated action plan hampers the industry's development. Budget constraints also pose challenges, as low salaries for cybersecurity professionals in government agencies reduce motivation and create vulnerabilities.

An analysis of global best practices shows that Ukraine is only in the early stages of establishing a national system for critical infrastructure protection. To effectively prevent and mitigate threats to critical infrastructure, it is necessary to adapt international best practices while considering military threats specific to Ukraine.

DISCUSSION

The main problem of this study is to ensure effective cyber protection of critical infrastructure of Ukraine in the conditions of hybrid warfare and other modern challenges. Special attention was paid to the analysis of compliance of the legal framework of Ukraine with international cybersecurity standards, such as ISO/IEC 27001 and NIST Cybersecurity Framework.

The main objective of the study was to conduct a comprehensive analysis of the current state of cybersecurity and critical infrastructure legal regulation in Ukraine and to assess the existing legal framework, in particular the Law of Ukraine “On Basic Principles for Ensuring Cybersecurity in Ukraine” and its compliance with international standards. It also aimed to identify the main shortcomings of the existing legislation and to propose changes to improve its effectiveness.

The first result of the study was the identification of a number of problems in Ukrainian legislation related to cybersecurity of critical infrastructure. One of the key conclusions is that while the current "Law on Basic Principles for Ensuring Cybersecurity in Ukraine" creates a general legal framework for ensuring cybersecurity, there are significant gaps. For example, the law lacks clear criteria for defining critical infrastructure, and there is no law regulating the protection of this infrastructure at the national level. Furthermore, it was found that there are no clear cybersecurity requirements for critical infrastructure operators.

With regard to compliance with international standards, it was found that Ukraine's legislative framework is only partially compliant with ISO/IEC 27001 and NIST standards. For example, Ukrainian legislation reflects well the principles of confidentiality, integrity, and availability of information, which are key requirements of ISO/IEC 27001. In practice, however, the level of implementation of these standards in Ukrainian infrastructure is low due to a number of problems, including limited funding, lack of coordination among government agencies, and low awareness of international standards in the private sector.

This refers to an attack on the Ukrainian government and banking system in January 2022. This hacking attack led to the temporary shutdown of several government websites and banking services. The analysis of the incident showed that most government organizations did not implement modern cybersecurity measures, such as multi-factor authentication and network segmentation, which are part of the requirements of international standards ISO/IEC 27001 and NIST. Despite the existence of legislation governing the protection of information, lack of funding and insufficient attention of organizations to risk management create additional vulnerabilities.

Another example concerns the activities of the private sector in Ukraine. Many of them have not switched to international standards due to insufficient awareness and the high cost of certification and implementation of cybersecurity systems. For example, in the Ukrainian IT sector, many companies operate on the international market, but a significant part of them do not meet the ISO/IEC 27001 standard due to the lack of motivation and support from the state. This makes them less attractive to international partners who need an advanced level of information security. These examples illustrate the gap between existing legislative requirements and the real situation in Ukraine's cybersecurity sector.

The results of this study confirm the conclusions of a number of international studies regarding the importance of implementing international standards for the protection of critical infrastructure. For example, a study by Alcaraz and Lopez (2012) indicates the need to implement a standardized information security management system (ISMS) to ensure cyber protection of critical objects. This coincides with our conclusions about the need to integrate ISO/IEC 27001 into the Ukrainian context. However, studies show that the reality in Ukraine is that financial and institutional obstacles significantly complicate this process.

Another example is the study by Anttil et al. (2012), which emphasizes the complexity of information security management in organizations. State institutions and private companies in Ukraine face difficulties in implementing a comprehensive approach to cybersecurity management due to the lack of uniform standards and regulatory mechanisms.

On the other hand, some aspects of this study are inconsistent with the findings of other researchers. For example, Almuhammadi and Alsaleh (2017) note that the implementation of the NIST Cybersecurity Framework is an effective tool for increasing the maturity of cybersecurity systems. However, this approach turned out to be ineffective in Ukraine due to the lack of a clear risk management mechanism at the national level and the weak integration of cyber risks into the overall risk management strategy.

Our survey revealed a surprising deficiency in the coordination among government agencies responsible for cybersecurity. Despite the presence of multiple responsible bodies, including the State Service of Special Communications, the Ministry of Digital Transformation, and the Security Service of Ukraine, the absence of effective inter-agency collaboration has led to the duplication of functions and delays in responding to cyber incidents. This issue stems from poorly defined authorities among these entities and gaps in the

existing legislation governing this area.

Despite international support in the form of technical assistance and grants, implementation of international cybersecurity standards remains limited. This can be explained both by the imperfection of national legal and organizational mechanisms, and by the lack of human resources capable of integrating these standards at the local level.

Furthermore, although Ukrainian legislation partially meets international standards, actual implementation is problematic due to limited funding for cybersecurity. For example, many government agencies and private companies do not have sufficient resources to modernize their cyber defense systems, leaving them vulnerable to cyber attacks. This was especially true during the 2022 cyberattack, which revealed that most government agencies are not equipped with modern cyber defense systems due to lack of funding. One of the main limitations of this study is that it is based on secondary data, i.e., analysis of current legislation, surveys, and reports. The lack of experimental or observational data may affect the accuracy of conclusions, especially in the context of practical aspects of cybersecurity, such as the effectiveness of certain defensive measures. In addition, the completeness of the findings may be limited because the analysis only included documents and case studies available at the time the study was completed.

Another limitation is that while this study focuses primarily on the experience of EU and NATO countries, the Ukrainian situation has unique characteristics and may require a different approach to the protection of critical infrastructure.

The scientific novelty of this study lies in the comparative analysis of the compliance of Ukrainian legislation in the field of cybersecurity with international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework. This made it possible to identify key gaps in the legislative framework and provide specific recommendations for its improvement. In particular, the need to adopt special legislation on critical infrastructure, establish clear standards for identification and protection of critical infrastructure objects, and introduce a cybersecurity audit mechanism is emphasized.

Limitations

The study's analysis covered only those documents and regulations and analysed specific cases that were available at the time of completion, which may have limited the completeness of the findings, as new regulations and cyber incidents may not have been taken into account. It is also possible that the experience was mainly from the EU and NATO. The second problem is that the study was based on secondary data (no experimentation, observation, etc.), which may affect the accuracy of the conclusions in the absence of detailed information on specific aspects of attacks or regulatory processes.

CONCLUSIONS AND RECOMMENDATIONS

In recent years, several problems have been solved in Ukraine, which allowed the country to fulfil its international obligations and improve its cybersecurity legislation, but this is not enough, and many more steps need to be taken to further improve it. Among these steps is the adoption of a comprehensive law on cybersecurity, as the 2017 law only sets the stage for further legislative development. Ukraine needs a comprehensive law that will regulate all aspects of cybersecurity by international standards. To do this, it is necessary to consult with various stakeholders and engage experts.

In addition, it is important to analyze the legal framework of the NIS Directive, in particular, to identify provisions that contradict the Directive and make the necessary amendments. Ukraine needs international assistance to develop the relevant draft laws. It is also necessary to harmonize the terminology in national legislation, as the adopted and existing laws use different terms, which complicates their implementation.

Another problem is the lack of strategic communication regarding cyber incidents. The NIS Directive requires the creation of protocols for the exchange of information about cyber incidents between stakeholders and

cybersecurity authorities to improve coordination and response efficiency. It is also necessary to adopt the Law on Critical Infrastructure Protection and secondary legislation, as although the Law on Cybersecurity and the Concept of Critical Infrastructure Protection have laid the groundwork, specific legislation is needed to regulate the protection of critical infrastructure (Verkhovna Rada of Ukraine, 2017).

An effective step would be to develop a law on public-private partnerships in the field of cybersecurity, as the current law on public-private partnerships does not cover this area. It is also necessary to consider in detail the distribution of powers between law enforcement agencies responsible for cybersecurity and address the effectiveness of their interaction.

An assessment of the implementation of the cybersecurity strategy adopted in 2016 is urgent, as no evaluation of its implementation has been conducted so far. In this regard, it is also necessary to develop a new strategy for the period 2025-2030, as the current strategy expires in 2025.

Suggestions for Future Research

The first area for future research should focus on exploring emerging cyber threats and their evolutionary trends to enable the timely adaptation of defence mechanisms. Secondly, research could investigate how implementing international standards impacts the practical aspects of cybersecurity at both global and national levels, including identifying issues that can be addressed collaboratively. A third potential research direction is the analysis of the effectiveness of various sources of cybersecurity funding, including governmental support, international investments, and public initiatives.

REFERENCES

Ablon, L., & Institute for Civil Justice (U.S.). (2016). *Consumer attitudes toward data breach notifications and loss of personal information*. Rand Corporation. https://www.jstor.org/stable/10.7249/j.ctt1bz3vwh

Alcaraz, C., & Lopez, J. (2012). Analysis of requirements for critical control systems. *International Journal of Critical Infrastructure Protection, 5(3-4)*, 137–145. https://doi.org/10.1016/j.ijcip.2012.08.003

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8,* 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST Cybersecurity Framework. *Computer Science & Information Technology (CS & IT), 7,* 29–37. https://doi.org/10.5121/csit.2017.70305

Ani, U. P. D., He, H., & Tiwari, A. (2016). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of cybersecurity Technology, 1(1),* 32–74. https://doi.org/10.1080/23742917.2016.1252211

Anttila, J., Jussila, K., Kajava, J., & Kamaja, I. (2012). Integrating ISO/IEC 27001 and other managerial discipline standards with processes of management in organizations. *In 2012 Seventh International Conference on Availability, Reliability and Security* (pp. 425–436). IEEE. https://doi.org/10.1109/ARES.2012.93

Bakalinska, O., & Bakalynskyi, O. (2019). Pravove zabezpechennia kiberbezpeky v Ukraini [Legal support of cybersecurity in Ukraine]. *Pidpryiemnytstvo, hospodarstvo i pravo, 9,* 100–108. https://doi.org/10.32849/2663-5313/2019.9.17 [In Ukrainian].

Banerjee, J., Basu, K., & Sen, A. (2018). On hardening problems in critical infrastructure systems. *International Journal of Critical Infrastructure Protection, 23*, 49–67. https://doi.org/10.1016/j.ijcip.2018.08.001

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *School of Finance, University of St. Gallen.* https://doi.org/10.2139/ssrn.2577286

Biryukov, D. S., & Kondratov, S. I. (2012). *Zakhyst krytychnoyi infrastruktury: problemy ta perspektyvy vprovadzhennya v Ukrayini* [Protection of critical infrastructure: Problems and prospects for implementation in Ukraine]. Kyiv: National Institute for Strategic Studies. https://niss.gov.ua/sites/default/files/2013-02/Sots_zahust-86178.pdf [In Ukrainian].

Boyko, V., Vasylenko, M., & Kukharenko, S. (2019). cybersecurity in the EU and member countries: Genesis and problems of

its enhancement. *Information Security of a Person, Society, State, 3(27)*, 57–69. https://journals.uran.ua/ispss/article/view/196117

Brown, C., Seville, E., & Vargo, J. (2017). Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study. *International Journal of Critical Infrastructure Protection, 18*, 37–49. https://doi.org/10.1016/j.ijcip.2017.05.002

Cabinet of Ministers of Ukraine. (2019). *Pro krytychnu infrastrukturu ta yii zakhyst, Proekt Zakonu No. 10328* [On critical infrastructure and its protection, Draft Law No. 10328]. Retrieved March 28, 2021, from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996 [In Ukrainian].

CSIS. (2014). *Net losses: Estimating the global cost of cybercrime*. Center for Strategic and International Studies.

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review, 26(1),* 69–75. https://doi.org/10.2478/raft-2021-0011

Denysov, A. I., Bershov, H. Y., Krykun, V. V., & Zhydovtseva, O. (2022). Protection of critical infrastructure facilities as a component of the national security. *Cuestiones Políticas, 39(71),* 789–799. https://doi.org/10.46398/cuestpol.3971.48

Diorditsa, I. V. (2017). Cybersecurity system: Essence and purpose. *Entrepreneurship, Economy and Law,* 109–116.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 04(02),* 92–100. https://doi.org/10.4236/jis.2013.42011

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb model. *Journal of Cybersecurity, 6(1),* Article tyaa005. https://doi.org/10.1093/cybsec/tyaa005

Groš, S. (2021). A critical view on CIS controls. *In 2021 16th International Conference on Telecommunications (ConTEL)*(pp. 1–6). IEEE. https://doi.org/10.23919/ConTEL52528.2021.9495982

Hnatiuk, S. O., Riabyi, M. O., & Liadovska, V. M. (2014). Vyznachennia krytychnoi informatsiinoi infrastruktury ta yii zakhystu: Analiz pidkhodiv [Critical information infrastructure definition and protection: Approach analysis]. *Zv'iazok, 4,* 3–7. [In Ukrainian].

Hobby, Y. (2020). The human right to cybersecurity: Problems of definition and guarantee. *Legal Bulletin, 2,* 37–43. https://doi.org/10.32837/yuv.v0i2.1701

Horbachenko, S. (2020). cybersecurity as a component of economic security of Ukraine. *Galician Economic Journal*, 66(5), 180. https://doi.org/10.33108/galicianvisnyk_tntu2020.05.180 [In Ukrainian].

ISO/IEC 27001:2013.*Information security management*. International Organization for Standardization. Retrieved September 10, 2024, from https://www.iso.org/isoiec-27001-information-security.html

Jamar Kattel, P., & Aros-Vera, F. (2020). Critical infrastructure location under supporting station dependencies considerations. *Socio-Economic Planning Sciences, 70,* 100726. https://doi.org/10.1016/j.seps.2019.07.002

Jirásko, D., Vaníček, I., & Vaníček, M. (2017). Interaction of landslide with critical infrastructure. In Mikoš, M., Arbanas, Ž., Yin, Y., & Sassa, K. (Eds.), *Advancing Culture of Living with Landslides. WLF 2017* (pp. 439–445). Springer. https://doi.org/10.1007/978-3-319-53487-9_64

Karchefsky, S., & Rao, H. R. (2017). Toward a safer tomorrow: Cybersecurity and critical infrastructure. In H. Ellermann, P. Kreutter, & W. Messner (Eds.), *The Palgrave handbook of managing continuous business transformation* (pp. 415–433). Palgrave Macmillan. https://doi.org/10.1057/978-1-137-60228-2_15

Kitagawa, K., Preston, J., & Chadderton, C. (2016). Preparing for disaster: A comparative analysis of education for critical infrastructure collapse. *Journal of Risk Research, 20(11),* 1450–1465. https://doi.org/10.1080/13669877.2016.1178661

Lewis, T. G. (2006). *Critical infrastructure protection in homeland security: Defending a networked nation*. John Wiley & Sons.

Liu, W., & Song, Z. (2020). Review of studies on the resilience of urban critical infrastructure networks. *Reliability Engineering & System Safety, 193,* 106617.

https://doi.org/10.1016/j.ress.2019.106617

National Institute of Standards and Technology (NIST). (2014). *Framework for improving critical infrastructure cybersecurity*. https://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

National Police of Ukraine. (2015). *Nakaz pro zatverdzhennia Polozhennia pro Departament kiberpolitsii Natsionalnoi politsii Ukrainy, Nakaz No. 85* [On Approval of the Regulation on the Cyber Police Department of the National Police of Ukraine, Order No. 85 (2015)]. Retrieved March 28, 2021, from http://tranzit.ltd.ua/nakaz/ [In Ukrainian].

Orlov, O. V., & Onyshchenko, Y. M. (2013). International cooperation in the fight against cybercrime. *Theory and Practice of Public Administration, 4,* 17–23.

Pescaroli, G., & Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards, 82(1),* 175–192. https://doi.org/10.1007/s11069-016-2186-3

Robertson, J., & Reilly, M. (2014). The map that shows why a pipeline explosion in Turkey matters to the U.S. *Bloomberg.* Retrieved May 14, 2015, from http://www.bloomberg.com/news/2014-12-10/the-map-that-shows-why-a-pipeline-explosion-in-turkey-matters-to-the-u-s-.html

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, tyw001. https://doi.org/10.1093/cybsec/tyw001

Saenko, M. I., Savela, E. A., & Topolyansky, Y. Y. (2021). International experience against cyber crime and cyber crime. *Uzhhorod National University Herald, Series: Law,* 64, 386–391. https://doi.org/10.24144/2307-3322.2021.64.71

Semenemko, O., & Lavreniuk, I. (2019). Khmarnitekhnolohii yak odyn z naiperspektyvnishykh napriamkiv rozvytku suchasnykh informatsiinykh tekhnolohii [Cloud technologies as one of the most promising directions of development of modern information technologies]. *Materialy IV Mizhnarodnoi naukovo-tekhnichnoi konferentsii "Teoretychni ta prykladni aspekty radiotekhniky, pryladobuduvannia i komp'iuternykh tekhnolohii"*, 59–61. [In Ukrainian].

Sheikhpour, R., & Modiri, N. (2012). An approach to map COBIT processes to ISO/IEC 27001 information security management controls. *International Journal of Security and Its Applications, 6(2)*, 13–28.

Slipachuk, L., Toliupa, S., & Nakonechnyi, V. (2019). The process of the critical infrastructure cybersecurity management using the integrated system of the national cybersecurity sector management in Ukraine. *IEEE.* https://doi.org/10.1109/AIACT.2019.8847877

Sopilko, I. (2021). Information security and cybersecurity : Comparative and legal aspect. *Scientific Works of National Aviation University. Series: Law Journal "Air and Space Law, 2(59),* 110–115. https://doi.org/10.18372/2307-9061.59.15603

Stine, K., Quill, K., & Witte, G. (2014). *Framework for improving critical infrastructure cybersecurity*. ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=915476

Sussy, B., Wilber, C., Milagros, L., & Carlos, M. (2015). ISO/IEC 27001 implementation in public organizations: A case study. *In 2015 10th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1–6). IEEE. https://doi.org/10.1109/CISTI.2015.7170355

Tkachenko, O., & Tkachenko, K. (2018). Cyberspace and cybersecurity: Problems, perspectives, technologies. *Digital Platform: Information Technologies in Sociocultural Sphere, 1*, 75–86. https://doi.org/10.31866/2617-796x.1.2018.147257

Trofymenko, O., Prokop, Y., Loginova, N., & Zadereyko, O. (2019). Cybersecurity of Ukraine: Analysis of the current situation. *Ukrainian Information Security Research Journal, 21(3).* https://doi.org/10.18372/2410-7840.21.13951

Verkhovna Rada of Ukraine. (2016). *Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky [On the National cybersecurity Coordination Center]* (Ukraine), 07.06.2016, No. 242/2016. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/242/2016#Text [In Ukrainian].

Verkhovna Rada of Ukraine. (2017). *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy, Zakon Ukrainy vid 05.10.2017 № 2163-VIII* [On the Basic Principles of Cybersecurity in Ukraine, Law of Ukraine on October 5, 2017 № 2163-VIII]. Retrieved March 28, 2021, from

https://zakon.rada.gov.ua/laws/show/2163-19/ed20211215#Text [In Ukrainian].

Verkhovna Rada of Ukraine. (2021). *Stratehiia voiennoi bezpeky Ukrainy "Voienna bezpeka – vseokhopliuiucha oborona"* [Military Security Strategy of Ukraine "Military Security – Comprehensive Defense"], 25.03.2021, No. 121/2021. Retrieved March 28, 2021, from https://zakon.rada.gov.ua/laws/show/121/2021#n2

White, G. B., & Sjelin, N. (2022). The NIST Cybersecurity Framework. In *Research Anthology on Business Aspects of Cybersecurity* (pp. 17). IGI Global. https://doi.org/10.4018/978-1-6684-3698-1.ch003

Zavgorodnya, Y. (2021). cybersecurity as an innovative protection in the political space of Ukraine. *National Technical University of Ukraine Journal. Political Science. Sociology. Law, 4(52),* 33–38. https://doi.org/10.20535/2308-5053.2021.4(52).248130