



UDC [347.19+342.9]:004.056(477+474.5)

DOI: <https://doi.org/10.32631/pb.2023.4.14>**MARIJA PLESKACH,**

Doctor of Philosophy in Law,
Vilnius Gediminas Technical University (Lithuania),
Faculty of Fundamental Sciences,
Department of Information Systems;
 <https://orcid.org/0000-0003-3296-5475>,
e-mail: pleskachmarija@gmail.com;

INGA TUMASONIENE,

Associate Professor, Doctor (Assoc. Prof. Dr.),
Vilnius Gediminas Technical University (Lithuania),
Faculty of Fundamental Sciences,
Department of Information Systems;
 <https://orcid.org/0000-0003-2408-5371>,
e-mail: inga.tumasoniene@vilniustech.lt

LEGAL SUPPORT FOR INFORMATION SECURITY OF LEGAL ENTITIES UNDER LITHUANIAN AND UKRAINIAN LEGISLATION

In the rapidly evolving digital landscape, the safeguarding of information security for legal entities has emerged as a critical concern. This article investigates and compares the legal frameworks governing information security for legal entities in Lithuania and Ukraine, addressing the pressing need to understand and enhance legal support in this field. The relevance of this research stems from the escalating challenges posed by cyber threats, necessitating a robust legal infrastructure to fortify information security. The study delves into the fundamental elements of information security as mandated by Lithuanian and Ukrainian laws. It analyses the legislative provisions, compliance requirements, and institutional mechanisms established in both jurisdictions to protect sensitive data and mitigate cyber risks faced by legal entities. A comparative analysis is conducted to elucidate the similarities, disparities, and effectiveness of the respective legal frameworks.

This research employs a multifaceted methodology and scientific methods to achieve comprehensive insights. It involves an extensive review of existing legal texts and regulations pertinent to information security in Lithuania and Ukraine. Additionally, case studies and practical examples are utilized to contextualize the application and enforcement of these legal provisions. The results of this study highlight the strengths and shortcomings within the legal frameworks of both countries concerning information security for legal entities. By examining the practical implications and challenges faced by businesses in adhering to these laws, this research aims to provide valuable insights for Ukrainian and Lithuanian companies concerned with maintaining a high level of their information security.

In conclusion, this article underscores the critical importance of a robust legal framework in protecting the information security of legal entities. It offers a comparative analysis of Lithuanian and Ukrainian legislation, presenting valuable findings and recommendations to fortify and harmonize legal support for information security in both jurisdictions.

Key words: *information security, cybersecurity, legal entities, critical infrastructure, legal support, information protection measures.*

Original Article

INTRODUCTION. The development of the information society and processes of globalization undoubtedly form the basis for effective socio-economic progress. However, alongside this, the information systems of legal entities have become extremely vulnerable to the realization of cyber threats and attacks.

In contemporary circumstances, information security stands as one of the most critical compo-

nents of national security. An analysis of Ukrainian and Lithuanian legislation, scientific sources, jurisprudence, as well as judicial practices, provides grounds to assert that the current state of addressing the legal protection of the information security of legal entities indicates the necessity to develop new approaches to understanding this form of legal protection, particularly in the context of intensifying Euro-integration processes. In this

regard, it is crucial to conduct additional new research on the legal support of information security for legal entities in accordance with the legislation of Lithuania and Ukraine. This is because the information security of legal entities directly impacts the security of critical infrastructure, upon which, in turn, people's lives depend.

A high level of information security stands as one of the key prerequisites for the full-fledged functioning and operations of enterprises, institutions, and organizations. However, a low level of information security can inflict more damage than physical destruction, as evidenced by widespread hacker attacks on critical infrastructure objects in Ukraine. This research is particularly pertinent and essential in the face of a sharp increase in cyberattacks directed at Ukraine and the European Union (EU). Currently, active participation in the establishment of an effective "European cyber defence" and the efficient implementation of new European legislation in this field in Lithuania and Ukraine is exceedingly crucial. Therefore, the primary idea of this research lies in the development of new approaches and the enhancement of existing methods for legal protection the information security of legal entities in Ukraine, based on the experiences of successful countries worldwide, especially Lithuania.

PURPOSE AND OBJECTIVES OF THE RESEARCH. *The purpose* of the research is to elucidate the essence of the concept and fundamental elements of legal support for information security of legal entities in Ukraine and Lithuania.

Project objectives include: to investigate the prerequisites for ensuring this type of information security; to find out the place of information security of legal entities in the national security system; to investigate the regulatory foundations of the mechanism of information security of legal entities in Ukraine and Lithuania; to reveal the problems of legal provision of information security of legal entities in Ukraine and Lithuania and to determine possible ways to solve them.

METHODOLOGY. The methodological basis of this article is a set of philosophical, general scientific and special methods of scientific knowledge. Among the philosophical methods, the dialectical method was used. The problem of ensuring information security of legal entities is complex and multifaceted and, therefore, in its study it involves the use of the specified method, which is manifested in the study of legal essence and preconditions for ensuring information security of legal entities in Lithuania and Ukraine; when revealing the concept and structure of information security of legal entities as an object of legal protection,

and as a phenomenon that is connected with other phenomena of social life, permeates the sphere of informational, social and other types of social relations, and which undergoes constant changes, rapidly develops. Among the general methods of research, analysis was mainly used to reveal the essence and elements of legal protection of information security of legal entities as an intermediate result in the study of the general problem of such protection, which made it possible to single out a number of features and signs of this type of legal protection. Among the special methods, the comparative legal method was used, for comparing the legislation of Ukraine and Lithuania, in researched area.

RESULTS AND DISCUSSION

1. *The legal essence and preconditions for ensuring information security of legal entities in Lithuania and Ukraine*

Lithuanian legislation defines a legal entity as an enterprise, institution, or organization with its own name that can independently acquire rights and obligations, act as a plaintiff or defendant in court proceedings¹. Furthermore, when analysing the societal relations associated with the institute of legal entity, Lithuanian lawyers commonly refer to the terms "firm" or "enterprise", while economists and legal professionals use these terms interchangeably (Tikniūtė, 2008, p. 68). The Civil Code of Ukraine provides a nearly identical definition of a legal entity. In particular, according to Part 1 of Article 80 of this regulatory document, a legal entity is an organization created and registered in accordance with the law. Legal entities can be established in the form of associations, institutions, and other forms stipulated by law².

Simultaneously, to uncover the essence and prerequisites for ensuring the information security of legal entities, considering their diverse range, types, and ownership forms, the greatest scientific and applied interest will revolve around *the objects of critical infrastructure*. This is due to the fact that the security of critical infrastructure objects directly impacts the lives and health of humans, as well as the functioning of other associated institutions, organizations, and business processes.

¹ Seimas of the Republic of Lithuania. (2000). *Civil Code of the Republic of Lithuania* (Law No. VIII-1864). <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.245495>.

² Verkhovna Rada of Ukraine. (2003). *Civil Code of Ukraine* (Law No. 435-IV). <https://zakon.rada.gov.ua/laws/show/435-15>.

Overall, both in Lithuania¹ and in Ukraine², *critical infrastructure objects* are defined as infrastructure facilities, systems, their components, and their entirety, which are essential for the economy, national security, and defence. Disruption in the functioning of these objects can cause harm to vital national interests of a particular country. Objects of critical infrastructure are most frequently subjected to negative influences and attacks by malevolent actors. Threats to the information security of critical infrastructure objects emerged almost concurrently with the advent of the information environment. At first, the main threats to information security were considered to be malicious actions such as theft of information from computers, unauthorized use, and corruption of information on computers. Later, with the development of information and communication networks, information-communication and digital technologies, digitalization, and automation of business processes, information insecurity evolved into the means of disseminating unreliable information through networks and viruses. Currently, security concerns apply to almost all entities within the global digital environment, including individual enterprise (Kachan, 2017).

Considering that information is generated in all spheres of activity and ensures the execution of various functions and tasks faced by different entities, primarily legal entities, it is essential to define the concept and content of information security as an activity aimed at creating conditions for development. There are various approaches to defining the concept of “information security”. Let’s highlight two approaches that, in our opinion, are the main ones. *The first approach* is the study of the regulatory-legal group (based on the analysis of regulatory acts), and *the second approach* is the analysis of the doctrinal group (based on the analysis of the definition of the concept in the works of scholars and researchers).

Within the *regulatory-legal group*, it is crucial to mention the Constitutions of Ukraine and the Republic of Lithuania. According to Article 17 of the Constitution of Ukraine, the protection of sov-

ereignty and territorial integrity of Ukraine, ensuring its economic and information security, are the most important functions of the state, representing the cause of the entire Ukrainian people³. In turn, in accordance with Article 135 of the Constitution of the Republic of Lithuania, the Republic of Lithuania is guided by universally recognized principles and norms of international law, striving to ensure the security and independence of the country.

By the Law of Ukraine “On the Basic Principles for the Development of an Information-Oriented Society in Ukraine for 2007–2015”, an attempt was made to delineate the concept of “information security”. According to paragraph 13 of this Law of Ukraine, “*information security*” is defined as the state of safeguarding vital interests of individuals, society, and the state, preventing harm caused by: incompleteness, untimeliness, and unreliability of the used information; negative informational influence; adverse consequences of information technology applications; unauthorized dissemination, use, and breach of the integrity, confidentiality, and availability of information⁴.

By extrapolating the aforementioned concept of «information security» onto critical infrastructure objects, the Law of Ukraine “On Critical Infrastructure” defines the *security of critical infrastructure* as the state of protection where the functionality, continuity of operation, recoverability, integrity, and resilience of critical infrastructure are ensured. Therefore, the security of critical infrastructure encompasses both physical protection of the respective object and protection against informational and cyber threats.

Similar approach is employed by the Lithuanian legislature in the Article 1 of The Law of Lithuania on the Protection of Objects of Importance to Ensuring National Security. This document defines objects that are significant for ensuring the national security of the state (enterprises, objects, property, and sectors of the economy), as well as property and territories within the protected zones of enterprises, objects, and property deemed essential for ensuring national security. These are safeguarded from all risk factors that could pose a

¹ The Methodology of identifying the information infrastructure of special importance adopted by the Resolution of the Lithuanian Government on the implementation of the cyber security law adopted on 13 August 2018, No. 818, which was later amended on 5 December 2018 by Government Resolution No. 1209.

² Verkhovna Rada of Ukraine. (2021). *On Critical Infrastructure* (Law No. 1882-IX). <https://zakon.rada.gov.ua/laws/show/1882-20>.

³ Verkhovna Rada of Ukraine. (1996). *Constitution of Ukraine* (Law No. 254к/96-ВР). <https://zakon.rada.gov.ua/laws/show/254к/96-вр>.

⁴ Verkhovna Rada of Ukraine. (2007). *On the Basic Principles for the Development of an Information-Oriented Society in Ukraine for 2007–2015* (Law No. 537-V). <https://zakon.rada.gov.ua/laws/show/537-16>.

threat to the interests of national security and eliminate the causes and conditions for the emergence of such factors¹.

Regarding the *doctrinal group*, it's worth noting that there is currently no single definition of "information security", making it a subject of debate within scholarly circles. In the scientific works of O. Dovgan, T. Tkachuk (2018, pp. 90–91), *information security* is considered as the protection of an object from information threats or negative influences associated with information and the non-disclosure of data about a particular object, which is classified as state secret. Scientists defines *information security* also as legal protection of the societal information environment. This ensures its formation and development in the interest of organizations and the state overall.

Therefore, it can be concluded that information security is:

- a complex, dynamic, integral system, with components that include smaller security subsystems (levels) for the security of individuals (persons, legal);
- the state of not only technological but also legal protection of the information environment;
- the result of managing real and/or potential threats (risks) in the information sphere.

Analysing the information security of critical infrastructure objects, it should be noted that among the most prevalent definitions of the concept of "enterprise information security" are the following:

- It refers to societal relations aimed at establishing and maintaining, at an appropriate (desired) level, the functioning of the respective information system, including that of an enterprise.
- It involves the correlation between the level of information protection and the level of information threats, along with the aggregate of measures and actions undertaken by authorized individuals directed at protecting information resources and the digital infrastructure of an enterprise (Abakumov, 2012, p. 13).

In our opinion, information security, like any form of security, encompasses both a static aspect and a dynamic one. Information security primarily constitutes a process rather than merely a result. Therefore, it should be defined as a set of

organizational, legal, and technical measures aimed at the continuous operation of the digital space, minimizing risks in its functioning to an acceptable minimum, with the purpose of protecting information resources. From the above, it follows that "information security of critical infrastructure objects" is an important component of information security, expressed in a combination of practical measures to ensure the protection and defence of the information system of such critical infrastructure objects. Also, it is worth noting that the information security of legal entities – critical infrastructure objects holds an extremely important position within the national security system and constitutes an integral part of it.

1.1. The structure of information security for critical infrastructure objects

The practice of information relations among legal entities (critical infrastructure objects) and the role of information in such activities allow for identifying the following main components, forming the *structure of information security for critical infrastructure objects*:

- Cybersecurity (computer and network security);
- Information-psychological security;
- Communication (corporate) security.

Lithuanian organizations indicate that cyberattacks are becoming increasingly dangerous, complex, and have a greater negative impact (Andrukaitytė, 2022).

Cybersecurity defence consists of computer security and network security. Computer security encompasses all issues related to safeguarding data stored and processed by a computer, considered as an autonomous system. These issues are addressed through operating system tools and programs, such as databases, as well as embedded hardware components of the computer. Network security pertains to all matters associated with device interaction within a network, primarily focusing on protecting data during transmission over communication lines and guarding against unauthorized remote network access.

Information-psychological security as a component of critical infrastructure object information security directly depends on the human factor. Accordingly, the means of ensuring information-psychological security of critical infrastructure objects can encompass: establishing staff work rules regarding cybersecurity, such as document handling policies (mandatory data backups and retention); guidelines for interacting with managers and corporate mail (software requirements, spam management); password

¹ Seimas of the Republic of Lithuania. (2002). *On the Protection of Objects of Importance to Ensuring National Security* (Law No. IX-1132). <https://investmentpolicy.unctad.org/investment-laws/laws/246/lithuania-law-on-the-protection-of-objects-of-importance-to-ensuring-national-security->.

requirements for segregating access rights to information and premises, continuous employee training, etc.

And finally, *communication (corporate) security of critical infrastructure objects* encompasses ensuring the protection of important information during interactions with other entities (via email, messengers, mobile communication) and properly structured business communication.

1.2. Sources of threats, main objectives, and principles of information security for a critical infrastructure object

In both Lithuania and Ukraine, the primary source of threats to the information security of critical infrastructure objects is *incidents related to the security of critical infrastructure*. An incident related to the security of critical infrastructure refers to an event or a series of adverse events of non-deliberate nature (natural, technical, technological, erroneous, including those caused by human factors), and/or those displaying signs of unauthorized interference in the functioning of critical infrastructure objects, posing a threat to their security, the system managing the technological processes of critical infrastructure objects, creating a likelihood of disrupting the normal operating mode of such objects (including disruption and/or blocking of operations, and/or unauthorized management of their resources), thereby jeopardizing their integrity¹. Among the main threats and risks to Lithuania's national security, the National Security Strategy of Lithuania identifies cyber risks², as well as cyber incidents (Tvaronavičienė, Plėta, Casa, 2021).

Considering the above, we can identify the following *main types of threats*:

- *Human factor (anthropogenic)*, encompassing: errors (intentional or unintentional) by employees; unlawful actions of criminals (grey and black hat hackers) and criminal organizations, state-sponsored terrorism; dishonest actions by competitors;

- *Technical and technological*, such as malicious software, viruses, substandard technical

means of information processing, technological factors, and so forth.

Overall, when defining the main goal of information security for a critical infrastructure object, it is essential to consider that it involves minimizing the possibility of losing the information resource of the critical infrastructure object or compromising the confidentiality, availability, and integrity of the respective information system. *Confidentiality* ensures that confidential data will only be accessible to those users who have been granted permission to access it (such users are referred to as authorized users). *Availability* ensures that authorized users will always receive access to the data. In turn, *integrity* refers to ensuring that data maintains accurate values, which is ensured by prohibiting unauthorized users from changing, modifying, destroying, or creating data in any way³.

One of the *purposes of information security* for critical infrastructure objects can be defined as the reduction of risks that may cause damage to the legal entity's reputation, as well as the creation of conditions for its effective operation. It is worth noting that the information security system of a critical infrastructure object should be reliable and efficient.

Generally, *reliability and efficiency* are determined by their compliance with established requirements (principles), *which include*:

- *Continuity of information security provision* – measures of information security are initiated upon its organization and are sustained throughout the entire existence of the critical infrastructure object, strengthening or loosening in specific situations, but never ceasing. Continuity arises from the impossibility of completely satisfying information security, as threats constantly persist in our lives.

- *Planned nature of information security* – establishing an appropriate sequence for implementing information security measures that would ensure a preventive nature in their impact on the emergence of hazards and threats.

- *Specificity of information security* – security measures must encompass specific objects and

¹ Verkhovna Rada of Ukraine. (2021). *On Critical Infrastructure* (Law No. 1882-IX). <https://zakon.rada.gov.ua/laws/show/1882-20>.

² Seimas of the Republic of Lithuania. (2021). *Resolution Amending Resolution No IX-907 of the Seimas of the Republic of Lithuania of 28 May 2002 on the Approval of the National Security Strategy* (Resolution No. XIV-795). <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3ec6a2027a9a11ecb2fe9975f8a9e52e?jfwid=rivwzvpvg>.

³ Ministry of Economy of the Republic of Lithuania. (2004). *Order of Concerning approval of information security requirements of enterprises and equipment of strategic significance for national security under the management of the Ministry of economy of Lithuania and other enterprises important for ensuring national security* (Order No. 4-349). <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.242169?jfwid=32wf8izs>.

actions of subjects of the critical infrastructure object; security measures should be associated with specific operations, agreements, relationships executed within a specific period.

– *Complexity of information security* – entails the necessity of applying various forms, methods, means, and measures in ensuring security for different types of information and information-related relationships.

The information security of a legal entity should be carried out along these *lines*: *Legal Direction*: this involves the development of effective state policies in ensuring information security for enterprises. *Organizational Direction*: this includes ensuring the preservation of a company's confidential information through the establishment of a corporate protection system. *Program-Technical Direction*: this involves the use of certified legal software and hardware tools. Undoubtedly, the *proper organization* forms the foundation of an effective information security system for critical infrastructure objects. Unfortunately, it must be acknowledged that in Ukraine, organization currently stands as one of the weakest aspects in ensuring the information security of critical infrastructure objects. An analysis of the practices concerning information security in critical infrastructure objects demonstrates that insufficient importance is given to the issue of its organization. In most cases, the leaders of security departments handle these matters at an almost primitive level¹.

Lithuanian security experts emphasize another crucial aspect in ensuring information security – *the financial aspect*. As noted by R. Žvirblis (2021), there is a need for physical, electronic, and engineering security systems, alongside adequate funding and the capability to develop and maintain a reliable information security system. The main obstacles for the field include challenges in the cyber capabilities of the Russian Federation (Fedorov, 2023).

2. The legal framework for ensuring information security of legal entities in Ukraine and Lithuania

The legal framework for ensuring information security of critical infrastructure objects in Lithuania and Ukraine requires examination. In the context of European integration processes, on

the eve of Ukraine's accession negotiations with the EU, studying the fundamental principles of legal norms' development in Lithuania in this sphere, as an EU member having achieved significant success in establishing a robust information security system, is exceptionally crucial for Ukraine. A comparative analysis of the normative foundations of the mechanism of information security for legal entities in Lithuania and Ukraine allows identifying both commonalities and distinctions. The legal regulation system for information security of critical infrastructure objects in both Lithuania and Ukraine encompasses a vast array of legal norms governing relationships in this sphere, legal relations arising from the application of legal norms, and relevant judicial acts. The *framework encompasses* international treaties (international law), national laws, and regulatory acts of state authorities regulating relationships in this sphere².

Let's outline *the structure of the primary legal acts* of both states aimed at ensuring the information security of critical infrastructure objects and conduct a comparative analysis (table 1).

In summary, the *regulatory framework governing the identification and protection of critical infrastructure in Lithuania can be divided into two subsystems* (Andžāns et al., 2021). *The first subsystem* entails defining and establishing the methodology for identifying critical infrastructure, focusing on critical information infrastructure and cyber security in particular. *The second subsystem* is based on the concept of national security and assesses the activities of enterprises, their facilities, and assets, especially concerning investments, transfers, and other operations, in terms of their importance to the country's national security. These two subsystems intersect but only partially and are based on different sets of criteria.

On the other hand, legislation in Ukraine concerning this area is quite systematic and extensive (as indicated in the table). However, it is still in the process of formation and requires harmonization with EU legislation. Active implementation of EU legislation regarding European critical infrastructure could expedite the convergence of approaches between both countries – Ukraine and Lithuania.

¹ 19th Cluster Session: "Cybersecurity in Healthcare and Medicine: Key Challenges and Threats". May 23, 2023. URL: <https://cybersecuritycluster.org.ua/en/events/19th-cluster-session-harmonization-of-critical-infrastructure-cybersecurity-systems-to-the-eu-standards/>.

² Legal System in Lithuania. <https://www.baltic-legal.com/legal-system-of-lithuania-eng.htm#:~:text=Lithuania%20has%20a%20Roman%20legal,laws%20adopted%20by%20the%20Parliament.>

Table 1

The structure of the primary legal acts of both states aimed at ensuring the information security of critical infrastructure objects

Title of a structural element of legal acts	Lithuania	Ukraine
International legislation (Latest legal acts of the EU)		
1. <i>The Digital Services Act (DSA) (2022)</i> establishes rules that apply to four main categories of participants in the online space: companies providing intermediary online services, companies offering hosting services, online platforms, and very large or super large online platforms ¹	Considering that Lithuania is a full member of the European Union, the implementation of the approaches laid out in this EU act into Lithuania's national legislation will require competent authorities to develop new proposals for further reforming the critical (information) infrastructure protection system	Ukraine aspires to become a full member of the European Union. Even at this stage, when Ukraine has obtained the status of a candidate country for EU membership, this necessitates the implementation of EU law approaches into Ukrainian national legislation, incorporating the corresponding standards in this field. Hence, Ukraine's integration into the EU Single Digital Market is impossible without adapting its national legislation to EU standards
2. <i>Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (2022)</i> ²	Considering that Lithuania is a member of the EU, the rules defined in this Directive automatically apply to it	In light of Ukraine's integration into the EU and considering the new requirements and regulatory mechanisms in this field, it is important for Ukraine to take these into account. Some provisions of the new EU Directive are identical to the norms of the Law of Ukraine "On Critical Infrastructure"
3. <i>Directive of the European Union on Network and Information Security (NIS) (2016/1148); NIS 2 Directive (2020)</i>	A similar approach is observed regarding the application of the provisions of these regulatory documents	
4. <i>EU Cyber Solidarity Act (2023)</i> The EU Cyber Solidarity Act aims to strengthen capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks. The proposal includes a European Cybersecurity Shield, made of Security Operation Centres interconnected across the EU, and a comprehensive Cybersecurity Emergency Mecha-	The Act entails the creation of two operational instruments. <i>The first</i> one is a network of operational security centres equipped with modern technologies and artificial intelligence, serving as a platform, the "European Cyber Shield", enabling timely detection and response to cyber threats. <i>The second element</i> involves establishing a dedicated cybersecurity reserve in collaboration with	It is worth noting that some of the expertise for the development of the aforementioned act was borrowed from Ukraine's practical experience, as cyber reserves have repeatedly proven their effectiveness

¹ Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

² Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

nism to improve the EU's cyber posture ¹	trusted private providers who would intervene upon request from member countries in case of large-scale cyber-attacks	
<i>Constitutional legislation</i>	The fundamentals of ensuring information security for legal entities are enshrined in Article 135 of the Constitution of the Republic of Lithuania and Article 17 of the Constitution of Ukraine, respectively	
<i>Laws are codified regulatory acts that include norms regarding information security</i>	<p><i>In Lithuania, these documents include:</i></p> <ul style="list-style-type: none"> – Resolution Amending Resolution No IX-907 of the Seimas of the Republic of Lithuania of 28 May 2002 on the Approval of the National Security Strategy. 16 December. 2021. No XIV-795. Vilnius. This document discloses vital national security interests, primary risk factors, dangers, and threats to these interests, establishes priorities, long-term and medium-term development tasks for the national security system, external, defence, and internal policies; – Resolution on the Approval of the National Cyber Security Strategy. 13 August. 2018. No. 818. Vilnius. 	<p><i>In Ukraine, this refers to:</i></p> <ul style="list-style-type: none"> – Decree of the President of Ukraine of September 14, 2020 No. 392/2020 “On the decision of the National Security and Defence Council of Ukraine of September 14, 2020 “On the National Security Strategy of Ukraine”²; – On the decision of the National Security and Defence Council of Ukraine dated October 15, 2021 “On Information Security Strategy”: Decree of the President of Ukraine of 2021, December 28, No. 685/2021; – On the decision of the National Security and Defence Council of Ukraine dated May 14, 2021 “On the Cyber Security Strategy of Ukraine”: Decree of the President of Ukraine of 2021, August 26, No. 447/2021
<i>Special laws in the field of information security</i>	<p><i>This includes:</i></p> <ul style="list-style-type: none"> – The Law on the Basics of National Security. December 19. 1996. No. VIII-49. Vilnius; – The Cyber Security Law of the Republic of Lithuania No. 818, adopted on 13 August 2018; – the consolidated package of legal norms, which includes the Methodology for the identification and protection of critical information infrastructure is provided by the Government resolution on the implementation of the Cyber Security Law of the Republic of Lithuania No. 818, adopted on 13 August 2018. 	<p><i>This includes:</i></p> <ul style="list-style-type: none"> – The Law of Ukraine of October 5, 2017 No. 2163-VIII “On the basic principles of ensuring cyber security of Ukraine”³; – The Law of Ukraine “On Protection of Information in Information and Communication Systems”; – General Requirements for Cybersecurity in Critical Infrastructure objects, dated June 19, 2019 No. 518⁴.

¹ European Commission. (2023). *EU Cyber Solidarity Act*. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>

² President of Ukraine. (2020). *On the Decision of the National Security and Defense Council of Ukraine of September 14, 2020 “On the National Security Strategy of Ukraine”* (Decree No. 392/2020). <https://www.president.gov.ua/documents/3922020-35037>.

³ Verkhovna Rada of Ukraine. (2017). *On the Basic Principles of Cybersecurity in Ukraine* (Law No. 2163-VIII). <https://zakon.rada.gov.ua/laws/show/2163-19/>

⁴ General Requirements for Cybersecurity in Critical Infrastructure objects, dated June 19, 2019 No. 518.

	<p>Additionally included in this package are: The Law No. XI-635 amending the Law on Civil Protection of the Republic of Lithuania, Resolution No. 717 of the Government of the Republic of Lithuania of 7 June 2010 approving the procedure for the recognition of establishments as establishments of National importance, and Government Resolution No. 943 of 17 August 2011 on the Procedure for the identification, designation and development of measures necessary to ensure the safety of European Critical Infrastructure; the Law on electronic communications (No. IX-2135), the Law on information society services (No. X-614) etc.</p> <p>Moreover, there exist more specific legal provisions that regulate individual sectors and issues related to the protection of critical information infrastructure</p>	
<p><i>Soft Law. International Standards</i></p>	<p><i>The main standards of Electrotechnical Commission (ISO/IEC) committee are:</i></p> <ul style="list-style-type: none"> - ISO/IEC 27000 series, which relate to information security management systems, their creation, evaluation, testing, modernization, etc.); - ISO/IEC 15408 (Common Criteria's) and 18045 Evaluation criteria for IT security (Information Technology Security Assessment Methodology); - ISO/IEC 20897 Security requirements and test methods for physically unclonable functions for generating non-stored security parameters; - a set of standards for the applicability of requirements and parameters of cybersecurity in production and their interrelation (Pleskach et al., 2020, p. 61). <p>ISO certification and other certification is also used in Lithuania, and aims to help organizations increase their sustainability and capitalization¹</p>	

3. Specific directions of legal provision for information security of legal entities in Lithuania and Ukraine, existing issues, and ways of resolving them

In Lithuania, according to the Government Resolution that outlines the Methodology for defining Critical Infrastructure, there are 14 sectors of critical infrastructure objects, each with a more detailed list of sub-sectors and services provided by organizations and companies.

Among these sectors are (Andžāns et al., 2021, p. 76):

- Energy sector (electric power, oil and its products).
- Transportation and postal sector.
- Financial sector.
- Health sector (healthcare infrastructure etc.).
- Drinking water supply, distribution, and management.
- Information technology and electronic communications.
- Environmental sector (monitoring air, water, and forests).

¹ ISO Certification in Lithuania. <https://factocert.com/lithuania/iso-certification-in-lithuania/>.

- *Civil protection sector* (emergency situations and services).
- *State defence sector*.
- *Food sector* (production, storage, and quality control).
- *Industrial sector*.
- *Foreign affairs and security policy sector*.
- *Public administration sector*.
- *Public safety and law enforcement sector* (public safety services, legal and criminal justice systems).

The current system for protecting critical infrastructure in Lithuania is based on the government's identification of specific sectors and services as critical infrastructure, followed by a particular sectoral ministry or other state institution responsible for overseeing the designated sector. The mentioned resolution separately regulates issues of information security for critical infrastructure objects, outlining organizational and technical cybersecurity requirements applied to cybersecurity subjects. This regulatory act serves as a basis for risk assessment, determining threat levels, and vulnerability of communication and information systems. It also outlines the respective responsibilities of operators of critical information infrastructure objects that manage state information resources, assigning responsibility to the National Cyber Security Centre for monitoring quality.

A global factor that could serve as a positive example for Ukraine is the consolidation of the critical information infrastructure protection system under the leadership of the Ministry of National Defence and the National Cyber Security Centre of Lithuania. As noted, this reform propelled Lithuania into the top ten leading countries in cybersecurity in less than five years. It also resulted in high scores in the Global Cybersecurity Index and fostered a positive stance among EU and NATO allies. Furthermore, it contributed to improving the state of critical information infrastructure protection in Lithuania¹.

However flawless the system of ensuring information security for critical infrastructure objects in Lithuania might be, it still has *a number of drawbacks* (Andžāns et al., 2021, p. 87):

- *Complexity of the legal norms system* and the overall system for protecting critical infrastructure, including issues related to ensuring the information security of critical infrastructure objects;

- *Tendency towards excessive regulation in the sphere and increased administrative pressure* (for instance, precedents of unjustified categorization of certain companies as vital or important for national security);

- *Absence of a properly functioning risk assessment system within governmental institutions*, which would enable a proper evaluation of the advantages and disadvantages of different methods for protecting critical infrastructure objects;

- *Insufficient awareness regarding information security among responsible individuals and the general population*;

- *Lack of clear requirements for suppliers considered reliable by Lithuania*, for instance, concerning the procurement of ICT systems.

Addressing the issue mentioned in the last point is extremely crucial, as demonstrated by the Ukrainian experience. Neglecting the reliability and safety concerns of ICT suppliers can have serious consequences not only for legal entities and individuals but also for national security as a whole. For instance, in 2023, Ukrainian journalists discovered that Russian intelligence services might have been receiving video feeds from surveillance cameras in Ukraine for years. Thousands of surveillance cameras in Ukraine were operating on the Russian software TRASSIR by the DSSL company. These cameras were purchased by ordinary citizens as well as businesses and state enterprises (Shapoval, 2023). The damage caused by the irresponsibility of entities entrusted with safeguarding information security is challenging to comprehend.

In Ukraine, there is currently a special law defining the legal and organizational principles of creating and operating the national critical infrastructure protection system known as the Law of Ukraine "On Critical Infrastructure". Part 4, Article 19 of this law provides a list of vital functions and/or services whose disruption leads to negative consequences for Ukraine's national security. These are considered top-priority targets for attacks by criminals, criminal organizations, and the aggressor country – the Russian Federation.

Among them, particularly include:

- *Governance and provision of essential public (administrative) services*;
- *Energy supply (including heat supply)*;
- *Water supply and sewage*;
- *Food supply*;
- *Healthcare*;
- *Pharmaceutical industry; production of vaccines, sustained operation of bio-laboratories*;
- *Information services*;
- *Electronic communications*;
- *Financial services*;
- *Transportation provision*;

¹ Lithuania ranks fourth in the Global Cybersecurity Index among European countries. <https://kam.lt/en/lithuania-ranks-fourth-in-the-global-cybersecurity-index-among-european-countries/>.

- *Defense, national security;*
- *Law and order, administration of justice, detention;*
- *Civil protection of the population and territories, rescue services;*
- *Space activity, space technologies, and services;*
- *Chemical industry;*
- *Research activity.*

In recent years, Ukraine has implemented numerous organizational, technical, and legal measures aimed at addressing information security issues in leading sectors of critical infrastructure. Specifically, a series of regulatory acts have been adopted to regulate this sphere, as mentioned earlier. Additionally, a significant step towards enhancing the information security system in key sectors of critical infrastructure was the establishment of the *National Cybersecurity Cluster*. This initiative aimed to strengthen the strategic potential of national cybersecurity, foster the development of a professional cyber community, and ensure a secure cyber environment in Ukraine¹.

The convening of subsequent sessions of the mentioned Cluster in 2023 helped identify a range of problematic issues related to ensuring information and cyber security in leading sectors of the region, particularly in *the energy sector, gas and oil extraction sector, regional enterprises, and the field of medicine*. Notably, experts in the energy sector highlighted that the issue of ensuring information security in this industry became critical due to the ongoing hybrid warfare, leading to a shift in the vector of cyber threats. In particular, it was identified *new cyber-attack trends* have been identified, including the dissemination of destructive components, disruption, and compromise of infrastructural elements within energy facilities.

In order to enhance the level of information security, specialists in the gas and oil extraction sector have established a specialized *Cybersecurity Center* with the following *key objectives*: improving the effectiveness and manageability of cybersecurity risk management processes; ensuring the integration of information systems for monitoring, analysis, and decision-making regarding information security incidents; ensuring business process continuity; proactive identification and prevention of cyber-attacks; responding to and combating incidents; incident investigation; multi-source obser-

vation capability; centralized analytics of diverse data for incident detection; timely response to incidents (rapid prevention and resolution of incidents). Additionally, *the Centre's operations involve the following stages*: monitoring, analysis, identification, response, recommendation formulation, and automatic or manual application of recommendations.

Addressing the issues of ensuring information and cyber security, regional enterprises, in addition to other measures, develop *their own security policies* within the framework of cyber defence, conduct training and cyber hygiene education for their personnel, and engage in external testing to identify vulnerabilities (20th Cluster Session).

Several challenges regarding the assurance of information security within critical infrastructure objects in Ukraine should be noted:

- *Tendency towards excessive regulation* in the field, intensification of administrative pressure;

- *Presence of norms within the sphere across legal acts of various legal force*. Significant aspects of this field are regulated by subordinate legal acts. An equally important problem for the effective provision of information security for legal entities is the inconsistency among regulatory legal norms, gaps in the law, and collisions between them;

- *Declarative nature of a significant number of legal norms* within information security legislation, lacking mechanisms for their implementation, resulting in a low level of enforcement in the field;

- *Insufficient coordination and harmonization of efforts* among responsible entities leading to functional duplications and the absence of a consolidated critical information infrastructure protection system under the guidance of a single state body;

- *Lack of knowledge sharing* for constructing a systematic information security provision process, shortage of qualified professionals, and inadequate remuneration levels for their work;

- *Insufficient funding for measures* related to ensuring information security for legal entities considered critical infrastructure objects.

4. Approaches to addressing problematic issues

When seeking solutions to the legal aspects of ensuring information security for legal entities in Lithuania and Ukraine, it is essential to remember that there is no singular, universally applicable solution that fits all without exception. This is due to the fact that each company or organization possesses different types of infrastructure, technical

¹ 20th Cluster Session: "Cybersecurity in Leading Industries of the Region". June 29, 2023. <https://cybersecuritycluster.org.ua/en/events/20th-cluster-session-regional-one/>.

aspects, and other diverse elements. But, it is important to note that having a basic model for ensuring information security of a critical infrastructure object is crucial. This model should encompass technical and organizational components (Levchuk, 2021):

- *Identification of vulnerable points.* Measures to ensure: compiling a list of all information resources that need to be protected;

- *Threat identification.* It is necessary to create a list of all possible (real and potential) threats to each individual information resource;

- *Assessment of threat level.* The construction of a scale of danger levels for each information resource must be carried out based on the potential consequences in the event of unauthorized access;

- *Access management control.* It is necessary to distribute the organizational structure of a legal entity – a critical infrastructure object into categories of access to protected information;

- *Counteraction.* This involves the development of measures aimed at preventing cases of unauthorized access to an information resource with an appropriate level of security;

- *Implementation.* Steps such as approval, implementation, and monitoring compliance with measures to organize information security for a legal entity – a critical infrastructure object are necessary;

- *Consequence mitigation.* This step involves developing rapid response measures to unauthorized interference (access) to protected information aimed at minimizing harm to the legal entity – a critical infrastructure object.

Regarding *the legislative activities* in ensuring information security for legal entities in Lithuania and Ukraine separately, it is worth noting that they should aim at legislatively establishing means of countering respective threats, as well as the means and methods of achieving them, ensuring adequate policies of state authorities. The activities of Ukraine and Lithuania on the international arena provide an opportunity to develop information security for legal entities by utilizing international norms.

Currently, one of the crucial directions in Ukraine's legal strategy for ensuring information security involves analysing and improving the regulatory framework in this field, particularly based on international standards, including EU legislation. An important act in this regard, mentioned earlier, is *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, 2022.*

This document includes the following provisions:

- Requirements for EU member states to adopt strategies to enhance the resilience of critical infrastructure operators providing essential services;

- Requirements for conducting risk analysis regarding the resilience of providing specified services at the national level and by critical infrastructure operators within all sectors and subsectors defined by the Directive;

- Obligations for critical infrastructure operators to implement resilience plans (including informational) composed of technical, security, and organizational measures according to identified threat levels and their impact.

Essentially, the aforementioned regulatory act provides an opportunity to conduct an impact assessment (or audit) of the actual state of critical infrastructure in both countries, including matters related to information security. This will allow an evaluation of the current system based on relevant criteria (risk assessment, effectiveness, efficiency, coherence, regulatory proportionality, and determinacy, etc.) and will be useful in terms of implementing corresponding legislation at the EU level in Lithuania and Ukraine, involving stakeholders.

In essence, harmonized cooperation, coordination, and a clear understanding of algorithms to counter cyber threats in different sectors form a reliable foundation for strengthening the national cyber and information security system.

CONCLUSIONS

1. As evidenced by this research, the legal framework regulating the information security of legal entities, particularly those constituting critical infrastructure, shares *numerous similarities between Lithuania and Ukraine:*

- national security strategies and cyber security policies establish fundamental directions for the national cyber security policies in both public and private sectors;

- both countries possess similar specialized legislation concerning issues of information and cyber security related to critical infrastructure entities;

- Ukraine and Lithuania legislatively identify analogous sources of threats to the information security of their critical infrastructure objects. For example, in Lithuania and Ukraine these threats encompass perceived external threats, initially originating from the authoritarian regime in Russia, and more recently in China.

2. At the same time, *certain differences* are observed, influenced by various factors:

– the necessity for *more active harmonization of Ukrainian legislation* with EU norms. This issue is less pressing for Lithuania;

– *the declarative nature of several provisions in Ukrainian specialized laws*, for example, the absence of published reports on the actual state of information and cyber security provision, the unavailability of such information, and the absence of accountability for not providing such reports are noticeable. In contrast to Ukraine, according to laws adopted in Lithuania, annual reports on the primary threats to national security are prepared and published in the first half of the year. Information security holds significant importance within these reports. The document is openly accessible for download and review¹;

– *institutional inconsistency, duplication of functions among bodies responsible for ensuring information security in Ukraine*, and the absence of a single authority overseeing this domain;

– without exaggeration, *Ukraine sets trends for allies, including Lithuania, in practical activities concerning the assurance of information security for critical infrastructure objects*. Ukrainian experience in combating threats is unique and worth

adopting. However, the difference lies in the fact that EU countries have more opportunities for financial involvement and greater political will to scale up Ukrainian expertise.

3. *Additionally, it is beneficial for both countries to:*

– facilitate active exchange of knowledge and experience in dealing with incidents related to information and cyber security threats, contributing to the establishment of a systematic process for ensuring the information security of legal entities within their respective countries;

– increase funding and engage in more active investment in measures to secure the information of legal entities considered critical infrastructure;

– enhance legislation in this field;

– implement control and oversight to ensure compliance with the current legislation on information security;

– develop and improve the system of scientific, methodological, material-technical, and personnel support for information security, both at the state level and within individual enterprises. Additionally, promote increased awareness and literacy among all stakeholders in this sphere.

REFERENCES

1. Abakumov, V. M. (2012). Information security of entrepreneurship as an object of administrative and legal protection. *Forum of Law*, 4, 10–16. http://nbuv.gov.ua/j-pdf/FP_index.htm_2012_4_3.pdf.
2. Andrukaitytė, M. (2022, May 19). *The number of cyber-attacks last year remained similar, but they were more dangerous*. JP.it. <https://jp.lt/kibernetiniu-ataku-skaicius-pernai-isliko-panasus-bet-jos-buvo-pavojingesnes/>.
3. Andžāns, M., Spruds, A., Sverdrup, U. et al. (2021). *Critical infrastructure in the Baltic states and Norway: strategies and practices of protection and communication*. Latvian Institute of International Affairs.
4. Dovgan, O., & Tkachuk, T. (2018). Information Security system of Ukraine: ontological dimensions. *Information and Law*, 1(24), 89–103.
5. Fedorov, M. (2023, April 4). *We are developing a digital state: join the discussion of the Strategy for the Development of the Innovation Ecosystem in Ukraine*. Ministry of Digital Transformation of Ukraine. <https://thedigital.gov.ua/news/rozvivaemo-tsfrovu-derzhavu-doluchaytesya-do-obgovorennya-strategii-rozvitku-ekosistemi-innovatsiy-v-ukraini>.
6. Kachan, O. (2017, April 2017). *Information security of the enterprise in the conditions of globalization* [Conference presentation abstract]. All-Ukrainian Economic Forum with international participation “Development of small and medium-sized businesses in the conditions of globalization of the world economy”, Zhytomyr, Ukraine.
7. Levchuk, V. (2021). *Information security of the enterprise*. SPAR. <https://spar.ua/blogs/informatsiyna-bezpeka-pidpriemstva>.
8. Pleskach, M., Pleskach, V., Semenchenko, A., Myalkovsky, D., & Stanislavsky, T. (2020). Standardization in the Field of Cybersecurity and Cyber Protection in Ukraine. *Information & Security*, 45, 57–76. <https://doi.org/10.11610/isij.4504>.
9. Shapoval, K. (2023). *Russia could receive videos from surveillance cameras in Ukraine for years*. CHAS.NEWS. <https://chas.news/news/rosiya-mogla-rokami-otrimuvati-video-z-kamer-sposterezhennya-v-ukraini-shemi>.
10. Tikniūtė, A. (2008). Doctrine of legal person: modern trends. *Jurisprudencija*, 2(104), 64–72.
11. Tvaronavičienė, M., Plėta, T., & Casa, S. (2021, May 13–14). *Cyber security management model for critical infrastructure protection* [Conference presentation abstract]. International Scientific Conference

¹ State Security Department of the Republic of Lithuania. (2019). *National threat assessment*. <https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-EN.pdf>.

“Contemporary issues in business, management and economics engineering”, Vilnius, Lithuania. <https://doi.org/10.3846/cibmee.2021.611>.

12. Žvirblis, R. (2021, April 6). *What is enterprise security?* LinkedIn. <https://www.linkedin.com/pulse/kas-yra-%C4%AFmon%C4%97s-saugumas-romualdas-%C5%BEvirblis>.

Received the editorial office: 14 November 2023

Accepted for publication: 17 December 2023

МАРІЯ ПЛЕСКАЧ,

*доктор філософії у галузі права,
Вільнюський технічний університет ім. Гедимінаса (Литва),
факультет фундаментальних наук,
кафедра інформаційних систем;
ORCID: <https://orcid.org/0000-0003-3296-5475>,
e-mail: pleskachmarija@gmail.com;*

ІНГА ТУМАСОНІЄНЕ,

*доктор філософії у галузі технічних наук, професор,
Вільнюський технічний університет ім. Гедимінаса (Литва),
факультет фундаментальних наук,
кафедра інформаційних систем;
ORCID: <https://orcid.org/0000-0003-2408-5371>,
e-mail: inga.tumasoniene@vilniustech.lt*

ЮРИДИЧНИЙ СУПРОВІД ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЮРИДИЧНИХ ОСІБ ВІДПОВІДНО ДО ЗАКОНОДАВСТВА ЛИТВИ ТА УКРАЇНИ

У цифровому середовищі, що швидко розвивається, забезпечення інформаційної безпеки юридичних осіб стало критично важливим питанням. У статті досліджено та порівняно правові межі, що регулюють інформаційну безпеку юридичних осіб у Литві та Україні, звернено увагу на нагальну потребу в розумінні та вдосконаленні правової підтримки у цій сфері. Актуальність дослідження зумовлена викликами, пов'язаними з кіберзагрозами, які вимагають надійної правової інфраструктури для зміцнення інформаційної безпеки. Охарактеризовано фундаментальні елементи інформаційної безпеки, передбачені литовським та українським законодавством. Проаналізовано законодавчі положення, відповідність вимогам та інституційні механізми, створені в обох юрисдикціях для захисту конфіденційних даних і зниження кіберризиків, з якими стикаються юридичні особи. З метою з'ясування подібностей, відмінностей та ефективності відповідних правових меж проведено порівняльний аналіз.

У дослідженні використано комплексну методологію та наукові методи для досягнення всебічного розуміння. Це детальний огляд існуючих правових текстів і нормативно-правових актів, що стосуються інформаційної безпеки в Литві та Україні. Крім того, тематичні дослідження та практичні приклади використано для контекстуалізації застосування і забезпечення дотримання цих правових норм. У результаті дослідження висвітлено сильні та слабкі сторони законодавчої бази обох країн щодо інформаційної безпеки юридичних осіб. На основі вивчення практичних наслідків і викликів, з якими стикається бізнес при дотриманні законів, надано цінну інформацію для українських та литовських компаній, зацікавлених у підтримці високого рівня своєї інформаційної безпеки.

Наголошено на критичній важливості надійної правової бази для захисту інформаційної безпеки юридичних осіб. Запропоновано порівняльний аналіз литовського та українського законодавства, цінні висновки та рекомендації щодо зміцнення та гармонізації правової підтримки інформаційної безпеки в обох законодавчих системах.

Ключові слова: *інформаційна безпека, кібербезпека, юридичні особи, критична інфраструктура, правове забезпечення, заходи захисту інформації.*

Цитування (ДСТУ 8302:2015): Pleskach M., Tumasoniene I. Legal support for information security of legal entities under Lithuanian and Ukrainian legislation. *Law and Safety*. 2023. No. 4 (91). Pp. 161–174. DOI: <https://doi.org/10.32631/pb.2023.4.14>.

Citation (APA): Pleskach, M., & Tumasoniene, I. (2023). Legal support for information security of legal entities under Lithuanian and Ukrainian legislation. *Law and Safety*, 4(91), 161–174. <https://doi.org/10.32631/pb.2023.4.14>.