UDC 342.7:347.121.2:004
DOI: 10.56215/naia-herald/1.2023.44

Social-legal foundations of information security of the state, society and individual in Ukraine

Iryna Sopilko*
Doctor of Law, Professor
Donetsk State University of Internal Affairs
25000, 1 Velika Perspektivna Str., Kropivnytskyi, Ukraine
https://orcid.org/0000-0002-9594-9280

Lesya Rapatska
PhD in Law
National Academy of Internal Affairs
03035, 1 Solomyanska Sq., Kyiv, Ukraine
https://orcid.org/0009-0001-8904-9083

■ **Abstract**. Ukraine is experiencing military aggression due to the full-scale invasion of Russia, which uses information weapons. Therefore, the problem of ensuring a sufficiently high level of information security in Ukraine is relevant. The purpose of the research – to highlight the essence and features of the concept of "information security", and related terms, and to perform a comprehensive analysis of the current regulatory framework on ensuring a reliable level of information security as the basis of national security. To achieve this purpose, the author uses empirical, theoretical and comprehensive methods of scientific research, namely: observation, comparison, abstraction, analysis and synthesis, and comparative-legal, Aristotelian, analogy and deduction methods. The author proves the significance of ensuring information security at the level of each entity as the foundation for the existence of the Ukrainian information society and a means of counteracting the aggressive actions of the Russian Federation. The factors influencing information security are identified, in the context of which the significant role of the culture of protection of society is demonstrated. The significance of ensuring an appropriate level of cybersecurity as a defining element of information defence, the provision of which should be as consistent as possible with the State information policy, is substantiated. The author outlines the potential consequences of failure to maintain a reliable level of information and cybersecurity against the background of a full-scale invasion, namely: the overthrow of the government, collapse of Ukraine's reputation in the international arena, chaotic processes in society and growing discontent, economic crisis and human casualties. The author describes the current state of information security in the country and suggests ways to improve it, in particular by reforming the existing legal regulation, considering the political experience of other countries and scientific achievements, transforming the State information policy with a focus on preventing information offences, international cooperation in the global information space and developing the information culture of the population. These recommendations can be used to eliminate shortcomings in the legal regulation of information security issues and to develop proposals for reforming the national information policy

■ **Keywords**: information; information space; cybersecurity; information warfare; cyber warfare

■ **Suggested Citation:**
Sopilko, I., & Rapatska, L. (2023). Social-legal foundations of information security of the state, society and individual in Ukraine. *Scientific Journal of the National Academy of Internal Affairs,* 28(1), 44-54. doi: 10.56215/naia-herald/1.2023.44.

■ *Corresponding author

■ Received: 18.12.2022; Revised: 28.02.2023; Accepted: 28.03.2023.

Introduction

Ukraine is an independent state, whose society is rightly called an information society, i.e. one that establishes, uses, and disseminates information. Thus, a massive Internet audience and a specific networked socio-cultural environment are being developed in Ukraine (Dubov *et al.*, 2010). Every day, almost every Ukrainian produces content, accumulates and processes various data, and establishes new information and a qualitatively new product – knowledge – from "raw" information. Such knowledge becomes a certain asset, as it can be transformed into a valuable resource that will contribute to Ukraine's economic development.

Modern Ukraine is suffering from a full-scale invasion by the Russian federation. The enemy began its actions back in 2014, initiating a hybrid war against Ukraine, in which it uses both permitted and prohibited means and techniques, including information warfare and cyber warfare technologies (Barna, 2019). Thus, the information security of independent Ukraine is under constant attack and therefore needs to ensure the necessary level of protection, which determines the relevance of the research. Thus, the relevance of this research is quite high, as its results and conclusions will help the Ukrainian authorities, legislators, individual organisations and individuals both to better perceive the risks of information security and to understand how to act to protect the state against a full-scale invasion by an aggressor country and to provide an objective justification for the costs.

Information warfare is a phenomenon that consists of methods and means of presenting information in such a way as to develop a public opinion in a specific social group that is favourable to the organisers of information propaganda. As a result, the victim of information influence should develop a different worldview on an issue than they had before, but necessarily favourable to the attacker; or the corresponding actions are taken to shake the existing opinion, provoke the victim to doubt, etc (Sopilko *et al.*, 2021). It is exactly what the Russian Federation (hereinafter – rf) has been doing for more than nine years to achieve its purposes. Thus, it is necessary to counteract the aggressor country both by military means and in the information environment. To do this, it is directly necessary to ensure an adequate level of protection of national information security, which is possible through the introduction of high-quality regulations.

The outlined issues are in great demand and have become the foundation of scientific research and the achievements of leading domestic and foreign scholars. In particular, P. Loft *et al.* (2022) highlight the importance of risk management and disclose the specifics of ensuring information security at the level of enterprises and institutions. The researchers emphasise the need to use "maturity models" and security standards in this regard. Such compliance strategies are an important requirement for the activities of many entities, but it is necessary to continue to search for better ways to appropriately protect information security. D.V. Dubov *et al.* (2010) define the information society as a humanitarian category characterised by qualitative transformations in society, shifting the main focus from production to non-production, changes like information flows, etc. In addition, these researchers include the information society itself and each person as an information subject. K. Yeganegi *et al.* (2020) explore using information technology and the role it plays in national security.

I.B. Koterlin (2022) analyses the impact of martial law on information security and the specifics of ensuring the rights and freedoms of citizens in these conditions. The legal and organisational aspects of combating destructive information influence in the state were explored by such scholars as R.F. Chernysh *et al.* (2022).

Despite the wide range of relevant studies, the essence and features of the concept of "information security" and other related terms require detailed analysis and elaboration.

The purpose of this research - to analyse the existing regulatory mechanisms and tools to ensure an adequate level of information security, which is an important element of national security. In addition, the research intends to provide qualitative proposals and recommendations in the context of overcoming the existing shortcomings and gaps in legal regulation and in Ukrainian information policy in general.

Literature Review

As of 2023, the number of scientific studies in the field of information security is growing, considering the activity of the aggressor country, the rf, in the framework of the hybrid war against Ukraine and the full-scale invasion. Information security in the sociological context is qualitatively explored in the work of R.I. Prodanyuk (2018). In their research, Y. Yuyrinets & M. Belkin (2022) focus on this phenomenon in the context of an informational understanding of culture. Studies of this concept as a purpose of an enemy waging information warfare are essential (Sopilko *et al.*, 2021).

An analysis of the available source base demonstrates the existence of different approaches to understanding information security, but there are three that scholars tend to favour. The first is based on computerisation and its goal of protecting information (Loft *et al.*, 2022). The sociological approach is followed by R.I. Prodanyuk (2018), and the legal and political approach by A.V. Svintsytskyi *et al.* (2022),

& I.M. Sopilko *et al.* (2021). Proponents of the latter approach assume that information security is inextricably linked to national and information and psychological security.

R.M. Alguliyev *et al.* (2020), exploring information security as a mandatory component of national security, proceeds from the analysis of its concept of the Republic of Azerbaijan. Thus, in their understanding, the security environment is a set of factors that affect both the sovereignty of the state and the inviolability of its borders, territorial integrity, preservation and maintenance of the welfare of society, and national interests (compliance with which properly ensures the activity and development of the individual). Therewith, scientists emphasise the importance of maintaining an appropriate level of protection of the vital interests of a person, society and the state in general from internal and external challenges and threats.

The aforementioned researcher I.B. Koterlin (2022), in the process of analysing the new Information Security Strategy 2021, comes to the apt conclusion about a clear change of emphasis in identifying threats in the relevant field with the restriction of human and civil rights. Among the relevant restrictions in this aspect, he notes the basic constitutional information rights, the need for which is caused by the inability to provide full protection against enemy arbitrariness.

T. Sozanskyy *et al.* (2020) emphasise the need to ensure information and cybersecurity as an element of it through public-private partnerships. It can be achieved through the development of such a partnership in the development of legislation and industry standards in the relevant area, and comprehensive state support for research designed to protect against cyberattacks. In addition, it applies to the development and implementation of a programme approach to developing effective cooperation in the exchange of information on cyber risks and incidents between the government and commercial entities and the introduction of a mechanism for state support for innovation in the cyber sphere. National policy must be based on flexible operational cybersecurity strategies.

The analysis of the sources demonstrates that there is a significant amount of work on this issue. However, research in this area should not be completed or stopped, as the developments of academics are no less important than the existing legal and regulatory framework, as they can become the foundation for improving the latter.

■ Materials and Methods

To achieve the purpose of the research, both empirical and theoretical and complex methods were used. The first group, empirical methods, was used at the stage of collecting the necessary data. The method of analysis and synthesis helped to obtain generalised information to reflect the characteristics of the entirety of information security as a social and legal phenomenon and related categories and for qualitative research of the issues under consideration. In the process of applying the method of comparing different approaches to understanding this concept, the author managed to establish similarities and differences of the phenomena examined, and, therewith, identify what is common to all the objects under comparison and their specific properties. The author also investigates and defines the concept of information security as an integral element of the security of the state in general, and cybersecurity, without which it is difficult to imagine sufficient information security in the modern world. The general doctrinal definition of information security and the official regulatory definition were explored, thereby clearly developing an understanding of the tasks and methods of functioning information security as a systemic entity.

The method of abstraction helped to move away from the insignificant properties and connections of information security and related categories and, therewith, highlight the important things in them for further stages of the research.

Among the complex methods, the author uses the analysis by decomposing the subject of research into components. A comprehensive analysis of information security as the foundation of the national security of the Ukrainian State and its integral part - cybersecurity and some other elements – is performed. The application of the comparative-legal method helped to identify the problematic aspects of law enforcement in the area of information security examined and helped to compare the current regulations in the field of information security in Ukraine at a sufficient level. In addition, the author uses the method of analogy to substantiate the truth of judgments through arguments and arguments based on the research of legal doctrine in the information security field.

The development of the methodological framework of the research was facilitated by using the Aristotelian method and the method of deduction. In addition, grouping methods were used in the course of the research, and therefore several significant recommendations and proposals for improving the existing regulatory framework in the field of information security were developed.

■ Results and Discussion

Every social activity, especially those related to production and management, cannot do without information processing and, accordingly, is conditioned by the problem of information security. Understanding the essence of the latter is particularly important for this research. Every day, the world is changing, the level of multidimensionality of social practices is increasing, and their functioning is directly related to the growing intensity of information processes

in society and the acceleration of data ageing. It is the reason for the intensification of new risks and threats, and the entrenchment of existing ones. The security of individuals, social development, and even the state as a complete system is determined by the presence or absence of information and the increasing rate of its ageing. And it is the increase in the intensity of communications in society that is responsible for this. Thus, information contributes to the intellectualisation of society, and therefore information security has taken a strong position as a category that requires comprehensive protection. Consequently, ensuring a high-quality state of information security at the level of each entity is the way to the existence of an information society in the state.

Security, in general, and information security, in particular, is influenced by technical, social, political, legal and economic factors in their interaction. Therefore, it is the security culture of society that is of particular significance, as it is the only way for it to understand the nature of information threats. This culture is based on a foundation of communication and processes related to the immediate transfer of data.

Cyberspace is an integral structural element of the information environment. The importance of ensuring a sufficient level of cyber defence is that even the slightest defence will establish risks to information security. The appropriate provision of cyberspace defence must be fully consistent with the information security framework and national policy in this area.

As part of this aggressive act of Russia against Ukraine, the enemy resorts to means and methods of conducting both information and cyber warfare. Consequently, cyber and information security is the foundation for preserving and ensuring the national security of the state. Without them, the victim of aggression will face a complete overthrow of the government system, significant damage to its reputation as an international actor, public distrust of the authorities, collapse of the country's economy and, most importantly, human casualties.

Importantly, both the state and its representatives, and every citizen who uses information technology, must work to ensure information security. It means continuously improving the skills of perception and critical evaluation of information, identifying reliable sources and detecting bias. Developing the information culture of the population is one of the ways to protect against destructive information influence.

The priority task is to master information hygiene, namely responding to news and events with prudence and accuracy and complying with digital security rules. It will help society protect itself from manipulation and adverse effects. In addition, every business and institution should ensure data protection to achieve its purposes and preserve its resources, legal status and reputation. Joint efforts of the population and institutions will help to establish a sustainable and secure information environment for the country.

Informatisation is the foundation for both business and other issues and has generally affected everyday life. Informatisation can be defined as a specific process of increasing the efficiency of data and information used in society using modern information technologies. Therewith, it is the process of transforming a society into an information society, which is particularly characteristic of Ukraine (Judge *et al.*, 2021; Tan *et al.*, 2021).

The relevant processes of informatisation are both good and adverse phenomenon that affects the existence of both individuals and social groups and states as international subjects. This informational influence has become a tool in the hands of aggressive subjects, particularly in the international arena, which is the cause of information wars that the world is facing more and more frequently (Zharovska & Ortynska, 2020). It can be counteracted by ensuring a sufficient level of information security at the national level, which will be discussed below.

The research of problems and tasks in any sphere of relations is based on the consistent development of the basic terminology, identification of structural and operational links between its elements, and determination of the means of defining the categories examined for comprehensive research. Therefore, it seems important, first of all, to conduct a detailed consideration of the fundamental concepts of "danger" and "security" based on different approaches. Notably, information security is an integral part of the national security of the state as a separate sovereign entity, and therefore the categories of danger and security should be assessed in the context of the latter.

The scientist V. Zaplatynskyi (2012) considers the concept examined here as the probability of conditions under which a particular energy, information, resource, etc., individually or together, can have a special impact on the system, resulting in specific consequences. Such consequences are perceived as adverse by the relevant subject at the instinctive, sensory or cognitive level even before the hazard occurs or after its respective adverse effects manifest themselves.

Understanding the concept of insecurity leads to the meaning and understanding of security. The first use of this term dates back to 1190 when it was understood as a state of peace of mind when a person considers himself or herself protected from any danger (Alguliyev *et al.*, 2020). The Merriam-Webster Dictionary (2023) defines security as the absence of danger; freedom from fear or anxiety; measures to protect against espionage or sabotage, crime, etc.; and the state of being able to access what is needed to meet one's basic needs. Security issues and challenges are interdisciplinary. Security should be understood as a complex, multilevel phenomenon.

The previously mentioned notion of national security can be seen as the security and defence of a nation-state, including its citizens, economy and institutions, which is seen as the responsibility of the government. The term "national defence" is used as a synonym (Cai, 2021). Concerning legislation as a source of law, in the context of considering the concept of security, it is necessary to mention, first of all, the provision of paragraph 9 of Article 1 of the Law of Ukraine "On National Security of Ukraine", according to which national security means protection against real or possible threats and risks to democratic constitutional principles, state sovereignty, territorial integrity of the state, and other national interests of the country[1].

According to some scholars, the risk of a decline in the quality of life of citizens is a real threat to national security (Li & Liu, 2021). Thus, national security should not be defined, as it used to be, purely through military issues and internal and external borders. In this regard, note the classification, according to which national security consists of the following types of security: military, energy, environmental, socio-political, scientific and technical, and information, etc (Alguliyev *et al.*, 2020). Thus, military, economic, social and information security is the foundation for the existence of the overall security of the state.

In addition, the concept of information as the basis of all "information" categories should be considered. This term has long been perceived as related to the social and communication activities of social subjects. In the broadest sense, it is data that has been organised to draw special conclusions according to the tasks and requirements. Therewith, such information should be well structured and processed to ensure the reliability of the data obtained (Bansal, 2020). The terms "data", "message", and "knowledge" are closely related to information, although, according to the authors, there are differences between them. Thus, data is some material for processing and further interpretation, and the result of such processes is the emergence of information. In this research, information and data are used interchangeably.

The scientific community qualifies the concept of information security in different ways, mostly focusing on one aspect of this issue and choosing the technical and technological aspects of this concept. The authors are convinced that the real problem for Ukrainian society is to ensure the security of human consciousness as the least protected link in the social system. After all, information in the modern world is an important condition for the progressive development of humanity in general. Therewith, it can lead to adverse transformations. It is the consciousness of each individual that develops the consciousness of society, which in turn is the basis for ensuring the information security of the entire state.

Having examined the social component of information security, next, consider its essence in the legal aspect. The United States of America is a leading country in the field of information technology, and therefore, much attention is paid to information security. Under the influence of a wide range of legislative and other regulations governing access to information, transfer and processing of relevant data, a qualitative standardisation in this area has been implemented. The main standardisation body in this area is the NIST, i.e. the National Institute of Standards and Technology, which includes the Computer Security Centre, which is represented by specialists from federal services, representatives of the academic sector and the country's most famous IT companies. According to the third edition of the NIST Interagency Report (NISTIR) No. 7298, the concept of information security includes the protection of information systems and data from unauthorised access and unlawful use, alteration, deletion and similar actions to ensure the confidentiality, integrity and availability of these objects (Paulsen & Byers, 2019). Thus, information security is a specific practice of preventing unauthorised actions with data, and this practice is applied regardless of the form of the information itself, which can be both electronic (i.e. digital) and "physical".

As for the domestic legal regulation of the relevant sphere, the definition of information security is given in draft law No. 4949 of 28.05.2014, "On the Principles of Information Security of Ukraine". According to it, InfoSec is "a state of protection of vital interests of a person and citizen, society and the state, which prevents damage due to incompleteness, untimeliness and inaccuracy of disseminated information, violation of the integrity and availability of information, unauthorised circulation of restricted information, and adverse information and psychological impact and intentional causing of adverse effects of information technology"[2]. However, this draft law never became law.

As for the legal regulations enacted in the Ukrainian state, notably, first of all, the Law of Ukraine of 01.09.2007 No. 537-V "On the Basic Principles of Development of the Information Society in Ukraine for 2007-2015". According to clause 13 of Section III, information security plays an important role in the development of the information society in the

[1]Law of Ukraine No. 2469-VIII "On the National Security of Ukraine". (2018, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text.
[2]Law of Ukraine No. 4949 "On the Principles of Information Security of Ukraine". (2014, May). Retrieved from https://ips.ligazakon.net/document/JG3TH00A.

Ukrainian state, and such security is considered to be the state of protection of vital interests of the three main information subjects – a person as an individual, society and the entire state. It is in this state that the relevant subjects can be protected from harm that may be caused by incomplete, inaccurate information or its untimely provision, from other adverse information impact and undesirable consequences in connection with using information technology, and from unauthorised dissemination or use of data, and, therewith, violation of the so-called "information security triad" (Al Reshan, 2021), which is the integrity, confidentiality and availability of information[1].

In addition, in early 2017, according to Presidential Decree No. 47/2017, the decision of the National Security and Defence Council of Ukraine (hereinafter – NSDC) "On the Doctrine of Information Security of Ukraine" (29.12.2016) came into force[2]. Paragraph 1 of this document states that Russia, which is waging a hybrid war against Ukraine, uses the information sphere as the main arena for confrontation, which involves "the latest information technologies of influence on the minds of citizens designed to incite national and religious hatred, propaganda of aggressive war, change the constitutional order by force or violate the sovereignty and territorial integrity of Ukraine". The Doctrine of Information Security of Ukraine defines the national interests of Ukraine in the information sphere, identifies potential and real threats to the realisation of such interests, and defines the areas and tasks of national policy in this field. Its main purpose is to help counteract the above-mentioned information influence of the aggressive Russia in the context of the hybrid war that it has started.

The Doctrine does not offer a specific definition of information security. However, it is stated that the fundamental principles on which this legal regulation operates are "observance of human and civil rights and freedoms, respect for the dignity of the individual, protection of their legitimate interests, and the legitimate interests of society and the state, ensuring the sovereignty and territorial integrity of Ukraine". The above-mentioned national interests of the country in the information sphere, according to clause 3, include the development of the information society in Ukraine, primarily in terms of its technological infrastructure; protection of compatriots from the aggressive influence of hostile destructive propaganda; promotion of the development of information and communication technologies and information resources, etc[3]. This document expired on 28.12.2021 based on the NSDC decision of 15.10.2021 "On the Information Security Strategy" (according to Presidential Decree No. 685/2021)[4].

This law defines information security of Ukraine as an element of the national security of the Ukrainian state and the state of protection of the territorial integrity and democratic constitutional order, and with them – state sovereignty and vital interests of all information subjects – the state itself, its society and every individual citizen. It is in this state that the constitutional rights and freedoms of everyone to information – to use, accumulate, disseminate and access reliable and objective information – will be reliably ensured. Accordingly, an effective system of protection and counteraction to damage caused by adverse information influences, which may include destructive propaganda, etc will function properly[5].

The Strategy has received rather contradictory opinions. For example, I. Koterlin (2022), a researcher both of the legal regulations and the state of InfoSec in Ukraine in general, believes that the Strategy demonstrates a shift in emphasis from identifying threats and responding to them to narrowing human and civil rights, as there is a strong need to ensure the impact of threats, both existing and possible, in the context of a full-scale invasion. As for specific examples of restrictions on constitutional information rights, the scholar notes the following: the right to secrecy of correspondence, etc. (Article 31 of the Constitution); non-interference with privacy (Article 32); freedom of thought (Article 34); ownership and disposal of property (Article 41).

All relevant approaches to understanding InfoSec can be divided into three groups:

1) the approach from the standpoint of information and communication technologies, i.e., those related to computerisation. Its supporters perform a categorical analysis based on the identification of hazards in the technical sphere. Thus, for them,

[1]Verdict of the Leninsky District Court on Case No. 405/2078/23. (2023). Retrieved from https://reyestr.court.gov.ua/Review/110901228.
[2]Decree of the President of Ukraine No. 47/2017 "On the Decision of the National Security and Defense Council of Ukraine of December 29, 2016 "On the Information Security Doctrine of Ukraine", (2021, February). Retrieved from https://zakon.rada.gov.ua/laws/show/47/2017#Text.
[3]Decree of the President of Ukraine No. 47/2017 "On the Decision of the National Security and Defense Council of Ukraine of December 29, 2016 "On the Information Security Doctrine of Ukraine", (2021, February). Retrieved from https://zakon.rada.gov.ua/laws/show/47/2017#Text.
[4]Decree of the President of Ukraine No. 685/2021 "On the Decision of the National Security and Defense Council of Ukraine of October 15, 2021 "On Information Security Strategy". (2021, December). Retrieved from https://zakon.rada.gov.ua/laws/show/685/2021#Text.
[5]Decree of the President of Ukraine No. 685/2021 "On the Decision of the National Security and Defense Council of Ukraine of October 15, 2021 "On Information Security Strategy". (2021, December). Retrieved from https://zakon.rada.gov.ua/laws/show/685/2021#Text.

information security is the immediate protection of information and the relevant infrastructure from accidental or intentional actions that harm information consumers, its confidentiality, integrity and availability. Accordingly, for this approach, the main purpose of information security is to reduce the number of losses due to the above-mentioned adverse activities (Loft *et al.*, 2022);

2) sociological approach. The concept considered by the proponents of this approach is seen as a component of cultural and social security (Prodanyuk, 2018);

3) legal and legal-political understanding. In this case, information security is inextricably linked to national and state security, and information and psychological security. Representatives of this scientific thought understand the concept examined as a state of security of objects, which allows achieving proper functioning of the system regardless of internal or external information influences. This approach has a subdivision of information security depending on the subject of information interaction - an individual (person, personality), the state and society (social group) (Alguliyev *et al.*, 2020; Sopilko *et al.*, 2021; Svintsytskyi *et al.*, 2022).

Separately, in terms of information security, the significance of ensuring a decent level of cyber security (cybersecurity) should be noted. As mentioned above, most of the economic, commercial, cultural, social and governmental activities are conducted in cyberspace, where states at all levels and individuals, and governmental and non-governmental institutions, organisations and agencies interact (Aghajani & Ghadimi, 2018). Most of the resources of world powers go to support such a space, and accordingly, a significant part of people's income and wealth is either derived from it or has a huge impact on it (Amir & Givargis, 2020).

In general, cyberspace – a set of interconnected information systems and users who interact with such systems in a specific period (Ottis & Lorents, 2010). V. Filinovych (2022) defines cyberspace as a specific area in the information environment, the structure of which is composed of interdependent networks of information systems infrastructure, including computer systems, the World Wide Web, etc. Accordingly, cyberspace is an important structural element of the information environment. Different parts of the daily life of society members are intertwined with this space, and therefore, the slightest instability, insecurity and risks in this space will directly affect various aspects of citizens' lives (Li *et al.*, 2020).

The previous paragraph emphasises the significance of ensuring a robust level of cybersecurity. It is important due to the daily interaction with computers, gadgets and the Internet, and the possibility of cybercrime should not be ignored. Cybersecurity can be defined as the state of security in cyberspace and the ability to prevent cyberattacks in such space. Ensuring data security in cyberspace should be qualitatively aligned with the basics of information security of higher-level systems (Filinovych & Hu, 2021).

During the hybrid war waged by Russia against independent Ukraine, the enemy country resorts to both information warfare and cyber warfare. Thus, the information security of the state, and cyber security, is the foundation of the country's national security. The consequences of information and cyber warfare can include the complete overthrow of the government system, which will directly pose a catastrophic threat to national security, and the destruction or significant damage to the state's image in the international arena with a corresponding deterioration in the country's political and economic relations. Internal chaos will reign in the country, trust in the government will decline, the national economy will be damaged, and human casualties are possible (Khan *et al.*, 2020; Furnell & Shah, 2020) as the security of the population is fully dependent on a reliable level of national security (and its structural elements).

In addition, in the context of national security, notably, according to the Decree of the President of Ukraine No. 392/2020 of September 14, 2020, the National Security Strategy of Ukraine was introduced. In particular, among the priorities for ensuring the latter, the document declares the improvement of the national cybersecurity system as the foundation for effectively countering threats in the existing security environment. Among the internal policy areas, the legal regulations points to ensuring national interests and security in combination with obtaining complete, reliable, preventive information on the current situation in Ukraine and the world[1].

In addition, it is important to emphasise that information security, as the foundation of national security, is an element of international security. The development and promotion of interstate cooperation in the global information space are important both for the Ukrainian state and other countries, as this is the only way to identify potential threats to both information and cyberspace in a timely and high-quality manner. Thus, the authors agree with this recommendation and, comparing it with the results obtained, highlight the following key points.

D.V. Dubov *et al.* (2010) described the sensitivity of Ukrainians to the information society and the existence of a special networked socio-cultural

[1]Decree of the President of Ukraine No. 392/2020 "On the Decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine". (2020, September). Retrieved from https://www.president.gov.ua/documents/3922020-35037.

environment in Ukraine. It, accordingly, involves the constant processing of information that accompanies any social activity. Therefore, problems in the field of information security will pose problems in such an environment. Accordingly, the security of every citizen, social group and state, in general, depends on information provision and the rate of data obsolescence.

Thus, the opinion of P. Loft *et al.* (2022) on the significance of managing information security risks at the organisational level through using "maturity models" and security standards should be supported. Concerning understanding the essence of information security, the authors are most inclined to the legal and political approach proposed by A.V. Svintsytskyi *et al.* (2022), regarding its connection with national and information and psychological security. However, in conjunction with this approach, the authors support the approach of R.I. Prodanyuk (2018) to understand information security as a component of cultural and social security. Accordingly, the security culture of society, through which society understands the content of information threats, is a crucial factor in the development of high-quality information security. Nevertheless, it is influenced to varying degrees by technical, social, political and other factors. The authors of the research support the thesis of G. Aghajani & N. Ghadimi (2018) about the importance of ensuring an appropriate level of cybersecurity since most socio-economic and other activities are conducted in cyberspace. Thus, ensuring a sufficient level of both information and cybersecurity is important, especially in the context of Russia's war against Ukraine, as they are the foundation for ensuring national security.

State authorities dealing with information and cybersecurity should implement public-private partnerships as a tool for ensuring this and adapt the acquired knowledge to modern conditions, and establish mechanisms for cooperation and partnership in the relevant areas (Sozanskyy *et al.*, 2020).

To overcome security challenges, the relevant security services – police, military, etc. – must use modern devices to collect information. It includes the installation of high-quality video surveillance systems and timely communications that allow for the rapid exchange of data on threats and incidents (Yeganegi *et al.*, 2020).

Equally significant is cooperation both in the information and cyber spheres and in other legal areas, such as the exposure and punishment of criminals. In this context, active negotiations are underway to establish a special international tribunal for the war waged by Russia against independent Ukraine, which is possible through the involvement of the UN International Court of Justice (Lanza, 2022). It is reasonable to assert that Ukraine needs to demonstrate its national and political maturity to declare itself to the world, therefore, a constant and high-quality dialogue between political elites and civil society is a must (Kravchenko, 2022).

Thus, information security is protection against enemy interference, in particular against information weapons used by the aggressor country to kill Ukrainians and destroy Ukraine.

Conclusions

Ukraine needs to ensure an appropriate level of information security, as it faces constant challenges and threats of information warfare and information terrorism. Russia actively uses such methods and techniques, which pose a threat to the national security and stability of the country. Relevant authorities are developing and implementing effective legislation in the field of information and cyber security based on positive international experience. Therewith, it should be considered that information security should not be a one-time object of protection; its protection is a permanent process of continuous maintenance.

It is determined that one of the most vulnerable aspects of Ukraine's national security is information security and cybersecurity as its integral element. The research identifies the need to ensure an appropriate level of information security, since the intensity of information processes in Ukrainian society is constantly growing, which leads to rapid data obsolescence and an increase in risks, both new and existing. In addition, it is proved that information security is influenced both by political and legal factors and by technical, economic and other factors, which necessitates an appropriate level and culture of security in society as an entity that understands the content of information threats. Cybersecurity is an important element of information security, and therefore requires no less protection, especially in the context of a full-scale invasion, when the enemy actively uses information and cyber warfare.

It is substantiated that the current legal regulation of the relevant area requires a qualitative transformation, considering the experience of the leading countries of the world and the scientific developments of representatives of academic circles. The national policy in the information sphere should be reviewed and reformed to prevent further information offences. A particular role should be given to interstate cooperation in the global information space, which is beneficial both for Ukraine and other countries. Public-private partnerships should be developed, which is an effective tool for achieving this purpose.

It is promising to identify the best ways to develop a national system of legal regulation of information security, considering the experience of leading countries, and to define their comprehensive tools that could consider all risks in this area in advance, and potential opportunities for improvement in this area.

The scientific originality of this research lies in the presentation of the relevant results, including the established options for the development of a national system of legal regulation of information security based on the experience of the leading world powers, which will contribute to a better understanding of possible challenges and risks in the relevant area, and, accordingly, will provide opportunities for their qualitative and rapid overcoming.

Acknowledgements

None.

Conflict of Interest

None.

References

[1] Aghajani, G., & Ghadimi, N. (2018). Multi-objective energy management in a micro-grid. *Energy Reports*, 4, 218-225. doi: 10.1016/j.egyr.2017.10.002.

[2] Al Reshan, M.S. (2021). IoT-based application of information security triad. *International Journal of Interactive Mobile Technologies*, 15(24), 61-76. doi: 10.3991/ijim.v15i24.27333.

[3] Alguliyev, R.M., Imamverdiyev, Y.N., Mahmudov, R.S., & Aliguliyev, R.M. (2020). Information security as a national security component. *Information Security Journal: A Global Perspective*, 30(1), 1-18. doi: 10.1080/19393555.2020.1795323.

[4] Amir, M., & Givargis, T. (2020). Pareto optimal design space exploration of cyber-physical systems. *Internet of Things*, 12, article number 100308. doi: 10.1016/j.iot.2020.100308.

[5] Bansal, S. (2020). *What is the difference between data and information?* Retrieved from https://www.analytixlabs.co.in/blog/difference-between-data-and-information/.

[6] Barna, O.S. (2019). Information space of Ukraine as a factor of social consolidation in the conditions of hybrid war. *State and Law. Legal and Political Sciences,* 86, 365-376. doi: 10.33663/1563-3349-2019-86-365.

[7] Cai, T. (2021). The significance of STEM education for national security. In *Intelligence and Law Enforcement in the 21st Century* (pp. 188-204). Hershey: IGI Global. doi: 10.4018/978-1-7998-7904-6.ch010.

[8] Chernysh, R.F., Ihnatiuk, M.V., & Zaritskyi, O.Y. (2022). Counteracting destructive information influence in Ukraine: Legal and organizational aspects. *Juridical Scientific and Electronic Journal*, 1, 213-216. doi: 10.32782/2524-0374/2022-1/54.

[9] Dubov, D.V., Ozhevan, O.A., & Hnatiuk, S.L. (2010). *Information society in Ukraine: Global challenges and national opportunities*. Kyiv: NISD.

[10] Filinovych, V. (2022). The place of cyberspace in the information environment and legal support for their functioning. In *Human rights in the era of digital transformations* (pp. 106-109). Kyiv: National Aviation University.

[11] Filinovych, V., & Hu, Z. (2021). Aviation and the cybersecurity threats. In *Proceedings of the international conference on business, accounting, management, banking, economic security and legal regulation research (BAMBEL 2021)* (pp. 120-126). doi: 10.2991/aebmr.k.210826.021.

[12] Furnell, S., & Shah, J.N. (2020). Home working and cyber security – An outbreak of unpreparedness? *Computer Fraud & Security*, 8, 6-12. doi: 10.1016/s1361-3723(20)30084-1.

[13] Judge, M.A., Manzoor, A., Maple, C., Rodrigues, J.J.P.C., & Islam, S.U. (2021). Price-based demand response for household load management with interval uncertainty. *Energy Reports,* 7, 8493-8504. doi: 10.1016/j.egyr.2021.02.064.

[14] Khan, S.K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, 148, article number 105837. doi: 10.1016/j.aap.2020.105837.

[15] Koterlin, I.B. (2022). Information security in the conditions of martial law in the aspect of ensuring informational rights and freedoms. *Actual Problems of Domestic Jurisprudence*, 1, 150-155. doi: 10.32782/392257.

[16] Kravchenko, V. (2022). The Russian war against Ukraine: Cyclic history vs fatal geography. *Journal of Ukrainian Studies*, 9(1), 201-208. doi: 10.21226/ewjus711.

[17] Lanza, G. (2022). The fundamental role of international (criminal) law in the war in Ukraine. *Orbis*, 66(3), 424-435. doi: 10.1016/j.orbis.2022.05.010.

[18] Li, N., Tsigkanos, C., Jin, Z., Hu, Z., & Ghezzi, C. (2020). Early validation of cyber-physical space systems via multi-concerns integration. *Journal of Systems and Software*, 170, article number 110742. doi: 10.1016/j.jss.2020.110742.

[19] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186. doi: 10.1016/j.egyr.2021.08.126.

[20] Loft, P., He, Y., Yevseyeva, I., & Wagner, I. (2022). CAESAR8: An agile enterprise architecture approach to managing information security risks. *Computers & Security*, 112(C), article number 102877. doi: 10.1016/j.cose.2022.102877.
[21] Merriam-Webster dictionary. (2023). Retrieved from https://www.merriam-webster.com/dictionary/security.
[22] Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications. In *Proceedings of the 5th international conference on information warfare and security* (pp. 267-270). Dayton: Academic Publishing Limited.
[23] Paulsen, C., & Byers, R. (2019). *Glossary of key information security terms.* Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.IR.7298r3.
[24] Prodanyuk, R.I. (2018). Information security in a sociological context: Before the problem statement. *Scientific and Theoretical Almanac "Grania"*, 21(4), 84-90. doi: 10.15421/171861.
[25] Sopilko, I., Svintsytskyi, A., Krasovska, Y., Padalka, A., & Lyseiuk, A. (2021). Information wars as a threat to the information security of Ukraine. *Conflict Resolution Quarterly*, 39(3), 333-347. doi: 10.1002/crq.21331.
[26] Sozanskyy, T., Krasnytskyi, I., Lutsyk, V., Yaremko, G., & Tuz, N. (2020). International practice of legal support of cyber security of the country. *Journal of Legal, Ethical and Regulatory Issues*, 23(2), 1-8.
[27] Svintsytskyi, A.V., Semeniuk, O.H., Ufimtseva, O.S., Irkha, Y.B., & Suslin, S.V. (2022). Countering fake information as a guarantee of state information security. *Security Journal*, 1-16. doi: 10.1057/s41284-022-00347-0.
[28] Tan, S., Xie, P., Guerrero, J.M., Vasquez, J.C., Li, Y., & Guo, X. (2021). Attack detection design for dc microgrid using eigenvalue assignment approach. *Energy Reports*, 7(1), 469-476. doi: 10.1016/j.egyr.2021.01.045.
[29] Yeganegi, K., Arbabi, Z., & Hussein, I.A. (2020). The role of information technology in national security. *Journal of Physics: Conference Series*, 1530, article number 012112. doi: 10.1088/1742-6596/1530/1/012112.
[30] Yuyrinets, Y., & Belkin, M. (2022). Informational understanding of culture in the context of information security of Ukraine. In *V International youth scientific legal forum* (pp. 132-134). Ternopil: Vector. doi: 10.33270/02201901.96.
[31] Zaplatynskyi, V. (2012). The new concept of the most general term «danger». In *International scientific conference security, extremism, terrorism* (pp. 267-277). Bratislava: Institute of Fire Engineering and Expertise of the Ministry of Internal Affairs of the Slovak Republic.
[32] Zharovska, I., & Ortynska, N. (2020). The information war as a modern globalization phenomenon. *Bulletin of the Lviv Polytechnic National University. Series: "Legal Sciences"*, 7(26), 26-61. doi: 10.23939/law2020.26.056.

Соціально-правові основи інформаційної безпеки держави, суспільства й особи в Україні

Ірина Сопілко
Доктор юридичних наук, професор
Донецький державний університет внутрішніх справ
25000, вул. Велика Перспективна, 1, м. Кропивницький, Україна
https://orcid.org/0000-0002-9594-9280

Леся Рапацька
Кандидат юридичних наук
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0009-0001-8904-9083

■ **Анотація**. Україна зазнає військової агресії у зв'язку із повномасштабним вторгненням росії, яка використовує також інформаційну зброю. Тому актуальною є проблема забезпечення достатньо високого рівня інформаційної безпеки в Україні. Мета дослідження – висвітлити суть й особливості поняття «інформаційна безпека», пов'язаних із нею термінів, здійснити всебічний аналіз чинного нормативно-правового масиву з питань забезпечення надійного рівня інформаційної безпеки як основи національної безпеки. Задля досягнення поставленої мети використано емпіричні, теоретичні та комплексні методи наукового дослідження, а саме: спостереження, порівняння, абстрагування, аналізу та синтезу, а також порівняльно-правовий, формально-логічний, методи аналогії та дедукції. Доведено важливість забезпечення інформаційної безпеки на рівні кожного окремого суб'єкта як підґрунтя для існування українського інформаційного суспільства та засобу протидії агресивним діям Російської Федерації. Визначено чинники впливу на інформаційну безпеку, у контексті чого засвідчено значущу роль культури захисту суспільства. Обґрунтовано важливість забезпечення достатнього рівня кібербезпеки як визначального елемента інформаційної оборони, надання якого має бути максимально узгодженим із державною інформаційною політикою. Окреслено потенційні наслідки недотримання надійного рівня інформаційної та кібербезпеки на фоні повномасштабного вторгнення, а саме: повалення влади, крах репутації України на міжнародній арені, хаотичні процеси в суспільстві та зростання рівня його невдоволення, економічна криза та людські жертви. Схарактеризовано наявний стан забезпеченості інформаційної безпеки в країні та запропоновано шляхи його вдосконалення, зокрема шляхом реформування наявного правового регулювання, з огляду на політичний досвід інших країн і наукові здобутки, трансформацію державної інформаційної політики з фокусом на попередженні вчинення інформаційних правопорушень, міжнародне співробітництво в глобальному інформаційному просторі та розвиток інформаційної культури населення. Надані рекомендації можна застосовувати для усунення недоліків у правовому регулюванні пов'язаних з інформаційною безпекою питань, а також для формування пропозицій з реформування державної інформаційної політики

■ **Ключові слова**: інформація; інформаційний простір; кібербезпека; інформаційна війна; кібервійна