EDUCATION OF ECONOMISTS AND MANAGERS
Volume 65, Issue 3, July–September 2022

Received 15 July 2022; Revised 20 September 2022; Accepted 18 October 2022

DOI: 10.33119/EEIM.2022.65.2

Klochko, A., Semenets-Orlova, I. (2022). Ensuring Information Security of Ukraine in the Conditions of Modern Development of Society. *Education of Economists and Managers*, 65(3), 23–39.
Retrieved from: https://econjournals.sgh.waw.pl/EEiM/article/view/3049

# Ensuring Information Security of Ukraine in the Conditions of Modern Development of Society

Anatolii Klochko

*Department of Public Administration*
*Interregional Academy of Personnel Management*

Inna Semenets-Orlova

*Department of Public Administration*
*Interregional Academy of Personnel Management*

## Abstract

The article pays special attention to the structural and functional characteristics and elements of national security as a factor in state and social development. The authors argue that the elements of the hierarchical world community: individuals, groups, classes, nation-states, and their various associations are under the constant influence of internal and external factors. The main objects of national security protection are defined as a triad consisting of the following components: man-society-state. The aim of the article is to consider the economic and political aspects of national security in the context of modern Ukrainian research.

The article states that the current stage in the formation and implementation of Ukraine's national security strategy is related to the need to protect its national interests in the face of new threats to its state sovereignty and territorial integrity. It was found that they determine the basic principles and current threats to national security, the relevant goals, as well as mechanisms to protect the national interests of Ukraine. It is proved that the main goal of Ukraine's state policy is to further strengthen national security as a key factor in sustainable social development.

It was emphasised that the modernisation of Ukraine's foreign policy and diplomatic service is aimed at strengthening its position in the international environment and ensuring the development of a system of collective security within the Euro-Atlantic community – the European Union and NATO. It is proved that one of the priority tasks of the state power is the complex implementation of the National Security Strategy of Ukraine in the conditions of growing asymmetric threats and conflict factors.

**Keywords:** national security, national interest, hybrid war, public administration

**JEL Classification:** H12, H41, H56

## Introduction

The effectiveness of the exercise of power in any state, including Ukraine, depends in no small part on its information support. It is impossible to imagine a positively functioning political structure without information, the development of mass political consciousness, the interaction of the subject and the object of politics. In the process of the influence of information and communications technologies, the image of state power, its political institutions and leaders is formed in the minds of the people, and the governing functions of the state are carried out with the greatest potential and least energy costs only when the system of information relations between the state, civil society, and the individual is well-developed.

The current state of social development is characterised as a stage in the formation of the information society. The information factor plays a significant role in the development of the Ukrainian state, namely, the problem of ensuring information security, which is primarily due to the need to counter illegal encroachment on the information space of Ukraine, the preservation of information resources and the protection of the population from negative information impact.

The balanced state information policy of Ukraine is formed as an integral part of its social and economic policy, based on the priority of national interests and threats to the national security of the country. Article 17 of the Constitution of Ukraine states: "Protecting the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of the entire Ukrainian people" (Constitution of Ukraine).

The state policy in the field of information security should be aimed at the accumulation and protection of national information resources, the development and implementation of modern secure information technologies, the construction of a secure national information infrastructure, the formation and development of information relations and be implemented by creating and ensuring the effective functioning of a holistic information security system in Ukraine. The aim of the article is to consider the economic and political aspects of national security in the context of modern Ukrainian research.

## Methodology

The article states that the current stage in the formation and implementation of Ukraine's national security strategy is related to the need to protect its national interests in the face of new threats to its state sovereignty and territorial integrity (hybrid war). In this context, the National Security Strategy of Ukraine (2015) and the Law on National Security of Ukraine (2018) are of paramount importance as long-term planning documents. It was found that they determine the basic principles and current threats to national security, the relevant goals as well as mechanisms to protect the national interests of Ukraine. The programme content of these documents is the basis for planning and implementation of state policy in the field of national security and defense of Ukraine.

## Results and discussion

According to a report by the US National Intelligence Council, information wars are becoming the dominant factor in the current century. They are carried out at all levels of the social structure of humanity including the blocs of states. The modern information revolution is unfolding against the backdrop of information wars, which with their main goal are to undermine the national security of states. Considering such approaches, the security information function of the state in all regions of the world is of particular importance (Onyshhenko, Gorovyj, & Popyk, 2014).

The situation in the world information space is due to the following:

- most countries of the world have faced problems of cyberterrorism, cybercrime, and other problems of information security;

- over the past decades, there has been a trend towards information aggression and violence;
- aggressive advertising, attempts to manipulate the consciousness of a person, periodically carried out information and psychological operations;
- almost 120 countries around the world (according to American experts) are developing information weapons or their elements (for comparison, the development of weapons of mass destruction is carried out in about 20 countries);
- the consequences of the use of modern information weapons (according to the conclusions of scientists and experts of European countries, Ukraine, the Russian Federation, and the USA) can be compared with the use of weapons of mass destruction;
- the latest challenges and threats in the information sphere pose a real threat to the security of mankind and the international legal order (Pylypchuk, 2016, pp. 3–7).

People have realised the value of information for a long time. It should be noted that in all periods of human development information was an integral part of the main work activity, survival, and self-improvement of people and played a role of the global factor of system-wide balance in economic and ecological complex (Sulyma & Shepelev, 2010, p. 292).

In a post-industrial society the role of information has changed. According to Gurovsky, information acquires the properties of a powerful means of influencing social and political, ideological and economic processes, becomes a kind of weapon that requires the creation of a system of counteraction, the protection of information resources belonging to state bodies, constituting state, professional, personal secrets (Gurovsky, 2014, p. 25).

Yakhno notes that the level of development of the information component is closely related to the security of the state: the period of formation of the mechanisms of the information society is very dangerous, since a country can entre the world infrastructures without creating protection mechanisms (Yakhno, 2010, p. 10).

The development of society, the introduction of innovative technologies has given rise to the phenomenon of computer terrorism, a real threat to the functioning of information and telecommunications systems of the state through the global Internet. There are no state borders for the world network, an attack can be carried out from anywhere in the world using gadgets that are available to everyone. Cyberterrorism refers to a deliberate motivated attack on information processed by a computer, computer system, or network; it is connected with a danger to life and health of people or other grave consequences, if such actions are committed in order to violate public security, intimidate the population, provoke a military conflict (Topchij, 2015, pp. 66). The Law of Ukraine, Basic Principles for Ensuring the Cyber Security of Ukraine, defines cyberterrorism as a terrorist activity carried out in or using cyberspace.

The annual report of experts of the World Economic Forum in Davos on global risks in the world noted that cyberattacks are ranked in the second place in terms of their negative impact on the world community after natural disasters (Global Risk Report, 2018).

The primary tasks of information protection in an automated system in the process of electronic interaction are prevention, distribution, modification, destruction, copying, blocking, and illegal replication of restricted access information.

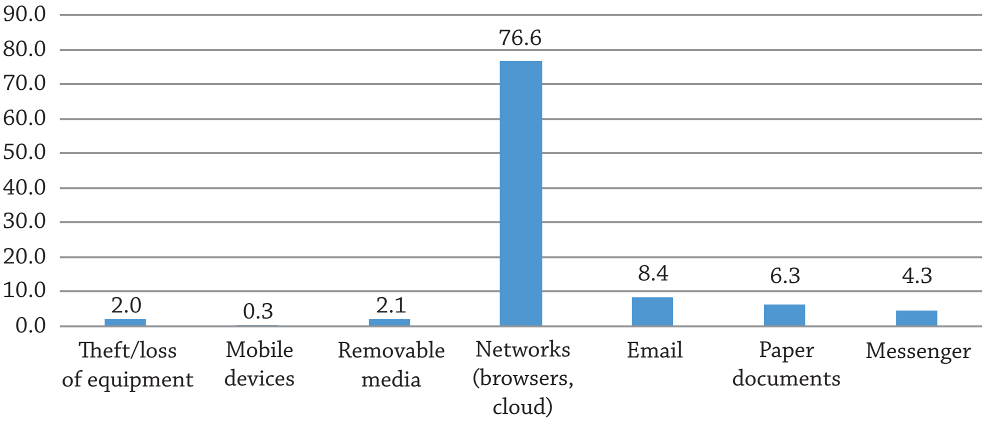
Figure 1 shows the distribution of information leakage channels according to the statistics of the analytical centre in the field of information security InfoWatch for 2019 (Global Study, 2019).

Key information activities include:

- analysis of potential and actual situations representing cyber threats;
- assessment of the nature of information security threats;
- integrated allocation of threat detection measures;
- implementation of measures to prevent the threat.

A multi-level information protection scheme using comprehensive cybersecurity solutions allows minimising the risks of eliminating the consequences of cyberattacks. To combat cybercrime, a multi-stakeholder approach is needed to prevent, respond to, and investigate cybercrime. The correct organisation of information security of data is designed to prevent emerging risks and eliminate their negative consequences.

**Figure 1 Information leakage channels**



Source: Global Study (2019).

The adopted National Security Strategy of Ukraine defines the priorities of the state policy of national security and the main directions for ensuring it, namely, strengthening the capabilities of the national cybersecurity system to counter cyber threats effectively in the modern security environment. Paragraph 63 of the Strategy notes that it is necessary to complete the creation of a national cybersecurity system, to develop the modern capabilities of cybersecurity and cyber defence actors and to strengthen their coordination system. It was emphasised that the state should recognise cyberspace as a space of rivalry, along with land, water, and air. Today's threats to cyber storage range from globalisation and international competition to infrastructure, information operations, and digital transformation.

Today cyberspace has become one of the most important components of the information space and the arena for conducting real wars in a virtual environment. Therefore, cybersecurity is the main element of regulation of cyberspace and at the same time the country's national security system.

The globalisation and inclusiveness of cyberspace make it very difficult to detect cyberspace threats and to implement appropriate state responses. Lipkan deduces the main cyber threats to the national security of Ukraine, namely:

- the threat of hybrid war by the Russian Federation;
- the insufficient level of cyber literacy and media culture of the population;
- the insufficient level of elaboration at the state level of a comprehensive holistic approach to communication policy;
- vulnerability to modern cyber threats of key domestic infrastructure and official electronic resources especially from cyberattacks by hackers;
- the physical obsolescence of the material base of cyberspace;
- the obsolescence and imperfection of modern forms and methods of combating cybercrime;
- the weakness of the State Secret Protection System in Ukraine, etc. (Lipkan, 2006).

It is to overcome these cyber threats that the creation of a single national cybersecurity system is necessary.

Bugaichuk and Shorokhova note that in order to develop further an active and effective cybersecurity system in Ukraine, it is necessary to do the following:

1) Clearly define the direction, content, forms, and methods of the state policy in the field of cybersecurity.
2) Create and streamline appropriate organisational structures that will ensure security in cyberspace.
3) Establish an effective security management process in cyberspace and create the appropriate conditions for the implementation of planned cybersecurity activities.
4) Establish a clear interaction between the relevant competent state bodies in the field of cybersecurity and appropriate effective coordination of their activities.

5) Create new mechanisms for state cybersecurity management through the opening of specialised scientific institutions, training centres, and experimental sites.
6) Conduct active research in the field of information operations, to promote development and scientific and technical work in this field (Bugaichuk & Shorokhova, 2018).

Prisyazhnyuk notes that only the state can count on leadership in economic, military, and political or other areas, have a strategic and tactical advantage, flexibly regulate the economic costs of developing weapons and military equipment, maintain an advantage in a number of advanced technologies, which poses an advantage in the media and information struggle (Prisyazhnyuk, 2013, p. 43).

Information security is not only an independent component of national security, but also an integral part of political, economic, defence, and other components of national security, because all types of relations between the subjects of information society are based on consumption and exchange of information. In this regard, Lipkan notes that national interests, threats to them, the management of these threats in all sectors of national security are expressed, realised through the information and information sphere (Lipkan, 2006, p. 25).

There is currently no holistic approach to defining 'information security' among researchers.

From the point of view of Sorokin, information security constitutes a state of protection of the person, society, state from information that is harmful or illegal, from information that has a negative impact on the consciousness of the person, impedes the sustainable development of the person, society, and state. Information security is the state of security of the information infrastructure, including computers, information and telecommunications infrastructure and information contained in them, which also ensures the sustainable development of the individual, society, and the state (Sorokin, 2014, p. 20).

Lipkan highlights the following approaches to determining the phenomenon of information security: the state of protection of national interests (Lipkan, 2006, pp. 25–30).

Abu defines information security as the state of information legislation and security institutions regulated by it, which guarantee the permanent availability of databases for the implementation of strategic decisions and the protection of information resources of the state (Abu et al., 2012).

Whitman and Mattord note that information security is a set of legal, organisational, and technical measures aimed at the formation and use of technological, infrastructure, and information resources for the protection of information of national importance, as well as the rights and legitimate interests of entities participating in information legal relations (Whitman & Mattord, 2014), while Von Solms defines information security as only technological and legal security of information activities ensuring its formation and development for the benefit of citizens, organisations, and the state as a whole (Von Solms, 1999, p. 50).

According to Kalyuzhny, information security is a group of information legal relations for the formation, support, and protection of living conditions necessary for a person, society, and the state, specialised legal relations for the creation, storage, dissemination, and use of information (Kalyuzhnyj & Bayev, 2009).

Ahmad believes that information security is the protection of the rules established by the legislation that regulate information processes in the country, ensuring the conditions guaranteed by the Constitution for the life of a person, the state, and society as a whole (Ahmad, Maynard, & Shanks, 2015).

Researchers Danilyan, Dzoban, and Panov define information security as the security of an object against information threats or negative impacts related to information and non-disclosure of data about an object constituting a state secret (Danilyan, 2002, p. 86). They also focus on the problem of information wars, since today it represents an effective and civilised path of colonisation of one country to another and, in addition, highlights such threats to information security as disclosure of information, constituting a state secret, the influence of the mass media on the consciousness of a person and society, providing state organisations with the full, reliable, and timely information necessary for decision-making, non-integration of Ukraine into the world information space, insufficient qualifications and activity of Ukrainian information services, the use of information technologies, crime, etc.

However, if we analyse the content and directions of research of the concept of information security, we can distinguish several approaches to determining the essence of this phenomenon, namely, understanding information security as:

- the state of information space security;
- the process of threat and hazard management, ensuring the information sovereignty of Ukraine;
- the state of protection of the national interests of Ukraine in the information environment;
- the protection of the rules established by law, according to which information processes take place in the state;
- the state of protection of the country’s national interests in the information sphere;
- public relations related to protection of vital interests of a person and citizen, society and the state from real and potential threats in the information space;
- an important function of the state;
- an integral part of political, economic, defence, and other components of national security.

Thus, the constructive way to define information security is to distinguish its basic features, which is derived from the concept of national security and should take into account its essential features.

The information security policy is implemented by a system of public authorities and civil society institutions.

In turn, the National Security Act identifies three objects of national and, accordingly, information security, which include:

- person and citizen – their constitutional rights and freedoms;
- society – its spiritual, moral, cultural, historical, intellectual, and material values; information and environment and natural resources;
- the state – its constitutional system, sovereignty, territorial integrity, and inviolability (On the national security of Ukraine, 2018).

The mechanisms for protecting the information security of Ukraine can be divided into two levels – legislative and administrative. The legislative level is the most important for ensuring information security. Most people do not commit illegal actions not because it is technically impossible, but because it is condemned and/or punished by society, because it is not accepted.

Two groups of activities are distinguished at the legislative level:

- measures aimed at creating and maintaining in society negative (including the application of penalties) attitudes towards violations and violators of information security;
- directing and coordinating measures to enhance public education in the field of information security, helping in the development and dissemination of information security tools.

The most important thing at the legislative level is to create a mechanism to harmonise the process of drafting laws with the realities and progress of information technologies. Laws cannot be ahead of life, but it is important that the lag is not too large, since in practice, among other negative aspects, it leads to a decrease in information security.

The administrative mechanism for ensuring information security covers institutions whose activities are aimed at the formation and implementation of information security.

The main goal of administrative measures is to form a programme of work in the field of information security and ensure its implementation, allocating the necessary resources and monitoring the state of affairs. The programme is based on a security policy that reflects the organisation's approach to protecting its information assets. The leadership of each organisation must recognise the need to maintain the security regime and allocate significant resources for these purposes.

The key to the creation of a reliable information security system today can only be the strengthening of the Ukrainian state itself and its state bodies responsible for ensuring information security in the country. In this regard, there are large-scale tasks related to the development of an information security system, the search for fundamentally new, non-standard forms of organisation, interaction, coordination of activities, and the improvement of all means aimed at ensuring the process of managing threats and dangers.

Ensuring information security in the information society is a necessity that becomes an attribute of the modern life of any social subject, and requires tireless work with information, includes interaction with various expert systems, delocalisation of actions, ensuring freedom and minimising risks.

The main goal of ensuring information security should be determined on the basis of a broad understanding of this concept as an important component of national security and a systemic factor in all spheres of life of individual, society, state, political, economic, social and cultural, scientific, technological, military, environmental, information, etc., components of national security. Thus, the priority of the state policy of information security should be the protection of: constitutional rights and freedoms of a person and citizen, ensuring the unity of their rights and duties; spiritual, moral and ethical, cultural, historical, intellectual and material values of society, its information and natural environment; constitutional system, sovereignty, territorial integrity, information security in political, economic, social and cultural, scientific, technological, defence and state security, environmental, information, etc. components of national security (Olijnyk, 2016, p. 75).

The information security of Ukraine has the main strategic task: to create a powerful national information space as the main aspect, which testifies the country's presence in the world information arena. Such a goal also implies the need to create a system to counter any information threat and defend its own information resources, environment, and infrastructure component of the country.

The national security of Ukraine in the information sphere should be considered as the integral integrity of four components – personal, public, commercial (corporate), and state security.

Therefore, the following elements should be taken into account in determining the nature of risks:

- a brief conceptual explanation to stakeholders of political security, its principles, standards and rules agreed upon with the current legislation and the principles of ensuring the continuity of the information security system of a person, society, commercial (corporate) structures, and the state;
- identification of objects and objectives;

- identification of structures suitable for ensuring the interests of all subjects to establish control over security objects, as well as risk assessment and risk management;
- identification of the status and functional roles, expectations, and responsibilities of the subjects involved, including reporting on events that carry potential threats.

Among the components of the information security system, the list of its threats occupies an important place.

An analysis of the sources shows that some scientists put an equal mark between the concepts of 'threats to information security' and 'threats to national security and national interests', which we do not agree with, since there is a common phenomenon and a separate one. Other scientists understand threats as a set of conditions, processes, and factors that impede the realisation of national interests or create a danger (Lipkan, 2003, p. 32). There are opinions that threats are specific and immediate forms of danger or a combination of negative factors or conditions (Nyzhnyk, Sytnyk, & Nyzhnyk, 2000, p. 132); a set of conditions and factors that endanger the vital interests of an individual, society, and the state in the field of information (Tarasenko, 2010, p. 156); explicit or potential actions that impede or make impossible the realisation of national interests in the field of information and pose a danger to the system of public administration, the life support of its systemically important elements (Lipkan, 2006, p. 75); One should agree with those researchers who consider threats to be a combination of negative factors or conditions. In determining their role, the accepted opinion is of Emelyanov and Streltsov: one of the sources of threats to the interests of society in the information sphere is the continuous complication of information systems and communication networks of critical infrastructures to ensure the life of society (Emelyanov & Strelczov, 1999, pp. 15–17).

Of the external threats to the information security of Ukraine in the foreign policy sphere, the greatest danger is the information impact of foreign political, economic, military, and information structures on the development and implementation of the foreign policy strategy of Ukraine; dissemination of misinformation about the foreign policy of Ukraine abroad; violation of the rights of Ukrainian citizens and legal entities in the information sphere abroad; attempts of unauthorised access to information and influencing information resources, information infrastructure of executive authorities implementing the foreign policy of Ukraine, Ukrainian missions and organisations abroad, representative offices of Ukraine to international organisations.

Of the internal threats to the information security of Ukraine in the foreign policy sphere, the greatest danger is violation of the established procedure for collecting, processing, storing, and transmitting information in executive bodies implementing the foreign policy of Ukraine; propaganda activities of political forces, public associations, mass media and individuals, distorting the strategy and tactics of foreign policy activities of Ukraine; a lack of public awareness of Ukraine's foreign policy activities.

The main challenges and threats to information security for Ukraine today are information war, information terrorism, and information crimes. They are caused by global information processes, progress in the development of information technologies, and the information component of the hybrid war of the Russian Federation against Ukraine.

The use of hybrid warfare technologies by the Russian Federation against Ukraine has turned the information sphere into a key arena of confrontation. It is against Ukraine that the Russian Federation uses the latest information technologies to influence the consciousness of citizens, aimed at inciting ethnic and religious hatred, propagating an aggressive war, changing the constitutional order by force or violating the sovereignty and territorial integrity of Ukraine (Doctrine of information security of Ukraine, 2017).

Sharing the opinion of Marutyan that the information front of the 'hybrid war' is unfolding in several directions at once (among the population in the conflict zone, among the population of the country against which the aggression is carried out, the territory of which is not covered by the conflict, among the citizens of the aggressor country, and among the international community), we determine the corresponding basic meaningful dimensions of disinformation: the causes and nature of the war in Ukraine; the possibility of ending the war as a result of 'minor concessions' and the impact of the war on the standard of living of the Ukrainian people; Russia's historical mission to collect land and protect the Russian-speaking population; the non-involvement of the Russian Federation in the civil war in Ukraine (Marutyan, 2018).

To strengthen opposition to the information war of Russia against Ukraine, it is important to study the experience of other countries. The USA, Great Britain, Israel, Germany, Russia, China are constantly under powerful external information influence, so they are forced to create national information protection systems. Information security systems of these countries are the most developed and have a sufficient active component, as a result of which it is possible to conduct information and psychological activities and cyber attacks against opposing countries (Levchenko, 2014, p. 168).

The lack of sufficient state tools for conducting information warfare is a pressing issue of the war with Russia. Ukrainian scientist Senchenko notes that Ukraine, in order to resist the information war against Russia effectively, needs to have at least: 1) an effective information warfare system to effectively confront the information war from Russia; 2) an effective concept of information war; 3) an information warfare strategy (Senchenko, 2014).

The aim of improving the state information policy in hybrid warfare is to create a national information security system for Ukraine, which provides for:

- developing and improving the regulatory framework for information security, which is now fragmented and fully responsive to pressing needs;
- establishment (definition) of a governing and coordinating body of the information security system of Ukraine within the structure of state executive bodies;
- identification (refinement) of the list of entities responsible for the state of information security;
- research and identification of technical, financial, and human resources requirements for the system;
- intensification of activities in the Ministry of Defence and the General Staff of the Armed Forces of Ukraine to create their own information security system as part of the national information security system (Subbot, 2015, p. 30).

## Conclusion

The main measures to ensure the information security of Ukraine in the foreign policy sphere are the development of the main directions of state policy in the field of improving information support for the foreign policy of Ukraine; development and implementation of a set of measures to strengthen the information security of the information infrastructure of executive authorities implementing the foreign policy of Ukraine, Ukrainian missions and organisations abroad, representative offices of Ukraine to international organisations; the creation of the conditions for work to neutralise disinformation spread there about the foreign policy of Ukraine by Ukrainian missions and organisations abroad; improving information support for work to counter violations of the rights and freedoms of Ukrainian citizens and legal entities abroad; improvement of information support of the subjects of Ukraine on issues of foreign policy activity, which fall within their competence.

The national interests of Ukraine in the field of information security should be the development of modern telecommunications technologies, in the protection of state information resources from unauthorised access. Modern information confrontations have shown that the information space of Ukraine needs additional protection from external negative information and psychological influences. Monopolisation of information leads to a certain circle of people managing the consciousness of citizens in order to make the necessary selfish decision for them. This development of events is particularly threatening for Ukraine in the context of the formation of the highest state authorities.

In order to prevent and counter existing and likely threats to information security, the strategic task of the state is to create and operate an information security mechanism. It provides for a consistent system of activities, a set of measures and state legal institutions designed to guarantee the unhindered realisation of the national interests of the state in the information sphere, the corresponding interests of a person and society, the prevention of information conflicts and the prompt elimination of them.

## References:

Abu, T.M., Khelifi, A., Barachi, M., & Ormandjieva, O. (2012). Guide to ISO 27001: UAE Case Study. *Issues in Informing Science & Information Technology*, 9(19), 331–349.

Ahmad, A., Maynard, S., & Shanks, G. (2015). A Case Analysis of Information Systems and Security Incident Responses. *International Journal of Information Management*, 35(6):717–723, DOI:10.1016/j.ijinfomgt.2015.08.001

Bugajchuk, K,. & Shoroxova, G. (2018). Zabezpechennya kiberbezpeky yak umova protydiyi terorystychnij diyalnosti: normatyvno-pravovi aspekty [Ensuring cybersecurity as a condition for countering terrorist activities: regulatory aspects]. *Protydiya terorystychnij diyalnosti*: mizhnarodnyj dosvid i jogo aktualnist dlya Ukrayiny: materialy II Mizhnarodnoyi naukovo-praktychnoyi konferenciyi (15.12.2017). Kyyiv: Nacionalna akademiya prokuratury Ukrayiny, pp. 135–138 [in Ukrainian].

Danilyan, O. (2002). Nacionalna bezpeka Ukrayiny: sutnist, struktura ta napryamky realizaciyi [Security of Ukraine: essence, structure, and directions of realization]: navchalnyj posibnyk. Xarkiv: Folio [in Ukrainian].

Doktryna informacijnoyi bezpeky Ukrayiny (2017) [Doctrine of information security of Ukraine]: uvedena u diyu Ukazom Prezydenta Ukrayiny: vid 25.02.2017 r., 47/2017. Retrieved from: http:// www.president.gov.ua [in Ukrainian].

Emelyanov, G., & Strelczov, A. (1999). Problemy obespechenyya bezopasnosty ynformacyonnogo obshhestva [Problems of information society security]. *Ynformacyonnoe obshhestvo*, 2. 15–17 [in Russian].

*Global Risks Report 2018* (2018). Retrieved from:http: www.weforum.org.

*Globalnoe yssledovanye utechek konfydencyalnoj ynformacyy v pervom polugodyy 2019 goda* (2019). [Global study of leaks of confidential information in the first half of 2019]. Retrieved from: https://infowatch.ru [in Russian].

Gurovsky, V. (2014). The role of public authorities in the field of information security of Ukraine [The role of public authorities in the field of information security of Ukraine]. *Bulletin of the Ukrainian Academy of Public Administration under the President of Ukraine*, 3, 21–31 [in Ukrainian].

Kalyuzhnyj, R., & Bayev, O. (2009). Normatyvno-pravove zabezpechennya informacijnoyi bezpeky Ukrayiny [Regulatory and legal support of information security of Ukraine]. *Pravova informatyka*, 4(24),5–12 [in Ukrainian].

*Konstytuciya Ukrayiny* [Constitution of Ukraine]: stanom na 1.09.2016 r. / *Verhovna Rada Ukrayiny*. Xarkiv: Pravo, [in Ukrainian].

Levchenko, O. (2014). Problemy i shlyaxy formuvannya systemy informacijnoyi bezpeky derzhavy [Problems and ways of formation of information security of the state]. *Zbirnyk naukovyx pracz Xarkivskogo universytetu Povitryanyx Syl*, 2(39), 166–168 [in Ukrainian].

Lipkan, V. (2003). A. *Teoretychni osnovy ta elementy nacionalnoi bezpeky Ukrainy* [Theoretical foundations and elements of national security of Ukraine]. Nacionalna akademiya vnutrishnix sprav Ukrainy. Kyyiv: Tekst. [in Ukrainian].

Lipkan, V. (2006). *Informacijna bezpeka Ukrayiny v umovax yevrointegraciyi* [Information security of Ukraine in the conditions of European integration]: navchalnyj posibnyk. Kyyiv: KNT [in Ukrainian].

Marutyan, R. (2018). *Informacijna skladova gibrydnoyi vijny proty Ukrayiny: suchasni vyklyky ta zagrozy* [Information component of the hybrid war against Ukraine: current challenges and threats]. Retrieved from: https://matrix-info.com [in Ukrainian].

Nyzhnyk, N., Sytnyk, G., & Nyzhnyk, V. (2000). *Nacionalna bezpeka Ukrainy* (metodologichni aspekty, stan i tendencii rozvytku) [National Security of Ukraine (methodological aspects, state and development trends)]: navchalnyy posibnyk. – Irpin [in Ukrainian].

Olijnyk, O. (2016). Pryncypy zabezpechennya informacijnoyi bezpeky Ukrayiny [Principles of information security of Ukraine]. *Yurydychnyj visnyk povitryane i kosmichne pravo*, 4(41), 72–78 [in Ukrainian].

Onyshhenko, O., Gorovyj, V., & Popyk, I. (2014). *Nacionalni informacijni resursy yak integratyvnyj chynnyk vitchyznyanogo sociokulturnogo seredovyshha: monografiya* [National information resources as an integrative factor of the domestic socio-cultural environment]. Nacionalna bibliotekaka Ukrayiny im. V.I. Vernadskogo. Kyyiv [in Ukrainian].

Pro nacionalnu bezpeku Ukrayiny (2018). [On the national security of Ukraine]: Zakon Ukrayiny, 2469-VIII vid 21.06.2018. *Vidomosti Verxovnoyi Rady,* 31, 241 [in Ukrainian].

Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny (2017) [On the basic principles of cybersecurity in Ukraine]: Zakon Ukrayiny vid 5 zhovt. 2017 r. # 2163-VIII. *Vidomosti Verxovnoyi Rady Ukrayiny*, 45, 403. Retrieved from: http:// zakon2.rada.gov.ua /laws/show/2163–19.

Prysyazhnyuk, M.M. (2013). *Informacijna bezpeka Ukrayiny v suchasnyx umovax* [Information security of Ukraine in modern conditions]. Visnyk nacionalnogo universytetu imeni Tarasa Shevchenka. Vijskovo-specialni nauky. Vyp.30, 32–46 [in Ukrainian].

Pylypchuk, V. (2012). Systemni pravovi problemy formuvannya informacijnogo suspilstva [Systemic legal problems of information society formation]: zb. nauk. st. ta tez; naukove povidomlennya za materialamy mizhnarodnoyi naukovo-praktychnoyi konferenciyi [“Informacijne suspilstvo i derzhava: problemy vzayemodiyi na suchasnomu etapi"], (Xarkiv, 26 zhovtnya 2012 r.). Xarkiv: NDI derzhavnogo budivnycztva ta miscevogo samovryaduvannya [in Ukrainian].

Senchenko, M. (2014). Zaporuka nacionalnoyi bezpeky v umovax informacijnoyi vijny [The key to national security in an information war]. *Visnyk Knyzhkovoyi palaty*, 6, 3–9.

Sorokin, O. (2014). Informacijna bezpeka ta yiyi skladovi: problemy vyznachennya konceptu [Information security and its components: problems of concept definition]. *Derzhava ta pravo*, 8, 18–22.

*Strategiya nacionalnoyi bezpeky Ukrayiny* (2020) [National Security Strategy of Ukraine]: Ukaz Prezydenta Ukrayiny vid 14.09.2020 r. # 392/2020. Rezhym dostupu: https://www.president.gov.ua/documents/3922020–35037

Subbot, A. (2015). *Informacijna bezpeka suspilstva* [Information security of society], *Viche,* 8, 29–31.

Sulyma, Ye.,. & Shepelev, M. (2010). *Globalistyka* [Globalism]. Kyyiv: Vyshha shk.

Tarasenko, R. (2010). *Informaciyne pravo: navchalno-metodychnyy posibnyk* [Information law]. Lugansk.

Topchij, V. (2015). Kiberteroryzm v Ukrayini: ponyattya ta zapobigannya kryminalno-pravovym ta kryminologichnymy zasobamy [Cyberterrorism in Ukraine: the concept and prevention of criminal law and criminological means]. *Naukovi visnyk Xersonskogo universytetu. Ser. Yurydychni nauky*, 6(3), 65–68.

Von Solms, R. (1999). Information security management: why standards are important, *Information Management & Computer Security*, 7(1), 50–58.

Whitman, M., & Mattord, H. (2014). *Management of information security*. Boston: Course Technology Cengage Learning.

Yaxno, O. (2006). *Ukrayina v suchasnomu geopolitychnomu prostori (polityko- medijny'j aspekt)* [Ukraine in the modern geopolitical space (political-media aspect)]: avtoref. dys. … kand. polit. nauk: 23.00.03. Kyyiv.

## Acknowledgements

The article is written by the authors within the framework of the young scientists' project *Realization of the young scientists' potential in integration of science, education, and business* (Ukrainian state registration No. 0120U102126).

### Anatolii Klochko

Expert in national security, a project monitoring specialist. Key responsibilities from January 2016 up to the present day: doing scientific research in the field of management of national security; analytical activity; projecting and implementation of change at the lowest operational level of an institution/public body (e.g.,

a department), as well as at the level of a public body as a whole; organisation and conducting of communication activities, educational master classes, workshops.
Postgraduate student at the Department of Public Administration, Interregional Academy of Personnel Management.
e-mail: kafedrapa@ukr.net
ORCID: 0000-0002-2624-5386

## Inna Semenets-Orlova

She holds a Master's degree in political science and law, Doctor of Public Administration, Associate Professor, the Head of the Department of Public Administration at Interregional Academy of Personnel Management.
Since 2014 engaged in developing and management of educational and research projects, cooperated with the Swiss Agency for Development and Cooperation SDC, Pädagogische Hochschule Zürich, Polish Aid. Research interests: state policy, regional development, support of civic activity to solve environmental problems in the regions of Ukraine. The author of more than 160 scientific papers, national expert of Swiss-Ukrainian projects: the DOCCU Project No. 7F-08698.01 and DECIDE, Laureate of the "Innovative Intellect of Ukraine" Honorary Silver Badge, winner of an international competitions for scientific works of young scientists in public administration, a member of a number of official working groups, international internships: of Uniwersytet Warszawski, Uniwersytet Jagiellonski; an individual grant from the Government of the Swiss Confederation to conduct a mass survey in 6 regions of Ukraine, a collective grant from Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ Ukraine) GmbH, to learn civic position in 8 regions of Ukraine. A member of the working groups on the development of the Concept of development of citizenship education in Ukraine and the Strategy for the development of citizenship education for the period up to 2022, a participant of meetings of a working group on preparation of a draft law on education for the second reading (2016, 2017).
e-mail: innaorlova@ukr.net
ORCID: 0000-0001-9227-7426