УДК 007:65.012.8

Боднар Ірина Романівна, iryna.bod@gmail.com,
ORCID ID: 0000-0002-6884-2058,
к.е.н., доцент, доцент кафедри міжнародних економічних відносин,
Львівський торговельно-економічний університет, м. Львів

КОНЦЕПЦІЇ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ З МЕТОЮ ГАРАНТУВАННЯ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Анотація. *Стрімкий і глобальний розвиток інформаційної сфери, сучасних інформаційних технологій, значною мірою впливає на політичну, економічну, соціокультурну, оборонну та інші складові процесів розвитку суспільства і держави. Інформаційні ресурси в сучасних умовах стають основним фактором життєдіяльності всіх сфер суспільства. Ефективність системи державного управління національними інформаційними ресурсами та гарантування їхньої безпеки,значною мірою визначає, в умовах війни, загальний рівень інформаційної і національної безпеки. Будь-які недоліки в структурі і функціонуванні системи державного управління призводять до збитків суспільства і держави. У зв'язку з цим у статті розглянуто ключові поняття та основи державної інформаційної політики в сфері інформаційної та національної безпеки. Аналізується діяльність держави в інформаційній сфері в умовах війни. Крім цього визначені основні напрями держави в сфері інформаційної безпеки. Запропоновані концептуальні підходи гарантування інформаційної безпеки.*

Стратегічне інформаційне протистояння є самостійним і принципово новим видом протистояння, здатним вирішувати конфлікт без застосування збройних сил у традиційному розумінні. В статті визначені закономірностей інформаційного протистояння та здійснено аналіз його кількісних характеристик. Проведено формалізацію рівнів інформаційної озброєності держави і механізми еволюції в залежності від ресурсного потенціалу конкретної держави та впливу зовнішнього оточення. При формуванні концепції державної інформаційної політики з метою гарантування інформаційної та національної безпеки України, варто виходити з необхідності прийняття таких базових принципів як відкритість інформаційної політики, рівність інтересів всіх учасників інформаційних відносин, системності, пріоритетності тощо. В цьому процесі головні заходи повинні бути спрямовані на забезпечення державних інтересів України і не суперечити соціальним інтересам громадян країни. Необхідні програми на фінансування державою інформаційного розвитку, забезпечення пріоритету права перед силою тощо.

Ключові слова: інформаційна безпека, інформаційні загрози, державна інформаційна політика, інформаційні ресурси, інформаційне суспільство, національна безпека.

Bodnar I. R., iryna.bod@gmail.com,
ORCID ID: 0000-0002-6884-2058,
Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of the International Economic Relations,
Lviv University of Trade and Economics, Lviv

CONCEPTS OF THE STATE INFORMATION POLICY IN ORDER TO GUARANTEE THE NATIONAL INFORMATION SECURITY OF UKRAINE

Abstract. *The rapid and global development of the information sphere and modern information technologies has a significant impact on the political, economic, socio-cultural, protection, and other components of the development of society and the state. Information resources in modern conditions are becoming a major factor in the life of all spheres of society. The effectiveness of the system of state management of national information resources and ensuring their security largely determines the overall level of information and national security in times of war. Any shortcomings in the structure and functioning of the public administration system lead to losses for society and the state. In this regard, the article considers the key concepts and foundations of state information policy in the field of information and national security. The activity of the state in the information sphere in the conditions of war has been analyzed. In addition, the main directions of the State in the field of information security have been determined. Conceptual approaches to ensuring information security are offered.*

Strategic information confrontation is an independent and fundamentally new type of confrontation capable of resolving the conflict without the use of armed forces in the traditional sense. Regularities of information confrontation have been determined and its quantitative characteristics have been analyzed. The article conducts formalization of levels of information weapons of the state and mechanisms of evolution depending on the resource potential of a specific state and the influence of the external environment. When developing the concept of the state information policy in order to ensure information and national security of Ukraine, it is necessary to proceed from the need to adopt such fundamental principles as openness of information policy, equality of interests of all participants in information relations, consistency, priority, etc. In this process, the main measures should be aimed at ensuring the state interests of Ukraine and not contradict the social interests of the citizens of the country. We need programs of state funding for information development, ensuring the priority of law over force, etc.

Keywords: information security, information threats, state information policy, information resources, information society, national security.

JEL Classification: D78, L96
DOI: https://doi.org/10.32782/1563-3950-2025-5-3

Formulation of the problem. In wartime, the scale of human activity is determined by risks, threats, and challenges. Accordingly, the methodology for understanding and accounting for them should be based on a clear understanding of the qualitative and quantitative aspects of the risks involved in each situation. Thus, in strategic planning in the United States, two terms are used: "threat" and "challenge" They indicate the ability of any country, group of individuals, or phenomenon to threaten ("threat") or counteract ("challenge") achieving information and national security objectives. To this end, it is important to identify the problems and justify the State's directions in the field of information security in the context of war. The purpose of the article is to provide a theoretical justification of the activities of public authorities that manage the information sphere, implement information policy with a view to protecting the national information space, and ensure information security in war conditions.

Analysis of research and publications. The information sphere and its state protection are the basis of scientific research by domestic and foreign scholars and researchers. However, the research on this scientific issue by international economists is insufficient, as their works are much less numerous than those of scholars in other fields.

Nevertheless, the theoretical aspects of the role of the state in the formation of the information society and in ensuring information security have been studied bysuchresearchersas I. V. Aristova [2020], K. I. Beliakov [2], G. G. Pocheptsov [2006], I. Ramone [2010], D. Lukianenko [2010], O. Sosnin [2011] and others.

The problem of determining the organizational and legal framework for the protection of information resources in Ukraine was analyzed by O. V. Oliinyk [2011]. He proposed a comprehensive analysis of the content of the concepts of "information security", and "information resources of the State", as well as conceptual approaches to the formation of principles for the protection of information resources of the State of various types.

O. O. Tykhomyrov draws attention to the problem of the reproduction of personnel in the field of information security [2014], as experienced specialists leave government agencies and go to work in commercial organizations due to low salaries.

Setting objectives. Despite the importance and relevance of studying the problem of information security in Ukraine in times of war, the number of works devoted to a comprehensive study of this issue is rather small, which influenced the choice of the topic of the study. Despite the importance and relevance of the study of the problem of information security of Ukraine in the conditions of war, the number of works devoted to the comprehensive study of this issue is quite small, which influenced the choice of the research topic. Therefore, in the article we will consider the main concepts and foundations of the state information policy in the

field of information and national security. We will analyze the activities of the state in the information sphere in the conditions of war. We will determine the levels of the state's information armament and the mechanisms of evolution depending on the resource potential of a specific state and the influence of the external environment.

Presentation of the main research material. A successful information policy can have a significant impact on the resolution of domestic, foreign, and military conflicts. Article 17 of the Constitution of Ukraine states: "To protect the sovereignty and territorial indivisibility of Ukraine, and to ensure its economic and informational security are the most important functions of the State and a matter of concern for all the Ukrainian people." [8]. The "Doctrine of National Information Security of Ukraine" (2016) defines the complex nature of current threats to national security in the information sphere [9]. Information security in today's post-industrial world, in which the main commodity is information that affects the state's tactical and strategic decision-making, is the basis of national security. Information security is one of the essential components of the country's national security. Ensuring it through the consistent implementation of a well-formulated national information strategy would greatly contribute to achieving success in solving problems in the political, military, social, economic, and other spheres of state activity.

Information security is the state of security of society, the state, the individual, the state of security of information resources that ensure the progressive development of vital areas for society [10]. The main information threat to national security is the threat of another party's influence on the country's information infrastructure, information resources, society, consciousness, and subconsciousness of the individual. This happens in order to impose on the other party (the state) the desired system of values, views, interests, and decisions in vital areas of social and state activity. In addition, the opposite, hostile party (the aggressor country) seeks to control the behaviour of people and the development of the situation in another country in the direction it desires. In fact, this is a threat to Ukraine's sovereignty in vital areas of public and state activity, which is realized at the information level in times of war.

Strategic information confrontation is an independent and fundamentally new type of confrontation capable of resolving a conflict without the use of armed forces in the traditional sense. In order to study the patterns of information confrontation and analyze its quantitative characteristics, it is necessary to formalize the levels of information armament of the state and the mechanism of evolution depending on the resource potential of a particular state and the influence of the external environment.

In this case, we will take the information state of Ukraine as a basis. As a basic model, we will consider the model of resolving an information

conflict between two countries, which is based on the Richardson-Kasparov model [11]. The model is based on the following hypotheses:

- in the process of an information conflict, each of the two states seeks to ensure the growth of the effectiveness of its information weapons in proportion to the level of information power;
- the economic potential of each country has/limits the impact on the growth rate of information capabilities;
- state institutions initiate an increase in the level of information capabilities, guided by their aspirations.

Let's introduce the notation N_1 (t), N_2 (t)for the levels of information armament of each side of the conflict, where t is time. Then the above conditions of the model can be formalized as a system of two ordinary differential equations:

$$\dot{N}_1 = M_1(L_1 - N_1)[1 - exp(-p_1(k_1N_2 - a_1N_1 + g_1))]$$
$$\dot{N}_2 = M_2(L_2 - N_2)[1 - exp(-p_2(k_2N_1 - a_2N_2 + g_2))], \quad (1)$$

where $M_1,\ M_2, L_1, L_2, p_1, p_2, a_1, a_2, k_1,\ k_2$ are positive time-independent coefficients.

The parameters of the model (1), by analogy with the terminology of T. Saati [11], are defined as follows:

k_1, k_2 - coefficients of reaction or defence against the enemy's information influence;

a_1, a_2- indicators of the relative costs of creation of information weapons;

$g_1 g_2$- claims (aggressiveness) ratio, if positive, or goodwill ratio, if negative;

M_1, M_2- the cost of existing information support;

L_1, L_2- limit values of information depending on each party's resources;

p_1, p_2- coefficients of the degree of importance of information costs.

Model (1) admits the existence of four special solutions that determine the coordinates of equilibrium positions:

a) $N_1^p = N_1^*, N_2^p = N_2^*$ b) $N_1^p = N_1^*, N_2^p = L_2$

c) $N_1^p = L_1, N_2^p = N_2^*$ d) $N_1^p = N_2^*, N_2^p = L_2$

(2)

where N_1^*, N_2^*- is a solution to a system of linear algebraic equations.

Suppose the functions $u_1 = r_1^0(x_1 - x_2)$ i $u_2 = r_2^0(x_2 - x_1)$characterize the policy of each country in the field of information confrontation, where the variables $x_1 = N_1 - N_1^*$, $x_2 = N_2 - N_2^*$denote the values of deviations from equilibrium levels of information

power.Herer_1^0, r_2^0 - the stationary control parameters. Taking into account the form of the function $u_1, u_2$the system (1) takes the form:

$$\dot{x}_1 = M_1(\delta_1 - x_1)[1 - exp(p_1(a_1x_1 - k_1x_2))] + r_1^0(x_1 - x_2)$$

$$\dot{x}_2 = M_2(\delta_2 - x_2)[1 - exp(p_2(a_2x_2 - k_2x_1))] + r_2^0(x_2 - x_1) \quad (3)$$

The mere fact of transformation of the original system (1) by introducing influence factors leads to a change in the coordinate structure of equilibrium positions, but the trivial value $x_1^* = 0,\ x_2^* = 0$coincides with the coordinates of the equilibrium position of the original system (1). This means that the policy of information confrontation between countries is aimed at increasing the costs of information capacities of each party to the conflict and requires the attraction of additional own resources.

The following conclusions can be drawn: every state that is part of the global information space must develop a set of measures for its sustainable information development in the face of fierce competition, taking into account information security factors. This requires

- understanding of information confrontation as a phenomenon that has a certain logic of development;
- creation of mathematical models and, on their basis, scenarios of information warfare;
- development of quantitative and qualitative indicators of information threats in order to improve decision-making mechanisms in the systems of state and military administration;
- development of a software product based on the national research and production potential to ensure maximum protection against external influences on computer communications;
- analysis of the state and technical audit of all means of information warfare, taking into account their compliance with modern requirements;
- consolidation of the activities of public authorities, political parties and mass media in the field of political information to neutralize the negative psychological impact on society.

In Ukraine, information is divided into two types: secret and confidential. According to the Law of Ukraine "On Information", secret information includes such information, the disclosure of which would harm a person, society and the state [12], and which includes state or other secrets determined by law. The list of types of secret information is determined by the state and enshrined in law. State secrets include information in the field of defence, economy, science and technology, foreign relations, state security and law enforcement, the disclosure of which may harm the national security of Ukraine and which are defined in accordance with the procedure established by law as state secrets and are subject to state protection.

In order to neutralize the threats of information and psychological influence on the mass and individual consciousness, which can cause damage to public and industrial health, as well as abuse of freedom of the media, it is expedient and urgent to develop a unified state policy in the field of information and psychological security [13] and the relevant regulatory framework aimed at solving the following tasks

- coordination of activities of public authorities and public associations, delimitation of powers of public authorities and local self-government in the relevant area

- establishing reasonable balances of "checks and balances" between the need for free exchange of information and permissible restrictions on its dissemination;

- preservation of the unified information and spiritual space of Ukraine, traditional foundations of public morality;

- development of legal awareness and psychological culture of citizens in the field of psychological and information security;

- training the population in methods of self-defense against negative information influences, the basics of safe behaviour in the modern information environment;

- development and support of domestic production of means of protection against negative information and psychological influences;

- organization of international cooperation on information security;

- creation of a national system of licensing, certification, examination and control in the field of information security;

- development and adoption of standards in the field of information security;

- examination to identify negative information and psychological influences and mandatory licensing of activities and information security and certification of relevant means and methods.

Establishment and operation of an information security system involves the implementation of the main stages of system supervision. These include the following:

- direct implementation of mechanisms to ensure the required level of security;

- monitoring of the system and its response to incidents (events) and implementation of political security using effective tools for tracking various "intrusions"

- testing the security system through continuous improvement of the audit;

- improving the system.

Below is a structural diagram of the formation and functioning of the information security system (Fig 1). Ensuring the continuity of the state information security system is one of the main tasks of the state policy in

the field of national security in general and information security of the state in particular.

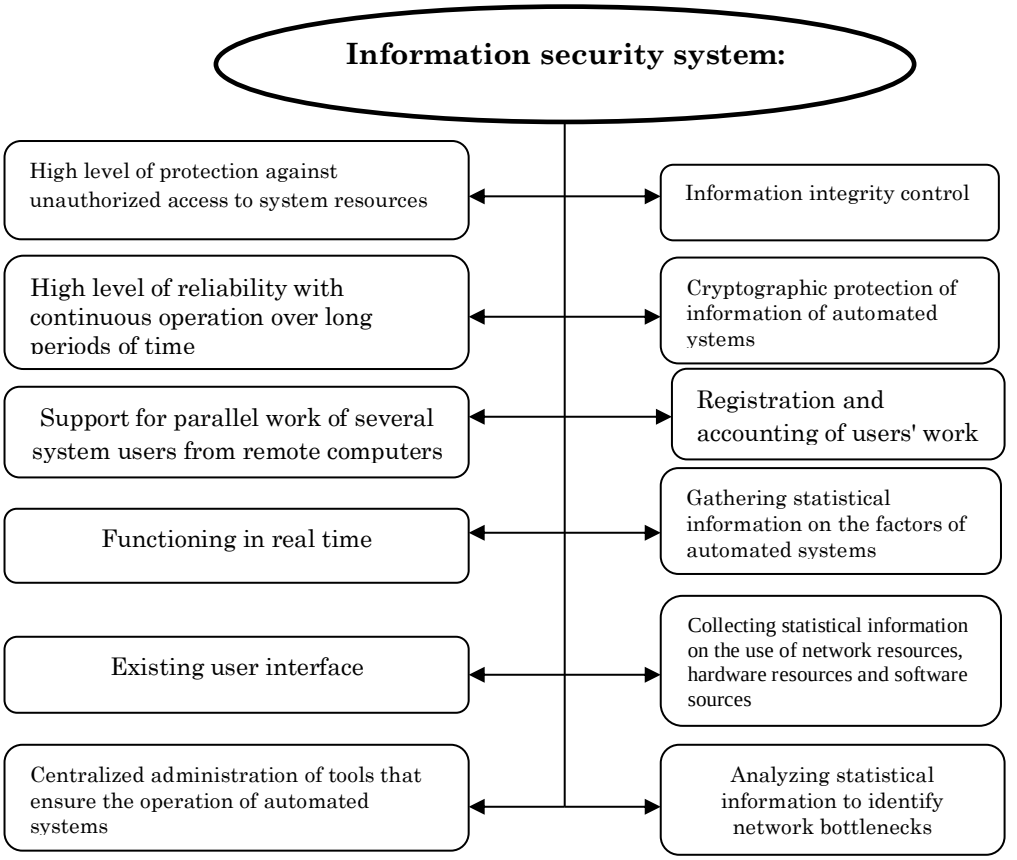

Fig. 1. Flowchart of formation and functioning of the information security system

Source: own elaboration

The first stage (1) is the stage of understanding the continuity of the state information security system. This phase is associated with the identification of critical points (objects) of protection. It is also about identifying the main internal and external threats that may become critical for the system. The second stage (2) is the stage of ensuring the system continuity strategy. At this stage, the tasks focus on identifying and selecting alternative solutions to restore the system in order to minimize threats to the main points of protection. The search for solutions balances the cost of protection systems with their effectiveness.

The third stage (3) is the development and implementation stage. At this stage, efforts are focused on structuring and documenting the

government continuity program. The fourth stage (4) is the development and "engraftment" of a continuous culture of information security of the state.

Analysing Fig.1, we can see that ensuring the continuity and operational transformation of the system depends on its ability to respond to new challenges and risks. The information security system provides for a high level of reliability and continuity of operation over long periods of time. In addition, it must have a high level of protection against unauthorized access to system resources. Its operation is carried out in real time, etc.

At this stage, the process of building an integrated system of ensuring the state's information security is launched. The fifth stage (5) is the stage of implementation, maintenance and audit of activities with the introduction of precise regulation (improvement, transformation) of the strategy of continuous functioning of the state information security system in the face of various crises. The sixth stage (6) is the stage of managing the state information security program by distributing and redistributing statuses and roles, which provides for responsibility, accountability, insurance (guarantees) and management in the context of implementing the overall plan for the continuity of the state information security system (Fig. 2).

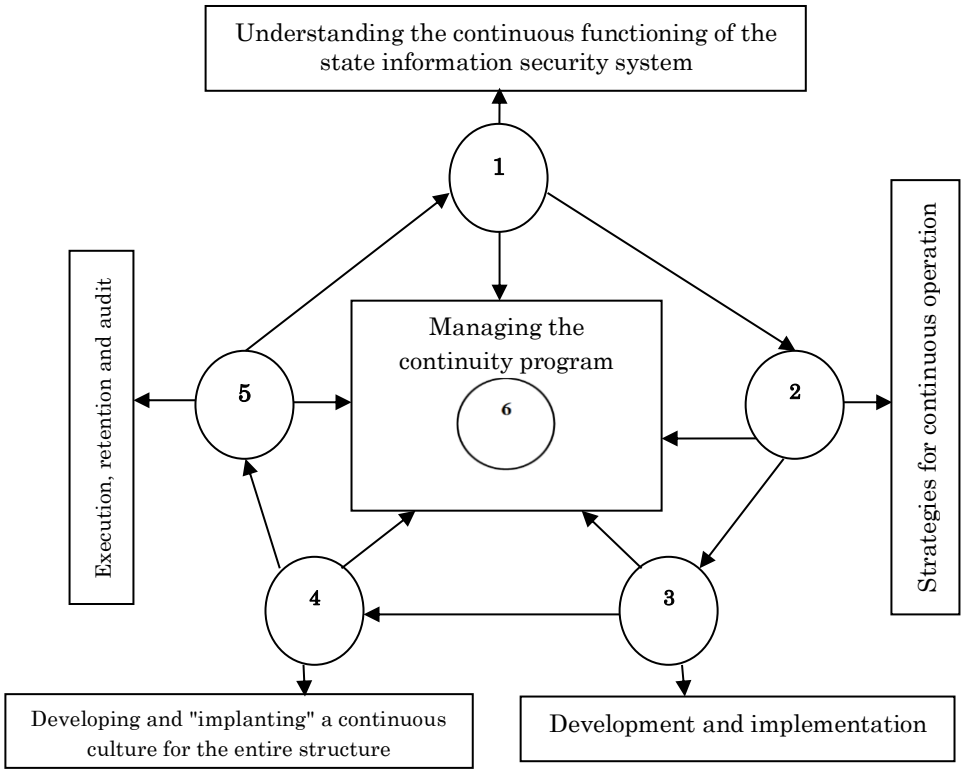

Fig. 2. The process of ensuring the continuity of the state information security system

Source: own elaboration

Analysing Fig. 2, we see that the process of ensuring such continuity can be divided into six main stages. Let us consider them more specifically. The national security of Ukraine in the information sphere should be considered as an integral integrity of four components – personal, public (social, commercial (corporate) and state security [14]. Therefore, in the process of determining the nature of risks, the following elements should be taken into account:

- a brief conceptual explanation to the interested parties of political security, its principles, standards and rules, consistent with the current legislation and principles of ensuring the continuity of the information security system of the individual, society, commercial (corporate) structures and the state;
- determination of objects and goals;
- determination of acceptable structures for establishing control over security objects, as well as risk assessment and risk management from the point of view of ensuring the interests of all subjects;
- defining the status and functional roles, expectations, and responsibilities of the involved entities, including reporting on events that pose potential threats.

In Ukraine, there is an objective need for such state and legal regulation of scientific, technological and information activities [15] that would meet the realities of the modern world and the level of development of information technologies, the norms of international law, but at the same time effectively protect Ukraine's own national interests. The most difficult tasks here are the following:

- harmoniously ensuring information security of the state, individual and society while simultaneously identifying urgent priorities;
- managing not only own interests, but also national interests of other countries;
- taking into account the realities of the modern world information space, which is moving towards indivisibility and the formation of a global information society.

Conclusions and prospects for further research. It is worth noting that it is critically important to implement the above schemes of ensuring the functioning of an effective system of information security of the state and the information protection system. To this end, it is advisable to develop the "Doctrine of National Information Security of Ukraine" with a clear definition of the areas (spheres) of responsibility of executive authorities for ensuring each stage of the state information security. The subject of constant attention within the time period defined by the doctrine

should be the revision of the list of "Threats to the National Security of Ukraine in the Information Sphere" both in terms of new threats and elimination of existing ones in the conditions of war, with the determination of the degree of possible consequences and intensity levels.

Given that the problem of ensuring the continuity of the state's information security system is a key one, the creation/restoration of the main areas of protection of the national security system in the information sphere is also a priority. The search for solutions should be dictated by the balance of the cost of such a protection system and its effectiveness. In order to implement this strategy in practice, a special body should be created integrated into the executive branch of power that would carry out its practical implementation and which, in addition to the implementation function, would be responsible for launching the process of building an integrated system of ensuring the state's information security, monitoring its implementation and formulating new strategies, taking into account the dramatic changes in the geostrategic situation of Ukraine, in the conditions of war.

ЛІТЕРАТУРА

1. Арістова І. В. Охорона права інтелектуальної власності в умовах цифрової економіки в Україні: *Матеріали міжнародної науково-практичної конференції «Захист прав, свобод і безпеки людини в інформаційній сфері в сучасних умовах» (м. Київ, 21 травня 2020 р.).* Вид-во НДІІП, 2020. С. 123-130. URL: https://drive.google.com/file/d/1N7R7286LEocplVEHNxBtIlqN4bjirMX4/view?usp=sharing.
2. Беляков К. І. Інформаційні технології як фактор терористичного акту. URL: http://www.mndc.naiau.kiev.UA/Gurnal/8text/g8_12.htm841/ 30.pdf.
3. Почепцов Г. Г. Інформаційна політика: навч. посібник. К. : Знання, 2006. 663 с.
4. Рамоне І. Глобальні трансформації та стратегії розвитку : монографія. К., 2010. 453 с.
5. Соснін О. Державне управління інформатизацією як виклик цивілізаційного зростання нації // *Зовнішні справи.* 2011. № 9. С. 38-41.
6. Олійник О. В. Позитивні та негативні впливи інформаційної революції на забезпечення інформаційної безпеки особи, суспільства, держави. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2011. № 25. С. 321-328.
7. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : монографія. Київ : Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.
8. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

9. Указ № 47/2017. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року. Про Доктрину інформаційної безпеки України. URL: https://www.president.gov.ua/documents/472017-21374.

10. Веб-сторінка інституту стратегічних досліджень. URL: http://www.niss.gov.ua.

11. Закон України "Про інформацію". URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.

12. Державна інформаційна політика. URL: http://merega.org.ua/law/projects/derzh polityka.

13. Захаренко К. В. Категорія "інформаційної безпеки" у вітчизняному науковому дискурсі. *Гуманітарний вісник ДВНЗ. Переяслав-Хмельницький державний педагогічний університет імені Григорія Сковороди.* 2015. № 37. С. 106-117.

14. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 08.09.2020).

REFERENCES

1. Aristova, I. V. (2020), Okhorona prava intelektualnoi vlasnosti v umovakh tsyfrovoi ekonomiky v Ukraini: *materialy mizhnarodnoi naukovo-praktychnoi konferentsii «Zakhyst prav, svobod i bezpeky liudyny v informatsiinii sferi v suchasnykh umovakh» (m. Kyiv, 21 travnia 2020 r.),* Vyd-vo NDIIP, s. 123-130, available at: https://drive.google.com/file/d/1N7R7286LEocplVEHNxBtIlqN4bjirMX4/view?usp= sharing.

2. Beliakov, K. I., Informatsiini tekhnolohii yak faktor terorystychnoho aktu, available at: http://www.mndc.naiau.kiev.UA/Gurnal/8text/ g8_12.htm841/30.pdf.

3. Pocheptsov, H. H. (2006), *Informatsiina polityka*: navch. posibnyk. Znannia, K., 663 s.

4. Ramone, I. (2010), *Hlobalni transformatsii ta stratehii rozvytku*: monohrafiia. K., 453 s.

5. Sosnin, O. (2011), Derzhavne upravlinnia informatyzatsiieiu yak vyklyk tsyvilizatsiinoho zrostannia natsii, *Zovnishni spravy,* № 9, s. 38-41.

6. Oliinyk, O. V. (2011), Pozytyvni ta nehatyvni vplyvy informatsiinoi revoliutsii na zabezpechennia informatsiinoi bezpeky osoby, suspilstva, derzhavy, *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka),* № 25, s. 321-328.

7. Tykhomyrov, O. O. (2014), *Zabezpechennia informatsiinoi bezpeky yak funktsiia suchasnoi derzhavy*: monohrafiia. Tsentr navch.-nauk. ta nauk.-prakt. vyd. NA SB Ukrainy, Kyiv, 2014, 196 s.

8. Konstytutsiia Ukrainy: Zakon Ukrainy vid 28.06.96 r. № 254k/96-VR, available at: https://zakon.rada.gov.ua/laws/show/254k/96-vr#Text.

9. Ukaz № 47/2017. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku. Pro Doktrynu informatsiinoi bezpeky Ukrainy, available at: https://www.president.gov.ua/documents/472017-21374.

10. Veb-storinka instytutu stratehichnykh doslidzhen, available at: http://www.niss.gov.ua.

11. Zakon Ukrainy "Pro informatsiiu", available at: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.

12. Derzhavna informatsiina polityka, available at: http://merega.org.ua/law/projects/derzhpolityka.

13. Zakharenko, K. V. (2015), Katehoriia "informatsiinoi bezpeky" u vitchyznianomu naukovomu dyskursi. *Humanitarnyi visnyk DVNZ.* Pereiaslav-Khmelnytskyi derzhavnyi pedahohichnyi universytet imeni Hryhoriia Skovorody, № 37, s. 106-117.

14. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.18 r. № 2469-VIII, available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text.