

DOI: 10.46340/eppd.2022.9.2.5

Andrii Pravdiuk, PhD in Law

ORCID ID: <https://orcid.org/0000-0002-5248-8111>

Vinnitsia National Agrarian University, Ukraine

PROBLEMS OF LEGAL REGULATION OF THE INFORMATION SECURITY SYSTEM IN UKRAINE

The article highlights the current problems of legal regulation of the information security system of Ukraine and suggests ways to overcome them. Emphasis is made on the fact that information threats (a growing number of large-scale disinformation campaigns, information wars that threaten Ukraine's democracy and sovereignty, a significant strengthening of the role of social networks and their influence in cyberspace, cybercrime, cyberterrorism, etc.) pose a number of global challenges. Under such conditions, the formation of an information security system is a necessary condition for the existence of a modern information society. The main scientific approaches to the formation of regulatory and legal support of the information security system of Ukraine are considered. The analysis of the concept of information security system is carried out and the main information threats are considered. It is noted that information security is an important component of national security.

The article analyzes the current national legislation governing the field of information security. It is noted that the mechanism of legal regulation of information security, in general, corresponds to international standards, principles, and norms of democracy. However, the rapid development of information technology and growing threats to Ukraine's national security determine the need for continuous improvement of the regulatory framework. The main shortcomings of the legislation in the field of information security are analyzed.

It is concluded that in order to improve the legal regulation of the information security system, clear structuring of the regulatory system, elimination of legislative gaps, and generalization of legal information security principles, it is necessary to codify information legislation. The formation of the national legal framework of the information security system will help strengthen the national security of our state and strengthen guarantees of respect for human and civil rights and freedoms.

Keywords: information security, information security system, information threats, cybersecurity, national security.

Formulation of the problem. Information security is an important component of the national security. Development of the information space, widespread use of information resources and technologies, development of the information infrastructure significantly affect the level of socio-economic, scientific, technical and cultural development of modern society. Therefore, the development of Ukraine as a sovereign, democratic, legal and economically stable state is possible due to information security. The growth of information threats (e.g. a growing number of large-scale disinformation campaigns, Russia's information policy, which is a threat to democracy and sovereignty of our state, significant strengthening of the role of social networks and their influence in cyberspace, cybercrime, cyberterrorism, etc.) causes a number of global challenges. To counteract information threats, one of the main goals of Ukraine is to improve legal regulation of legal relations in the field of information security.

The purpose of the article is to investigate current issues of legal regulation of the information security system in Ukraine and suggest possible ways to solve them.

Analysis of recent research and publications. Problems of the legal regulation of information security were studied by such researchers as V. Antoniuk, V. Bohush, V. Bryzhko, S. Hutsu, O. Dzioban, K. Zakharchenko, O. Zolotar, R. Kaliuzhnyi, O. Lytvynenko, V. Lipkan, O. Oliinyk, L. Nalyvaiko, V. Petryk, O. Ryzhuk, T. Tkachuk and others. However, considering rapid development of the information society and a growing impact of information threats to our country, the problems of legal regulation of information security are very relevant and require further research.

Presentation of the main material. Ukraine is experiencing the process of establishing a national information security system, which requires appropriate regulatory and legal support and formation of the qualitative legal framework. An important step towards the formation of such a legal framework is the adoption of the Information Security Strategy in December 2021, the main purpose of which is to ensure information security of Ukraine, its information space, support of social and political stability by information means and measures, support of the state defense, protection of state sovereignty, territorial integrity, democratic constitutional order, support for the rights and freedoms of every citizen¹.

Information security is an important component of the national security, which includes control over the spread of misinformation, protection of information space, counteraction to information threats, promoting the functioning of the information society and at the same time guarantees respect for all constitutional human and civil rights.

Information security is a systemic and complex phenomenon formed under the influence of various external and internal factors, such as the political situation, potential or real threats, the state and level of development of the information society. As noted by O. Zolotar, information security is a complex, dynamic, integrated social system, the components of which are the subsystems of security of the individual, state and society. It is the interdependent, systemic information unity of the latter that constitutes a qualitative certainty aimed to protect vital interests of man, society and the state, to ensure their competitive, progressive development².

At the present stage of Ukraine's development in conditions of building information society, the problem of information security and creation of legal mechanisms for its regulation is a strategic goal.

Modern challenges of the state caused by the influence of a complex of socio-demographic, economic, political, legal, informational, psychological and technological factors require systemic approaches and changes. The current state of the legislative framework for the national security and information security, as its component, can be defined as the state of the system, which is in the process of formation, and therefore inevitably has the qualities of a transitional stage.

The Information Security Strategy defines information security as a state of protection of the state sovereignty, territorial integrity, democratic constitutional order, other vital interests of man, society and the state, which adequately ensures constitutional and human rights to collect, store, use and disseminate information, access to reliable and objective information, there is an effective system of protection and counteraction to harm through the spread of negative information influences, including coordinated dissemination of inaccurate information, destructive propaganda, other information operations, unauthorized dissemination, use and violation of information integrity, restricted access³. In our opinion, this definition is quite complete and reflects the essence of this multifaceted and complex phenomenon.

The Doctrine of Information Security of Ukraine identifies the following threats to information security of the country: "special information operations aimed at undermining defense capabilities, demoralizing the personnel of the Armed Forces of Ukraine and other military formations, provoking extremist manifestations, fueling panic, aggravating and destabilizing socio-political and socio-economic situation, incitement of interethnic and interfaith conflicts in Ukraine; special information operations conducted by the aggressor state in other states in order to create a negative image of Ukraine in the world; information expansion of the aggressor state and the structures controlled by it, in particular by expanding its own information infrastructure on the territory of Ukraine and in other states; information domination of the aggressor state in the temporarily occupied territories; insufficient development of the national information infrastructure, which limits Ukraine's ability to effectively combat information aggression and actively act in the information sphere to realize the national interests of Ukraine; inefficiency of the state information policy, imperfection of the legislation concerning the regulation of public relations in the information sphere, uncertainty of the strategic narrative, insufficient level of media culture of the society; spreading calls for radical action, propaganda of isolationist and autonomist concepts of regional coexistence in Ukraine"⁴.

¹ *Стратегія інформаційної безпеки, 2021* (Президент України). *Офіційний сайт Верховної Ради України* <<https://zakon.rada.gov.ua/laws/show/685/2021#Text>> (2022, January, 03).

² Золотар, О. (2018). *Інформаційна безпека людини: теорія і практика*. Київ: АртЕк, 154-155.

³ *Стратегія інформаційної безпеки, 2021* (Президент України). *Офіційний сайт Верховної Ради України* <<https://zakon.rada.gov.ua/laws/show/685/2021#Text>> (2022, January, 03).

⁴ *Доктрина інформаційної безпеки України, 2017* (Президент України). *Офіційне інтернет-представництво Президента України* <<https://www.president.gov.ua/documents/472017-21374>> (2022, February, 05).

According to Ostroukhov V., Prysiazhniuk M., Farmahei O., Chekhovska M., there can be distinguished three main types of information security depending on the subject: information security of the individual, information security of society and information security of the state.

Thus, information security of the state is the status of its security and information development, when information actions, special information operations, information wars, information terrorism, illegal withdrawal of information by special technical means and computer crime do not cause significant harm to national interests. A necessary level of information security of the state is provided by creating conditions for harmonious development of information infrastructure of the state, realization of constitutional human rights and freedoms in the interests of the state, i.e. strengthening the constitutional order, sovereignty and territorial integrity of the country, establishing political and social stability, economic development.

Information security of society is an opportunity for society and its individual members to freely exercise their constitutional rights related to the free receipt, processing, creation and dissemination of information, as well as the degree of their protection from destructive information influence. The necessary level of information security of society is provided by a set of political, economic, organizational measures aimed at preventing, identifying and neutralizing those circumstances, factors and actions that may damage or harm the information rights, needs and interests of the country and its citizens. It is worth noting that the information security of the individual and society are closely linked. Information security of society and individuals depends on the level of: intelligence, special theoretical and practical training; critical thinking, moral and spiritual improvement; harmonious development of personality in society; technical means of protection.

Researchers treat information security of a person as a state of protection of a person's psyche and health from destructive information influence, which leads to inadequate perception of reality and (or) deterioration of his/her physical condition. A necessary level of information security of the individual is provided by the level of person's training at which protection and realization of its vital interests and harmonious development is reached irrespectively of information threats available; the ability of the state to create conditions for the harmonious development and meeting human needs for information, regardless of the information threats available; guarantee of the development and use of the information environment in the interests of man; protection from various kinds of information threats¹.

Information security is based on three structural elements. They are as follows: information security in the field of human and civil rights and freedoms (management of real or potential threats to ensure the right to information); information and psychological security (management of real or potential threats that may harm the human psyche, society); information and technical security (management of potential or real threats to protect computer and telecommunications technologies)².

According to Perun T., information security should be considered as a system of public relations that expresses the relationship between the interests of the individual, society and the state in the field of information and legal protection, covering the state of protection of the individual, society and the state in the information space, information resources of the state, information and information resources, information and telecommunication infrastructure from possible internal and external threats in the conditions of association of Ukraine and the EU and formation of information society³.

Legal support of information security can be defined as a holistic system of legal regulation of public relations that arise when countering threats to the national security of Ukraine in the information sphere. Thus, this legal phenomenon has its own subject of legal regulation. The peculiarities of legal relations regulated by it arise primarily from the specifics of the information sphere of society, the content of which involves social activities on the creation, dissemination, transformation and consumption of information. At the same time, information and relevant infrastructure should be the object of relations related to such activities⁴.

¹ Остроухов, В., Присяжнюк, М., Фармагей, О., Чеховська, М. (2021). *Інформаційна безпека*. Київ: Ліра, 11.

² Панченко, О. (2020). *Державне управління інформаційною безпекою в епоху турбулентності*. Київ: Національний університет цивільного захисту України, 80-81.

<<https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disPanchenko.pdf>> (2022, February, 05).

³ Перун, Т. (2019). *Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні*. Львів: Національний університет «Львівська політехніка», 4 <<https://lpnu.ua/sites/default/files/2020/dissertation/1683/dysertaciyanazdobuttyuanaukovogostupenyakandydataurydychnyh naukperunats.pdf>> (2022, February, 05).

⁴ Ткачук, Т. (2019). *Правове забезпечення інформаційної безпеки в умовах євроінтеграції України*. Ужгород: ДВНЗ «Ужгородський національний університет», 126 <<https://www.uzhnu.edu.ua/uk/infocentre/get/19617>> (2022, February, 05).

Legal mechanisms supporting information security should regulate the relationship between the subjects of information security, determine their rights, duties and responsibilities; regulate the actions of the subjects of information security at all levels, namely people, society, state; establish the procedure for the application of legal means to ensure information security.

According to O. Panchenko, the system of legal regulation of information security, in its turn, includes a number of legal norms regulating relations in this area, legal relations arising based on the application of legal norms, and relevant law enforcement acts¹.

Legal norms form the basis for ensuring information security and determine the effectiveness of the state, society and individual citizens in protecting the national interests of Ukraine in the information sphere. This database also includes norms of international treaties of Ukraine, laws of Ukraine, acts of the President of Ukraine, government resolutions, normative acts of public authorities that regulate relations in this area.

Legal regulation of information security is the legal regulation of people's behavior, which aims to prevent manifestation of threats to the objects of information security or minimize negative consequences of manifestation of these threats. This area is formed by aggregate social relations that have the following main features: belonging to the information relationship or dependence on them; connection with the objects of national interests in the information sphere; dependence of manifestations of security threats on the objects of national interests in the information sphere. The targeted orientation of information security is determined by a set of public relations related to information and information infrastructure in various spheres of society and public administration, implementation of the legal status of information entities, manifestations of threats that could harm national interests².

Legal functioning of the national system of information security of Ukraine is provided by the Constitution of Ukraine, the Law of Ukraine "On Information", the Law of Ukraine "On Information Protection in Information and Telecommunication Systems", the Law of Ukraine "On the National Security of Ukraine", the Law of Ukraine "On Personal Data Protection", The Law of Ukraine "On State Secrets", the Law of Ukraine "On the National Informatization Program", "On Public Procurement", "On Information"; "On Electronic Documents and Electronic Document Management", "On Electronic Communications", "On Basic Principles of Cyber Security of Ukraine", Decree of the President of Ukraine "On the Doctrine of Information Security of Ukraine", the Concept of the National Security of Ukraine and other legislative and legal acts regulating relations in the information sphere.

Information security in Ukraine is guaranteed by the Constitution of Ukraine, and Article 17 declares that "protection of the sovereignty and territorial integrity of Ukraine, support of its economic and information security are the most important functions of the state, the concern of all Ukrainian people"³.

The system of legal regulation of information security in general corresponds to international standards, principles and norms ensuring human and civil rights and freedoms, which testifies to its developed nature, in particular, the right to freedom of speech, receipt and dissemination of information. However, rapid development of information technology (along with the growth of violations of legislation in the information sphere, encroachment on human and civil rights and freedoms) and growing threats to the national security of Ukraine (war of the Russian Federation, hacker attacks on strategic sites, etc.) are becoming indicators of imperfections in legal bases for the regulation of public relations in the field of information security, require constant updates of the legal framework for the national security in the information sphere.

An important component of information security is a comprehensive protection of these rights and legitimate interests from the unpredictable and harmful effects of certain information technology environment created by society itself, i.e. from side effects of technological and organizational processes on the individual (person and citizen), society, and the state. At the same time, the information security system is designed to neutralize these negative effects on people and help maintain the stability of society and the state, which institutions, in turn, must ensure this neutralization. In other words, the main feature of the state of security

¹ Панченко, О. (2020) Державне управління інформаційною безпекою в епоху турбулентності. *Національний університет цивільного захисту України*, 132 <<https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disPanchenko.pdf>> (2022, February, 05).

² Ткачук, Т. (2019). *Правове забезпечення інформаційної безпеки в умовах євроінтеграції України*. Ужгород: ДВНЗ «Ужгородський національний університет», 104 <<https://www.uzhnu.edu.ua/uk/infocentre/get/19617>> (2022, February, 05).

³ *Конституція України*, 17, 1996 (Верховна Рада України). *Офіційний сайт Верховної Ради України* <<https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text,%202022,%2022%20січня>> (2022, February, 05).

in the information sphere (information security) is the optimal balance of interests of man, society and the state. Factors ensuring information security of the state are guaranteeing: 1) security of public access information, communication networks, information and telecommunication systems, technical and software means of information manipulation, access to information; 2) confidentiality of information with limited access; 3) protection of the individual, society and the state from the harmful effects of certain types of information (in this case it is not about information classified as restricted, but about the types that can harm these subjects of information relations)¹.

That is why Ukraine's information security is currently becoming a strategic goal of the state. An extremely important step in determining the basic principles of forming an effective legal framework is the Information Security Strategy. The strategy identifies current challenges and threats to Ukraine's national security in the information sphere, strategic goals and objectives aimed at counteracting such threats, protection of individuals' rights to information and protection of personal data.

The legal basis of the Strategy is the Constitution of Ukraine, laws of Ukraine, Ukraine's National Security Strategy approved by the Decree of the President of Ukraine on September 14, 2020 No 392, as well as international treaties approved by the Verkhovna Rada of Ukraine. The Strategy presents the analysis of global and national challenges and information threats, identifies the main directions and objectives of the Strategy.

One of the most important goals is to counteract misinformation and information operations, first of all, those of the aggressor state, "aimed at eliminating Ukraine's independence, overthrowing the constitutional order, violating the sovereignty and territorial integrity of the state, propaganda of war, violence, cruelty, incitement to national, interethnic, racial, religious hatred and enmity, acts of terrorism, encroachment on human rights and freedoms".

To ensure the implementation of this goal, it is planned to create a system aimed to combat disinformation and hostile or criminal information operations; strengthen responsibility for disseminating unreliable information (misinformation); introduce effective mechanisms for detecting, recording, restricting access and/or deleting information from the Ukrainian segment of the Internet, the placement of which is restricted or prohibited by law; ensure effective interaction of state bodies, local self-government bodies and civil society institutions when forming and implementing the state policy in the information sphere, etc.

One of the important strategic goals of information security is to ensure a comprehensive development of Ukrainian culture and establishment of Ukrainian civic identity. Based on the above-mentioned, it becomes obvious that there is a need to make appropriate changes to the legislation in the field of Ukrainian culture, e.g. to ensure the use of the Ukrainian language in all spheres of public life.

Enhancement of the level of media culture and media literacy of society as a strategic goal of information security will ensure "effective resistance to the aggressor state and resilience to a wide range of threats, including those in the information sphere", as stated in the Strategy².

Ensuring respect for the rights of individuals to collect, store, use and disseminate information, freedom of expression, protection of privacy, access to objective and reliable information, and protection of journalists' rights and security during their professional duties, combating the dissemination of illegal content is an important strategic goal in the field of information security of man and citizen. Its implementation is aimed to provide constitutional guarantees of man and citizen in the field of information. The priority tasks for the legislator are to improve the legislation on access to public information, comply legal regulations with the international acts that are mandatory for Ukraine and improve the legislation on personal data protection, as well as introduce effective mechanisms ensuring its implementation, protection of information space of Ukraine from illegal content.

Another strategic goal is the information reintegration of Ukrainian citizens living in the temporarily occupied territories and adjacent territories of Ukraine to the all-Ukrainian information space, restoration of their right to information.

Formation of the national information security system is impossible without the creation of an effective system of strategic communications. Therefore, one of the strategic goals is to create and develop a system of strategic communications, ensure effective information interaction and dialogue between public authorities, local governments and society as well as effective development of the international information activities in Ukraine.

¹ Довгань, А. Ткачук, Т. (2019) Концептуальні засади забезпечення інформаційної безпеки. *Інформація і право*, 88-89 <http://ippi.org.ua/sites/default/files/12_11.pdf> (2022, February, 05).

² *Стратегія інформаційної безпеки, 2021* (Президент України). *Офіційний сайт Верховної Ради України* <<https://zakon.rada.gov.ua/laws/show/685/2021#Text>> (2022, January, 23).

Development of the information society and raising the level of the dialogue culture as a strategic goal will be ensured through public discussion of current issues of social development; development of the national network of television and radio broadcasting by the state operator, and distribution of Ukrainian information content to them; promotion of the creation of broadcasting system of territorial communities, which will ensure the expansion of communication opportunities and reduce conflicts within territorial communities, ensuring their information; stimulation of innovations and support of comprehensive development and protection of the national information infrastructure, in particular its telecommunication component, as a set of various information (automated) systems, information resources, telecommunication (electronic communication) networks, means of communication and information flow management, organizational and technical structures, mechanisms that ensure their functioning, etc¹.

It should be noted that the document defines a number of tasks aimed to improve legal regulation of information security and comply provisions of legal acts with the norms of international acts that are mandatory for Ukraine to be implemented through systematic reviewing and amending relevant legislation and other regulations in information sphere.

The Strategy implementation should result in the protected information space of Ukraine; effective functioning of the system of strategic communications; effective counteraction to the distribution of illegal content; a sustainable process of information reintegration of Ukraine's citizens living in the temporarily occupied territories of Ukraine, and the spread of Ukrainian television and radio broadcasting in the territories of Ukraine adjacent to the temporarily occupied territories; significant increase in the level of media culture and media literacy of the population; observance of the constitutional rights of a person to free express of their views and beliefs, protection of privacy; protection of journalists' rights; and formation of Ukrainian civic identity.

Since information threats for the vital interests of the man, society and state are concentrated in cyberspace, the Cyber Security Strategy of Ukraine 2021 became an important step towards the improvement of legal regulation of information security. This document defines that cybersecurity as one of the priorities of the national security².

The Cyber Security Strategy identifies the main national challenges and threats in cyberspace, in particular, active use of cyber means in the international competition; rapid progressive changes in the information and communication technologies, militarization of cyberspace and development of cyber weapons, impact of the COVID-19 pandemic, introduction of new technologies without cybersecurity measures, aggression of the Russian Federation against Ukraine in cyberspace, cybercrime, cyber espionage, cyberterrorism, etc.

One of the reasons for the implementation of cyber threats is the imperfection of the legal framework in the field of cybersecurity, as well as its obsolescence in the field of information protection, slow implementation of the European legislation and low level of legal responsibility for violating legislation in this area.

A strategic goal of the Cyber Security Strategy is to build up the national cybersecurity system. Priorities of ensuring cyber security of Ukraine are as follows: securing cyberspace in order to protect the state sovereignty and to develop the society; protection of the rights, freedoms and legitimate interests of Ukraine's citizens of in cyberspace; European and Euro-Atlantic integration in the field of cybersecurity. Strategic goals are determined in accordance with the basic principles of building the national cybersecurity system.

The most important ones include effective cyber defense, effective counteraction to intelligence and sabotage activities in cyberspace and effective counteraction to cybercrime; development of asymmetric tools, reliable cyber defense, professional development, cyber-friendly society, scientific and technical support of cybersecurity, secure digital services, international cooperation in this field, etc.

To ensure information security in cyberspace, strategic objectives are provided to improve legal framework of information security, in particular, "at the legislative level regulate the issue of complete involvement of the private sector and civil society in measures aimed to deter destructive activities in cyberspace; ... increase the efficiency of the system of protection of citizens' personal data through harmonization of Ukraine's legislation with the relevant EU legislation and strengthening the responsibility

¹ *Стратегія інформаційної безпеки, 2021* (Президент України). *Офіційний сайт Верховної Ради України* <<https://zakon.rada.gov.ua/laws/show/685/2021#Text>> (2022, January, 23).

² *Стратегія кібербезпеки України, 2021* (Президент України). *Офіційне інтернет-представництво Президента України* <<https://www.president.gov.ua/documents/4472021-40013>> (2022, February, 01).

for violating the established requirements; ... regulate the issue of public-private partnership in the field of cybersecurity at the legislative level having defined the forms and methods of such partnership, strengthened mutual trust and provided possibility of implementing pilot projects in this area", etc¹.

A countermeasure to information threats is Ukraine's integration into the global and regional European information space; integration into international information as well as information and telecommunication systems and organizations; creation of the personal national model of information space and ensuring development of information society; modernization of the entire information security system of the state, formation and implementation of effective information policy and improvement of legislation on information security, harmonization of the national legislation with international standards and effective legal regulation of information processes².

The balance achieved at a certain time in the system of legal norms related to information relations, including those in the field of information security, is not absolute. Remedies are always limited by the level of social development. The goals set by the legislator are ideal in essence and are not always consistent with the level of development, implementation and use of information technology.

This leads to inconsistencies in the relationship between the goals and means chosen to achieve them. Intensification of the law-making process on the regulation of legal relations in the information sphere is significantly complicated by the lack of a coherent system of regulation of legal relations and rapid development of this segment of legislation³.

Based on the analysis of the above-mentioned documents, the main steps aimed to improve the regulatory framework of the information security system involve preparation of new and amending current laws and regulations governing relations in the field of protection of vital interests of the man, society and state from internal and external threats; protection of sovereignty, support of political and social stability, territorial integrity of Ukraine; protection of critical information infrastructure; ensuring the development of information and communication technologies; ensuring Ukraine's participation in the international information security system.

Improvement of the legal framework of information security should be based on the following key principles: the principle of formation and application of norms of international law as an integral part of the legal system of Ukraine; the principle of ensuring the balance of interests of the man, society and state; coordination of activities of public authorities in order to improve legal framework for information security⁴.

In our opinion, considering a large number of regulations in the field of information security, the need to improve them through various external and internal influences on the development of the information society, the need for a systematic approach to lawmaking, building an effective system of information legislation, the issue of codification of information legislation is quite urgent. The problem of codification of information legislation has been broadly discussed by the researchers and experts for decades, but it has not been resolved yet. However, it is the information code that can become a legal basis for creating an effective information security system, which will determine the basic norms and principles of legal regulation of public information relations in the information society and global information space, including information security system. Legislation and bylaws should be based on the basic norms and principles of the code, but at the same time be dynamic and take into account rapid changes in the information society and external influences.

Conclusions. Ukraine's information security system is currently requiring effective regulatory support. Information security is guaranteed by the Constitution of Ukraine and regulated by the current legislation. However, under current conditions of the information society development, the growth of external and internal information threats to Ukraine's existence as a sovereign and democratic state, respect for human

¹ *Стратегія кібербезпеки України, 2021* (Президент України). *Офіційне інтернет-представництво Президента України* <<https://www.president.gov.ua/documents/4472021-40013>> (2022, February, 01).

² Ільницька, У. (2016). Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*, 1, 30 <<https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf>> (2022, February, 05).

³ Малашко, О. (2020). Нормативно-правове забезпечення інформаційної безпеки в Україні. *Міжнародний науковий журнал «Інтернаука»*, 14 (94), 30 <<http://dspace.lvduvs.edu.ua/handle/1234567890/3369>> (2022, February, 05).

⁴ Ткачук, Т. (2019). *Правове забезпечення інформаційної безпеки в умовах євроінтеграції України*. Ужгород: ДВНЗ «Ужгородський національний університет» <<https://www.uzhnu.edu.ua/uk/infocentre/get/19617>, 118> (2022, February, 05).

and civil rights and freedoms, there is a problem of improving the legal framework that would ensure reliable information security system. An important step towards the formation of such a legal framework is the adoption of the Information Security Strategy, which is a strategic guideline for reforming information security legislation until 2025.

In our opinion, codification of information legislation is necessary for effective improvement of the normative and legal regulation of the information security system, clear structuring of the system of normative and legal acts, elimination of legislative gaps, consolidation of general principles of information relations, uniform parameters of legal framework of information security.

Formation of the national legal framework of the information security system, i.e. bringing information security relations in line with international standards, will strengthen national security of our state as well as guarantees of human and civil rights and freedoms in the democratic state governed by the rule of law.

References:

1. *Doktryna informatsiinoi bezpeky Ukrainy, 2017* (Prezydent Ukrainy) [Doctrine of Information Security of Ukraine, 2017 (President of Ukraine)]. *Ofitsiine internet-predstavnytstvo Prezidenta Ukrainy* [Official Internet Representation of the President of Ukraine] <<https://www.president.gov.ua/documents/472017-21374>> (2022, February, 01). [in Ukrainian].
2. Dovhan, A., Tkachuk, T. (2019) Kontseptualni zasady zabezpechennia informatsiinoi bezpeky [Conceptual principles of information security]. *Informatsiia i pravo, 1* (28), 86-99. [Information and law] <http://ippi.org.ua/sites/default/files/12_11.pdf> (2022, February, 01) [in Ukrainian].
3. Ilnytska, U. (2016). Informatsiina bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydii nehatyvnyim informatsiino-psykholohichnym vplyvam [Information security of Ukraine: modern challenges, threats and mechanisms for counteracting negative information and psychological influences]. *Politychni nauky* [Political science], 1, 27-32 <<https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf>> (2022, February, 01). [in Ukrainian].
4. *Konstytutsiia Ukrainy, 17 1996* (Verkhovna Rada Ukrainy) [Constitution of Ukraine, 17, 1996 (Verkhovna Rada of Ukraine)]. *Ofitsiinyi sait Verkhovnoi Rady Ukrainy* [Official site of the Verkhovna Rada of Ukraine]. <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (2022, January, 23). [in Ukrainian].
5. Malashko, O. (2020). Normatyvno-pravove zabezpechennia informatsiinoi bezpeky v Ukraini [Regulatory and legal support of information security in Ukraine]. *Mizhnarodnyi naukovi zhurnal Internauka* [International Scientific Journal Internauka], 94 <<http://dspace.lvduvs.edu.ua/handle/1234567890/3369>> 14 > [in Ukrainian].
6. Ostroukhov, V. Prysiashniuk, M. Farmahei, O. Chekhovska, M. (2021). *Informatsiina bezpeka* [Information security]. Kyiv: Lira. [in Ukrainian].
7. Panchenko, O. (2020) Derzhavne upravlinnia informatsiinoiu bezpekoiu v epokhu turbulentnosti [Public administration of information security in the era of turbulence]. *Natsionalnyi universytet tsvyvilnoho zakhystu Ukrainy* <<https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disPanchenko.pdf>> (2022, February, 01). [in Ukrainian].
8. Perun, T. (2019). Administrativno-pravovyi mekhanizm zabezpechennia informatsiinoi bezpeky v Ukraini [Administrative and legal mechanism for ensuring information security in Ukraine]. Lviv: Natsionalnyi universytet «Lvivska politekhnika» <https://lpnu.ua/sites/default/files/2020/dissertation/1683/dysertaciyanzdobuttya_naukovogostupenyakandydatayurydychnyh_nauk_perunats.pdf> (2022, February, 01). [in Ukrainian].
9. *Stratehiia informatsiinoi bezpeky, 2021* (Prezydent Ukrainy) [Information Security Strategy, 2021 (President of Ukraine)]. *Ofitsiinyi sait Verkhovnoi rady Ukrainy* [Official site of the Verkhovna Rada of Ukraine] <<https://zakon.rada.gov.ua/laws/show/685/2021#Text>> (2022, January, 13). [in Ukrainian].
10. *Stratehiia kiberbezpeky Ukrainy, 2021* (Prezydent Ukrainy) [Cybersecurity Strategy of Ukraine, 2021 (President of Ukraine)]. *Ofitsiine internet-predstavnytstvo Prezidenta Ukrainy* [Official Internet Representation of the President of Ukraine] <<https://www.president.gov.ua/documents/4472021-40013>> (2022, February, 01). [in Ukrainian].
11. Tkachuk, T. (2019). Pravove zabezpechennia informatsiinoi bezpeky v umovakh yevrointehratsii Ukrainy. [Administrative and legal mechanism for ensuring information security in Ukraine]. DVNZ «Uzhhorodskiy natsionalnyi universytet», <https://www.uzhnu.edu.ua/uk/infocentre/get/19617> (2022, February, 01). [in Ukrainian].
12. *Zakon pro vykonavche provadzhennya, 1999* (Verkhovna Rada Ukrainy). [Law on Enforcement 1999 (Verkhovna Rada of Ukraine)]. *Ofitsijnyj visnik Ukrajinny* [Official Bulletin of Ukraine], 19, 194. [in Ukrainian].
13. Zolotar, O. (2018). *Informatsiina bezpeka liudyny: teoriia i praktyka* [Human information security: theory and practice]. Kyiv: ArtEk [in Ukrainian].