

УДК 327(477):005.575.659.4

Lesya Kachkovska,

PhD in History, Associate Professor of the Department of Museology,
Monument Studies, and Information-Analytical Activities,

Lesya Ukrainka Volyn National University,

kachkovska.lesja@vnu.edu.ua

ORCID ID: 0000-0003-3206-1580;

Yevhenija Voznyuk,

PhD in Political Science, Associate Professor, Head of the Department
of International Communications and Political Analysis,

Lesya Ukrainka Volyn National University,

vozniukjane.vippo@gmail.com

ORCID ID: 0000-0002-7828-7430

DOI 10.29038/2524-2679-2024-01-85-102

COUNTERING INFORMATION THREATS IN UKRAINE: CURRENT ISSUES FOR SOLVING AT THE STATE LEVEL

The article analyses the importance of information as a special means of waging war in the modern communication environment. Attention is focused on legislative documents, the main source of legal protection of information relations. The activity of domestic state authorities regarding the security of the information space against internal and external threats is characterized. Two approaches are applied to analyse the category “national security”: the first considers national security through the prism of “national interests”; the second connects national security with the system of basic national values at both the structural and functional levels. Summarizing the changes made to the legislative documents, the vector of improvement and harmonization of Ukrainian legislation and regulation on information security with the best global practices has been proven. It was determined that the main components of the information security policy are regulating information relations to ensure the rights and freedoms of citizens, health and morality, information relations in the field of commerce, information relations, territorial integrity and public order and maintenance of legality.

Key words: information, information security, hybrid war, law, legislator, threat, influence, society.

Леся Качковська,

Волинський національний університет імені Лесі Українки,
ORCID ID: 0000-0003-3206-1580;

Євгенія Вознюк,

Волинський національний університет імені Лесі Українки,
ORCID ID: 0000-0002-7828-7430

ПРОТИДІЯ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ В УКРАЇНІ: АКТУАЛЬНІ ПИТАННЯ ДЛЯ ВИРІШЕННЯ НА ДЕРЖАВНОМУ РІВНІ

У статті проаналізовано значення інформації як спеціального засобу ведення війни в сучасному комунікаційному середовищі. Акцентовано увагу на законодавчих документах, які є основним джерелом правової охорони інформаційних відносин. Охарактеризовано діяльність вітчизняних органів державної влади щодо безпеки інформаційного простору від внутрішніх та зовнішніх загроз. Для аналізу категорії «національна безпека» застосовано два підходи: перший розглядає національну безпеку крізь призму «національних інтересів»; другий пов'язує національну безпеку із системою базових національних цінностей як на структурному, так і на функціональному рівнях. Підсумовуючи зміни, внесені до законодавчих документів, доводимо вектор удосконалення та гармонізації українського законодавства й нормативно-правової бази з інформаційної безпеки з кращими світовими практиками. Визначено, що основними складовими частинами політики інформаційної безпеки є регулювання інформаційних відносин щодо забезпечення прав і свобод громадян, здоров'я та моральності, інформаційних відносин у сфері комерційної діяльності, інформаційних відносин, територіальної цілісності й громадського порядку та забезпечення законності.

Ключові слова: інформація, інформаційна безпека, гібридна війна, право, законодавець, загроза, вплив, суспільство.

1. INTRODUCTION

Nowadays, there is a sharp increase in the number of public administration bodies, organizations, firms and companies, teams and specialists to create and use information, information products and information technologies in Ukraine as well as in the whole world. The widespread introduction and use of modern information computer technologies, which has been happening rapidly recently, has led to a significant increase in the volume of social relations of a special nature - information relations, that is relations that are directly related to the creation and circulation of information.

The peculiarity of such social relations nature is defined by the fact that in some cases they have an independent role and are self-sufficient, and in other ones, they are auxiliary, that is, they accompany other social relations and ensure their implementation [31].

It should be noted that informational social relations have always played a significant role in the development of mankind. But a feature of the modern stage in society's development is a significant increase in the dependence of the results of the political, social, economic, legal, and personal activities of all public and civil law subjects, without exception, on the quality of information relations. Therefore, modern society is trying to adequately respond to this through appropriate transformations of state and legal institutions. The consequence of this in many countries, in particular in Ukraine, was the appearance at first of single, and over time, a whole series of normative legal acts on the legal regulation of informational social relations, or, in other words, the creation of informational legislation.

Thus, taking into account the growing importance of information relations in the life of an individual, society and the state, as well as the current state of the process of studying the issues of information legislation, solving the scientific problem of creating theoretical, methodological and practical foundations for the development of information law and information legislation of Ukraine as a whole, and in their separate segments, is relevant.

2. RESULTS

The protection of information security is carried out by implementing a considered and balanced policy of the state in the information sphere. Taking into consideration the fact that the policy in the information security system is a comprehensive social phenomenon it has a complex nature and includes internal and external political, economic, technological, military and

other elements. It requires a comprehensive approach based on the norms of administrative law in the formation of information security [16].

Since it is about the implementation of state policy under the conditions of increasing external threats and dangers, as well as the socio-economic and socio-political crisis observed in Ukraine, the issues of ensuring information security become especially urgent. The transformations that are taking place in Ukraine have also covered the humanitarian sphere, which is an important factor in the reproduction of the nation. Under such conditions, the formation of a balanced state information policy based on systematic scientific research of the phenomena of the information sphere becomes of urgent importance. The leading place among them takes information security.

The key features of the general structure in ensuring information security remain insufficiently disclosed, which negatively affects the formation of state information policy. Improvement of legal mechanisms for ensuring information security should become a priority pillar of the state policy of Ukraine.

The interdisciplinary nature of information security, covering technical, legal, economic and psychological aspects, leads to extreme complexity and multi-level system connections, components of information security. Awareness of the peculiarities of each of them will contribute to the processes of understanding the complexity of ensuring information security, forming a complex of tactical and strategic areas of activity in the field of ensuring information security, harmonizing national information legislation, which collectively creates important foundations for an effective state information policy [14].

At the same time, it should be noted that in the current legislation, the security management mechanism is insufficiently regulated, there is no clear regulation of the conceptual and categorical apparatus. The law does not define the status of environmental, economic, information and state security, or the extent of their correlation with the original term “national security”. While analysing the category ‘national security’, two approaches are used: the first considers national security through the prism of “national interests”, the second one connects national security with the system of basic national values at both the structural and functional levels.

Scholars in the field of administrative law define national security based on the activity of special bodies that ensure it. Thus, Yu. Bytyak understands national security as “a state of protection of state sovereignty, constitutional order, territorial integrity, economic, scientific and technical and defence potential of Ukraine, the legitimate interests of the state and the rights of

citizens from the intelligence and subversive activities of foreign special services, encroachments by individual organizations, groups and individuals” [2].

O. Kopan considers national security to be “the state of the country, thanks to which the system of state legal and social guarantees ensures the implementation of sovereignty, constitutional order and territorial integrity of the state, comprehensive development and protection of the interests of the entire country’s population from the intelligence and the foreign special services subversive activities, encroachments on the part of individual organizations, groups and individuals” [8].

Therefore, the National Security Strategy of Ukraine approved by the Decree of the President of Ukraine dated May 26, 2015 regulates the determination of the problems in ensuring national security, their priorities, sequence and systematic implementation [27].

In this regard, the National Security Strategy of Ukraine outlines the restoration of the territorial integrity of democratic institutions throughout its territory, the reintegration of temporarily occupied territories after their liberation. The main goals of the Strategy are: minimizing threats to state sovereignty and creating conditions for restoring the territorial integrity of Ukraine within the internationally recognized state border of Ukraine, guaranteeing the peaceful future of Ukraine as a sovereign and independent, democratic, social, and legal state; affirming the rights and freedoms of a person and a citizen, ensuring a new quality of economic, social and humanitarian development, ensuring the integration of Ukraine into the European Union and forming the conditions for joining NATO [27].

The National Security and Defense Council was established to implement the national security policy in the country. The authority determines the priority tasks in the field of national security, priorities and strategies for responding to emerging threats including information, a strategy to prevent possible threats based on the Constitution of Ukraine and the Law of Ukraine “On the National Security and Defense Council”. The body gives instructions to the relevant departments providing the relevant directions as the components of national security. The result of the existence and development of national security is the creation of a national security system [24].

At the same time, informational, intellectual, political, military, economic, state, environmental and other elements of the country’s security are components of national security.

Investigating the issue of information security B. A. Kormych claims that the state having in its arsenal a huge set of means to influence public relations

in the information sphere, should naturally act as the main subject of information security policy. If we consider information security as certain conditions, parameters and characteristics of information processes that take place in the information sphere of the state, then it is the state with the help of normative and legal regulations to determine uniform, universally binding standards of information processes that correspond to the ideas about the security of those forces that carry out political authorities in this country [9].

Today, the development of a coherent, flexible, dynamic policy of information security in Ukraine is a logical step on the way to the information future taking into account the multifaceted nature of the information security phenomenon, the prospective trends of changes in the information space, the peculiarities of the geopolitical situation, and the economic state of the country. It will be reflected in the public consciousness as well as on at the legal conceptual and doctrinal level and in the area of effective information legislation, which has a systematized nature.

Thus, domestic researchers such as Ya. Zharkov, M. Dzyuba, I. Zamaryeva determine the state policy of ensuring information security in Ukraine as an integral component of the Ukraine state policy to provide national security that contains an officially accepted system of views and practical activities of state authorities and management. It is aimed to ensure such a position of social subjects, in which the action of any information threat does not lead to a decrease in the level of their information security below the permissible level, which is dangerous due to the high probability of negative information impacts [6].

In addition, an important vector in the implementation of the state policy to provide information security is the formation of national self-awareness, a national worldview based on a national idea.

Repeated cyber intrusions into Ukrainian information and industrial systems indicate the need for changes in the legislative and regulatory framework of information security.

On March 15, 2022 the Verkhovna Rada of Ukraine adopted amendments to the Law “On the Protection of Information Stored in Information and Telecommunication Systems”. This can be considered as a big step forward. The current law obliges all “state information resources” and “access to information restricted by law” to be processed in a system that implements the so-called “comprehensive information protection system” (CIPS) [22].

A comprehensive information protection system is defined as a set of organizational and technical measures for information protection, the completeness of which is subject to attestation by the state regulator. In other words,

a comprehensive information protection system is an information security management system that must be confirmed by state expertise. If the exam is passed successfully, the system will receive an attestation document. This document allows the information system to process, store and transmit certain classes of information.

In general, a comprehensive information protection system is a useful information security management system. It addresses a range of risks and measures that apply in many environments. Thanks to its strict verification and confirmation process, many Ukrainian security experts, primarily in the public sector, consider a comprehensive information protection system as the only means to ensure proper IT system security.

However, there is another part of the security community in Ukraine, mainly from the private sector, which considers the comprehensive system of information protection and its legislative and regulatory framework to be outdated, rigid and economically inefficient.

Amendments to the Law “On the Protection of Information in Information and Telecommunication Systems” are a kind of compromise to these extreme views. The main changes relate to the definition of certain classes of confidential information from the regulation of the comprehensive information protection system.

In particular, a comprehensive system of information protection is now mandatory only for information systems that process, store or transmit: state secrets; official information and information of state registers or unified registers, the creation of which is provided for by legislation.

All other “government information resources” and “access to information to which access is restricted by law” can be processed, stored and transmitted in IT systems without a comprehensive information protection system.

However, such IT systems must meet the following requirements: an information security management system (ISMS) must be created; compliance of such ISMS with Ukrainian information security standards must be certified by an assessment body accredited by the National Accreditation Agency of Ukraine or a national accreditation agency of another country, if the National Accreditation Agency of Ukraine and such a national accreditation agency of a foreign country are members of an international or regional organization and/ or concluded an agreement with such an organization on mutual recognition of the results of conformity assessment; cryptographic means used as means of control in such ISMS must have a positive expert opinion based on the results of state examination; none of the elements of the ISMS should be located on the territory of Ukraine, which is not under the control of the Ukrai-

nian government, or on the territory of countries declared by the Ukrainian parliament as aggressors or under sanctions according to Ukrainian legislation, or countries that are members of customs unions with the aforementioned countries; special requirements for the above information established by the Government of Ukraine must be met [1].

No matter how the above-mentioned amendments to the law look, they improve the current legislative and regulatory framework of the comprehensive information protection system. In particular, they recognize that “government information resources” have different values and therefore may require different levels of protection. Instead of a rigid and strictly controlled information protection system, amendments to the law introduce an ISMS that can be more flexible, fit for purpose and cost-effective. In general, changes to the law can be seen as an act of deregulation.

In summary, the changes to the law are a big step towards improving and harmonizing Ukrainian legislation and regulation of information security with the best global practices.

There are many other similar legislative initiatives in Ukraine, and in the future, we should expect a fundamental change in the legal landscape of information security.

It is worth emphasizing that information security policy is multi-vector in nature. Its main components are: regulation of information relations to ensure national security, territorial integrity and public order, maintain legality; regulation of information relations to ensure the rights and freedoms of citizens, health and morality; regulation of information relations in the field of commercial information [10].

Taking into account national interests and threats in the information sphere, the legislator proposes the following main directions of state policy on issues of national security in the information sphere such as ensuring the information sovereignty of Ukraine; improving the state regulation of the development of the information sphere by creating legal and economic prerequisites for the development of the national information infrastructure and resources, introducing the latest technologies in this area, filling the domestic and global information space with reliable information about Ukraine; active involvement of the mass media in the fight against corruption, abuse of office, and other phenomena that threaten the national security of Ukraine; ensuring unwavering observance of citizens’ constitutional right to freedom of speech, access to information, prevention of unlawful interference by state authorities, local self-government bodies, and their officials in the activities of mass media, discrimination in the information sphere and persecution of journalists for

political positions; the application of comprehensive measures to protect the national information space and counter the monopolization of the information sphere of Ukraine [23].

In addition, the unity and interrelationship of the directions of state policy regarding information security can be ensured by legal mechanisms defined at the legislative level, including: clearly formulated goals and objectives of state policy in this area; ensuring the interaction of state and public institutes for the implementation of interdepartmental directions of the state policy of ensuring information security; organization of a system of informing subjects operating in the field of information security about current problems, identification of potential and real threats and dangers and their sources, as well as appropriate measures and means for their prevention, neutralization and liquidation of possible consequences; ensuring coordinated and purposeful actions of subjects operating in various spheres of life of society and the state on issues of adequate response to identified potential and real threats and dangers; provision of national leadership, coordination and control in the field of information security [15].

It is worth noting that the President of Ukraine Decree of “On the Interdepartmental Commission on Information Policy and Information Security and Defence of Ukraine” dated of February 8, 2002 (as amended on June 18, 2009) establishes the Interdepartmental Commission on Information Policy and Information Security. The latter acts as a consultative and advisory body at the Council of National Security and Defence of Ukraine and is aimed to provide thorough state analysis and define possible threats to the national security of Ukraine in the information sphere. One of the objectives is generalization of international experience in the formation and implementation of information policy and analysis of the industry programs implementation and the taking measures related to the implementation by ministries and other central bodies of the executive power of state policy in the information sphere. The body provides designing and submission of proposals to the President of Ukraine and the National Security and Defence Council of Ukraine. Regarding the last task, such proposals relate to the definition of Ukraine’s national interests in the information sphere, conceptual approaches to the formation of state information policy and ensuring Ukraine’s information security. It is focused on implementing systemic measures to improve the information policy of Ukraine as well as implement the state strategy for the development and protection of the national information space and Ukraine’s entry into the world information space. It targets improvement of the legal and scientific support system of Ukraine’s information security and the development

of the state information infrastructure on issues of its material and technical base modernization and adequate financial support. The body is responsible for organization and order of ministries interdepartmental interaction, other central bodies of executive power in the field of ensuring information security; improvement of the President of Ukraine operational information and analytical support system [11].

The study of the above-mentioned body tasks allows us to conclude that cooperation is ensured exclusively by executive authorities in the field of information security in Ukraine. At the same time, we need such an organization that would be able to ensure the coordination not only of representatives of the state apparatus but also of non-state entities providing the informational component of national security. The interaction of state and public administration is one of the most important conditions of socio-economic development, state building in the system of the individual, society, and state information security.

The next important aspect related to the formation and implementation of the state information security policy is the attribution of information security to the most important function of the state, which should, first of all, involve the formation of the policy by the relevant state bodies and the legal mechanisms for its implementation in the field of information security. An important role in this direction of activity belongs to state bodies, which, by the granted powers in the spheres of their responsibility, must provide organizational, regulatory, legal, methodical, scientific, technical and financial support for the implementation of the state information security policy [12].

Taking into account the current state of information security in Ukraine, the following matters such as coordination of all the entities activities that exercise certain powers in this area; application at the national level of means and measures of state influence aimed at effective and high-quality implementation of laws and other normative legal acts on information security.

Ensuring information security as a matter for the entire Ukrainian people follows from the constitutional legal norm: “The bearer of sovereignty and the only source of power in Ukraine is the people. The people exercise power directly and through state authorities and local self-government bodies” [7].

Therefore, the state, which ensures the formation and implementation of the state information security policy, must implement the political will of the people, at least its majority. For this purpose, the state creates the necessary legal basis and organizational structure of the entities entrusted with the relevant functions.

For this purpose, the Ministry of Culture and Information Policy of Ukraine (hereinafter referred to as the Ministry of Culture and Information Policy of Ukraine) was established. O. Tkachenko was appointed to the post of the Minister. According to the Regulation on the Ministry of Culture and Information Policy of Ukraine, the Ministry is the central body of the executive power. Its activities are directed and coordinated by the Cabinet of Ministers of Ukraine. The Ministry of Culture and Information Policy is the main body in the system of executive power central bodies. It ensures the formation and implementation of state policy in the spheres of culture, state language policy, popularization of Ukraine in the world, state foreign language, information sovereignty of Ukraine (in terms of powers to manage a complete property complex Ukrainian National Information Agency “Ukrinform”) and information security. The authority ensures the formation and implementation of state policy in the fields of cinematography, restoration and preservation of national memory, international relations, religion and protection of the national minorities’ rights in Ukraine, arts, cultural heritage protection, museum affairs, export, import and return of cultural values [5].

MCIP is the main body in the system of executive power central bodies, which ensures the formation and implementation of state policy in the information and publishing sphere, and also ensures the formation and implementation of state policy in the sphere of television and radio broadcasting.

Based on the analysis of the researched areas of state policy on ensuring information security in Ukraine, the implementation of a comprehensive approach to solving information security problems, and the formation and implementation of state policy in this area should be based on the awareness of threats and dangers. Their sources should be a qualitative basis for the administrative and legal determination of powers and functions of the information security and regulation organizational support system of relations in this field of activity.

To determine the scientific, information-technical, legal, economic and organizational mechanisms for the implementation of a unified policy on the formation and development of the information security system, it is necessary to adopt the Law “On Information Security”.

In modern conditions, it is the systematic approach to information security that should be the defining direction of state policy, on which the existence of a sovereign and independent state, its national security, socio-economic development, and responsible place in the world community depend [30].

Therefore, information security is one of the country’s national security main components. Its provision with the use of a qualitatively formulated na-

tional information policy would significantly contribute to the success in the performance of tasks in the political, military-political, military, economic, social and other spheres of state activity. In particular, the implementation of a successful information policy can significantly affect the reduction of social tension and the resolution of foreign policy and military conflicts.

Information security and information protection bodies together with legislation form the state system of information security and information protection. This state system includes: bodies of legislative, executive and judicial power; legislation regulating relations in the field of information security, information protection and information resources; regulatory legal framework for information protection; information protection services (bodies) of enterprises, organizations, institutions [28].

The Verkhovna Rada of Ukraine as a body of legislative power adopts laws regulating relations in the field of information security and information protection.

The regulatory framework is formed based on normative legal acts in the field of information issued by the bodies of various branches of government.

Executive bodies (the Cabinet of Ministers of Ukraine (hereinafter referred to as the Government), which include ministries with their subordinate bodies, local executive bodies) implement laws. For this purpose, the Government adopts relevant resolutions in the field of information protection and issues orders, which are subordinate regulatory legal acts. Ministries and their subordinate bodies, following their purpose, develop and approve such normative acts as: provisions, instructions, rules, methodological recommendations. Normative acts of this level also include orders and letters from heads of executive bodies [32].

Authorities regulating relations in the field of information security and information protection include:

- Security Service of Ukraine;
- State Service for Special Communications and Information Protection of Ukraine;
- Ministry of Defence Ukraine;
- Foreign Intelligence Service of Ukraine;
- Ministry of Internal Affairs of Ukraine, to which National Police of Ukraine, Administration of the State Border Service of Ukraine, State Migration Service of Ukraine, State Service of Ukraine for Emergency Situations are subordinate;
- State Fiscal Service of Ukraine, subordinate to Ministry of Finance of Ukraine;

- State enterprise Ukrainian Research and Training Center for Problems of Standardization, Certification and Quality;
- Center for Countering Disinformation;
- Center for strategic communications and information security [29].

The Security Service of Ukraine is a special state law enforcement agency that ensures the state security of Ukraine and is subordinate to the President of Ukraine. The Security Service of Ukraine performs, in particular, the functions of protecting state secrets.

The State Service for Special Communications and Information Protection of Ukraine is a state body that is appointed to ensure the functioning and development of the state government communications system, the formation and implementation of state policy in the fields of cryptographic and technical information protection, telecommunications, the use of radio frequency resources of Ukraine, postal communications special purpose communication, government field service communication, as well as other tasks under the law [19].

The Ministry of Internal Affairs of Ukraine fights against criminals in the information sphere and against computer crimes [21].

The State Fiscal Service of Ukraine is obliged to prevent the illegal import and export of “pirated” products from Ukraine, thus ensuring the protection of copyright and patent rights [20].

The state enterprise Ukrainian Research and Training Centre for Standardization, Certification and Quality Problems develops standards in the field of information protection and creates prerequisites for bringing the national standardization system closer to international and European norms and rules [13].

The judiciary supervises and prosecutes violations of legislation in the information sphere. In their activity, courts are governed by articles of the Criminal and Civil Codes of Ukraine.

The Centre for Countering Disinformation is a centre for countering current and projected threats to Ukraine’s national security and national interests in the information sphere, ensuring Ukraine’s information security, effective countering of propaganda, destructive disinformation influences and campaigns, preventing manipulation of public opinion [18].

The centre started work on April 6, 2021. At the beginning of May, the President of Ukraine Volodymyr Zelenskyy approved the Regulation, which established that the Centre is subordinate to the National Security and Defence Council of Ukraine (hereinafter referred to as the NSDC), the general direction and coordination of its activities is carried out by the secretary of the NSDC [3].

The work of the Centre for Countering Disinformation covers such areas as the military direction, the fight against crime and corruption, foreign and domestic policy, the economy, infrastructure, ecology, health care, the social sphere, and the scientific and technological direction. However, the main focus is on countering the spread of false information on the Internet and fakes in the media. The Centre does not have punitive functions for misinformation and will not be able to apply sanctions, but it can make submissions to the National Security Council regarding certain violations.

The Centre for Strategic Communications and Information Security focuses its work on strategic communications, which include the development of Russian counter-narratives, conducting information campaigns, including Ukrainian narratives in the Government's daily communication; creation of an online resource that actively responds to computer attacks; regular notification of hybrid aggression by Russia at the international level, joint development of mechanisms to counter disinformation with international partners [17].

The formation, implementation and coordination of the state information policy, as well as ensuring the information sovereignty of Ukraine, is carried out by a specially authorized central body of executive power following the functions assigned to it.

The tasks of the central executive body in the field of state information policy are the development of conceptual documents in the field of sustainable development of the information space and control over their implementation in the system of executive bodies. Coordination of the activities of the central executive authorities is also carried out to ensure the sustainable development of the information space of Ukraine. An important task is the preparation of normative documents that regulate the procedure for relations with the public of state authorities and the publication of information about their activities, as well as the coordination and control of the activities of the units of the central executive authorities that carry out communication with the public [4].

The main subjects of Ukraine state information policy implementation are such central bodies of executive power, which form and implement state policy in the following areas: in the spheres of education and science, intellectual property, scientific, scientific-technical and innovative activities, informatization, formation and use of national electronic information resources, creating conditions for the development of the information society, as well as in the field of state supervision (control) over the activities of educational institutions, regardless of their subordination and form of ownership; in the spheres of culture and arts, protection of cultural heritage, export, import and return of cultural values, state language policy, as well as in the sphere of formation

and implementation of state policy in the field of cinematography (the latter is State Cinema); in the sphere of informatization, electronic government, formation and use of national electronic information resources, development of information society; in the sphere of television and radio broadcasting, information and publishing spheres [26].

Therefore, the information security of Ukraine is achieved through a balance between the information rights and freedoms of various legal entities and the protection of national information sovereignty. At the same time, only those actions that are directed within the limits of the current legislation and the Constitution, based on the principles of the rule of law and equality of all before the law, give a positive result both for society as a whole and for an individual citizen.

3. CONCLUSIONS

The further progress of mankind is connected with the wide implementation of ICT or, in other words, with the construction of an information society. Its development, the high dynamics of the increase in the number of social relations based on the wide use of information and information processes, the sharp increase in the significance of these relations for all spheres of human activity, society and the state determine the relevance and necessity of studying the theoretical, methodological and practical problems of legal support of the information sphere, the basis of which is information law and information legislation.

One of the key parts of the military-technological revolution in the modern world is the possibility of developing a new form of warfare, which is often called information warfare. The evolution of information warfare depends on technological change, systems development, and the adaptation of operational approaches and organizational structures to take advantage of this new opportunity. In the military industry, much attention is rightly focused on assessing the doctrinal, operational, and organizational issues of the information warfare revolution. However, much less attention has been paid to the specific impact of information warfare on technological research and acquisition.

Threats of information wars, speculative (hostile, aggressive) information influences urgently raise the issue of information security. The legislator identified the main threats to information security, taking into account the dynamism and radicalism of possible changes, as well as due to intensive scientific and technical progress. Therefore, any law is unlikely to be able to or should contain an exhaustive list of such threats to reflect modern problems. The absence of such a threat as limiting the exercise of the rights and freedoms of a person and

a citizen regarding the use, dissemination and storage of information is considered a significant deficiency in the law.

There is also a specific problem of protecting information during the acquisition and development of such systems. Because dependence on commercial technologies creates concomitant vulnerabilities to commercial technologies, it is important to assess the risks posed by these vulnerabilities “upfront and early” in the development cycle.

The already existing methodologies for conducting mentioned assessments as part of the engineering process and such methodologies themselves should be strengthened and extended to all new or modified systems. In addition, concerns about product integrity due to software backdoors should be addressed. Since such issues are of interest to commercial structures as well, the military should seek to work much more closely with traditionally non-defense firms that provide much of the information for the military’s information infrastructure to solve these problems.

We hope that domestic legislation and software products in the field of information security will have new modern content and meet the high international level.

REFERENCES

1. Deregulative changes in information security in Ukraine. URL: https://www.aster-slaw.com/ua/press_center/publications/deregulative_changes_in_information_security_in_ukraine/ (in Ukraine).
2. Bytiak, Yu. P., Bohutskyi, V. V., Harashchuk, V. M. (2000). *Administratyvne pravo Ukrainy*. Kharkiv, 520 p. (in Ukraine).
3. V Ukraini zapratsiuvav Tsentр protydiї dezinformatsii. URL: <https://www.radiosvoboda.org/a/news-tsentр-protydiya-dezinformatsiya/31189623.html> (in Ukraine).
4. Hurovskyi, V. O. (2014). Rol orhaniv derzhavnoi vlady u sferi zabezpechennia informatsiinoi bezpeky Ukrainy. *Visnyk Ukrainskoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy: Fakhovyi zbirnyk*. Kyiv, № 3, p. 21–31 (in Ukraine).
5. Deiaki pytannia diialnosti Ministerstva kultury ta informatsiinoi polityky. *Postanova Kabinetu Ministriv Ukrainy vid 16 zhovtnia 2019 r.*, № 885. URL: <https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text> (in Ukraine).
6. Zharkov, Ya. M., Dziuba, M. T., Zamaruieva, I. V. (2008). *Informatsiina bezpeka osobystosti, suspilstva, derzhavy: Vydavnycho-polihrafichnyi tsentr «Kyivskyi universytet»*, 274 s. URL: https://mil.univ.kiev.ua/files/7_50255454.pdf. (in Ukraine).
7. Konstytutsiia Ukrainy. *Vidomosti Verkhovnoi Rady Ukrainy (VVR)*, 1996, № 30, p. 141. URL: <http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80> (in Ukraine).
8. Kopan, O. V. (2017). Destabilizatsiia sotsialno-politychnoi sytuatsii – provokatsiia vnutrishnoderzhavnoho konfliktu. *Informatsiia i pravo : Fakhovyi zbirnyk*, № 4, p. 73–78. URL: http://nbuv.gov.ua/UJRN/Infpr_2017_4_9. (in Ukraine).

9. Kormych, B. A. (2004). *Informatsiina bezpeka : orhanizatsiino-pravovi osnovy : navch. posibnyk*. Kyiv: Kondor, 384 p. (in Ukraine).
10. Kosach, P. D. (2002). *Informatsiina bezpeka yak osnova natsionalnoi bezpeky*. Kyiv : ZAT Vydavnychiy dim «DEMShch», 144 p. (in Ukraine).
11. Lipkan, V. A., Maksymenko, Yu. Ye., Zhelikhovskiy, V. M. (2006). *Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii: navchalnyi posibnyk*. Kyi : KNT, 280 p.
12. Mahda, Ye. (2015). *Hibrydna viina : vyzhyty i peremohty*. Kharkiv: Vivat, 320 p. (in Ukraine).
13. Ofitsiinyi sait Derzhavnoho pidpriemstva «Ukrainskyi naukovo-doslidnyi i navchalnyi tsentr problem standartyzatsii, sertyfikatsii ta yakosti». URL: <http://uas.org.ua/ua/> (in Ukraine).
14. Perun, T. S. (2019). *Administratyvno-pravovyi mekhanizm zabezpechennia informatsiinoi bezpeky v Ukraini*. Lviv: Natsionalnyi universytet «Lvivska politehnika», 268 p. (in Ukraine).
15. Petryk, V. *Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby* URL: www.justinian.com.ua/article.php. (in Ukraine).
16. Pocheptsov, H. (2006). *Informatsiina polityka : navch. posibnyk*. Kyiv: Znannia, 663 p. (in Ukraine).
17. *Prezentovano Tsentr stratehichnykh komunikatsii ta informatsiinoi bezpeky* URL: <https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki> (in Ukraine).
18. *Prezydent zatverdyyv Polozhennia pro Tsentr protydii dezinformatsii*. URL: <https://www.president.gov.ua/news/prezident-zatverdiv-polozhennya-pro-centr-protidyyi-dezinfor-68317>. (in Ukraine).
19. *Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy: Zakon Ukrainy vid 23.04.2021. Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2006, № 30, st. 258* (in Ukraine).
20. *Pro Derzhavnu fiskalnu sluzhbu Ukrainy: postanova Kabinetu ministriv Ukrainy vid 21 travnia 2014, № 236*. URL: <https://zakon.rada.gov.ua/laws/show/236-2014-%D0%BF#Text> (in Ukraine).
21. *Pro zatverdzhennia Polozhennia pro Ministerstvo vnutrishnykh sprav Ukrainy: postanova Kabinetu ministriv Ukrainy vid 28 zhovtnia 2015, № 878*. URL: <https://zakon.rada.gov.ua/laws/show/878-2015-%D0%BF#Text>. (in Ukraine).
22. *Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh: Zakon Ukrainy vid 04.07.2020, № 31, st. 286*. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>. (in Ukraine).
23. *Pro zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2014*. URL: www.president.gov.ua/dokument/17588.html. (in Ukraine).
24. *Pro osnovy natsionalnoi bezpeky Ukrainy: Zakon Ukrainy vid 19 cherv (2003), № 964-IV, 2003, № 9, st. 351*. URL: <https://zakon.rada.gov.ua/laws/show/964-15#Text> (in Ukraine).
25. *Pro Radu natsionalnoi bezpeky i oborony Ukrainy: zakon Ukrainy vid 05 bereznia 1998, № 183/98–VR*. URL: <http://zakon4.rada.gov.ua/laws/show/183/98>. (in Ukraine).

26. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2014 roku «Pro zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 01.05.2014 № 449/2014 URL: <https://zakon.rada.gov.ua/laws/show/n0004525-14#Text>. (in Ukraine).

27. Pro stratehiiu natsionalnoi bezpeky Ukrainy : Ukaz Prezydenta Ukrainy vid 12.02.2007. *Uriadovyi kurier*. (in Ukraine).

28. Pro skhvalennia Stratehii rozvytku informatsiinoho suspilstva v Ukraini: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 15.05.2013. № 386-r. *Uriadovyi kurier*, № 105, p. 26–27 (in Ukraine).

29. Sashchuk, H. Informatsiina bezpeka v systemi zabezpechennia natsionalnoi bezpeky. URL: http://www.journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php. (in Ukraine).

30. Svitova hibrydna viina : ukraïnskyi front : monohrafiia /za zah. red. V. P. Horbulina. Kyiv: NISD, 2017. 496 p. (in Ukraine).

31. Shubina, O. V. (2014). Derzhavna informatsiina bezpeka: problemy vyznachennia kontseptu. *Derzhava ta prava: Fakhovyi zbirnyk*, № 3, p. 26–31 (in Ukraine).

32. Yudin, O. K. (2004). Informatsiina bezpeka derzhavy. Kharkiv: Konsum, 508 p. (in Ukraine).

Матеріал надійшов до редакції 07.03.2024 р.

УДК 32.019.5]:070.16:551.5

Євгенія Тихомирова,

доктор політичних наук, професор кафедри міжнародних комунікацій та політичного аналізу,

Волинський національний університет імені Лесі Українки,

evgenia.tyhomirova@vnu.edu.ua

ORCID ID: 0000-0002-5017-5875

DOI 10.29038/2524-2679-2024-01-102-122

ЛАНДШАФТ ДЕЗІНФОРМАЦІЇ ЩОДО ЗМІНИ КЛІМАТУ: ДЕНІАЛІСТСЬКИЙ РАКУРС

Ужито метафору «ландшафт дезінформації щодо зміни клімату» для акцентування багатогранності проблеми кліматичної дезінформації як складної інформаційної системи з багатьма взаємодіючими змінними.