UDC 32.019.51

R. Chernysh

O. Piroh

P. Hrushevska

THREATS TO THE STATE SECURITY OF UKRAINE IN THE INFORMATION SPHERE IN THE REALITIES OF THE RUSSIAN-UKRAINIAN WAR

The article formulates the concept of "threats to the State security of Ukraine in the information sphere", identifies these threats in the realities of the russian-ukrainian war. It is stated that the information security system as a component of the state security system is generally characterised by appropriate forces and means. At the same time, the author focuses on the main areas of activity of state bodies (including law enforcement and special bodies) for effective ensuring of the state security of Ukraine in the information sphere.

Keywords: *state security in the information sphere, Internet, cybersecurity, cyber threats, national security.*

Statement of the problem. In order to ensure Ukraine's democratic development, maintain its European integration course and preserve its integrity in the context of the russian-ukrainian war, it is necessary to intensify large-scale reform processes. This is especially true of the organisation and functioning of the national security and defence sector, the democratic transformation of key civil institutions and the introduction of modern principles of public administration.

With the increased use of information technologies in the context of the russian-ukrainian war, control over information flows is becoming one of the main goals of the confrontation. In such circumstances, the struggle revolves around influencing public opinion. The confrontation in the information sphere has logically led to the start of the so-called "information arms race". With the development of information technologies and their active use in the realities of the russian-ukrainian war, the issue of ensuring Ukraine's state security in the information sphere is extremely relevant. Our state must systematically improve conceptual measures of information security, because information threats to national interests are much more dynamic than, for example, economic or political ones.

Analysis of recent research and publications. The outlined issues have been studied by domestic security experts, lawyers, and managers, in particular: S. Bielay, A. Blahodarnyi, V. Horbulin, O. Dovhan, M. Dzeveliuk, I. Doronin, V. Krutov, V. Lipkan, A. Marushchak, V. Petryk, V. Pylypchuk, V. Polev, M. Prysiazhniuk, A. Tarasiuk, T. Tkachuk and many other scholars.

These authors have made a significant contribution to the development of legal and organisational regulation of legal relations in the information sphere. However, despite the achievements of Ukrainian and foreign scholars, given the extremely fast pace of informatisation, including the current stage – digitalisation, a significant number of issues of the subject matter raised still remain insufficiently researched and require scientific substantiation with a view to further implementation in practice.

The purpose of the article is to formulate the concept of "threats to the State security of Ukraine in the information sphere", to highlight these threats in the realities of the russian-ukrainian war, to disclose the main measures aimed at countering the latter, and also to determine the main areas of activity of State bodies (including law enforcement and special ones) with a view to effectively ensuring the State security of Ukraine in the information sphere.

Summary of the main material. On the way of its development, each country faces the challenge of finding new directions and means of countering information threats. In the context of ensuring Ukraine's information security, it should be borne in mind that the State is included in the list of countries most susceptible to information manipulation by the aggressor country [14].

According to the authors of the article, a certain reserve in this counteraction is to improve the organisation of the work of state bodies (including law enforcement and special) to ensure timely targeted neutralisation of these threats (preferably at the stage of preparation for their implementation or at the initial stage).

According to the US Senator George McGovern, "...one of the ways to strike a nation is to restrict the flow of information, cutting off contacts between its consumers, and building an information wall. This is how a new term – "information sovereignty" – entered the international lexicon. At the same time, attempts by an individual nation to block the flow of information from the outside can contribute to the undermining of its economy rather than to its development. In addition, every technological breakdown opens the nation to invasion from the outside" [4].

In modern conditions, "information potential" is becoming one of the most important factors in ensuring national security along with "economic potential", "military potential", etc. The level of development and security of the information environment actively influence the state of political, economic and other components of Ukraine's national security [10, p. 26].

The rapid development of the global information space and the use of information and communication technologies in all spheres of life contribute to the expansion of the information society in Ukraine and determine the importance of information security issues. In such circumstances, one of the main tasks of the state is to create a comprehensive system of information threat assessment and appropriate response to ensure state security in the information sphere [11]. In order to regulate the above activities and to legislate that ensuring the information security of Ukraine is one of the most important functions of the state, the Information Security Strategy was approved on 28 December 2021. This document identifies current challenges and threats to Ukraine's national security in the information sphere, strategic goals and objectives aimed at countering such threats, protecting the rights of individuals to information and protecting personal data. Its purpose is to strengthen the capacity to ensure the information security of the state, its information space, support social and political stability, defence of the state, protection of state sovereignty, territorial integrity of Ukraine, democratic constitutional order, and ensuring the rights and freedoms of every citizen by information means and measures [12].

At the same time, according to the authors, national intelligence services with their information and analytical potential should play a significant role in such a comprehensive system.

Threats to the state security of Ukraine in the information sphere can be formulated as a system of conditions and factors that lead or may lead to damage to important state, public and personal interests through the possible destructive impact of information on the consciousness (subconscious) and behaviour of citizens, as well as through technical impact on information resources and infrastructure.

The system of threats to the state security of Ukraine in the information sphere may include the following categories:

– threats to the security of information and the relevant infrastructure, which include risks associated with misuse, unauthorised access, damage or loss of information, as well as attacks on information infrastructure (cyber-attacks or computer viruses);

– threats to the security of information subjects and social relations between them from actions (influences) of an informational nature, which include manipulation of information in order to influence the consciousness and behaviour of citizens, forming the desired impression and manipulating social relations in order to influence public order [7, 9];

– threats to the current procedure for exercising the rights and interests of information subjects, which include actions aimed at violating laws, rights and freedoms, in particular in the field of information (spreading disinformation, discrediting, obstacles to access to information or restriction of freedom of speech).

According to U. Ilnytska, threats to Ukraine's national security in the information sphere include:

1) possible restriction of freedom of speech and free access of citizens to information;

2) distortion, distortion, blocking, concealment and subjective reflection of information;

3) illegal dissemination of information;

4) dissemination of unreliable open data;

5) information conquest of other countries and destructive information intrusion into the state information space, when states with greater information potential use the opportunity to strengthen their influence through the media on the population and public of a country with lesser opportunities in the information sphere;

6) creation and functioning of uncontrolled information flows in the state information space;

7) spreading the cult of violence and cruelty through the media;

8) Ukraine's slow entry into the global information space;

9) the recklessness of the national information policy and the lack of important infrastructure in the information sphere;

10) spread of disinformation via the Internet [6, p. 30].

The latter provision somewhat narrows the possibilities of spreading disinformation [16], since other sources of dissemination (not only the Internet or social networks [1]) can be used for this purpose.

Also, according to the authors, these threats should include the slow response of state bodies (including law enforcement and special agencies) to challenges and threats to state security in the information sphere, which accelerates negative processes and leads to their increase. It should be noted that this feature is typical for most countries with economies in transition [3].

The issue of ensuring the state interests and state security in the field of obtaining and using information is currently quite relevant. Information security is ensured by the implementation of a unified state policy in the field of national information security, a system of economic, political and organisational measures adequate to existing and potential threats to national interests (personal, public and state) in the information sphere.

In order to ensure and maintain the required level of state security in the information space, a system of legal norms regulating relations in the information sphere is being developed and implemented. It provides for the definition of key areas of activity of public administration bodies, creation or reorganisation of bodies and forces ensuring information security, as well as the formation of a mechanism for controlling their activities.

The opinion of V. Lipkan is noteworthy, as he notes that the process of forming the key elements of the information security system is not yet complete. Considering the general lack of formation of the national security system and the uncertainty of the state information policy is appropriate in this context. In addition, the imperfection of the legal and regulatory framework for the processes under study negatively affects the quality of public administration in this area [8].

Thus, the above-mentioned gaps in the legal framework governing legal relations in the information sphere pose significant obstacles to qualitative changes in this area of public relations. Insufficient clarity and interconnectedness of measures and theoretical developments to ensure the country's information security make it difficult for state authorities to fully fulfil their obligation to ensure information security as an integral part of national security. The development and implementation of an effective system of counteracting unlawful acts that have signs of crimes in the information sphere requires the development of effective norms of national legislation and departmental regulations of the security and defence sector.

The information security system as a component of the state security system is generally characterised by appropriate forces and means. In this context, forces can be considered as the subjective composition of the information security system, i.e. people, organisations, structures, special bodies that protect information; means – as technologies and various technical, software, linguistic, legal and organisational resources. They include telecommunication channels used for collecting, forming, analysing, transmitting or receiving information data related to state security in the information sphere, as well as measures aimed at strengthening this security.

In today's information society, each entity plays an important role in ensuring state security in the information sphere. Due to the synergistic features of information security, any of the subjects can simultaneously be an object of information security and a source of possible threats or a channel for their spread. In this regard, the success of information security depends not only on special state structures, but also on each subject of information relations, which must protect itself in the information sphere. At the same time, the state is a special subject of information security, since it has the ability to act directly and uses legal means to regulate information relations. In addition, it should be borne in mind that the state plays a special role among the subjects of information security, because only it has a wide potential, which includes not only economic, political and ideological means of indirect influence, but also direct administrative action. This means that the state can use legal means to regulate information relations and directly influence information security [13].

The state as a subject of information security bears increased responsibility in ensuring security in the information sphere [2, p. 152]. However, it is worth noting that in the current conditions of development of the information society, each subject of information relations (citizens, organisations or enterprises) is independently responsible for their security (in particular in the

information sphere). Thus, joint interaction of the state and all subjects of information relations in ensuring the above security is a key factor of success in this area.

The analysis of classifications of threats to Ukraine's state security in the information sphere shows that there is no single established approach to identifying their individual types, since each researcher of the outlined issues applies relevant subjective criteria, so it is difficult to make such a list unified and exhaustive. The authors agree with R. Khmelevskyi's opinion that "...even detailed lists of threats cannot be exhaustive and stable. This is due to the fact that the sources of threats can be diverse: people, hardware, models, algorithms, software and technological processing schemes, external environment, etc." [15].

In the context of the russian-ukrainian war, given the dynamic change in the operational situation, the current threats to the state security of Ukraine in the information sphere include the following:

– creating an atmosphere of spirituality in Ukrainian society, directed against culture and historical heritage;

– manipulation of public opinion and political orientation of the population in order to create political tension and chaos;

– destabilisation of political relations, conflicts and distrust between parties, associations and movements;

– provoking social, political, ethnic and religious clashes;

– insufficient information support for government and administration, which can lead to a decrease in the efficiency of their work and erroneous management decisions;

– disinformation and discrediting the actions of state authorities in order to reduce their authority;

– Initiation of protests, strikes, and other acts of civil disobedience;

– undermining the authority of the state in the international arena and obstructing cooperation with other countries;

– creating and strengthening opposition organisations and movements, including far-right and far-left organisations;

– discrediting national identity and historical facts;

– changes in the system of worldview values and attitudes;

– diminishing the importance of achievements in science, technology and other fields, distorting facts in order to negatively influence the decisions of the highest state authorities;

– creating preconditions for economic, spiritual or military defeat and reducing the desire of the population to fight and win;

– promotion by the aggressor of its own way of life as an example for other nations;

– undermining the morale of the population through "war fatigue", political scandals and disbelief in victory, which can lead to a decrease in the defence capability and combat potential of the Armed Forces of Ukraine;

– damage to critical infrastructure, including hardware, software and systems to protect against unauthorised access to information, etc.

In the current situation, it is possible to formulate the following groups of basic measures aimed at countering traditional and new threats to Ukraine's state security in the information sphere and eliminating the factors that lead to their emergence:

a) political and diplomatic measures – political and diplomatic efforts to strengthen international cooperation, conclude international treaties and agreements, build alliances and partnerships with other countries to ensure collective security in the information sphere;

b) military measures – strengthening of the country's defence capability, development of military infrastructure, modernisation of military forces and military operations to protect the state security of Ukraine in the information sphere;

c) legal (legislative) measures – development and adoption of regulatory legal acts to regulate the sphere of information security, including the fight against terrorism, cyber threats, cybercrime, etc;

d) information and psychological measures – conducting information campaigns, appropriate psychological influence on the public, forming a positive image of the country, combating disinformation and propaganda, and forming a "culture of information consumption" among the population;

e) economic measures – development of economic sectors, attraction of investments, ensuring economic stability, combating financial threats in the information sphere;

f) scientific and technological measures – scientific research, development of technologies and innovations aimed at detecting, predicting and counteracting new threats in the information sphere, including cyber espionage and cyber-attacks on critical infrastructure;

g) organisational (administrative and procedural) measures – development and implementation of effective organisational structures, procedures and policies that promote information security (may

include the creation of specialised information security departments, determination of procedures for controlling access to information, regular inspection and updating of security systems, etc.);

i) physical measures – physical protection of information infrastructure, data storage facilities (primarily critical infrastructure facilities), restriction of physical access to confidential information and installation of video surveillance and control systems;

j) technical (hardware and software) measures – the use of special hardware and software for information protection, data encryption, incident detection and recovery, data backup [5] and other technical means to ensure state security in the information sphere.

These measures contribute to the creation of a comprehensive information security system that considers various threats and uses different methods to prevent and localise them.

Conclusions

In view of the above, with the development of information technologies and their active use in the context of the russian-ukrainian war, the issue of ensuring Ukraine's state security in the information sphere is quite relevant. In such circumstances, our state must systematically improve conceptual measures of information security, since information threats to national interests are much more dynamic than economic or political ones. At the same time, it is necessary to consider the rapid emergence of new technologies, mechanisms and means of exerting destructive information influence on society.

Given the challenges of today, state agencies (including law enforcement and special agencies) should focus their efforts on analytical work, tracking trends, interdependencies and phenomena that may pose a threat to state security (including in the information sphere).

In order to ensure the state security of Ukraine in the information sphere, the authors believe that the main efforts of state bodies (including law enforcement and special agencies) should be directed to the following key aspects:

– active response to threats: improving mechanisms for responding to cyberattacks and other threats in real time;

– cyber security: ensuring protection of computer systems, networks and information from cyber-attacks, including the use of effective encryption methods, incident detection and prevention, and training of personnel in cyber security standards;

– information intelligence: analysing and monitoring the information space to identify potential threats and risks; developing information systems for collecting and processing data, detecting disinformation and manipulative information;

– legislative and regulatory framework: optimisation of the departmental framework of legal acts regulating activities in the information sphere;

– international cooperation: development of mechanisms for cooperation with foreign intelligence services and international organisations to exchange information on threats, develop joint strategies and standards, and coordinate information security measures;

– improving the system of training and professional development: updating educational programmes, curricula and teaching materials for training and professional development of the SSU employees in the field of information security;

– education and awareness: raising the level of critical thinking and awareness of the population and representatives of state authorities and local self-government on cybersecurity and personal data protection in the information sphere (including by teaching them the basic principles of cybersecurity and safe use of information technology).

References

1. Chernysh R., Pohrebnaia V., Montrin I., Koval T. and Paramonova O. (2020). Formation and application of communication strategies through social networks: Legal and Organizational Aspects. *International Journal of Management*. Vol. 11. No. 6. P. 476–488. DOI: https://doi.org/10.34218/IJM.11.6.2020.041 [in English].

2. Shilin M., Shmotkin O., Chernysh R., Konyk T., & Botvinkin O. (2022). Formation and formulation of state policy to ensure national security: Theoretical and Legal Aspects. *Amazonia Investiga*. Vol. 11. No. 57. P. 152–161. DOI: https://doi.org/10.34069/AI/2022.57.08.16 [in English].

3. Vlasenko T. O., Chernysh R. F., Dergach A. V., Lobunets T. V., Kurylo O. B. (2020). Investment Security Management in Transition Economies: Legal and Organizational Aspects. *International Journal of Economics and Business Administration*. Vol. 8. No. 2. P. 200–209 [in English].

4. Dzeveliuk M. V. (2017). *Servisna derzhava yak funktsionalna model suchasnoi derzhavy* [The service state as a functional model of the modern

state]. *Aktualni problemy derzhavy i prava*, vol. 78, pp. 60–67 [in Ukrainian].

5. Dovhan O., Tarasiuk A., Tkachuk T. (2021). *Kiberbezpeka "suspilstva znan"* [Cyber security of the "knowledge society"]. Kyiv; Odesa : Feniks [in Ukrainian].

6. Ilnytska U. (2016). *Informatsiina bezpeka Ukrainy: suchasni vyklyky, zahrozy ta mekhanizmy protydii nehatyvnym informatsiino-psykholohichnym vplyvam* [Information security of Ukraine: modern challenges, threats and countermeasures against negative informational and psychological influences]. *Politychni nauky*, no. 2-1, pp. 27–32 [in Ukrainian].

7. Petryk V. M., Bed V. V., Prysiazhniuk M. M. (2018). *Informatsiino-psykholohichne protyborstvo* [Informational and psychological conflict]. Kyiv : VIPOL [in Ukrainian].

8. Lipkan V. A., Makymenko Yu. Ye., Zhelikhovskyi V. M. (2006). *Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii* [Information security of Ukraine in the conditions of European integration]. Kyiv : KNT [in Ukrainian].

9. Petryk V. (2009). *Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby* [The essence of information security of the state, society and the individual]. *Yurydychnyi zhurnal*. Retrieved from: http://surl.li/nfhlyp (accessed 10 May 2024) [in Ukrainian].

10. Prysiazhniuk M. M., Klymchuk O. O., Tykva V. L. (2014). *Kurs lektsii z navchalnoi dystsypliny "Informatsiina bezpeka derzhavy"* [Course of lectures on the educational discipline "Information security of the state"]. Kyiv : Tsentr navchalnykh, naukovykh ta periodychnykh vydan [in Ukrainian].

11. *Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2014 r., uvedeno v diiu Ukazom Prezydenta Ukrainy "Pro zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy" № 449/2014* [Decision of the National Security and Defense Council of Ukraine "On measures to improve the formation and implementation of state policy in the field of information security of Ukraine" activity no. 449/2014]. (2014, May 1). Retrieved from: http://surl.li/xzsbmu (accessed 10 May 2024) [in Ukrainian].

12. *Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 r., uvedeno v diiu Ukazom Prezydenta Ukrainy "Pro Stratehiiu informatsiinoi bezpeky" № 685/2021* [Decision of the National Security and Defense Council of Ukraine "On the Information Security Strategy" activity no. 685/2021]. (2021, December 28). Retrieved from: http://surl.li/uelqso (accessed 10 May 2024) [in Ukrainian].

13. Tykhomyrov O. O. (2023). *Prava liudyny: informatsiinyi vymir* [Human rights: information dimension]. Odesa : Yurydyka [in Ukrainian].

14. *Ukraina seriozno vrazhena informatsiinymy manipuliatsiiamy rf* [Ukraine is seriously affected by information manipulation of the russian federation]. Retrieved from: http://surl.li/yjwjxf (accessed 10 May 2024) [in Ukrainian].

15. Khmelevskyi R. M. (2016). *Doslidzhennia otsinky zahroz informatsiinii bezpetsi obiektiv informatsiinoi diialnosti* [Research on the assessment of threats to information security of objects of information activity]. *Suchasnyi zakhyst informatsii*, no. 4, pp. 65–70 [in Ukrainian].

16. Chernysh R. F. (2019). *Pravovyi dosvid krain Yevropeiskoho Soiuzu u sferi protydii poshyrenniu feikovoi informatsii* [Legal experience of the countries of the European Union in the field of combating the spread of fake information]. *Pidpryiemnytstvo, hospodarstvo i pravo*, no. 10, pp. 123–128. Retrieved from: http://surl.li/qqmylq (accessed 10 May 2024) [in Ukrainian].

The article was submitted to the editorial office on 18.10.2024

УДК 32.019.51

Р. Ф. Черниш, О. В. Пірог, П. Ю. Грушевська

ЗАГРОЗИ ДЕРЖАВНІЙ БЕЗПЕЦІ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ У РЕАЛІЯХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Сформульовано поняття «загрози державній безпеці України в інформаційній сфері». Їх можна сформулювати як систему умов і чинників, що призводять або можуть призвести до заподіяння шкоди важливим державним, суспільним та особистим інтересам унаслідок можливого деструктивного впливу інформації на свідомість (підсвідомість) і поведінку громадян, а також через технічний вплив на інформаційні ресурси та інфраструктуру.

Установлено, що система захисту інформації як складник системи безпеки держави в цілому характеризується відповідними силами і засобами.

У цьому контексті сили можна розглядати як суб'єктний склад системи захисту інформації, тобто людей, організації, структури, спеціальні органи, які здійснюють захист інформації; засоби – як технології, так і різноманітні технічні, програмні, лінгвістичні, правові та організаційні ресурси. До них належать телекомунікаційні канали, які використовуються для збирання, формування, аналізу, передачі чи отримання інформаційних даних стосовно безпеки держави в інформаційній сфері, а також заходи, спрямовані на посилення цієї безпеки.

Акцентовано увагу на основних напрямах діяльності державних органів (зокрема правоохоронних та спеціальних) щодо ефективного забезпечення державної безпеки України в інформаційній сфері.

Ключові слова: *державна безпека в інформаційній сфері, мережа Інтернет, кібербезпека, кіберзагрози, національна безпека.*

Chernysh Roman – Candidate of Law, Associate Professor, Expert in the Field of Information Security
https://orcid.org/0000-0003-4176-7569

Piroh Oleksandr – Candidate of Technical Sciences, Associate Professor of the Department of Computer Engineering and Cybersecurity, State University of Zhytomyr Polytechnic
https://orcid.org/0000-0003-4176-7569

Hrushevska Polina – Second (Master's) Degree Student of Polissia National University
https://orcid.org/0009-0009-5891-6656