



Current State of Information Security in Ukraine

**Sergii Hryshchenko¹, Volodymyr Savchenko², Andrii Kumeiko³,
Nino Patsuriia⁴, Viktoriia Rieznikova⁵**

Abstract

Information security has always been and is now one of the priority goals of the modern state, and is also a factor in ensuring its sustainable development. In the current conditions of military aggression of the neighboring state, an important place is occupied by information propaganda, which is constantly used by the enemy. In this regard, the front for the struggle is including the information space, which is why this study is relevant. The aim of the study is to analyze the impact of military aggression by the Russian Federation on information security in Ukraine. The research methods were: dialectical, special-legal and system-structural methods. According to the results of the study, information security is a key characteristic of national security, which reflects the state of protection of the state and society from unreliable information influence. It is proved that in 2022 there are about fifty normative-legal support of information security, which regulates and determines the sphere of information security in Ukraine. It has been determined that since 2014 Ukraine has actually suffered from constant information attacks by the Russian Federation, and the first propaganda sentiments were manifested before 2014 in the form of broadcasting on Russian television contradictory historical facts that Crimea suddenly became part of the USSR and its cultural the history of Kievan Rus is recognized as a legacy. The materials of this study can be useful for students and teachers of legal specialties, in particular when considering the discipline of Information Law of Ukraine, Constitutional Law of Ukraine.

Keywords

Information Security, Responsibility, Cyber-Attack, State Information Policy, Propaganda, Wax Aggression

¹ Ukrainian Research Institute of Special Equipment and Forensic Science, Kyrylivska Str. 103, 02000 Kyiv, Ukraine. E-mail: sergii_hryshchenko@sci-academy.cc.

² National University of Life and Environmental Sciences of Ukraine, Heroiv Oborony Str. 15, 03041 Kyiv, Ukraine. E-mail: volodymyr_savchenko@pltch-sci.com.

³ National Academy of Security Service of Ukraine, Mykhailo Maksymovych Str. 22, 03022 Kyiv, Ukraine. E-mail: Kandriina24@gmail.com.

⁴ Taras Shevchenko National University of Kyiv, Volodymyrska Str. 60, 01033 Kyiv, Ukraine. E-mail: nino_2005@ukr.net.

⁵ Taras Shevchenko National University of Kyiv, Volodymyrska Str. 60, 01033 Kyiv, Ukraine. E-mail: reznikova.vv78@gmail.com.

I. Introduction

In modern conditions of social development, the formation of an information society is one of the fundamental resources for the development of civilization. In the conditions of globalization of information resources, it becomes possible to integrate information systems in all countries without exception by joining a common information space, accumulating global information and telecommunication networks, and gradually introducing modern information technologies to all areas of social life.

The tendency to increase the openness of society, the wide use of information and communication technologies create prerequisites for possible illegal actions regarding information, its users, as well as information communication systems, which leads to a decrease in the level of information security of the state.

Information security is an important integral component of the state's national security. The creation of a developed and protected environment is the main condition for the development of society and the competitiveness of the state. An effective system of measures to ensure information security of citizens, society and the state makes it possible to timely warn and identify potential and real threats to national interests and prevent losses in the socio-economic sphere. At the same time, information security is one of the highest priorities for the modern state, as well as a factor for its stable development. It is quite logical that constant failures in the information security system can cause man-made, socio-political changes, or can affect the activities of state administration bodies.

The state of information security is influenced by both internal and external factors: the political situation in the state and in general in the world, the general level of economic, social and informational development of the country. Interested in the development of this sector are not only business structures that actively apply innovations in this area, but also state institutions, for which the issue of national security is the most important. Therefore, the need for national security belongs to the conceptual foundations of society. All this necessitates a thorough study of the "state information security" category. It is also worth noting that in the conditions of full-scale military aggression of the Russian Federation against Ukraine, achieving an appropriate level of information security is particularly relevant.

The analysis of the latest research and publications indicates the relevance of analyzing the current state of information security among scientists, among whom it is necessary to note the works of: Hryshchuk et al. (2020), who in his work analyzes information security from the perspective of the normatively regulated security state of the entire Ukrainian information space. Also, such a space is provided by appropriate legal means and has a number of legal indicators that can objectively reflect: the level of legal culture and legal awareness; the level of general crime and some of its varieties; reflect the overall quantity and quality of legal material; include legal gaps and ineffectiveness of individual legal acts that regulate information security; general shortcomings in the execution of court decisions, etc. In the study of Kostyanaya et al. (2021) it was concluded that information is an extremely important indicator or part of public life, in connection with which access to timely and reliable information, provided by the activities of the state and mass media,

becomes an important component in supporting the principle of the rule of law and development of civil society. According to their analysis, the information that accumulates in today's conditions can easily go beyond the borders of one state, which, among other things, confirms the importance of having international standards for ensuring the right to access to information. Gorbachev and Dibrov (2021) determined that it is the information plane that has a dual purpose. Thus, directors in the dialogues and monologues of various actors can represent the informational environment of military-political conflicts, within the framework of the films they analyze, to some extent polar, in particular: friends-strangers, barbarians-civilization, or those who make unforgivable mistakes, etc. Such a unique structure is usually displayed quite simply. Another important work is the study of Dutchak et al. (2020), within which reasoned conclusions were made regarding the development of international legal acts in the field of Internet communication and which could define key concepts and apply to such relations in order to prevent possible collisions in the legislation of other states. It is such documents that should contain relevant issues for the international community regarding the jurisdiction of states in the public network space. At the same time, only in the case of successful regulation of Internet communications at the international and national levels can we count on positive dynamics in all spheres of social life in the future and take into account the significant impact of the Internet on global processes, including international relations. The purpose of the study is a comprehensive analysis of the current legislation of Ukraine and scientific works of Ukrainian and foreign scientists in the field of information security.

This analysis highlights opportunities for international cooperation in enhancing Ukraine's information security. Collaborative measures with allied nations and global organizations can provide access to advanced cybersecurity technologies, shared intelligence on emerging threats, and collective strategies to counteract disinformation campaigns.

II. Methodology

In the process of analyzing the current state of information security in Ukraine, a complex of general scientific and special legal methods was used. In particular, with the help of general scientific methods of analysis and synthesis, the concept of information security was analyzed and its definition was provided. The relationship between national security and society's information security was determined using the dialectical method of cognition. The system-structural method was used in the formation of the classification model of legal norms that influence the information sphere and security, as well as the classification of information security by categories depending on the locality of the military aggression of the Russian Federation. The special legal method was used to determine the legal nature of the studied phenomena and formulate the relevant legal concepts.

The research was carried out using three successive stages:

- * At the first stage, an analysis of doctrinal works was carried out regarding the essence and modern understanding of information security. It was found that information security is a key characteristic of national security, which reflects the state and society's protection against unreliable information influence.

- * At the second stage, the analysis of the main normative legal acts in the field of information security was carried out and some of them were characterized. As of 2022, there are about fifty regulatory and sub-legal regulatory acts that will regulate and define the field of information security in Ukraine. Four categories of legal norms influencing the information sphere and security were also identified: legal norms defining key goals and objectives, as well as directions of state activity in the information sphere; legal norms defining subjects of state support (regulation) in the information sphere, as well as their administrative and legal status; legal norms determining the procedure for the interaction of subjects of state power with the relevant subjects of information and communication relations; legal norms regulating the administrative and legal status of subjects of information relations.
- * At the third stage, conclusions were drawn and the impact of military aggression on Ukraine's information security was clarified. In particular, it was emphasized that the information propaganda of the Russian Federation began long before the full-scale invasion of the territory of Ukraine and even before the occupation of Crimea. This was confirmed by the presence of false and distorted information about the history of Ukraine, its territories that belonged to Kievan Rus since the time. The need to develop a Strategy/Concept that will determine the specifics of access to population information, depending on the locality of the Russian Federation's military aggression, has also been proven.

During the analysis of the current state of information security of Ukraine, the following legal acts were used: Law of Ukraine "On National Security of Ukraine" (Verkhovna Rada of Ukraine, 2018), Law of Ukraine "On Information" (Verkhovna Rada of Ukraine, 1996), Law of Ukraine "On Concept of the National Informatization Program" (Verkhovna Rada of Ukraine 1998), Law of Ukraine "On the Basic Principles of Information Society Development in Ukraine for 2007–2015" (Verkhovna Rada of Ukraine, 2007), Law of Ukraine "On the Cabinet of Ministers of Ukraine" (Verkhovna Rada of Ukraine, 2014), Law of Ukraine "On Television and Radio Broadcasting" (Verkhovna Rada of Ukraine, 1996), Law of Ukraine "On Telecommunications" (Verkhovna Rada of Ukraine, 2003), Decree of the President of Ukraine "Doctrine of Information Security of Ukraine" (Verkhovna Rada of Ukraine, 2017).

III. Results and Discussion

The essence of the modern understanding of information security

In the process of the development of the information society and the improvement of information and communication technologies, a certain transformation of social relations took place, because the gradual introduction of informatization in the future benefits the shift of emphasis on business development, the increase of efficiency in all spheres of social relations and the life of society as a whole. The rapid development of information technologies is primarily aimed at their gradual introduction into the economic potential of the state, which makes it possible to change the understanding of the unified information space. In a certain way, there was also a renewal of economic relations and their transfer

to the information space. It is within such a space that the production of intellectual (informational) products (including works, goods and services) has gained significant importance, and the overall speed of information transmission has also increased (Lytvyn et al., 2021). The state information policy, defined in modern concepts and strategies in all spheres of public life, leads to an accelerated increase in the use of personal data by officials in their activities. Along with the emergence of new intellectual property and the latest information technologies, new problems arise regarding their protection (Bukhanevych et al., 2021). In today's conditions, in times of full-fledged information dependence of society, when the role of mass media in the world market is increasing, of course, issues related to ensuring the appropriate level of information for each person remain relevant. The second important aspect is the implementation of the appropriate regulation of the right to information, which can be obtained from various sources, such as mass media or telecommunications. Information is an important component of social life, and therefore ensuring priority access to timely and reliable information is a priority of our state. In addition, freedom in the information plane, including, provides freedom of access to information, and this is an indicator of democracy and effective respect for the provision of human rights (Kostyanaya et al., 2021).

The use of special forms and methods of state management of information security is explained by the need for a timely response to military or political threats. In such cases, the state is always the key subject of information security (Hryshchuk et al., 2020).

Particular attention is paid to the problems related to guaranteeing the information security of Ukraine caused by anti-Ukrainian influences that carry ideas of violence, separatism, as well as national enmity, that is, in their essence, they are attempts to destroy the national authenticity of Ukraine, contain manifestations of encroachment on the constitutional system of Ukraine, encroach on its territorial integrity. The problem of information security became especially noticeable, with the growth of hostilities on the territory of Ukraine in the conditions of a full-scale invasion of the Russian Federation. Although long before the full-scale invasion, the Russian Federation was spreading false information about the Ukrainian nation and its territories on its information resources.

After all, information is always the basis for the rational and safe development of the modern information society. At the same time, information can also be a weapon capable of influencing the worldview of a person, the entire population, in turn forming a negative attitude towards certain phenomena, towards the state or society as a whole, because it can distort events and facts, which affects the quality and effectiveness of modern reforms in society, etc.

The National Security Strategy of Ukraine calls the conduct of information warfare in Ukraine in the absence of a comprehensive communication policy, as well as the unsatisfactory level of media culture among society, as particularly tangible threats to national security (Bielay and Korniienko, 2018). In addition, the issue of cyber security is also gaining special importance. Increasingly, it is the information space that is the arena for conducting a wide range of subversive operations, from theft of valuable information to large-scale acts of cyberterrorism (Gurzhiy, 2018).

As for the very essence of the concept of “information security”, according to Chmyr is an independent component of state security, which has a dual legal nature. This is due to the following factors:

- * “the aspiration of each state to realize and protect its own national interests aimed at the formation and accumulation of national information potential in the conditions of globalization of world information processes”;
- * “the existing possibility of informational pressure on Ukraine, even informational aggression on the part of the developed countries of the world with the aim of obtaining unilateral advantages in the political, economic, military and other spheres, as well as informational influence on the consciousness and subconsciousness of individuals, on the family, society and the state, which threatens state security with the need not only to develop and strengthen the national information potential, but also to protect against a wide range of existing and potential information threats”;
- * “the existence of a real need to protect all subjects of information relations from possible negative consequences of the introduction and use of information technologies, etc.” (Chmyr, 2018).

As noted by Panchenko “information security” can contain three key components. Accordingly, the first serves to satisfy the information needs (requirements) of the subjects of the information environment. After all, it is quite logical that if the subject does not have a sufficient level of information, there will not be a sufficient level of information security. In addition, the information needs of each subject will differ, but in any case, the lack of the necessary information will have negative consequences. The second component concerns information security itself. This includes the requirements of reliability, completeness, and timeliness of information, which must be observed throughout the time of information exchange, because otherwise it may result in making wrong decisions or the inability to perceive information. Therefore, the information must be protected from influences that may violate its status. And the third component concerns the protection of the subjects of informational relations from negative informational influence (Panchenko, 2019).

Ilnytska (2016) notes that information security in the context of national security should be defined in two aspects. In the first, as an independent element of the national security of an individual country, and in the second – as an integrated component of other security: political, economic or military. At the same time, she notes that usually information security is a state of protection of important vital interests of an individual, the state or society, the presence of which minimizes the risk of damages due to unreliability, lack of timeliness or incompleteness of information.

It is worth noting that information security is a multi-level, complex and systemic phenomenon, the prospects and state of which are directly influenced by internal and external factors. Key among such factors is: state and level of information and communication development of the state; the presence of potential internal and external threats; the political situation in the world; the state of politics within the state. At the same time, information security is a social, complex and dynamic system, the components of which are state, society and individual security subsystems (Zolotar, 2018).

Lipkan (2009) rightly notes that the information security of Ukraine is an organic component of national security, and therefore it is necessary to ensure the proper state of regulatory and legal support for such a process. The scientist is convinced that it is effective information legislation that can influence the consolidation of the state information policy, which includes, among other things, the achievement of an appropriate level of national security in the information field.

Integration of Comparative Analysis based on two counties: Finland and Estonia

Examples from other countries facing similar challenges demonstrate the value of a comprehensive approach. To compare, we will examine the experiences of Finland and Estonia. For instance, Estonia's experience in countering cyberattacks through investments in digital infrastructure and education provides valuable lessons. Similarly, Finland's proactive disinformation education initiatives underscore the importance of preparing society to critically assess information.

Estonia, despite being a small state, has established itself as a leader in cybersecurity, leveraging its extensive expertise to provide critical support to Ukraine in the aftermath of Russia's invasion in February 2022. Estonia has played a vital role in protecting Ukrainian digital infrastructure and ensuring cybersecurity resilience, emphasizing practical and diplomatic efforts through initiatives such as the creation of the IT Coalition and the Tallinn Mechanism. These achievements reflect Estonia's longstanding commitment to cybersecurity and its ability to act as a facilitator for coordination during times of chaos (Crandal, 2024).

Initially, Estonia refrained from using its cyber support for Ukraine as an opportunity to enhance its global status. This decision was shaped by the urgency of the crisis and the prioritization of military support messaging. However, as the situation stabilized, Estonia began integrating status-seeking strategies while maintaining its focus on effective cyber assistance. Furthermore, Estonia's efforts highlight the importance of international collaboration and learning from Ukraine's experiences to build mutual cyber resilience (Crandal, 2024).

These contributions underscore Estonia's high level of cybersecurity expertise and its recognition as a global leader in this domain. By combining technical innovation with strategic diplomacy, Estonia continues to set a benchmark for leveraging cybersecurity to support allied nations during critical times.

Finland, as a leader in digitalization and cybersecurity, can offer valuable support to Ukraine in strengthening its information security amid ongoing challenges. With its high standard of cybersecurity and globally recognized expertise, Finland is well-positioned to assist Ukraine in building robust digital defenses. Finnish collaboration between public and private sectors, which has been instrumental in its own success, could serve as a model for Ukraine to enhance its public-private partnerships in the information security domain (Paananen et al., 2024).

Finland could support Ukraine by sharing best practices in digital infrastructure protection and by providing technical assistance in developing cybersecurity frameworks. Training

programs facilitated by Finnish experts could target Ukrainian public officials, IT specialists, and military personnel to improve their capabilities in countering cyberattacks and disinformation. Moreover, Finland's experience in raising public awareness through campaigns to build societal resilience against misinformation could be adapted to Ukraine's context, helping to mitigate the effects of propaganda (Paananen et al., 2024).

By fostering bilateral cooperation, Finland and Ukraine could work towards establishing a shared understanding of emerging threats and jointly developing strategies to address them. This partnership would not only strengthen Ukraine's immediate defenses but also contribute to the development of long-term information security resilience in both nations, enhancing stability in the broader region (Paananen et al., 2024; Crandal, 2024).

Immediate actions for policymakers should include countering propaganda through unified communication strategies and fortifying cybersecurity infrastructure to defend against cyberattacks. Specifically, targeted training programs for military personnel and public officials can mitigate phishing risks, while public awareness campaigns can enhance societal resilience to disinformation.

In conclusion, Ukraine's information security strategy must integrate these lessons while fostering international partnerships. Strengthening legislative frameworks, enhancing institutional capacity, and promoting public-private collaboration will be pivotal in ensuring Ukraine's resilience against current and future information threats. This approach not only addresses immediate risks but also establishes a foundation for long-term stability and security in the digital age.

Analysis of the main legal acts in the field of information security in Ukraine

Information security is a key characteristic of national security, which reflects the state and society's protection against unreliable informational influence.

If we consider the regulatory and legal guarantees of information security, it should be noted that as of 2022 there are about fifty regulatory and sub-legal regulatory acts that will regulate and define the field of information security in Ukraine. In particular, within the scope of the study, it is worth considering some of such normative legal acts. Among the key normative legal acts, it is necessary to single out the Law of Ukraine "On National Security" and the "Doctrine of Information Security of Ukraine" (Verkhovna Rada of Ukraine, 2017).

The Law of Ukraine "On National Security" defines that "state policy in the spheres of national security and defense is aimed at protecting: people and citizens – their lives and dignity, constitutional rights and freedoms, safe living conditions; society – its democratic values, well-being and conditions for sustainable development; of the state – its constitutional system, sovereignty, territorial integrity and inviolability; territory, natural environment – from emergency situations" (Verkhovna Rada of Ukraine, 2018).

Important aspects accumulated by the current version of the Information Security Doctrine of Ukraine – there is a definition of real threats to the national security of Ukraine specifically in the information sphere, namely: "situations, instigation of inter-ethnic and inter-confessional conflicts in Ukraine; implementation of special information operations

aimed at undermining defense capabilities, demoralizing the personnel of the Armed Forces of Ukraine and other military formations; the ineffectiveness of the state information policy, the imperfection of the legislation regarding the regulation of public relations in the information sphere, the uncertainty of the strategic narrative, the insufficient level of media culture of the society; information dominance of the aggressor state in the temporarily occupied territories; conducting special information operations by the aggressor state in other states with the aim of creating a negative image of Ukraine in the world; information expansion of the aggressor state and its controlled structures, in particular by expanding its own information infrastructure on the territory of Ukraine and in other states; insufficient development of the national information infrastructure, which limits Ukraine's ability to effectively counter information aggression; spread of calls for radical actions, propaganda of federalism and separatism in Ukraine. It is worth noting that the modern Information Security Doctrine fully complies with international standards in the field of national security" (Verkhovna Rada of Ukraine, 2017).

Taking into account the fact that a significant number of legal norms influence the information sphere and security, it is worth making a certain classification of such norms for a more systematic representation and perception. At the same time, it should be noted that it is more expedient to distinguish such norms depending on the object of state regulation and combine them into four groups:

- * legal norms that determine the key goals and tasks, as well as the directions of the state's activity in the information sphere (these include the norms enshrined in Articles 3, 10, 17, 31, 32, 34 of the Constitution of Ukraine (Verkhovna Rada of Ukraine, 1996), in Article 6 of the Law of Ukraine "On Information", the Law of Ukraine "On the Basic Principles of the Development of the Information Society in Ukraine for 2007–2015"; in Chapters IV, VI of the Law of Ukraine "On the Concept of the National Informatization Program", including others that have purposeful importance for the proper functioning of the entire state administration system in the information sphere.
- * legal norms defining subjects of state support (regulation) in the information sphere, as well as their administrative and legal status. In addition to the above-mentioned norms of the Constitution of Ukraine concerning bodies in the field of information, also here can be attributed the norms that determine the legal status of individual state authorities. For example, Art. 20 of the Law of Ukraine "On the Cabinet of Ministers of Ukraine" also defines the authority to carry out state policy in the field of informatization, to promote the creation of a unified information space, etc. (Verkhovna Rada of Ukraine, 2014).
- * legal norms determining the procedure for the interaction of subjects of state power with the relevant subjects of information and communication relations. It is possible to include legal norms regarding the procedure for applying certain methods of state regulation in the information sphere. An example of such norms is Art. 23–37 of the Law of Ukraine "On Television and Radio Broadcasting", which determine the procedure for implementing such a method of regulation as licensing in the field of television and radio broadcasting (Verkhovna Rada of Ukraine, 1993).

- * legal norms regulating the administrative and legal status of subjects of information relations. For example, it is possible to cite Art. 39 of the Law of Ukraine “On Telecommunications”, accordingly, telecommunications operators are assigned the obligation to “timely submit annually to the central executive authority in the field of communications information about their telecommunications networks for working out mobilization plans; at their own expense, to install on their telecommunications networks the technical means necessary for the implementation of operative-search measures by the authorized bodies, and to ensure the functioning of these technical means, as well as to facilitate the implementation of operational-search measures, etc.” (Verkhovna Rada of Ukraine, 2003).

As you can see, there is a fairly significant number of legal norms that in a certain way affect the sphere of information security in Ukraine, while such influence can be indirect or tangential to information security. The system of information security of the state can be described as a separate part of the general system of national security, which is a set of state bodies, non-state institutions and citizens who have the duty to coordinate the implementation of activities to ensure the information security of the population through the use of uniform norms of rights and to effectively counter information threats based on modern conditions.

The state of influence of military aggression on the information security of Ukraine

An important aspect for ensuring information policy was also the adopted Decree of the President of Ukraine No. 152/2022 of March 19, 2022, which implemented the decision of the National Security and Defense Council of Ukraine of March 18, 2022 “Regarding the implementation of a unified information policy under martial law”. Its essence lies in the fact that nationwide TV channels, whose programming content consists mainly of informational and/or information-analytical programs, are united on a single informational platform of strategic communication – a 24-hour informational marathon “Unified News #UArazom”. This helps the population to receive round-the-clock, reliable news about the news of martial law in Ukraine (Verkhovna Rada of Ukraine, 2022a).

In view of the full-scale invasion of the Russian Federation, temporarily occupied territories are emerging that require special protection from the state, which must ensure, among other things, uninterrupted access to information. In this regard, we propose to classify the provision of information security by categories: information security for the population of Ukraine that was not occupied and lives in relatively “peaceful” territories; information security for the armed forces of Ukraine, military personnel, and medics performing their duties for the protection of the population, taking a direct part in military aggression against the enemy; information security for citizens of Ukraine located in the temporarily occupied territories, including the Autonomous Republic of Crimea. Based on this classification, the legislative body needs to consider the possibility of developing appropriate Strategies/Concepts that will determine the specifics of access to population information depending on the locality of the military aggression of the Russian Federation. Separately, I would like to mention the Law of Ukraine “On Amendments to the Criminal

and Criminal Procedural Codes of Ukraine on Ensuring Counteraction to the Unauthorized Dissemination of Information on the Delivery, Transfer of Weapons, Weapons, and War Supplies to Ukraine, the Movement, Transfer, or Placement of Armed Forces” adopted in the first months of the full-scale invasion Forces of Ukraine or other military formations formed in accordance with the laws of Ukraine, committed under conditions of war or a state of emergency, according to which criminal liability was introduced for the distribution of photos and video recording of any information about the positions of our military, as well as the movement of armed formations and weapons (Verkhovna Rada of Ukraine, 2022b). Such actions of the legislator in a certain way were justified by the increasingly frequent publications on the Internet of photos and video materials, even of ordinary citizens of Ukraine, which could unknowingly cause harm and openly provide important information for the aggressor, thereby reducing the strength of our military. The same applies to the prohibition of photo and video recording of the arrival locations in the first minutes and the publication of such information tools on the Internet.

Regarding potential or future threats to Ukrainian information security, it is worth noting the following that in the conditions of a full-scale invasion, quite often letters appear on the e-mail addresses of Ukrainian servicemen on services such as meta and i.ua (Butina, 2022). It is in such cases that phishing attacks can be recorded, the targets of which can be individual private mailboxes of Ukrainian defenders or persons close to the latter. In this case, the aggressor does not abandon attempts and opportunities to harm the information security of our country. In such a case, an effective mechanism can be constant and long-term clarification work on preventing the opening of such files by the military, as well as determining the consequences that may be caused by such actions.

IV. Conclusion

In the conditions of modern military actions of the Russian Federation in relation to the Ukrainian territorial integrity, the information space of Ukraine is also suffering, propagandistic and psychological influences or threats are spreading. In this regard, the security and protection of state information sovereignty, as well as the creation of an effective and powerful information security system of Ukraine, is a priority task for both state bodies and non-state institutions.

Information protection is a guarantee of security and one of the primary tasks of the state. Active development within the post-industrial society leads to the fact that information becomes a full-fledged resource on the same level as economic, financial and production resources. The state of protection of the information space, which is able to ensure the realization of national interests, the preservation of the state's stability against internal and external negative factors that pose a threat and are associated with the active development of digitalization, depends on a correctly constructed system of state security management. Information security has turned into an urgent global problem of our time. It should be considered on the same level as the problems of preserving and developing culture, ending war and armed conflicts, ensuring economic, ecological, demographic and energy security. The legislative body should consider the possibility of developing Strategies or Concepts that will determine the specifics of access to public information depending on the locality

of the military aggression of the Russian Federation. After all, the level of access to information of the population living in temporarily occupied territories is significantly different from the similar access of the population living in relatively “peaceful” territories.

In the context of Ukraine’s ongoing conflict and the associated challenges to its information security, this study underscores the critical need to strengthen the state’s capacity to safeguard its information space. Ukraine’s information sovereignty is continuously under threat from propaganda, cyberattacks, and disinformation campaigns, emphasizing the importance of a robust and adaptive information security framework.

In improving its information security, Ukraine can learn from leading international examples such as Finland and Estonia. Estonia’s effective coordination mechanisms, such as the IT Coalition and the Tallinn Mechanism, provide a model for rapid crisis response. Similarly, Finland’s expertise in public-private cooperation and its focus on disinformation education highlight the importance of societal resilience and strategic partnerships. This will allow Ukraine to strengthen the legal framework, promote cooperation, and build a robust defence against current and future information threats.

References

- Bielay, S. V., Korniienko, D. M. (2018). *Today’s information security is an integral part of military security. In Actual problems of information security management of the state: collection of abstracts of reports of scientific and practical conference* (pp. 12–14). Kyiv: National Academy of Security Service of Ukraine.
- Bukhanevych, O., Koropatnik, I., Zubov, O., Lytvyn, N., Havrylyuk, R. (2021). Mechanism of administrative and legal regulation of the use of personal data by local governments. *Amazonia Investiga*, 10(48), 218–227.
- Butina, M. (2022). Cyber defense during the war: How to protect yourself and your business from cyber-attacks. *LIGA:ZAKON*. Retrieved from https://biz.ligazakon.net/analitics/210086_kberzakhist-pd-chas-vyni-yak-ubezpechiti-sebe-ta-svy-bznes-ud-kberatak.
- Chmyr, Ya. I. (2018). Problems of information security in the system of public administration. *Aspects of Public Administration*, 6(9), 16–22.
- Crandall, M. (2024). Understanding Estonia’s Cyber Support for Ukraine: Building Resilience, Not Status. *Applied Cybersecurity & Internet Governance*, 3(1), 78–90. <https://doi.org/10.60097/ACIG/190396>.
- Dutchak, S., Opolska, N., Shchokin, R., Durman, O., Shevtsov, M. (2020). International aspects of legal regulation of information relations in the Global Internet Network. *Journal of Legal, Ethical and Regulatory Issues*, 23(3). Retrieved from <https://www.abacademies.org/articles/international-aspects-of-legal-regulation-of-information-relations-in-the-global-internet-network-9305.html>.
- Gorbachev, M. V., Dibrov E. A. (2021). Transformation of the information space of the military-political conflict zone in Donetsk and Luhansk. *Journal of Legal, Ethical and Regulatory Issues*, 24(1). Retrieved from <https://www.abacademies.org/articles/transformation-of-the-information-space-of-the-militarypolitical-conflict-zone-in-donetsk-and-luhansk-11295.html>.

- Hryshchuk, V., Hryshchuk, O., Fedina, N., Parasiuk, V., Batiuk, O. (2020). Administrative and legal mechanism of information security in Ukraine. *Journal of Legal, Ethical and Regulatory Issues*, 23(5). Retrieved from <https://www.abacademies.org/articles/administrative-and-legal-mechanism-of-information-security-in-ukraine-9698.html>.
- Hurzhii, T. (2018). Information law: The challenges of hybrid warfare. *Foreign Trade: Economics, Finance, Law*, 4, 16–26.
- Ilnytska, U. (2016). Information security of Ukraine: Current challenges, threats and mechanisms for counteracting negative information and psychological influences. *Humanitarian Vision*, 2(1), 27–32.
- Kostyanaya, Yu., Kulzhabaeva, Zh., Abaydeldinov, E., Tlepina, Sh., Sabirov, K. (2021). International legal standards for implementing the right to access to information. *Journal of Legal, Ethical and Regulatory Issues*, 24(4). Retrieved from <https://www.abacademies.org/articles/international-legal-standards-for-implementing-the-right-to-access-to-information-10705.html>.
- Lipkan, V. A. (2009). *National security of Ukraine*. Kyiv: KNT.
- Lytvyn, N. A., Boreyko, N. M., Artemenko, O. V., Subina, T. V., Sliusarenko, S. V. (2021). Taxation of E-commerce as one of the phenomena of society development. *Studies of Applied Economics*, 39(9). <https://doi.org/10.25115/eea.v39i9.5657>.
- Paananen, R., Soikkeli, M., Aro, M., Kuusisto, T., Rusila, T., Tuulensuu, T. (2024). *Finland's Cyber Security Strategy 2024–2035*. Helsinki: Prime Minister's Office.
- Panchenko, O. A. (2019). Problems of legal support of the state management of information security. *Public Administration: Improvement and Development*, 11. <https://doi.org/10.327-02/2307-2156-2019.11.3>.
- Verkhovna Rada of Ukraine. (1992). *Law of Ukraine No. 2657-XII "On information"*. Retrieved from <http://zakon.rada.gov.ua/laws/show/2657-12>.
- Verkhovna Rada of Ukraine. (1993). *Law of Ukraine No. 3759-XII "On television and radio broadcasting"*. Retrieved from <http://zakon.rada.gov.ua/laws/show/3759-12>.
- Verkhovna Rada of Ukraine. (1996). *Constitution of Ukraine*. Retrieved from <https://zakon.rada.gov.ua/laws/show/254к/96-bp>.
- Verkhovna Rada of Ukraine. (1998). *Law of Ukraine No. 75/98-VR "On the Concept of the National informatization program"*. Retrieved from <https://zakon.rada.gov.ua/laws/show/75/98-bp>.
- Verkhovna Rada of Ukraine. (2003). *Law of Ukraine No. 1280-IV "On telecommunications"*. Retrieved from <http://zakon.rada.gov.ua/laws/show/1280-15>.
- Verkhovna Rada of Ukraine. (2007). *Law of Ukraine No. 537-V "On the Basic principles of information society development in Ukraine for 2007–2015"*. Retrieved from <https://zakon.rada.gov.ua/laws/show/537-16>.
- Verkhovna Rada of Ukraine. (2014). *Law of Ukraine No. 794-18 "On the Cabinet of Ministers of Ukraine"*. Retrieved from <http://zakon2.rada.gov.ua/laws/show/794-18>.
- Verkhovna Rada of Ukraine. (2017). *Decree of the President of Ukraine No. 47/2017 "Doctrine of information security of Ukraine"*. Retrieved from <http://zakon.rada.gov.ua/laws/show/47/2017>.

Verkhovna Rada of Ukraine. (2018). *Law of Ukraine No. 2469-VIII “On the national security of Ukraine”*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2469-19#n355>.

Verkhovna Rada of Ukraine. (2022a). *Decree of the President of Ukraine No. 152/2022 “On the implementation of the decision of the National Security and Defense Council of Ukraine of March 18, 2022” “On the implementation of a unified information policy in martial law”*. Retrieved from <https://www.president.gov.ua/documents/1522022-41761>.

Verkhovna Rada of Ukraine. (2022b). *Law of Ukraine No. 2160-IX “On Amendments to the Criminal and Criminal Procedure Codes of Ukraine on Ensuring Countermeasures against the Unauthorized Dissemination of Information on the Dispatch, Movement of Weapons, Weapons, and War Supplies to Ukraine, Movement, Movement, or Placement of the Armed Forces of Ukraine or other military formations formed in accordance with the laws of Ukraine, committed under conditions of war or a state of emergency”*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2160-20#Text>.

Zolotar, O. O. (2018). *Human information security: Theory and practice*. Kyiv: ArtEk Publishing House.