UDK 342.9
DOI https://doi.org/10.24144/2307-3322.2025.91.3.30

# INFORMATION SECURITY AS A COMPONENT OF THE STATE'S INFORMATION POLICY

**Rizenko O.V.,**
*Candidate of Law, Associate Professor,*
*Associate Professor of the Department*
*of Administrative and Information Law,*
*Institute of Law, Psychology and Innovative Education*
*of the National University «Lviv Polytechnic»*
*ORCID: 0009-0006-9525-1719*
*e-mail: Olena.V.Rizenko@lpnu.ua*

**Rizenko O.V. Information security as a component of the state's information policy.**

It is emphasized that ensuring the consistent and systematic activity of state and legal institutions aimed at the effective realization of national interests in the field of information security is of paramount importance. Military actions in Ukraine have caused a number of legal restrictions on the rights of citizens, in particular, on traveling outside the state, and, in part, on access to certain types of information that are closed during the war. Such issues are resolved by state bodies and subjects of state policy in the field of information security, which can be conditionally divided into two main groups: state bodies that directly implement information policy and mass media and communication structures. It is established that it is important to develop international cooperation in the field of information security, because in the modern globalized space, states can jointly resist cybercrime, the spread of unfair, illegal propaganda. The information policy of Ukraine is one of the key mechanisms for supporting and implementing the state's European integration course. Its main goal is to increase the level of awareness of the population, promote the implementation of reforms and ensure the gradual entry of Ukraine into the European space.

Ukraine has developed an «Information Security Strategy», which outlines the main challenges and threats facing the national security of Ukraine in the information sphere. The document defines strategic guidelines, goals and objectives aimed at countering these threats, ensuring the right of citizens to access information, as well as protecting personal data.

It has been proven that information security is implemented on the basis of a number of fundamental principles of general national security and reflects the degree of protection of key national values.

Today, it is important that the state's information policy is aimed at combating enemy sabotage in the information space. This approach involves: development and improvement of legislation regulating information security in the state; interaction of law enforcement agencies with the population regarding warnings about provocations in the information space; formation of information culture among citizens.

**Key words:** information security, state information policy, information space, citizens' rights, information security legislation.

**Різенко О.В. Інформаційна безпека як складова інформаційної політики держави.**

Зазначено, що важливо забезпечувати послідовну та системну діяльність державних і правових інституцій, спрямовану на ефективну реалізацію національних інтересів у сфері інформаційної безпеки. Воєнні дії в Україні стали причиною ряду законних обмежень прав громадян, зокрема, на виїзд за межі держави, і, частково, на доступ до інформації певного типу, що під час війни є закритою. Такі питання вирішують державні органи і суб'єкти державної політики у сфері інформаційної безпеки, які умовно можна поділити на дві основні групи: державні органи, що безпосередньо реалізують інформаційну політику і засоби масової інформації та комунікаційні структури.

Встановлено, що важливо розвивати міжнародну співпрацю у сфері інформаційної безпеки, адже в сучасному глобалізованому просторі держави спільно можуть протистояти кіберзлочинності,

поширенню недобросовісної, протиправної пропаганди. Інформаційна політика України виступає одним із ключових механізмів підтримки та реалізації євроінтеграційного курсу держави. Її основна мета полягає у підвищенні рівня поінформованості населення, сприянні впровадженню реформ і забезпеченні поступового входження України до європейського простору.

В Україні розроблена «Стратегія інформаційної безпеки», що окреслює основні виклики та загрози, що постають перед національною безпекою України у сфері інформації. У документі визначено стратегічні орієнтири, цілі та завдання, спрямовані на протидію цим загрозам, забезпечення права громадян на доступ до інформації, а також захист персональних даних.

Доведено, що інформаційна безпека реалізується на основі низки фундаментальних принципів загального забезпечення національної безпеки та відображає ступінь захищеності ключових національних цінностей.

Сьогодні важливо щоб інформаційна політика держави була спрямована на боротьбу з диверсіями ворога в інформаційному просторі. Такий підхід передбачає: розвиток та удосконалення законодавства, що регулює питання інформаційної безпеки в державі; взаємодію правоохоронних структур з населенням щодо попередження про провокації в інформаційному просторі; формування в громадян інформаційної культури.

**Ключові слова:** інформаційна безпека, інформаційна політика держави, інформаційний простір, права громадян, законодавство про інформаційну безпеку.

**Problem statement.** Today in Ukraine, the issue of security is relevant both at the national level and in the international arena. Russia's military aggression against Ukraine has brought to the forefront, along with the problem of national security, the issue of security in the information space.

The information policy of the state should be aimed at ensuring and implementing the fundamental rights of citizens and their security. For proper information security, authorized state bodies should form an appropriate regulatory and legal framework that will clearly regulate and regulate the use of the information space. It is important to prevent violations of citizens' rights to information, as well as to prevent the aggressor from interfering in the information space of our state with the aim of manipulating citizens' consciousness and committing provocative actions.

The information policy of the state should be aimed at solving the problem of forming an information culture among citizens and ensuring the security of using information resources and sources.

**Analysis of recent research and publications.** Important aspects of the formation and development of information security as a component of the state's information policy are highlighted by such Ukrainian scientists as G. Bondar, S. Yesimov, Yu. Kobets, M. Kovaliv, S. Leshyk, O. Lipchuk, I. Lomaka, Yu. Nikolayets, T. Savosko, D. Smotrych, V. Tereshchenko, M. Shevchuk, O. Yarema. It should be noted that although the issues of information security as a component of national security have been developed by scientists, the issue of regulatory and legal regulation of information security during the period of military operations in Ukraine requires research.

**The purpose of the article** is to study information security as a component of the state's information policy and the features of regulatory and legal regulation of the issue of information security during a crisis period in the development of society.

**Presentation of the main material.** The information policy of the state is regulated by legislation and a number of subordinate regulatory legal acts. According to the Law of Ukraine «On Information», the key areas of state information policy are: guaranteeing free access to information for every citizen; ensuring equal conditions for the creation, collection, receipt, storage, use, dissemination, protection and defense of information; creating favorable conditions for the development of the information society in Ukraine; ensuring openness and transparency of the activities of state authorities and local self-government bodies; developing information systems and networks, as well as developing e-government; constant updating, replenishment and preservation of national information resources; guaranteeing the information security of the state; developing international cooperation in the field of information and integrating Ukraine into the global information space.

The right to information means that every person has the opportunity to freely receive, store, use, disseminate and protect information necessary for the exercise of their rights, freedoms and legitimate interests. At the same time, the exercise of this right should not violate the public, political, economic, social, spiritual, environmental and other rights and freedoms of other persons, as well as the interests of legal entities [1].

Military actions in Ukraine have led to a number of legal restrictions on the rights of citizens, in particular, on travel outside the state, and, in part, on access to certain types of information that are closed during the war.

Such issues are resolved by state bodies and subjects of state policy in the field of information security. They can be conditionally divided into two main groups: a) state bodies that directly implement information policy; b) mass media and communication structures.

The state occupies a special place among the subjects of both information policy and the information security system, because it is it that has specific resources, powers and tools to counter information threats. The system of state information security has a clear structure, encompassing four main power subsystems that form the branches of government in accordance with their competences in this area: the institution of the head of state, the legislative, executive and judicial branches [2, pp. 42–49].

In addition to the legislative and executive bodies of individual states, there are a number of influential international organizations, interest groups, specialized institutions and institutes in the world that are engaged in the development of basic principles, directions, research and practical mechanisms for implementing information policy. The main tasks of such structures are to determine priority areas of technical development that can have a significant social impact, support scientific research in the field of alternatives to state policy, as well as contribute to increasing the level of public support and developing dialogue between specialists working on the creation and implementation of technologies in the process of implementing information policy [3, pp. 22–28].

It is important to develop international cooperation in the field of information security, because in the modern globalized space, states can jointly resist cybercrime, the spread of unscrupulous, illegal propaganda.

The information policy of Ukraine is one of the key mechanisms for supporting and implementing the European integration course of the state. Its main goal is to increase the level of awareness of the population, promote the implementation of reforms and ensure the gradual entry of Ukraine into the European space.

The main areas of implementation of information policy include: 1) improving the legislative and regulatory framework in the field of information; 2) conducting large-scale information campaigns aimed at raising citizens' awareness of the processes of European integration. Ensuring the stable functioning of independent mass media and supporting the activities of public organizations that contribute to the development of a democratic information space [4, pp. 53–60].

Ukraine has developed an "Information Security Strategy", which outlines the main challenges and threats facing Ukraine's national security in the information sphere. The document defines strategic guidelines, goals and objectives aimed at countering these threats, ensuring citizens' right to access information, and protecting personal data.

The main goal of the Strategy is to strengthen the state's potential to guarantee its information security, protect the national information space, promote social and political stability, maintain defense capability, protect state sovereignty, territorial integrity, constitutional order, and respect for the rights and freedoms of every citizen.

The implementation of this goal involves the implementation of a set of measures aimed at preventing and neutralizing information threats, in particular aggressive information influences and special operations by the aggressor state, aimed at undermining the sovereignty and unity of Ukraine. Important components are strengthening the information resilience of the state and society, establishing effective interaction between authorities, local governments and the public, as well as developing international cooperation in the field of information security on the principles of partnership and mutual support [5].

Today, Ukraine is defending itself from an unprincipled enemy that violates not only the norms and rules of warfare, but also the general principles of the existence of a civilized society. We see that the enemy uses disinformation, fake data, and involves minors in illegal activities. Such actions harm national security and disrupt the lawful functioning of the state's information space.

An important factor is the consistent and systematic activity of state and legal institutions aimed at the effective implementation of national interests in the field of information security. Such institutions should not only promptly respond to the spread of fake or unreliable messages, but also prevent the emergence of information conflicts, contributing to the formation of a high level of information culture in society as a whole. At the same time, taking into account the existing global threats and challenges, an important condition for effective counteraction to information aggression is the active involvement

of international organizations, institutions and the world community in this process. After all, modern practice shows that war in the information space has no state borders [6, pp. 121–127].

Information security of Ukraine is an integral part of national security. It reflects the degree of protection of key national values: state sovereignty, territorial integrity, democratic constitutional order and vital interests of citizens, society and the state. This state is ensured by the proper implementation of constitutional rights and freedoms of a person to access, collect, use and disseminate reliable and objective information. In addition, it provides for the existence of an effective system of counteraction and protection against harm caused by hostile information influences, in particular: coordinated dissemination of false data, destructive propaganda, other information operations, as well as unauthorized dissemination, use or violation of the integrity of information with limited access.

Information threat is a potential or real negative phenomena, trends or factors that arise in the information sphere and are directed against a person, society or state. Their goal is to complicate or make impossible the achievement of national interests and the preservation of national values of Ukraine. Such influences can directly or indirectly harm the interests of the state, its national security and defense.

Information measures of state defense are a set of coordinated actions that are planned and carried out by the subjects of ensuring the national security and defense of Ukraine (both in peacetime and in special, war or emergency states). These actions include forecasting, identifying and preventing information threats in the military sphere, deterring and repelling armed aggression, countering information threats from the aggressor country, as well as implementing other necessary steps within the framework of information confrontation [5].

In the context of the modern information society, dynamic changes are taking place that increase the importance of ensuring the information security of the state. Therefore, in order to more effectively counteract these challenges and achieve a high level of security for society, it is necessary to introduce a comprehensive approach to security.

Comprehensive provision of information security covers: 1. Infrastructure and citizens' rights. It is necessary to develop the information infrastructure and the data processing industry, while ensuring compliance with the rights and freedoms of citizens in cyberspace. This is the key to the security and confidentiality of information flows. 2. Informatization and professionalism. Priority should be given to the informatization of the social sphere, material production and resource management. It is also important to increase the professional level of regional management for the successful implementation of state information policy. In addition, highly qualified training of specialists in the field of information technologies is critically needed, which will ensure more reliable protection of telecommunications systems and information resources. 3. Resources and international integration. It is necessary to accumulate and store information resources for their use in the general security system, taking into account the dynamics of information changes. It is also important to stimulate the development of the information industry with the aim of its entry and competition in international markets [7, pp. 113–118].

The organizational component of information protection covers a whole range of measures. To implement these tasks, in accordance with current legislation and the regulatory framework, specialized security services or units responsible for data protection are created at all enterprises, ministries and departments (regardless of the form of ownership). The legal framework for information protection is formed on the basis of regulatory acts that enshrine fundamental human rights and freedoms, as well as establish liability for offenses in the field of information security. Ukraine has already adopted a number of key laws and regulatory documents aimed at ensuring information security. These include, in particular, the Laws of Ukraine: "On Information Protection in Information and Telecommunications Systems"; «On State Secrets»; «On the Protection of Personal Data»; «On Copyright and Related Rights». Currently, there is a need to update (new edition) the Law of Ukraine «On Information» and other relevant legislative acts to bring them into line with the standards of the Council of Europe. Information security is an integral part of the overall security system of the state. In essence, it is a coordinated activity carried out by state authorities, non-state organizations and citizens in the information sphere on the basis of current legislation [8, pp. 82–87].

Information security is classified by its scope of application into three main categories: state security, organizational security and personal security.

Information security can be classified into [9, p. 329]:

1. Information security of the state. This is the level of protection of key interests of citizens, society and the state itself, at which it is impossible to cause harm due to a number of factors: – use of incomplete, untimely or false information; – negative impact in the information space; – destructive consequences from the use of information technologies; – unauthorized distribution, use or violation of the integrity, confidentiality and availability of information resources.

2. Information security of the organization. It is interpreted as a purposeful activity of management bodies and responsible persons. It involves the use of permitted methods and resources to achieve such a state of security of the information environment that guarantees its stable operation and dynamic development.

3. Information security of the individual. It is characterized as a state of protection of a person, various social groups and associations from external influences that can, against their will and desire, lead to a change in the mental state and psychological characteristics, modify behavior and limit freedom of choice.

Information security is implemented on the basis of a number of fundamental principles of general national security. The key principles of this system include the priority of individual rights, which consists in recognizing the highest value of the rights and freedoms of a person and a citizen. Also, the rule of law (strict adherence to the rule of law in all processes), peaceful settlement (giving preference to contractual (peaceful) instruments for resolving any conflicts), adequate response (ensuring the timeliness and compliance of measures to protect national interests with the level of real and potential threats, (cooperation and separation of powers (clear division of functions and effective interaction between state bodies involved in the field of national security), democratic oversight (implementation of democratic civilian control over the activities of the Military Organization and other structures included in the national security system), international integration (use of mechanisms and systems of international collective security in the interests of Ukraine [9, p. 331].

Highly qualified specialists should be involved in the development of technologies and means that ensure information security. Also, an important factor is working with the population. Citizens should develop a culture of using, perceiving and processing information, especially during a crisis period in the development of society.

V.V. Tereshchenko notes that The strength and stability of the social system directly depend on the level of coordination of actions between state administration bodies and the mass media (media). Such cooperation provides a two-way connection between civil society and the state. War and the hostile information policy of the aggressor state are aimed at sowing beliefs in instability and worsening of the socio-economic situation. This activates destructive factors of a political and ideological nature that pose a threat to national values, ideals and traditions. Ultimately, such actions destroy the structures of socialization of the individual and create a danger to the vital activity of a person, society and the state as a whole. The long process of reforming socio-political relations in Ukraine has set a strategic task for scientists, politicians and statesmen: to develop an effective state information policy. It should serve as an instrument for regulating the interaction of all elements of the socio-political system, primarily the state, civil society and the media. Success in The solution of this problem directly depends on the level of political culture of society, the maturity of its political consciousness, and the adequacy of political ideology to socio-political realities [10, pp. 391–395].

However, today we can already identify a number of key areas for increasing media literacy among the population. These areas are focused on developing a critical attitude towards dubious information content.

It is necessary to develop a negative attitude towards such types of information as anonymous data (any information coming from unknown or anonymous sources), unsubstantiated assessments (information messages that contain value judgments, but do not provide justification for the conclusions made), dubious conclusions (messages that comment on rumors or unverified information and form certain conclusions on their basis), undisclosed sources (distribution of information from unnamed sources, or if the author of the message refuses to identify the origin of the data), unconfirmed links (familiarization with content whose sources cannot be confirmed through appropriate links).

Citizens should be particularly wary of the sudden emergence of new resources that disseminate insider information, sources that provide information in a one-sided and unbalanced manner, data from experts whose knowledge, skills and abilities cannot be reliably established, or whose forecasts are mostly wrong. It is also important to convince society that the source of high-quality analytics should primarily be recognized scientists and qualified specialists [11, p. 58].

**Conclusions.** Comprehensive information security includes: security in the infrastructure sector and citizens; ensuring informatization and professionalism of regional administration; accumulation and storage of information resources; international integration and exchange of experience. To implement these tasks, it is necessary to develop the main directions of information policy implementation, which include: 1) improving the legislative and regulatory framework in the information sector; 2) conducting large-scale information campaigns aimed at raising citizens; awareness of the processes of European integration. During martial law in Ukraine, it is important to: develop and improve legislation regulating information security in the state; strengthen the interaction of law enforcement agencies with the population regarding warnings about provocations in the information space; form an information culture among citizens.

**REFERENCES:**


1. Pro informatsiiu. Zakon Ukrainy. [About information. Law of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy (VVR),* 1992, № 48, st. 650. Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text [in Ukrainian].
2. Bondar H.L., Rakutina L.O. (2019). Informatsiina polityka ta informatsiina bezpeka. [Information policy and information security]. *Publichne upravlinnia ta mytne administruvannia*, № 4 (23). 42–49. [in Ukrainian].
3. Savosko T. (2024). Osoblyvosti formuvannia derzhavnoi informatsiinoi polityky. [Peculiarities of forming state information policy]. *Aspekty publichnoho upravlinnia*, Tom 12(1). 22–28. [in Ukrainian].
4. Leshyk S.V. (2024). Instytutsiino-pravovyi mekhanizm informatsiinoi polityky Ukrainy v protsesi yevrointehratsii. [Institutional and legal mechanism of Ukraine's information policy in the process of European integration]. *Politychne zhyttia*. № 3. 53–60. [in Ukrainian].
5. Pro «Stratehiiu informatsiinoi bezpeky». [About the «Information Security Strategy»]. *Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy* vid 15 zhovtnia 2021 roku. Retrieved from https://zakon.rada.gov.ua/laws/show/685/2021#Text [in Ukrainian].
6. Smotrych D.V., Brailko L. (2023). Informatsiina bezpeka v umovakh voiennoho stanu. [Information security under martial law]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu*, Vypusk 77(2). 121–127. [in Ukrainian].
7. Lomaka I.I., Lypchuk O.I., Kobets Yu.V. (2022). Informatsiina bezpeka derzhavy: teoretyko-metodolohichni zasady ta osoblyvosti v umovakh zbroinoho konfliktu. [Information security of the state: theoretical and methodological principles and features in conditions of armed conflict]. *Rehionalni studii*, № 31. 113–118. [in Ukrainian].
8. Shevchuk M.O. (2024). Orhanizatsiino-pravovi zasady zakhystu informatsii. [Organizational and legal principles of information protection]. *Aktualni problemy vitchyznianoi yurysprudentsii*, № 4. 82–87. [in Ukrainian].
9. Kovaliv M.V., Yesimov S.S., Yarema O.H. (2022). Informatsiine pravo Ukrainy [Information law of Ukraine]: navchalnyi posibnyk. Lviv: Lvivskyi derzhavnyi universytet vnutrishnikh sprav, 416. [in Ukrainian].
10. Tereshchenko V.V. (2023). Osoblyvosti derzhavnoi informatsiinoi polityky v umovakh viiny. [Peculiarities of state information policy in wartime]. *Yurydychnyi naukovyi elektronnyi zhurnal*, 2023. № 2. 391–395. [in Ukrainian].
11. Nikolaiets Yu. (2024). Derzhavna informatsiina polityka Ukrainy v umovakh povnomasshtabnoho voiennoho vtorhnennia Rosiiskoi Federatsii: suspilno-mobilizatsiinyi potentsial i efektyvnist. [State information policy of Ukraine in the conditions of a full-scale military invasion of the Russian Federation: social mobilization potential and effectiveness]. *Political Studies*, № 1 (7). 42–67. [in Ukrainian].