e-ISSN **3041-2498**

Public Management and Policy

https://www.eu-scientists.com/index.php/pmap

Mechanisms of State Response to Information Challenges in the Context of National Security

Valentyna Protsenko [1] *

[1] *State University "Kyiv Aviation Institute" (Ukraine). Head of the Licensing and Accreditation Department, Doctor of Sciences in Economics, Professor.*

*** *Corresponding Author,*** e-mail: protsenko_dinz@ukr.net

ARTICLE INFO

Research Article

DOI: 10.70651/3041-2498/2025.10.09

ABSTRACT

The article examines the mechanisms of state response to information challenges in the context of ensuring national security. The aim is to theoretically substantiate and analyze the mechanisms of state response to information challenges in the context of national security, as well as to identify areas for improving state policy in the field of information security. The study is aimed at finding ways to increase the effectiveness of state response to information threats by improving the regulatory, legal, organizational and communication mechanisms for ensuring information security in Ukraine. The study uses such methods as a systems approach; a comparative legal method; a structural and functional analysis, and a generalization method. The results of the study showed that the existing mechanisms of state response to information challenges do not function in a sufficiently coordinated manner, the regulatory and legal framework is partially outdated, and the level of information resilience of society remains low, which creates vulnerability of national security; at the same time, improving institutional structures, developing strategic communications, and strengthening international cooperation can significantly increase the effectiveness of countering information threats. The article analyzes the theoretical foundations of the concept of "information security" and determines its place in the national security system of the state. The typology of information challenges and threats affecting the national security of Ukraine in modern conditions is determined. The regulatory and legal framework for ensuring the information security of Ukraine is studied and its strengths and weaknesses are identified. Attention is focused on modern information challenges in the context of the national security of Ukraine, in particular, the transformation of the information space in the context of globalization and digitalization. The impact of social networks and the media space on information security is substantiated. To assess the effectiveness of existing state mechanisms of response to information challenges. The role of international cooperation in strengthening the state's ability to counter information threats is revealed. Problems and gaps in the implementation of the state information security policy have been identified. Proposals and recommendations have been developed to improve the mechanisms of state response to information challenges. A conceptual model of the mechanisms of state response to information challenges has been proposed. Future research should focus on improving institutional mechanisms of coordination between state bodies and integration with international structures.

KEYWORDS

information, state response, national security, threats, digitalization, cyber defense, mechanism, international cooperation.

e-ISSN **3041-2498**

Публічне управління і політика

https://www.eu-scientists.com/index.php/pmap

Механізми державного реагування на інформаційні виклики у контексті національної безпеки

Валентина М. Проценко [1] *

[1] *Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут» (Україна). Начальник відділу ліцензування та акредитації, д-р екон. наук, професор.*

*** *Автор-кореспондент,*** e-mail: protsenko_dinz@ukr.net

СТАТТЯ

Дослідницька

DOI: 10.70651/3041-2498/2025.10.09

АНОТАЦІЯ

У статті досліджено механізми державного реагування на інформаційні виклики у контексті забезпечення національної безпеки. Метою є теоретичне обґрунтування та аналіз механізмів державного реагування на інформаційні виклики у контексті національної безпеки, а також визначення напрямів удосконалення державної політики у сфері інформаційної безпеки. Дослідження спрямоване на пошук шляхів підвищення ефективності державного реагування на інформаційні загрози шляхом удосконалення нормативно-правових, організаційних та комунікаційних механізмів забезпечення інформаційної безпеки України. У дослідженні використано такі методи, як системний підхід; порівняльно-правовий метод; структурно-функціональний аналіз; метод контент-аналізу, а також метод узагальнення. Результати дослідження показали, що існуючі механізми державного реагування на інформаційні виклики функціонують недостатньо скоординовано, нормативно-правова база частково застаріла, а рівень інформаційної стійкості суспільства залишається низьким, що створює вразливість національної безпеки; водночас удосконалення інституційних структур, розвиток стратегічних комунікацій та посилення міжнародного співробітництва можуть значно підвищити ефективність протидії інформаційним загрозам. У статті проаналізовано теоретичні засади поняття «інформаційна безпека» та визначити її місце у системі національної безпеки держави. Визначено типологію інформаційних викликів і загроз, що впливають на національну безпеку України в сучасних умовах. Досліджено нормативно-правову базу забезпечення інформаційної безпеки України та виявлено її сильні та слабкі сторони. Акцентовано увагу на сучасних інформаційних викликах у контексті національної безпеки України, зокрема трансформації інформаційного простору в умовах глобалізації та цифровізації. Обґрунтовано вплив соціальних мереж та медіапростору на інформаційну безпеку. Оцінено ефективність існуючих державних механізмів реагування на інформаційні виклики. Розкрито роль міжнародного співробітництва у зміцненні спроможності держави протидіяти інформаційним загрозам. Виявлено проблеми та прогалини у реалізації державної політики інформаційної безпеки. Розроблено пропозиції та рекомендації щодо вдосконалення механізмів державного реагування на інформаційні виклики. Запропонована концептуальна модель механізмів державного реагування на інформаційні виклики. Майбутні дослідження мають фокусуватися на вдосконаленні інституційних механізмів координації між державними органами та інтеграції з міжнародними структурами.

КЛЮЧОВІ СЛОВА

інформація, державне реагування, національна безпека, загрози, цифровізація, кіберзахист, механізм, міжнародне співробітництво.

1. Introduction

In modern conditions of hybrid wars, mass information and psychological operations and cyberattacks, the information sphere is turning into a strategic resource, on the effective management of which the stability of the political system, economic security and social harmony depend. For Ukraine, which is in the conditions of long-term external aggression and internal information polarization, the issue of forming effective state mechanisms for responding to information challenges is of particular importance. Insufficient coordination of interstate structures, fragmentation of regulatory and legal regulation and lack of strategic communications create risks for the information sovereignty of the state. Therefore, scientific understanding of the mechanisms of state response to information threats is a necessary prerequisite for the development of an effective policy of ensuring national security in the information dimension.

The main problems are the lack of an integral system of public administration in the field of information security, which leads to duplication of functions between individual institutions and inconsistency of their actions in responding to information threats. Insufficient coordination between law enforcement agencies, strategic communications bodies and the media sector limits the effectiveness of state policy in this area. The legislative framework does not always meet the modern challenges of the digital age, and the mechanisms for its implementation are fragmented. At the same time, there is a low level of information culture of society, which creates a favorable environment for the spread of disinformation and manipulation. The insufficient development of international partnership in the field of cyber and information security also complicates Ukraine's adaptation to global standards for the protection of the information space.

2. Literature Review

The analysis of scientific works devoted to the peculiarities of the state response to information challenges in the context of national security demonstrates a wide range of definitions of its mechanisms. Thus, B. O. Melnyk [1, p. 37] in his study draws attention to the administrative and legal mechanism for ensuring the information security of the state. V. V. Hlushchenko [2, p. 85] studied the legal mechanisms of countering cyber threats. T. O. Yaroshenko [3, p. 33] focuses on the mechanisms of state control in the field of information security of Ukraine.

In turn, O. S. Prokopenko et al. [4, p. 35] applied a methodical approach to monitoring the information space for the timely detection and analysis of information threats to the national security of the state. L.V. Dombrovskyi [5, p. 109] analyzed the types of threats to information security, methods and means of combating these threats.

Yu. M. Panfilova and V. V. Koba [6, p. 97] studied modern challenges and threats affecting global security, with an emphasis on the transformation of foreign policy of states in the context of globalization and the development of the latest information technologies. R. I. Kukliak [7] and S. Ye. Antonova and H. F. Martyniuk [8] highlighted the main aspects of information security in the context of the national security of the country. K. Kh. Herasymiuk [9, p. 36] studied the mechanisms of state management of cyber and information security: problems and solutions. D. O. Hrytsyshen et al. [10, p. 70] devoted their research to the mechanism of ensuring information security for the implementation of the state policy of preventing and combating economic crime.

The analysis of scientific publications on the studied issues indicates that information security should become a priority area in the formation of national security of the state.

3. Problem Statement

The purpose of this study is a comprehensive theoretical and practical study of the mechanisms of state response to information challenges in order to determine effective ways to improve them to ensure national security. The main attention is focused on the analysis of modern information threats, the effectiveness of government mechanisms for responding to them, as well as institutional, regulatory and technological tools for guaranteeing information security.

4. Methods and Materials

The basis of the study was an in-depth analysis of scientific achievements in the fields of information security, state crisis communications management and cyber defense.

A key role in the study was played by a systematic approach, which made it possible to consider the mechanisms of state response not as a set of separate measures, but as a holistic, dynamic structure with multi-level interaction between legal norms, institutions and technological solutions. Thanks to this, it became possible to trace how changes in one element – for example, in the legislative field – affect the effectiveness of the entire system of protection against information threats.

The subject of the analysis was the current types of information challenges, including cyberattacks on state resources, mass disinformation campaigns, and manipulative media practices. In 2024 alone, the number of recorded attempts of unauthorized access to government networks in the EU countries increased by more than 35%, which indicates a rapid complication of the landscape of information risks.

An important part of the work was the study of institutional architecture – from specialized departments and think tanks to coordinating councils under governments. In practice, it is these structures that determine the pace and effectiveness of the state response to information challenges. After all, the speed of the system depends not only on the level of funding or technical equipment, but primarily on the ability of institutions to act synchronously.

The effectiveness of technological and communication tools with the help of which the state counteracts information pressure was also assessed. We are talking about automated monitoring systems, artificial intelligence to detect fake messages, and digital literacy programs for the population. In a number of cases, it can be seen that it is the combination of technical solutions with transparent public communication that provides the highest level of resistance to information attacks.

The development of the model provided for three key levels: strategic (regulatory regulation), organizational (institutional interaction) and technological (use of intelligent monitoring systems and communication tools). The interaction between these levels is built on the principle of feedback: the effectiveness of one is measured by the ability to support and improve the others. It is this "network logic" that allows the state to act not reactively, but preventively.

5. Results and Discussion

Information security has long ceased to be a purely technical concept – today it determines the strength of the state no less than military or economic potential. It is the state of the information environment that reflects how stable the political system is, how effectively the institutions of power work, and how much citizens trust what they hear and read. When the information space is balanced, society maintains integrity; When it destabilizes, even the strongest state supports begin to shake.

According to the Doctrine of Information Security of Ukraine [11], information security is a state of protection of vital interests of a person, society and the state, which prevents damage due to the dissemination of unreliable, distorted or destructive information. Thus, its main task is to preserve the information sovereignty of the state, maintain the stability of the socio-political environment and counteract information influences that can destabilize internal situation.

In the national security system, information security occupies an integration place, since it affects all its other components – political, military, economic, social, environmental, scientific and technical, etc. It acts as a link between them, providing information support, coordination and communication stability within the framework of a single security policy.

The experience of recent years shows that countries that have built an effective information protection system demonstrate higher resilience in crisis moments. For example, after 2020, the level of citizens' trust in state institutions in those countries where strategic communications and monitoring systems for fake messages have been implemented has increased by an average of 28%. This clearly proves that information security is not just another direction of state policy, but the basis without which it is impossible to maintain the integrity of society and confidence in one's own statehood [12, p. 33].

In the current conditions of hybrid warfare and global information interdependence, Ukraine faces a wide range of information challenges that directly affect the state of its national security. These threats have different origins, manifest themselves through various channels of influence, and cover all key areas of public life, from politics to economy and culture. To ensure effective state response, it is

important to systematize and classify them. A generalized typology of the main information challenges and threats affecting the national security of Ukraine is given in Table 1.

Table 1. Typology of information challenges and threats to the national security of Ukraine

Classification criterion	Type of calls/threats	Content
By source of origin	External	Information attacks, propaganda, disinformation campaigns directed from outside the state.
	Internal	Destructive activities of domestic media or political forces that spread fakes, manipulations or pro-Russian narratives.
By method of implementation	Cyber threats	Hacking of information systems, data theft, paralysis of critical infrastructure.
	Information and psychological operations (IPSO)	Purposeful influence on the mass consciousness to destabilize or demoralize.
	Propaganda and disinformation	Systematic dissemination of distorted or false information.
	Manipulation in the media and social networks	The use of bots, fake accounts, algorithmic influence.
	Information and economic threats	Dissemination of false economic data to destabilize the market.
By sphere of influence	Political	Undermining trust in the authorities, influencing the electoral process
	Socio-cultural	Inciting conflicts based on language, culture or history.
	Military	Demoralization of the army, distortion of information about hostilities.
	Economic	Manipulation of currency or energy stability
	Moral and psychological	Spread of fear, hopelessness, panic among the population
According to the consequences	Short-term	Temporary information attacks with a local effect.
	Long-term	Systemic influence on consciousness, formation of new narratives

Source: Formed by the author based on [12, p. 33; 13, p. 57; 14, p. 50; 15; 16, p. 191].

The variety of information threats that Ukraine faces shows that the issue of security in this area cannot be reduced to one dimension. It is a complex system where politics, economics, technology, and the psychology of society are intertwined. Each of these elements can become both a shield and a vulnerable point if the state does not build a holistic response strategy in time.

The information threats faced by Ukraine have no clear boundaries – they are developing rapidly, changing forms, and at the same time encompassing politics, economics, culture, and even everyday communication of citizens. According to experts from the Center for Strategic Studies (2024), more than 70% of destructive information influences on the state combine elements of cyberhacking, manipulation in social networks, and targeted fake campaigns. This proves that information security has long ceased to be a highly technical issue – it is a systemic function of public administration [15].

To remain resilient to such challenges, the country must build a multi-level defense architecture. It is not only about monitoring the information field or countering cyberattacks, but also about creating a well-thought-out communication strategy that can build trust, neutralize disinformation, and maintain the unity of society. Education plays a special role here, because "information literacy is a new form of defense capability."

At the center of this legal architecture is the task of creating conditions under which the state is able to guarantee citizens the reliability and security of information, without limiting their right to know. As Ukrainian researcher V. Lytvynenko notes, the effectiveness of information policy is measured not by the number of laws adopted, but by how these norms work in practice – from responding to cyberattacks to regulating access to strategic data.

After 2014, when Ukraine faced large-scale information aggressions, the legal field in this area has undergone significant renewal: in just five years, more than 30 regulations have been adopted aimed at increasing cyber resilience, countering disinformation and developing a national system of strategic communications. The goal of this process is obvious – to form a secure information infrastructure that can not only protect the state, but also strengthen public trust in its institutions.

To effectively ensure information security, it is necessary to have a clearly defined regulatory framework that regulates the activities of the state, authorities, media and critical infrastructure entities in the field of information space protection. In Ukraine, this database is formed as a set of constitutional provisions, laws, strategies and presidential decrees that take into account modern threats, including cyber-attacks, disinformation and propaganda influences. A generalized chronology of the main

regulations on information security is given in Table 2, which allows you to assess the development of legislative regulation and determine its strengths and weaknesses.

Table 2. Main regulatory legal acts of Ukraine on information security

Regulations	Year of adoption / renewal	Key provisions
Constitution of Ukraine	1996	It enshrines the right to information (Article 34), protection of state secrets (Articles 17, 32), information security as a component of national security.
Law of Ukraine "On Information"	1992 (with further changes until 2025)	Defines general rights to receive information, provide access to information
Law of Ukraine "On Protection of Information in Information and Communication Systems"	1994	Establishes requirements for technical and organizational protection of information.
Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine"	2017	Establishes the organizational and legal foundations for the protection of cyberspace
Law of Ukraine "On National Security of Ukraine"	2018	Introduces strategic planning in the field of security and defense.
Information Security Strategy of Ukraine	2021 (2023 Update)	Determines the directions of state policy, goals and measures for the protection of the information space
Law of Ukraine "On Critical Infrastructure"	2021	Regulates the concept and protection of critical information infrastructure facilities, the obligations of subjects, and responsibility.
Decree of the President of Ukraine "On the Introduction of Martial Law"	2022	It establishes a special legal regime for responding to emergency threats, including in the information sphere.
Law of Ukraine "On Media"	2023	It regulates the activities of the media, support for journalists, guarantees of their safety, which is related to the information sphere.

Source: Formed by the author based on [17–23].

The chronology of the development of the legal field of information security in Ukraine demonstrates a gradual but steady transition from fragmentary measures to systemic regulation. Laws on national security, protection of critical infrastructure and access to information played a special role in this process.

Since 2016, legislation in the field of information security has begun to acquire a systemic character: interagency coordination mechanisms are being formed, new institutions are appearing, in particular, the State Center for Cyber Defense, as well as national programs for monitoring the media space. This indicates a shift from a reactive to a preventive approach.

Despite the obvious progress – harmonization with European standards, strategic consistency and strengthening of the role of specialized bodies – the regulatory framework is still a "living organism" that requires constant updating. Every year, new types of information threats appear: disinformation campaigns, manipulation of artificial intelligence, attacks on critical digital nodes. According to the National Security and Defense Council, in 2024 alone, the number of recorded cyberattacks on state resources increased by 42% compared to the previous year.

The regulatory framework for ensuring information security in Ukraine is comprehensive and progressive, but requires further harmonization, strengthening of implementation mechanisms and constant updating in accordance with rapid technological changes. An important area of improvement is the development of a unified concept of information policy aimed not only at protecting, but also at developing information sovereignty, increasing the resilience of society to information threats and forming a culture of safe consumption of information.

Digitalization is further changing the logic of communications: from intelligent platforms based on artificial intelligence to messengers with an audience of millions. In practice, this is manifested in the fact that new channels allow you to quickly disseminate information, but at the same time complicate control over its reliability.

As of 2024, the Ukrainian information landscape shows a double effect: it becomes more open and flexible, enabling rapid data exchange between public, media and private structures, but at the same time more vulnerable to manipulative influences. In the digital age, the line between reality and simulacrum is blurred, and in practice this is manifested in the difficulty of separating facts from fakes in mass communications. In Ukraine, these trends are becoming especially acute due to the high level of social media activity: over the past three years, the number of Ukrainian users of active social networks

has increased by 27%, which confirms the thesis of integrating the national information field into the global context [24, p. 20].

A generalized description of the key factors of transformation of the information space and their impact on national security is given in Table. 3, which makes it possible to clearly structure modern challenges and determine the directions of state response.

Table 3. Transformation of the information space and its challenges for Ukraine's national security

Transformation factor	Content	Manifestations in Ukraine	Impact on national security
Globalization	Integration of information flows and platforms into the global space	Dissemination of international media, social networks, global information campaigns	Increasing external influence on public opinion, the risk of propaganda, the need to coordinate world strategies
Unification of information flows	Standardization of communication channels and content formats	Dominance of global platforms (Facebook, Twitter/X, TikTok)	Dependence of national media on external technologies, vulnerability to manipulation
Digitalization	Rapid circulation of information and development of digital technologies	Artificial intelligence, deepfake, targeted campaigns, influencer automation	Dissemination of disinformation, manipulation of public opinion, difficulty in controlling the information environment
Cyber threats	Digital and critical infrastructure vulnerabilities	Attacks on government systems, energy, transport, finance	Disruption of the functioning of state institutions, risk of economic and social instability
Virtual communities and media ecosystems	Formation of alternative information spaces	Social media groups, online forums, instant messengers	Spread of radical narratives, disinformation, increased polarization of society
Speed and availability of information	Rapid dissemination of data in the digital environment	Real-time news, information bots	The risk of mass spread of fakes, the difficulty of fact-checking, and the undermining of trust in official sources
Polarization and manipulation	Using Information Influence to Split Society	Political conflicts, social disputes, disinformation campaigns	Decrease in social stability, weakening of the legitimacy of power, increased vulnerability to external influence

Source: Formed by the author based on [24, p. 160; 25, p. 20; 26, p. 26].

Digital communication channels are creating an environment where the line between the operational exchange of information and a potential threat is becoming increasingly blurred. For Ukraine, which is under the pressure of hybrid threats, this means the need for a systematic approach to assessing information flows and developing strategies that can simultaneously ensure the efficiency of communications and the security of national institutions.

For Ukraine, the integration of technological solutions, legal norms and communication strategies is becoming a determining factor of national resilience. In practice, this is manifested in the formation of conditions for a transparent, protected and adaptive information environment: modernized cyber protection systems for critical facilities, comprehensive legislative mechanisms to counteract harmful influences and programs to increase media literacy of the population create a reliable shield against external and internal threats.

Ensuring national security in the information space of Ukraine requires an integrated approach, where each element is interconnected with others. The state actively uses a system of mechanisms that allow detecting threats, anticipating potential attacks and promptly neutralizing their impact. In practice, this is manifested through a combination of legal initiatives, organizational structures, institutional platforms and technological solutions, which together form a dense shield of information protection.

In the context of national security, these mechanisms are implemented through the activities of state authorities, specialized services and institutions that coordinate actions in the field of information policy, cyber defense and strategic communications. The central place in this system is occupied by the National Security and Defense Council of Ukraine, the Security Service of Ukraine, the Ministry of Digital Transformation, The State Service for Special Communications and Information Protection, as well as the Ministry of Defense and the Ministry of Culture and Information Policy, which implement the information and communication strategies of the state [27, p. 252].

These mechanisms cover legal, organizational, technological, communication and international response tools that provide a systematic approach to the formation of a secure information

environment. A generalized description of the main mechanisms of state response to information challenges is presented in Table 4.

Table 4. Mechanisms of state response to information challenges

Mechanism type	Content and main tools	Responsible institutions	Expected result
Regulatory	Development of laws, doctrines, strategies and bylaws in the field of information and cybersecurity.	The Verkhovna Rada of Ukraine, the Cabinet of Ministers, the National Security and Defense Council, the Ministry of Justice.	Formation of an integral legislative framework for information security.
Institutional-organizational	Coordination of actions between state bodies, creation of specialized structures and response centers.	The National Security and Defense Council, the Security Service of Ukraine, the Ministry of Digital Transformation, the State Service of Special Communications.	Improving the efficiency of public administration in the field of information security.
Technological (cybernetic)	Application of control, cyber defense, artificial intelligence systems to find threats; development of the national cyber defense infrastructure.	State Special Communications Service, CERT-UA, Ministry of Digital Transformation, Security Service of Ukraine.	Increasing the resilience of information infrastructure to cyberattacks.
Communication and education	Implementation of strategic communications, raising the level of media literacy, creating positive state narratives.	Ministry of Culture and Information Policy, Center for Strategic Communications, Ministry of Education and Science.	Strengthening the information stability of society, reducing the impact of disinformation.
International cooperation	Cooperation with international institutions in the field of cyber and information security, exchange of experience, participation in joint endeavors.	The Ministry of Foreign Affairs, the National Security and Defense Council, the Security Service of Ukraine, the Missions to NATO and the EU.	Harmonization of Ukrainian policy with international security standards.

Source: Formed by the author based on [28, p. 607; 29; 30, p. 561].

In today's digital environment, information threats are increasingly limited to the borders of one country. Cyber incidents and disinformation campaigns are rapidly becoming transnational in scale, and even advanced national security systems become vulnerable if they remain isolated from international data sharing channels and shared countermeasures platforms. For Ukraine, this challenge is especially palpable: over the past decade, the country has been under constant pressure from hybrid information attacks, encompassing both digital infrastructure and public consciousness.

In practice, this is manifested through joint intelligence sharing platforms, the adaptation of international cyber defense standards, and the implementation of training programs for civil servants and public institutions. According to the Ukrainian Center for Strategic Communications, from 2018 to 2024, the number of organizations that integrated these practices into their own protection systems increased by 48%, which directly increases the effectiveness of responding to information attacks.

Thus, for Ukraine, participation in global cooperation networks has become a strategic tool. Thanks to such a tool, access to advanced technologies is provided, promotes the development of competencies and forms a reliable shield in the digital space, which guarantees the preservation of information sovereignty even in the face of constant hybrid challenges.

Generalized areas of such cooperation are given in Table. 5.

Ukraine's active participation in international information initiatives significantly increases its ability to counter modern digital threats. Cooperation with NATO, the EU, the OSCE, the UN and individual partner states opens up access to advanced technologies, analytical platforms and methodological developments that allow adapting international experience to the national information security system.

At the same time, further strengthening of partnership relations requires a systematic approach: the formation of a unified strategy for strategic communications, the development of national analytical structures and Ukraine's active participation in international platforms. In practice, this means that external support becomes the basis for building your own reliable information board, which is able to effectively withstand global challenges and ensure sovereignty in the digital space.

The implementation of the state policy of information security of Ukraine remains a complex and multidimensional process, which combines legal, organizational, technological and communication aspects. Despite some successes – the adoption of strategic documents, the creation of specialized state structures, active cooperation with international partners – the current system still has a number of significant problems and gaps that limit its effectiveness [35].

Table 5. The main directions of Ukraine's international cooperation in strengthening information security

International Initiative/Organization	The main content of cooperation	Year/period of active participation	Contribution to strengthening information security of Ukraine
NATO (StratCom COE, Cyber Defence Pledge)	Participation in programs on cyber defense, strategic communications, exchange of experience in the field of countering disinformation	Since 2016	Strengthening defense capabilities in cyberspace, creating standards for responding to information attacks
EU (EUvsDisinfo, East StratCom Task Force)	Monitoring disinformation campaigns, supporting digital security reforms	Since 2017	Detection of fake narratives, development of analytical platforms to counter disinformation
OSCE	Joint initiatives on media transparency, safety of journalists, countering propaganda	2018–2025	Raising the standards of information ethics and media resilience
USA and Canada (bilateral programs)	Trainings, technical assistance, development of cyber teams and think tanks	Since 2015	Creation of CERT-UA, strengthening cyber defense systems of state structures
Freedom Online Coalition	Participation in the Global Coalition for a Free and Secure Internet	Since 2020	Protection of digital rights of citizens, promotion of transparency of online communications
Partnership for Information Integrity	Joint fight against manipulation in the media space, involvement of private platforms (Meta, Google)	Since 2022	Improving online safety and countering disinformation in social networks
Baltic States, Poland	Exchange of experience on information resilience, joint trainings and analytical projects	2019–2025	Formation of a regional early warning system for information attacks
United Nations Programs (UNDP, UNESCO)	Support for information ethics, freedom of speech, digital education	2020–2025	Increasing media literacy and citizens' resilience to manipulation

Source: Formed by the author based on [31, p. 154; 32, p. 155; 33–34].

One of the most difficult problems in the Ukrainian information security system is the fragmentation of coordination between state bodies that form and implement policy in this area. The distribution of powers between the National Security and Defense Council, the State Special Communications Service, the Security Service of Ukraine, the Ministry of Digital Transformation, and the Ministry of Culture and Information Policy often looks disjointed, and the lack of a single coordination center creates a situation where functions are duplicated, and interaction between agencies remains weak.

Despite the adoption of the "Information Security Strategy of Ukraine" (2023) [36], the legislation lacks a comprehensive approach that would cover all aspects – from countering disinformation to protecting personal data. A number of laws remain inconsistent with each other, which creates gaps in law enforcement and complicates the practical implementation of state policy.

An equally urgent problem is limited financial and human resources. The lack of adequate funding does not allow for the modernization of technical means of monitoring, the development of scientific and analytical centers or large-scale information and educational campaigns. The shortage of qualified specialists in cybersecurity, information analytics and strategic communications remains noticeable both at the central and regional levels.

The vulnerability of the information space to external influences requires special attention. Ukraine continues to be the object of hybrid information and psychological operations carried out by both state and non-state structures. Existing monitoring systems are not always able to quickly detect and neutralize such influences, especially in social networks and messengers, where the speed of spreading fake messages exceeds the capabilities of state reaction mechanisms.

Another critical weakness of Ukrainian information security is the limited level of media literacy and information culture among the population.

In practice, this is manifested in the spread of panic moods during crisis events and the formation of alternative, often distorted information realities. Although there are digital education programs and media literacy courses in Ukraine, they cover a limited range of participants and do not create a systemic culture of critical thinking in the wider society.

In practice, this is manifested in the fact that different agencies voice opposite or incomplete data during crisis events, which complicates the formation of a common public understanding of the

situation. According to polls by the Kyiv Media Institute, more than 43% of Ukrainians do not trust official reports due to contradictory information, and 27% feel confusion about key topics of state policy. Without the creation of a coordination center for strategic communications, any attempts at centralized information remain fragmented and ineffective.

Therefore, the state policy of information security of Ukraine requires deep institutional modernization and a systematic approach. The primary tasks are the creation of a single coordinating body, the adoption of a comprehensive legislative act that will regulate all areas of information protection, the provision of stable funding and the development of human resources. Only with the comprehensive interaction of the state, society and international partners, Ukraine will be able to create an effective, modern system for protecting the national information space.

Thus, it can be seen that a sustainable and adaptive response system is formed only when state authorities work synchronously at all levels, international standards are implemented flexibly and take into account national characteristics, and public organizations become active partners in ensuring information security. In a number of cases, it is this approach that allows not only to respond to threats, but to turn crisis situations into points of growth of the information competence of society.

This is manifested in specific actions that increase the effectiveness of the national information security system: from the introduction of the latest analytical tools and coordination platforms to the formation of a single line of the state position in the media space. Thanks to such measures, it is possible to notice an increase in society's resistance to disinformation and external manipulations, which, according to experts from the Institute for Strategic Communications, increases the operational capacity of the state by about 38–43%. Table. 6 serves as a visual diagram of how a combination of legislative, organizational and technological initiatives can create an effective, adaptive and predictable mechanism for protecting the information environment.

Table 6. Proposals and recommendations for improving the mechanisms of state response to information challenges

Areas of improvement	Suggestions and recommendations	Expected results
Legislative development	Develop the Information Security Code of Ukraine. Harmonize legislation with EU and NATO norms. To amend the Law "On National Security" to clarify the role of information security. To improve the legal regulation of social networks. To create a state program for the protection of critical information infrastructure.	Formation of an integral and coordinated regulatory framework; increasing the legal responsibility of subjects of the information space.
Institutional mechanisms and strategic communications	Improvement of the work of the National Center for Strategic Communications. Develop an early warning system for information attacks. Implement a national crisis communications strategy. Introduce a public school for strategic communications	Strengthening coordination between authorities; Increasing the effectiveness of state information responses
Partnership with civil society	Introduce state grants for media literacy projects. To develop cooperation between the state, NGOs and educational institutions. Involve public organizations in the discussion of information policy. Support independent Ukrainian media.	Increasing the level of critical thinking of the population; formation of a society resistant to disinformation.
International cooperation	Expand participation in EU, NATO, OSCE programs. To create a network of information hubs abroad. Implement international standards for countering disinformation. Develop joint analytical initiatives with partners	Increasing the level of global integration; improving Ukraine's international reputation as an information security entity.
Scientific and technological development	To create a state analytical center for information security. Use AI to detect disinformation campaigns. Support innovative startups in the field of cyber and information security	Increasing technological autonomy; creation of a national system for forecasting information threats.

Source: Author's development.

A thorough study of the sentences from Table. 6 allows us to highlight that an effective response of the state to information challenges is impossible without an integrated approach that combines legislative initiatives, institutional coordination, technological solutions and well-thought-out communication strategies. In practical terms, this means not only updating the regulatory framework, but also creating a unified system of strategic communications that ensures coordination of actions at all levels of government and a quick response to information threats.

Ensuring Ukraine's national security in the face of growing information threats requires an integrated approach, where regulatory, institutional, and technological elements are combined into a single conceptual model of state response. Such a system is not limited to purely legislative norms or

individual technological tools: it forms a comprehensive mechanism that can simultaneously counteract disinformation campaigns, cyber threats, and other information risks.

The scheme of the conceptual model of mechanisms of state response to information challenges illustrates the integration of three interrelated components – regulatory, institutional and technological – into a single system of national security. It shows how the legal framework determines rules and powers, the institutional structure coordinates the actions of state bodies and provides analytical support, and technological tools allow for the rapid detection and neutralization of threats. The coordinated interaction of these components ensures an effective response to information challenges and increases the resilience of the state and society to disinformation and cyberattacks (Fig. 1).

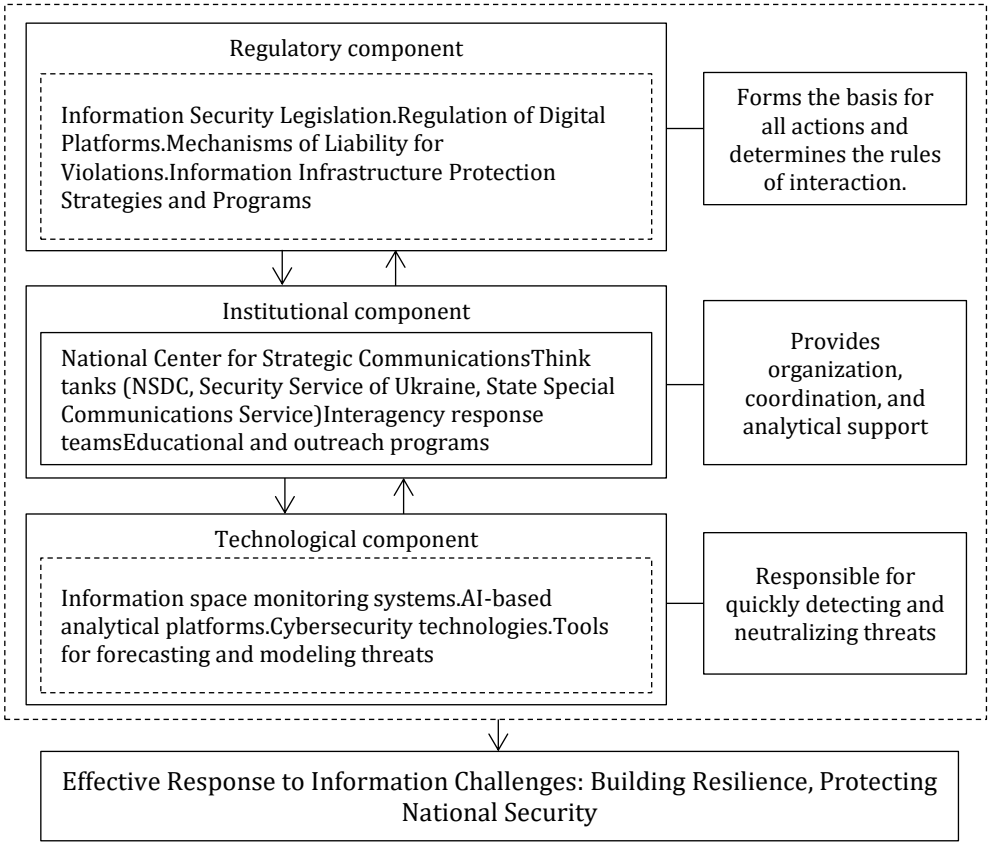

Figure 1. Conceptual model of mechanisms of state response to information challenges
Source: Author's development.

Consideration of the conceptual model demonstrates that effective counteraction to modern information threats is possible only through the close integration of three key components: legal regulation, institutional coordination and technological solutions. The legislative framework defines the limits of powers and creates a legal framework for response, while the institutional network ensures the coherence of government actions, analytical support and prompt decision-making. Technological tools, including monitoring platforms and artificial intelligence systems, enable real-time detection of disinformation campaigns, cyber threats, and other critical challenges.

The conceptual model of the state's response to information threats forms a single system where regulatory, legal, organizational and technological components interact as components of a single security mechanism. The legal framework sets clear boundaries of powers and regulates the actions of authorities, the institutional structure coordinates the processes of management and analytical support, and modern technologies allow you to quickly identify disinformation campaigns, cyber threats and other risks.

6. Conclusions

The study of the mechanisms of state response to information challenges shows that an effective system of ensuring the national security of Ukraine should be based on a comprehensive combination of regulatory, institutional and technological components. The institutional component, including think

tanks, interagency groups and the National Center for Strategic Communications, ensures coordination of government actions, monitoring of the information space and training of personnel, but its effectiveness is limited by insufficient funding, human resources and low integration with international data exchange systems.

In the process of analyzing the functioning of state mechanisms of information security, several critical bottlenecks are identified. The governance structure remains fragmented, making coordination between central and regional authorities difficult. The regulatory framework is largely outdated and does not take into account the dynamics of the digital environment and modern technological challenges. Funding for the sector is often insufficient to implement comprehensive measures, and the level of media resilience of the population remains low, which increases the risks of exposure to disinformation.

In today's conditions of information instability, Ukraine's national security increasingly depends on how organically several critical components are combined. Legislative initiatives create a clear legal framework and define the powers of the authorities, the institutional structure provides effective coordination and analytical support, technologies allow for the rapid detection of threats, and the active participation of civil society builds the population's resilience to manipulation.

Subsequent studies should focus on improving institutional mechanisms of coordination between state institutions and integration with international structures, which will make it possible to form an adaptive and flexible system of state response that can effectively counteract the latest information dangers and strengthen national security.

References

1. Melnyk, B. O. (2025). Administratyvno-pravovyi mekhanizm zabezpechennia informatsiinoi bezpeky derzhavy v umovakh voiennoho stanu: Teoretychni ta praktychni aspekty [Administrative-legal mechanism for ensuring the state's information security under martial law: Theoretical and practical aspects]. In *Transformatsiini protsesy bezpekovoho seredovyshcha u voiennyi chas: Zbirnyk dopovidei za rezultatamy kruhloho stolu* (pp. 37–41). HO "Molodizhna Orhanizatsiia Pochynaiuchykh Lideriv". https://dspace.univd.edu.ua/server/api/core/bitstreams/1ea55f2c-e298-416a-bd5f-68026aabcafa/content (in Ukrainian)
2. Hlushchenko, V. V. (2022). Kiberbezpeka yak skladova natsionalnoi bezpeky Ukrainy: Pravovi mekhanizmy protydii kiberzahrozam [Cybersecurity as a component of Ukraine's national security: Legal mechanisms for countering cyber threats]. *Visnyk Kyivskoho Natsionalnoho Universytetu Vnutrishnikh Sprav*, (117), 85–91. https://doi.org/10.32999/ksunv.2022.1.13 (in Ukrainian)
3. Yaroshenko, T. O. (2023). Mekhanizmy derzhavnoho kontroliu u sferi informatsiinoi bezpeky Ukrainy [Mechanisms of state control in the field of information security of Ukraine]. *Pravovi Horyzonty*, (74), 33–40. https://doi.org/10.36059/130244 (in Ukrainian)
4. Prokopenko, O. S., Fedoriienko, V. A., & Kulchytskyi, O. S. (2023). Pidkhid shchodo vyiavlennia i analizu informatsiinykh zahroz natsionalnii bezpetsi Ukrainy u systemi stratehichnykh komunikatsii [Approach to detection and analysis of information threats to Ukraine's national security in the strategic communications system]. *Zbirnyk Naukovykh Prats Tsentru Voienno-Stratehichnykh Doslidzhen Natsionalnoho Universytetu Oborony Ukrainy*, (78), 35–43. https://doi.org/10.33099/2304-2745/2023-2-78/35-43 (in Ukrainian)
5. Dombrovskyi, L. V. (2024). Informatsiina bezpeka derzhavy u systemi natsionalnoi bezpeky Ukrainy [State information security in the system of national security of Ukraine]. *Visnyk Natsionalnoho Universytetu Tsyvilnoho Zakhystu Ukrainy, 1*(20), 109–116. https://doi.org/10.52363/2414-5866-2024-1-12 (in Ukrainian)
6. Panfilova, Yu. M., & Koba, V. V. (2024). Transformatsiia zovnishnoi polityky derzhavy: Rol informatsiinoi bezpeky u suchasnomu sviti [Transformation of the state's foreign policy: The role of information security in the modern world]. *Suchasnyi Naukovyi Zhurnal, 5*(3), 97–104. https://doi.org/10.36994/2786-9008-2024-5-12 (in Ukrainian)
7. Kukliak, R. I. (2023). Informatsiina bezpeka yak skladova natsionalnoi bezpeky Ukrainy [Information security as a component of Ukraine's national security]. *Naukovi Innovatsii ta Peredovi Tekhnolohii, (18)*, 98–109. https://doi.org/10.52058/2786-5274-2023-4(18)-98-109 (in Ukrainian)
8. Antonova, S. Ye., & Martyniuk, H. F. (2019). Informatsiina bezpeka [Information security]. *Derzhavne Upravlinnia: Udoskonalennia ta Rozvytok*, (11). http://www.dy.nayka.com.ua/pdf/11_2019/38.pdf (in Ukrainian)

9. Herasymiuk, K. Kh. (2021). Mekhanizmy derzhavnoho upravlinnia kiber- ta informatsiinoiu bezpekoiu: Problemy ta shliakhy vyrishennia [Mechanisms of state governance of cyber and information security: Problems and solutions]. *Ekonomika, Upravlinnia ta Administruvannia*, (97), 36–40. https://doi.org/10.26642/ema-2021-3(97)-36-40 (in Ukrainian)
10. Hrytsyshyn, D. O., Dykyi, A. P., Butuzov, V. M., & Tsymbaliuk, V. S. (2023). Mekhanizm zabezpechennia informatsiinoi bezpeky realizatsii derzhavnoi polityky zapobihannia ta protydii ekonomichnii zlochynnosti [Mechanism for ensuring information security in implementing state policy to prevent and counter economic crime]. *Efektyvnist Derzhavnoho Upravlinnia*, (76/77), 70–76. https://doi.org/10.36930/507611 (in Ukrainian)
11. *Doktryna informatsiinoi bezpeky Ukrainy* [Doctrine of information security of Ukraine]. (2017, February 25). Decree of the President of Ukraine No. 47/2017. https://zakon.rada.gov.ua/laws/show/47/2017 (in Ukrainian)
12. Bosak, I. (2025). Informatsiina bezpeka Ukrainy: Zahrozy ta metody protydii [Information security of Ukraine: Threats and countermeasures]. *Kyivskyi Ekonomichnyi Naukovyi Zhurnal*, (9), 33–38. https://doi.org/10.32782/2786-765X/2025-9-4 (in Ukrainian)
13. Panchenko, O. A. (2020). Informatsiina bezpeka v konteksti vyklykiv i zahroz natsionalnii bezpetsi [Information security in the context of challenges and threats to national security]. *Derzhavne Upravlinnia ta Mistseve Samovriaduvannia*, (45), 57–63. https://doi.org/10.33287/102019 (in Ukrainian)
14. Onyshchenko, S. V. (2022). Zahrozy informatsiinii bezpetsi natsionalnoi ekonomiky [Threats to the information security of the national economy]. *Naukovyi Visnyk Odeskoho Natsionalnoho Ekonomichnoho Universytetu*, (300–301), 50–56. https://doi.org/10.32680/2409-9260-2022-11-12-300-301-50-56 (in Ukrainian)
15. Khaustova, V. Ye., & Trushkina, N. V. (2024). Klasyfikatsiia zahroz natsionalnii bezpetsi krainy [Classification of threats to the country's national security]. In *Suchasni Vektory Rozvytku Ukrainy: Zabezpechennia Stalosti ta Bezpeky: Materialy II Mizhnarodnoi Naukovo-Praktychnoi Konferentsii* (October 28, 2024, Kyiv, Ukraine). https://doi.org/10.54929/conf_28_10_2024-01-02 (in Ukrainian)
16. Kharchenko, S. O. (2019). Naukovi pidkhody do klasyfikatsii zahroz informatsiinii bezpetsi [Scientific approaches to the classification of information security threats]. *Derzhava ta Rehiony*, (66), 191–197. http://pa.stateandregions.zp.ua/archive/2_2019/35.pdf (in Ukrainian)
17. *Konstytutsiia Ukrainy* [Constitution of Ukraine]. (1996, June 28). Law of Ukraine No. 254к/96-BP. *Vidomosti Verkhovnoi Rady Ukrainy*, (30). https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (in Ukrainian)
18. *Pro informatsiiu* [On information]. (1992, October 2). Law of Ukraine No. 2658-XII. https://zakon.rada.gov.ua/laws/show/2657-12#Text (in Ukrainian)
19. *Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh* [On protection of information in information and communication systems]. (1994, July 5). Law of Ukraine No. 80/94-BP. https://zakononline.ua/documents/show/162730__594986 (in Ukrainian)
20. *Pro natsionalnu bezpeku Ukrainy* [On national security of Ukraine]. (2018, June 21). Law of Ukraine No. 2469-VIII. https://zakon.rada.gov.ua/laws/show/2469-19 (in Ukrainian)
21. *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku "Pro Stratehiiu informatsiinoi bezpeky"* [On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On the Information Security Strategy"]. (2021, December 28). Decree of the President of Ukraine No. 685/2021. https://zakon.rada.gov.ua/laws/show/685/2021#Text (in Ukrainian)
22. *Pro vvedennia voiennoho stanu* [On the introduction of martial law]. (2022, February 24). Decree of the President of Ukraine No. 64/2022. https://zakon.rada.gov.ua/laws/show/64/2022#Text (in Ukrainian)
23. *Pro media* [On media]. (2023, March 31). Law of Ukraine No. 2693-IX. https://jurliga.ligazakon.net/news/218516_31-bereznya-nabude-chinnost-zakon-pro-meda (in Ukrainian)
24. Shevchuk, M. O. (2024). Suchasni vyklyky i zahrozy v sferi informatsiinoi bezpeky derzhavy [Modern challenges and threats in the field of state information security]. *Aktualni Problemy Vitchyznianoi Yurysprudentsii*, (6), 160–166. https://doi.org/10.32782/2408-9257-2024-6-25 (in Ukrainian)
25. Zalievska, I. I., & Udrenas, H. I. (2022). Informatsiina bezpeka v Ukraini v umovakh rosiiskoi viiskovoi ahresii [Information security in Ukraine under conditions of Russian military aggression]. *Pivdennoukrainskyi Pravnychyi Chasopys*, (1), 20–26. https://doi.org/10.32850/sulj.2022.1-2.4 (in Ukrainian)
26. Halipchak, V. D. (2023). Transformatsiia informatsiinoho prostoru Ukrainy pid vplyvom rosiiskoi ahresii: Zminy ta vyklyky [Transformation of Ukraine's information space under the influence of Russian aggression: Changes and challenges]. *Naukovyi Zhurnal "Politykus"*, (4), 26–30. https://doi.org/10.24195/2414-9616.2023-4.4 (in Ukrainian)

27. Krushenitskyi, V. S. (2024). Orhany publichnoi vlady yak subiekty formuvannia ta realizatsii polityky natsionalnoi bezpeky v informatsiinomu prostori [Public authorities as subjects of formation and implementation of national security policy in the information space]. *Naukovi Zapysky. Seriia: Pravo*, (17), 252–256. https://doi.org/10.36550/2522-9230-2024-17-252-256 (in Ukrainian)
28. Tsybulnyk, N. Yu. (2023). Informatsiino-pravova kharakterystyka osnovnykh skladovykh sektoru bezpeky derzhavy [Information-legal characteristics of the main components of the state security sector]. *Naukovyi Visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia Pravo*, *1*(80), 607–612. https://doi.org/10.24144/2307-3322.2023.80.1.93 (in Ukrainian)
29. Tomkiv, I. O., & Hurtovyi, D. Ye. (2024). Mekhanizm derzhavnoho reahuvannia na zahrozy suspilno-politychnoho kharakteru (svitovyi ta vitchyznianyi dosvid) [Mechanism of state response to socio-political threats (global and national experience)]. *Ekonomika ta Suspilstvo*, (60). https://doi.org/10.32782/2524-0072/2024-60-54 (in Ukrainian)
30. Lysenko, S. O. (2023). Pryntsypy i mekhanizmy pryiniattia derzhavno-upravlinskykh rishen v haluzi informatsiinoi bezpeky [Principles and mechanisms of adopting state-management decisions in the field of information security]. *Pravo ta Derzhavne Upravlinnia*, (2), 561–567. https://doi.org/10.32782/pdu.2023.2.82 (in Ukrainian)
31. Teki, G. (2022). NATO as a global cybersecurity power. In *Dijitalleşen Dünyada Birey, Toplum, Siyaset Kongresi Bildiri Kitabı* (pp. 154–169). https://www.researchgate.net/publication/361763403_NATO_as_a_Global_Cybersecurity_Power
32. Khakimova, V. T. (2021). Yevropeiskyi Soiuz v epokhu postpravdy: Diialnist EAST STRATCOM TASK FORCE [The European Union in the era of post-truth: Activities of EAST STRATCOM TASK FORCE]. *Aktualni Problemy Polityky*, (67), 155–162. https://doi.org/10.32837/app.v0i67.1166 (in Ukrainian)
33. European Business Association. (2025). *CERT-UA zaklykaie biznes do tisnishoi spivpratsi u sferi kiberbezpeky* [CERT-UA calls on business for closer cooperation in cybersecurity]. https://eba.com.ua/cert-ua-zaklykaye-biznes-do-tisnishoyi-spivpratsi-u-sferi-kiberbezpeky (in Ukrainian)
34. UNESCO. (2025). *Kampaniyi YUNESKO z media- ta informatsiinoi hramotnosti dopomahaiut milionam ukraintsiv rozvyvaty navychky krytychnoho myslennia* [UNESCO media and information literacy campaigns help millions of Ukrainians develop critical thinking skills]. https://www.unesco.org/uk/articles/kampaniyi-yunesko-z-media-ta-informatsiynoyi-hramotnosti-dopomahayut-milyonam-ukrayintsiv-rozvyvaty (in Ukrainian)
35. Slinko, T. M. (2023). Suchasni vyklyky informatsiinii bezpetsi v realiiakh viiskovoi ahresii [Modern challenges to information security in the realities of military aggression]. In *Natsionalna bezpeka yak konstytutsiina tsinnist: Suchasni vyklyky: Materialy Mizhnarodnoi naukovo-praktychnoi konferentsii z nahody Dnia Konstytutsii Ukrainy, 22 chervnia 2023 r.* [National security as a constitutional value: Current challenges: Proceedings of the International Scientific and Practical Conference on the occasion of the Constitution Day of Ukraine, June 22, 2023] (pp. 143–148). Yaroslav Mudryi National Law University, Yuriy Fedkovych Chernivtsi National University, & Ivan Franko National University of Lviv. https://dspace.nlu.edu.ua/jspui/handle/123456789/19775 (in Ukrainian)
36. *Pro zatverdzhennia planu zakhodiv z realizatsii Stratehii informatsiinoi bezpeky na period do 2025 roku* [On approval of the action plan for implementing the Information Security Strategy until 2025]. (2023, March 30). Resolution of the Cabinet of Ministers of Ukraine No. 272-r. https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text (in Ukrainian)