

DOI: 10.52363/passa-2025.2-10

UDC: 351.746.1:316.334.3(477

Novak V., Director of the Department of Critical Infrastructure Protection, Administration of the State Service of Special Communications and Information Protection of Ukraine

ORCID: 0009-0003-6516-0742

Burtovyi R., doctoral student at the National University of Civil Defence of Ukraine, Cherkasy

ORCID: 0009-0004-4568-0094

RESOURCE POTENTIAL OF SOCIAL INSTITUTIONS IN THE STATE INFORMATION SECURITY MANAGEMENT SYSTEM IN UKRAINE

The article is devoted to the study of the resource potential of social institutions as subjects of the state information security management system in Ukraine. The theoretical foundations of information security management in the context of mediatization of society and technological determination of information risks are considered. The functions and resources of key social institutions – the state, education, family, media and civil society – in countering information threats are analyzed. Particular attention is paid to the impact of the hypernetwork model of media communications on the expansion of the information risk zone and the transformation of management mechanisms. Based on the analysis of current challenges to Ukraine's information security, particularly under martial law, priority areas for developing the resource potential of institutional management subjects are identified. The necessity of integrating formal and informal control mechanisms, strengthening inter-institutional cooperation, and adapting management tools to the dynamics of technological changes in the media space is substantiated.

Keywords: *information security, public administration, social institutions, resource potential, mediatization, information risks, hypernetwork model, media communications, Ukraine.*

Problem Statement and Its Connection with Relevant Scientific and Practical Tasks.

The transformation of the information space under the influence of rapid technological development of media communications creates fundamentally new challenges for the state information security management system. The mediatization of social life, characterizing the current stage of civilizational development, generates complex management problems related to the need to protect the national information space under conditions of hypernetwork organization of media communications. This issue is particularly relevant for Ukraine, which has been facing large-scale information aggression since 2014, and since 2022 – under conditions of full-scale war. The Information Security Strategy of Ukraine, approved by Presidential Decree No. 685/2021 of December 28, 2021, defines information security as a state of protection of state sovereignty in which constitutional human rights and freedoms to information are ensured and an effective system for countering negative information influences exists [7]. The implementation of this strategy requires rethinking the role and resource potential of social institutions as subjects of information security management.

Research on media consumption among Ukrainians demonstrates critical trends: growing distrust of traditional information sources (from 7.7% in 2023 to 15.2% in 2024 of those who do not trust any source), dominance of social networks as the main channel for receiving news (73.4% of the population), intensification of information flows against the background of declining media literacy in certain population groups [5]. At the same time, the media literacy index of Ukrainians, despite adaptation to wartime realities, remains unstable, indicating insufficient effectiveness of existing information security management mechanisms [3]. The technological determination of information risks manifests in multiple aspects. First, the hypernetwork organization of the media space creates conditions for instantaneous dissemination of destructive content, minimizing possibilities for preventive control. Second, the rhizomorphic and decentralized nature of network structures limits the effectiveness of traditional hierarchical state management mechanisms. Third, the adaptivity and omnipresence of media form new challenges for all social institutions, forcing them to transform functions and develop specific management resources [4; 8].

Analysis of current cyber threats to Ukraine's critical infrastructure confirms the scale of the problem: in 2024, over 3 million information security events were recorded, of which

28 thousand were classified as critical [4]. This actualizes the issue not only of technical protection of information systems but also of developing institutional capacity to counter information threats at all levels of social organization. The problem of ensuring information security under modern conditions cannot be solved exclusively through state coercion or technical control. It requires a comprehensive approach based on mobilizing resources of all social institutions – education, family, media, civil society – each possessing specific functions and capabilities to influence different aspects of information security [7; 8; 9].

The scientific and practical significance of researching the resource potential of social institutions lies in the need to develop conceptual foundations for an integrated information security management system that considers the specifics of mediatized society, technological dynamics of information risks, and peculiarities of functioning of different institutional subjects. Particularly relevant is the definition of mechanisms for coordinating institutional activities, optimizing the distribution of management functions, and adapting their resource potential to the challenges of hyperinformation society.

Analysis of Recent Domestic and Foreign Research. The issue of information security and mechanisms for its provision is actively developed in domestic public administration science, however, the question of resource potential of social institutions as systemic management subjects remains insufficiently researched. Theoretical foundations of state information security are laid in works by I. Bosak, who comprehensively examines types and kinds of information threats to national security, methods of protecting information sovereignty, and strategic directions of state policy in this sphere. The author rightly emphasizes the necessity of clear performance of duties by each subject of the information security system and ensuring high level of their interaction [1]. However, functional distribution between institutional subjects and specifics of their management resources require further conceptualization.

O. Puhachov analyzes problems of ensuring Ukraine's information security in the context of rapid development of information technologies and globalization. The researcher substantiates that information security integrates into various spheres of state security – political, economic, social – while simultaneously acting as a separate element of the national security system [7]. However, the question of how different social institutions can

compensate for limited state resources in ensuring this integration remains unaddressed. L. Velychko and M. Bilokon research hybrid threats to transport infrastructure, revealing challenges for state regulation and national security. Their work demonstrates how sectoral threats require inter-institutional coordination and mobilization of resources from various management subjects [2]. This approach can be extrapolated to the broader context of information security, where institutional interaction acquires critical significance.

Significant contribution to understanding modern challenges of information security is made by A. Ilyenko's research group, which analyzes cyber threats to critical infrastructure. The authors record qualitative change in the nature of threats: over 3 million information security events in 2024 indicate that traditional technical control mechanisms prove insufficient without involving social institutions in preventive work [4]. However, the question about specific mechanisms of such involvement and criteria for evaluating their effectiveness remains open. Empirical studies of media consumption and media literacy conducted by OPORA Civic Network and Detector Media NGO record alarming trends. Growing distrust of all information sources (15.2% in 2024 versus 7.7% in 2023), dominance of social networks as the main channel for receiving news, fatigue from news content – all this points to a crisis of traditional media space institutions and the necessity of searching for new forms of ensuring information security [3; 5; 10]. At the same time, these studies do not offer systematic analysis of how different institutions could respond to these challenges.

USAID-Internews research reveals a paradoxical situation: Ukrainians show highest trust to family and friends (85%), while trusting official state institutions significantly less [10]. This questions the effectiveness of vertical management models and actualizes the role of informal social institutions in the information security system.

Conceptualization of social institution in the Great Ukrainian Encyclopedia emphasizes key characteristics of institutions: stability, complex organization, presence of formal and informal norms, performance of specific functions [9]. However, in the context of information security, it remains unclear how exactly these characteristics transform under the influence of mediatization and what new functions institutions acquire under conditions of hyperinformation society. Critical analysis of scientific literature reveals several gaps. First, there is a lack of comprehensive research that would consider the system of social institutions

as an integral subject of information security management rather than limiting itself to analyzing the state's role. Second, the specifics of resource potential of different institutions and mechanisms of its mobilization under conditions of technological transformation of media space are insufficiently studied. Third, there is absence of research that would systematically analyze how mediatization of society changes functional distribution between institutions and generates need for new forms of inter-institutional coordination.

The purpose of the article is theoretical substantiation and empirical analysis of the resource potential of social institutions as subjects of the state information security management system under conditions of society mediatization and technological transformation of the information space.

Presentation of Main Research Material with Full Justification of Obtained Scientific Results. Social institutions, as defined by the Great Ukrainian Encyclopedia, are supra-personal formations that form the macrostructure of society and are characterized by stability, complex organization, and ability to regulate social practices through a system of formal and informal norms [9]. In the context of information security management, social institutions act not merely as objects of protection but as active management subjects, each possessing specific resource potential. We define the resource potential of an institution as a set of material, organizational, normative, communicative, and symbolic capabilities that can be mobilized to perform management functions in the sphere of information security. A key feature of institutional resources is their complementarity: management effectiveness is achieved not through dominance of one institution but through coordination and mutual complementation of different institutional subjects.

Ukraine's Information Security Strategy defines information security as a component of national security, a state of protection of state sovereignty and constitutional rights of citizens, in which an effective system for countering negative information influences exists [6]. However, implementation of this strategy requires clear understanding of which institutions, with what resources, and at which management levels can ensure this protection. Mediatization, understood as penetration of media logic into all spheres of social life and transformation of social practices under influence of media technologies, radically changes conditions of social institutions' functioning.

Studies of media consumption among Ukrainians demonstrate the scale of these changes: 73.4% of population receive news from social networks, while traditional television is used by only 42.7% of respondents [5]. Particularly indicative is the decline in trust toward the telemarathon format from 45% in 2022 to 17% in 2024 [3]. These data indicate a crisis of traditional media institutions and actualization of the role of new actors in the information space. At the same time, growing distrust of all information sources, when 15.2% in 2024 do not trust any source compared to 7.7% in 2023, points to a systemic problem of legitimacy of information intermediaries [5]. In this situation, institutions based on interpersonal trust acquire special significance: USAID-Internews research records that 85% of Ukrainians trust family and friends, which significantly exceeds trust in any media or state institutions [10].

The modern media space is characterized by hypernetwork organization, where information circulates not through centralized channels but through multiple decentralized nodes with horizontal connections. This model generates specific challenges for information security management. The rhizomorphic nature of the network, that is, its ability to grow in any direction without clear hierarchy, limits effectiveness of traditional regulatory mechanisms. State control oriented toward formal mass media institutions proves insufficient in situations where information spreads through messengers, social networks, and private communication channels. Decentralization and equalization of content creators' statuses lead to weakening of professional standards and normative requirements for information. If previously the journalism institution through editorial policy, professional ethics, and legal responsibility ensured a certain level of information quality, now any user can become a news source, often without adhering to any verification standards [1; 7].

Network openness to any subjects creates opportunities for malicious activity. Research on cyber threats to critical infrastructure records over 3 million information security events in 2024, of which 28 thousand were classified as critical [4]. These figures demonstrate not only technical but also social dimension of the problem: technological vulnerabilities are exploited through manipulating user behavior, using social engineering methods, creating disinformation campaigns. Network adaptivity, that is, its ability to change configuration in response to external influences, nullifies effectiveness of targeted control measures. Blocking

one channel of destructive content dissemination leads to its instant reproduction in other forms and on other platforms. Media omnipresence, their ubiquity in everyday life, means that avoiding contact with potentially harmful information becomes practically impossible, which is especially critical for vulnerable population groups [6; 8].

The state possesses the most formalized and structured resource potential in the sphere of information security. Normative-legal resources include legislative framework regulating information space, mechanisms of legal responsibility for disseminating destructive information, tools for technical protection of critical infrastructure. O. Puhachov rightly emphasizes that information security integrates into various spheres of state security and requires coordination of numerous state bodies' activities [7]. However, research reveals significant limitations of state resources. Formal control mechanisms prove ineffective under conditions of hypernetwork organization of media space, as regulatory attempts encounter the problem of extraterritoriality: a significant portion of content is created and disseminated through platforms beyond national state jurisdiction.

State institutions also face legitimacy problems. Declining trust in state information sources limits effectiveness of official communication campaigns. Research records decline in trust toward the Presidential Office from 69% in 2023 to 44% in 2024 [10]. This means that even reliable information disseminated through state channels may be perceived skeptically by the population. Under martial law conditions, redistribution of state resources toward security and defense sector objectively limits possibilities for financing media literacy programs, developing civic education, and supporting independent media [2].

The education institution possesses unique resource of systematic influence on forming critical thinking and skills of safe behavior in information space. The media literacy index of Ukrainians demonstrates that education level directly correlates with media competence: among persons with general secondary education, 41% have low media literacy level, while among those with higher education only 16% [3]. However, resource potential of educational institutions is insufficiently realized due to fragmentation of systematic integration of media education into curricula. Under war conditions, educational institutions themselves require adaptation to new realities: distance learning, relocation of institutions, psychological trauma of educational process participants create additional challenges for implementing

educational functions. At the same time, educational institutions possess critically important resource of long-term influence, as forming media literacy in children and youth creates foundation of society's information resilience for decades ahead.

Family as a basic social institution possesses resource of informal control and formation of primary models of information behavior. USAID-Internews research records a paradoxical situation: Ukrainians show highest trust precisely to family and friends, which significantly exceeds trust in any institutionalized information sources [10]. This indicates that family actually performs function of primary information verification, filtering and interpreting information flows for its members. However, family institution resources are limited by parents' media literacy level and possibilities for controlling children's information consumption. Media omnipresence means that children access information not only at home but also through mobile devices, at school, in communication with peers. Domestication of media technologies, that is, their penetration into home space, blurs traditional boundaries between public and private, complicating parental control [6; 9].

Professional media possess resource of expertise, reputation, organized editorial processes of information verification. I. Bosak emphasizes importance of media role in information security system, stressing necessity of adhering to professional standards and ethical norms [1]. However, media consumption research reveals crisis of trust in traditional media: trust in television decreased, trust in print media fell from 30.3% in 2023 to 18% in 2024 [5]. This crisis is partially explained by conflict between professional mission of media and commercial logic, as 51% of Ukrainians believe media work in interests of authorities, 40% in their own interests, 24% in interests of owners and investors [3]. Such situation undermines symbolic resource of media institutions, that is, their ability to form agenda and legitimize certain event interpretations. At the same time, emergence of new forms of media institutionalization should be noted: independent fact-checking organizations, public media, media literacy platforms form alternative segment of media space oriented precisely toward enhancing information security [3].

Civil society institutions possess resource of horizontal mobilization, ability to quickly respond to information threats through civic initiatives, volunteer projects, awareness campaigns. Unlike vertical state structures, civil society organizations can work with

local communities considering their specifics and needs. Media literacy index research demonstrates society's demand for civic control: 44% of Ukrainians support criticism of authorities in media, considering it an important element of democracy [3]. This indicates awareness of public oversight role in ensuring information security. However, civil society resources are limited by dependence on external financing, fragmentation of activities, insufficient coordination between different organizations, and under war conditions part of civil sector resources redirects toward humanitarian aid and army support [7; 8].

Analysis of individual institutions' resource potential leads to conclusion about necessity of integrated information security management model. No institution in isolation possesses sufficient resources for effectively countering information threats in mediatized society. Effectiveness is achieved through synergy of institutional resources, when state normative mechanisms are complemented by educational programs for enhancing media literacy, professional media standards, informal family control, and horizontal mobilization of civil society. L. Velychko and M. Bilokon in their research on hybrid threats substantiate necessity of inter-institutional coordination and distribution of responsibility between different subjects [2]. Extrapolating this approach to information security sphere, we can assert that integrated model requires clear distribution of functions between institutions while maintaining mechanisms of their coordination and interaction.

Key challenge of implementing such model in Ukrainian realities is necessity of forming coordination mechanisms between institutions. Information Security Strategy creates formal basis for such coordination [6], however practical implementation requires developing specific interaction protocols, distributing responsibility, creating platforms for information exchange between institutional subjects. Experience of information security system functioning under martial law conditions demonstrates both potential and limitations of existing inter-institutional interaction mechanisms, actualizing need for their improvement based on clear understanding of each institutional subject's resource capabilities.

Conclusions. The conducted research confirms that effective information security management under conditions of society mediatization is impossible without comprehensive mobilization of resource potential of all social institutions. Analysis of Ukraine's information security system functioning reveals critical dependence of its effectiveness on different

institutional subjects' ability to coordinate their activities and mutually complement each other's limited resources. It has been established that hypernetwork organization of modern media space generates qualitatively new challenges for traditional management mechanisms. Rhizomorphic nature, decentralization, and omnipresence of media networks limit effectiveness of vertical management models. Empirical research data demonstrate that 73.4% of Ukrainians receive news through social networks, while distrust of all institutionalized information sources is growing. This situation actualizes role of informal institutions, primarily family, which 85% of population trust.

The research revealed specific limitations of state institutions' resource potential: extraterritoriality of media content, declining trust in state sources, redistribution of resources toward defense narrow possibilities of state management. At the same time, state retains unique resource of normative-legal regulation and coordination of other institutional subjects' activities. Educational institutions possess critically important resource of long-term influence through forming media literacy, however this potential is insufficiently realized due to fragmentation of media education integration into curricula. Conceptual contribution of research is substantiation of integrated information security management model based on synergy of different social institutions' resources. Such model's effectiveness is achieved through clear distribution of functions while maintaining coordination and interaction mechanisms. Ukraine's Information Security Strategy creates formal basis for such coordination, however practical implementation requires developing specific interaction protocols and mechanisms for evaluating inter-institutional cooperation effectiveness. For Ukraine functioning under conditions of full-scale war and confronting large-scale information aggression, developing resource potential of social institutions acquires special relevance. Prospects for further research are connected with developing mechanisms for assessing individual institutions' resource potential, creating methodologies for analyzing inter-institutional interaction effectiveness, and studying foreign experience of integrated information security management models.

References:

1. Bosak, I. (2025). *Informatsiyna bezpeka Ukrayiny: zahrozy ta metody protydyiy*

- [Information Security of Ukraine: Threats and Countermeasures]. Kyivskyi ekonomichnyi naukovyi zhurnal, 9, 33-38. <https://doi.org/10.32782/2786-765X/2025-9-4>
2. Index of Media Literacy of Ukrainians 2020–2024 (fifth wave). (2025). Detector Media NGO. <https://detector.media/infospace/article/240621/2025-05-06-indeks-mediagramotnosti-ukraintsiv-za-2024-rik/>
 3. Ilyenko, A., Ilyenko, S., Yakovenko, O., Halych, Ye., & Pavlenko, V. (2025). Suchasni kiberzahrozy krytychnoyi infrastruktury Ukrayiny ta svitu [Modern Cyber Threats to Critical Infrastructure of Ukraine and the World]. Kiberbezpeka: osvita, nauka, tekhnika, 3(27), 150-164. <https://doi.org/10.28925/2663-4023.2023.27.719>
 4. Media Consumption of Ukrainians: Third Year of Full-Scale War. (2024). OPORA Civic Network. <https://oporaua.org/viyna/doslidzhennya-mediaspozhyvannya-ukrayinciv-tretyi-rik-povnomasshtabnoyi-viyni-25292>
 5. Presidential Decree No. 685/2021 "On the Information Security Strategy". (2021, December 28). <https://zakon.rada.gov.ua/go/685/2021>
 6. Puhachov, O.I. (2024). Problemy zabezpechennya informatsiynoyi bezpeky Ukrayiny v suchasnykh umovakh [Problems of Ensuring Information Security of Ukraine in Modern Conditions]. Problemy suchasnykh transformatsiy. Seriya: pravo, publichne upravlinnya ta administruvannya, 12. <https://doi.org/10.54929/2786-5746-2024-12-02-15>
 7. Social Institution. (2025). Velyka Ukrayinska Entsyklopediya [Great Ukrainian Encyclopedia]. https://vue.gov.ua/Соціальний_інститут
 8. System of Information Security Management in the Context of Modern Challenges. (2024). Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriya "Yurydychni nauky", 1, 130-136. <https://doi.org/10.32999/ksu2307-8847/2024-1-18>
 9. Ukrainian Media: Attitudes and Trust in 2024. (2024). USAID-Internews Research. <https://detector.media/infospace/article/234411/2024-11-07-naybilsh-nadiynim-dzherelom-informatsii-dlya-ukraintsiv-zalyshayutsya-rodyna-y-druzi-doslidzhennya-usaid-internews/>

10. Velychko, L.Yu., & Bilokon, M.V. (2024). Hibrydni zahrozy transportniy infrastrukturi: vyklyky dlya derzhavnoho rehulyuvannya ta natsionalnoyi bezpeky [Hybrid Threats to Transport Infrastructure: Challenges for State Regulation and National Security]. *Teoriya ta praktyka derzhavnoho upravlinnya*, 2(79), 442-464. <http://doi.org/10.26565/1727-6667-2024-2-23>