UDC 351.862.4

O. Ursol

DEVELOPMENT OF DEMOCRATIC CIVILIAN CONTROL IN THE FIELD OF PUBLIC MANAGEMENT OF CRITICAL INFRASTRUCTURE INFORMATION SECURITY OF UKRAINE

The relevance of ensuring the information security of Ukraine's critical infrastructure in the context of full-scale armed aggression and the growth of cyber threats, with an emphasis on the need to combine the effectiveness of security policy with compliance with democratic principles, has been substantiated. The essence and significance of democratic civilian control as a key mechanism for ensuring transparency, accountability and legality of the activities of the subjects of the security and defense sector are revealed. The main directions of development of the civil control system have been identified, in particular, the improvement of the regulatory framework, the formation of institutional capacity, the development of the organizational component and the strengthening of social elements. It is concluded that the formation of an effective system of democratic civilian control is an important prerequisite for strengthening national security, increasing the stability of the state and ensuring its European and Euro-Atlantic integration. Prospects for further research are outlined.

Keywords: *critical infrastructure, public administration and administration, democratic civilian control, security and defense sector, crisis situations, state security, protection of critical infrastructure facilities.*

Statement of the problem. The relevance of the study of public administration in the field of information security of Ukraine's critical infrastructure is determined by the increasing importance of the information space as a key factor of national security in the context of hybrid threats and digitalization. Critical infrastructure facilities, in particular energy, transport, communications, financial and medical spheres, are increasingly dependent on information and communication technologies. At the same time, such dependence not only increases their efficiency functioning, but also forms new risks associated with cyber threats, information attacks and other destructive influences.

In the context of full-scale armed aggression against Ukraine, the number and intensity of cyberattacks on state information resources, management systems and critical infrastructure facilities has significantly increased, which necessitates the formation of an effective system of public information security management. In this regard, it is of particular importance to ensure the continuity of the functioning of critical systems and proper protection of information resources. At the same time, the priority is to increase resilience to cyber threats and ensure timely response to incidents.

In the context of the above, the study of the development of democratic civilian control in the field of public management of information security of the critical infrastructure of Ukraine, which is due to the need to ensure a balance between the effectiveness of security measures and compliance with democratic principles, transparency and accountability of the authorities, is of no less importance. Critical infrastructure, which operates on the basis of complex information and communication systems, requires not only technical protection, but also effective mechanisms of democratic oversight that ensure the legality, validity and controllability of managerial decisions. In this context, it is important to involve civil society institutions, independent experts and parliamentary control in the formation and implementation of state policy in the field of information security.

Additional relevance to the study is Ukraine's course towards European and Euro-Atlantic integration, which provides for the introduction of the principles of good governance, the rule of law and civilian control over the security sector. This requires improving the regulatory framework, developing institutional mechanisms for accountability, transparency and effective

Copyright © 2026 Honor and Law / Честь і Закон, O. Ursol

interaction between the state, the private sector and the public. Therefore, the development of democratic civilian control is a necessary condition for increasing the resilience of the information security system, strengthening public trust and ensuring the national security of Ukraine in the face of modern challenges.

Analysis of recent research and publications. The development of democratic civilian control in the field of public management of information security of Ukraine's critical infrastructure is interdisciplinary, so it was studied by representatives of various scientific areas – public administration, law, national security, cybersecurity and economics.

A sufficient number of studies have been conducted on the diverse issues of critical infrastructure protection. In particular, O. I. Yaremenko and Y. I. Strakhnitsky investigated theoretical approaches to defining the definition of critical infrastructure as an object of public administration [1]. Actual problems and ways to solve them on the protection of national critical information infrastructure were studied by D. S. Melnyk [2]. The dissertation on the administrative and legal regulation of the state system of critical infrastructure protection of Ukraine was carried out by S. S. Telenik [3]. The theoretical and legal foundations of ensuring information security of Ukraine were developed by O. D. Dovgan [4]. Scientists S. G. Gordienko and I. M. Doronin substantiated the information and legal aspects of the protection of critical infrastructure in Ukraine [5]. Researchers A. V. Ilyenko, V. A. Telushchenko and O. V. Dubchak have identified modern cyber threats to critical infrastructure in Ukraine and the world [6]. O. S. Trofimov focused on improving the security policy of information systems of critical infrastructure facilities in Ukraine on the basis of the ZERO TRUST concept [7]. The security dimension of critical infrastructure from the point of view of economics was studied by O. I. Baranovsky [8].

The study of problematic issues of democratic civilian control in the field of functioning of components of the security and defense sector has been paid attention by a large scientific community. The concept and procedures of public control over the activities of the National Police as a subject of the security and defense sector were studied by V. V. Bezega [9]. Scientist M. V. Sitsinska studied the elements of public control in the system of democratic civilian control over the security and defense sector [10], as well as the issue of rationality of public control over the activities of state authorities in the field of security and defense [11]. Researchers A. V. Chub and E. M. Naydyon substantiated the issue of development of democratic civilian control over the activities of the system of security and defense sector bodies of Ukraine.

At the same time, it is appropriate to note that insufficient attention was paid to the study of the problematic issues of democratic civilian control in the field of public management of information security of the critical infrastructure of Ukraine, which actualized the direction of the study.

The purpose of the article is to study democratic civilian control in the field of public management of information security of critical infrastructure of Ukraine, as well as substantiating proposals for further development of this topical problem.

Summary of the main material. In the context of full-scale armed aggression and growing cyber threats, the state is forced to strengthen control and regulation in the field of information security, which at the same time actualizes the risks of excessive centralization, restriction of citizens' rights and freedoms and a decrease in the level of public trust.

As D. S. Melnyk emphasizes, Ukraine still has significant problems in the legal regulation of the functioning and protection of the national critical information infrastructure, as well as the imperfection of state policy in this area, especially in the context of increased risks of sabotage, terrorist and cyber-attacks on the relevant facilities. In this regard, in order to ensure an adequate level of their protection, it is necessary to complete the formation of an integral legislative framework, create an effective national protection system and introduce unified approaches to ensuring their stable functioning. At the same time, it is important to introduce international standards, develop public-private partnership and intensify international cooperation in this area [2, p. 13].

According to S. G. Gordienko and I. M. Doronin, the information and legal aspects of the protection of critical infrastructure indicate the presence of a number of problems that can be conditionally divided into two groups. The first group is related to the difficulty of classifying individual elements as critical infrastructure facilities, since the current legislative approaches are mainly focused on physical objects and do not sufficiently take into account the specifics of information infrastructure, information resources and data processing systems. The second group of

problems concerns the definition of organizational measures of information protection and restriction of access to information about such objects, because ensuring a balance between the open data policy and transparency of public administration, public access and security needs is a difficult task [5, p. 122].

Scientists O. I. Yaremenko and Y. I. Strakhnitsky emphasize that critical infrastructure is a component of the national infrastructure, which determines its key importance for ensuring the functioning of society, the economy and the sustainable development of the state as a whole. The analysis of the approaches of different countries to the interpretation of the term "critical infrastructure" gives grounds to assert the existence of a priority triad in the structure of its content "person – society – state", which reflects the objects of national infrastructure that are crucial for ensuring civil, public and state security [1, p. 80].

According to A. V. Ilyenko, V. A. Telushchenko and O. V. Dubchak, one of the key aspects is the development of international cooperation and information exchange between government agencies, the private sector and specialized organizations, which provides an opportunity to respond to the latest challenges in a timely manner. Interstate interaction and exchange of experience are becoming important in countering global threats, and the implementation of international standards, in particular the NIS2 directive, contributes to the formation of unified cyber defense mechanisms. The need to increase the level of personnel training and the introduction of clear policies for access to information systems is emphasized, since the human factor continues to be one of the most vulnerable elements of cybersecurity [6, p. 162].

Therefore, based on the analysis of the above-mentioned scientific research, it can be concluded that in the field of protection of critical infrastructure, the scientific community is currently interested in the issue of interaction and cooperation between the authorities and the public. Additional relevance is determined by Ukraine's course towards integration into the European and Euro-Atlantic security space, which provides for the harmonization of national legislation and the introduction of international standards in the field of cyber and information security. It is important to develop effective public-private cooperation in this area. In these conditions, the improvement of coordination mechanisms of public administration, a clear delimitation of powers and the development of systems for monitoring, analysis and forecasting of threats with the involvement of mechanisms of democratic civilian control are of particular importance.

Democratic civilian control in the field of security and defense is a key condition for the functioning of a legal, democratic state, as it ensures accountability, transparency and legality of the activities of law enforcement agencies. Its importance lies in preventing excessive concentration of power in the security sector, preventing abuses, violations of citizens' rights and freedoms, as well as in building public trust in state institutions. Through the mechanisms of parliamentary, governmental, judicial and public control, the activities of the security forces are ensured that the activities of the security forces comply with national legislation and democratic principles.

In the context of modern security challenges, in particular military aggression and hybrid threats, the importance of democratic civilian control does not decrease, but, on the contrary, increases, since it makes it possible to combine the effectiveness of defense activities with compliance with the principles of the rule of law. At the same time, it contributes to improving the quality of management decisions, ensures the rational use of resources and forms a system of checks and balances in the security and defense sector. Thus, democratic civilian control is not only a tool of oversight, but also an important factor in strengthening national security, the resilience of the state and its Euro-Atlantic integration.

Democratic civilian control is of particular importance in the field of public management of information security of Ukraine's critical infrastructure. Rapid digitalization and the growing dependence of key industries, in particular energy, transport, communications and the financial system, on information and communication technologies are increasing the requirements for the management of this area. In this regard, effective governance requires not only technical and organizational solutions, but also ensuring an appropriate level of accountability, transparency and control.

In this context, democratic civilian control is an important tool for ensuring the legality of managerial decisions, preventing abuses and increasing the efficiency of the information security system. It contributes to the involvement of civil society, the expert community and the private sector in the formation and implementation of public policy, which makes it possible to improve the quality of governance and adaptability

to modern threats. Therefore, the development of public administration in the field of information security of Ukraine's critical infrastructure should be based on a combination of effective security mechanisms with the principles of democratic civilian control, which ensures the stability, openness and reliability of the state security system.

Scholars A. V. Chub and E. M. Naydyon note that the establishment of effective democratic civilian control is considered as an important step towards improving civil-military relations, ensuring the rule of law and accountability of law enforcement agencies to society. This is not only an urgent requirement of our time, but also a necessary condition for the functioning of the rule of law with a developed civil society. This approach meets the standards of states with established democracies and contributes to the processes of Euro-Atlantic integration of Ukraine [12, p. 151, 152].

According to the current legislation, the system of civil control covers control exercised by the President of Ukraine, the Verkhovna Rada of Ukraine, the National Security and Defense Council of Ukraine, the Cabinet of Ministers of Ukraine, other executive authorities and local self-government bodies, as well as judicial control and public supervision. Citizens of Ukraine exercise the right to participate in civil control through the activities of public associations, deputies of local councils or directly by appealing to the Commissioner for Human Rights of the Verkhovna Rada of Ukraine or other state bodies in accordance with the Constitution of Ukraine and current legislation [13].

Public associations established and registered in accordance with the procedure established by law shall be guaranteed the opportunity, within the framework of the legislation and their statutory activities, to receive information from state bodies on the functioning of the security and defense sector (except for information with limited access), to conduct scientific research in the field of national security and defense and to publish their results, as well as to create appropriate analytical centers and expert platforms. They have the right to carry out public examination of draft regulations, state programs and decisions, submit their proposals to state authorities, as well as participate in public discussions, parliamentary hearings and other forms of open dialogue on the development of the security and defense sector, covering the issues of social and legal protection of military personnel, law enforcement and intelligence officers, veterans and members of their families [13].

Supervision over compliance with the legislation during the implementation of measures to protect critical infrastructure is carried out by the Verkhovna Rada of Ukraine in accordance with the procedure established by the Constitution of Ukraine. Relevant parliamentary committees, in particular the one that deals with national security and defense issues, as well as the committee whose competence includes the issues of cybersecurity of critical information infrastructure facilities, at their meetings consider the report of the authorized body on the results of an independent audit of the effectiveness of the critical infrastructure protection system. Based on the results of consideration of this report, the Verkhovna Rada Committee on National Security and Defense has the right to initiate the submission of relevant issues to the Parliament [14].

The right to exercise public supervision in the field of critical infrastructure protection is exercised by citizens of Ukraine through participation in public associations, through deputies of local councils, as well as directly through appeals to the Commissioner for Human Rights of the Verkhovna Rada of Ukraine or other state bodies. In addition, citizens can participate in the work of public councils under the bodies that form and implement state policy in this area, initiate an independent audit of their activities, as well as get access to the open part of reports on ensuring the protection of critical infrastructure facilities. Access to information in the field of critical infrastructure protection for the purpose of public supervision may be limited in accordance with the level of state secrets [14].

Scientist V. V. Bezega defines the essence of control in the general sense as the activity of authorized entities, which is carried out on the basis of legislation and consists in observing, identifying and fixing shortcomings in the work of controlled objects, as well as in preventing and preventing violations of the rule of law regime [9, p. 98].

M. V. Sitsinska refers to eight levels of public control in the system of democratic civilian control over the activities of competent state authorities in the field of security and defense: therapy, manipulation, informing, counseling, reconciliation, partnership, delegation of authority and direct public control. At the same time, the scientist notes that in Ukrainian conditions, public control is the highest level of public participation, which is implemented mainly "from below", on the basis of private initiative. It is an important form of democratic governance and a way of involving citizens in the exercise of civilian control over the

activities of the security and defense sector, as well as in the processes of managing society and the state [10, p. 115]. In addition, the author notes that the current state of civil society institutions in Ukraine only partially meets the tasks of effective democratic control over the processes of national security formation. Non-governmental organizations registered in the state have a limited influence on the development of state policy in the field of national security, and their practical activities are often used in the interests of individual political or business projects [11, p. 110].

Thus, the analysis of modern scientific thought and the practical state of functioning of the mechanisms of democratic civilian control in the sphere of national security of Ukraine makes it possible to identify promising components of the development of democratic civilian control in the field of public management of information security of critical infrastructure of Ukraine. It is advisable to consider these components as a multidimensional system that combines regulatory, institutional, organizational and social elements (Figure 1). In the future, we will briefly reveal their content.

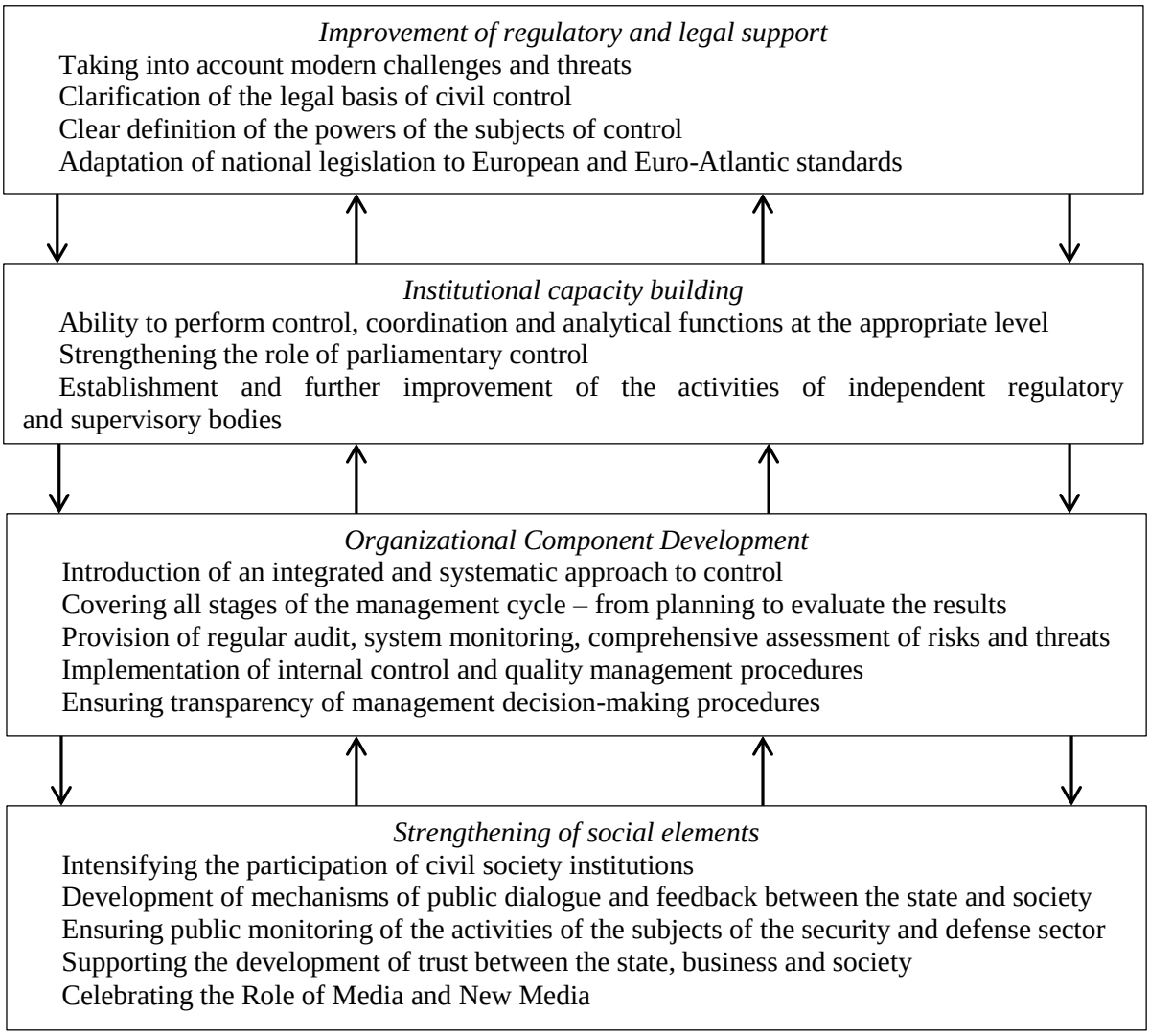

Figure 1 – Prospective components of the development of democratic civilian control in the field of public management of information security of critical infrastructure of Ukraine

First, the key direction is the improvement of regulatory and legal support, which should form a holistic and coordinated basis for the functioning of democratic civilian control in the field of information security of critical infrastructure. In this context, it is necessary not only to formally update the legislation, but also to systematically rethink it taking into account the current challenges and threats associated with digitalization, cyber risks and hybrid impacts. Special attention should be paid to the clarification of the legal foundations of civil control, which provides for the detailing of its principles, forms and mechanisms of implementation. It is important to ensure a clear definition of the powers of control entities, including public authorities, parliamentary structures, specialized bodies in the field of cybersecurity, as well as civil society institutions. This approach will help to avoid duplication of functions, increase the level of coordination and ensure effective interaction between all participants in the control process. The key strategic direction is the adaptation of national legislation to European and Euro-Atlantic standards. This involves implementing modern approaches to cyber defense, risk management, incident response, and ensuring the resilience of critical infrastructure. Such harmonization will ensure consistency of approaches to the protection of critical facilities, strengthen international cooperation and promote Ukraine's integration into the common security space.

Secondly, an important component is the development of institutional capacity, which is a necessary prerequisite for the effective functioning of the system of democratic civilian control in the field of information security of critical infrastructure. It is not only about the formal existence of the relevant institutions, but also about their real ability to carry out control, coordination and analytical functions at the appropriate level. In this context, it is of particular importance to strengthen the role of parliamentary control, which should ensure systematic oversight over the activities of security and defense sector bodies, the formation and implementation of state policy in the field of information security. This provides for the intensification of the activities of relevant committees, the improvement of the procedures for parliamentary hearings, the introduction of regular reporting by the relevant bodies, as well as an increase in the level of expert support of people's deputies. An important direction is the creation and further improvement of the activities of independent regulatory and supervisory bodies, which should have a sufficient level of autonomy, resource provision and professional competence. Such institutions should perform the functions of monitoring, auditing, assessing risks and responding to violations in the field of information security, while ensuring a balance between state interests and citizens' rights.

Thirdly, the organizational component provides for the introduction of an integrated and systematic approach to the implementation of control in the field of information security of critical infrastructure, which covers all stages of the management cycle – from planning to evaluation of results. Such an approach should be based on clearly defined procedures, standards and regulations that ensure the consistency of actions of all control entities and increase the effectiveness of management decisions. The key elements of this component are regular audit, system monitoring, as well as comprehensive assessment of risks and threats. Risk assessment, in turn, contributes to the identification of priority areas of protection and rational allocation of resources. Special attention should be paid to the introduction of internal control and quality management procedures, which will increase the discipline of implementation of decisions and ensure their compliance with the defined goals. At the same time, it is important to ensure transparency of management decision-making procedures, which will increase public trust and strengthen the accountability of authorities. At the same time, it is necessary to maintain an appropriate level of confidentiality of information, especially that related to security vulnerabilities or having limited access. The balance between openness and security of information is a key condition for the effective functioning of the control system.

Fourthly, the social elements of the development of democratic civilian control in the field of public management of information security of Ukraine's critical infrastructure are a significant component of ensuring its effectiveness, since they determine the level of citizen involvement, trust in state institutions and transparency of management processes. First of all, it is about intensifying the participation of civil society institutions, in particular public organizations, think tanks, professional associations and independent experts in the formation and evaluation of state policy in the field of information security. Their involvement in public consultations, expert discussions and the development of regulations contributes to improving the quality of management decisions and taking into account

public interests. An important direction is the development of mechanisms of public dialogue and feedback between the state and society. This includes the creation of open platforms for discussing cybersecurity issues, holding public hearings, publishing reports from authorities, as well as ensuring access to public information within the limits that do not harm national security. Such openness contributes to the accountability of authorities and the strengthening of democratic institutions.

A separate aspect is the provision of public monitoring of the activities of the subjects of the security and defense sector. This can be implemented through independent research, analytical reports, public examinations and the activities of supervisory boards. Such control increases transparency, helps to identify problematic aspects and stimulates the improvement of public policy. Equally important is the support for the development of trust between the state, business and society. In the field of information security, this is especially relevant, since a significant part of critical infrastructure is privately owned. Effective interaction between these actors, based on the principles of partnership, responsibility and information exchange, is a prerequisite for the sustainability of the entire system. In addition, it is advisable to emphasize the role of the mass media and new media, which perform the function of informing society, shaping public opinion and exercising public control. At the same time, it is important to ensure their accountability, compliance with journalism standards, and countering disinformation.

Summing up, it can be argued that the development of democratic civilian control in this area should be based on the principles of transparency, accountability, consistency and partnership between the state, business and civil society, which together will ensure an appropriate level of information security of Ukraine's critical infrastructure. Comprehensive improvement of regulatory and legal support creates the necessary prerequisites for the formation of an effective, transparent and accountable system of democratic civilian control, which is able to adequately respond to modern challenges in the field of information security of critical infrastructure in Ukraine. The development of institutional capacity provides for the comprehensive strengthening of organizational, functional and personnel capabilities of control entities, which generally ensures the effectiveness of democratic civilian control and increases the level of information security of the state. The organizational component is a practical mechanism for the implementation of democratic civilian control, ensuring its consistency, continuity and effectiveness in the field of information security of critical infrastructure. The social elements of the development of democratic civilian control are to ensure broad participation of citizens, openness and accountability of the authorities, the formation of a culture of cybersecurity and the strengthening of partnership between the state and society, which generally contributes to increasing the level of information security of Ukraine's critical infrastructure.

Conclusions

Based on what is stated in the article, it is possible to come to the following conclusions.

1. In the context of full-scale armed aggression and growing cyber threats, the issue of ensuring the information security of Ukraine's critical infrastructure is becoming strategically important, while at the same time actualizing the need to maintain a balance between security and compliance with democratic principles. Democratic civilian control is a key tool for ensuring transparency, accountability and legality of the activities of security and defense sector actors, as well as an important factor in preventing excessive concentration of power and violation of the rights and freedoms of citizens. Its importance is especially important in the context of hybrid threats, as it ensures a combination of the effectiveness of security policy with the principles of the rule of law.

2. The development of a system of democratic civilian control in the field of information security of critical infrastructure should be carried out on the basis of an integrated approach, which involves improving the regulatory framework, strengthening institutional capacity, introducing effective organizational control mechanisms and intensifying public participation. An important role in this is played by the harmonization of legislation with European and Euro-Atlantic standards, the development of public-private partnership and international cooperation, the expansion of the participation of civil society institutions, the development of mechanisms for public dialogue and ensuring an appropriate level of access to information, provided that security requirements are maintained.

3. The formation of an effective system of democratic civilian control in the field of public management of information security of Ukraine's critical infrastructure is a necessary prerequisite for strengthening national security and increasing the

resilience of the state. Such a system should be developed on the basis of consistency, openness, accountability and partnership between the state, society and the private sector. Its introduction will contribute to the proper protection of national interests and strengthening citizens' trust in state institutions, as well as support for Ukraine's European and Euro-Atlantic course.

Further scientific research will be aimed at substantiating innovative approaches to the formation of state information security policy for Ukraine's critical infrastructure.

References

1. Yaremenko O. I., Strakhnitskyi Ya. I. (2022). *Teoretychni pidkhody do vyznachennia definitsii krytychnoi infrastruktury yak obiektu derzhavnoho upravlinnia* [Theoretical approaches to defining the concept of critical infrastructure as an object of public administration]. *Publichne upravlinnia ta mytne administruvannia*, no. 1, pp. 76–82. DOI: https://doi.org/10.32836/2310-9653-2022-1.13 [in Ukrainian].

2. Melnyk D. S. (2022). *Zakhyst natsionalnoi krytychnoi informatsiinoi infrastruktury: aktualni problemy ta shliakhy yikh vyrishennia* [Protection of the national critical information infrastructure: current problems and ways to solve them]. *Administratyvne pravo i protses*, vol. 3, no. 38, pp. 5–16. DOI: https://doi.org/10.17721/2227-796X.2022.3.01 [in Ukrainian].

3. Telenyk S. S. (2021). *Administratyvno-pravove rehuliuvannia derzhavnoi systemy zakhystu krytychnoi infrastruktury Ukrainy* [Administrative and legal regulation of the state system of critical infrastructure protection in Ukraine]. Doctor's thesis. Zaporizhzhia, p. 467 [in Ukrainian].

4. Dovhan O. D. (2016). *Teoretyko-pravovi osnovy zabezpechennia informatsiinoi bezpeky Ukrainy* [Theoretical and legal foundations of ensuring information security of Ukraine]. Extended abstract of doctor's thesis. Kyiv, p. 46 [in Ukrainian].

5. Hordiienko S. H., Doronin I. M. (2024). *Informatsiino-pravovi aspekty zakhystu krytychnoi infrastruktury Ukrainy* [Information and legal aspects of critical infrastructure protection in Ukraine]. *Informatsiia i pravo*, vol. 3, no. 50, pp. 115–123. DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311678 [in Ukrainian].

6. Ilienko A. V., Teliushchenko V. A., Dubchak O. V. (2025). *Suchasni kiberzahrozy krytychnoi infrastruktury Ukrainy ta svitu* [Modern cyber threats to critical infrastructure of Ukraine and the world]. *Kiberbezpeka: osvita, nauka, tekhnika*, vol. 3, no. 27, pp. 150–164. DOI: https://doi.org/10.28925 /2663-4023.2023.27. 719 [in Ukrainian].

7. Trofimov O. S. (2025). *Vdoskonalennia polityky bezpeky informatsiinykh system obiektiv krytychnoi infrastruktury Ukrainy na osnovi kontseptsii ZERO TRUST* [Improvement of security policy of information systems of critical infrastructure objects based on the ZERO TRUST concept]. *Telekomunikatsiini ta informatsiini tekhnolohii*, vol. 3, no. 88, pp. 15–25. DOI: https://doi.org/10. 31673/2412-4338.2025. 038702 [in Ukrainian].

8. Baranovskyi O. I. (2025). *Krytychna infrastruktura: bezpekovyi vymir* [Critical infrastructure: security dimension]. *Acta Academiae Beregsasiensis. Economics*, vol. 1, no. 8, pp. 13–37. DOI: https://doi.org/10.58423 /2786-6742/ 2025-8-13-37 [in Ukrainian].

9. Bezeha V. V. (2020). *Poniattia ta protsedury zdiisnennia hromadskoho kontroliu za diialnistiu Natsionalnoi politsii yak subiekta sektoru bezpeky yi oborony* [Concept and procedures of public control over the activities of the National Police as a subject of the security and defense sector]. *Naukovyi visnyk publichnoho ta pryvatnoho prava*, no. 3, pp. 96–101. DOI: https://doi.org/10. 32844/2618-1258.2020.3.17 [in Ukrainian].

10. Sitsinska M. V. (2013). *Elementy hromadskoho kontroliu v systemi demokratychnoho tsyvilnoho kontroliu nad sektorom bezpeky i oborony* [Elements of public control in the system of democratic civilian control over the security and defense sector]. *Investytsii: praktyka ta dosvid*, no. 14, pp. 112–115. Retrieved from: http://www.investplan.com.ua/pdf/14_2013/ 28.pdf (accessed 15 March 2026) [in Ukrainian].

11. Sitsinska M. V. (2013). *Aktualni pytannia ratsionalnosti hromadskoho kontroliu za diialnistiu orhaniv derzhavnoi vlady u sferi bezpeky i oborony* [Current issues of rationality of public control over the activities of state authorities in the field of security and defense]. *Ekonomika ta derzhava*, no. 4, pp. 108–110. Retrieved from: http://nbuv.gov.ua/UJRN/ecde_2013_4_31 (accessed 15 March 2026) [in Ukrainian].

12. Chub A. V., Naidon Ye. M. (2025). *Demokratychnyi tsyvilnyi kontrol za diialnistiu systemy orhaniv sektoru bezpeky i oborony Ukrainy* [Democratic civilian control over the activities of the system of bodies of the security and defense sector of Ukraine]. *Analitychno-porivnialne pravoznavstvo*, vol. 1, no. 4, pp. 147–152. DOI:

https://doi.org/10.24144/2788-6018.2025.04. 1.23 [in Ukrainian].

13. *Zakon Ukrainy "Pro natsionalnu bezpeku" № 2469-VIII* [Law of Ukraine about the National Security activity no. 2469-VIII]. (2018, June 21). *Vidomosti Verkhovnoi Rady Ukrainy*. Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text (accessed 15 March 2026) [in Ukrainian].

14. *Zakon Ukrainy "Pro krytychnu infrastrukturu" № 1882-IX* [Law of Ukraine about the Critical Infrastructure activity no. 1882-IX]. (2021, November 16*). Vidomosti Verkhovnoi Rady Ukrainy*. Retrieved from: https://zakon.rada.gov.ua /laws/show/1882-20#Text (accessed 15 March 2026) [in Ukrainian].

The article was submitted to the editorial office 20.03.2026
Accepted for publication after peer review 17.04.2026
Publication date 29.05.2026

УДК 351.862.4

О. І. Урсол

РОЗВИТОК ДЕМОКРАТИЧНОГО ЦИВІЛЬНОГО КОНТРОЛЮ У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ КРИТИЧНО ВАЖЛИВОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Проведений аналіз засвідчує, що в умовах повномасштабної збройної агресії та зростання кіберзагроз питання забезпечення інформаційної безпеки критично важливої інфраструктури України набуває стратегічного значення, водночас актуалізуючи необхідність збереження балансу між безпекою та дотриманням демократичних принципів. Установлено, що наявні проблеми нормативно-правового регулювання, інституційної взаємодії та організаційного забезпечення знижують ефективність функціонування системи захисту критичної інфраструктури, що потребує їх комплексного вдосконалювання.

З'ясовано, що демократичний цивільний контроль є ключовим інструментом забезпечення прозорості, підзвітності та законності діяльності суб'єктів сектору безпеки і оборони, а також важливим чинником недопущення надмірної концентрації влади та порушення прав і свобод громадян. Його значення особливо зростає в умовах гібридних загроз, оскільки він забезпечує поєднання ефективності безпекової політики з принципами верховенства права.

Обґрунтовано думку, що розвиток системи демократичного цивільного контролю у сфері інформаційної безпеки критично важливої інфраструктури має здійснюватися на основі комплексного підходу, який передбачає вдосконалення нормативно-правової бази, зміцнення інституційної спроможності, запровадження ефективних організаційних механізмів контролю та активізацію суспільної участі. Важливу роль при цьому відіграють гармонізація законодавства з європейськими та євроатлантичними стандартами, а також розвиток державно-приватного партнерства та міжнародного співробітництва.

Суттєвим резервом підвищення ефективності контролю є розширення участі інститутів громадянського суспільства, розвиток механізмів публічного діалогу та забезпечення належного рівня доступу до інформації за умови збереження вимог безпеки. Водночас потребує подальшого вдосконалювання інституційна структура контролю і підвищення її реальної спроможності впливати на формування державної політики.

Висновлено, що формування ефективної системи демократичного цивільного контролю у сфері публічного управління інформаційною безпекою критично важливої інфраструктури України є необхідною передумовою зміцнення національної безпеки, підвищення стійкості держави та забезпечення її поступу в напрямі європейської та євроатлантичної інтеграції. Така система має базуватися на принципах системності, відкритості, підзвітності та партнерства, що в сукупності забезпечить належний рівень захисту національних інтересів і довіри суспільства до державних інституцій.

Ключові слова: *критична інфраструктура, публічне управління та адміністрування, демократичний цивільний контроль, сектор безпеки і оборони, кризові ситуації, державна безпека, захист об'єктів критичної інфраструктури.*

Ursol Oleksii – Postgraduate Student of the Department of Public Management and Administration, Leonid Yuzkov Khmelnytskyi University of Management and Law
https://orcid.org/0009-0006-9847-4694