UDC 351.862.4

O. Ursol

THEORETICAL FOUNDATIONS FOR THE FUNCTIONING AND DEVELOPMENT OF PUBLIC ADMINISTRATION IN THE FIELD OF INFORMATION SECURITY OF UKRAINE'S CRITICAL INFRASTRUCTURE

The author addresses the need to substantiate the theoretical foundations for the functioning and development of public administration in the sphere of information security of Ukraine's critical infrastructure. They establish that information security must be ensured through the involvement of all domestic stakeholders in the information relations sector. It should operate under conditions of effective cooperation between the state, civil society, the private sector, and individual citizens. The study identified that, at present, the regulatory and legal framework concerning the protection of critical infrastructure facilities in Ukraine remains underdeveloped. The research highlighted the continuing relevance of examining information security issues pertaining to the nation's critical infrastructure. It is demonstrated that ensuring the information security of Ukraine constitutes one of the most vital state functions in maintaining national safety.

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

Statement of the problem. Contemporary evolution of Ukrainian society is increasingly marked by the emergence of crisis situations that pose significant threats to national security. The convergence of global civilizations and other processes associated with globalization are invariably accompanied by war conflicts. That is evidenced by the numerous armed clashes and terrorist attacks taking place in recent years. Regrettably, Ukraine is not immune to these grave challenges. Amid ongoing military aggression by the russian federation, critical infrastructure facilities consistently become primary targets for hostile actions.

The war perils arising from the attack against Ukraine have imposed new requirements on public administration, particularly with regard to safeguarding critical facilities. The principal factors underlying the persistence of such threats include Ukraine's geopolitical position and the insufficient effectiveness of public authorities in preventing risks at crucial infrastructure sites.

Consequently, establishing the necessary conditions for the development of information security within Ukraine's critical infrastructure complex has become a fundamental task for official governance. Ensuring information reliability requires the involvement of all domestic actors as part of information relations and effective cooperation among the state, civil society, the private sector, and individual citizens. Such collaboration is essential for the successful advancement of the media domain and for the general protection of critical facilities against emerging threats.

Analysis of recent research and publications. Numerous distinguished Ukrainian scholars and practitioners have thoroughly examined the issues surrounding the functioning and development of public policy in the sphere of protection of critical infrastructure facilities in Ukraine. Notably, the criminological aspects of countering perpetrations against critical infrastructure sites have been explored by O. Batiuk, O. Kobzar, O. Komisarov, D. Pavlov, I. Yevtushenko, S. Kuznichenko, M. Puzyrov, and other researchers. In addition, the response of various components of the security and defense sector to the perils affecting strategic facilities protection has been addressed in the works of S. Bielai, V. Matsiuk, I. Volkov, S. Horielyshev, D. Pavlov, V. Yevsieiev, V. Pokaichuk, O. Cherkashyn, among others. Furthermore, the enhancement of state policy in the field of critical infrastructure security has been studied by D. Biriukov, O. Yermenchuk, S. Kondratov, V. Bukhariev, S. Gnatiuk, N. Seilova, V. Sydorenko, M. Domaratskyi, O. Sukhodolia, Y. Strahnitskyi, and others.

Overall, scholars have addressed a substantial range of problematic aspects related to the protection of critical infrastructure assets. However, the issue of public administration in the domain of information security for Ukraine's vitally important facilities at the national level has remained largely unexplored. This gap underscores the academic relevance of the present article.

The purpose of the article is to investigate the theoretical foundations for the functioning and development of public administration in the field of information security of Ukraine's critical infrastructure, as well as to identify adequate directions for its further improvement.

Summary of the main material. In the previous studies [1, 2], the author established that the current regulatory and legal framework for the protection of critical infrastructure in Ukraine remains underdeveloped. At present, the Law of Ukraine "On National Security of Ukraine" [3] and the Law of Ukraine "On Critical Infrastructure" [4] are in force.

According to the Law "On National Security" [3], homeland security is defined as the protection of state sovereignty, territorial integrity, the democratic constitutional order, and other national interests of Ukraine from real and potential threats. National interests encompass the vital benefits of the individual, society, and the state, the realization of which guarantees Ukraine's national sovereignty, its progressive democratic development, as well as safe living conditions and the well-being of its citizens. This law also introduces the concept of the "national system for the protection of critical infrastructure," defined as the aggregate of management bodies, forces, and means of central and local executive authorities, local self-regulation bodies, and important infrastructure operators responsible for shaping and/or implementing state policy in the area of strategic facilities protection [3].

The legislator [4] defines the security of critical facilities as a condition in which their functionality, operational continuity, recoverability, integrity, and resilience are ensured. The protection of crucial infrastructure comprises all types of activities conducted before or during the creation, operation, restoration, and reorganization of a critical facility, aimed at the timely identification, prevention, and neutralization of threats to the security of such assets, as well as the minimization and elimination of consequences in the event that such threats materialize [4].

The reviewed laws of Ukraine form the basis for the functioning of public administration in the sphere of information security for crucial infrastructure. To further explore the theoretical underpinnings of public administration development in the domain of information safety for Ukraine's critical infrastructure, it is advisable to conduct a more in-depth analysis of academic sources on the subject. The following section considers several of the most significant recent scientific contributions in the field.

Researchers S. Bielai and I. Lavrov, in their study [5], have drawn attention to the need for substantiating a comprehensive system for the protection of critical infrastructure facilities at the state level. They conducted an analysis of regulatory acts governing the powers of Ukraine's security and defense sector components, which are responsible for developing and implementing state policy around critical infrastructure coverage. The authors asserted the particularly significant role and place of the National Guard of Ukraine in safeguarding crucial facilities. They also outlined directions for further scientific inquiry into the protection of Ukraine's infrastructure. Their findings indicate that organizing critical asset security is a complex process involving not only preventive mechanisms but also coordination and management aspects. Effective operation of that system requires highly qualified specialists with extensive training, retraining, and practical experience [5].

The authors of article [6] identified the importance of examining the methodological foundations for investigating issues related to the protection of critical infrastructure. They conducted an expert survey to assess current challenges in this domain in Ukraine. Overall, the survey results indicate that ensuring the security of critical infrastructure facilities remains a pressing issue, demanding a comprehensive approach and concerted efforts from various entities and authorities, including the ongoing refinement of legislation and the legal framework in that sphere. Respondents noted the need to enhance personnel qualifications, ensure efficient management, and improve coordination between security and defense sector components. They also highlighted the importance of developing innovative technologies to raise the level of security, as well as the necessity for investment in advanced safety technologies and systems to guarantee the appropriate protection of vital infrastructure. In addition, the authors demonstrated the need to create models for responding to threats against critical facilities under various conditions, including special periods and peacetime. This approach requires systematic and flexible planning to address potential risks in any context. It is assumed that developing such models will increase the effectiveness of security measures and bolster readiness for a range of crisis scenarios [6].

Scholars O. Batiuk and I. Yevtushenko conducted a study [7] focused on the significance of forensic science in counteracting crimes targeting critical infrastructure facilities. They emphasized both the theoretical and practical value of forensic science and provided a definition for the mechanism of committing crimes at strategic sites. According to their perspective, the mechanism of a crime at a critical infrastructure facility should be understood as the process by which the offense is done, including the method employed and all actions undertaken by the perpetrator, which result in the formation of both material and immaterial traces that can be used for the detection and investigation of the crime [7].

Article [8] presents the findings of an investigation into the forensic and operational-combat support for countering terrorist and sabotage threats against critical infrastructure. The study highlights that forensic and operational-combat support for counteracting terrorist and sabotage threats is aimed at establishing the conditions necessary for creating an optimal structure for such countermeasures, defining its stages, and outlining specific actions of those involved. The authors conclude that, despite fundamental differences in the subject matter and the particular features of internal and external interactions at different levels, all aspects of criminalistic and service and fighting support for countering terrorist and sabotage perils to critical infrastructure share a dual purpose. That includes forming the legal, organizational, scientific-technical, personnel, and other prerequisites for law enforcement agencies to maintain constant readiness for uncovering and inspecting crimes through the use of forensic techniques, tools, and recommendations; and implementing these conditions in practice through professionally competent and tactically sound investigative activities in daily operations [8].

In his dissertation [9], M. Domaratskyi substantiated and developed the theoretical foundations and scientific-practical recommendations for improving public administration in the field of critical infrastructure security in Ukraine. He provided a constituent definition of vital facilities as an object of governance and described the mechanisms of state management for the protection of critical facilities. The author also characterized the national system for ensuring the security and coverage of strategic assets.

That work further analyses the experience of foreign countries in public administration of critical infrastructure, highlights the specific features of critical infrastructure governance in Ukraine, and evaluates the national regulatory and administrative support for managing crucial assets. The author improved the state mechanisms for ensuring security and enhancing the effectiveness of critical infrastructure protection. He identified key directions for the development of the public administration system dedicated to safeguarding crucial infrastructure and proposed approaches for refining state policy in this domain.

M. Domaratskyi argued that the practical implementation of public administration measures concerning strategic risks to critical infrastructure requires the use of a systemic-legal, political, informational, economic, and organizational-administrative toolkit within a comprehensive mechanism for higher management of vital infrastructure. Additionally, the researcher suggested ways to improve the state security policy on critical facilities protection in Ukraine. He developed a set of measures to implement the primary mechanisms and stages for introducing national policy in the field of security for automated management systems of strategic facilities [9].

Researcher Y. Strahnitskyi, in his dissertation [10], addressed the scientific challenge of synthesizing the theoretical and methodological features of contemporary state policy for critical infrastructure protection, as well as providing a theoretical rationale for doctrinal perspectives focusing on improving public administration mechanisms for safeguarding critical infrastructure and formulating relevant scientific and practical recommendations. For the first time, the scholar substantiated the scientific and methodological framework for the comprehensive application of mechanisms and procedures for developing and implementing strategies to maintain the protection level of crucial assets, considering the current geopolitical and military context, based on a cluster approach. He also introduced into scientific discourse the definition of "critical infrastructure resilience cluster," among other concepts [10].

In his academic article [11], D. Biriukov explored the role of the critical infrastructure protection concept within the national security framework of the EU. The author provided a brief overview of the stages involved in implementing this concept within the regulatory and legal documents of the European Union. He also characterized the main factors and trends that generate threats to critical objects in EU countries. D. Biriukov concluded that, due to its geographical position, Ukraine forms part of the pan-European energy and transport space. Consequently, Ukraine is de facto connected to the European infrastructure network. Given that reality creates opportunities for dialogue on critical facilities security between the competent authorities of Ukraine and those of its European neighbors [11].

Summing up the review of scientific literature addressing the functioning of public administration in the field of information safety for critical infrastructure, it is evident that the issue of information security for Ukraine's vital infrastructure remains highly relevant. Therefore, it is appropriate to further analyze the current condition of the conceptual and strategic foundations for the functioning and advancement of public administration in this area.

Ensuring information security for Ukraine stands as one of the most significant state functions in the context of safeguarding national safety. The current Information Security Strategy of Ukraine [12] defines the pressing challenges and threats to the country's national safety within the information domain. It also establishes the strategic goals and objectives aimed at countering such threats, protecting individuals' rights to information, and safeguarding personal data. The overarching aim of this strategy is to enhance Ukraine's capabilities in maintaining information independence for the state and its media space. It also seeks to support social and political stability, bolster national defense, and safeguard state security and territorial integrity, as well as the democratic constitutional order and the rights and freedoms of every citizen [12].

According to the Information Security Strategy [12], information threats refer to potentially or actually negative phenomena, trends, and factors of informational influence on individuals, society, and the state. Such perils are applied within the information domain with the aim of impeding or complicating the realisation of national interests and the preservation of Ukraine's national values. They may directly or indirectly harm the interests of the state, its national security, and defence. The main priorities for ensuring data safety in Ukraine are resilience and cooperation. Achieving them requires the fulfilment of a set of strategic objectives and tasks.

Strategic Goal 1 is to counter disinformation and information operations – primarily those conducted by the aggressor state – which are directed, among other aims, at undermining Ukraine's independence, overthrowing the constitutional order, violating state sovereignty and territorial integrity, promoting war, violence, and cruelty, inciting national, ethnic, racial, or religious hatred and hostility, perpetrating terrorist acts, and infringing on human rights and freedoms [12].

This highlights that counteracting disinformation and information operations, especially those originating from the attacker state and designed to facilitate terrorist activities, currently constitutes a highly relevant research priority. Moreover, the proliferation of cyber threats targeting critical infrastructure, as well as the ongoing development of tools for their implementation, necessitate the adaptation of both strategies and tactics for countering such threats. Timely detection of vulnerabilities and cyberattacks, rapid incident response, and the prompt dissemination of information about such incidents have become increasingly significant. These steps are essential to minimizing the potential damage caused by cyber threats to critical infrastructure.

Cyberspace, alongside other physical domains, has been recognized as one of the potential perils of military operations. There is a growing trend towards the creation of cyber forces, whose responsibilities include not only safeguarding critical infrastructure against cyberattacks but also conducting pre-emptive offensive operations in cyberspace. These operations involve disabling the adversary's vital assets by targeting and destroying the information systems that control such facilities.

At present, the regulatory framework for the cyber protection of critical infrastructure has been enhanced. The procedures for identifying vital assets and the general requirements for their cybersecurity have been established. Specialized cybersecurity and cyber defense centers (units) have been set up within the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Bank of Ukraine, the Ministry of Infrastructure of Ukraine, the Ministry of Defense of Ukraine, and the Armed Forces of Ukraine.

In agreement with the Cybersecurity Strategy of Ukraine [13], to achieve cyber resilience, Ukraine, in cooperation with private sector stakeholders, the academic community, and civil society, will strengthen national cyber preparedness and protection. This will be achieved through the development of a National Response Plan for crisis situations in cyberspace, which will set out mechanisms for responding to nationwide cyberattacks on critical infrastructure and outline measures for subsequent recovery; the implementation of a risk-based approach to cybersecurity measures for crucial infrastructure; the introduction of continuous assessments of the safety posture of critical facilities and state information resources for vulnerabilities; and the establishment of an information security audit system, primarily at crucial asset sites and other relevant objects.

According to the draft Concept of Information Security of Ukraine [14], information security is understood as the protection status of the vital interests of individuals, citizens, society, and the state. This guard prevents harm caused by incomplete, untimely, or unreliable dissemination of information; breaches of the integrity and availability of information; unauthorized circulation of restricted information; as well as negative information-psychological influences and the intentional infliction of adverse consequences using information technologies.

The primary objective of state security policy on the data sector is to safeguard information sovereignty, preserve the spiritual and cultural values of the Ukrainian people, support the development of national self-identity and civilizational unity, create an advanced information society and national information space within Ukraine, and facilitate its transformation into an information-driven state and a fully-fledged participant in the European and international community [14].

Having analyzed both current and future conceptual regulatory documents [12, 13, 14], it is important to emphasize that in the sphere of information security, special attention must be paid to the protection of individuals and citizens, society, and the state from information threats. Such threats include potentially or really adverse phenomena, tendencies, and factors of informational influence on individuals, society, and the state, which are used within the information sphere to obstruct or complicate the realization of national interests and the preservation of Ukraine's national values. These perils may directly or indirectly cause damage to state security interests, safety, and defense.

The draft Law of Ukraine "On the Principles of Information Security of Ukraine" [15] proposed a classification of threats within the information domain. For individuals and citizens, that encompasses the safeguarding of constitutional rights and freedoms regarding the collection, storage, use, and dissemination of information; the right to communicate in one's native language; the prevention of unauthorized interference with the content, processing, transmission, and use of personal data; and protection from the negative effects of information technologies and information-psychological impacts. Priorities for the society include the preservation and enhancement of the spiritual, cultural, and moral values of the Ukrainian people and citizens of all nationalities; the provision of information support for socio-political stability, interethnic and interfaith harmony, and the development of civil society. For the state, the focus lies on ensuring information sovereignty; preventing information aggression, expansion, and blockades by foreign countries, organizations, groups, or individuals; the formation and implementation of effective state policy in the information sphere by official authorities and civil society institutions; information-infrastructure support for socio-economic and scientific-technical development; the cultivation of a positive image of Ukraine; the establishment and advancement of an information society; and Ukraine's integration into the European and global information space [15].

It is entirely reasonable to agree with that position and to add that the main directions of state security policy regarding Ukraine's independence in the information sphere, which were defined by the Law of Ukraine "On the Fundamentals of National Security" [16] (repealed in 2018), remain relevant today. These streamlines include: ensuring Ukraine's information sovereignty; improving state regulation of the development of the information sector by creating legal and economic prerequisites; actively engaging mass media; guaranteeing the consistent observance of constitutional rights to freedom of speech and access to information; and undertaking comprehensive measures to protect the national information space and counter the monopolization of Ukraine's information sector, among others.

To summarize, it is possible to note that public authorities effective in the sphere of information security must guarantee the constitutional rights and freedoms of individuals and citizens in the information domain; defend information sovereignty, the constitutional order, and the territorial integrity of Ukraine; ensure legal and scientific-technical support for the establishment and development of Ukrainian information society; uphold universal and national values within the national information space, and preserve and develop the spiritual and cultural traditions of the Ukrainian people. They should also foster a domestic industry of high-technology information products, develop and implement advanced information technologies and software; and, by encouraging domestic producers, establish and update the national information infrastructure, as well as national information resources, products, and services. Furthermore, they must ensure the protection of personal data, restrict access to information where necessary, provide technical information security, and develop international cooperation on communication safety issues [1, 2].

Thus, the relevance of the research topic concerning the establishment of public administration in the field of information security for Ukraine's critical infrastructure, as well as the directions for further studies on this issue, are determined by the following factors:

– the prospect of governing bodies fulfilling their tasks in ensuring the information security of critical infrastructure facilities;

– the need to improve the organizational and legal foundations of public administration in data safety for Ukraine's crucial infrastructure;

– the divergence between current scientific approaches to building systems for protecting critical facilities in the EU and NATO countries compared to those in Ukraine;

– the insufficient development of theoretical and methodological principles regarding the functioning of public administration bodies and components of the security and defense sector in the area of protecting Ukraine's vital assets, specifically in relation to ensuring information security;

– and the practical significance of state mechanisms for safeguarding the data safety of critical infrastructure.

Conclusions

Based on the conducted analysis, the following outcomes can be drawn.

1. Under the conditions of ongoing armed hostility by russia, critical infrastructure facilities in Ukraine remain constant targets for the enemy state. Military threats resulting from that aggression impose new demands on public administration, especially in the domain of critical facilities security. Creating the necessary prerequisites for developing information safety within Ukraine's crucial infrastructure constitutes a key responsibility of public authorities. Ensuring information security requires the involvement of all domestic stakeholders in the data domain and effective collaboration between the state, civil society, the private sector, and individual citizens to foster the effective growth of the media environment and to jointly protect the country's crucial facilities from threats.

2. Currently, the regulatory framework for the protection of critical infrastructure in Ukraine remains underdeveloped. Existing Ukrainian legislation provides a basis for the functioning of government administration in the field of information security for critical infrastructure. Further study of the theoretical foundations for the development of public administration in this domain included a performed analysis of relevant scientific literature. The issue of studying information security for critical infrastructure, specifically the conceptual and strategic principles underpinning the operation and advancement of public administration in this field, remains highly relevant.

3. Safeguarding Ukraine's information security stands as one of the state's most vital functions in ensuring national safety. Countering disinformation and information operations – primarily those conducted by the aggressor state and aimed at enabling terrorist acts – has become a crucial area of research. Additionally, the proliferation of cyber threats to critical

infrastructure facilities and the evolution of tools used in such attacks necessitate changes in counterstrategy and tactics. Rapid detection of vulnerabilities and cyberattacks, as well as timely response and dissemination of information about them, have become increasingly significant in minimizing potential damage.

4. The analysis of current and prospective conceptual regulatory acts confirms that, within the sphere of information security, it is essential to ensure the protection of individuals, society, and the state from information threats. Such threats may be actual or potential negative phenomena, trends, or factors of information influence affecting individuals, society, and the state. These threats are utilized within the information environment to impede or complicate the realization of national interests and the preservation of Ukraine's national values, and may directly or indirectly harm state interests, national security, or defense capability.

Future scientific research will focus on exploring the methodological foundations for the functioning and development of public administration in the field of information security for Ukraine's critical infrastructure.

References

1. Ursol O. I. (2025). *Aktualizatsiia doslidzhennia stanovlennia publichnoho upravlinnia u sferi informatsiinoi bezpeky krytychno-vazhlyvoi infrastruktury Ukrainy* [Actualization of the study of the formation of public administration in the field of information security of critical infrastructure of Ukraine]. Proceedings of the 4th International scientific and practical conference *"Publichne upravlinnia v Ukraini: vyklyky sohodennia ta hlobalni imperatyvy"* (Ukraina, Khmelnytskyi, February 7, 2025). Khmelnytskyi : KhUUP imeni Leonida Yuzkova, pp. 138–140 [in Ukrainian].

2. Ursol O. I. (2025). *Do pytannia rozvytku kontseptualnykh zasad zabezpechennia informatsiinoi bezpeky Ukrainy* [On the development of conceptual foundations for ensuring information security of Ukraine]. Absract of Papers *"Vseukrainskoi naukovo-praktychnoi onlain-konferentsii zdobuvachiv vyshchoi osvity i molodykh uchenykh, prysviachenoi Dniu nauky"* (Zhytomyr, May 12–17, 2025). Zhytomyr : Zhytomyrska politekhnika, pp. 748–749 [in Ukrainian].

3. *Zakon Ukrainy "Pro natsionalnu bezpeku Ukrainy" № 31* [The Law of Ukraine about national security of Ukraine activity no. 31]. (2018, June 21). Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text (accessed 7 May 2025) [in Ukrainian].

4. *Zakon Ukrainy "Pro krytychnu infrastrukturu" № 1882-IX* [The Law of Ukraine about critical infrastructure activity no. 1882-IX]. (2021, November 16). Retrieved from: https://zakon.rada.gov.ua/laws/show/1882-20 (accessed 7 May 2025) [in Ukrainian].

5. Lavrov I. S., Bielai S. V. (2023). *Teoretychni zasady formuvannia systemy zakhystu obiektiv krytychnoi infrastruktury Ukrainy* [Theoretical principles of formation of the system of protection of critical infrastructure of Ukraine]. *Chest i zakon,* no. 2 (85), pp. 5−11 [in Ukrainian].

6. Lavrov I. S., Bielai S. V. (2024). *Metodolohichni zasady vyvchennia problem zakhystu obiektiv krytychnoi infrastruktury* [Methodological principles of studying the problems of critical infrastructure protection]. *Bezpeka derzhavy,* no. 1 (3), pp. 75−82 [in Ukrainian].

7. Batiuk O. V., Yevtushenko I. Ye. (2022). *Znachennia nauky kryminalistyky u zabezpechenni protydii zlochynam na obiektakh krytychnoi infrastruktury* [The importance of the science of criminalistics in ensuring the counteraction to crimes at critical infrastructure facilities]. *Chest i zakon,* no. 2 (81), pp. 42−47 [in Ukrainian].

8. Komisarov O. H., Batiuk O. V., Pavlov S. P. (2021). *Kryminalistychne ta sluzhbovo-boiove zabezpechennia protydii terorystychnii ta dyversiinii zahrozam na obiektakh krytychnoi infrastruktury* [Criminalistics and service-combat support for countering terrorist and sabotage threats at critical infrastructure facilities]. *Chest i zakon,* no. 4 (79), pp. 33−39 [in Ukrainian].

9. Domaratskyi M. B. (2022). *Derzhavne upravlinnia zabezpechenniam bezpeky krytychnoi infrastruktury v Ukraini* [Public administration of critical infrastructure security in Ukraine]. Candidate′s thesis. Kharkiv : National University of Civil Defense of Ukraine, p. 259 [in Ukrainian].

10. Strakhnitskyi Ya. O. (2024). *Osoblyvosti formuvannia ta realizatsii derzhavnoi polityky u sferi zakhystu krytychnoi infrastruktury* : PhD thesis. Vinnytsia : Vinnytskyi derzhavnui pedahohichnyi universytet, p. 312 [in Ukrainian].

11. Biriukov D. (2019). *Kontseptsiia zakhystu krytychnoi infrastruktury yak element*

zahalnoievropeiskoi bezpekovoi polityky [The Concept of critical infrastructure protection as an element of the common european security policy]. *Naukovi zapysky*, no. 6 (68), pp. 106−115 [in Ukrainian].

12. *Ukaz Prezydenta Ukrainy "Pro Stratehiiu informatsiinoi bezpeky" № 685/2021* [Decree of the President of Ukraine about information security strategy activity no. 685/2021]. (2021, December 28). Retrieved from: https://surl.li/yefbkh (accessed 7 May 2025) [in Ukrainian].

13. *Ukaz Prezydenta Ukrainy "Pro Stratehiiu kiberbezpeky Ukrainy" № 447/2021* [Decree of the President of Ukraine about cybersecurity Strategy of Ukraine activity no. 447/2021]. (2021, August 26). Retrieved from: https://surl.li/qnputy (accessed 1 January 2025) [in Ukrainian].

14. *Proekt "Kontseptsiia informatsiinoi bezpeky Ukrainy"* [Draft Concept of Information Security of Ukraine]. (2014, June 9). Retrieved from: https://www.osce.org/files/f/documents/0/2/175056.pdf (accessed 7 May 2025) [in Ukrainian].

15. *Proekt Zakonu Ukrainy "Pro zasady informatsiinoi bezpeky Ukrainy" № 4949* [Draft Law of Ukraine about principles of information security of Ukraine activity no. 4949]. (2014, May 28). Retrieved from: https://surl.li/seqjoz (accessed 7 May 2025) [in Ukrainian].

16. *Zakon Ukrainy "Pro osnovy natsionalnoi bezpeky" № 964-IV* [The Law of Ukraine about principles of national security activity no. 964-IV]. (2003, June 19). Retrieved from: https://zakon.rada.gov.ua/laws/show/964-15#Text (accessed 7 May 2025) [in Ukrainian].

The article was submitted to the editorial office on 10 May 2025

УДК 351.862.4

О. І. Урсол

ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ І РОЗВИТКУ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРИТИЧНО ВАЖЛИВОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Актуалізовано питання обґрунтування теоретичних основ функціонування і розвитку публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України. Установлено, що інформаційна безпека має забезпечуватися з участю всіх внутрішніх суб'єктів інформаційних відносин і за умов ефективної взаємодії держави з громадянським суспільством, а також приватним сектором та окремими громадянами в інтересах ефективного розвитку інформаційної сфери і спільного захисту від загроз об'єктам критичної інфраструктури держави. Визначено, що на цей час нормативно-правова база щодо захисту об'єктів критичної інфраструктури в Україні є слаборозвиненою. Зазначено, що актуальним залишається питання дослідження інформаційної безпеки критично важливої інфраструктури України в частині концептуальних і стратегічних засад функціонування і розвитку публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України. Доведено, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави щодо забезпечення національної безпеки. Протидія дезінформації та інформаційним операціям, насамперед держави-агресора, що спрямовані на вчинення терористичних актів, є наразі вкрай актуальним напрямом дослідження. Крім того, поширення кіберзагроз на об'єкти критичної інфраструктури та вдосконалення інструментарію їх реалізації зумовлюють необхідність зміни стратегії і тактики протидії їм. Набувають значущості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди. Визначено подальші перспективні напрями дослідження.

Ключові слова: *критична інфраструктура, публічне управління та адміністрування, 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