UDC 351.861.3:004.056

D. Prokopovych-Tkachenko

V. Zvieriev

I. Kozachenko

THE MODERN CHALLENGE OF THE DIGITAL WORLD AND THE ROLE OF THE NATIONAL CYBERSECURITY COORDINATION CENTER IN ENSURING THE INFORMATION SECURITY OF THE STATE

The role of the National Cybersecurity Coordination Center in the formation of the state defense system is analyzed. Its effectiveness in countering such modern threats as cyberattacks and information aggression is assessed. The key functions of the National Cybersecurity Coordination Center are also determined: threat monitoring, coordination of cybersecurity entities, and implementation of the latest technologies.

Directions for improving the national cybersecurity system and ensuring the digital resilience of the state are proposed. The need to harmonize legislation with international standards is emphasized. Attention is focused on the importance of cooperation between state and private institutions in the field of cyber defense.

Keywords: *information, security, cyber threats, monitoring, infrastructure, technologies, standards.*

Statement of the problem. The rapid development of digital technologies is accompanied by the emergence of new threats that affect the information security of the state. In particular, the increase in the number and complexity of cyberattacks creates serious challenges for the protection of critical information infrastructure [1]. The use of information and communication technologies in public administration, the financial sector and defense significantly increases the risks of unauthorized access to information, data manipulation and disruption of the functioning of state systems [2]. In this regard, there is a need to develop comprehensive cyber defense strategies that provide for effective monitoring of threats, coordination between cybersecurity entities and the implementation of modern protection technologies [3]. The National Cybersecurity Coordination Center (NCCC) plays a key role in ensuring the information security of Ukraine. It coordinates measures aimed at protecting the state cyber infrastructure, countering cyberattacks and harmonizing national standards with international requirements [4]. However, the increasing complexity of cyber threats requires continuous improvement of methods for analyzing, predicting, and neutralizing potential attacks. Technologies such as artificial intelligence, big data analysis, and automated cyber defense systems are becoming important tools in the fight against digital threats [5]. However, the effectiveness of cybersecurity measures depends not only on technological solutions, but also on regulatory support, international cooperation, and human resources [6].

Analysis of recent research and publications. The issues of information security and cyber protection of state structures are the subject of numerous scientific studies. A significant number of works have analyzed modern cyber threats, assessed the effectiveness of countermeasures, and developed strategic approaches to ensuring information security.

M. Hutsaliuk emphasizes the increasing role of state bodies in creating mechanisms for the prompt detection and neutralization of threats [3]. In his opinion, the development of information and communication technologies significantly increases the vulnerability of state structures to cyber attacks, therefore, it is necessary to constantly improve the national cyber protection system.

The issue of integrating international experience into the sphere of information security of Ukraine is considered by E. Zakharov, noting that cooperation with such international organizations as NATO and

the EU contributes to increasing the effectiveness of cyber protection through the adaptation of leading world practices to national realities [4].

An important aspect of cybersecurity is I. Losiev considers the use of artificial intelligence and big data analysis to predict threats [5]. In his study, he substantiates that the use of automated monitoring systems allows to significantly reduce the response time to incidents and increase the overall effectiveness of cyber protection of state structures.

At the same time, a number of works emphasize the need to improve the regulatory framework in the field of cybersecurity. Thus, according to O. Nesterenko [6], the rapid development of digital technologies requires regular updating of legislation to effectively counter new threats.

Thus, we conclude that one of the key challenges in the field of cybersecurity is the need to increase the level of coordination between state bodies, expand international cooperation and introduce innovative technologies to protect critical information infrastructure. In this context, the activities of the National Cybersecurity Coordination Center are of strategic importance for ensuring the information security of the state.

The purpose of the article is a comprehensive analysis of the role of the National Cybersecurity Coordination Center in ensuring the information security of the state in the context of modern digital challenges, as well as a study of its functions and tasks regarding coordination between state bodies, the private sector and international partners.

Particular attention is paid to the issues of monitoring and analysis of cyber threats, the development of the regulatory framework, the introduction of modern cyber defense technologies, in particular artificial intelligence and big data analysis for predicting attacks [2]. The impact of international experience and cooperation strategies of Ukraine with the EU and NATO in the field of cybersecurity is separately considered [3].

The results of the study make it possible to formulate practical recommendations for improving cyber defense mechanisms, in particular in terms of strengthening coordination between cybersecurity entities, strengthening the technical capabilities of the NCCC, and adapting international standards to national practice [4].

Summary of the main material. The study of the functioning of the National Cybersecurity Coordination Center as the main element of state information security management was carried out on the basis of an interdisciplinary approach, including methods of system analysis, mathematical modeling, big data processing and machine learning.

To assess the effectiveness of the NCCC, the system analysis method was used, which allows us to consider the Center as part of a complex cybersecurity infrastructure that interacts with government agencies, the private sector and international partners. The methodology for modeling the interaction of cybersecurity entities was used to analyze the impact of the Center on the overall stability of the national information infrastructure. Artificial intelligence and machine learning methods are used in cyber threat modeling and attack forecasting, which allows us to assess current trends and predict the development of threats in the digital space. Cluster analysis and deep learning algorithms were used to identify patterns in cyber incidents. The vulnerability assessment of critical information infrastructure was carried out using mathematical modeling methods, in particular, building attack models, and scenario analysis, which makes it possible to develop adaptive response mechanisms. Probabilistic risk assessment models were used to analyze potential threats in real time. When assessing information interaction between the NCCC and other cybersecurity entities, network analysis methods were used to identify key nodes of information exchange and assess the effectiveness of coordination mechanisms. An analysis of the data flow between state structures, private companies and international partners was conducted to identify possible points of vulnerability. The assessment of the compliance of the legislative framework with international standards was carried out using comparative analysis methods, which made it possible to identify discrepancies between the current regulatory legal acts of Ukraine and the recommendations of international organizations such as the EU and NATO. The results of the study are based on an analysis of open sources, including reports from international organizations, scientific publications, analytical materials, and official documents from government agencies, which ensured the objectivity and scientific validity of the conclusions.

The key functions of the National Cybersecurity Coordination Center are monitoring cyber threats, developing protection strategies, and integrating modern technologies such as artificial intelligence and big data analysis [3]. Due to this, the NCCC plays a leading role in building a sustainable

cybersecurity ecosystem that is able to effectively respond to modern challenges, predict potential threats, and coordinate interagency interaction [4].

Particular attention is paid to the implementation of adaptive management mechanisms that allow the system to quickly respond to changes in the external environment, minimizing risks to the state [5]. In this context, harmonization of the regulatory framework with international standards also plays a crucial role in increasing the effectiveness of cyber defense measures [6].

Thus, the NCCC acts not only as the main coordinating body, but also as an integration element that ensures the consistency of actions of all entities of the information security system. Its activities are aimed at strengthening the state's resilience to cyberattacks, forming a secure information environment, and creating a strategically oriented model of cyber defense [7].

In the modern digital world, the rapid development of information and communication technologies creates new opportunities for state, economic and social development, while at the same time being accompanied by numerous challenges and threats to information security. Protection of critical information infrastructure, countering cyberattacks and information aggression have become key areas of ensuring national security. The complex information security system of the state is based on the integration of various elements (technologies, processes, human resources and infrastructure) that interact in a single ecosystem. In this context, the definition of the role of the National Cybersecurity Coordination Center as the main link in the complex information security system of the state becomes particularly relevant [1]. Let us consider its main functions. A deep understanding of these functions is the basis for analyzing the effectiveness and prospects for further development of the cybersecurity system of Ukraine [2].

The National Cybersecurity Coordination Center also performs a number of important functions that ensure the integration and coherence of actions of cybersecurity entities aimed at protecting the state's information space. One of the key functions is to constantly monitor cyber threats: identifying potential attacks, analyzing malicious software, and assessing the level of risks for the state information infrastructure [3]. The center provides 24-hour monitoring of cyberspace, using advanced big data analysis and artificial intelligence technologies for the rapid detection of threats [5]. Thanks to this, the NCCC can predict the development of attacks and implement protective measures in a timely manner.

The National Cybersecurity Coordination Center plays a leading role in protecting the critical information infrastructure of the state. Security standards are developed, systems are tested for vulnerabilities, and modern protective mechanisms are implemented [4]. Particular attention is paid to protecting energy, financial, transport, and communication systems, which are the objects of the most powerful cyberattacks [3]. In its activities, the Center is also based on international experience and standards, which contributes to increasing the level of infrastructure security [6]. One of the main tasks of the NCCC is to ensure coordination between government agencies, the private sector, academic institutions, and international partners. The Center coordinates the actions of various cybersecurity entities to effectively exchange information on threats, avoid duplication of functions, and increase the effectiveness of joint activities [1]. Cooperation with international organizations (NATO and the EU) is especially important, which allows Ukraine to adapt best practices and technologies.

The NCCC is actively engaged in analyzing current threats and forecasting their development. To do this, the Center uses big data analysis tools, artificial intelligence, and machine learning [5]. This makes it possible not only to assess current trends in the field of cyber threats, but also to create models for predicting possible attacks in the future. Such tools are important for strategic planning and determining priorities in the field of cybersecurity [7].

Within the framework of modeling the state's information security as a complex technogenic system, it is proposed to consider the National Cybersecurity Coordination Center as the main management element that affects all components of the system. The NCCC acts as an integrator and regulator that ensures coordination between the components of the system, maintaining its functional integrity and adaptability to external and internal threats. In the context of technical infrastructure, the NCCC must ensure constant monitoring of all its elements: services, servers, communication networks and protection systems, including. The center implements mechanisms for automatically detecting vulnerabilities and updating protective equipment, which allows minimizing risks associated with incorrect settings or lack of updates. For this purpose, such modern

technologies as artificial intelligence and big data analysis are actively used. In organizational processes, the NCCC plays the role of a strategic coordinator, ensuring consistency of approaches to risk management, development of security policies and incident response planning. The Center implements training programs to improve the competence of personnel responsible for information security and monitors compliance with security standards in all sectors. The NCCC pays special attention to the human factor, as personnel are an important element in the information security system. The Center implements standards of safe behavior, training programs, and mechanisms for operational user support. Measures are also taken to prevent internal threats associated with the activities of insiders or attackers. Thus, the NCCC plays a critically important role in ensuring interaction between all elements of the state's information security system, creating conditions for its functional stability and effective response to modern challenges.

Figure 1 shows the structure of the National Cybersecurity Coordination Center as the main management element in the complex model of state information security.

The National Cybersecurity Coordination Center is located at the center of the system and affects all its components, ensuring coordination, monitoring and risk management. The technical infrastructure (servers, communication networks and protection systems) is subject to constant monitoring by the NCCC. The center ensures the identification of vulnerabilities, the introduction of modern technologies and control over the stability of technical protection. Organizational processes covering risk management, security policy formation and incident response planning are coordinated by the NCCC to ensure the integration of standards and consistency of actions between all cybersecurity entities. The human factor is an important component covering personnel training, security support and monitoring of user actions. The NCCC ensures the implementation of training programs, standards of conduct and minimization of risks associated with human errors. Information resources such as critical data, communication channels and classified information are protected through constant control by the NCCC, which ensures their preservation and inaccessibility to attackers. External threats, including cyberattacks, geopolitical risks, and environmental challenges, are analyzed and forecasted, and the NCCC organizes countermeasures against these threats. Thus, the NCCC plays a key role in forming an integrated information protection system, ensuring its adaptability and resilience to modern challenges.

The development of a technological base to counter post-quantum threats is one of the key areas of improvement for the National Cybersecurity Coordination Center. Given the potential danger posed by post-quantum computing, the NCCC must adapt existing security systems to new challenges. This involves the implementation of cryptographic algorithms that are resistant to quantum attacks, which will allow protecting critical data even if traditional encryption methods are broken. Quantum random number generators that increase the reliability of encryption keys also need to be integrated.

As part of the development of self-organizing and adaptive mechanisms, the NCCC must implement systems for automatic monitoring and response to cyber threats based on artificial intelligence and machine learning technologies. Thanks to this, the Center will be able not only to promptly detect and neutralize threats, but also to adapt existing security policies to changes in the digital environment. An important component is the creation of decentralized security networks based on blockchain technologies, which ensure the reliability and resilience of systems to external influences.

The Center should also intensify cooperation with international partners to exchange experience in countering post-quantum threats and integrating the best global practices into the national cybersecurity system. The legislative framework in the field of information security needs to be improved, given the prospects for the development of quantum technologies and the need to integrate international standards into national practice. This involves the creation of regulatory acts aimed at protecting critical information infrastructure from new threats, as well as ensuring support for scientific research in the field of post-quantum cryptography and quantum computing. Therefore, the development of the NCCC as a key element of the state's information security should be aimed at creating an integrated system capable not only of confronting modern challenges, but also of adapting to future threats in the post-quantum world.

The diagram (Figure 2) models the main processes of implementing the National Cybersecurity Coordination Center as the main element of the state cyber defense system.

Monitoring of cyber threats is carried out by analyzing network traffic, detecting anomalies using artificial intelligence and predicting potential threats. Protection of critical infrastructure is ensured by security audits, vulnerability testing, automatic protection updates and integration of blockchain technologies.

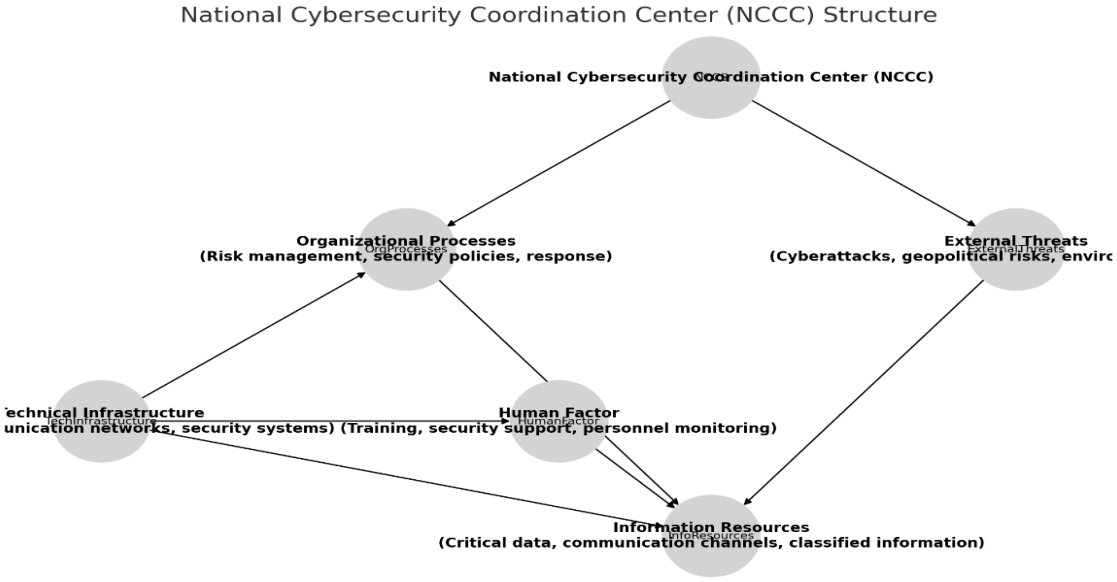

Figure 1 – NCCC structure and key elements

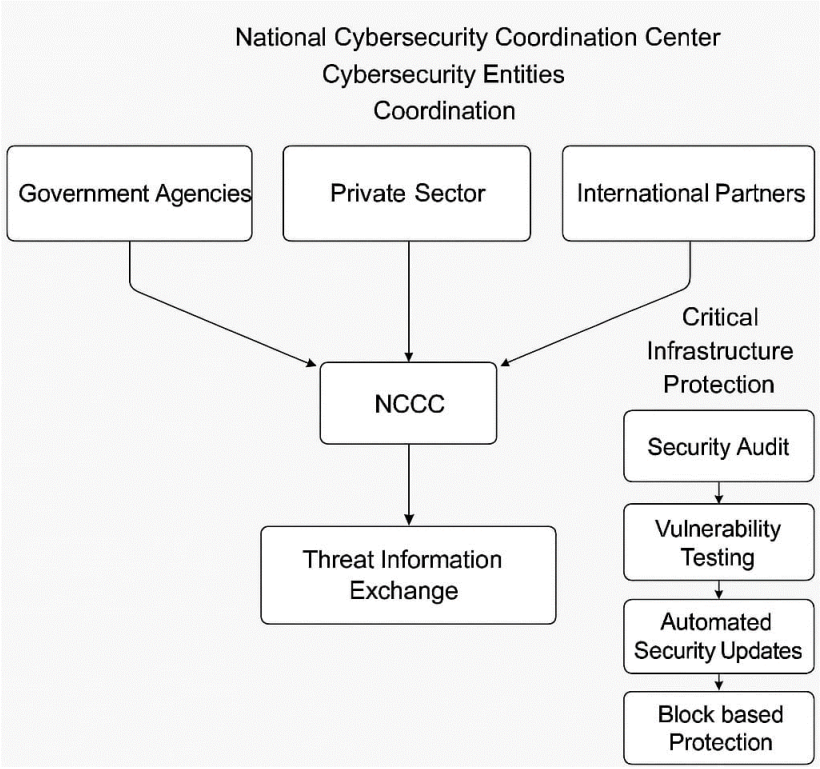

Figure 2 – NCCC Implementation Model

Coordination of cybersecurity entities consists in ensuring interaction between state bodies, the private sector and international partners to exchange information about threats. Development of human resources involves the creation of training programs, certification of specialists, advanced training and the formation of an expert environment. Integration of post-quantum technologies includes the development of cryptographic algorithms resistant to quantum attacks, quantum random number generators and decentralized security networks. The scheme reflects the relationship between these components and demonstrates how the National Cybersecurity Coordination Center performs the functions of monitoring, analyzing, coordinating and protecting the state's information infrastructure.

Thus, the National Cybersecurity Coordination Center is the main element of the state's cybersecurity system, which ensures threat monitoring, protection of critical infrastructure, coordination of inter-sectoral interaction, and forecasting of future challenges [1, 2]. Its activities contribute to the formation of a secure digital environment that meets modern challenges.

Conclusions

The National Cybersecurity Coordination Center is a key element of the national cybersecurity system, ensuring coordination between government agencies, the private sector and international partners. An analysis of current trends in the field of information security indicates the need to improve mechanisms for monitoring cyber threats, integrate advanced technologies and develop effective strategies for responding to cyberattacks. The introduction of artificial intelligence and big data analysis allows us to significantly increase the level of cyber defense, contributing to proactive threat detection and prompt decision-making. Expanding the powers of the National Cybersecurity Coordination Center in the field of protecting critical information infrastructure requires the integration of post-quantum technologies and the development of new cryptographic methods resistant to attacks by quantum computers. The use of quantum random number generators and decentralized security systems based on blockchain are promising areas for strengthening the state's information defense. At the same time, the implementation of these technologies requires significant financial investments and the creation of an appropriate regulatory framework that will regulate their use.

One of the main challenges in the development of the National Cybersecurity Coordination Center remains ensuring effective interaction between all cybersecurity actors. The latest approach involves creating a centralized platform for exchanging information about cyber threats, which will ensure a prompt response to potential attacks and prevent their negative consequences. Coordination between the public sector, business and scientific institutions plays a crucial role in building a sustainable cyber ecosystem.

Training personnel in the field of cybersecurity requires special attention, since the shortage of highly qualified specialists is one of the key factors limiting the development of an effective protection system. The implementation of specialized educational programs, certification of experts and creation of conditions for continuous professional development are considered necessary.

Thus, the National Cybersecurity Coordination Center plays a leading role in ensuring the information security of the state, but its further development requires a comprehensive approach. This includes technological innovations, improving regulatory frameworks, expanding international cooperation, and strengthening human resources. Integration of modern threat analysis methods, automation of response processes, and adaptation to future challenges such as post-quantum threats will allow Ukraine to create an effective and sustainable cyber defense system capable of countering modern threats in the digital world.

References

1. Bulashenko A., Brui M. (2010). *Informatsiina bezpeka* [Information security]. Proceedings of the *"Naukovo-metodychna konferentsiia vykladachiv, spivrobitnykiv i studentiv"* (Sumy, April 27, 2010). Sumy : SumDU, part 2, pp. 13–16. Retrieved from: https://surl.lu/zflugg (accessed 8 February 2025) [in Ukrainian].

2. Potapenko O. K. (2011). *Derzhavna informatsiina polityka ta bezpeka* [State information policy and security]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Seriia: filosofiia, politolohiia*, vol. 102, pp. 48–51 [in Ukrainian].

3. Hutsaliuk M. (2005). *Informatsiina bezpeka u suchasnomu suspilstvi* [Information security in

modern society]. *Pravo Ukrainy*, no. 7, pp. 71–74 [in Ukrainian].

4. Zakharov Ye. (2013). *Informatsiina bezpeka: shcho zakhyshchaiemo?* [Information security: what do we protect?]. *Svoboda vyslovliuvan i pryvatnist*, no. 4, pp. 3–6 [in Ukrainian].

5. Losiev I. (2014). *Informatsiina bezpeka: yak ukripyty* [Information security: how to strengthen]. *Den*, no. 82-83, p. 19 [in Ukrainian].

6. Nesterenko O. (2011). *Svoboda informatsii chy informatsiina bezpeka?* [Freedom of information or information security?]. *Svoboda vyslovliuvan i pryvatnist*, no. 1, pp. 3–9 [in Ukrainian].

7. Althobaiti O. S., Dohler M. (2020). Cybersecurity Challenges Associated With the Internet of Things in a Postquantum World. *IEEE Access*, vol. 8. DOI: 10.1109/ACCESS.2020.3019345 [in English].

8. Batechko O., Tsymbalenko N. V. (2016). *Informatsiina bezpeka pidpryiemstva* [Enterprise information security]. Proceedings of XV All-Ukrainian scientific conference of young scientists and students *"Naukovi rozrobky molodi na suchasnomu etapi"* (Ukraine, Kyiv, 28–29 April 2016). Kyiv : KNUTD. Retrieved from: https://surl.li/vrykvu (accessed 9 February 2025) [in Ukrainian].

9. Administratsiia (2023). *Natsionalnyi klaster kiberbezpeky* [National cybersecurity cluster]. Retrieved from: https://surl.li/qmqkwt (accessed 9 February 2025) [in Ukrainian].

10. Hlushkov V. (2010). *Informatsiina bezpeka (sotsialno-pravovi aspekty)* [Information security (social and legal aspects)]. *Pravo Ukrainy*, no. 9, pp. 311–313 [in Ukrainian].

11. Kisilevych-Chornoivan O. M. (2009). *Informatsiina bezpeka ta mizhnarodna informatsiina bezpeka: problema vyznachennia poniat* [Information security and international information security: problem of defining concepts]. *Yurysprudentsiia: teoriia i praktyka*, no. 8 (58), pp. 11–18 [in Ukrainian].

12. *Ukaz Prezydenta Ukrainy "Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky" № 242/2016* [Decree of the President of Ukraine "On the National Cybersecurity Coordination Center" activity no. 242/2016]. (2016, June 7). Retrieved from: https://surl.li/dyvbwc (accessed 9 February 2025) [in Ukrainian].

13. Zawoad S., Hasan R. (2012). Proof of past data possession in Cloud Forensics. Proceedings of International Conference on Cyber Security (USA, New York, December 14–16, 2012). Retrieved from: https://arxiv.org/abs/1211.4328 (accessed 10 February 2025) [in English].

14. Weber R. (2010). Internet of Things – New Security and Privacy Challenges. *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30. DOI: 10.1016/j.clsr.2009.09.008 [in English].

15. Solovii H. R. (2006). *Mizhnarodna informatsiina bezpeka: polskyi dosvid* [International information security: Polish experience]. *Aktualni problemy mizhnarodnykh vidnosyn*, no. 65, part 1, pp. 45–47 [in Ukrainian].

16. Shopina I. M. (2023). *Informatsiina bezpeka tsyfrovoi transformatsii* [Information security of digital transformation]. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav. Seriia: yurydychna*, vol. 1, pp. 28–35. DOI: 10.32782/2311-8040/2023-1-4 [in Ukrainian].

17. Conti M., Dehghantanha A., Franke K., Watson S. (2018). Internet of Things Security and Forensics: Challenges and Opportunities. *Future Generation Computer Systems*, vol. 78, pp. 544–546. DOI: 10.1016/j.future.2017.09.007 [in English].

18. *Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" № 2163-19* [Law of Ukraine On the basic principles of cybersecurity of Ukraine activity no. 2163-19]. Retrieved from: https://surl.li/enchzc (accessed 8 February 2025) [in Ukrainian].

19. Marakova I. I., Syropiatov O. A. (2006). *Informatsiina bezpeka kompleksnykh system zviazku* [Information security of complex communication systems]. *Ukrainian Information Security Research Journal*, vol. 8, no. 4 (31). Retrieved from: https://surl.li/qmopwp (accessed 11 February 2025) [in Ukrainian].

20. Subbot A. (2015). *Informatsiina bezpeka suspilstva* [Information security of society]. *Viche*, no. 8 (388), pp. 29–31 [in Ukrainian].

21. Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A. (2015). Security, Privacy and Trust in Internet of Things: *The Road Ahead. Computer Networks*, vol. 76, pp. 146–164. DOI: 10.1016/j.comnet.2014.11.008 [in English].

The article was submitted to the editorial office on 7 March 2025

УДК 351.861.3:004.056

Д. І. Прокопович-Ткаченко, В. П. Звєрєв, І. М. Козаченко

СУЧАСНИЙ ВИКЛИК ЦИФРОВОГО СВІТУ І РОЛЬ НАЦІОНАЛЬНОГО КООРДИНАЦІЙНОГО ЦЕНТРУ КІБЕРБЕЗПЕКИ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Стрімкий розвиток цифрових технологій створює нові можливості для економічного, соціального та культурного розвитку, але водночас формує й численні загрози, що негативно впливають на національну безпеку держав. Інформаційна безпека держави як складник національної безпеки стає головним елементом захисту від таких викликів сучасності, як кібератаки, інформаційна агресія та порушення функціонування критичної інфраструктури. У цьому контексті Національний координаційний центр кібербезпеки відіграє ключову роль у координації, інтеграції та управлінні заходами із забезпечення інформаційної безпеки держави.

Національний координаційний центр кібербезпеки виконує низку важливих функцій: моніторинг кіберзагроз, аналіз сучасних тенденцій у сфері кібербезпеки, реагування на інциденти, а також упровадження стратегій захисту. Центр координує співпрацю між державними органами, приватним сектором, академічними установами і міжнародними партнерами. Особливими напрямами його діяльності є розроблення стандартів захисту критичної інформаційної інфраструктури, прогнозування загроз і створення ефективних механізмів кіберзахисту.

Розширення повноважень Національного координаційного центру кібербезпеки супроводжується впровадженням таких сучасних технологій, як штучний інтелект, автоматизація процесів та використання великих даних для аналізу ризиків. Центр також активно працює над удосконаленням законодавчої бази, що регулює сферу кібербезпеки, забезпечуючи гармонізацію з міжнародними стандартами. Координація між суб'єктами кібербезпеки дає змогу зменшити дублювання функцій і підвищити ефективність системи.

Отже, Національний координаційний центр кібербезпеки являє собою головний елемент забезпечення інформаційної безпеки держави. Його діяльність спрямована на адаптацію до сучасних загроз, зміцнення стійкості держави до кібератак та формування безпечного інформаційного простору.

Ключові слова: *інформація, безпека, кіберзагрози, моніторинг, інфраструктура, технології, стандарти.*

Prokopovych-Tkachenko Dmytro – Candidate of Technical Sciences, Associate Professor, Head of the Department of Cybersecurity, University of Customs and Finance
https://orcid.org/0000-0002-6590-3898

Zvieriev Volodymyr – Candidate of Technical Sciences, Senior Researcher, Associate Professor of the Department of Software Engineering and Cybersecurity, State University of Trade and Economics
https://orcid.org/0000-0002-0907-0705

Kozachenko Ihor – Head of the Department of the State Center for Cyber Defense, State Service for Special Communications and Information Protection of Ukraine
https://orcid.org/0000-0002-0774-7284