UDC 351.861.3:004.056

D. Prokopovych-Tkachenko

V. Zvieriev

I. Kozachenko

INTEGRATION OF SECURITY OPERATIONS CENTERS (SOC) INTO UKRAINE'S NATIONAL SECURITY SYSTEM

The article explores the integration of Security Operations Centers (SOC) into Ukraine's national security system, emphasizing their role in strengthening cybersecurity resilience and protecting critical infrastructure. Given the increasing number of cyberattacks targeting Ukraine, SOCs serve as key components in detecting, monitoring, and responding to threats in cyberspace. The study analyzes the global experience of SOC implementation, particularly in the USA, EU, and NATO, where automated threat analysis systems, artificial intelligence, and big data analytics are widely employed to enhance cybersecurity operations. A significant part of the study is devoted to the challenges Ukraine faces in implementing SOCs, including insufficient funding, a shortage of qualified cybersecurity specialists, outdated legislation, and the need for integration with existing cybersecurity mechanisms. The article identifies key directions for SOC development in Ukraine, including the adoption of AI-driven cybersecurity technologies, expansion of international cooperation, and improvements in specialist training programs. The research also highlights the need for a comprehensive approach to SOC integration, focusing on centralized coordination between state institutions, private sector actors, and international cybersecurity organizations such as ENISA and CERT-UA. The authors emphasize the importance of implementing automated threat detection and response systems, developing machine learning models for cyber threat intelligence, and enhancing international collaboration in cybersecurity policymaking.

Keywords: *security operations center (SOC), cybersecurity, national security, hybrid warfare, cyber attacks, critical infrastructure protection, threat monitoring, artificial intelligence, big data analysis, incident response, international cooperation.*

Statement of the problem. In the current conditions of dynamic development of information technologies and growing cyber threats, ensuring the cybersecurity of the State is becoming one of the priority tasks of national security. Ukraine, as a state subject to systematic cyberattacks (by state and non-state actors), needs an effective system for detecting, monitoring and responding to cyber incidents. Security Operations Centres (SOCs) are key elements of such a system, as they provide rapid response to threats, analyse potential risks and coordinate the actions of public and private cybersecurity actors.

One of the main problems is the fragmentation of Ukraine's current cybersecurity system, which is due to the lack of a unified strategy for integrating the SOC into the national security infrastructure. The lack of centralised management, effective exchange of information between public and private entities, and imperfect regulatory framework pose significant challenges to the effective functioning of the SOC. The experience of leading countries shows that it is advisable to build SOCs based on innovative technologies, including artificial intelligence, machine learning and behavioural analysis, which increase the accuracy and speed of response to threats.

At the same time, an important area of development is the expansion of international cooperation, primarily with the EU, NATO and ENISA, to strengthen coordination in the field of cyber defence. The successful functioning of the SOC is also impossible without proper staffing: Ukraine has an acute shortage of certified

specialists in this field. Therefore, the article analyses current approaches to personnel training, including the introduction of international certification programmes and educational initiatives.

Given the growing number and sophistication of cyberattacks, the integration of the SOC into Ukraine's national security system is critical. Solving this problem requires a comprehensive approach that includes technological modernisation, development of the regulatory framework, human resources and international coordination. Such an approach will help strengthen the state's cyber resilience and effectively protect critical information systems.

Analysis of recent research and publications. The issue of integrating security operation centres into Ukraine's national security system is being actively studied in the scientific literature. The most developed SOCs operate in the USA, EU and NATO, where standardised approaches to threat monitoring, automated response systems and effective coordination between the public and private sectors have been implemented [3, 6]. The reports of the European Union Agency for Network and Information Security (ENISA) and the Cooperative Cyber Defence Centre of Excellence (CCDCOE) emphasise the importance of centralised SOC management to ensure rapid response [3]. In Ukraine, the Computer Emergency Response Team of Ukraine (CERT-UA) and the National Coordination Centre for Cybersecurity (NCCC) are studying SOC issues, analysing cyberattacks in 2014–2024. In their research paper [8], the authors draw attention to insufficient funding, staff shortages, and the need to update the regulatory framework [9]. The technological aspects of SOC, including the introduction of artificial intelligence and machine learning for threat analysis, are also considered separately [5, 6]. Automation of processes makes it possible to increase the efficiency of response and minimise the human factor. There is a critical shortage of qualified personnel, which requires the introduction of educational programmes and international certification of specialists [10, 12].

Thus, recent studies confirm the need for a comprehensive approach to SOC integration, including legislative improvements, technology development, training and international cooperation [3, 6].

The purpose of the article is to study the role of security operations centres in the national cybersecurity system of Ukraine, to analyse the international experience of their implementation, challenges for Ukraine, and prospects for development with due regard for the latest technologies, international cooperation and staffing.

Summary of the main material. The study applies a comprehensive methodological approach that combines several scientific methods of analysis to ensure a comprehensive study of the functioning of security operation centres in Ukraine. The method of comparative analysis was used to compare the peculiarities of SOC functioning in Ukraine with the practices adopted in the international environment, in particular in the United States and the European Union [2]. This makes it possible to identify key differences in approaches to the organisation of SOCs, the level of their integration into state cybersecurity systems, the use of automated technologies, and the level of cooperation with the private sector [4].

The analysis of international experience is extremely important for developing recommendations for improving SOCs in Ukraine and harmonising their activities with European and global standards [7]. The data analysis method was used to systematise and process information on cyber incidents recorded in Ukraine during 2014–2024 [6]. The parameters studied include statistics on the number and types of attacks, sources of threats, the nature of vulnerabilities exploited by attackers, and response measures taken by the SOC [9]. This method makes it possible to identify patterns in the development of cyber threats, assess the effectiveness of the SOC in different periods, and identify key areas for improving the cyber defence infrastructure [10].

The method of structural analysis is used to determine the organisational structure of SOCs, their functional capabilities, as well as mechanisms of interaction with public and private institutions that ensure cybersecurity in Ukraine [3]. In particular, the study analyses such aspects as information security event management, threat detection, incident response, traffic monitoring, as well as SOC interaction with public authorities, the National Cybersecurity Coordination Centre (NCCC), CERT-UA and international partners [8]. The study of the SOC structure allows assessing their operational effectiveness, the degree of integration into the national cyber defence system, and the ability to adapt to new challenges [12].

The forecasting method is applied to assess the potential directions of SOC development in Ukraine, in particular the introduction of innovative technologies in the field of cybersecurity [5]. Particular attention is paid to the prospects of using artificial intelligence, neural network algorithms and digital twins to improve the processes of monitoring, analysing and responding to cyber threats [13]. Predictive analysis also makes it possible to assess long-term risks to Ukraine's cybersecurity, including post-quantum threats that may arise

from the development of quantum computing, and to develop recommendations for adapting the SOC to future technological changes [14].

The method of expert analysis was used to assess the effectiveness of SOCs, identify the main problems and develop strategic measures to improve their performance [11]. The opinions of cybersecurity experts, representatives of government agencies, think tanks, and private companies working in the field of information security were studied [15]. The analysis of expert opinions makes it possible to draw conclusions about the compliance of current approaches with international standards, assess the degree of readiness of SOCs to respond to modern threats and identify priority steps for their development [18].

Thus, the use of these methods creates a comprehensive picture of the state of SOCs in Ukraine, their role in the national cybersecurity system, and also allows to identify the main challenges and prospects for development in the context of global trends in cybersecurity [20].

To confirm the significance of SOCs in Ukraine's cybersecurity system, it is worth looking at examples of successful detection and neutralisation of large-scale cyberattacks over the past decade. SOCs have played a key role in restoring critical systems, isolating infected environments, and implementing real-time countermeasures. Table 1 provides a chronology of the most significant cyber incidents that challenged public and private actors, and describes the response of security operations centres.

Table 1 – Examples of attacks neutralised in Ukraine using SOC (2014–2024)

Year	Event	Overview	Source
2014	Attack on the Central Election Commission of Ukraine	A large-scale cyberattack on the CEC servers aimed at disrupting the electoral process. System restored thanks to SOC and CERT-UA	[2]
2015	Attack on energy infrastructure (BlackEnergy)	Cyberattack on Ukraine's energy system, causing power outages. The malware has been identified BlackEnergy	[2]
2017	NotPetya Virus attack	A massive cyberattack by the NotPetya virus, affecting government agencies and the private sector. Affected systems are isolated	[1]
2021	WhisperGate Campaign	The WhisperGate malware campaign aimed at destabilising government systems is detected. Protective measures taken	[2]
2022	DDoS attacks on the "Diia" platform and government services	SOC neutralised numerous DDoS attacks on "Diia" portals and government services	[2]
2024	Continuous improvement of the SOC	Improving the SOC, implementing automated technologies, and cooperating with international partners such as ENISA	[3]

During the 2014 attack on the servers of the Central Election Commission, the SOC, in coordination with CERT-UA, neutralised malware that could have destabilised the electoral process [2]. In 2015, during the BlackEnergy attack on the SOC's energy infrastructure, malware was identified and measures were developed to restore energy systems [2]. In 2017, the NotPetya virus attack demonstrated the SOC's ability to respond quickly to mass incidents, isolating the affected systems and reducing the scale of the disaster [1, 3]. After the start of the full-scale intrusion in 2022. SOC, using modern automated technologies to protect the national cyberspace, actively blocked DDoS attacks on government services, including the Diia platform [2, 3].

Thanks to these functions, SOCs have become an integral part of Ukraine's national cybersecurity system, helping to protect critical infrastructure from the growing number and sophistication of attacks. Security Operations Centres are effective not only in detecting threats but also in strengthening the information space, which is a strategic factor in countering hybrid warfare.

Integration of the SOC into the national security infrastructure is a key task to ensure effective protection of the state against modern cyber threats. This process requires close coordination between government agencies such as CERT-UA, the Security Service of Ukraine, the Ministry of Digital Transformation, and private entities involved in information security. The main elements of such integration are the exchange

of data on cyber threats, unification of incident response standards, and standardisation of risk analysis and management processes [1, 2].

To improve the level of information security in Ukraine, it is necessary to consider SOC not only from a practical perspective, but also to integrate scientific and technological approaches to their development. The use of innovative adaptive models built on the basis of neural networks will allow for more accurate detection of cyber threats in real time. Such models can learn by analysing data sets from past attacks and predict new threat vectors with a high level of accuracy. For example, the introduction of digital twin technology to simulate the operation of an SOC can be an effective tool for modelling and analysing potential attack scenarios, as well as for testing response methods in a controlled environment [3].

Digital twins allow for the creation of accurate virtual copies of cybersecurity systems that can be used to test new security methods without risking real-world infrastructure. Combined with neuro-predictive algorithms, these technologies make it possible to predict potential attacks and respond to them before they cause damage. For example, neural networks can analyse network traffic, detect anomalies, and automatically activate defence mechanisms before an attack reaches a critical scale [3].

In addition, the integration of the SOC into the global security system involves active cooperation with international organisations such as ENISA to share best practices and use advanced cybersecurity solutions. This makes it possible to harmonise national approaches with global ones and ensure a higher level of cyber defence of the state [3].

The diagram in Figure 2 illustrates the main functions of a security operations centre, which are key to ensuring an organisation's cybersecurity. The SOC is the leading centre that performs a coordinating role in the following tasks: event and incident management; information security analysis; vulnerability management; web application protection; protection against cyber threats, DDoS attacks; and brand preservation. In addition, he is responsible for the operation of security tools, ensuring the integrity, availability and confidentiality of information assets. The diagram clearly demonstrates an integrated approach to risk management based on the interaction of technological, process and analytical components.

The diagram shows the key functions of a security operations centre (SOC), which provide a comprehensive approach to cyber defence for an organisation. The SOC is a central hub that coordinates various aspects of information security and performs a number of important tasks. Security operations involves the proper configuration, monitoring and support of security systems such as firewalls, antivirus software and intrusion detection systems. Information security event and incident management involves monitoring network traffic, detecting anomalies, analysing incidents and responding promptly to threats to minimise their impact on business processes. Vulnerability management is aimed at identifying and eliminating weaknesses in software, systems and networks to prevent potential attacks. Web application security ensures that web applications are safe from attacks, including SQL injections, cross-site scripting (XSS) and other types of malicious activity. Information security analysis involves collecting, processing and analysing data on cyber threats to develop defence strategies and prevent future attacks. DDoS protection involves preventing distributed denial-of-service attacks aimed at overloading systems and disrupting their operation. Brand protection involves monitoring the information space to detect reputational threats related to data leaks, phishing attacks or illegal use of the brand. Protection against cyber threats and attacks ensures the integrity, confidentiality and availability of data, and counteracts modern threats such as phishing, viruses and malware.

The diagram above demonstrates the multi-component nature of an SOC, which combines technological tools, analytics and processes to create an integrated cyber defence system. The SOC not only performs a reactive function in responding to threats, but also plays a proactive role in preventing them and minimising the impact on the information infrastructure.

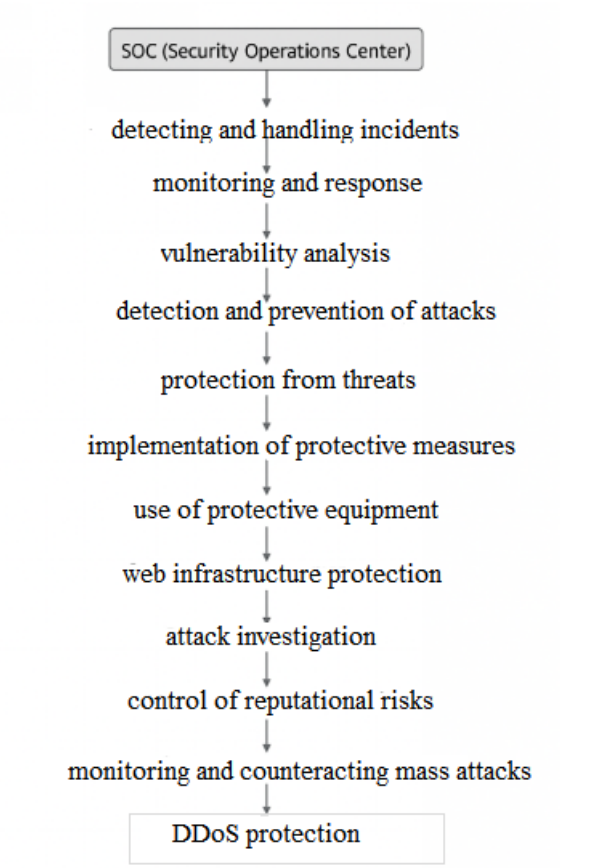

Figure 2 – Functional structure of a security operations centre (SOC)

Implementing the integration of the SOC into Ukraine's national security system requires a comprehensive approach that includes the introduction of modern technologies, the creation of an effective data exchange platform and the development of human resources. One of the key aspects is the use of automation technologies to monitor and respond to cyber threats. The introduction of artificial intelligence, machine learning, and neuro-predictive algorithms can significantly reduce incident response times and improve the accuracy of threat analysis. However, to ensure the long-term effectiveness of SOCs, it is necessary to take into account future challenges, including post-quantum threats that may make traditional cryptographic algorithms vulnerable. Implementing cryptographic solutions that are resistant to attacks using quantum computers will help protect information infrastructure from potential future risks.

An important component of SOC integration is the creation of a centralised platform for the exchange of information on cyber threats between government agencies, the private sector and international partners. Such a system should ensure rapid data analysis, coordination of actions and joint response to incidents in real time. The use of big data analysis and artificial intelligence technologies will help to increase the efficiency of the SOC and improve the overall level of cybersecurity.

Another important challenge is the shortage of qualified cybersecurity professionals, which limits the ability of the SOC to function effectively. Addressing this issue requires the development of specialised training programmes, the introduction of certification systems, and the creation of conditions for the professional development of existing staff. An important role in this process is played by an interdisciplinary approach that includes training in adaptive security methods that can effectively respond to complex and dynamic threats. As a result of these measures, Ukraine's SOC can become not only an element of response to cyber threats, but also an integrated self-organised system that uses adaptive algorithms to ensure the resilience of the state's information infrastructure. This will allow to effectively counter current and future threats, strengthening national security in the context of digital transformation.

Table 2 – Main directions of SOC integration into the national security system

Direction of implementation	Key events	Expected outcomes
SOC automation	Implementation of artificial intelligence, machine learning, cryptographic solutions resistant to quantum attacks	Improving the accuracy and speed of threat response, reducing risks
Data exchange platform integration	Creating a centralised information exchange system, using big data to analyse threats	Better coordination between public and private entities, more effective fight against cyber threats
Training in the field of cybersecurity	Development of training programmes, certification of specialists, staff development	Increasing the number of qualified specialists, reducing the outflow of personnel abroad

To ensure the effective integration of the SOC into the national security system of Ukraine, attention should be paid to the development of a legal framework that would clearly define the role, functions and powers of the SOC, as well as the mechanisms of their interaction with other cybersecurity actors. This involves the creation of laws and regulations governing the exchange of information on cyber incidents, standardisation of threat response procedures, and the provision of legal grounds for SOC activities.

Another important aspect is to raise public awareness of cyber threats and the role of SOCs in neutralising them. It is advisable to conduct information campaigns, educational programmes and trainings for various categories of the population, as well as to promote the development of a cybersecurity culture in organisations and institutions. Ensuring proper awareness and training of personnel will contribute to the more effective use of SOC capabilities and increase the overall level of cyber resilience of the state.

Conclusions

The integration of security operation centres into the national security system of Ukraine is a strategic task that ensures the protection of critical infrastructure and strengthens the state's resilience to modern cyber threats. The analysis has shown that SOCs perform a key function in detecting, monitoring, analysing and neutralising cyberattacks, and their effectiveness directly depends on the level of technological development, human resources and the level of coordination between public and private entities.

Despite the achievements in SOC functioning, the problems of infrastructure fragmentation, lack of qualified specialists and limited funding remain relevant. The challenges of hybrid warfare, targeted attacks on critical facilities, and the development of quantum technologies require the implementation of new strategies. One of the leading areas of modernisation is the integration of synergy principles that contribute to the creation of adaptive and self-organising systems. The use of artificial intelligence, machine learning, digital twins and predictive algorithms makes it possible to increase the speed and accuracy of response to hidden and complex threats.

In this context, the development of post-quantum cryptographic solutions is of particular importance, as they should ensure long-term protection of information systems. At the same time, the issue of personnel training remains relevant: the introduction of interdisciplinary programmes, certification and state support will help to form a professional personnel reserve in the field of cyber defence. In addition, it is important to take into account international experience, including standardised response protocols, centralised information exchange systems and active international cooperation.

Areas for further research include formalising the model of an integrated SOC, taking into account the Ukrainian context, developing algorithms for automated incident management, adapting post-quantum cryptographic solutions to real-world conditions, and studying the effectiveness of cross-sectoral coordination in the national cybersecurity system. It is also promising to analyse the regulatory mechanisms for building a national SOC system with the participation of the private sector and international partners.

References

1. CERT-UA (2017). *Povidomlennia pro virus NotPetya: analiz i zakhody reahuvannia* [Notification about NotPetya virus: analysis and response measures]. Kyiv. Retrieved from: https://cert.gov.ua (accessed 8 February 2025) [in Ukrainian].

2. CERT-UA (2022). *Kiberzakhyst uriadovykh system pid chas viiskovykh dii* [Cyberprotection of government systems during hostilities]. Kyiv. Retrieved from: https://cert.gov.ua (accessed 8 February 2025) [in Ukrainian].

3. ENISA (2021). Cybersecurity Guide for SOCs. Athens : ENISA. Retrieved from: https://www.enisa.europa.eu (accessed 8 February 2025) [in English].

4. CERT-UA (2020). *Kiberzakhyst krytychnoi infrastruktury: pidkhody do reahuvannia* [Cybersecurity of critical infrastructure: response approaches]. Kyiv. Retrieved from: https://cert.gov.ua (accessed 8 February 2025) [in Ukrainian].

5. *Zakon Ukrainy "Pro natsionalnu bezpeku Ukrainy" № 2469-VIII* [Law of Ukraine about the National Security of Ukraine activity no. 2469-VIII]. (2018, June 21]. Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19 (accessed 8 February 2025) [in Ukrainian].

6. NCICC (n.d.). National Cybersecurity and Communications Integration Center. Retrieved from: https://www.cisa.gov (accessed 8 February 2025) [in English].

7. Sopilko I. M. (2021). *Informatsiina bezpeka ta kiberbezpeka: porivnialno-pravovyi aspekt* [Information security and cybersecurity: comparative legal aspect]. *Yurydychnyi visnyk. Seriia: povitriane i kosmichne pravo*, no. 59, 110–115. DOI: https://doi.org/10.18372/2307-9061.59.15603 [in Ukrainian].

8. Belkin L., Yurynets Yu., Belkin M., Kryvolap Ye. (2022). *Spivvidnoshennia poniat "informatsiina bezpeka", "bezpeka informatsii", "kiberbezpeka" v konteksti bezpekovykh stratehii Ukrainy 2020–2021 rokiv* [The correlation of the concepts "information security", "security of information", "cybersecurity" in the context of Ukraine′s security strategies in 2020–2021]. *Yurydychnyi visnyk. Seriia: povitriane i kosmichne pravo*, no. 3 (64), 78–86. DOI: https://doi.org/10.18372/2307-9061.64.16893 [in Ukrainian].

9. Bulashenko A. V., Brui M. (2010). *Informatsiina bezpeka* [Information security]. Sumy : SumDU. Retrieved from: http://essuir.sumdu.edu.ua/handle/123456789/21090 (accessed 8 February 2025) [in Ukrainian].

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

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

12. Batechko O., Tsymbalenko N. V. (2016). *Informatsiina bezpeka pidpryiemstva* [Information security of an enterprise]. Kyiv : National University of Technologies and Design. Retrieved from: https://er.knutd.edu.ua/handle/123456789/4464 (accessed 8 February 2025) [in Ukrainian].

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

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

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

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

17. 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].

18. Solovii H. R. (2006). *Mizhnarodna informatsiina bezpeka: polskyi dosvid* [International information security: Polish experience]. *Aktualni problemy mizhnarodnykh vidnosyn*, vol. 65, no. 4.1, pp. 45–47 [in Ukrainian].

19. Hutsaliuk M. (2005). *Informatsiina bezpeka u suchasnomu suspilstvi* [Information security in modern society]. *Pravo Ukrainy*, no. 7, pp. 71–74 [in Ukrainian].

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

21. Marakova I. I., Syropiatov O. A. (2006). *Informatsiina bezpeka kompleksnykh system zviazku* [Information security of complex communication systems]. *Ukrainian Information Security Research Journal*, iss. 8, no. 4 (31). DOI: 10.18372/2410-7840.8.4977 [in Ukrainian].

The article was submitted to the editorial office on 15 April 2025

УДК 351.861.3:004.056

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

ІНТЕГРАЦІЯ ОПЕРАЦІЙНИХ ЦЕНТРІВ УПРАВЛІННЯ БЕЗПЕКОЮ (SOC) У СИСТЕМУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Досліджено інтеграцію операційних центрів управління безпекою (SOC) у систему національної безпеки України. Розглянуто роль інформаційної безпеки як складної техногенної системи, що забезпечує стійкість державних інституцій і захист критичної інфраструктури від кіберзагроз.

У сучасних умовах військово-політичних викликів, зокрема гібридної війни, цілеспрямованих кібератак, дезінформаційних кампаній та загрози дестабілізації інформаційного простору, операційні центри управління безпекою відіграють ключову роль щодо моніторингу, виявлення і реагування на загрози у кіберпросторі. З огляду на глобальну цифровізацію та стрімкий розвиток технологій кібернападів уряди багатьох країн світу приділяють значну увагу розвитку операційних центрів управління безпекою, упровадженню автоматизованих систем аналізу кіберзагроз, а також розбудові ефективних механізмів взаємодії між державними структурами і приватним сектором.

Авторами проаналізовано міжнародний досвід функціонування операційних центрів управління безпекою, зокрема практики США, ЄС і НАТО, які ефективно використовують автоматизовані системи реагування, штучний інтелект та аналіз великих даних для оперативного виявлення й нейтралізації загроз. Запровадження операційних центрів управління безпекою в Україні потребує розв'язання низки проблем, серед яких: недостатнє фінансування, кадровий дефіцит, необхідність модернізації нормативно-правової бази, інтеграція з уже існуючими системами кіберзахисту.

Визначено основні напрями розвитку операційних центрів управління безпекою в нашій державі. Ідеться про впровадження інноваційних технологій, зокрема штучного інтелекту, машинного навчання та аналізу поведінкових загроз, а також розширення співпраці з міжнародними партнерами і вдосконалення підготовки фахівців у сфері кібербезпеки.

Розвиток операційних центрів управління безпекою є невід'ємним складником підвищення кіберстійкості держави, важливим інструментом забезпечення національної безпеки. Комплексний підхід до побудови SOC, який передбачає технологічну модернізацію, міжнародне співробітництво та кадрове забезпечення, дасть змогу Україні посилити захист своїх критичних інформаційних систем і забезпечити оперативне реагування на нові загрози у цифровому середовищі.

Ключові слова: *операційний центр управління безпекою (SOC), кібербезпека, гібридна війна, кібератаки, інформаційна безпека, критична інфраструктура, моніторинг загроз, штучний інтелект, аналіз великих даних, міжнародне співробітництво, національна безпека.*

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