https://doi.org/10.31891/2307-5732-2025-355-78
УДК 004.056.53

SYSOIENKO SVITLANA
Cherkasy State Technological University
https://orcid.org/0000-0002-0009-337X
e-mail: s.sysoienko@chdtu.edu.ua
BABENKO VIRA
Cherkasy State Technological University
https://orcid.org/0000-0003-2039-2841
e-mail: v.babenko@chdtu.edu.ua
LADA NATALIIA
State Scientific Research Institute of Armament and Military Equipment Testing and Certification
https://orcid.org/0000-0002-7682-2970
e-mail: ladanatali256@gmail.com

INFORMATION SECURITY INCIDENT MANAGEMENT AT CRITICAL INFRASTRUCTURE FACILITIES

The paper analyzes in detail modern approaches, international standards (CobiT, ITIL, ISO/IEC 27000) and national legislation, which regulate cyber incident management, as well as the features of their application in conditions of military conflict. Particular emphasis is placed on the role of state bodies, such as the State Service for Special Communications and Information Protection and CERT-UA, which coordinate cyber protection and incident response measures. The key stages of incident management - preparation, rapid response and recovery - are identified as integral components of the cycle of continuous improvement of the cyber security system. Particular attention is paid to technological tools for increasing the cyber resilience of CI: the implementation of SIEM systems for monitoring and analyzing threats in real time, the automation of response, as well as the use of internationally recognized incident information exchange protocols (for example, Traffic Light Protocol - TLP). The need to form coordinated interdepartmental response teams, clearly allocate roles and areas of responsibility, as well as build effective communication between government agencies, the private sector and CI operators is emphasized. No less important is the emphasis on personnel training: regular trainings, simulation exercises and assessment of the effectiveness of measures using metrics make it possible to maintain a high level of readiness for cyber incidents. The results of the study can become the basis for the development of an integrated national system for managing information security incidents, which will provide an adequate level of strategic facilities protection and contribute to strengthening the state's cyber resilience. The proposed approaches and recommendations have a direct impact on reducing the risks of cyber threats, minimizing potential losses and guaranteeing the continuity of Ukraine's vital functions in the conditions of constant challenges of modern cyberspace.

Keywords: information security, cyber incident, critical infrastructure facility, cyber threat, incident management.

СИСОЄНКО СВІТЛАНА, БАБЕНКО ВІРА
Черкаський державний технологічний університет
ЛАДА НАТАЛІЯ
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки

УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

В роботі детально проаналізовано сучасні підходи, міжнародні стандарти (CobiT, ITIL, ISO/IEC 27000) і національне законодавство, що регламентують управління кіберінцидентами, а також особливості їх застосування в умовах військового конфлікту. Окремо акцентовано на ролі державних органів, таких як Державна служба спеціального зв'язку та захисту інформації та CERT-UA, які координують заходи з кіберзахисту та реагування на інциденти. Визначено ключові етапи управління інцидентами – підготовка, швидке реагування і відновлення – як невід'ємні складові циклу безперервного удосконалення системи кібербезпеки. Особливу увагу приділено технологічним засобам підвищення кіберстійкості КІ: впровадженню SIEM-систем для моніторингу та аналізу загроз у режимі реального часу, автоматизації реагування, а також застосуванню міжнародно визнаних протоколів обміну інформацією про інциденти (наприклад Traffic Light Protocol – TLP). Підкреслено необхідність формування скоординованих міжвідомчих команд реагування, чіткого розподілу ролей і зон відповідальності, а також побудови ефективної комунікації між державними структурами, приватним сектором та операторами КІ. Не менш важливим є акцент на підготовці кадрів: регулярні тренінги, імітаційні вправи та оцінка ефективності заходів за допомогою метрик дозволяють підтримувати високий рівень готовності до кіберінцидентів. Результати дослідження можуть стати основою для розроблення інтегрованої національної системи управління інцидентами інформаційної безпеки, яка забезпечить адекватний рівень захисту стратегічних об'єктів і сприятиме зміцненню кіберстійкості держави. Запропоновані підходи та рекомендації мають безпосередній вплив на зниження ризиків кіберзагроз, мінімізацію потенційних збитків і гарантування безперервності життєво важливих функцій України в умовах постійних викликів сучасного кіберпростору.

Ключові слова: *інформаційна безпека, кіберінцидент, об'єкт критичної інфраструктури, кіберзагроза, управління інцидентами.*

Стаття надійшла до редакції / Received 29.05.2025
Прийнята до друку / Accepted 26.06.2025

Problem statement

Critical infrastructure is the basis of the functioning of modern society, and its security directly affects the national economy, state security and the lives of citizens. With the development of digital technologies, the need to ensure reliable protection of information systems and networks that are part of critical infrastructure is increasing [1-2]. However, any development has a reverse side in the form of threats. Every day, the state, society and ordinary

citizens are faced with information security incidents.

The increase in the number, variety and complexity of cyber threats aimed at key facilities requires the improvement of information security incident management systems in order to effectively implement countermeasures and minimize possible negative consequences of cyber incidents [3]. In particular, in the conditions of a hybrid war against Ukraine, cyberattacks on energy, transport and communication systems are becoming systemic, which threatens national security [4]. It is urgent to conduct a comprehensive analysis of existing models of critical information infrastructure protection, their regulatory support, technological implementation and organizational structure in order to develop recommendations for creating a national critical infrastructure protection system that would meet modern challenges in the field of cyber security, since effective management of information security incidents (ISI) is a key element in ensuring the stability and continuity of the functioning of critical infrastructure facilities (CIF). The study aims to reveal current problems related to information security incidents and propose effective methods for identification, analysis and response to certain incidents directed at critical infrastructure facilities.

Research and publication analysis

In current conditions of digital transformation, information security incidents are becoming increasingly alarming. The rapid development of information technology is accompanied by an increase in cybercrime: in 2023, global losses reached $8 trillion, and by the end of 2025, $10.5 trillion is predicted. Of particular danger are cyberattacks on critical infrastructure facilities, which can cause significant economic, social and humanitarian consequences [5].

The work [6] carries out an analysis of the best global practices for protecting critical information infrastructure, the implementation of elements of which at the legislative level and in practice will make it possible to qualitatively improve the process of protecting Ukraine's critical information infrastructure. The authors of [7] study the impact of cyber espionage and cyberattacks on CIF in war conditions, emphasizing the importance of a comprehensive approach to protection. In the work [8], a study of modern SIEM systems is carried out. The proposed system is designed to solve a number of current cyber security problems and meets the basic requirements of international standards and best global practices for creating cyber incident management systems.

The work [9] describes the architecture of the system, which includes mechanisms for preventing, responding to and processing cyber incidents, focused on the European critical information infrastructure (CII). The authors emphasize the need for an adaptive approach to threat detection, integration with external data sources and maintenance of interaction processes between organizations. In the study [10], the authors analyze the transition from cyber incident management to cyber crisis management in the EU, focusing on new legislative initiatives that require mandatory incident reporting and the creation of new management bodies. The work [11] analyzes and reviews innovations and modern approaches used to ensure cyber security in the context of investigating security incidents at the CIF. Research and implementation of new strategies and approaches in this area can contribute to responding to new cyber threats, while maintaining the reliability and functioning of society, and increasing the level of protection of important information systems.

Analysis, systematization and consideration of current issues of the strategy for responding to information security risks, as well as understanding the degree of economic feasibility of applying certain security measures in relation to the manifestation of possible information security incidents are considered in [12].

Formulation of the objectives of the article

The purpose of the work is: to improve the strategies for managing information security incidents at critical infrastructure facilities, taking into account the specificity of these facilities and features of cyber threats. To achieve the purpose set in the work, modern cyber incidents and information security incident management systems are reviewed, legal regulation in the field of information security incident management is studied; critical infrastructure facilities and features of information protection on them are analyzed. The results of the study can be used to develop an information security incident management system for critical infrastructure facilities.

Presentation of the main material

With the beginning of a full-scale war against Ukraine, cyberspace has become an important front. A study of PwC's global information security trends in 2022 showed that 40% of cyberattacks lead to a shutdown of operations, 39% - to the loss of confidential data, 32% - to a decrease in product quality, 29% - to material damage, and 22% - to threats to people's lives [13]. This highlights the vulnerability of automated and robotic systems in today's environment. In such challenging conditions, timely response to information security incidents and the development of an effective cyber defense system, especially at critical infrastructure facilities, are of particular importance. Cyber incident management should be based on international best practices and recommendations.

At the state level, cyber security is provided within the national system that includes the National Security and Defense Council of Ukraine, the State Service for Special Communications and Information Protection, the Security Service of Ukraine, the Ministries of Internal Affairs and Defense, intelligence agencies, and other entities. A special role in this system is played by the State Service for Special Communications and Information Protection and the National Cyber Security Coordination Center under the National Security and Defense Council [14]. The process of responding to incidents is technically complex and requires the involvement of highly qualified specialists [13]. Timely response makes it possible to localize and eliminate the consequences of incidents, preserve reputation and resources, as well as restore the operability of information systems. This process includes identifying

vulnerabilities, testing the effectiveness of protection mechanisms, and analyzing the system architecture. Incident management should meet the highest global cyber security standards. The information security incident management process is a central element of an organization's cyber security system, aimed at reducing risks to information assets. Incidents can be both intentional (unauthorized access, malware) and accidental (technical failures, human errors) ones. Incident management should be based on the PDCA (Plan–Do–Check–Act) model, which ensures continuous process improvement and compliance with international standards. The structure should include identification of responsibilities, detection of incidents, their documentation, analysis and response in accordance with regulatory requirements and standards [15].

International normative regulation in the field of information security incident management is based mainly on such standards and recommendations for IT process management:

CobiT (Control Objectives for Information and Related Technology) is an international IT management framework in which the *DS5* process is dedicated to security, in particular incident response.

ITIL 4 (Information Technology Infrastructure Library) considers information security as a four-phase (planning, implementation, assessment, maintenance) cyclic process and provides for measures at strategic, tactical and operational levels.

BS (British Standards) and the activities of the UKAS agency focus on the requirements for auditors and companies conducting certification audits in the field of IS.

ISO/IEC 15408 defines general criteria for assessing IT products from a security perspective and is used within the framework of compliance with the requirements of payment systems and technical audit [16].

The ISO/IEC 27000 series (including ISO/IEC 27001, ISO/IEC 27002) is the basis for information security management, covering all key aspects, including incident management. ISO/IEC 27001 provides for the certification of organizations that have implemented an IS management system in accordance with international requirements [17].

The regulatory and legal framework in the field of cyber security in Ukraine [18] is formed as a multi-level system covering laws, decrees, standards, departmental acts and methodological documents (Table 1). Its goal is to create a holistic system for responding to information security incidents, regardless of the form of ownership, industry or organization size.

Table 1

The main Laws of Ukraine regulating the field of information security incident management [18]

THE LAWS OF UKRAINE	
"On the Basic Principles of Ensuring Cyber Security in Ukraine" https://zakon.rada.gov.ua/laws/show/2163-19#Text	"On Approval of General Requirements for Cyber Protection of Critical Infrastructure Facilities" https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
"On Scientific Technical Information" https://zakon.rada.gov.ua/laws/show/3322-12#Text	"On Information" https://zakon.rada.gov.ua/laws/show/2657-12#Text
"On Copyright and Related Rights" https://zakon.rada.gov.ua/laws/show/3792-12#Text	"On Information Protection in Information and Communication Systems" https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
"On State Secrets" https://zakon.rada.gov.ua/laws/show/3855-12#Text	"On the Protection of Personal Data" https://zakon.rada.gov.ua/laws/show/2297-17#Text

The Law of Ukraine "On the Basic Principles of Ensuring Cyber Security in Ukraine" [19], which has laid legal foundations for building a national cyber security system, identified responsible bodies (in particular, the State Service for Special Communications, the Security Service of Ukraine, the National Bank of Ukraine, the National Cyber Security Coordination Center under the National Security and Defense Council of Ukraine) and established requirements for reporting cyber incidents, is a key element of this system.

Violation of CI or its destruction can cause significant losses, including mass human casualties, disruption of basic state functions, and destabilization of society. According to the regulatory legal acts of Ukraine, the structure of CI covers the following sectors: fuel and energy, digital technologies and communications, information protection, healthcare, food and agro-industrial system, finance and economy, transport and logistics, life support systems, industry, public safety and civil protection, environmental safety, defense, justice and execution of sentences, state registration, science and research, electoral process, social protection, information space. It is the comprehensive approach to the analysis of Ukraine's critical infrastructure that provides for intersectoral interdependence, multidisciplinary risk assessment and integration of protection measures at all levels: technological, organizational, legal and cyber ones. In the conditions of hybrid warfare and growing cyber threats, maintaining of critical infrastructure resilience is a national security priority.

Cyber protection of CIF is considered as part of the national cyber security system and is mandatory at each stage of the infrastructure life cycle. The manager or owner of the facility is responsible for implementing and maintaining the cyber protection system. If state information resources or information with limited access are processed at CIF, the Comprehensive Information Protection System (CIPS) is subject to state expertise. In the absence of such information, the system is subject to verification by an independent audit. One of the key requirements is to

promptly inform the government Computer Emergency Response Team in Ukraine (CERT-UA) about cyber incidents. CERT-UA [20] acts as a situational cyber protection center, a functional unit of the Security Service of Ukraine. Information security incident management at critical infrastructure facilities is a key component of the national cyber protection system. Such a system should provide real-time detection of malicious activity, analysis of network anomalies, response to cyber incidents, and processing of internal and external threat reports.

The cyber incident management procedure includes three sequential stages:

- ***preparation*** - creation of policies, instructions, communication channels, backups, and testing of the response system;
- ***response*** - detection, registration, classification of the incident, activation of responsible persons, and elimination of an active threat;
- ***further maintemance*** –analysis of causes, assessment of damage, updating of protection tools, and generation of reports.

The use of a response structure that involves systematic documentation and investigation of incidents makes it possible to strengthen the resilience of the organization's IT systems. The implementation of the principles of the Traffic Light Protocol, which establishes a standardized model for exchanging information about threats between participants, is particularly effective [21].

Effective cyber incident management is one of the key functions for ensuring the cyber resilience of critical infrastructure facilities. The main elements of this activity are the following:

Response planning: includes the detection and classification of cyber incidents, their documentation, determination of the impact on services and formation of response policies, construction of typical scenarios for the development of cyber incidents for personnel training, creation of agreed internal regulatory documents that determine the response procedure, as well as formation of a structured response team, including roles, authorities and areas of responsibility.

Tools and procedures: involve the use of automated incident capturing, analyzing and registering tools, such as SIEM systems, conducting of regular personnel training, including modeling of cyber incidents and simulation exercises, as well as assessment of the effectiveness of response based on predefined metrics, detection, response and recovery time.

Interaction with stakeholders: requires timely information to internal and external stakeholders, including information security services, management, law enforcement agencies and regulators. Internal and external communication procedures, including crisis messages, as well as the format for reporting on incidents, are defined.

Personnel roles and responsibilities: specific officials are appointed to be responsible for implementing the cyber incident management plan. Their functions are formalized in job descriptions, taking into account the contribution to the assessment of work efficiency.

Program maintenance and improvement: all documents, including response plans, procedures and job descriptions, should be reviewed at least annually or when the regulatory framework changes. An ongoing cyber incident management program enables the organization to minimize the impact of serious incidents, restore critical functions and ensure resilience.

Ensuring coherence between technological, organizational and legal aspects of managing cyber incidents can reduce losses, ensure continuity of service provision and fulfill obligations to society and the state.

Conclusions from this study and prospects for further research in this area

The study has confirmed that effective cyber incident management at critical infrastructure facilities is a key factor in ensuring national security and the resilience of vital systems. The implementation of international standards and best practices, such as CobiT, ITIL and ISO/IEC 27000, allows for a systematic approach to detecting, responding to and recovering from cyber incidents. The coordination of actions between government agencies, the private sector and CI operators that ensures a quick and effective response is an important component. The emphasis on the use of modern technologies, in particular SIEM systems, automation of response processes and standardized information exchange protocols, contributes to increasing the efficiency and accuracy of threat detection. Training of specialists and conducting of training courses are an integral part of the formation of a highly effective cyber security system.

Further research in the field of cyber incident management should be directed towards the development of intelligent systems for monitoring and analyzing cyber threats using artificial intelligence and machine learning. No less important is the study of mechanisms for integrating multi-level protection systems and improving protocols for interaction between cyber security participants. The development of risk assessment models taking into account the features of hybrid and cyber wars, which will allow for more accurate forecasting of potential threats and planning of protection measures, is another promising direction. The study of social aspects of cyber security, including increasing user awareness and developing a security culture, will contribute to the formation of a comprehensive approach to ensuring the protection of critical infrastructure.

References

1. Sysoienko S. V. Vyklyky ta mozhlyvosti inzhenerno-tekhnichnoho zakhystu informatsii u krytychnii infrastrukturi / S. V. Sysoienko // Research in Science, Technology and Economics: Collection of Scientific Papers “International Scientific Unity” with Proceedings of the 2nd International Scientific and Practical Conference, March 5–7, 2025. – Luxembourg, Luxembourg, 2025. – S. 369–371. – ISBN 979-8-89704-985-1 (series). – DOI:

https://doi.org/10.70286/ISU-05.03.2025

2. Pomaza-Ponomarenko A. L. Osoblyvosti vyznachennia obiektiv krytychnoi infrastruktury ta spivvidnesennia z obiektamy pidvyshchenoi nebezpeky / A. L. Pomaza-Ponomarenko, D. V. Taraduda // Zbirnyk tez dopovidei Vseukrainskoi naukovo-praktychnoi konferentsii, 30 trav. 2024 r. – Kharkiv, 2024. – S. 82–83.

3. Pro krytychnu infrastrukturu [Elektronnyi resurs] : Zakon Ukrainy // Vidomosti Verkhovnoi Rady (VVR). – 2023. – № 5, st. 13. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/1882-20#Text (data zvernennia: 01.05.2025). – Nazva z ekrana.

4. Bielai S. V. Teoretychni osnovy formuvannia systemy zakhystu obiektiv krytychnoi infrastruktury Ukrainy / S. V. Bielai, I. S. Lavrov // Chest i zakon. – 2023. – № 2 (85). – S. 5–11. – DOI: https://doi.org/10.33405/2078-7480/2023/2/85/282518

5. Cybersecurity Ventures Report on Cybercrime [Electronic resource], July 23, 2024. – Mode of access: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime

6. Gnatyuk S. Analiz krashchykh svitovykh praktyk shchodo zakhystu krytychnoi informatsiinoi infrastruktury / S. Gnatyuk, Y. Polishchuk, Y. Sotnichenko, D. Zhaksigulova // Kiberbezpeka: osvita, nauka, tekhnika : elektronne fakhove naukove vydannia. – 2020. – № 2 (10). – S. 184–196. – DOI: https://doi.org/10.28925/2663-4023.2020.10.184196

7. Komissarova N. O. Systema kiberzakhystu obiektiv krytychnoi infrastruktury v umovakh vedennia viiny / N. O. Komissarova, P. D. Krutikov // Naukovyi visnyk Kyivskoho instytutu Natsionalnoi hvardii Ukrainy. – 2024. – № 2. – S. 43–48. – DOI: https://doi.org/10.59226/2786-6920.2.2024.43-48

8. Gnatyuk S. Systema koreliuvannia podii ta upravlinnia intsydentamy kiberbezpeky na obiektakh krytychnoi infrastruktury / S. Gnatyuk, R. Berdibayev, V. Sydorenko, O. Zhyharevych, T. Smirnova // Kiberbezpeka: osvita, nauka, tekhnika : elektronne fakhove naukove vydannia. – 2023. – № 3 (19). – S. 176–196. – DOI: https://doi.org/10.28925/2663-4023.2023.19.176196

9. Papastergiou S. Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE) / S. Papastergiou, H. Mouratidis, E. M. Kalogeraki // Engineering Applications of Neural Networks (EANN 2019). Communications in Computer and Information Science / ed. by J. Macintyre, L. Iliadis, I. Maglogiannis, C. Jayne. – Springer, Cham, 2019. – Vol. 1000. – P. 476–487. – DOI: https://doi.org/10.1007/978-3-030-20257-6_41

10. Ruohonen J. From Cyber Security Incident Management to Cyber Security Crisis Management in the European Union / J. Ruohonen, K. Rindell, S. Busetti // arXiv. – 2025. – 2504.14220. – DOI: https://doi.org/10.48550/arXiv.2504.14220

11. Kozachok V. Analiz tekhnolohii rozsliduvannia intsydentiv bezpeky na obiektakh krytychnoi infrastruktury / V. Kozachok, M. Drapatyi // Kiberbezpeka: osvita, nauka, tekhnika : elektronne fakhove naukove vydannia. – 2024. – № 2 (26). – S. 374–391. – DOI: https://doi.org/10.28925/2663-4023.2024.26.699

12. Hordiienko S. B. Aktualni pytannia upravlinnia IT ryzykamy na obiektakh krytychnoi informatsiinoi infrastruktury / S. B. Hordiienko // Telekomunikatsiini ta informatsiini tekhnolohii. – 2022. – № 1 (74). – S. 29–35. – DOI: https://doi.org/10.31673/2412-4338.2022.012935

13. Doslidzhennia hlobalnykh tendentsii informatsiinoi bezpeky: osnovni vysnovky [Elektronnyi resurs] // PwC. – Rezhym dostupu: https://www.pwc.com/ua/uk/survey/2018/strengthening-digital-society-against-cyber-shocks.html

14. The National Coordination Center for Cybersecurity is stepping up cooperation with international cyber technology vendors [Electronic resource]. – Mode of access: https://rnbo.gov.ua/en/Diialnist/4658.html?PRINT

15. PDCA: Potuzhnyi instrument upravlinnia vdoskonalenniam biznesu [Elektronnyi resurs]. – 7 trav. 2025 r. – Rezhym dostupu: https://itez.com.ua/blog/pdca-cycle-business-optimization.html

16. ISO/IEC 27001:2022. Information technology – Security techniques – Information security management systems – Requirements [Electronic resource] / International Organization for Standardization. – Geneva, Switzerland, 2022. – Mode of access: https://www.iso.org/home.html

17. ISO/IEC 27002:2022. Information technology – Security techniques – Code of practice for information security controls [Electronic resource] / International Organization for Standardization. – Geneva, Switzerland, 2022. – Mode of access: https://www.iso.org/home.html

18. Skybytskyi V. Normatyvno-pravove zabezpechennia zakhystu krytychnoi infrastruktury Ukrainy vid kiberzahroz [Elektronnyi resurs] / V. Skybytskyi // Collection of Scientific Papers «ΛΌΗΟΣ», (Dec. 13, 2024; Zurich, Switzerland). – 2025. – S. 257–260. – DOI: https://doi.org/10.36074/logos-13.12.2024.055. – Rezhym dostupu: https://archive.logos-science.com/index.php/conference-proceedings/article/view/2545/2582

19. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [Elektronnyi resurs] : Zakon Ukrainy // Vidomosti Verkhovnoi Rady (VVR). – 2017. – № 45, st. 403). – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/2163-19#Text

20. Skorystaitesia nashoiu dopomohoiu z pytan zapobihannia, vyiavlennia ta usunennia naslidkiv kiberintsydentiv [Elektronnyi resurs]. – Rezhym dostupu: https://cert.gov.ua/

21. Zahalni pravyla obminu informatsiieiu pro kiberintsydenty. Protokol TLP [Elektronnyi resurs]. – Rezhym dostupu: https://cip.gov.ua/ua/news/zagalni-pravila-obminu-informaciyeyu-pro-kiberincidenti-protokol-tlp