Annual International Scientific Conference
"Competitiveness and Innovation in the Knowledge Economy"
September 26-27, 2025
Chisinau, Republic of Moldova

DOI: https://doi.org/10.24818/cike2025.59

CYBER INCIDENT MANAGEMENT: APPROACHES AND BEST PRACTICES

LIUDMYLA VOLODYMYRIVNA RYBALCHENKO
PhD, Associate Professor
Dnipropetrovsk State University of Internal Affairs, Dnipropetrovsk region, Ukraine
e-mail: luda_r@ukr.net
ORCID ID: 0000-0003-0413-8296

OLHA ANDRIIVNA HABORETS
PhD, Associate Professor
Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine
e-mail: olga-gaborets@ukr.net
ORCID ID: 0000-0001-7791-6795

Abstract: When analysing the state of the modern digital environment, it is necessary to emphasise that cyber threats pose a constant risk factor for both private companies and government institutions. It has been established that cyberattacks have become targeted, and their number is on the rise. Therefore, in order to quickly detect, respond to, and reduce the level of cyber incidents, it is necessary to create more effective mechanisms for countering and managing information security incidents.

The purpose of this article is to study cyber incidents that have a negative impact on the country's information space and pose threats to all areas of activity.

It has been found that cyber incidents vary in nature, including phishing attacks, sending spam to mailboxes, fraudulent messages, hacking private accounts, ransomware, creating complex and targeted attacks on critical infrastructure, and attacks that cause significant financial losses and lead to user distrust of the resources they use most often are also common.

The research used the methods of analysis, synthesis, evaluative and situational, comparative, graphical and generalisation.

It is becoming increasingly difficult to counter cyber threats, as with the development of information technology, fraudsters and cybercriminals are complicating and refining their methods of influence, which is why new, more effective methods of countering them are being developed.

It has been established that cyber attacks most often have political and economic factors, so such attacks pose a particular threat when high-tech means are used. Areas such as economic, social and national security are the most at risk, where cyber incidents pose a significant threat. Therefore, the development of effective and efficient strategies for managing such cyber incidents is currently a pressing issue.

The article concludes that there is a need to develop an effective and comprehensive approach to detecting, responding to, and restoring information that has been damaged after cyber incidents. It is discussed that with the increase in the level of threats, the requirements for the creation of modern approaches to integrating all important measures to ensure the resilience of digital systems to cyber threats, which have become increasingly widespread in recent years, are only possible through a combination of modern innovative technologies, the creation of effective security policies and international cooperation.

Thus, cyber incident management is a continuous process that requires the training of highly qualified cybersecurity specialists, the creation of effective technical protection, interaction between teams, and a culture of security within the organisation. In the context of growing cyber threats and crime, it is important for law enforcement agencies to develop effective strategies to combat crime and take measures to protect the rights and freedoms of every citizen and the security of the entire state.

Keywords: cyber incidents, technological innovations, security policy, digital systems, cyber attacks, confidential information
JEL Classification: G14, H56, L86

INTRODUCTION

The purpose of the article is to reveal the essence of the process designed for effective cyber incident management, to create important directions for the development of measures, methods and mechanisms aimed at preventing incidents, responding to possible cyber attacks and managing them using modern innovative technologies.

An important aspect in this area is the development of a regulatory framework, regulatory documents, and the updating of the existing legislative framework for the reliable and effective management of information security incidents.

Even the best information security infrastructure cannot guarantee the absence of intrusions or other harmful, malicious actions. The information security management system (ISMS) is part of the overall management system based on business risk assessment for the creation, implementation, operation, continuous monitoring, analysis, support and improvement of information security (IS). An incident in an information security system is considered to be an undesirable (unexpected) event or series of events in the security system that could jeopardise business operations and the protection of certain information. The speed with which an organisation can identify, analyse, prevent and respond to incidents will limit the damage caused and reduce recovery costs.

Presentation of the main research material

Computer security incident management is the process of identifying, analysing and responding to events that pose a threat to information systems. Effective incident management is based on a combination of human resources, technical infrastructure and tools that enable an organisation to detect, localise and neutralise threats in a timely manner.

To ensure an adequate response to cyber incidents, specialised teams are created to manage security events. Their responsibilities include developing clear response procedures, defining roles and areas of responsibility, providing the necessary technologies and security measures, and training personnel to respond quickly in crisis situations.

In 2024, the implementation of malware in emails increased by 349% compared to the previous year worldwide (Department of Cyber Police..., 2024).

In today's digital world, cyber incidents pose one of the most serious threats to all areas of activity — from small businesses to large government agencies and critical infrastructure facilities. Despite the advantages of digitalisation, it creates new vulnerabilities that attackers can exploit to gain unauthorised access to confidential information, manipulate data or disrupt important systems.

A cyber incident is any event that could compromise the confidentiality, integrity or availability of information or information resources. Such events can be either intentional (e.g., phishing, malware, DDoS attacks, or insider actions) or accidental (e.g., equipment failures or user errors).

International standards are used to build an effective cyber incident response system, in particular NIST SP 800-61, which defines incident management as a continuous process.

Companies entering international markets need to prove their reliability in the field of cybersecurity. This requires compliance with international standards such as ISO/IEC 27001 and PCI DSS, as well as adherence to best practices and regulatory requirements such as NIST CSF, NIS2, SOC 2, DORA, CCPA, etc. In Europe, there is a particular focus on protecting personal data and improving the cyber resilience of critical enterprises, which is regulated by the GDPR and NIS2 acts.

The cyber incident management process is usually divided into four main phases:

1. Preparation — creating policies, procedures, and technical response tools.
2. Detection & Analysis — identifying incidents and determining their scope.
3. Response (Containment, Eradication & Recovery) — isolating, eliminating the threat and restoring systems.

4. Post-Incident Activity — analysing causes, assessing consequences and improving protective mechanisms.

In 2025, Ukraine continues to face a hybrid war involving large-scale cyberattacks on government agencies and critical infrastructure. During this period, CERT-UA actively responds to incidents, including attacks on energy systems, financial institutions, and military networks.

In April 2025, a DDoS attack on the country's power grid was recorded, aimed at disrupting the power supply to several large cities. Thanks to the prompt actions of CERT-UA and cooperation with international partners, in particular CISA (USA), the attack was stopped at an early stage, vulnerabilities were eliminated, and systems were restored within a few hours.

This incident contributed to the emergence of international cooperation initiatives aimed at creating new backup communication channels, which are extremely necessary during military operations, in order to facilitate an effective response to large-scale cyber threats.

Since cyberattacks are a frequent occurrence and critical infrastructure and government information systems must be reliably protected, the latest measures have been implemented to strengthen the protection of information and communication systems. An important area of focus has been the development of a digital platform designed to monitor cyber threats, detect suspicious activity, and implement mechanisms to respond to cyber threats in real time.

In the summer of 2025, a group of international terrorists planned a cyberattack targeting the energy infrastructure of several states. Such suspicious cyber activity was detected thanks to the effective work of special services and the use of security system monitoring, which made it possible to avoid negative consequences and ensure the uninterrupted operation of energy systems.

In addition, an attempt to leak confidential information through a phishing attack on a platform belonging to government agencies and designed for data exchange between them was detected, blocked and prevented in a timely manner.

This case became the basis for the development of a new strategy for responding to cyberterrorism, which made it possible to improve the speed of response for cyber defence through the use of international cooperation. Thus, international cooperation in overcoming and combating cyberterrorism consists of concerted efforts between public and private entities, which make it possible to prevent potential large-scale attacks and create a reliable system for international cybersecurity.

Results and discussion

In their work, Rybachenko et al. (2022) draw attention to the information protection system that belongs to the organisational structure, stating that in order to create effective protection of information from cyber incidents, it is necessary to ensure constant monitoring using innovative technologies. To ensure Ukraine's information security, it is important to create a set of organisational and technical measures that will become effective means of protection against cybercrime worldwide. It is noted that only together with European countries can reliable protection be built, including through the introduction of appropriate laws regulating activities in the field of cyber protection. The European Union Directive on Network and Information Security (NIS2), which is a document on protection against cyber incidents, sets out the basic requirements for security in the digital system and the creation of protective measures in the field of cybersecurity (2022).

Research shows that in 2023, the number of detected malicious and phishing attacks increased by 27% compared to 2022. It has been established that the greatest risk occurred due to access to cloud applications, where nearly 83 billion access attempts were recorded (Dovhan et al., 2024).

It is noted that countering cyber threats is an integral part of ensuring Ukraine's national security in the field of information security and is a priority task for the effective protection of the state (Kolosovsky, 2023).

The theft of personal data and information leaks have a significant impact on the state of insecurity and reduce the level of data confidentiality (Sverdlyk, 2022).

My personal contribution is proposals to update the existing regulatory and legislative framework for reliable and effective management of information security incidents. Cybersecurity issues are relevant in the context of the modern development of the information society, the growth of cybercrime, and are particularly important in preventing the consequences of the use of cyberterrorism in hybrid wars. Therefore, it is necessary to build a cybersecurity system for Ukraine, taking into account the rapid trends in the development of cyberspace, modern challenges, and threats to its security.

Conclusion

Most European countries will work on implementing new European cybersecurity legislation regarding the currently voluntary option for businesses to certify that their products comply with EU cybersecurity standards. The European Commission will regularly assess the need to make a particular certification scheme mandatory. The certification scheme used may define one or more levels of security: basic, substantial or high.

At the basic level, ICT manufacturers or service providers will be able to carry out conformity assessments themselves. In the case of significant or high levels of assessment, this will be carried out by national cybersecurity certification bodies. EU Member States will develop rules on penalties for violations of the EU Cybersecurity Certification Framework and Schemes and will grant broader powers to cybersecurity authorities to ensure cooperation and the application of ENISA recommendations.

Cyber incident management is not a one-off action, but a continuous, cyclical process that requires technical training, clear policies, interaction between teams and, most importantly, a culture of security within the organisation. In the face of growing cyber threats, only those companies that are prepared for attacks will be able to effectively protect their assets, reputation and customer trust.

References:

1. ISO/IEC 27035:2020-2024 — Information technology — Information security incident management. https://www.iso27001security.com/html/27035.html
2. Rybalchenko, L., & Ohrimenco, S. (2024). The impact of cybersecurity and crime on national security. Philosophy, Economics and Law Review, 4(2), 62-72. doi: 10.31733/2786-491X-2024-2-62.
3. Rybalchenko, L., & Grebinyuk, A.M. (2020). Fundamentals of Information Security Management: Textbook. - Dnipro: Dnipro State University of Internal Affairs. – 144 c.
4. Department of Cyber Police of the National Police of Ukraine. (2024). Retrieved from https://cyberpolice.gov.ua.
5. Rybalchenko L.V., & Kosychenko O.O., & Klinitskyi I.I. Ensuring economic security of enterprises taking into account the peculiarities of information security. *Philosophy, Economics and Law Review*. Volume 2, no. 1, 2022 p. 96-102. doi:10.31733/2078-3566-2022-5-121-126
6. Directive of the European Parliament and of the Council No. 2022/2555 "On Network and Information Security (NIS2) and the operation of the domain name system DNS". (2022, December). Retrieved from https://www.nis-2-directive.com/.
7. European Union Agency for Network and Information Security. (2022). Retrieved from https://www.enisa.europa.eu/.
8. Dovhan, O., & Lytvynova, L., & Dorohykh, S. (2024). *Cybersecurity in the information society: Information and analytical digest*. Kyiv: State Scientific Institution "Institute of Information, Security and Law of the National Academy of Sciences of Ukraine"; Vernadsky National Library of Ukraine.
9. Kolosovskyi, E. (2023). The current state of cybersecurity of Ukraine in the conditions of wartime. *Legal Scientific Electronic Journal*, 12, 402-405. doi: 10.32782/2524-0374/2023-12/100.
10. Sverdlyk, Z. (2022). Cybersecurity and cyber defence: Issues on the agenda in Ukrainian society. *Ukrainian Journal of Library and Information Science*, 10, 175-188. doi: 10.31866/2616-7654.10.2022.269495.