DOI (Issue): https: //doi.org/10.36486/np.2022.3(57) Issue 3(57) 2022

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Гладиш С.В.* Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах. *Реєстрація, зберігання і обробка даних*. 2008. Т. 10. № 1. С. 116–124.

2. Рекомендация МСЭ-Т X.1216 (09/2020) "Требования к сбору и сохранению доказательств инцидентов кибербезопасности". URL: https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-X.1641-201609-I!!PDF-R&type=items (дата звернення: 12.09.2022).

3. *Козаченко П.П., Панаско О.М.* Управління інцидентами в контексті інформаційної безпеки підприємства. *Specialized and multidisciplinary scientific researches*. Vol. 2. P. 119–120 (дата звернення: 12.09.2022).

4. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури: наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 р. № 601. URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciinoyi-infrastrukturi (дата звернення: 13.09.2022).

5. *Довгань О.Д., Тарасюк А.В.* Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. *Інформація і право*. 2018. № 3 (26). С. 94–103.

6. Управління інцидентами інформаційної безпеки. URL: https://studfile.net/preview/16435760/ (дата звернення: 12.09.2022).

7. Нові стандарти для інформаційної безпеки: ДП "Волинський науково-виробничий центр стандартизації, метрології та сертифікації". URL: http://volynstandart.com.ua/info_security/4193/news/ (дата звернення: 13.09.2022).

8. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. К.: НІСД, 2018. 84 с.

9. Кібербезпека і інформаційна безпека. Стандарт ISO/IEC 27032. URL: https://ua.ikmj.com/cybersecurity-and-information-security-iso-iec-27032/ (дата звернення: 12.09.2022).

10. *Дрюков В.* Управление инцидентами и событиями информационной безопасности. URL: https://safe-surf.ru/specialists/article/5236/611719/ (дата звернення: 11.09.2022).

REFERENCES

1. *Hladysh S.V.* (2008). Reiestratsiia, zberihannia i obrobka danykh. "Support for decision-making regarding the management of information security incidents in organizational and technical systems". No 1. P. 116–124 [In Ukrainian].

2. Rekomendatsiia MSE-T X.1216 (09/2020) "Trebovaniia k sboru y sokhraneniiu dokazatielstv intsydientov kybierbiezopasnosti". "Requirements for Collecting and Preserving Evidence of Cybersecurity Incidents". (09/2020). Recommendation ITU-T X.1216. URL: https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-X.1641-201609-I!!PDF-R&type=items. (Date of Application: 12.09.2022) [In Russian].

3. *Kozachenko P.P., Panasko O.M.* Upravlinnia intsydentamy v konteksti informatsiynoi bezpeky pidpryiemstva. "Incident management in the context of enterprise information security". Specialized and multidisciplinary scientific researches, No 2. P. 119–120. [In Ukrainian].

4. Pro zatverdzhennia Metodychnykh rekomendatsii shchodo pidvyshchennia rivnia kiberzakhystu krytychnoi informatsiinoi infrastruktury. "Order of the State Special Communications Administration On the approval of Methodological recommendations for increasing the level of cyber protection of critical information infrastructure from October 6 2021, No 601". URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciinoyi-infrastrukturi. (Date of Application: 12.09.2022) [In Ukrainian].

5. *Dovhan O.D., Tarasjuk A.V.* (2018). Hlobalna kultura kiberbezpeky v systemi zapobihannia kiberzlochynnosti v Ukraini. "Global culture of cyber security in the system of cybercrime prevention in Ukraine". Informatsiia i pravo. No 3. P. 94–103. [In Ukrainian].

6. Upravlinnia intsydentamy informatsiinoi bezpeky. "Management of information security incidents". URL: https://studfile.net/preview/16435760/. (Date of Application: 12.09.2022) [In Ukrainian].

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).19

7. Novi standarty dlia informatsinoi bezpeky. “New standards for information security”: SE “Volyn Scientific and Industrial Center for Standardization, Metrology and Certification”. URL:http://volynstandart.com.ua/info_security/4193/news/. (Date of Application: 13.09.2022) [In Ukrainian].
8. *Dubov D.* (Eds.). (2018). Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy. “Public-private partnership in the field of cyber security”: international experience and opportunities for Ukraine. Kyiv: NISD. 84 p. [In Ukrainian].
9. Kiberbezpeka i informatsiyna bezpeka. “Cyber security and information security”. ISO/IEC 27032 standard. URL: https://ua.ikmj.com/cybersecurity-and-information-security-iso-iec-27032/. (Date of Application: 12.09.2022) [In Ukrainian].
10. *Driukov V.* Upravlieniie intsydientami i sobytyyamy informatsionnoi biezopasnosti. “Information security incident and event management”. URL: https://safe-surf.ru/specialists/article/5236/611719/. (Date of Application: 11.09.2022) [In Russian].

UDC 343.973

Sakharova Olena,
Candidate of Juridical Sciences, Senior Research Officer, Head of the Department,
State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0002-9759-5324

ESSENCE AND CONTENT OF THE CYBER INCIDENT INVESTIGATION PROCEDURE IN ACCORDANCE WITH ISO AND NIST INTERNATIONAL STANDARDS

The article reveals the essence and content of the procedure for investigating cyber incidents in accordance with the international standards ISO and NIST. In particular, according to ISO/IEC 27042:2015, the author provides a definition of the concept of “investigation of cyber incidents” and provides the stages of the procedure for investigating a cyber incident. The article systematically analyzes the content of an intelligent decision support system for managing cyber incidents. At the same time, the author focuses on the fact that the system of cyber protection measures should be based on regulatory documents, national and international standards, established practices for protecting information and ensuring cyber security, which develop along with cyber security technologies.

The analysis of the organizational and technical model of cyber defense, the identification and investigation of cyber incidents and cyber crimes, based on international risk-oriented cyber security management standards: ISO/IEC 27032: 2012 “Information technology. Security techniques. Guidelines for cybersecurity”, ISO/IEC 27037:2012 “Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence”, ISO/IEC 27041:2015 “Guidance on assuring suitability and adequacy of incident investigative method”, ISO/IEC 27043:2015 “Information technology. Security techniques. Incident investigation principles and processes”, Recommendations of the International Telecommunication Union MCE-T X.1216 (09/2020) “Requirements for the collection and preservation of evidence of cybersecurity incidents”.

In the process of conducting the study, the author also emphasizes that the international standard NIST SP 800-61 “Computer security incident handling guide”

presents a collection of "best practices" for building processes for processing, managing and responding to cyber incidents.

At the end of the article, the author comes to the conclusion that today in Ukraine a number of regulatory documents on the technical protection of information (ND TZI), as well as on a comprehensive system of information protection, are obsolete and have proven to be ineffective for many years, so it is advisable to introduce an information management system security in accordance with the ISO/IEC 27000 series of standards, which allows you to optimize the process of protecting information resources and managing risks for these resources.

Keywords: cyber incidents, ISO and NIST international standards, cyber incident investigation, cyber attacks, cyber crimes, cyber incident investigation procedure.

Отримано 10.10.2022