UDC 004.056.5

METHODS FOR DETERMINING THE CATEGORIES OF CYBER INCIDENTS AND ASSESSING INFORMATION SECURITY RISKS

Kopytsia Oleksandr, Uzlov Dmytro

V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine
oleksandr.kopytsia@student.karazin.ua, dmytro.uzlov@karazin.ua

Received: on November 2023. Accepted: on December 2023.

Abstract: *The article is devoted to the study of categories of cyber incidents and their prioritization in the context of information security. It discusses the main sources that provide information about cyber threats and defines their role in detecting and analyzing incidents, and provides tools for collecting and analyzing data. The concepts of event, incident, and crime and the relationship between them are discussed. The author provides a classification of various types of cyber threats, how they are coded, their characteristics and impact on information systems. Examples of the use of cyber incident classification are given. The authors of the article also consider specific types of cyber incidents that may occur in various fields of activity and the threats they pose to various information systems. The necessity and methods of determining priorities in responding to cyber threats are substantiated, which allows for the effective allocation of resources and the implementation of preventive cyber security measures. The approach to assessing and classifying incidents according to their possible impact on the organization's activities, information security and ability to recover from cyber attacks is revealed. The article highlights various approaches and methodologies for identifying and managing information security risks, including the use of standards, models and assessment tools. This article is a resource for cybersecurity professionals, researchers, and executives interested in risk management and information asset protection in today's digital environment.*

Keywords: *Cyber Security, Cyber Incident, Intrusion Detection System, Categories of Cyber Incidents, Prioritization of Incidents, Information Security Risks.*

1. Introduction

Cybersecurity in today's world is defined as a critical component of security as our society becomes increasingly digital. Means of protecting personal information, information systems and data of corporations and financial institutions, government agencies and critical infrastructure help to reduce the risks of cyberattacks and their consequences. Given the rapid technological development, the importance of cybersecurity is increasing as new technologies, such as the Internet of Things and artificial intelligence, create new vulnerabilities that require effective protection strategies. Thus, cybersecurity is becoming essential to ensure stability, protect personal information and national interests, requiring cooperation between government, business and civil society to develop and implement effective measures.

Prioritizing the handling of cyber incidents depending on the risks they pose to information systems is a crucial element of effective cyber defense. This allows cybersecurity professionals to optimize the use of resources, directing them to the most critical scenarios and minimizing possible losses for the organization. Rapid response to high-risk cyber incidents ensures that critical systems remain functional and helps to avoid negative consequences for business processes. Taking risks into account also helps to take preventive measures, improve security strategies, and comply with regulatory requirements. This systematic approach to cybersecurity management allows it to effectively detect, respond to, and prevent cyber threats, providing reliable protection for information systems and preserving the organization's reputation.

2. Detecting cyber security incidents

Collecting and analyzing data on cyber incidents is a task that presents a number of challenges and complexities. First, information about cyber threats can be scattered across a variety of sources, such as system logs, network data, information from antivirus systems, vulnerability reports, etc.

This requires the development of a comprehensive strategy for collecting and integrating data from various sources.

An additional challenge is that attackers are constantly improving their methods, using new technologies and tactics to evade detection. This poses a challenge for cybersecurity analysts: to constantly update their knowledge and tools to effectively detect and analyze new threats.

When it comes to tools for collecting and analyzing cyber incident data, there are a variety of software and hardware tools. Software tools include security intrusion detection systems (*SIEMs*), which provide centralized log collection and analysis, as well as intrusion detection systems (*IDSs*) and vulnerability detection systems (*VDSs*). Some platforms, such as Splunk, ELK Stack, or IBM QRadar, allow you to aggregate data from different sources and provide event correlation capabilities to identify potential threats.

There are also advanced tools for analyzing network traffic, such as Wireshark, or for detecting anomalies in systems, such as Darktrace. It is also important to use intelligent data analysis systems based on artificial intelligence (*AI*) to automatically detect anomalies and patterns that may indicate cyber threats.

The following event logs can be used by an organization to assist with detecting and investigating cyber security incidents [1]:

- Cross Domain Solutions: May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.
- Databases: May assist in identifying anomalous or malicious application or user behavior indicating an exploitation attempt or successful compromise.
- Domain Name System services: May assist in identifying attempts to resolve malicious domain names or Internet Protocol (IP) addresses indicating an exploitation attempt or successful compromise.
- Email servers: May assist in identifying users targeted with phishing emails thereby helping to identify the initial vector of a compromise.
- Gateways: May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.
- Multifunction devices: May assist in identifying anomalous or malicious user behavior indicating a cyber security incident or malicious insider activity.
- Operating systems: May assist in identifying anomalous or malicious activity indicating an exploitation attempt or successful compromise.
- Remote access services: May assist in identifying unusual locations of access or times of access indicating an exploitation attempt or successful compromise.
- Security services: May assist in identifying anomalous or malicious application or network traffic indicating an exploitation attempt or successful compromise.
- Server applications: May assist in identifying anomalous or malicious application behavior indicating an exploitation attempt or successful compromise.
- System access: May assist in identifying anomalous or malicious user behavior indicating an exploitation attempt or successful compromise.
- User applications: May assist in identifying anomalous or malicious application or user behavior indicating an exploitation attempt or successful compromise.
- Web applications: May assist in identifying anomalous or malicious application or user behavior indicating an exploitation attempt or successful compromise.
- Web proxies: May assist in identifying anomalous or malicious network traffic indicating an exploitation attempt or successful compromise.

3. Categories of cyber incidents

Not all events recorded in logs are directly indicative of cyber incidents, and this is due to several factors. First, log files include a wide range of information that can be the result of normal system or network operation. Many events can be related to normal operations, system updates, or even erroneous questions from users. Secondly, not every unusual or anomalous event is a cyber incident. Some anomalies can be the result of temporary system malfunctions, misconfigurations, or random events. Without the proper context and analysis, it is difficult to determine whether an event poses a real cybersecurity threat.

For the purpose of defining categories of incidents it is important to have a clear concept of the different scopes of an event, an incident and a crime.

An event can be defined as any observable occurrence that happened at a point in time in a system or network, especially one of importance. Thus, an event does not necessarily imply an adverse situation or a malicious activity [2].

For instance, «*to send an email*» or «*to make a phone call*» are events with no malicious implication.

On the other hand, a security incident necessarily implies a human-caused adverse event, usually with a malicious nature, which is oriented to cause a disruption of any system or network.

It is important to underline that incidents arising from negligence, as well as attempts that fail, also fall under the concept of a security incident. Examples of security incidents are «*SQL injection*» or «*Cross-Site Scripting*» attacks.

As can be observed below in Fig. 1, any security incident is considered an event but not any event is considered a security incident.

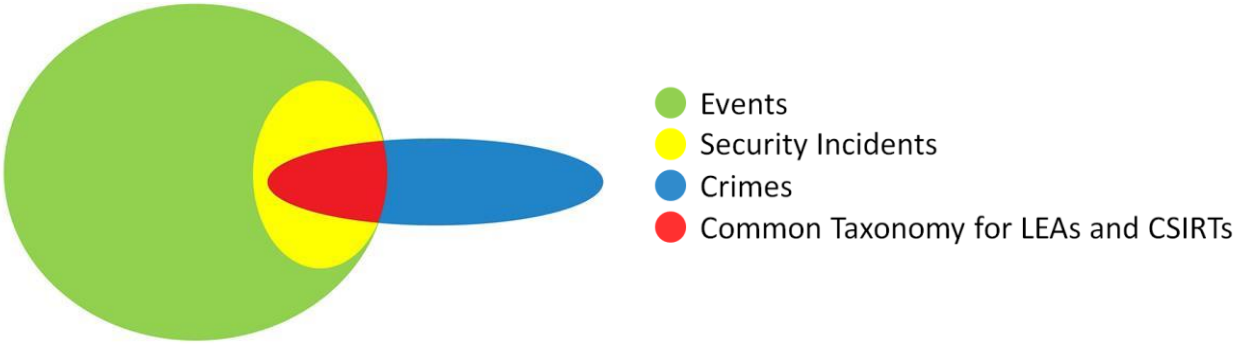

Fig 1 - Events, Security incidents, Crimes and Common Taxonomy ecosystem

Also not every security incident has a crime penalty, therefore only the security incidents able to be criminally prosecuted will be the ones falling under the scope of Common Taxonomy for *LEAs* and *CSIRTs* To clarify this, see the Fig. 1 below.

Different categories of cyber incidents manifest themselves in different ways in information systems and have different impacts on them. The threat level of a cyber incident may depend on its category. There are many different lists of cyber incident categories that take into account different aspects and characteristics of digital threats such as the type of attack, privacy impact, attack targets, and methods used by attackers. For example, the State Service for Special Communications and Information Protection of Ukraine provides the following list, which is developed using and complies with the recommendations of the *European Cyber Security Agency* (*ENISA Reference Incident Classification Taxonomy*), as well as the joint document of ENISA and the *European Cybercrime Centre Europol* (*Common Taxonomy for Law Enforcement and The National Network of CSIRTs*) [3].

According to the Table 1, a cyber incident can be described using the incident category code and the incident type code:

Example 1: Incident code: 01.01; Incident type: Spam.

Example 2: Incident code: 02.04; Incident type: Malicious connection.

Table 1 - Categories of cyber incidents

Code xx	Incident category	Code xx	Type of incident	Description of the type of incident
1	*2*	*3*	*4*	*5*
01.	**Abusive content**	01	Spam	*Sending unwanted messages or a large number of messages (flooding)*
02.	**Malicious Code**	01	Malware infection	*Spyware detected in the system*
		02	Malware distribution	*Distributing spyware, for example, by sending out emails containing malware attachments or links to download it.*
		03	Command & Control (C2)	*A system that is used as a command and control point for a botnet and/or serves as a collection point for information stolen by botnets.*
		04	Malicious connection	*Connection attempts from/to IP/URL - an address associated with a known spyware, such as C2C, or a distribution resource for components associated with a particular botnet activity.*
03.	**Information Gathering**	01	Scanning	*Collecting information about systems or networks.*
		02	Sniffing	*Unauthorized interception (logical or physical) and analysis of network traffic. Unauthorized monitoring and reading of network traffic.*
		03	Phishing	*An attempt to collect information about a user or system using social engineering techniques (mass emails aimed at collecting data, may contain links to phishing sites)*
04.	**Intrusion Attempts**	01	Vulnerability exploitation attempt	*Attempted intrusion by exploiting a vulnerability in a system, component, or network*
		02	Login attempts	*An attempt to log in to services or authentication/access mechanisms. An unsuccessful attempt to match authentication credentials or use previously compromised credentials that are no longer relevant.*

Continuation of the Table 1

1	*2*	*3*	*4*	*5*
05.	**Intrusion**	01	Account compromise	*Actual intrusion into a system, component or network by compromising a user or administrator account*
		02	System compromise	*An actual intrusion into a system or its component, service, or application through the exploitation of a vulnerability in a component or network. Unauthorized access to a system or component bypassing the access control system.*
06.	**Availability**	01	DoS/DDoS	*An impact on the normal functioning of a system or service that is achieved by sending requests from one or more sources to the target resource to overload the bandwidth or system resources.*
		02	Sabotage	*Actions (intentional or unintentional) aimed at damaging the system, interrupting processes, changing or deleting information, etc.*
		03	Outage, no malice	*Failure of a system or its components without malicious interference.*
07.	**Information Content Security**	01	Unauthorized access to information	*Unauthorized access to information. Unauthorized sharing of a specific set of information.*
		02	Unauthorized modification of info	*Unauthorized modification or deletion of a certain set of information.*
08.	**Fraud**	01	Fraudulent site	*Creating phishing sites to collect authentication or other user data. Using the institution's resources for purposes other than those intended.*
09.	**Vulnerable**	01	Vulnerability	*The presence of known vulnerabilities in the system or its components that are open to exploitation.*
		02	Misconfiguration	*Flaws in the settings that can be exploited by an attacker (default settings, etc.).*
10.	**Other**	01	Undetermined incident	*Insufficient data to process the incident.*

4. Incident prioritization

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following [4]:

- Functional Impact of the Incident. Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems. Incident handlers should consider how the incident will impact the existing functionality of the affected systems. Incident handlers should consider not only the current functional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained.
- Information Impact of the Incident. Incidents may affect the confidentiality, integrity, and availability of the organization's information. For example, a malicious agent may exfiltrate sensitive information. Incident handlers should consider how this information exfiltration will impact the organization's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertained to a partner organization.
- Recoverability from the Incident. The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances it is not possible to recover from an incident (*e.g., if the confidentiality of sensitive information has been compromised*) and it would not make sense to spend limited resources on an elongated incident handling cycle, unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an incident may require far more resources to handle than what an organization has available. Incident handlers should consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.

Combining the functional impact to the organization's systems and the impact to the organization's information determines the business impact of the incident—for example, a distributed denial of service attack against a public web server may temporarily reduce the functionality for users attempting to access the server, whereas unauthorized root-level access to a public web server may result in the exfiltration of *personally identifiable information* (*PII*), which could have a long-lasting impact on the organization's reputation.

The recoverability from the incident determines the possible responses that the team may take when handling the incident. An incident with a high functional impact and low effort to recover from is an ideal candidate for immediate action from the team. However, some incidents may not have smooth recovery paths and may need to be queued for a more strategic-level response—for example, an incident that results in an attacker exfiltrating and publicly posting gigabytes of sensitive data has no easy recovery path since the data is already exposed; in this case the team may transfer part of the responsibility for handling the data exfiltration incident to a more strategic-level team that develops strategy for preventing future breaches and creates an outreach plan for alerting those individuals or organizations whose data was exfiltrated. The team should prioritize the response to each incident based on its estimate of the business impact caused by the incident and the estimated efforts required to recover from the incident [5]. An organization can best quantify the effect of its own incidents because of its situational awareness.

Table 2 provides examples of functional impact categories that an organization might use for rating its own incidents. Rating incidents can be helpful in prioritizing limited resources.

Table 3 provides examples of possible information impact categories that describe the extent of information compromise that occurred during the incident. In this table, with the exception of the "None" value, the categories are not mutually exclusive and the organization could choose more than one.

Table 2 – Functional Impact Categories

Category	Definition
None	*No effect to the organization's ability to provide all services to all users*
Low	*Minimal effect; the organization can still provide all critical services to all users but has lost efficiency*
Medium	*Organization has lost the ability to provide a critical service to a subset of system users*
High	*Organization is no longer able to provide some critical services to any users*

Table 3 – Information Impact Categories

Category	Definition
None	*No information was exfiltrated, changed, deleted, or otherwise compromised*
Privacy Breach	*Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated*
Proprietary Breach	*Unclassified proprietary information, such as protected critical infrastructure information (PCII),was accessed or exfiltrated*
Integrity Loss	*Sensitive or proprietary information was changed or deleted*

Table 4 shows examples of recoverability effort categories that reflect the level of and type of resources required to recover from the incident.

Table 4 - Recoverability Effort Categories

Category	Definition
Regular	*Time to recovery is predictable with existing resources*
Supplemented	*Time to recovery is predictable with additional resources*
Extended	*Time to recovery is unpredictable; additional resources and outside help are needed*
Not Recoverable	*Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation*

5. Criticality levels of cyber incidents

Taking into account the above, the following consider a list of criticality levels of cyber incidents developed by the State Service for Special Communications and Information Protection of Ukraine [6]:

- *level 0, non-critical (white)* - a cyber incident/cyber attack does not threaten the sustainable, reliable and normal operation of information, electronic communication, information and communication systems, technological systems;
- *level 1, low (green)* - a cyber incident/cyber attack directly threatens the sustainable, reliable and normal operation of information, electronic communication, information and communication systems, technological systems, but does not threaten the security (*confidentiality, integrity and availability*) of information and data processed by them;
- *level 2, medium (yellow)* - a cyber incident/cyber attack directly threatens the sustainable, reliable and normal operation of information, electronic communication, information and communication systems, technological systems, which creates prerequisites for violating the security (*confidentiality, integrity and availability*) of information and data processed by

them, and creates prerequisites for the termination of functions and/or provision of services by critical infrastructure;

- *level 3, high (orange)* - a cyber incident/cyber attack directly threatens the stable, reliable and normal operation of information, electronic communication, information and communication systems, technological systems, violates the security *(confidentiality, integrity and availability)* of information and data processed by them, resulting in potential threats to national security and defense, the state of the environment, the social sphere, the national economy and its individual sectors, and the termination of business. Response at this level may require the involvement of forces and means of more than one main actor of the national cybersecurity system;
- *level 4, critical (red)* - a cyber incident/cyber attack directly threatens the stable, reliable and normal operation of several information, electronic communication, information and communication systems, technological systems, violates the security (confidentiality, integrity and availability) of information and data processed by them, resulting in real threats to national security and defense, the state of the environment, the social sphere, the national economy and its individual sectors, and the cessation of A cyber incident/cyber attack may have a cross-border impact. Response at this level requires the involvement of forces and means of the main actors of the national cybersecurity system;
- *level 5, emergency (black)* - a cyber incident/cyber attack directly threatens the sustainable, reliable and normal operation of a significant number of information, electronic communication, information and communication systems, technological systems, violates the security *(confidentiality, integrity and availability)* of information and data processed by them, resulting in imminent threats to the full functioning of the state or threats to the lives of Ukrainian citizens. A cyber incident/cyber attack may have a cross-border impact. Response at this level requires maximum involvement of the forces and means of the main actors of the national cybersecurity system and other cybersecurity actors.

6. Information security risk assessment methods

The development of Information Security Risk Assessment methods is a key element of effective cybersecurity and risk management in the modern information environment. This is important due to the complexity of cyber threats that are constantly changing and evolving. Today's information environment faces diverse and ever-changing cyber threats, and creating risk assessment methods helps identify, analyze, and manage these threats. Attackers are constantly developing new methods and techniques, so it is important to have effective methods to identify, assess, and manage these threats. Information is one of the most valuable assets for many organizations, so risk assessment methods help determine which data is most valuable and vulnerable. This makes it possible to develop strategies to protect it effectively.

Most organizations have limited resources, so it's important to allocate those resources effectively to maximize security. Risk assessment methods help to prioritize and cost cybersecurity measures. The risk assessment also takes into account compliance and regulatory requirements, helping to determine how well existing standards are met and where improvements can be made. The idea that risk assessment is a tool for proactively identifying potential problems and solving them before they lead to cyber incidents is important. Creating risk assessment methods is a strategically important task for any organization seeking to ensure reliable cybersecurity and reduce the impact of information threats.

There are a significant number of Information Security Risk Assessment (*ISRA*) methods that have been developed by various organizations. These methods help to identify, analyze and manage risks to ensure effective cyber defense:

- CIRA is a risk assessment method developed primarily by Rajbhandari and Snekkenes [7]. CIRA frames risk regarding conflicting incentives between stakeholders, such as information asymmetry situations and moral hazard situations. It focuses on the stakeholders, their actions and perceived outcomes of these actions.
- CORAS is a UML (*Unified Modeling Language*) model-based security risk analysis method developed for InfoSec. CORAS defines a UML-language for security concepts such as threat, asset, vulnerability, and scenario, which is applied to model incidents.
- The CCTA Risk Analysis and Management Method (*CRAMM v.5*) is a qualitative *ISRA* method. *CRAMM* is specifically built around the supporting tool with the same name and refers to descriptions provided in the repositories and databases present in the tool.
- FAIR (*Factor Analysis of Information Risks*) is a risk assessment method and one of the few primarily quantitative *ISRA* approaches. FAIR breaks risks down into twelve specific factors, which contains four well-defined factors for the loss and probability calculations. FAIR includes ways to measure the factors and to derive quantitative analysis results.
- The Norwegian National Security Authority Risk and Vulnerability Assessment (*NSM ROS*) [8] approach was designed for aiding organizations in their effort to become compliant with the Norwegian Security Act.
- OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) Allegro methodology is the most recent method of the *OCTAVE*-family, aimed at being less extensive than the previous installments of *OCTAVE*. It is a lightweight version of the original *OCTAVE* and was designed as a streamlined process to facilitate risk assessments without the need for InfoSec experts and still produce robust results.
- ISO/IEC 27005:2011 - Information technology, Security techniques, Information Security Risk Management details the complete process of *ISRM/RA*, with activities with each task. Centers on assets, threats, controls, vulnerabilities, consequences and likelihood.
- The current installment of the NIST SP 800-30 - Guide for Conducting Risk Assessments is at revision one, and was developed to further statutory responsibilities under the Federal Information Security Management Act. NIST SP 800-30 rev. one was designed for larger and complex organizations. The purpose of the publication was to produce a unified information security framework for the U.S. federal government, and the framework shows signs of being created to manage complexity.
- The ISACA (*Information Systems Audit and Control Association*) Risk IT Framework and Practitioner Guide is an *ISRM/RA* approach where the Practitioner Guide complements the Risk IT Framework. The former provides examples of how the concepts from the framework can be realized. It is an established approach developed by *ISACA*, based on ValIT and CobIT, and, therefore, has a business view on risks, defining several risk factors.
- Privacy impact assessments are methods that are supposed to address risks to privacy in a system or a project. The Norwegian Data Protection Authority's (*Datatilsynet*) Risk Assessment of Information Systems (*RAIS*) are *ISRA* guidelines that primarily are designed for aiding data handlers in their effort to become compliant with the Norwegian Data Protection and Privacy Act and corresponding regulations.
- Outsourcing services to the cloud brings new risks to the organization. Microsoft's Cloud Risk Decision Framework is a method for risk assessing cloud environments [9].

7. Conclusions

Detecting and analyzing cyber incidents is a task that requires significant resources and a wide range of data from a variety of sources. Analysts and cybersecurity professionals need to quickly collect, process, and analyze information to effectively detect and respond to cyber threats. Determining the categories of cyber incidents and their criticality levels is a complex process that also requires significant resources. This is an important component of properly classifying and prioritizing incidents to ensure a fast and effective response to the most critical events. Improving the cyber incident response process is driven by a large number of developed information security risk assessment methods. These methods allow organizations to effectively identify, assess and manage risks, as well as improve their security strategies. The application of these methods contributes to a more accurate and systematic approach to cybersecurity management and ensures reliable protection of information assets.

References

[1] ASD's ACSC - Guidelines for Cyber Security Incidents. Access mode: http://surl.li/pslnn
[2] ENISA, EUROPOL - Common Taxonomy for Law Enforcement and The National Network of CSIRTs - Access mode: https://www.europol.europa.eu/sites/default/files/documents/common_taxonomy_for_law_enforcement_and_csirts_v1.3.pdf
[3] CERT-UA - List of categories of cyber incidents. Access mode: https://cert.gov.ua/recommendation/16904
[4] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. Access mode: http://www.itref.ir/uploads/editor/d3d149.pdf
[5] NIST Special Publication 800-61 rev.2 Computer Security Incident Handling Guide. Access mode: https://csrc.nist.gov/pubs/sp/800/61/r2/final
[6] Resolution of the Cabinet of Ministers of Ukraine dated 04.04.2023 No. 299, Some issues of response by cybersecurity entities to various types of events in cyberspace. Access mode: https://zakon.rada.gov.ua/laws/show/299-2023-п
[7] Einar Snekkenes. Position paper: Privacy risk analysis is about understanding conflicting incentives. In Simone Fischer-Haubner, Elisabeth Leeuw, and Chris Mitchell, editors, *Policies and Research in Identity Management, volume 396 of IFIP Advances in Information and Communication Technology*, pages 100–103. Springer Berlin Heidelberg, 2013. 113
[8] NSM. Veiledning i risiko- og sï£¡rbarhetsanalyse (guidelines for risk and vulnerability assessments). Technical report, Nasjonal Sikkerhetsmyndighet (Norwegian National Security Authority), 2006. 12, 32, 33, 43, 113, 119, 128, 131, 133, 135
[9] Doctoral theses at NTNU, 2017:153. Gaute Bjørklund Wangen. Cyber Security Risk Assessment Practices. Core Unified Risk Framework, pages 111-131. Access mode: http://surl.li/pslmi

Надійшла: Листопад 2023. **Прийнята**: Грудень 2023.

Автори:
Копиця Олександр, аспірант кафедри безпеки інформаційних систем і технологій, Харківський національний університет (ХНУ) імені В. Н. Каразіна, Харків, Україна.
E-mail: oleksandr.kopytsia@student.karazin.ua

Узлов Дмитро, к.т.н., доцент, в.о. декана факультету комп'ютерних наук, ХНУ ім. В. Н. Каразіна, Харків, Україна.
E-mail: dmytro.uzlov@karazin.ua

Методи визначення категорій кіберінцидентів та оцінки ризиків інформаційної безпеки.

Анотація. Стаття присвячена вивченню категорій кіберінцидентів та їх пріоритезації в контексті інформаційної безпеки. Розглядаються основні джерела, що надають інформацію про кіберзагрози й визначається їх роль у виявленні та аналізі інцидентів, наводяться інструменти для збору, та аналізу даних. Розглядаються поняття події, інциденту і злочину та співвідношення між ними. Наводиться класифікація різноманітних типів кіберзагроз, спосіб їх систематизації, характеристики та вплив на інформаційні системи. Представлені приклади використання класифікації кіберінцидентів. Автори розглядають, також, специфічні види кіберінцидентів, що можуть виникнути в різних сферах діяльності та небезпеки для інформаційних систем які вони становлять. Обгрунтовується необхідність та методи визначення пріоритетів у реагуванні на кіберзагрози, що дозволяє ефективно розподіляти ресурси та здійснювати попереджувальні заходи з кібербезпеки. Розкривається підхід до оцінки та класифікації інцидентів за їх можливим впливом на діяльність організації, захист інформації та здатність відновлюватися після кібератак. Висвітлюються різноманітні підходи та методології для визначення та управління ризиками в сфері інформаційної безпеки, що включають в себе використання стандартів, моделей та інструментів оцінки. Матеріали статті є додатковим ресурсом відомостей для фахівців з кібербезпеки, дослідників та керівників, які цікавляться питаннями управлінням ризиками та захистом інформаційних активів у сучасному цифровому середовищі.

Ключові слова: кібербезпека, кіберінцидент, IDS, категорії кіберінцидентів, пріоритизація інцидентів, ризики безпеки.