УДК 004.056:004.738.5:378.4

КІБЕРБЕЗПЕКА У СФЕРІ ВІДКРИТОГО ДОСТУПУ: ПРИНЦИПИ ЗАХИСТУ НАВЧАЛЬНО-НАУКОВИХ РЕСУРСІВ

CYBERSECURITY IN THE FIELD OF OPEN ACCESS: PRINCIPLES FOR PROTECTING EDUCATIONAL AND SCIENTIFIC RESOURCES

[1]Dmytro Dets, [2] Oksana Syvolap, [3] Alina Barduk
[1]Дмитро Дец, [2]Оксана Сиволап, [3]Аліна Бардук

[1,2,3]Odesa National University of Technology, Odesa, Ukraine
ORCID: [1]https://orcid.org/0000-0002-8556-5451, [2] https://orcid.org/0000-0001-8011-980X
E-mail: [1]dec@ontu.edu.ua , [2]kasiosandra@gmail.com, [3]index@ontu.edu.ua

DOI: 10.15673/atbp.v%vi%i.3081

Abstract. *The modern era is characterized by the rapid development of information and communication technologies (ICT), which are increasingly integrating into all spheres of social life, including science, education, governance, economy, defense, and security. The issue of cybersecurity has become particularly significant, as the digital environment involves a continuous exchange of sensitive information, making every user or organization a potential target for malicious activities. Given the external and internal challenges Ukraine has faced in recent years, ensuring cyber protection, particularly of educational and scientific content, has become especially relevant.*

Open-access repositories are an essential component of the modern scientific space, providing free knowledge exchange. However, they are also vulnerable to cyberattacks, which can lead to the loss or compromise of valuable information. In this context, studying global experience in organizing cybersecurity systems, particularly involving both state structures and the private sector, is highly relevant.

Modern cyber threats are becoming increasingly complex, ranging from simple hacking to the use of high-tech malicious software, social engineering methods, DDoS attacks, data theft, and information substitution. Counteracting such threats requires a systematic approach, including the implementation of effective protection methods and technologies, continuous monitoring of information security status, attack identification mechanisms, and legal responses to incidents.

Special attention should be paid to the security of educational and scientific content distributed through open digital platforms. This content is not only the result of intellectual activity but also the foundation for further research and educational processes. Therefore, its protection from cyber threats is crucial for ensuring the continuity of scientific communication and knowledge development. For this reason, systematizing information on the state and development of protection measures for open-access educational and scientific content, as well as developing and implementing effective cybersecurity measures, is an extremely important scientific and practical task.

Аннотація. *Сучасна епоха характеризується бурхливим розвитком інформаційно-комунікаційних технологій (ІКТ), які все глибше інтегруються у всі сфери суспільного життя, включаючи науку, освіту, управління, економіку, оборону та безпеку. Особливої ваги набуває проблема кібербезпеки, адже у цифровому середовищі відбувається постійний обмін чутливою інформацією, і кожен користувач чи організація може стати об’єктом зловмисної діяльності. В умовах зовнішніх і внутрішніх викликів, що постали перед Україною в останні роки, питання забезпечення кіберзахисту, зокрема навчально-наукового контенту, набуло особливої актуальності. Репозиторії відкритого доступу (open access) є важливою складовою сучасного наукового простору, що забезпечують вільний обіг знань, але водночас вони стають вразливими до кібератак, що може призвести до втрати або компрометації цінної інформації.*

У цьому контексті актуальним є вивчення світового досвіду організації систем захисту у кіберпросторі, зокрема – щодо залучення до цієї діяльності як державних структур, так і приватного сектору. Сучасна кіберзагроза набуває все складніших форм: від звичайного злому до застосування високотехнологічного зловмисного програмного забезпечення, з використанням методів соціальної інженерії, DDoS-атак, викрадення даних, підміни інформації. Протидія таким загрозам вимагає системного підходу: впровадження ефективних методів і технологій захисту, постійного моніторингу стану інформаційної безпеки, використання механізмів ідентифікації атак, а також правового реагування на інциденти.

Особливу увагу слід приділити безпеці навчально-наукового контенту, що поширюється через відкриті цифрові платформи. Такий контент є не лише результатом інтелектуальної діяльності, а й основою для подальших досліджень та освітніх процесів, тому його захист від кіберзагроз є запорукою безперервності наукової комунікації та розвитку знань. Саме тому систематизація інформації про стан і розвиток засобів захисту навчально-наукового контенту у відкритому доступі, а також розробка і впровадження дієвих заходів кібербезпеки є вкрай важливою науковою і практичною задачею.

Keywords: information and communication technologies (ICT), cybersecurity, digital environment, cyber defense, open access repositories, information security, social engineering, DDoS attacks, security monitoring, automatic control, Business process automation, business process management automation tools

Ключові слова: інформаційно-комунікаційні технології (ІКТ), кібербезпека, цифрове середовище, кіберзахист, репозиторії відкритого доступу, інформаційна безпека, соціальна інженерія, DDoS-атаки, моніторинг безпеки, автоматичного керування, Автоматизація бізнес-процесів, засоби автоматизації управління бізнес-процесами

Introduction

The last few years have been a period of extremely rapid and large-scale changes in the field of information and communication technologies. The development of the computer sphere directly affects this process. For our state, this period turned out to be full of new challenges and threats to cybersecurity, which were actualized due to a number of external and internal factors. At the same time, the inadequacy and inconsistency of the national system for protecting the state's security in cyberspace formed in previous periods led to the fact that Ukraine quite fully felt the consequences of the implementation of threats to cybersecurity, and successful cyberattacks, motivated by the interests of individual state entities, led to significant damage to numerous communication systems and critical infrastructure facilities [1].

Each system requires the presence of technologies that can optimize work with it. Analysis of existing foreign experience shows that in some states, testing the readiness of infrastructure facilities for cyberattacks and cyberincidents is an established practice and an integral part of the national cybersecurity system. Moreover, representatives of the private sector are actively involved in this activity along with state bodies.

The state implements its measures to ensure information security through relevant bodies, and citizens, public organizations and associations with the necessary powers, in accordance with the legislation [2].

Having analyzed various approaches to protecting educational and scientific information content posted in open access format from cyber attacks, the main tasks can be summarized as follows:

− systematization of information on the status and development of the protection of educational and scientific information content;

Considering all of the above, the development of principles for protecting educational and scientific information content posted in open access format from cyber attacks is a relevant direction for research.

Theoretical justification

The modern world cannot be imagined without the use of web resources by society. However, the traditional situation remains that when something is widely used by society, it needs protection. In this case, it is data protection [6].

The number of Internet users is growing rapidly, which expands the opportunities for attackers to benefit from the possibility of applying malicious software to a larger number of computer systems. The main object for attackers is information, for which it is necessary to ensure its integrity, availability and confidentiality during storage, which is determined by security standards [3].

A cyber-attack is an attempt to implement a cyber threat, i.e. any circumstances or events that may cause a violation of information security policy and/or cause damage to an automated system [4].

The ability to determine the source of a cyber attack is very helpful in stopping such attacks. If this capability were well developed, it would act as a deterrent against such attacks, as precise knowledge of the source of such attacks could be used for legal, criminal, economic, or military sanctions [13]. The process of tracing an attack to its source could also reveal useful details that would help develop effective countermeasures against similar attacks in the future. It could even allow an ongoing attack to be interrupted [5].

Modern malware is a complex multifunctional software systems and complexes, which are built using effective methods of creating software tools and methods of distributing malicious code.

Malicious software is detected using various means. The effectiveness and reliability of detection significantly depend on the architecture of such tools, as well as their positioning and location in computer systems, in particular, local networks. Studies of known antivirus methods and tools indicate that the implementation of new principles, models and

methods for detecting specific types of malicious software by creating appropriate systems requires further development [3].

Computer network security involves organizing its state in such a way that its information and software and hardware resources will be protected from harmful effects from both users and attackers.

Information security activities are carried out using various methods, tools and techniques, which together constitute methods. A method involves a certain sequence of actions based on a specific plan. Methods can vary significantly and depend on the type of activity in which they are used, as well as the scope of application.

Methods of ensuring information security:

- physical;
- software and hardware;
- managerial;
- technological;
- user level;
- network;
- procedural.

At the physical level, the organization and physical protection of information resources, information technologies used and management technologies are carried out.

At the software and technical level, user identification and verification of authenticity, access management, logging and auditing, cryptography, shielding, and ensuring high availability are carried out.

At the management level, organizational, technological and technical measures are managed, coordinated and controlled at all levels by a unified information security system.

At the technological level, information security policy is implemented through the use of a complex of modern automated information technologies.

At the user level, the implementation of information security policy is aimed at reducing the reflexive impact on information security objects, preventing information influence from the social environment.

At the network level, this policy is implemented in the format of coordinating the actions of the components of the management system, which are interconnected by one goal.

At the procedural level, measures are taken that are implemented by people. Among them, the following groups of procedural measures can be distinguished: personnel management, physical protection, maintaining working capacity, responding to security violations, and planning resuscitation work [9].

Analysis of research and publications in recent years

Data protection is one of the most important tasks in the modern world. Open access repositories are a type of data source that fosters open access publishing activities and are also valuable resources for analysts (open access analytics with open access repository).

This article [5] describes three approaches to locating a remote host on a network: whois, traceroute, and distributed traceroute. whois is a primary database that contains information about networks and is maintained by the InterNic organization. The Whois service is available to any Internet user and queries can be made by email. Whois has the limitation that it provides information only about top-level domains, but the computers associated with a domain can be widely distributed [10].

Traceroute is a program that displays the route followed by an

IP datagram across the Internet from its source host to its destination host. It uses the TTL (Time To Live) field of the IP header. Each router that processes an IP datagram decrements the TTL field. When the TTL field reaches zero, the router must discard the packet and send an error message to the originator of the datagram.

An approach to distributed tracing using multiple paths through the Internet was presented in [11]. The basic idea is to run a traceroute from several geographically distributed computers to the same target computer [11]. The article also discusses the Time Delay Method, which compares the time delays between the victim computer and the attacking computer.

The article [6] presents a general view of DoS attacks and one of the approaches to their classification, namely by the nature of the impact, by the purpose of the impact, by the condition of the attack initiation, by the presence of feedback with the attack object, by the location relative to the attack object, by the OSI model level at which the attack is carried out. It then describes two principles of DoS attack detection: signature and behavioral. Methods for detecting DoS attacks: contextual search methods (signature); state analysis methods (signature); methods based on statistical models (behavioral); production rule methods (combined); methods for simulating the behavior of biological systems. The causes of DoS attacks in a computer system can be classified as follows: an error in the program code, which leads to access to unused fragments of the address space, execution of an invalid instruction or other unhandled exceptional situation, when the server application crashes; insufficient verification of user data, which leads to an infinite or long cycle, exhaustion of processor resources, allocation of too much RAM; flood - an attack associated with a large number of usually meaningless or incorrectly formatted requests to a computer system or network equipment, which led to a system failure due to exhaustion of system resources - processor, memory or communication channels; attacks of the second type - attacks on security systems, leading to their false activation and unavailability of the computer system [12].

In general, there are two methods for detecting DoS attacks - analysis of network information flow and analysis of operating system or application logs. The first approach to detecting attacks is more effective due to the real-time response. Therefore, the main research is now aimed at developing methods and procedures for detecting attacks in network traffic. Here, the main task is to identify malicious traffic. Most attacks are currently difficult to distinguish from normal user actions, at the same time, the opposite statement is also true - often user activities cause effects identical to the effect of conducting a distributed denial of service attack [7].

The thesis [8] describes that, at present, there is an intensive introduction of new information technologies, their penetration into all spheres of vital interests of the state and society, but information technologies have led to the emergence of a number of significant problematic issues. The danger of unauthorized interference in the operation of computer, information and telecommunication systems is increasing.

Problems of information security of Ukraine in modern conditions, the principles of ensuring information protection are extremely relevant and require in-depth study. Today, there is a discussion around this issue, in particular, around the assessment of information security criteria, the characteristics of potential threats and their structure, as well as the principles of building a reliable system for protecting national interests in the information sphere from external and internal threats both for the state (society) itself and for a specific person.

The development of an information protection system is impossible without knowledge of the possible consequences of threats. Next comes the classification of threats, the author divided them into 3 groups: information security, method of implementation, by location of the source of the threat. The point about information security refers to the threat to the confidentiality of data and programs; threats to the integrity of data, programs, hardware; threats to data availability; threats to the denial of operations. In the section on the method of implementation, the author talked about cases - hardware or software malfunctions, erroneous actions of employees or users, unintentional errors in software and hardware security, etc.; intentional – are aimed at causing damage to the information system or users and can be implemented through a prolonged mass attack with unauthorized requests or viruses, that is, their consequences lead to the destruction (loss) of information, modification (changing information to erroneous information that is correct in form and content, but has a different meaning), familiarization with it by third parties persons, actions of natural and man-made nature.

He pointed out the current security threats directed against information resources in modern information and communication systems for the creation of an effective information security system, the development and improvement of existing methods of its protection. He also drew attention to the system of principles that allows for the effective organization of information protection work. [8]

Article [14] describes the ways of unauthorized access to information and some classic means of protection. Technical means - electrical, electromechanical, electronic, etc. type of device. Software - programs specially designed to perform functions related to information protection. Mixed hardware-software means that implement the same functions as hardware and software means separately, and have intermediate properties. Organizational means consist of organizational and technical (preparation of premises with computers, laying of a cable system taking into account the requirements for restricting access to it, etc.) and organizational and legal (national legislation and work rules established by the management of a particular enterprise). At the moment, these means of protection are not effective and the current state requires an integrated approach. Specialized software means of protecting information from unauthorized access generally have better capabilities and characteristics than built-in means of network OSs. Firewalls are most often used. Special intermediate servers are created between the local and global networks, which inspect and filter all network/transport layer traffic passing through them. All network/transport layer traffic between the local and global networks is completely prohibited - there is no routing as such, and access from the local network to the global network is made through special intermediary servers.

The article [15] discusses the analysis of vulnerabilities that can be found in systems that are in demand in a large number of hosting providers: cPanel on CentO. SQL injection is one of the most common types of security vulnerabilities in web applications. Security misconfiguration encompasses several types of vulnerabilities, all focused on insufficient maintenance or insufficient attention to server configuration. Due to the software that includes potential malicious code, they will often interfere with the work of the actual owner. These are the so-called "false positive" triggers that will stop the display of updates due to the fact that they contain keywords that can potentially be used maliciously. Security as a component is an important element of the overall quality of service PQoS is an assessment of the quality of information service from the point of view of the user's perception as a consumer of this service. There is always a human element in every digital security measure, as social engineers will try to trick hosting owners or hosting service providers into sharing login credentials to resources that are otherwise inaccessible to them. This method of hacking does not require in-depth technical knowledge and complex scripts, so no firewall can protect it.

The article [16] discusses how data is crucial for many NGOs and researchers to monitor and evaluate the deployment or intervention and report to donors. For example, organizations may collect information about patients during clinic visits to assess the prevalence of pests in rural areas, or document infrastructure that needs repair. ODK enables the use of digital forms and will be used as a platform by many organizations.

The security issues of data collection are a very important issue. The authors discuss the Open Data Kit (ODK), which was originally created by researchers in 2008 with the aim of providing a common tool to facilitate data collection. ODK allows the creation of digital forms without deep technical expertise. It supports traditional text and multiple-choice questions and uses sensors on devices to collect a variety of data types, including GPS location and photos. The authors

conducted surveys and interviews with organizations using ODK to understand what threat models are being addressed in the field.

Using the threat model, survey, and interview results, it is possible to provide recommendations to organizations seeking to keep their data secure

Practical part

Cyberattacks are the main threats of the modern world. The data sample on cyberattacks totals terabytes of information. To solve the tasks of this master's project, open data that is in the public domain was taken as a basis.

This allowed us to form not only a data analysis methodology, but also an information and analytical model based on modern data mining tools.

Open data that was obtained from the data.world repository for one institution, the number of attempts to steal data, the type of this data, the format of documents, the language in which the web platform of this organization is written, etc.

Given the volume of data, data mining tools were used.

Data Mining is a data analysis method designed to search for previously unknown patterns in large amounts of information. These patterns make it possible to make effective management decisions and optimize business processes.

Data Mining technology performs the following tasks:

Classification task - determining a category for each object of research. In the field of fintech, such a task will be assessing the creditworthiness of potential borrowers. This will help reduce the risk of losing money when working with non-creditworthy clients;

Forecasting task, i.e. identifying new possible values in a certain numerical sequence. In e-commerce, such a task is solved for preliminary setting of prices depending on seasons and trends. Thanks to this, it is possible to predict the level of sales;

Clustering (segmentation) task - dividing a set of objects into groups according to any criteria. For example, segmenting data about online store buyers by age, gender or preferences helps to form special offers for each group;

Relationship determination task - identifying the frequency of sets of objects that occur among a set of sets. This method helps, in particular, to determine the composition of the consumer basket and optimize the placement of information about related products in the online store;

The task of sequence analysis is to identify patterns in sequences of events. This analysis can be used to track the pages on which visitors most often interrupt the site. This method of working with data allows you to eliminate the shortcomings of sites and increase their traffic;

The task of deviation analysis is to identify data that significantly differs from the norm. This analysis is used in fintech to detect fraudulent transactions with bank cards. It allows you to provide reliable customer protection.

The task of studying complex systems and processes is often to verify the presence and establish the type of relationship between independent variables x_i (predictors, factors), the values of which can be changed by the researcher and have a certain predetermined error, and the dependent variable (response) z.

Classical regression analysis includes methods for constructing mathematical models of the systems under study, methods for determining the parameters of these models and checking their adequacy. It assumes that regression is a linear combination of linearly independent basis functions of factors with unknown coefficients (parameters). Factors and parameters are deterministic, and responses are equiprecise (i.e. have the same variances) uncorrelated random variables.

The usual procedure for classical regression analysis is as follows. First, a hypothetical model is chosen, i.e. hypotheses are formulated about the factors that significantly affect the studied characteristic of the system, and the type of response dependence on the factors. Then, based on the available empirical data on the dependence of the response on the factors, the parameters of the selected model are estimated. Then, its adequacy is checked using statistical criteria. When constructing regression models of real systems and processes, the above assumptions are not always met.

In most cases, their failure to comply leads to incorrect application of the procedures of classical regression analysis and requires the use of more complex methods of empirical data analysis. The postulate of equal accuracy and uncorrelatedness of responses is not mandatory. In case of its failure, the procedure for constructing a regression model changes to some extent, but does not become significantly more complicated.

A more complex problem is the choice of the model and its independent variables. In classical regression analysis, it is assumed that the set of factors is given uniquely, all significant variables are present in the model, and there are no alternative ways of selecting factors. In practice, this assumption is not met. Therefore, there is a need to develop formal and informal procedures for transforming and comparing models. To find optimal formal transformations, the methods of factor and discriminant analysis are used.

Increasing the stability of estimates can be achieved by abandoning the requirement for their unbiasedness. The development of this area of research led to the emergence of ridge, or ridge regression analysis.

Most often, the task of building a regression model is formulated as follows. It is necessary to find a function of a given class for which the functional:

$$F(\alpha) = \sum_{i=1}^{n} (z_i(\alpha, X) - y_i)^2 \to min$$

In this expression ($z_i(\alpha, X)$ – the value of the function approximating the dependence at the i-th point, y_i – the corresponding value of the empirical dependence,

α – the vector of parameters to be found,

X – the vector of independent variables.

The resulting function z (α, X) is called the (mean-square) regression model.

The method of finding it is called the least squares method. To determine the parameters of regression models, one can solve problems of minimizing other functionals, in particular:

$$F(\alpha) = \sum_{i=1}^{n} \left| z_i(\alpha, X) - y_i \right| \rightarrow min$$

$$F(\alpha) = max \left| z_i(\alpha, X) - y_i \right| \rightarrow min$$

The resulting regression models are called, respectively, mean absolute (median) and minimax.

Conclusion

Thus, the modern realities of the digital world necessitate constant attention to cybersecurity issues, especially in the context of protecting educational and scientific content that is in open access. An analysis of existing methods and means of combating cyber threats allows us to conclude that the most effective approach is a combination of technical, organizational and legal protection measures. The use of multi-level methods - from physical and software-technical to management and network - provides comprehensive protection of information at different stages of its life cycle. The implementation of modern antivirus systems, means of detecting anomalies in network traffic, cryptography technologies and multi-factor authentication is a necessary component of effective cybersecurity.

Successful counteraction to cyberattacks also requires a high culture of information security among users, who must comply with security policies and have the skills to respond to potential threats. In addition, it is extremely important to develop mechanisms for identifying the sources of cyberattacks, which allows not only to prevent repeated incidents, but also to hold perpetrators accountable. In this context, research in the field of network route tracing, time delay analysis and behavioral traffic models is promising.

Summarizing the above, it can be noted that ensuring the security of educational and scientific content in open access format is an important task both at the state and inter-institutional levels. This requires the introduction of the latest technologies, adaptation of international experience, development of regulatory and legal mechanisms, as well as raising the awareness and responsibility of all participants in the information process. Only a comprehensive approach to addressing cybersecurity issues will allow us to effectively protect valuable scientific resources from cyber threats, maintain their availability, integrity and confidentiality, and ensure the sustainable development of the digital scientific and educational environment.

Перелік використаних джерел

1. Http://academy.ssu.gov.ua/ua/page/page_1581426264.htm // Національна академія Служби безпеки України: [Веб-сайт]. URL: http://academy.ssu.gov.ua (дата звернення: 12.03.2025).
2. Міжнародна інформаційна безпека // міжнародна інформація та суспільні комунікації. Луцьк. С. 326.
3. Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (2023). Towards a machine learning-based framework for DDOS attack detection in software-defined iot (SD-iot) networks. Engineering Applications of Artificial Intelligence, 123, 106432.
4. Вікіпедія // Вікіпедія. - URL: https://uk.wikipedia.org/wiki/Перелік_кібератак (дата звернення: 07.12.2024
5. Detecting a cyber-attack source in real time R. Romanyak[1] , A. Sachenko[1] , S. Voznyak[1] , G. Connolly[2] , G. Markowsky[2]
6. Прогнозування та аналіз ddos - атак на інформаційні web – ресурси / Вінницький національний технічний університет. - Вінниця. - 1 с.
7. Н.Р., Кондратенко. Виявлення аномалії на основі стохастичної нейротехнології / Кондратенко. Н.Р., Никитюк. О.М.. // Вінницький національний технічний університет. – 2015. – 15. – С. 23-27.
8. Awan, M. J., Farooq, U., Babar, H. M. A., Yasin, A., Nobanee, H., Hussain, M., ... & Zain, A. M. (2021). Real-time ddos attack detection system using big data approach. Sustainability, 13(19), 10743.
9. Suhag, A., & Daniel, A. (2023). Study of statistical techniques and artificial intelligence methods in distributed denial of service (DDOS) assault and defense. Journal of Cyber Security Technology, 7(1), 21-51.
10. Savage, S., Wetherall, D., Karlin, A. And Anderson, T. “Practical Network Support for IP Traceback,” 295– 306. Proceedings of ACM SIGCOMM 2000. Stockholm, Sweden, Aug. 28–Sept. 1, 2000. New York: Association for Computing Machinery, 2000.
11. Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (ddos) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions. International Journal on Semantic Web and Information Systems (IJSWIS), 18(1), 1-43.
12. А.П., Кортко. Види ddos - атак та алгоритм виявлення ddos – атак типу flood – attack / Кортко. А.П.. // науковий журнал «Комп’ютерно – інтегровані технології: освіта, наука, виробництво». – 2015. – 18. – С. 18-25

13. Lee H., and Park, K. “On the Effectiveness of Probabilistic Packet Marking for IP Traceback Under Denial of Service Attack”. Proceedings of IEEE INFOCOM 2001. Anchorage, Alaska, April 22–26, 2001. New York: IEEE Computer Society Press, 338–347, 2001.
14. Димкар В. М. Захист інформації в комп'ютерних мережах / В. М. Димкар, І. В. Фірман; Львівський національний університет імені Івана Франка Департамент політики Міністра МВС України. - Львів. - 45.49 с.
15. Ghanbari, M., & Kinsner, W. (2022). Detecting ddos attacks using polyscale analysis and deep learning. In Research Anthology on Smart Grid and Microgrid Development (pp. 1078-1096). IGI Global.
16. Computer security for data collection technologies // Development Engineering. - . - № 3. - С. 1-11.

Reference

1. Http://academy.ssu.gov.ua/ua/page/page_1581426264.htm // Natsional`na akademiya Sluzhbi bezpeki Ukrayini: [Veb-sayt]. URL: http://academy.ssu.gov.ua (data zvernennya: 12.03.2025).
2. Mizhnarodna informatsiyna bezpeka // mizhnarodna informatsiya ta suspil`ni komunikatsiyi. Luts`k. S. 326.
3. Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (2023). Towards a machine learning-based framework for DDOS attack detection in software-defined iot (SD-iot) networks. Engineering Applications of Artificial Intelligence, 123, 106432.
4. Vikipediya // Vikipediya. - URL: https://uk.wikipedia.org/wiki/Perelik_kiberatak (data zvernennya: 07.12.2024
5. Detecting a cyber-attack source in real time R. Romanyak1 , A. Sachenko1 , S. Voznyak1 , G. Connolly2 , G. Markowsky2
6. Prohnozuvannya ta analiz ddos - atak na informatsiyni web – resursi / Vinnits`kiy natsional`niy tekhnichniy universitet. - Vinnitsya. - 1 s.
7. N.R., Kondratenko. Viyavlennya anomaliyi na osnovi stokhastichnoyi neyrotekhnolohiyi / Kondratenko. N.R., Nikityuk. O.M.. // Vinnits`kiy natsional`niy tekhnichniy universitet. – 2015. – 15. – S. 23-27.
8. Awan, M. J., Farooq, U., Babar, H. M. A., Yasin, A., Nobanee, H., Hussain, M., ... & Zain, A. M. (2021). Real-time ddos attack detection system using big data approach. Sustainability, 13(19), 10743.
9. Suhag, A., & Daniel, A. (2023). Study of statistical techniques and artificial intelligence methods in distributed denial of service (DDOS) assault and defense. Journal of Cyber Security Technology, 7(1), 21-51.
10. Savage, S., Wetherall, D., Karlin, A. And Anderson, T. “Practical Network Support for IP Traceback,” 295– 306. Proceedings of ACM SIGCOMM 2000. Stockholm, Sweden, Aug. 28–Sept. 1, 2000. New York: Association for Computing Machinery, 2000.
11. Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (ddos) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions. International Journal on Semantic Web and Information Systems (IJSWIS), 18(1), 1-43.
12. A.P., Kortko. Vidi ddos - atak ta alhoritm viyavlennya ddos – atak tipu flood – attack / Kortko. A.P.. // naukoviy zhurnal «Komp’yuterno – intehrovani tekhnolohiyi: osvita, nauka, virobnitstvo». – 2015. – 18. – S. 18-25
13. Lee H., and Park, K. “On the Effectiveness of Probabilistic Packet Marking for IP Traceback Under Denial of Service Attack”. Proceedings of IEEE INFOCOM 2001. Anchorage, Alaska, April 22–26, 2001. New York: IEEE Computer Society Press, 338–347, 2001.
14. Dimkar V. M. Zakhist informatsiyi v komp"yuternikh merezhakh / V. M. Dimkar, I. V. Firman; L`vivs`kiy natsional`niy universitet imeni Ivana Franka Departament politiki Ministra MVS Ukrayini. - L`viv. - 45.49 s.
15. Ghanbari, M., & Kinsner, W. (2022). Detecting ddos attacks using polyscale analysis and deep learning. In Research Anthology on Smart Grid and Microgrid Development (pp. 1078-1096). IGI Global.
16. Computer security for data collection technologies // Development Engineering. - . - # 3. - S. 1-11.

Отримана в редакції 24.01.2025. Прийнята до друку 26.02.2025. Received 24 January 2025. Approved 26 Februry 2025. Available in Internet 28 March 2025.