

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

№ 1(7)/2024

НАУКОВИЙ ЖУРНАЛ

ISSN 2707-1758

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

УДК 004

DOI: <https://doi.org/10.17721/ISTS>

Представлено результати досліджень за такими напрямками: інформаційна та кібернетична безпека, комп'ютерні науки та інформаційні технології, інформаційно-комунікаційні системи, телекомунікації та радіотехніка.

Для науковців, докторантів, аспірантів, фахівців відповідних напрямів, студентів.

ГОЛОВНИЙ РЕДАКТОР	Бучик Сергій, д-р техн. наук, проф. (Україна)
ВІДПОВІДАЛЬНІ СЕКРЕТАРІ	Даков Сергій, канд. техн. наук (Україна) Торошанко Олександр, канд. техн. наук (Україна)
РЕДАКЦІЙНА КОЛЕГІЯ	Бернаш Марчін, д-р техн. наук, (Польща); Браїловський Микола, канд. техн. наук, доц. (Україна); Гопеєнко Віктор, д-р техн. наук, проф. (Латвія); Данієлієн Рената, д-р техн. наук, доц. (Литва); Зюбіна Руслана, канд. техн. наук, доц. (Польща); Іларіонов Олег, канд. техн. наук, доц. (Україна); Казакова Надія, д-р техн. наук, проф. (Україна); Корнієнко Богдан, д-р техн. наук, проф. (Україна); Лаптев Олександр, д-р техн. наук, ст. наук. співроб. (Україна); Лукова-Чуйко Наталія, д-р техн. наук, проф. (Україна); Мілош Улман, д-р техн. наук, проф. (Чеська Республіка); Морозов Віктор, канд. техн. наук, проф. (Україна); Наконечний Володимир, д-р техн. наук, проф. (Україна); Пархоменко Іван, канд. техн. наук, доц. (Україна); Плескач Валентина, д-р екон. наук, проф. (Україна); Рудзійоніс Вітаутас, д-р техн. наук, проф. (Литва); Субач Ігор, д-р техн. наук, доц. (Україна); Снитюк Віталій, д-р техн. наук, проф. (Україна); Толюпа Сергій, д-р техн. наук, проф. (Україна)
Адреса редколегії	вул. Богдана Гаврилишина, 24, м. Київ, 04116 ☎ (38044) 481 44 07, e-mail: fit@univ.net.ua
Затверджено	вченою радою факультету інформаційних технологій 10.06.24 (протокол № 15)
Зареєстровано	Національною радою України з питань телебачення і радіомовлення Рішення № 357 від 15.02.2024 Ідентифікатор друкованого медіа: R30-02757
Засновник і видавець	Київський національний університет імені Тараса Шевченка, Видавничо-поліграфічний центр "Київський університет". Свідоцтво внесено до Державного реєстру ДК № 1103 від 31.10.02
Адреса видавця	ВПЦ "Київський університет" 6-р Тараса Шевченка, 14, м. Київ, 01601 ☎ (38044) 239 32 22, 239 31 58, 239 31 28 e-mail: vpc@knu.ua

INFORMATION SYSTEMS AND TECHNOLOGIES SECURITY

№ 1(7)/2024

SCIENTIFIC JOURNAL

ISSN 2707-1758

TARAS SHEVCHENKO NATIONAL UNIVERSITY OF KYIV

UDC 004

DOI: <https://doi.org/10.17721/ISTS>

The scientific publication presents the results of research in such areas as Information and Cyber Security, Computer Science and Information Technology, Information and Communication Systems, Telecommunications and Radio Engineering.

For scientists, doctoral students, graduate students, specialists, students.

EDITOR-IN-CHIEF

Buchykh Serhii, DSc (Engin.), Prof. (Ukraine)

EXECUTIVE SECRETARIES

Dakov Serhii, PhD (Engin.) (Ukraine)
Toroshanko Oleksandr, PhD (Engin.) (Ukraine)

EDITORIAL BOARD

Bernas Marcin, PhD (Engin.) (Poland); Brailovskyi Mykola, PhD (Engin.), Assoc. Prof. (Ukraine); Danieliene Renata, PhD (Engin.), Assoc. Prof. (Lithuania); Gopejenko Viktor, DSc (Engin.), Prof. (Latvia); Ilarionov Oleh, PhD (Engin.), Assoc. Prof. (Ukraine); Kazakova Nadiia, DSc (Engin.), Prof. (Ukraine); Kornienko Bogdan, DSc (Engin.), Prof. (Ukraine); Laptiev Oleksandr, DSc (Engin.), Senior Researcher (Ukraine); Lukova-Chuiko Nataliia, DSc (Engin.), Prof. (Ukraine); Milos Ulman, DSc (Engin.), Prof. (Czech Republic); Morozov Viktor, PhD (Engin.), Prof. (Ukraine); Nakonechnyi Volodymyr, DSc (Engin.), Prof. (Ukraine); Parkhomenko Ivan, PhD (Engin.), Assoc. Prof. (Ukraine); Pleskach Valentyna, DSc (Econ.), Prof. (Ukraine); Rudzionis Vytautas, DSc (Engin.), Prof. (Lithuania); Subach Ihor, DSc (Engin.), Assoc. Prof. (Ukraine); Snytyuk Vitaliy, DSc (Engin.), Prof. (Ukraine); Toliupa Serhii, DSc (Engin.), Prof. (Ukraine); Ziubina Ruslana, PhD (Engin.), Assoc. Prof. (Poland)

Address

24, Bohdan Hawrylyshyn str., Kyiv, 04116
☎ (38044) 481 44 07,
e-mail: fit@univ.net.ua

Approved by

the Academic Council of the Faculty of Information Technology
10.06.24 (protocol № 15)

Registered by

the National Council of Ukraine on television and radio broadcasting
Decision № 357 of 02.15.2024
Identifier of printed media: R30-02757

Founder and Publisher

Taras Shevchenko National University of Kyiv,
Publishing and Polygraphic Center "Kyiv University"
Certificate of entre into the State Register
ДК № 1103 from 31.10.02

Address

PPC "Kyiv University"
14, Taras Shevchenko Blvd., Kyiv, 01601
☎ (38044) 239 32 22, 239 31 58, 239 31 28
e-mail: vpc@knu.ua

ЗМІСТ

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ДАКОВ Сергій, ЛАПТЄВА Тетяна Удосконалення методів оцінювання захисту комп'ютерної системи від шкідливого програмного коду	5
ТОЛЮПА Сергій, ШЕВЧЕНКО Анатолій, КУЛЬКО Андрій Особливості забезпечення безпеки критичних інфраструктур	11
ТОРОШАНКО Олександр, ЩЕБЛАНІН Юрій, КУРЧЕНКО Олег Порівняння моделей зрілості процесів інформаційної безпеки організації (компанії)	24
ФЕСЕНКО Андрій, МИРОШНИЧЕНКО Марія Порівняння постквантових стандартів у розрізі впровадження у класичні алгоритми електронного підпису	31
ХОРОШКО Володимир, БРАІЛОВСЬКИЙ Микола, ПАРХОМЕНКО Іван, КИРИЧУК Тарас Модель реалізації управління доступом до інформаційних активів у концепції нульової довіри	39

КОМП'ЮТЕРНІ НАУКИ

МИРУТЕНКО Лариса, ШЕСТАК Яніна, ЛОБАН Анастасія Дослідження індексів теоретичної відповідності для українського алфавіту з пробілом	45
НАКОНЕЧНИЙ Володимир, САЙКО Володимир, МОРДВИНЦЕВ Микола, ЛУЦЕНКО Владислав Переваги та небезпеки використання CHATGPT	52

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

ТОЛЮПА Сергій, ЛАПТЄВ Сергій Удосконалення методу виявлення радіосигналів за допомогою топологічної ідентифікації загроз	62
--	----

CONTENTS

CYBERSECURITY AND INFORMATION PROTECTION

DAKOV Serhii, LAPTIEVA Tetiana Improvement of computer system protection assessment methods against harmful software code	5
TOLIUPA Serhii, SHEVCHENKO Anatoliy, KULKO Andriy Features of ensuring security of critical infrastructures.....	11
TOROSHANKO Oleksandr, SHCHEBLANIN Yurii, KURCHENKO Oleg Comparison of organization (company) information security process maturity models	24
FESENKO Andrii, MYROSHNICHENKO Maria Comparison of post-quantum standards as implemented in classical electronic signature algorithms.....	31
KHOROSHKO Volodymyr, BRAILOVSKYI Mykola, PARKHOMENKO Ivan, KYRYCHUK Taras Model of implementation of management of access to information assets in the concept of zero trust.....	39

COMPUTER SCIENCE

MYRUTENKO Larysa, SHESTAK Yanina, LOBAN Anastasiia Research of indices of theoretical correspondence for the Ukrainian alphabet with spaces	45
NAKONECHNYI Volodymyr, SAIKO Volodymyr, MORDVYNTSEV Mykola, LUTSENKO Vladyslav Advantages and risks of using CHATGPT.....	52

INFORMATION SYSTEMS AND TECHNOLOGIES

TOLIUPA Serhii, LAPTIEV Serhii Improvement of the method of detection of radio signals with the help of topological identification of threats	62
---	----



КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.056

DOI: <https://doi.org/10.17721/ISTS.2024.7.5-10>

Serhii DAKOV, PhD (Engin.)
ORCID ID: 0000-0001-9413-3709
e-mail: dacov@ukr.net

Taras Shevchenko National University, Kyiv, Ukraine

Tetiana LAPTIEVA, PhD Student
ORCID ID: 0000-0002-7291-1829
e-mail: tetiana1986@ukr.net

Taras Shevchenko National University, Kyiv, Ukraine

IMPROVEMENT OF COMPUTER SYSTEM PROTECTION ASSESSMENT METHODS AGAINST HARMFUL SOFTWARE CODE

Background. *The issue of ensuring information security (IS) of state information systems today is not only not losing relevance, but with the development of the concept of eGovernment in countries and an increase in the number of e-services, it is becoming increasingly important.*

methods were used against malicious code

Methods. *The work used the method of analyzing the evaluation of the protection of the computer system against malicious software code, with the help of the method of optimization and evaluation of the protection of the computer system, the method of malicious software code was improved.*

Results. *The work improving the method of assessing the information security of computer systems from malicious software includes a recommendatory aspect of building e-government.*

Conclusions. *Cybersecurity threats, such as spam, phishing, spyware, and botnets, pose challenges for governments, especially for such young governments in any developing country. Malicious authors (hackers) create new combined threats to counter the security of the information system. New threats make it possible to bypass system firewalls, workstation configurations and various other intrusion detection systems. Many governments are working on cybersecurity legislation to help protect consumers and themselves. Some legislative efforts are focused on establishing government structures to provide support against systemic attacks. Some government legislation has been designed to prosecute criminals in order to deter criminal activity. The legislation has well developed a basis for the detection, analysis and internal prevention of malicious software.*

To effectively manage cybersecurity threats, governments must be involved from the beginning of the process to the end of the process. Businesses need to know where and to whom to report security risk information, and the government needs to support it. Improving the method of assessing the information security of computer systems from malicious software contains a recommendatory aspect of building an electronic government. The steps of building e-government, in contrast to the existing ones, differ in the completeness of the content of each stage of building e-government.

Keywords: *identification, information security, eGovernment, organization of information security, firewalls.*

Background

The issue of ensuring information security (IS) of state information systems today is not only not losing relevance, but with the development of the concept of eGovernment in countries and an increase in the number of e-services, it is becoming increasingly important.

The issue of ensuring information security (IS) of state information systems today is not only not losing

relevance, but with the development of the concept of eGovernment in countries and an increase in the number of e-services, it is becoming increasingly important.

The uncontrolled growth of the influence of information and communication technologies (ICT) on the post-industrial society, the emergence of the danger of a gap between the information elite and consumers has led, in turn, to a significant

© Dakov Serhii, Laptieva Tetiana, 2024



complication of the task of extracting data necessary for governments to make weighted, adequate to the conditions of the situation, and also their protection from all sorts of destructive influences – challenges, in fact, undisguised cyber crimes and threats (Prandini, & Ramilli, 2014).

One of the main conditions for the transition of society to the state of a developed information society is to ensure the necessary and sufficient level of IS. The success of creating a sustainable estate system directly depends on how protection against modern Cyber Threats will be implemented. An effective level of IS is the timely identification and assessment of new risks and current cyber threats, regular assessment of the security of eGovernment infrastructure components. The state of IS eGovernment essentially depends on threats that may cause irreparable harm to the entire state system. That is why the study of the main threats and the assessment of IS objects of information activities (OIA) for the construction of effective information systems is relevant.

The purpose of the article. Improving the method of assessing the information security of computer systems from malicious software for formation and development of e-government in the European Union (EU).

Analysis of literary sources. More and more scientists are showing interest in the information society, which quickly began to develop as a concept for a new social order. The basic principles and problems of its development were examined in the works of R. Abdeev, R. Aron, D. Bell, N. Wiener, M. Zgurovsky, M. Castells, S. Kuchinsky, E. Masuda, A. Rakitova, E. Toffler, F. Fukuyama, and other scientists.

In modern conditions, the problem of information security is not a narrow technological category but goes into the area of conceptual substantiation of the management of social processes. And especially today, the problems of information security are of particular importance when the government sets itself the task of developing the information society and integrating it into the global information space.

The globalization of the information space and the development of the information society (eGovernment) leads to the emergence of problems that are rather difficult to cope with within the country. All these problems require further and in-depth study. Unfortunately, a comprehensive study of the problems of eGovernment development, as well as related information security issues, was not enough. Therefore, the study of information security, the problems of formation and development of e-government in the European Union (EU), as well as the study of possible ways to create an information and cybersecurity system in our country are very relevant.

Methods

The work used the method of analyzing the evaluation of the protection of the computer system against malicious software code, with the help of the method of optimization and evaluation of the protection of the computer system, the method of malicious software code was improved.

Results

The European Commission planned to shape the directions of eGovernment in Europe. The EU had no direct influence on the administrations of the Member States, but the EU financed a lot of multinational projects within the Research Framework Programme.

On the European's national level, there exists eGovernment Directives and Master plans at EU, but Ukraine just started development of it in the last decade. On the international level the European Commission (EC) sets the posts; so, under the name "Accelerating eGovernment in Europe for the Benefit of All" the i2010 Government Action Plan was developed. The Progress is different in diverse countries in EU, but the general patter of development is similar. In general, one discerns the following four waves (Marco P., & Marco R., 2021, pp. 285–288):

- Promote access – Web presence;
- Provide (particular) services online;
- Transform the institution so by automating and reengineering of processes;
- Next-Generation-Government (i.e. dropping the "e" as ICT having become self-evident);
- They recognized the following challenges;
- Joining up administrations by establishing interoperability and identity management;
- Increasing usage by better designed services and knowledge enhancement;
- Opening up to Public Governance with systems supporting e-Participation and e-Law.

The track record of sustainable eGovernment initiatives in rural areas is difficult to measure (Benjamin et al., 2015, pp. 391–400). In Richard Heeks's classic paper on eGovernment "Most eGovernment-for-Development Projects Fail" informed that 85% of eGovernment projects in developing countries fail. The World Bank reported in a "Task Managers' ICT Toolkit" that projects with Information and Communication Technology components had an "alarmingly high failure rate", with 50% suffering disputes and 80% requiring contract amendments (Malik, Peter, & Omer (2015), pp. 15–20). Prandini et al. informs, that managers embraced this technology as if it simply were a new, enhanced version of World Wide Web. They neglected the less-obvious aspects of the technology,



and thus bringing on significant security problems. Malicious attackers could quite easily exploit the vulnerabilities in these systems to hijack the process and lead to wrong decisions.

New cyber security threats have been introduced in the last decade or two. Malware developers create more efficient software with the advancement of network security systems. Governmental legislation offers support to companies that operate with sensitive consumer information. Attacks centred on manipulation and fraud of financial markets is one of the top cyber security threats now. Spam, phishing, and spyware were once seen as isolated challenges for organizations, hackers are now creating hybrid threats that can even infiltrate Government systems. Cyber threats such as spam, phishing, spyware and botnets present problems for governments, especially for such young governments as Ukraine or any other developing countries. Hackers create new dangerous mixed threats to circumvent the protection of the organizations information system OIA. The US federal government has taken steps to information protection (IP) the private sector and for government organizations, but efforts must be made as a collective

to improve cyber security reporting. Fig. 1 from shows how blended threats may bypass traditional security controls.

On the other hand, as Raiv Sandhu from the University of Texas at San Antonio stated, that the large-scale adoption of internet services across diverse populations is one indicator that the average consumer is reasonably comfortable with the collateral risks. Many nations and militaries, including Ukraine, are preparing offensive and defensive cyber capabilities.

Improving the lives of people by employing the Internet of Things becomes a reality. On the other hand, we must secure the systems against cybercriminals, hackers, and malicious computer applications or systems, who would certainly want to disrupt such systems or try to breach the privacy of people who will be connected to such networks.

Many cybersecurity problems occur on a worldwide scale. Benjamin Edwards, Steven Hofmeyr studied a large high-resolution data set of messages sent from 260 ISPs in 60 countries over the course of a decade.

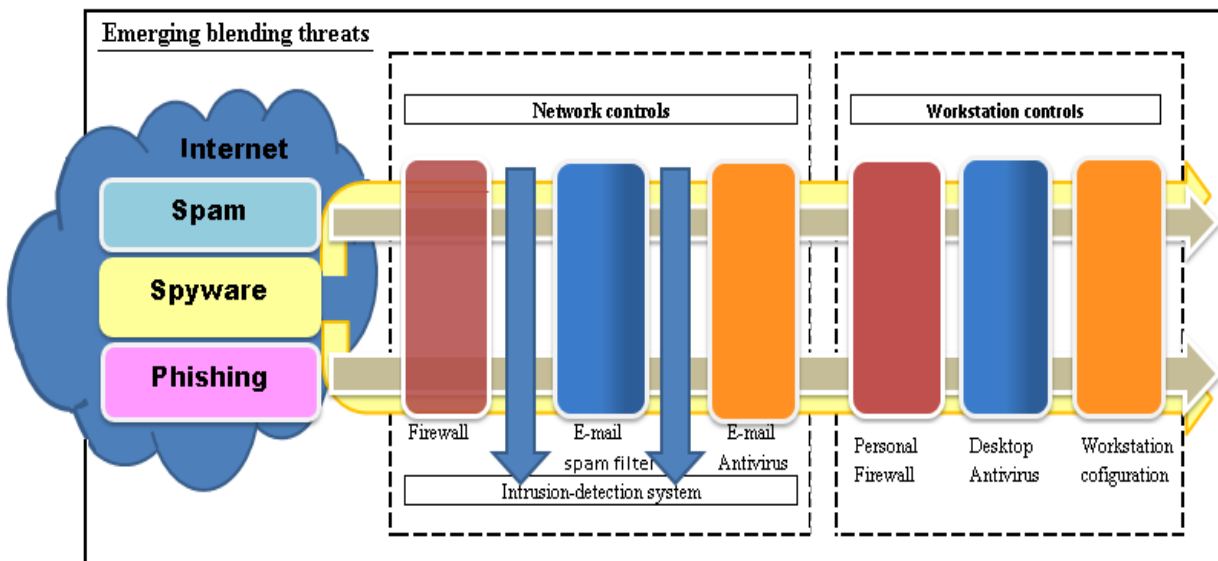


Fig. 1. Blended Threats Bypassing Traditional Security Controls

They found, that many cybersecurity problems occur at a global scale, involving nations, corporations, or individuals whose actions have impact around the world. Another security problem is related to insecure sharing data. "Sharing data is gaining importance in recent years due to proliferation of social media and a growing tendency of governments to gain citizens' trust through being transparent". They stress that privacy enhancement techniques must be used to prevent unsavoury disclosure of personal data

Existing and in-development solutions. In V. Z. Tabakov, Malik Shahzad Awan and Peter Burnap investigate stealthy and dynamic techniques and attack vectors used by cyber criminals. They have made network infrastructure more vulnerable to security breaches the organization. Cyberattacks involving advanced evasion techniques often bypass security controls, and even if detected at a later time could still remain in the system for a long time without any monitorable trace. Such types of cyberattacks are costing billions of dollars to the OIA and



for management organizations across the globe. It has been predicted that a 50% increase in security budgets will be observed to rapidly detect and respond to targeted attacks.

It's a well know approach to use firewalls between business and process control networks and many believe that this is an ideal solution for plant floor Cyber Security. But research shows that few firewalls are properly configured and that many control system security incidents bypass the firewall. Many organizations have implemented several levels of firewall defences even between different divisions in the same organization. It allows the prevention of a breach in the system if the whole organization firewall was bypassed.

To improve information security and data protection of eGovernment and Governmental information resources and system of systems on the governmental level, the authors propose to analyze security threats before malicious attacks, during attacks and after attacks:

1) Before attacks:

- All equipment and all software, applications and systems must be certified, as is described in (LapteV 2020), especially this is related to all open source systems and proprietary products;

- All critical software must be patched and updated regularly or as fast as possible after any vulnerability or security threat was discovered. Many organizations have their own test labs to test obtained software applications and systems for security risks;

- As we mentioned above, we suggest using several levels of firewall defences even between different divisions in the same organization. It will allow the prevention of a breach in the system more deeply and isolate problem inside of the organization;

- Security information and event management (SIEM) implementation.

It is necessary to implement the following information security measures at the OIA:

- Industrial control systems (ICS) and Supervisory control and data acquisition (SCADA) networks for supervisory purposes as well as control capabilities for process management;

- Virtual Private Network solutions (VPN); Network Access Control (IAM/NAC);

- Application Control.

2) During attacks:

- Intrusion Prevention System (IPS), which is a technique combining the techniques of the firewall with that of the IDS properly. IDS – is a defence system, which detects hostile activities in a network: to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and/or block a suspected connection;

- Full packet capture (FPC);

- Antivirus software;

- Email/Web security solutions.

3) After attacks:

- Intrusion Detection Systems (IDS);

- Forensic Capture System (Forensics);

- Security information and event management (SIEM).

As an example of a security web services framework we present a Multi-Level Secure Framework (MLSF) for web services from at Fig. 2.

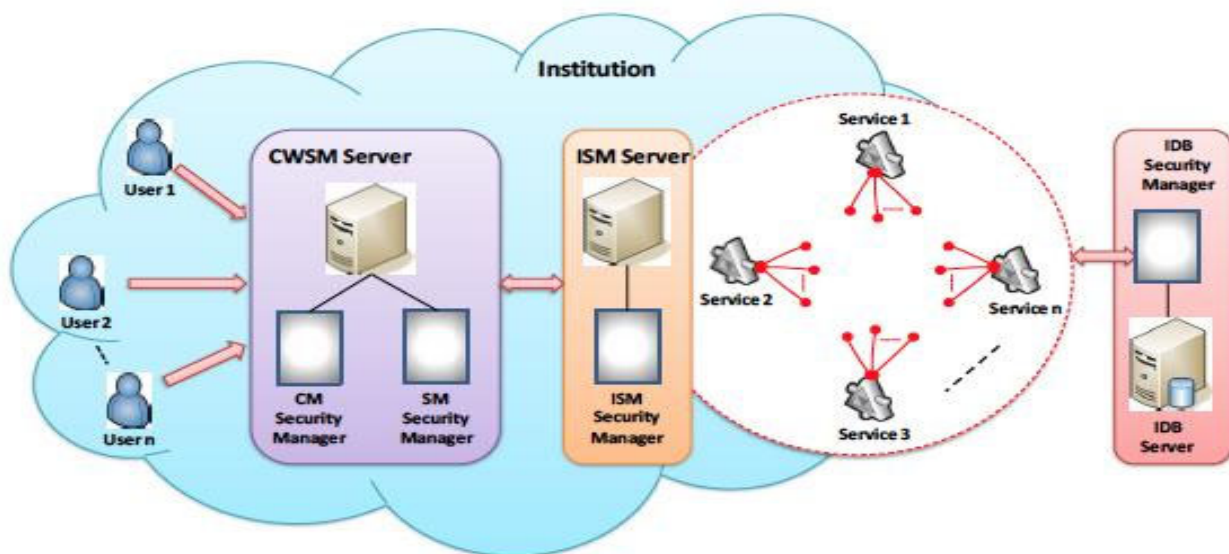


Fig. 2. Architecture for Multi-Level Secure Composite Web Services



The demonstrated framework provides essential infrastructure for various operations such as acquiring user information, connectivity, authentication and communication to facilitate secure web services for multiple users. CM is the Client Manager, CWSM is the Composite Web Services Manager, ISM – Institution Service Manager, SM – Service Manager, IDB – Institution DB. More information about shown framework can be obtained from .

In turn, considering information security in government organizations and in other OIA, information security should consist of the following parts: audit of point analysis, protection of access to the infrastructure, monitoring at all levels of the network. It is also necessary to conduct an analysis of system vulnerabilities, possible scenarios for the realization of threats, probability of realization of the threats and their origin.

The probability of implementing each i -th threat in relation to the j -th asset is determined using equation (1):

$$d_{rj} = 1 - p_{ri} \times \prod_{i=1}^m (1 - p_{rji}), \quad (1)$$

where n – the number of threats; m – the number of assets; p_{ri} – possibility of carrying out the i -th threat; d_{rj} – the possibility of implementing at least one threat of the j -th asset.

Implementation scenarios for security objects can be presented by bayesian networks of trust

$$BN_{O3} = \langle A, Tab_{O3} \rangle, \quad (2)$$

where $A = \{a_i\}_{i=1}^{NA}$ the plurality of offending actors; NA – number of all offender actions; Tab_{O3} – the set of probability tables for each of the actions a_i with "parent" actions parents (a_i).

If we consider dangerous programs as tools of unauthorized exposure, to assess the effectiveness of the organization's IP tools, the task is to synthesize a complex indicator based on the systematization of the relevant particular indicators and solve it as the task of building an optimal assessment.

It is also necessary to pay attention to the analysis of threats to IS resources in management systems and consider the means of integrated IP as an element of an integrated security system. Since one of the main causes of confidential information (CI) leakage is the human factor, it is advisable for an OIA to proceed from the suggestions of the author. And for the effective solution of questions on IP it is proposed to create a mathematical model of the CI and take appropriate countermeasures.

The following tasks can be solved in this direction:

a) a study of the motives pushing people to violate contracts and offenses;

b) the development of mechanisms for managing sensitive information carriers;

c) development of methods for informational impact on users of automated systems.

When building a model of a problem situation, let us denote by i the number of the operator-secret carrier:

$$i = \overline{1, N}. \quad (3)$$

The next step is to determine the full amount of confidential information Q :

$$Q = \sum_{i=1}^K q_i, \quad (4)$$

where q_i – is the volume of the CI block used by the i -th operator.

Then, $k(q_i)C(q_i)$ – is the "sale price" of the q_i block for a competitor, where $k(q_i)$ – is the utility coefficient of the q_i block for a competitor, $k(q_i) > 0$. And $C(q_i)$ – is the cost of q_i block, consisting of the cost of its development, implementation and operation at Fig. 3.

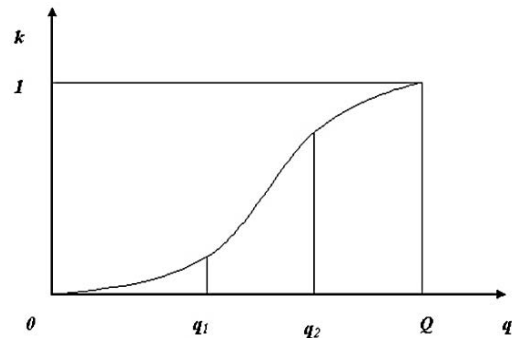


Fig. 3. Typical dependence of the utility coefficient of information $k(q_i)$ on its volume q_i

A typical dependence of the utility coefficient of information $k(q_i)$ on its volume q_i is shown in Fig. 3

To exclude the sale of confidential information, we presume that it is enough to fulfill the condition:

$$p l_i (n D(q_i) + l B(q_i)) + p 2_i R(q_i) \triangleright \triangleright k(q_i) C(q_i) - S(q_i) - p 3_i U(q_i).$$

Where $p l_i$ – the probability of exposing the seller; N – the number of months, the seller would work in the organization without offense; $D(q_i)$ – monthly salary; l – the number of awards; $B(q_i)$ – the size of premiums; $p 2_i$ – probability of damage in case of exposure; $R(q_i)$ – the amount of moral and material damage, expressed in money.

If the manager of the j -th unit acts as the seller of confidential information, then i and q_i should be replaced, respectively, by j and m_j . If the seller is the administrator, then q should be replaced by Q .

Discussion and conclusions

Cybersecurity threats, such as spam, phishing, spyware, and botnets, pose challenges for governments, especially for such young governments in any



developing country. Malicious authors (hackers) create new combined threats to counter the security of the information system. New threats make it possible to bypass system firewalls, workstation configurations and various other intrusion detection systems. Many governments are working on cybersecurity legislation to help protect consumers and themselves. Some legislative efforts are focused on establishing government structures to provide support against systemic attacks. Some government legislation has been designed to prosecute criminals in order to deter criminal activity. The legislation has well developed a basis for the detection, analysis and internal prevention of malicious software.

To effectively manage cybersecurity threats, governments must be involved from the beginning of the process to the end of the process. Businesses need to know where and to whom to report security risk information, and the government needs to support it. Improving the method of assessing the information security of computer systems from malicious software contains a recommendatory aspect of building an electronic government. The steps of building e-government, in contrast to the existing

ones, differ in the completeness of the content of each stage of building e-government.

Authors' contribution: Serhii Dakov – analysis of sources, preparation of a literature review or theoretical foundations of research; Tetiana Laptieva – conceptualization; methodology, collection of empirical data and their validation; empirical research.

REFERENCES

Marco, P., & Marco, R. (2021). Security considerations about the adoption of web 2.0 technologies in sensitive eGovernment processes. *In Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance, ICEGOV'11* (pp. 285–288), New York, USA, ACM.

Benjamin, E., Hofmeyr, S., Forrest, S., & Michel, van Eeten (2015). Analyzing and modeling longitudinal security data, Promise and pitfalls. *In Proceedings of the 31st Annual Computer Security Applications Conference, ACSAC 2015* (pp. 391–400), New York, USA, ACM.

Malik, S., Peter, B., & Omer, F. Rana (2015). Estimating risk boundaries for persistent and stealthy cyber-attacks. *In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense, SafeConfig'15* (pp. 15–20), New York, USA, ACM.

Отримано редакцією журналу / Received: 17.03.24

Прорецензовано / Revised: 27.03.24

Схвалено до друку / Accepted: 13.05.24

Сергій ДАКОВ, канд. техн. наук

ORCID ID: 0000-0001-9413-3709

e-mail: dacov@ukr.net

Київський національний університет імені Тараса Шевченка, Київ, Україна

Тетяна ЛАПТЄВА, асп.

ORCID ID: 0000-0002-7291-1829

e-mail: tetiana1986@ukr.net

Київський національний університет імені Тараса Шевченка, Київ, Україна

УДОСКОНАЛЕННЯ МЕТОДІВ ОЦІНЮВАННЯ ЗАХИСТУ КОМП'ЮТЕРНОЇ СИСТЕМИ ВІД ШКІДЛИВОГО ПРОГРАМНОГО КОДУ

Вступ. Питання забезпечення інформаційної безпеки державних інформаційних систем нині не лише не втрачає актуальності, але з розвитком концепції електронного урядування в країнах та збільшенням кількості електронних послуг, стає все важливішим для протидії шкідливому програмному коду.

Методи. Використано метод аналізу оцінювання захисту комп'ютерної системи від шкідливого програмного коду; за допомогою методу оптимізації оцінювання захисту комп'ютерної системи вдосконалено метод захисту від шкідливого програмного коду.

Результати. Удосконаленням методики оцінювання інформаційної захищеності комп'ютерних систем від шкідливого програмного забезпечення є рекомендаційний аспект побудови електронного урядування.

Висновки. Загрози кібербезпеці, такі як: спам, фішинг, шпигунське програмне забезпечення та ботнети, створюють проблеми для урядів, особливо для молодих урядів, у будь-якій країні, що розвивається. Зловмисники (хакери) створюють нові комбіновані загрози для протидії безпеці інформаційної системи. Нові загрози дозволяють обійти системні брандмауери, конфігурації робочих станцій і різні інші системи виявлення вторгнень. Багато урядів працюють над законодавством про кібербезпеку, щоб допомогти захистити споживачів і себе. Окремі законодавчі зусилля зосереджено на створенні державних структур для забезпечення підтримки проти системних атак. З метою стримування злочинної діяльності розроблено певні державні законодавства для переслідування зловмисників. Законодавством також добре розроблено основу для виявлення, аналізу та внутрішньої профілактики шкідливого програмного забезпечення.

Для ефективного управління загрозами кібербезпеці уряди мають брати участь у цьому процесі від початку до його завершення. Підприємства повинні знати, куди та кому повідомляти інформацію про ризики у безпеці, а держава має це підтримувати. Удосконалення методики оцінювання інформаційної захищеності комп'ютерних систем від шкідливого програмного забезпечення містить рекомендаційний аспект побудови електронного уряду. Етапи побудови електронного урядування, на відміну від існуючих, відрізняються повнотою змісту кожного етапу побудови електронного урядування.

Ключові слова: ідентифікація, інформаційна безпека, електронний уряд, організація інформаційної безпеки, брандмауери.

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.



УДК 004.415.056.5(075)

DOI: <https://doi.org/10.17721/IJSTS.2024.7.11-23>

Сергій ТОЛЮПА, д-р техн. наук., проф

ORCID ID: 000-0002-1919-9174

e-mail: tolupa@i.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

Анатолій ШЕВЧЕНКО, бригадний генерал

ORCID ID: 0000-0003-2723-0378

e-mail: anatolii.shevchenko@knu.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

Андрій КУЛЬКО, асп.

ORCID ID: 0009-0006-1185-0774

e-mail: kulko452@gmail.com

Київський національний університет імені Тараса Шевченка, Київ, Україна

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНИХ ІНФРАСТРУКТУР

Вступ. Стрімкий розвиток інформаційних технологій за останні два десятиліття вплинув на функціонування особливостей об'єктів критичної інфраструктури. Ці технології почали використовувати не лише як засіб обміну та оброблення інформації, а і як інструмент для заподіяння шкоди. Захист державних інтересів у політичному контексті є першоосновою забезпечення національної безпеки країни, що пояснює необхідність створення та постійний розвиток потужної кібернетичної безпеки. Об'єкти критичної інфраструктури є складними, просторово розподіленими, багатокomпонентними системами, стійка робота яких критично важлива для функціонування економіки та життєдіяльності суспільства. Вони мають багаторівневу структуру, яка включає: рівень технічних компонентів; соціальний рівень; організаційний рівень і рівень державного управління.

Методи. Порівняно інформаційні системи і за допомогою методу оцінювання дослідження захищеності систем покращено й оптимізовано систему захисту інформації.

Результати. Результатом роботи є дослідження критичних інфраструктур як соціотехнічних систем, що потребують оцінювання складних взаємодій між технічними, соціальними й організаційними рівнями системи. Тому критичну інфраструктуру варто розглядати як єдине ціле. Необхідно наголошувати на одночасному спільному розгляді технічних, організаційних і соціальних факторів, що визначають стан системи та динаміку її розвитку. Щоб забезпечити безпеку таких систем, потрібно вийти за межі традиційного підходу до оцінювання проєктних ризиків і перейти до нової парадигми, що ґрунтується на забезпеченні безпеки критичної інфраструктури за критерієм стійкості до позапроєктних впливів. У зв'язку з необхідністю включити до розгляду позапроєктні аварії на критичній інфраструктурі, межі досліджень мають бути суттєво розширені. Заходи щодо забезпечення безпеки повинні бути спрямовані не лише на створення захисних бар'єрів, покликаних попередити реалізацію проєктних аварій, що постулюються, але і на підвищення стійкості та живучості критичної інфраструктури у разі позапроєктних впливів, тобто зосередитися на запобіганні великомасштабним катастрофам і тривалим перервам у функціонуванні, а побудова багатокритеріальної моделі для оцінювання рівня захищеності об'єктів критичної інфраструктури дасть повнішу картину стану об'єкта критичної інфраструктури.

Висновки. Наявні нині методики безпеки технічних систем розроблено для систем, що мають чіткі межі і добре визначені переліки загроз. Для цих систем можуть бути створені бази даних зі статистики аварій, які дозволяють кількісно оцінювати та верифікувати моделі. Вказані методики, що базуються на побудові сценарних "дерев" (моделі типу "дерево" подій, "дерево" відмов), розроблені без урахування позапроєктних впливів і не дозволяють належно врахувати складність критичних інфраструктур, функціонування яких визначається взаємодією технічних, організаційних і соціальних факторів.

Ключові слова: кібербезпека, об'єкти критичної інфраструктури, інформаційні системи, стійкість, кіберпотужність.

Вступ

У багатьох країнах реалізується концепція критичної інфраструктури, яка дозволяє зосере-

ISSN 2707-1758

дитися на системах, мережах та окремих об'єктах, руйнування чи порушення роботи яких матиме серйозні негативні наслідки для національної

© Толюпа Сергій, Шевченко Анатолій, Кулько Андрій, 2024



безпеки. Стрімкий розвиток інформаційно-комунікаційних технологій за останні два десятиліття вплинув на функціонування особливостей об'єктів критичної інфраструктури. Ці технології почали використовувати не лише як засіб обміну й оброблення інформації, а і як інструмент для заподіяння шкоди. Захист державних інтересів у політичному контексті є першоосновою гарантування національної безпеки країни, що пояснює необхідність створення та постійний розвиток потужної кібернетичної безпеки.

Об'єкти критичної інфраструктури є складними, просторово розподіленими, багатокомпонентними системами, стійка робота яких критично важлива для функціонування економіки та життєдіяльності суспільства. Об'єкти критичної інфраструктури (ОКІ) мають багаторівневу структуру, яка включає: рівень технічних компонентів (машини, обладнання й апаратура); соціальний рівень (персонал, що обслуговує технічні компоненти критичної інфраструктури); організаційний рівень (взаємодія служб компанії, що експлуатує ОКІ) та рівень державного управління (нормативні та органи контролю, які здійснюють нагляд і державне регулювання у сфері діяльності КІ). Складність критичних інфраструктур (КІ) обумовлено: складністю їхньої структури (складними взаємозалежностями та нелінійними зв'язками між компонентами й рівнями системи, а також між різними компонентами КІ); складним характером явищ і процесів, що спостерігаються в ході експлуатації ОКІ (Бірюков, & Кондратов, 2012).

Метою статті є те, що ОКІ представляють собою технічні об'єкти, на яких зберігають, переробляють / перетворюють або транспортують / передають небезпечні речовини, енергії та / або інформаційні потоки. Ці об'єкти можуть бути джерелами важких аварій і катастроф, які є предметом традиційного аналізу ризиків, на основі якого будують карти ризиків для територій розміщення об'єктів критичних інфраструктур і приймають рішення про будівництво або модернізацію останніх.

Огляд літератури. Нині розв'язання питань забезпечення безпеки критичної інфраструктури та управління станом їхньої захищеності описано в роботах вітчизняних і зарубіжних дослідників, а саме: В. Л. Бурячка, С. С. Бучика, С. О. Гнатюка, С. П. Євсєєва, С. В. Казмирчука, О. Г. Корченка, О. О. Кузнецова, І. Ю. Субача, Т. Ртасека, G. Elmasry, P. Albers, O. Camp та ін.

Процес розвитку та впровадження новітніх інформаційних технологій забезпечують безпрецедентні умови для накопичення і використання

інформації, а також створюють фундаментальну залежність від їхнього нормального функціонування всіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем і об'єктів критичних національних інфраструктур і дає можливість негативно налаштованим елементам й угрупованням скористатися нею для реалізації протиправних дій у кібернетичному просторі шляхом порушення цілісності, доступності й конфіденційності інформації та нанесення шкоди інформаційним ресурсам й інформаційним системам. У цьому разі особливе занепокоєння викликає можливість застосування інформаційних технологій у кібернетичному просторі в інтересах здійснення воєнно-політичного та силового протипротива, тероризму і проведення хакерських атак, що нині досить актуально, враховуючи воєнний стан (Довгань, 2013, с. 17–20).

Інформаційна сфера, яка є одним з основних факторів розвитку сучасного суспільства, активно впливає на стан соціально-політичної та економічної галузей діяльності. Складність процесів, які відбуваються в розподілених інформаційних системах (РІС), постійно зростає. Це призводить до того, що РІС, які використовують для зберігання інформації, обміну інформацією та розв'язання різного типу завдань у всіх сферах людської діяльності, можуть стати об'єктом зловживань.

Кожна розподілена інформаційна система ОКІ має свої особливості, які обумовлені сферою її застосування. Важливість і відповідальність задач, розв'язуваних за допомогою розподілених систем у реальному масштабі часу, обумовили високі вимоги до надійності цих систем, у яких, найчастіше, неможливе проведення технічного обслуговування під час функціонування, і відмова всієї розподіленої інформаційної системи, або її окремих компонентів може призвести до негативних наслідків.

Дослідження сучасних науково обґрунтованих підходів підвищення ефективності складних технічних систем дозволили дійти висновку, що за останні роки сформувався новий пріоритетний підхід, який пов'язаний із забезпеченням в інформаційній системі властивості функціональної стійкості ОКІ.

Властивість функціональної стійкості КІ розглядають як можливість складної технічної системи, до якої належать усі без винятку компоненти КІ, успішно завершити поставлене завдання за регламентованої кількості змін у стані



самої системи, тобто зберегти її працездатність після прояву припустимої кількості відмов і зовнішніх дестабілізуючих впливів (Гнатюк, & Лядовська, 2013, с. 55–57).

Функціональна стійкість спрямована, в першу чергу, на поліпшення характеристик відмовостійкості й живучості, але не обов'язково показників надійності окремих комплексувальних елементів. Оскільки теорія функціональної стійкості перебуває у стадії розвитку, то формування основних показників функціональної стійкості є важливим напрямом наукових досліджень.

Проблему функціональної стійкості інформаційних систем досліджували в роботах О. А. Машкова, О. В. Барабаша, Д. М. Обідіна, Ю. В. Кравченка, О. А. Кононова. Питання відмовостійкості систем аналізували в роботах А. А. Авіжисніса, В. А. Машкова, О. Ю. Ільїна, Ю. М. Коростіля, В. А. Савченка та інших учених.

Методи

За допомогою методу дослідження порівняно інформаційні системи. Методом оцінювання дослідження захищеності систем покращенню й оптимізовано систему захисту інформації.

Результати

Наявність тісних взаємозв'язків між компонентами КІ є їхньою принципово важливою особливістю, яка визначально впливає на характер їхнього функціонування у штатних і позаштатних ситуаціях. З одного боку, пов'язаність елементів КІ підвищує їхню ефективність, дозволяючи раціонально використовувати та перерозподіляти наявні ресурси й потужності, а з іншого – робить їх схильними до великомасштабних катастроф, величезний розмір збитків від яких не дозволяє нехтувати ними, незважаючи на низьку ймовірність реалізації ризиків.

Щодо аналізу ризиків взаємопов'язаних інфраструктурних систем, то доводиться мати справу з двосторонніми залежностями між компонентами КІ, тому прийнято говорити про взаємозалежність елементів КІ. Ці взаємозалежності існують як для елементів, що належать до однієї інфраструктури, так і для елементів різних інфраструктур. В останньому випадку говорять про взаємозалежності між різними ОКІ (Юдін, & Пирогов, 2016, с. 88).

Наявність сильних зв'язків між елементами КІ робить їх схильними до каскадних сценаріїв аварій, які охоплюють велику кількість об'єктів інфраструктури, причому хід реалізації аварії визначається структурою зв'язків між елементами. Крім масштабів потенційних аварій, наявність внутрішньо- та міжінфраструктурних залежностей визначально впливає на динаміку

поширення аварій, призводячи до реалізації комбінованих механізмів досягнення граничних станів, різкої інтенсифікації процесів деградації та потоку відмов елементів КІ.

Через складну структуру ОКІ та складний характер взаємодій між значною кількістю елементів можливості сценарного аналізу за допомогою традиційного інструментарію (дерев подій, дерев відмов, баєсових мереж, нейронних мереж) виявляються обмеженими. Для опису розвитку збурень у критичних інфраструктурах застосовують мережні моделі, які активно використовують математичний апарат теорії графів. Мережі є надзвичайно гнучкою абстракцією, яка може широко застосовуватися у вивченні інфраструктурних систем. Причому може бути побудована ієрархія математичних моделей різної складності, що дозволяють описати різні аспекти ризиків інфраструктурних систем щодо можливих ініціюючих впливів. За допомогою зазначених моделей вдається описати багато властивостей та особливостей мережних систем: хаос, самоорганізація, статистичні розподіли, критичність.

Прийнято виокремлювати три типи взаємозалежностей між компонентами інфраструктурних систем, які можуть бути між компонентами й однієї інфраструктури, і різних інфраструктур.

Фізичні взаємозв'язки, які спостерігають, коли речовина, енергія або інформація фізично передається від одного компонента до іншого компонента (тої чи іншої) інфраструктури. У цьому разі вихідний продукт, який створюється або переробляється однією інфраструктурою, використовується як вхідний продукт компонентом іншої інфраструктури. Очевидно, що аварії в компонентах однієї КІ можуть викликати каскади відмов, що поширюються на компоненти іншої КІ.

Кібервзаємозалежність є інформаційно залежною, якщо стан її елементів залежить від інформації, що передається інформаційною мережею. У зв'язку зі швидким розвитком інформаційних технологій, система управління будь-якою системою залежить від якості роботи інформаційної мережі.

Територіальні взаємозалежності – інфраструктури, компоненти яких розміщені територіально безпосередньо близько один від одного і можуть зазнавати безпосереднього впливу у надзвичайних ситуаціях на компонентах іншої інфраструктури (Бурячок, & Толюпа, 2015, с. 288).

Особливість сучасних КІ полягає в тому, що вони стають транскордонними, а в деяких випадках – глобальними. Просторова довжина КІ,



поряд із наявністю тісних взаємозв'язків між ними, робить їхнє функціонування залежним від величезної кількості факторів, пов'язаних зі станом природно-техногенно-соціального середовища в різних регіонах світу. Значний обсяг небезпечних речовин, енергії та інформації, що зберігаються, транспортуються та переробляються критичними інфраструктурами, а також їхня величезна роль в економіці та житті людей, зумовлюють можливість великомасштабних аварій на ОКІ та тяжкість наслідків, що виникають у разі таких аварій, для населення й об'єктів економіки. Складність критичних інфраструктур значно перешкоджає створенню ефективних систем захисту, оскільки стає практично неможливим провести детальний сценарний аналіз системи, виявити всі значущі небезпечні сценарії та визначити комплекс заходів і бар'єрів захисту, спрямованих на парировання всіх можливих загроз.

Разом із тим аналіз практики, що склалася у сфері функціонування ОКІ, свідчить, що їхнє проєктування, будівництво й експлуатацію здійснюють відповідно до традиційної парадигми технічного забезпечення безпеки технічних систем (ТЗ). Ця парадигма передбачає: аналіз можливих сценаріїв розвитку відмов у системі; ідентифікацію найбільш значущих сценаріїв; створення захисних бар'єрів, вкладених у попередження цих сценаріїв.

Структурна складність ОКІ, їхня винятково важлива роль у життєдіяльності людей і функціонуванні економіки, а також тяжкість наслідків, що неминуче виникають у разі аварій на КІ, повинні визначити особливий порядок і спеціальні вимоги у сфері забезпечення їхньої безпеки. Сучасні тенденції у сфері забезпечення безпеки критичних інфраструктур передбачають формування нової парадигми, яка має доповнити традиційні зусилля щодо забезпечення безпеки КІ системою заходів, спрямованих на підвищення їхньої стійкості до можливих екстремальних впливів.

Врахування особливостей критичних інфраструктур у розробленні стратегії забезпечення їхньої захищеності. Як зазначено, сучасні об'єкти критичної інфраструктури є складними технологічними системами, функціонування яких визначається взаємодією технічних, соціальних, організаційних та управлінських факторів. Традиційний підхід до моделювання технологічних систем, що широко використовується у забезпеченні їхньої безпеки, передбачає декомпозицію системи на технічну, соціальну й організаційну підсистеми, які потім розглядають окремо в межах відповідних дисциплін. У такому випадку не враховують ні взаємні впливи підсистем, ні їхню взаємодію на системному рівні.

Варто зазначити, що зусилля захисту ОКІ традиційно фокусуються на технічних аспектах. Завдяки цьому досягнуто значного прогресу у сфері забезпечення надійності технічних компонентів КІ. Однак можливості цього підходу близькі до вичерпання. Це пов'язано з тим, що КІ більше неспроможні розглядатися як переважно технічні системи, а стають дедалі більше техносоціальними системами.

Завдяки бурхливому розвитку інформаційних технологій в останні десятиліття ОКІ стають все складнішими. Це означає, що в оцінюванні безпеки КІ з'являється дуже багато чинників, які підлягають обліку. Це відбувається внаслідок складних нелінійних взаємодій між компонентами КІ, сильної зв'язаності між різними підсистемами, а також того, що КІ та навколишнє середовище починають змінюватися швидше, ніж вони можуть бути описані й досліджені. Тому виникає ситуація нестачі інформації про КІ і, отже, обмеженість можливостей прогнозування їхньої поведінки й управління ними. Причому на певних режимах неможливо детально описати закони функціонування КІ й розробити правила управління.

Відмінність між повністю визначеними та не повністю визначеними системами стає надзвичайно важливою у розробці комплексу заходів щодо безпеки. Особливість деяких систем полягає у тому, що виявляється неможливим повний опис їхньої поведінки та прогнозування їхнього стану за різних умов і на різних режимах експлуатації. Внаслідок цього для таких складних систем, як критичні інфраструктури, практично неможливо створити закритий перелік проєктних впливів, яким система може піддаватися протягом її експлуатації. У зв'язку із цим традиційна стратегія забезпечення безпеки КІ, заснована на розробленні комплексу захисних бар'єрів, покликаних парировати проєктні впливи, не може бути успішною.

Тому необхідно розробити методи забезпечення безпеки, що дають змогу мати справу з недовизначеними системами. Потрібно використовувати підходи, що розвиваються в межах нового бачення, що отримало назву *теорія забезпечення стійкості технічних систем до екстремальних впливів* (Resilience Engineering). Цей напрям концентрує увагу на створенні систем, які здатні: продовжувати (принаймні частково) виконувати запропоновані ним функції після того, як вони отримують пошкодження, зазнавши позапроєктних впливів; досить швидко відновлювати свій початковий функціональний рівень після позапроєктного впливу.



Принципи забезпечення стійкості критичної інфраструктури. Стійкість до екстремальних впливів є ключовим поняттям у випадках позапроектних впливів і позапроектних сценаріїв аварій у складних технічних системах, до яких належать КІ. Сучасні інфраструктурні системи (системи водо-, електро- і газопостачання, транспортні, телекомунікаційні мережі) стають дедалі складнішими, взаємозалежними, динамічно змінюваними, дедалі більше виявляють нелінійні властивості. У зв'язку із цим стає неможливо заздалегідь – у процесі проектування – спрогнозувати багато несприятливих подій або їхнє поєднання, а також сценарії відмов, які вони ініціюють, і, отже, заздалегідь передбачити повний комплекс захисних заходів, що дозволяє побудувати системи захисту від вичерпного переліку позапроектних впливів / сценаріїв. На перший план у такому разі виходить завдання підвищення стійкості інфраструктурних систем до проектних впливів. Традиційні заходи щодо зниження ризику та забезпечення безпеки, що передбачають створення систем захисту від проектних впливів та аварій, повинні доповнюватися заходами щодо забезпечення стійкості до позапроектних впливів та аварій. У такій постановці, крім традиційних питань, на які доводиться відповідати під час забезпечення безпеки технічних систем, – "які проектні сценарії відмови можуть відбутися в системі?" і "яких захисних заходів потрібно вжити, щоб запобігти цим сценаріям?", повинні доповнюватися питаннями: "Що потрібно зробити, щоб забезпечити стійкість системи стосовно заздалегідь невідомих екстремальних впливів?".

Під стійкістю ТЗ до екстремальних впливів розуміють здатність системи, що зазнала позапроектного впливу, підтримувати певний рівень експлуатаційних характеристик і повертатися на нормальний рівень функціонування (тобто відновлюватися) протягом певного інтервалу часу. Система, стійка до екстремальних впливів, має відповідати таким вимогам:

- живучість, тобто здатність функціонувати та певною мірою виконувати запропоновані функції за наявності локальних ушкоджень, що виникають унаслідок екстремальних впливів;
- надмірність, тобто наявність резервних зв'язків, альтернативних шляхів передачі навантаження та дублювальних елементів, які можуть бути задіяні у надзвичайній ситуації;
- ресурсозабезпеченість, тобто наявність у системі ресурсів, які можуть бути задіяні у разі екстремальної дії;

- здатність до швидкого відновлення, яка визначається інтервалом часу, протягом якого пошкодження можуть бути ліквідовані, тобто система буде відновлена і вийде на номінальний рівень.

Інфраструктуру вважають стійкою, якщо їй властиві низька ймовірність відмови, незначна шкода, що реалізується у разі відмови (кількість постраждалих, економічна й екологічна шкода) та малий час відновлення системи (повернення системи у нормальний стан із виходом у штатний режим експлуатації та на штатну потужність / продуктивність).

Формування багатокритеріальної моделі для оцінювання рівня захищеності об'єктів критичної інфраструктури. До багатокритеріального класу належать такі завдання: оцінювання рівня захисту об'єктів критичної інфраструктури від ризику стороннього кібервпливу. Для колегіального розв'язання цих завдань в умовах невизначеності та конфліктності між існуючими методами математичного моделювання, методами формування та дослідження узагальнених показників якості з використанням графоаналітичних та подібних підходів, експертними методами розв'язання складних завдань оцінювання та вибору будь-яких об'єктів, зокрема і спеціальних об'єктів призначення, а також аналізу та прогнозування ситуацій із великою кількістю суттєвих факторів, найраціональнішими та визначальними є експертні методи. Вони дають можливість глибше дослідити явища, які суттєво впливають на рівень захисту як держави в цілому, так і її окремих об'єктів інформаційної та кібернетичної інфраструктури від впливу внутрішніх і зовнішніх кібернетичних втручань і загроз, визначити найбільш важливе і значуще в цих процесах, не оминаючи тих деталей і взаємозв'язків, без яких неможливо побудувати модель досліджуваної проблеми. Метою цієї моделі є оцінка готовності об'єктів інформаційної та кібернетичної інфраструктури для безпечного функціонування в умовах стороннього кібервпливу та встановлення вимог до власних систем кібербезпеки на основі так званого "індексу кіберпотужності". Його величина залежить від виявлених відхилень від стандартного режиму роботи систем і мереж інтелектуальної власності й інформаційних технологій, а також апаратного та програмного забезпечення за допомогою аналізу чотирьох основних категорій, кожна з яких включає багато узагальнених показників, а саме:

- існуюча нормативно-правова база; ставлення влади до забезпечення кібербезпеки; наявність національної стратегії кібербезпеки (доктрини



тощо); наявність нормативно-правового забезпечення сфери кібербезпеки; наявність міжнародних зобов'язань країни у сфері кібербезпеки; наявність співпраці між державними та приватними структурами у сфері кібербезпеки; стан розвитку політики кіберзахисту; рівень активності керівництва країни щодо кіберзахисту; рівень активності інформаційної та кібернетичної інфраструктури з питань кіберзахисту;

- умови соціально-економічного розвитку держави; рівень освіти, науки і техніки; частка населення з вищою освітою; частка населення зі знанням іноземної мови, зокрема й англійської; частка дослідно-конструкторських робіт із кібербезпеки; рівень виконання науково-дослідної та дослідницько-конструкторської роботи (дослідження та розробки) інженерно-технічним персоналом; рівень розвитку інноваційного середовища; стан витрат на науково-дослідну та дослідницько-конструкторську роботу; стан патентної та раціоналізаторської роботи (кількість патентів); стан залучення приватного та венчурного капіталу;

- наявність розгалуженої технологічної інфраструктури: якісний стан технологічної інфраструктури; рівень використання мережі

інтернет (включно з розподілом точок доступу Wi-Fi); рівень використання мобільного зв'язку та соціальних мереж; рівень упровадження технологічної інфраструктури; рівень фінансування впровадження інформаційно-комунікаційних технологій (щодо валового внутрішнього продукту); рівень безпеки послуг;

- ступінь використання ІКТ та інформаційно-технологічного забезпечення у розвитку інформаційного суспільства; використання ІКТ у корпоративних мережах, інтелектуальних транспортних системах; використання інтернет-ресурсів для розміщення пропозицій щодо надання товарів і послуг; замовлення товарів і послуг.

На основі наведених показників, які характеризують здатність об'єктів критичної інфраструктури забезпечувати кібербезпеку та підтримувати безпечні функції власних об'єктів інформаційної та кібернетичної інфраструктури, можна побудувати ієрархічну схему їхніх показників (табл. 1), у якій значення попереднього рівня "І" визначається значеннями відповідних показників 1-го рівня. Цю категорію приведено у відповідність із набором специфічних показників, які у свою чергу представлено елементарними характеристиками, які називають індексами.

Таблиця 1

Ієрархічна схема рівня критичності кібербезпеки

Рівень 1–4	Категорії	Індикатори	Індекси
Критичність кібербезпеки, якій згідно з вихідними параметрами присвоюють рівень	Наявність нормативної бази	Ставлення керівництва держави до питань кібербезпеки	$A_{1_1}, A_{1_2}, A_{1_3}, A_{1_4}$
		Стан розвитку політики кіберзахисту	A_{2_1}, A_{2_2}
	Стан соціально-економічного розвитку держави	Освітній, науково-технічний рівень	$B_{1_1}, B_{1_2}, B_{1_3}, B_{1_4}$
		Інноваційне середовище та рівень розвитку	$B_{2_1}, B_{2_2}, B_{2_3}$
	Наявність розгалуженої технологічної інфраструктури	Якісний стан технологічної інфраструктури	C_{1_1}, C_{1_2}
		Рівень упровадження технологічної інфраструктури	C_{2_1}, C_{2_2}
	Ступінь використання ІКТ та ІБ	Використання інформаційно-комунікаційних технологій у локальній мережі	D_{1_1}, D_{1_2}
		Використання інтернет-ресурсів у комерційній діяльності	D_{2_1}, D_{2_2}

Кожній категорії рівня 2, кожному показнику рівня 3 та кожному показнику рівня 4 ієрархії за правилом, наприклад за допомогою експертного опитування, може бути присвоєно певний номер (табл. 2). Обов'язковою умовою

такого присвоєння є врахування того, що вага категорій, показників та індексів одного рівня завжди має дорівнювати одиниці.

Значення категорій і показників якості визначають способом наведеним у табл. 3.



Таблиця 2

Значення вагових коефіцієнтів категорій і показників рівня критичності КС

Позначення категорій і показників критичності	Вагові коефіцієнти категорій і позначення показників	Вагові коефіцієнти категорій і показників	Сума вагових коефіцієнтів показників
Наявність нормативної бази	g_1	0,26	
Ставлення держави до питань кібербезпеки	a_1	0,75	1,0
Розроблення політики кіберзахисту держави	a_2	0,25	
Стан соціально-економічного розвитку держави	g_2	0,25	
Освітній, науково-технічний рівень	b_1	0,68	1,0
Рівень розвитку іновативного середовища	b_2	0,32	
Наявність розгалуженої технологічної інфраструктури	g_3	0,26	
Якісний стан технологічної інфраструктури	c_1	0,22	1,0
Рівень упровадження технологічної інфраструктури	c_2	0,78	
Ступінь використання ІКТ та ІБ	g_3	0,23	
БІКТ	d_1	0,71	1,0
Використання ресурсів інтернету	d_2	0,29	

Таблиця 3

Порядок визначення категорій і показників рівня критичної кібербезпеки

<p>Наявність нормативно-правової бази –</p> $\left\{ \begin{array}{l} a_1 - < \textit{The attitude of the leadership to cybersecurity} > \\ + a_2 - < \textit{The state of cyber defense policy development} > \end{array} \right\}$ <p>де a_1 і a_2 – вагові коефіцієнти відповідних ідентифікаторів рівня 3, де $a_1 + a_2 = 1$</p>	(1)
<p>Ставлення керівництва до кібербезпеки – $-a_1 \cdot A_{11} + a_{12} \cdot A_{12} + a_{13} \cdot A_{13} + a_{14} \cdot A_{14} =$</p> $= \sum_i a_{1i} \cdot A_{1i}; i = \overline{1,4},$ <p>де $a_{11}, a_{12}, a_{13}, a_{14}$ – вагові коефіцієнти рівня 3 для $A_{11}, A_{12}, A_{13}, A_{14}$;</p> $a_{11} + a_{12} + a_{13} + a_{14} = \sum_i a_{1i} = 1$	(2)
<p>Стан розвитку політики кіберзахисту – $a_{21} \cdot A_{21} + a_{22} \cdot A_{22} = \sum_i a_{2i} \cdot A_{2i}; i = \overline{1,2}$,</p> <p>де a_{21}, a_{22} – вагові коефіцієнти відповідних показників рівня 3 для A_{21} and A_{22};</p> $a_{21} + a_{22} = \sum_i a_{2i} = 1$	(3)
<p>Стан соціально-економічного розвитку –</p> $\left\{ \begin{array}{l} b_1 - (\textit{level of education, science and technology}) \\ b_2 - (\textit{the level of development of the innovation environment}) \end{array} \right\}$ <p>де b_1 and b_2 – вагові коефіцієнти відповідних показників рівня 3 $cb_1 + b_2 = 1$</p>	(4)
<p>Рівень освіти, науки і техніки – $b_{11} \cdot B_{11} + b_{12} \cdot B_{12} + b_{13} \cdot B_{13} + b_{14} \cdot B_{14} = \sum_i b_{1i} \cdot B_{1i}; i = \overline{1,4}$,</p> <p>де $b_{11}, b_{12}, b_{13}, b_{14}$ – вагові коефіцієнти відповідних показників рівня 4 для B_{11}, B_{12}, B_{13} and B_{14};</p> $b_{11} + b_{12} + b_{13} + b_{14} = \sum_i b_{1i} = 1$	(5)



Закінчення табл. 3

Рівень розвитку інноваційного середовища – $b_{2_1} \cdot B_{2_1} + b_{2_2} \cdot B_{2_2} + b_{2_3} \cdot B_{2_3} = \sum_i b_{2_i} \cdot B_{2_i}; i = \overline{1,3}$, де $b_{2_1}, b_{2_2}, b_{2_3}$ – вагові коефіцієнти відповідних показників рівня 4 для $B_{2_1}, B_{2_2}, B_{2_3}$; $b_{2_1} + b_{2_2} + b_{2_3} = \sum_i b_{1_i} = 1$	(6)
Наявність розгалуженої технологічної інфраструктури – $\begin{cases} c_1 - (\text{qualitative state of technological infrastructure}) \\ c_2 - (\text{the level of implementation of technology infrastructure}) \end{cases}$ де c_1 та c_2 – вагові коефіцієнти відповідних ідентифікаторів рівня 3 з $c_1 + c_2 = 1$	(7)
Стан розвитку політики кіберзахисту – $c_{1_1} \cdot C_{1_1} + c_{1_2} \cdot C_{1_2} = \sum_i c_{1_i} \cdot C_{1_i}; i = \overline{1,2}$, де c_{1_1}, c_{1_2} – вагові коефіцієнти відповідних показників рівня 4 для C_{1_1} and C_{1_2} ; $c_{1_1} + c_{1_2} = \sum_i c_{1_i} = 1$	(8)
Рівень реалізації технологічної інфраструктури – $c_{2_1} \cdot C_{2_1} + c_{2_2} \cdot C_{2_2} = \sum_i c_{2_i} \cdot C_{2_i}; i = \overline{1,2}$, де c_{2_1}, c_{2_2} – вагові коефіцієнти відповідних показників 4 рівня для C_{2_1} and C_{2_2} ; $c_{2_1} + c_{2_2} = \sum_i c_{2_i} = 1$	(9)
Ступінь використання ІКТ та ІБ – $\begin{cases} d_1 - (\text{use of ICT}) \\ d_2 - (\text{Using the Internet}) \end{cases}$ де d_1 і d_2 – вагові коефіцієнти відповідних ідентифікаторів рівня 3 з $d_1 + d_2 = 1$	(10)
Використання ІКТ – $d_{1_1} \cdot D_{1_1} + d_{1_2} \cdot D_{1_2} = \sum_i d_{1_i} \cdot D_{1_i}; i = \overline{1,2}$, де d_{1_1}, d_{1_2} – вагові коефіцієнти відповідних показників рівня 4 для D_{1_1} and D_{1_2} ; $d_{1_1} + d_{1_2} = \sum_i d_{1_i} = 1$	(11)
Застосування інтернету – $d_{2_1} \cdot D_{2_1} + d_{2_2} \cdot D_{2_2} = \sum_i d_{2_i} \cdot D_{2_i}; i = \overline{1,2}$, де d_{2_1}, d_{2_2} – вагові коефіцієнти відповідних показників рівня 4 для D_{2_1} and D_{2_2} ; $d_{2_1} + d_{2_2} = \sum_i d_{2_i} = 1$	(12)

Використовуючи формули (2), (3), (5), (6), (8), (9), (11) і (12) з табл. 3 та застосовуючи дані анкети експерта, який регулює значення індексів та їхніх вагових коефіцієнтів, можна розрахувати значення показників рівня 3, таких як:

- створення державного керівництва для забезпечення кібербезпеки;
- стан розробки політики кіберзахисту;
- освітній, науково-технічний рівень;
- рівень розвитку інноваційного середовища;
- якісний стан технологічної інфраструктури;
- рівень фінансування технологічної інфраструктури;
- використання інформаційно-комунікаційних технологій;
- використання інтернет-ресурсів.

Експертна анкета для оцінювання рівня критичності кібербезпеки за параметрами наявності нормативно-правової бази на тему ставлення влади до питань кібербезпеки

Для визначення значення індексів експерт відповідає на такі питання:

- A_{1_1} – чи має держава національну стратегію кібербезпеки (доктрину, концепцію тощо)?
- A_{1_2} – чи функціонує в державі система нормативного забезпечення кібербезпеки?

- A_{1_3} – чи виконуються міжнародні зобов'язання у сфері кібербезпеки на державному рівні?

- A_{1_4} – чи існує співпраця державних і приватних структур у сфері кібербезпеки?

Відповіді на перше запитання:

- стратегія зрозуміла з чітко визначеними цілями та часовими межами;
- стратегія нечітка, незрозуміла або формальна;
- стратегія тільки розробляється;
- стратегії немає.

Відповідні значення показників 1,0; 0,4; 0,2; 0. Ваговий коефіцієнт a_{1_1} , що відповідає показнику A_{1_1} , має значення 0,4.

Відповіді на друге запитання:

- законодавство охоплює всі аспекти кібербезпеки;
- є певні закони, але лише деякі з них виконуються;
- є певні закони, але жоден із них не виконується;
- законодавство не сформоване.

Відповідні значення показників 1,0; 0,6; 0,2; 0. Ваговий коефіцієнт a_{1_2} , що відповідає показнику A_{1_2} , має значення 0,3.

Відповіді на третє запитання:

- держава практично виконує міжнародні договори;



- держава ратифікувала підписані міжнародні договори;
- держава приєдналася до міжнародних договорів;
- держава не має підписаних міжнародних зобов'язань.

Відповідні значення показників 1,0; 0,6; 0,2; 0.

Ваговий коефіцієнт a_{13} , що відповідає показнику A_{13} , має значення 0,2.

Відповіді на четверте питання:

- держава доклала значних зусиль для розвитку державно-приватного співробітництва.
- держава доклала активні, але недостатні зусилля для розвитку державно-приватного співробітництва.
- державно-приватне партнерство не реалізовано.

Відповідні значення показників 1,0; 0,5; 0.

Ваговий коефіцієнт a_{14} , що відповідає показнику A_{14} , має значення 0,1.

Отже, значення вагового коефіцієнта показників становлять 0,4; 0,3; 0,2; 0,1.

Експертна анкета для оцінювання рівня критичності кібербезпеки за параметрами доступності нормативно-правової бази для розроблення політики протидії кіберзлочинності

Для визначення показників A_{21} та A_{22} експерт відповідає на запитання:

- A_{21} – який рівень державного лідерства у сфері кіберзахисту?
- A_{22} – який рівень активності інформаційної та кібернетичної інфраструктури в кібербезпеці?
- Відповіді на перше запитання:
 - у державі створено орган виконавчої влади з питань кіберзахисту, діяльність якого визнана ефективною (значення показника 1,0);
 - є певні недоліки в діяльності органу виконавчої влади з питань кіберзахисту (значення показника 0,5);
 - орган виконавчої влади з питань кіберзлочинності в державі відсутній (значення показника 0).

Показник A_{21} відповідає ваговому коефіцієнту a_{21} , значення якого становить 0,5.

Відповіді на друге запитання:

- рівень реакції суб'єктів інформаційної та кіберінфраструктури на прояв сторонніх кіберінвестицій високий середній (значення індикатора 1,0);
- рівень реагування суб'єктів інформаційної та кібернетичної інфраструктури на прояв сторонніх кібернетичних впливів є періодичним і спонтанним (значення показника 0,5);
- суб'єкти інформаційної та кіберінфраструктури не займаються питаннями стороннього кібервпливу (значення індикатора 0).

Показник A_{22} відповідає ваговому коефіцієнту a_{22} , значення якого становить 0,5.

Експертна анкета для оцінювання рівня критичності кібербезпеки за параметрами стану соціально-економічного розвитку держави на рівні освіти, науки і технологій

Для визначення показників експерт відповідає на такі запитання:

- V_{11} – який відсоток населення держави має вищу освіту? (визначається як відсоток молоді віком від 18 до 22 років, яка здобуває освіту за денною формою навчання, до загальної кількості студентів зазначеного віку в країні).
- V_{12} – яка частина населення в державі знає іноземну мову, особливо англійську? (визначається на базі державного центру вивчення англійської мови).
- V_{13} – яка частина науково-дослідних робіт у державі присвячена дослідженням питань кібербезпеки? (визначається на основі інформації реєстраційного органу НДДКР).
- V_{14} – який рівень залучення до виконання НДДКР напряму кібербезпеки інженерно-технічного персоналу? (визначається як кількість спеціалістів, які задіяні у виконанні НДДКР на 1 млн населення країни).

Наступні відповіді на перше запитання "високий"; "середній"; "низький" зі значеннями показників 1,0; 0,5; 0.

Показник V_{11} відповідає ваговому коефіцієнту b_{11} , значення якого становить 0,2.

Відповіді на інші питання збігаються з попередніми і мають такі вагові коефіцієнти:

- b_{12} , значення якого дорівнює 0,2;
- b_{13} , значення якого 0,3;
- b_{14} , значення якого 0,3.

Експертна анкета для оцінювання рівня критичності кібербезпеки за параметрами стану соціально-економічного розвитку держави за рівнем розвитку інноваційного середовища.

Для визначення показників експерт відповідає на такі запитання:

- V_{21} – який стан витрат у державі на НДДКР у сфері кібербезпеки? (визначається як відношення поточних і капітальних витрат на НДДКР до рівня ВВП);
- V_{22} – який стан державного патенту та інноваційної діяльності у сфері кібербезпеки? (визначається як кількість патентних заявок на 1 млн населення країни);
- V_{23} – яка умова залучення приватного та венчурного капіталу у сферу кібербезпеки? (визначається відсотком приватного та венчурного капіталу до рівня ВВП країни).



Наступні відповіді на всі запитання:

- "достатній" зі значенням 1,0;
- "середній" зі значенням 0,5;
- "недостатній" зі значенням 0.

Відповідно, значення вагових коефіцієнтів b_{2_1} , b_{2_2} та b_{2_3} показників становлять 0,3; 0,4; 0,3.

Експертна анкета для оцінювання рівня критичності кібербезпеки за параметрами наявності розгалуженої технологічної інфраструктури для статусу якості технологічної інфраструктури

Для визначення значення показників C_{1_1} та C_{1_2} експерт відповідає на такі запитання:

▪ C_{1_1} – який рівень використання інтернету? (вказує кількість інтернет-користувачів на 100 осіб; розраховується на основі інформації JiWire (Wi-Fi-бази даних – точка доступу в 142 країнах));

▪ C_{1_2} – який рівень використання мобільних і соціальних мереж? (вказує кількість користувачів мобільного зв'язку на 100 осіб у відсотках від кількості користувачів до загальної кількості користувачів інтернету).

У першому випадку відповіді "високий" зі значенням показника 1,0; "середній" зі значенням показника 0,5; "низький" зі значенням показника 0; відповідають ваговому коефіцієнту c_{1_1} , значення якого становить 0,5.

Відповідно, відповіді на друге запитання відповідають попереднім і їхній ваговий коефіцієнт c_{1_2} також має значення 0,5.

Експертна анкета для оцінювання рівня критичності кібербезпеки на основі наявності розгалуженої технологічної інфраструктури за рівнем технологічної інфраструктури. впровадження .

Для визначення значення показників C_{2_1} і C_{2_2} експерт відповідає на такі запитання:

▪ C_{2_1} – який рівень фінансування заходів із впровадження ІКТ? (визначається як відсоток загального обсягу програмного забезпечення, обладнання та ІТ-послуг до рівня ВВП);

▪ C_{2_2} – який рівень безпеки послуг? (вказує на кількість серверів, які використовують технологію шифрування даних для захисту даних обміну трафіком).

У першому випадку "достатній" зі значенням показника 1,0 відповіді; "середній" зі значенням показника 0,5; "недостатній" зі значенням показника 0; відповідають ваговому коефіцієнту c_{2_1} , значення якого становить 0,5.

Згідно з наведеними вище даними, відповіді на друге запитання відповідають попереднім і їхній ваговий коефіцієнт c_{2_2} також має значення 0,5.

Експертна анкета для оцінювання рівня критичності кібербезпеки за ступенем використання ІКТ та ІТС за рахунок застосування інформаційно-комунікаційних технологій у локальній мережі

Для визначення значення показників D_{1_1} експерт D_{1_2} відповідає на такі запитання:

▪ D_{1_1} – який рівень використання ІКТ у корпоративних мережах?

▪ D_{1_2} – який рівень використання ІКТ в інтелектуальних транспортних системах?

Відповіді на перше запитання:

▪ широке використання корпоративних мереж по всій країні (значення 1,0);

▪ рівень розвитку корпоративних мереж досить високий (значення 0,6);

▪ розробляються плани впровадження корпоративних мереж (значення 0,2);

▪ в країні немає корпоративних мереж (значення 0).

Зазначимо, що показник D_{1_1} відповідає ваговому коефіцієнту d_{1_1} , значення якого становить 0,5.

Відповіді на друге запитання:

▪ високий рівень використання ІТС для розв'язання важливих функцій (зі значенням 1,0);

▪ рівень використання ІТС для розв'язання важливих функцій нижче середнього рівня (зі значенням 0,5);

▪ інтелектуальних транспортних систем не існує (зі значенням 0).

Показник D_{1_2} відповідає ваговому коефіцієнту d_{1_2} , значення якого також дорівнює 0,5.

Експертна форма для оцінювання рівня критичності кібербезпеки за ступенем використання ІКТ та ІТС із метою використання інтернет-ресурсів у торгівлі

Для визначення значення показників D_{2_1} експерт D_{2_2} відповідає на такі запитання:

▪ D_{2_1} – який відсоток користувачів інтернету розміщують пропозиції щодо надання товарів і послуг?

▪ D_{2_2} – який відсоток інтернет-користувачів замовляють товари та послуги?

Відповіді на питання показника D_{2_1} :

▪ більше 55 відсотків (значення показника 1,0);

▪ від 25 до 54 відсотків (значення показника 0,5);

▪ 0 до 24 відсотків (значення показника 0).

Ідентифікатор D_{2_2} визначається ваговим коефіцієнтом d_{2_1} і його значення становить 0,5.

Наступні відповіді на друге питання:

▪ більше 80 відсотків (значення показника 1,0);

▪ від 40 до 79 відсотків (значення показника 0,5);

▪ 0 до 39 відсотків (значення показника 0).

Відповідно, показнику D_{2_2} відповідає ваговий коефіцієнт d_{2_2} , значення якого становить 0,5.



За формулами (1), (4), (7) і (10) розраховують значення комплексних показників (категорій) другого рівня, такі як:

- а) наявність нормативної бази ($G_1^{\text{факт}}$);
- б) стан соціально-економічного розвитку держави ($G_2^{\text{факт}}$);
- в) наявність розгалуженої технологічної інфраструктури ($G_3^{\text{факт}}$);
- г) ступінь використання ІКТ та ІТС ($G_4^{\text{факт}}$).

Індекс кіберпотужності ($G_{\text{sec.level}}$) з погляду експерта можна розрахувати за такою формулою:

$$G_{\text{sec.level}} = \left(\sum_{i=1}^n (g_i \times G) \right) \times 100\%, \quad (13)$$

де g_i – ваговий коефіцієнт s категорій другого рівня ієрархії $G_i^{\text{факт}}$; n – кількість категорій (в цьому випадку $n=4$).

Рішення щодо спроможності держави протистояти кібератакам здійснюватиметься за 100-бальною шкалою за таким правилом:

- якщо $90 < g_{\text{sec.level}} < 100$, то рівень захисту держави від ризику зовнішнього кібервпливу вважають достатньо високим для забезпечення безпечного функціонування її об'єктів інформаційної та кіберінфраструктури;

- якщо $45 < g_{\text{sec.level}} < 90$, то рівень захисту держави від ризику зовнішнього кібервпливу можливий для забезпечення безпечного функціонування її об'єктів інформаційної та кіберінфраструктури;

- якщо $g_{\text{sec.level}} < 45$, то рівень захисту держави від ризику зовнішнього кібервпливу вважають недостатнім для забезпечення безпечного функціонування її об'єктів інформаційної та кіберінфраструктури.

Дискусія і висновки

Існуючі нині методики безпеки технічних систем розроблено для систем, що мають чіткі межі і добре визначені переліки загроз. Для цих систем можуть бути створені бази даних зі статистики аварій, які дозволяють кількісно оцінювати та верифікувати моделі. Ці методики, що базуються на побудові сценарних "дерев" (моделі типу "дерево" подій, "дерево" відмов), були розроблені без урахування позапроектних впливів і не дозволяють належно врахувати складність критичних інфраструктур, функціонування яких визначається взаємодією технічних, організаційних і соціальних факторів.

У зазначених методиках аварії, що розвиваються в технічних системах, розглядають як лінійні послідовності подій. Ці моделі мають обмежені можливості, коли доводиться описувати розвиток аварій у складних техносоціальних системах, як критичні інфраструктури,

які передбачають нелінійні взаємодії між компонентами, петлі зворотних зв'язків, множинні джерела аварій тощо. Традиційний підхід до моделювання аварій не дозволяє описувати сценарії відмов у складних системах, які, зазвичай, відбуваються не внаслідок окремої події, що ініціює (технічної відмови елемента системи або помилки оператора), а є наслідком кількох взаємопов'язаних факторів, що діють на різних рівнях системи. До цих факторів належать технічні відмови, людські помилки, зовнішні екстремальні впливи, латентні умови, пов'язані з такими аспектами, як практика управління діючою системою або етнокультурні особливості персоналу, зовнішні ініціувальні події.

Дослідження критичних інфраструктур як соціотехнічних систем потребує оцінювання складних взаємодій між технічними, соціальними й організаційними рівнями системи. Тому КІ варто розглядати як єдине ціле. Причому необхідно наголошувати на одночасному спільному розгляді технічних, організаційних і соціальних факторів, що визначають стан системи та динаміку її розвитку. Щоб забезпечити безпеку таких систем, необхідно вийти за межі традиційного підходу до оцінювання проектних ризиків і перейти до нової парадигми, що ґрунтується на забезпеченні безпеки КІ за критерієм стійкості до позапроектних впливів. У зв'язку з необхідністю включити до розгляду позапроектні аварії на КІ, межі досліджень мають бути суттєво розширені. Заходи щодо забезпечення безпеки повинні бути спрямовані не тільки на створення захисних бар'єрів, покликаних попередити реалізацію проектних аварій, що постулюються, але і на підвищення стійкості та живучості КІ у разі позапроектних впливів, тобто зосередитися на запобіганні великомасштабним катастрофам і тривалим перервам у функціонуванні.

Можливість позапроектних впливів, що мають низьку ймовірність реалізації та тяжкі наслідки, має враховуватися під час оцінювання захищеності критичних інфраструктур. Це вимагатиме реалізації додаткових заходів, спрямованих на підвищення стійкості КІ у випадку позапроектних впливів.

Нова парадигма забезпечення безпеки КІ й інших складних систем має концентрувати увагу не лише на створенні захисних бар'єрів і реалізації охоронних заходів, спрямованих на парировання проектних аварій, а й на підвищенні стійкості КІ щодо позапроектних аварій. Причому новий підхід до забезпечення безпеки КІ, що розробляється, має розглядатися не як заміна, а скоріше як доповнення до традиційного підходу.



Отже, запропонована стратегія дасть можливість отримати кількісну оцінку рівня захисту ОСІ від ризику зовнішнього кібернетичного впливу, встановити організаційні вимоги до власних систем кібернетичної безпеки та розробити заходи, спрямовані на підвищення їхньої ефективності. Підставою для таких дій може бути виявлення відхилень від нормального режиму роботи ІР, ІТ-систем і мереж, а також відповідного програмного й апаратного забезпечення, зокрема і виявлення таких ознак:

- поломка окремих компонентів електронних систем;
- зміна алгоритмів функціонування програмного забезпечення в ІТ-системах і системах управління мережами;
- несанкціоновані зміни файлів (їхніх розмірів і останньої дати модифікації);
- порушення безпеки обміну інформацією, протоколів передачі даних вхідного або вихідного трафіку, а також прав доступу до ІР-користувачів;
- уповільнення завантаження і роботи ПК;
- зменшення обсягу оперативної пам'яті;
- виконання неконтрольованих процесів тощо.

Крім того, у процесі завантаження ОС може виявлятися багато помилок, через неможливість збереження файлів у потрібних каталогах, а також незрозумілі системні повідомлення, музичні та візуальні ефекти.

Внесок авторів: Сергій Толюпа – концептуалізація; методологія; аналіз джерел; Анатолій Шевченко – збір емпіричних даних та їхня валідація; емпіричне дослідження; Андрій Кулько – підготування огляду літератури або теоретичних засад дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Бірюков, Д., & Кондратов, С. (2012). *Захист критичної інфраструктури, проблеми та перспективи впровадження в Україні*. Національний інститут стратегічних досліджень.

Гнатюк, С., & Лядовська, В. (2013,). Критерії визначення елементів критичної інфраструктури держави. У Р. Сущенко, Л. Веремесенко, Д. Шелунцов (Ред.). *Матеріали XXIII Всеукраїнської практичної конференції. Іноваційний потенціал світової науки XXI століття* (с. 55–57). Національна академія СБУ. <https://zp.edu.ua/>

Довгань, О. (2013). Критична інфраструктура як об'єкт захисту від кібернетичних атак. У Н. М. Мармоленко, О. П. Власенко, С. В. Ангелуца, Н. М. Лашкет (Ред.). *Інформаційна безпека: виклики та загрози сучасності: матеріали науково-практичної конференції* (с. 17–20). Національна академія СБУ. <https://er.nau.edu.ua/bitstream/NAU/27208/1/2013>

Юдін, А., & Пирогов, Г. (2013). Аналіз та оцінка нормативних документів, що використовуються для забезпечення інформаційної безпеки систем Smart Grid. *Правова, нормативна та метрологічна функціональність системи захисту інформації в Україні*, 1, 88.

Бурячок, В., Толюпа, С., Толубко, В., & Хорошко О. (2022). Інформаційна та кібербезпека: соціотехнічний аспект. У С. Даков, О. Горошанко, Я. Шестак, Ю. Бабенко (Ред.). *VII міжнародна науково-практична конференція: Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)* (с. 288). Київський національний університет імені Тараса Шевченка. <https://pcsits.knu.ua/>

REFERENCES

Buryachok, V., Tolyupa, S., Tolubko, V., & Khoroshko, O. (2022). Information and cyber security: socio-technical aspect. In S. Dakov, O. Toroshanko, Ya. Shestak, Yu. Babenko. *VII international scientific and practical conference, Problems of cyber security of information and telecommunication systems (PCSITS)* (p. 288). Taras Shevchenko National University of Kyiv [in Ukrainian]. <https://pcsits.knu.ua/>

Biryukov, D., & Kondratov, S. (2012). *Protection of critical infrastructure, problems and prospects of implementation in Ukraine*. National Institute of Strategic Studies [in Ukrainian].

Dovgan, O. (2013). Critical infrastructure as an object of protection against cyber attacks. In N. M. Marmolenko, O. P. Vlasenko, S. V. Angelutsa, N. M. Lashket (Eds.). *Information security: modern challenges and threats: materials of the scientific and practical conference* (pp. 17–20). National Academy of the Security Service of Ukraine [in Ukrainian]. <https://er.nau.edu.ua/bitstream/NAU/27208/1/2013>

Hnatyuk, S., & Lyadovska, V. (2013,). Criteria for determining the elements of the state's critical infrastructure. In R. Sushchenko, L. Veremeyenko, D. Sheluntsov (Eds.). *Materials XXIII All-Ukrainian pr. Conference. Innovative potential of global science of the 21st century* (pp. 55–57). National Academy of the Security Service of Ukraine [in Ukrainian]. <https://zp.edu.ua/>

Yudin, A., & Pirogov, G. (2013). Analysis and assessment of regulatory documents used to ensure information security of Smart Grid systems. *Legal, regulatory and metrological functionality of the information protection system in Ukraine*, 1, 88 [in Ukrainian].

Отримано редакцією журналу / Received: 17.03.24
Прорецензовано / Revised: 27.03.24
Схвалено до друку / Accepted: 13.05.24



Serhii TOLIUPA, DSc (Engin.), Prof.
ORCID ID: 000-0002-1919-9174,
e-mail: tolupa@i.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Anatoliy SHEVCHENKO, brigadier general
ORCID ID: 0000-0003-2723-0378
e-mail: anatolii.shevchenko@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Andriy KULKO, PhD Student
ORCID ID:0009-0006-1185-0774,
e-mail: kulko452@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

FEATURES OF ENSURING SECURITY OF CRITICAL INFRASTRUCTURES

Background. *The rapid development of information technologies over the past two decades has impacted the functioning of critical infrastructure facilities. These technologies have begun to be used not only for the exchange and processing of information, but also as a tool for reducing harm. The protection of sovereign interests in the political context is the primary basis for ensuring the national security of the country, which explains the need for the creation and constant development of strong cyber security. Critical infrastructure facilities are foldable, spaciouly distributed, rich in component systems, the stability of the robot is critical for the functioning of the economy and the livelihood of the household. They have a rich structure, which includes: a range of technical components; social rheum; organizational level and level of state governance.*

Methods. *For monitoring information systems and methods for assessing the security of systems.*

Results. *The investigation of critical infrastructures as socio-technical systems will require an assessment of the complex interactions between the technical, social and organizational levels of the system. Therefore, it is important to look at critical infrastructure as a whole. In this case, it is necessary to speak at a one-hour close examination of the technical, organizational and social factors that indicate the structure of the system and the dynamics of its development. Schobstecchita to the nonsense of such systems, it is not possible to pray beyond the traditions of the tradition to the zziki projected Riziki, to go to the new paradigmes, and the blessing of the nonsense of the critical sinfrastructure for the criterly wrecks to the designed areas. Due to the need to include the consideration of design basis accidents on critical infrastructure, the scope of surveillance may be expanded accordingly. Come to the point of ensuring the safety of those responsible not only for the creation of dry-barriers that occur ahead of the implementation of project-based accidents that are postulated, but also for the improvement of the resistance and survivability of critical infrastructure times beyond the project inflows, in order to focus on avoided large-scale disasters and troubling interruptions in the functioning of, and the creation of a rich criteria model for assessing the level of security of critical infrastructure objects will give a more comprehensive picture of the status of the critical infrastructure object.*

Conclusions. *The current safety methods for technical systems are divided into systems that have clear boundaries and well-defined danger flows. For these systems, a database of accident statistics can be created, which allows for precise evaluation and verification of models. These methods, which are based on case-by-case scenario "trees" (models of the type "tree" of ideas, "tree" of views), were fragmented without the coordination of design inputs and do not allow for proper management of the complexity of critical infrastructures functioning in is determined by the interaction of technical, organizational and social factors.*

Keywords: *cyber security, critical infrastructure facilities, information systems, resilience, cyber power.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.



УДК 004.056

DOI: <https://doi.org/10.17721/ISTS.2024.7.24-30>

Олександр ТОРОШАНКО, канд. техн. наук, асист.

ORCID ID: 0000-0002-2354-0187

e-mail: toroshanko@gmail.com

Київський національний університет імені Тараса Шевченка, Київ, Україна

Юрій ЩЕБЛАНІН, канд. техн. наук ст. наук. співроб.

ORCID ID: 0000-0002-3231-6750

e-mail: y.shcheblanin@gmail.com

Київський національний університет імені Тараса Шевченка, Київ, Україна

Олег КУРЧЕНКО, канд. техн. наук, доц.

ORCID ID: 0000-0002-3507-2392

e-mail: kuro1@ukr.net

Київський національний університет імені Тараса Шевченка, Київ, Україна

ПОРІВНЯННЯ МОДЕЛЕЙ ЗРІЛОСТІ ПРОЦЕСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ (КОМПАНІЇ)

Вступ. Зростання зловмисної активності в інформаційному та кібернетичному просторах ставить перед керівниками підприємств (організацій) і власниками компаній додаткові завдання та вимоги щодо захисту своїх активів. Втрата активів, наприклад, фінансового або технологічного, може призвести до неможливості виконання компанією своєї базової функції – приносити прибуток.

Методи. Використано методи аналізу ризиків інформаційної безпеки.

Результати. Організації витрачають значні фінансові ресурси на придбання й експлуатацію технологій захисту, створюють відповідні структурні підрозділи, завданнями яких є оцінювання та забезпечення відповідного рівня інформаційної безпеки підприємства (компанії). Водночас існує ризик настання ситуації, коли, використовуючи сучасніші технології, зловмисники зможуть подолати систему захисту компанії та завдати неповоротних втрат як фінансових, так і репутаційних.

Висновки. Одним із напрямів розв'язання цієї проблеми є створення системи управління інформаційною безпекою (СУІБ), яка є складовою загальної системи управління організації (компанії) і ґрунтується на оцінюванні бізнес-ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки організації (підприємства). СУІБ містить організаційну структуру організації (компанії), її політики, питання планування, контроль за дотриманням вимог посадових обов'язків, впровадження сучасних практик, контроль та супроводження процесів ресурсів. Крайці світові практики, для оцінювання рівня інформаційної безпеки організації, рекомендують використовувати підхід, що базується на можливостях моделей зрілості процесів. Отримані результати можна використовувати для вдосконалення або оптимізації створеної системи інформаційної безпеки організації (компанії). Нині для організації (компанії) доступний великий набір моделей оцінювання зрілості інформаційної безпеки, побудованих на схожих принципах. Причому реальне використання таких моделей досить обмежене, в першу чергу через слабе прив'язування до особливостей конкретних організацій.

В роботі розглянуто моделі зрілості процесів, їхню структуру та можливості використання у процесі оцінювання рівня інформаційної безпеки.

Ключові слова: модель, оцінювання зрілості, загроза, інформаційна безпека.

Вступ

Зростання зловмисної активності в інформаційному та кібернетичному просторах ставить перед керівниками підприємств (організацій) і власниками компаній додаткові завдання та вимоги, щодо захисту своїх активів. Втрата активів, наприклад, фінансового або технологічного, може призвести до неможливості

виконання компанією своєї базової функції – приносити прибуток.

Для досягнення зазначеної мети доцільно впроваджувати й активно використовувати сучасні інформаційні технології та рішення з інформаційної та кібернетичної безпеки. Саме такий підхід створює основу для якісного забезпечення безпеки основних процесів компанії

© Торощанко Олександр, Щєбланін Юрій, Курченко Олег, 2024



(організації). Керівники компаній зацікавлені, щоб реалізовані бізнес-процеси відповідали концепції захисту своїх активів, що полягає у зменшенні ймовірності кількості помилок або зловмисних дій із боку працівників компанії та бізнес-партнерів.

Ненадання належної уваги оцінюванню рівня інформаційної безпеки та захисту інформації в компанії може призвести до репутаційних ризиків і банкрутства. Відповідно діяльність, орієнтована на аналіз загроз і ризиків, є визначальною у побудові ефективної системи інформаційної та кібернетичної безпеки. Відповідно до статистики, витікання 20 % інформації з обмеженим доступом, що належить компанії, в 60 випадках зі 100 призводить до банкрутства підприємства (Гребенніков, & Щєбланін, 2018).

Прийняття рішення щодо розроблення та впровадження системи управління інформаційною безпекою в організації має відповідати рівню організаційного та технологічного розвитку компанії, а саме її процесів забезпечення інформаційної безпеки. Вимоги до впровадження рішень з інформаційної та кібернетичної безпеки мають враховувати рівні зрілості процесів у конкретній організації (компанії).

Нині гостро постає питання підвищення рівня інформаційної безпеки підприємства, яка напряму впливає на залучення інвестицій і впровадження сучасних технологій.

Використання "моделей зрілості" дозволяє визначити рівень технологічного й організаційного розвитку компанії та, відповідно, її бізнес-процесів, розвиток інформаційних технологій (ІТ) компанії значно впливає на конкурентоспроможність, а забезпечення її базових показників інформаційної безпеки – на неперервну діяльність.

Мета статті – порівняти можливості використання моделей зрілості ІТ-процесів під час оцінювання рівнів інформаційної безпеки організації (компанії).

Методи

В роботі використано методи аналізу ризиків інформаційної безпеки.

Результати

Оцінювати та вдосконалювати свої розробки з питань інформаційної та кібернетичної безпеки компаніям може суттєво допомогти використання моделей зрілості процесів інформаційної безпеки.

Інструментом вимірювання стану процесу на основі набору метрик, які являють собою певні характеристики, є модель зрілості. Використання метрик, запропонованих у моделях, дає змогу оцінити стан процесів інформаційної безпеки (ІБ),

що у свою чергу є характеристикою рівня зрілості. Після завершення оцінювання зрілості процесів, керівництво ухвалює відповідні рішення щодо впровадження заходів із підвищення рівня зрілості процесів інформаційної безпеки організації (компанії).

У практиці зарубіжних країн широко розвинене застосування моделей зрілості, які є як інструментом управління, так і інструментом оцінювання рівня інформаційної безпеки компанії.

Національні компанії зрідка використовують підхід оцінювання та забезпечення інформаційної безпеки, оснований на моделях зрілості, хоча в цьому є необхідність. Наприклад, стандарт ДСТУ ISO/IEC 27001 вимагає наявності в організації процедури аналізу ризиків. Тому виникає актуальне питання, яким чином забезпечити виконання вимог стандарту, з урахуванням обсягу робіт, рівня деталізації та масштабів організації (компанії). В більшості випадків фахівці з інформаційної безпеки орієнтуються на масштаб організації і дуже рідко аналізують рівень її організаційного та технологічного розвитку. Саме відповідь на це питання допоможе надати модель зрілості, яка враховує рівень зрілості процесів інформаційної безпеки організації (компанії).

Залежно від того, який рівень зрілості мають процеси інформаційної безпеки організації, є сенс впроваджувати ту чи іншу діяльність, наприклад, якщо рівень низький, то реалізація процедури оцінювання ризиків із залученням значних ресурсів є недоцільною і може полягати у експертному оцінюванні ризиків та визначенні найпріоритетніших напрямків безпеки. Якщо рівень зрілості процесів інформаційної безпеки в організації на високому рівні, тоді має бути реалізована процедура оцінювання ризиків з урахуванням спеціалізованих методів, шкал тощо.

Для оцінювання рівня інформаційної безпеки відомо більше 10 моделей, які мають свої переваги й недоліки, в межах статті розглянемо найвідоміші з них:

- Business Process Management Maturity Model (BPMM) – розроблена компанією Gartner Group;
- Open Information Security Management Maturity Model (O-ISM3) – розроблена незалежним консорціумом The Open Group;
- NISTIR-7358 методологія PRISMA – розроблена National Institute of Standards and Technology;
- Community Cyber Security Maturity Model (CCSMM) – розроблена The Center for Infrastructure Assurance and Security The University of Texas;
- Cybersecurity Capability Maturity Model (C2M2) – розроблена Міністерством енергетики (DOE) США (Department of Energy..., 2014).



Модель Business Process Management Maturity Model (BPM3M) – це модель, розроблена фахівцями аналітичної компанії Gartner Group, яка виділяє чотири рівні – з нульового до третього.

Нульовий рівень – необхідність забезпечення інформаційної безпеки організацією належним чином не усвідомлена і формально таке завдання не ставиться. Служба ІБ не створена. Підрозділ інформаційних технологій використовує традиційні механізми й засоби захисту інформації в локальній обчислювальній мережі та сервісах інтернету, а також операційного середовища та додатків (операційні системи, СУБД, системи підтримки та прийняття рішень тощо).

Перший рівень – проблему забезпечення ІБ керівництво організації розглядає лише у технічній площині. Службу ІБ не створено. Організаційні заходи підтримки ІБ не вживаються. Фінансування здійснюється в межах єдиного бюджету на ІТ. Підрозділ ІТ додатково до засобів рівня 0 може залучати засоби відмовостійкості, резервного копіювання інформації, джерела безперебійного живлення, міжмережні екрани, віртуальні приватні мережі, антивірусні засоби, засоби шифрування тощо.

Другий рівень – важливість забезпечення ІБ керівництвом організації усвідомлено та розглядається як взаємопов'язаний комплекс організаційних і технічних заходів. В організації впроваджено методики аналізу ризиків ІБ, які відповідають мінімальному рівню захищеності інформаційної системи. Визначено склад і структуру штатної служби ІБ. Розроблено політику безпеки організації. Фінансування, створення та підтримку системи забезпечення ІБ ведуть з окремого бюджету. Служба ІБ додатково до засобів рівнів 0 та 1 упроваджує засоби захисту від несанкціонованого доступу, системи виявлення вторгнень, засоби шифрування, а також організаційні заходи, які відповідають прийнятій політиці безпеки (зовнішній та внутрішній аудит ІБ, плани захисту та безперервності бізнесу, план дій у позаштатних ситуаціях тощо).

Третій рівень – проблему забезпечення ІБ організацією усвідомлено повною мірою. Поряд із бізнес-культурою існує поняття культури ІБ. Активно застосовуються методики повного кількісного аналізу ризиків ІБ та відповідні інструментальні засоби. Введено штатну посаду – керівника служби ІБ (CISO). Визначено склад і структуру групи внутрішнього аудиту ІБ (CISA), групи попередження та розслідування комп'ютерних злочинів, групи економічної безпеки. Керівництвом організації затверджено концепцію

та політику ІБ, план захисту й інші нормативно-методичні матеріали та посадові інструкції. Фінансування виділяють виключно у межах окремого бюджету. Служба ІБ додатково до засобів рівнів 0–2 звертається до засобів централізованого управління ІБ і засобів інтеграції з платформами управління мережними ресурсами.

Отже, модель BPM3M є багатовимірною й дозволяє аналізувати процеси організації за такими критеріями: керівництво, персонал, стратегія, методики, ІТ тощо.

Модель Open Information Security Management Maturity Model розроблена незалежним консорціумом The Open Group і враховує вимоги ISO/IEC 27000.

Модель оцінює рівень зрілості функціонування процесів системи управління інформаційною безпекою організації (компанії) та орієнтована допомагати фахівцям з інформаційної безпеки оцінювати власну робочу інфраструктуру та планувати процеси управління інформаційною безпекою компанії (The Open Group Releases Maturity Model for Information Security Management).

Головною вимогою O-ISM3 є задокументованість, вимірюваність і керованість процесами управління інформаційною безпекою, також мають бути зафіксовані бізнес-цілі компанії, на основі яких визначають мету й основні завдання управління інформаційною безпекою. Модель O-ISM3 відрізняється від інших тим, що вона передбачає оцінювання зрілості всіх процесів (заходів безпеки), які використовують у системі управління інформаційною безпекою. Тому керувати контролем (згідно з процесним підходом) можливо за допомогою оцінювання рівня його зрілості.

В моделі O-ISM3 застосовано чотири рівні управління інформаційною безпекою, саме вони дозволяють оцінити зрілість процесів ІБ (The Open Group Releases Maturity Model for Information Security Management):

- базовий, який належить до загального управління та включає три види контролю;
- стратегічний (керівництво і забезпечення) рівень, де встановлюють стратегічні цілі, здійснюють координаційні дії та розробляють механізм забезпечення ресурсами, який містить чотири види контролю;
- тактичний (впровадження й оптимізація) рівень, на якому розробляють і впроваджують систему управління інформаційною безпекою за допомогою встановлення специфічних цілей та управління ресурсами, включає 12 видів контролю;
- операційний (виконання і звітність) рівень, цілей якого досягають технічними процесами та передбачають 26 видів контролю.



Процеси управління за моделлю O-ISM3 класифіковано на п'ять рівнів зрілості:

- 1-й рівень зрілості – Initial (початковий);
- 2-й рівень зрілості – Managed (керований);
- 3-й рівень зрілості – Defined (орієнтований);
- 4-й рівень зрілості – Controlled (контрольований);
- 5-й рівень зрілості – Optimized (оптимізований).

Метрики моделі розділено на такі типи: діяльність, масштаб, відсутність, результативність, навантаження, якість, ефективність (Activity, Scope, Unavailability, Effectiveness, Load, Quality, Efficiency) й описують ресурсовитратність обраного методу управління. Поточний рівень процесу, залежить від наявної документації та метрик, які використовують для управління ним.

Отже, модель O-ISM3 розроблена для різних типів організацій (компаній), комерційних фірм, неурядових організацій та

- може бути використана в організації (компанії) незалежно від розміру, контексту та її ресурсів;
- вимагає високої професійної підготовки фахівців з інформаційної безпеки та потребує високої деталізації процесів інформаційної безпеки;
- дозволяє організаціям (компаніям) визначати пріоритетність інвестицій у безпеку та оптимізувати їх за потреби;
- дозволяє безперервно покращувати систему управління інформаційною безпекою на основі використання метрик (Рой, Рябчун, & Єрмошин, 2020).

Модель зрілості NISTIR 7358 – методологія PRISMA, яку розроблено National Institute of Standards and Technology, засновано на Capability Maturity Model (CMM) Software Engineering Institute (SEI).

Методологія PRISMA (Гребенніков, & Щєбланін, 2018) створена з метою виявлення й оцінювання слабких місць у процесах управління інформаційною безпекою, забезпечення рентабельності впровадження СУІБ, оцінювання комерційних пропозицій у вказаній сфері та встановлення можливості їхнього застосування в державних ІТ-системах США.

Запропонована модель представляє собою підхід, оснований на процесах оцінювання ризиків та оцінювання ефективності управління ІБ.

Особливістю моделі PRISMA є те, що документи з ІБ оцінюють за такими основними напрямками ІБ (Computer security resource center):

- управління інформаційною безпекою та культура;
- інформаційне планування безпеки;
- розуміння процесів безпеки, навчання й освіти;

- ресурси та бюджет;
- управління життєвим циклом системи безпеки;
- сертифікація та акредитація системи інформаційної безпеки;
- захист критичної інфраструктури;
- інциденти та реагування на них;
- засоби безпеки та контролю.

В результаті використання моделі PRISMA користувач отримує таблицю, яка відображає оцінку зрілості процесів ІБ. В моделі PRISMA застосовано п'ять рівнів, а саме:

- 1-й рівень зрілості – Policies (політики);
- 2-й рівень зрілості – Procedures (процедури);
- 3-й рівень зрілості – Implementation (впровадження);
- 4-й рівень зрілості – Test (тестування);
- 5-й рівень зрілості – Integration (інтеграція).

Вищого рівня зрілості ІБ досягають лише тоді, коли попереднього рівня зрілості вже досягнуто. П'ятий рівень зрілості являє собою найвищий рівень забезпечення інформаційної безпеки.

Для оцінювання зрілості ІБ організації (компанії), проводять розгляд та аналіз документації з ІБ, беруть інтерв'ю у працівників організації та оцінюють розбіжності кожного з напрямів ІБ.

Для оцінювання напрямів ІБ вводять критерії, які мають бути документально зафіксовані. Ці критерії являють собою метрики моделі й застосовуються на кожному з рівнів зрілості.

Оцінка виконання організацією критерію, тобто оцінка метрики, може мати таку класифікацію: "Відповідний", "Частково відповідний", "Невідповідний".

Оцінка зрілості ІБ починається з першого рівня (Policies (політики)), якщо для всіх розглянутих документів критерію оцінка "Невідповідний", то весь рівень отримує ту саму оцінку за вказаним критерієм. Однак, якщо у критерії для деяких документів є оцінка "Відповідний", але оцінка одного або більшої кількості документів "Частково відповідний" / "Невідповідний", тоді загальна оцінка критерію для рівня буде "Частково відповідний".

Отже, методологію PRISMA, як варіант, можна застосовувати в оцінюванні процесів СУІБ:

- незважаючи на масштаби організації (компанії) та її ресурси;
- коли основою для оцінювання рівня зрілості СУІБ компанії є документи, в яких описано та затверджено відповідні бізнес-процеси;
- коли рівень оцінювання процесів має значення "Частково відповідний" і визначається у відсотках виконаної реалізації.



Модель оцінювання зрілості процесів забезпечення інформаційної безпеки (Community Cyber Security Maturity Model). Зусилля урядових організацій і приватних компаній у США були зосереджені на розробленні програми безпеки, яка надала б їм інструмент спільного прогнозування кібератак, їх виявлення, реагування на них і відновлення процесів організацій (компаній).

Завдання полягало не лише в тому, щоб мати інформацію, де вони в даний час перебувають у плані їхньої підготовки до відбиття кібератаки, але і де вони мають перебувати, щоб покращити свій поточний стан. Для розв'язання поставленого завдання була створена суспільна модель зрілості кібербезпеки – Community Cyber Security Maturity Model .

Модель розробляли з урахуванням досвіду використання моделей зрілості програмного забезпечення Capability Maturity Model (СММ або SW-CMM) та інженерних систем безпеки Systems Security Engineering Capability Maturity Model (SSE-CMM), що дозволяло розробити варіанти взаємодії різних організацій (компаній) між собою, спрямовані на підвищення ефективності протидії кіберзлочинності (The Systems Security Engineering Capability Maturity Model). Така модель враховує не лише метрики, а й технології, відомі вразливості та методи тестування, спільне використання яких дозволить оцінити поточний стан рівня інформаційної безпеки організації (компанії).

В розробленій моделі виділено рівні зрілості, які враховують типи загроз і діяльність із рівнів (The Systems Security Engineering Capability Maturity Model):

1-й рівень зрілості – Security Aware (про безпеку відомо);

2-й рівень зрілості – Process Development (розвиток процесів);

3-й рівень зрілості – Information Enabled (встановлено інформування);

4-й рівень зрілості – Tactics Development (розвиток тактики);

5-й рівень зрілості – Full Security Operational Capability (повна безпека експлуатованих можливостей).

Для оцінювання рівня зрілості процесів організації (компанії) в моделі запропоновано такі критерії:

- перелік загроз, які слід розглядати та які можуть бути усунені (The Threat Addressed);
- метрики: громадяни, керівництво, виробництво (Citizens, Government, Industry);
- інформаційний обмін (Information Sharing);

- технології безпеки (Technology);
- навчання (Training);
- тестування (Test).

Cybersecurity Capability Maturity Model (C2M2) – модель зрілості можливостей кібербезпеки є інструментом для оцінювання й покращення рівня кібербезпеки. Була розроблена 2012 р. енергетичним сектором Міністерства енергетики США.

Використання C2M2 дозволяє організаціям усіх секторів, типів і розмірів оцінити та вдосконалити свої програми кібербезпеки та підвищити їхню операційну стійкість. C2M2 зосереджено на впровадженні й управлінні методами кібербезпеки, пов'язаними з активами ІТ та операційних технологій (ОТ), а також із середовищами, в яких вони працюють.

Модель зрілості можливостей ES-C2M2 використовує чотирирівневу структуру для оцінювання стану безпеки кожної області. Ці рівні можуть бути представлені у вигляді трьохетапного процесу. Перший етап являє собою відправну точку з відсутніми процесами менеджменту інформаційної безпеки й невизначеними політиками безпеки. На другому етапі акцент роблять на впровадження стандартів безпеки і формалізованих процесів управління. Останній етап передбачає практично повністю автоматизоване управління безпекою підприємства. На цьому етапі досягають максимально можливого рівня захисту від кіберзагроз, а сама організація отримує стійкість до кібератаки.

В таблиці наведено порівняльний аналіз розглянутих моделей зрілості за такими критеріями як: тип моделі, кількість рівнів зрілості, масштаб моделі та рівень професійної підготовки працівників.

Розглянуті моделі зрілості створено з метою розв'язання конкретних задач і завдань. Вони використовують процесний підхід для визначення рівня зрілості, причому відсутнє єдине трактування поняття зрілості, в силу того, що кожна модель орієнтована на розв'язання конкретного завдання.

Для визначення рівня інформаційної безпеки необхідно враховувати конкретний набір метрик, які дозволяють розкрити рівень зрілості процесів інформаційної безпеки. Кожна модель пропонує використовувати свій набір метрик для оцінювання зрілості процесів, збігів серед яких практично немає.



Таблиця

Порівняння моделей зрілості оцінювання рівня ІБ

Критерії оцінювання моделей	ВРМММ	O-ISM3	NISTIR 7358	CCSMM	C2M2
Тип моделі	Описова	Описова	Описова	Описова	Описова
Кількість рівнів зрілості	4	5	5	4	4
Масштаб моделі	Уся структура організації	СУІБ організації	Документація ІБ організації	Процеси ІБ організації	ІТ-активи підприємства
Рівень професійної підготовки працівників	Середній	Високий	Середній	Низький	Середній

До недоліків можна віднести такий: розглянуті моделі не враховують рівень забезпеченості ресурсами процесів інформаційної безпеки організації. Водночас такі критерії, як розвиненість і стабільність процесів управління українських і зарубіжних компаній мають значні відмінності, що вимагає проведення адаптації моделей зрілості для їхнього використання.

Дискусія і висновки

Розглянуті моделі зрілості процесів рекомендуються до використання кращими світовими практиками у сфері інформаційної безпеки. Вони дозволяють керівникам компаній контролювати стан інформаційної безпеки, своєчасно реагувати на інциденти інформаційної безпеки й розробляти напрями модернізації ІБ та СУІБ організації (компанії).

Результати оцінювання зрілості процесів СУІБ відповідають на такі важливі питання:

- рівень документування бізнес-процесів і процесів ІБ;
- яким способом і з використанням яких ресурсів забезпечуються вимоги до підтримки того чи іншого процесу на заданому рівні;
- чи дотримується організація (компанія) рекомендацій кращих практик зі створення та підтримки функціонування СУІБ тощо.

Проведені дослідження показали, що для оцінювання можливості впровадження розглянутих моделей зрілості на практиці є потреба глибокого розуміння базової моделі організації (тобто треба знати, для якого переліку завдань вона розроблялась), не можливо впевнено стверджувати, чи можна її застосовувати для розв'язання наших завдань.

Досліджені в роботі моделі зрілості процесів доцільно використовувати як еталон для розроблення моделі зрілості, беручи за основу власну базову модель з урахуванням метрик, властивих конкретному об'єкту. Оптимальним рішенням нині виглядає впровадження будь-якої

з існуючих моделей оцінювання з подальшою її адаптацією і розширенням під власні потреби.

Подальші дослідження доцільно проводити, створюючи модель оцінювання, яка враховуватиме національну нормативно-правову базу, рівень підготовки фахівців організації (компанії) та обсяг фінансування процесів ІБ.

Внесок авторів: Олександр Горошанко – концептуалізація; методологія; аналіз джерел, підготовка огляду літератури або теоретичних засад дослідження; Юрій Щєбланін – збір емпіричних даних та їхня валідація; Олег Курченко – емпіричне дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Гребенніков, А., & Щєбланін, Ю. (2018). Аналіз використання моделей зрілості процесів у ході оцінювання рівня інформаційної безпеки. *Сучасний захист інформації*, 1(33), 33–37.

Рой, Я. В., Рябчун, О. П., & Єрмошин, В. В. (2020). Модель зрілості можливостей системи кібербезпеки на об'єктах критичної інфраструктури енергетичного сектору ES-C2M2. *Кібербезпека: освіта, наука, техніка*, 2(10), 67–72.

Department of Energy: Cybersecurity Capability Maturity Model (2014). Version 1.1, Department of Homeland Security. <https://www.energy.gov/ceser/cybersecurity-capability-maturity-/model-c2m2>

REFERENCES

Department of Energy: Cybersecurity Capability Maturity Model (2014). Version 1.1, Department of Homeland Security. <https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>.

Grebennikov, A., Shcheblanin, Yu. (2018). Analysis of the use of process maturity models during the assessment of the level of information security. *Modern information protection*, 1(33), 33–37 [in Ukrainian].

Roy, Y. V., Ryabchun, O. P., & Yermoshin, V. V. (2020). Maturity model of cyber security system capabilities at critical infrastructure facilities of the energy sector ES-C2M2. *Cyber security: education, science, technology*, 2(10), 67–72 [in Ukrainian].

Отримано редакцією журналу / Received: 17.03.24
 Прорецензовано / Revised: 27.03.24
 Схвалено до друку / Accepted: 13.05.24



Oleksandr TOROSHANKO, PhD (Engin.), Assist.
ORCID ID: 0000-0002-2354-0187
e-mail: toroshanko@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Yurii SHCHEBLANIN, PhD (Engin.), Senior Researcher
ORCID ID: 0000-0002-3231-6750
e-mail: y.shcheblanin@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Oleh KURCHENKO, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-3507-2392
e-mail: kurol@ukr.net
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

COMPARISON OF ORGANIZATION (COMPANY) INFORMATION SECURITY PROCESS MATURITY MODELS

Background. *The increase in malicious activity in the information and cyberspace poses a challenge to the leaders of enterprises (organizations) and the leaders of companies with additional tasks and benefits to protect their assets. The loss of assets, for example, financial or technological, can make it impossible for the company to achieve its basic function - to generate profits.*

Methods. *The work used the information security risk analysis method.*

Results. *Creation and promotion of current information security systems. Organizations spend significant financial resources on the development and operation of technology protection, create various structural subdivisions, such as the assessment and provision of a similar level and information security of the enterprise (company). At the same time, there is a real risk of the current situation if malicious and more current technologies are able to rig the system to protect the company and cause irrevocable costs, both financial and reputational.*

Conclusions. *One of the main directions of this problem is the creation of an information security management system (ISMS), which is a warehouse management system for an organization (company) and is assessed without bears the risks of creating, implementing, operating, operational monitoring, review, support and thorough information security organizations (enterprises). The ISMS includes the organizational structure of the organization (company), its policies, nutritional planning, monitoring of labor costs, promotion of daily practices, control and support of resource processes. As a best practice, to assess the level of information security of an organization, it is recommended to use a different approach that is based on the capabilities of process maturity models. The extracted results can be used to thoroughly and optimize the created information security system of the organization (company). There are currently a wide range of information security maturity assessment models available to organizations based on similar principles. In this case, it is realistic to select such models to be limited, first and foremost through a weak connection to the characteristics of specific organizations.*

The work examines models of the maturity of processes, their structure and the ability to evolve in the course of assessing the level of information security.

Keywords: *model, maturity assessment, threat, information security.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.



УДК 004.38

DOI: <https://doi.org/10.17721/IJSTS.2024.7.31-38>

Андрій ФЕСЕНКО, канд. техн. наук, доц.

ORCID ID: 0000-0001-5154-5324

e-mail: andrii.fesenko@knu.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

Марія МИРОШНІЧЕНКО, студ.

ORCID ID: 0009-0008-3535-661X

e-mail: mrshnchnkmaria@gmail.com

Київський національний університет імені Тараса Шевченка, Київ, Україна

ПОРІВНЯННЯ ПОСТКВАНТОВИХ СТАНДАРТІВ У РОЗРІЗІ ВПРОВАДЖЕННЯ У КЛАСИЧНІ АЛГОРИТМИ ЕЛЕКТРОННОГО ПІДПISУ

Вступ. Дослідження розробки й упровадження постквантових стандартів, а також аналіз і порівняння вже існуючих алгоритмів, на основі яких може засновуватись функціонування стандартів у сфері електронного цифрового підпису. Одним з основних питань стало вивчення міграції класичної криптографії до постквантової. Наведено порівняння трьох популярних постквантових стандартів: CRYSTALS-Dilithium, Falcon та SPHINCS+. В результаті дослідження обрано найоптимальніший із стандартів до впровадження у класичні схеми електронного підпису.

Зазначене дослідження є актуальним у зв'язку зі зростанням інтересу до квантових технологій і потребою у забезпеченні безпеки електронних комунікацій у майбутньому квантовому світі.

Методи. Використано методи міграції класичної криптографії до постквантової. Це важливе питання, оскільки потужність квантових комп'ютерів може вразити деякі існуючі криптографічні алгоритми. Проведено аналіз можливостей переходу до нових стандартів та їхньої відповідності вимогам безпеки. Наведено порівняння трьох популярних постквантових стандартів: CRYSTALS-Dilithium, Falcon та SPHINCS+. Це дозволяє визначити найоптимальніший та найнадійніший стандарт для впровадження у класичні схеми електронного підпису. Автори обґрунтовують вибір оптимального стандарту, враховуючи його властивості та відповідність вимогам безпеки.

Результати. Стаття містить важливі результати дослідження у галузі постквантових стандартів для електронного цифрового підпису, що можуть бути корисними для розробників криптографічного програмного забезпечення й інженерів з інформаційної безпеки.

Додатково розглянуто питання щодо викликів і перешкод у впровадженні постквантових стандартів, таких як складність реалізації, вартість інфраструктури та задачі стандартизації. Висвітлено перспективи майбутнього розвитку постквантової криптографії та вплив її впровадження на сучасні системи електронного підпису. Це допоможе читачам отримати повніше розуміння та контекст щодо важливості й потенційних викликів у цій області.

Висновки. Falcon і CRYSTALS-Dilithium відомі високою швидкістю підписування і помірно великим розміром ключа, що робить їх практичними для багатьох застосувань. SPHINCS+, незважаючи на свою відмовостійкість, має меншу швидкість і вимагає більшого розміру ключа. Вибір між CRYSTALS-Dilithium, Falcon і SPHINCS+ залежатиме від конкретних потреб застосування, а також від компромісів між швидкістю, розміром ключа та відмовостійкістю. Зазвичай ці системи пропонують високу швидкість підписування, і це одна з їхніх ключових переваг. Вони призначені для використання у швидких операціях, наприклад, на серверах чи вбудованих системах.

Ключові слова: електронний підпис, постквантова криптографія, криптогнучкість, постквантові стандарти.

Вступ

Криптографія є вирішальним інструментом для безпеки нашого цифрового суспільства і використовується практично всюди. Наприклад, вона захищає наші онлайн-комунікації, зберігає

дані на пристроях у секреті, навіть, якщо ми їх втратимо, і захищає цілісність та автентичність цифрових записів.

Нині безпека цифрових інфраструктур значною мірою базується на криптографії з відкритим

© Фесенко Андрій, Мирошніченко Марія, 2024



ключем (також відомий як "асиметрична криптографія"). Актуальність теми полягає у тому, що з кожним новим етапом розвитку квантових технологій зростає загроза сучасній криптографії, на якій заснована безпека функціонування більшості державних установ. Для попередження злому сучасної системи шифрування інформації впровадження постквантових стандартів уже зараз є нагальною потребою, поки квантовий комп'ютер все ще перебуває на стадії розробки.

Щоб попередити загрозу сучасній асиметричній криптографії з боку квантових комп'ютерів, неминучим стало виникнення галузі криптографічних досліджень – постквантової криптографії. Названа галузь передбачає розроблення та дослідження асиметричних криптосистем, які не можуть бути зламані навіть за допомогою потужних квантових комп'ютерів. Методи переважно базуються на розв'язанні математичних задач, для яких сьогодні невідомі як класичні алгоритми, так і квантові.

Електронний підпис – це електронні дані у зашифрованій формі, які додаються підписантом до інших електронних даних, наприклад електронних документів, звітності, або ж логічно з ними пов'язуються та використовуються ним як заміник справжнього особистого підпису. Отже, ключів при застосуванні ЕП існує два – особистий і відкритий. Відкритий ключ використовують для зчитування особистого ключа, до якого підписант подав звітність. Особистий може бути записаний, наприклад, на флешку чи інший носій.

У схемі електронного підпису (рис. 1) повідомлення надається зі значенням, яке дозволяє перевірити автентичність, цілісність і неzapечене авторство повідомлення. Схеми цифрового підпису є асиметричними криптосистемами. Закритий ключ використовують для генерування підпису, відкритий ключ можна застосувати для перевірки підпису.



Рис. 1. Схема електронного підпису

Мета. Необхідність досліджень узваної теми полягає у систематизації знань і результатів, отриманих у процесі опрацювання інформації, оскільки дослідження і розвиток постквантових методів допомагають розв'язувати багато ключових проблем, пов'язаних із постквантовими технологіями. Аналіз методів створення постквантових стандартів сприяє розробленню потужніших квантових комп'ютерів та ефективніших квантових алгоритмів. Це відкриває нові можливості для розв'язання складних обчислювальних

задач. Аналіз методів створення постквантових стандартів допомагає розробити нові квантові криптографічні протоколи, які можуть стати основою майбутньої безпеки мереж та інформаційних систем. Розвиток постквантових стандартів є ключовим для квантової комунікації, яка може забезпечити надійне передавання даних захищеними від перехоплення зловмисниками.

Методи

У роботі використано методи міграції класичної криптографії до постквантової. Це важливе



питання, оскільки потужність квантових комп'ютерів може вразити деякі існуючі криптографічні алгоритми. Також проведено аналіз можливостей переходу до нових стандартів та їхньої відповідності вимогам безпеки.

Крім того, наведено порівняння трьох популярних постквантових стандартів: CRYSTALS-Dilithium, Falcon та SPHINCS+. Це дозволяє визначити найоптимальніший і найнадійніший стандарт для впровадження у класичні схеми електронного підпису. Автори обґрунтовують вибір оптимального стандарту, враховуючи його властивості та відповідність вимогам безпеки.

Результати

Класичну схему електронного підпису використовують для забезпечення автентичності та цілісності електронної інформації, яку надає або підписує особа, чи сутність у цифровому форматі. Основні кроки цієї схеми такі.

1. Генерування ключів. Спочатку сторона, яка буде підписувати повідомлення, створює пару ключів – приватний ключ і відкритий ключ. Приватний ключ залишається суто конфіденційним і не повинен розголошуватися.

2. Підписання даних. Для підпису повідомлення суб'єкт використовує свій приватний ключ і криптографічний алгоритм, щоб створити цифровий підпис. Цей підпис додається до повідомлення.

3. Передавання повідомлення і підпису. Спільно з підписаним повідомленням суб'єкт також може надіслати свій відкритий ключ іншій стороні або опублікувати його в загальнодоступному реєстрі, якщо це необхідно для перевірки підпису.

4. Перевірка підпису. Отримуючи підписане повідомлення і відкритий ключ, інша сторона може використовувати криптографічний алгоритм, щоб перевірити цифровий підпис. Якщо підпис правильний, то це свідчить про те, що повідомлення не було змінено після підписування і було підписане особою з відповідним приватним ключем.

5. Довіра до ключа. Один із важливих аспектів класичної схеми електронного підпису – це підтвердження довіреності відкритого ключа, що використовується для перевірки підпису. Це може включати використання довірених центрів сертифікації ключів (ЦСК) або мережу блокчейну для підтвердження відповідності відкритого ключа конкретній особі або сутності.

Класичні алгоритми електронного підпису базуються на обчислювальній складності певних математичних завдань, таких як факторизація

великих чисел, обчислення дискретного логарифма тощо. Нині ці алгоритми вважають безпечними завдяки складності вказаних обчислень на класичних комп'ютерах.

Проте квантові обчислення можуть потенційно стати загрозою для безпеки цих класичних алгоритмів електронного підпису. Квантові комп'ютери мають здатність розв'язувати деякі математичні завдання, які є важкими для класичних комп'ютерів, набагато швидше. Зокрема, алгоритм Шора може дуже ефективно факторизувати великі числа і зламувати RSA-шифрування. Це означає, що, коли в майбутньому буде побудований потужний квантовий комп'ютер, то класичні алгоритми електронного підпису, які засновані на розглянутих математичних задачах, можуть бути вразливими (Горбенко та ін., 2017).

CRYSTALS-Dilithium

Загальна оцінка. Dilithium є схемою підпису з високою ефективністю, порівняно простою реалізацією, сильним теоретичним обґрунтуванням – довгою історією вивчення. Вказана схема є гарним вибором для великої кількості криптографічних застосувань. Тому NIST обрав цю схему для стандартизації.

Безпека. Безпека Dilithium ґрунтується на Module-LWE, чого вже достатньо для того, щоб показати, що відкритий ключ не розкриває інформації про секретний ключ.

Механізм Crystals-Dilithium є ЕП, що має надійну безпеку від атак на вибране повідомлення, його стійкість базується на складності проблем ґратки над модульними ґратками. Поняття безпеки означає, що порушник, який має доступ до "оракула" підпису, не може виробити підпис повідомлення, підпис якого він ще не бачив, а також не може створити інший підпис повідомлення, яке він уже бачив підписаним.

Механізм ЕП Crystals-Dilithium є консервативний за параметрами і дозволяє зменшити розмір відкритого ключа та відносно легко дозволяє змінювати рівень криптостійкості, змінюючи розміри параметрів і ключів.

Функціональну реалізацію алгоритму зображено на рис. 2. Оскільки багато програм вимагають передавання як відкритого ключа, так і підпису (напр., ланцюжки сертифікатів), розроблена схема мінімізує суму цих параметрів. Відповідно до обмеження, щодо уникнення дискретної вибірки Гаусса, відомо, що Dilithium має найменшу комбінацію розмірів підпису та відкритого ключа з усіх схем постквантового підпису (Горбенко, & Ганзя, 2014).

**Gen**

```

01  $\mathbf{A} \leftarrow R_q^{k \times \ell}$ 
02  $(\mathbf{s}_1, \mathbf{s}_2) \leftarrow S_{\eta}^{\ell} \times S_{\eta}^k$ 
03  $\mathbf{t} := \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$ 
04 return  $(pk = (\mathbf{A}, \mathbf{t}), sk = (\mathbf{A}, \mathbf{t}, \mathbf{s}_1, \mathbf{s}_2))$ 

```

Sign(sk, M)

```

05  $\mathbf{z} := \perp$ 
06 while  $\mathbf{z} = \perp$  do
07    $\mathbf{y} \leftarrow S_{\gamma_1}^{\ell}$ 
08    $\mathbf{w}_1 := \text{HighBits}(\mathbf{A}\mathbf{y}, 2\gamma_2)$ 
09    $c \in B_{60} := \text{H}(M \parallel \mathbf{w}_1)$ 
10    $\mathbf{z} := \mathbf{y} + c\mathbf{s}_1$ 
11   if  $\|\mathbf{z}\|_{\infty} \geq \gamma_1 - \beta$  or  $\|\text{LowBits}(\mathbf{A}\mathbf{y} - c\mathbf{s}_2, 2\gamma_2)\|_{\infty} \geq \gamma_2 - \beta$ , then  $\mathbf{z} := \perp$ 
12 return  $\sigma = (\mathbf{z}, c)$ 

```

Verify($pk, M, \sigma = (\mathbf{z}, c)$)

```

13  $\mathbf{w}'_1 := \text{HighBits}(\mathbf{A}\mathbf{z} - c\mathbf{t}, 2\gamma_2)$ 
14 if return  $\|\mathbf{z}\|_{\infty} < \gamma_1 - \beta$  and  $[c = \text{H}(M \parallel \mathbf{w}'_1)]$ 

```

Рис. 2. Шаблон для схеми підпису Crystals-Dilithium

Falcon

Falcon (Fast Fourier Lattice-based Compact Signatures over NTRU) – схема на ґратках, що використовує підхід Hash-And-Sign. Теоретична безпека Falcon підтверджується доказом у моделі QROM на основі складності SIS над NTRU ґратками. Консервативні оцінки складності підпису Falcon мають ті самі значення, що і для Dilithium. В ньому ідеалізовано швидкі компактні підписи на основі ґратки Фур'є. Конструкція ЕП Falcon є простою, в ньому реалізуються теоретичні межі для хешування й ЕП на основі ґратки. В механізмі використовують клас криптографічних ґраток (клас ґраток NTRU) та зразок "лазівки", реалізуючи швидку вибірку Фур'є.

Falcon має найменші розміри відкритого ключа та підпису серед кандидатів третього

раунду. Falcon дуже швидко перевіряє підпис. Вироблення підпису відбувається дещо повільніше за Dilithium, а генерування ключів – значно повільніше. З урахуванням цієї інформації, можна сказати, що Falcon може бути гарним вибором у деяких спеціалізованих протоколах, проте у загальному випадку поступається Dilithium згідно з Post-Quantum Cryptography. Round 2 Submissions. (<https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions>).

Блок-схему генерування ключів алгоритму Falcon зображено на рис. 3.

Алгоритм генерування ключів зображено на рис. 4. Ця процедура є основним алгоритмом формування підпису.

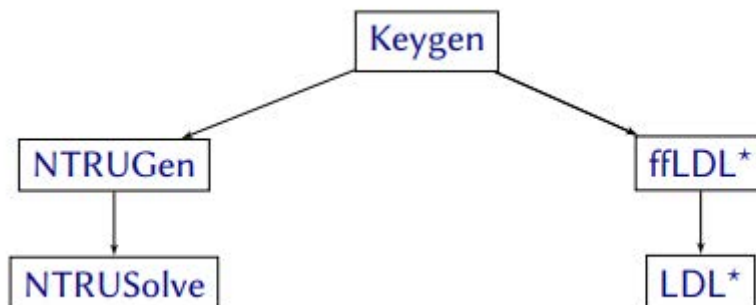


Рис. 3. Блок-схема генерування ключів



Require: A monic polynomial $\phi \in \mathbb{Z}[x]$, a modulus q
 Ensure: A secret key sk , a public key pk

- 1: $f, g, F, G \leftarrow \text{NTRUGen}(\phi, q)$ ▷ Solving the NTRU equation
- 2: $\mathbf{B} \leftarrow \left[\begin{array}{c|c} g & -f \\ \hline G & -F \end{array} \right]$
- 3: $\hat{\mathbf{B}} \leftarrow \text{FFT}(\mathbf{B})$ ▷ Compute the FFT for each of the 4 components $\{g, -f, G, -F\}$
- 4: $\mathbf{G} \leftarrow \hat{\mathbf{B}} \times \hat{\mathbf{B}}^*$
- 5: $\mathbf{T} \leftarrow \text{ffLDL}^*(\mathbf{G})$ ▷ Computing the LDL^* tree
- 6: for each leaf $leaf$ of \mathbf{T} do ▷ Normalization step
- 7: $leaf.value \leftarrow \sigma / \sqrt{leaf.value}$
- 8: $sk \leftarrow (\hat{\mathbf{B}}, \mathbf{T})$
- 9: $h \leftarrow gf^{-1} \pmod q$
- 10: $pk \leftarrow h$
- 11: return sk, pk

Рис. 4. Алгоритм генерування ключів

Falcon був обраний для стандартизації тому, що NIST має впевненість у його безпеці (якщо реалізація виконана правильно з урахуванням атак) та тому, що він має малий розмір відкритого ключа та підпису, що важливо у багатьох застосуваннях.

SPHINCS+

SPHINCS+ – це схема підпису без збереження стану на основі хешу.

Конструкція. Схема поєднує використання одноразових підписів, кількох підписів, дерев Меркла та гіпердерев для створення схеми цифрового підпису, яка підходить для загального застосування.

Зауважимо, що криптографічна безпека SPHINCS+ ґрунтується лише на безпеці використовуваних базових хеш-функцій. Це припущення щодо безпеки не залежить від того, на яких

базуються інші схеми підписів фіналістів (напр., Dilithium і Falcon), тому SPHINCS+ забезпечує успішний **запасний варіант у разі непередбачених криптоаналітичних атак.**

Продуктивність. Через спосіб формування підписів SPHINCS+ генерування та перевірка ключів відбувається набагато швидше. Навіть для безпеки Категорії 1 найменші (і найповільніші) вибори параметрів дають підпис, розмір якого становить близько 8 кБ і є набагато більшим, ніж у альтернативних схемах підпису, таких як Falcon або Dilithium (Горбенко та ін., 2018):

- w : розмір слів, які використовуються;
- l_1 : фіксована кількість слів, розмір яких становить w , повідомлень, які потрібно підписати;
- l_2 : фіксована кількість слів, розмір яких становить w , значення перевірки парності, що використовується в алгоритмі підпису (рис. 5).

- Keygen()
 1. Let $sk = (s_i)_{i=1, \dots, \ell}$ where the s_i are uniformly random w -bits words;
 2. For $1 \leq i \leq \ell$, $p_i \leftarrow H^{w-1}(s_i)$;
 3. *public key*: $pk \leftarrow (p_1, \dots, p_\ell)$, *private key*: sk .
- Sign(m, sk)
 1. Express m in base w : $m = (m_1 m_2 \dots m_{\ell_1})_w$;
 2. Compute the parity-check value $C \leftarrow \sum_{i=1}^{\ell_1} (w - 1 - m_i)$;
 3. Express C in base w : $C = (C_1 C_2 \dots C_{\ell_2})_w$;
 4. $\mathbf{b} = (b_1, b_2, \dots, b_\ell) \leftarrow (m_1, \dots, m_{\ell_1}, C_1, \dots, C_{\ell_2})$ – we will later call it the *b-vector* of m ;
 5. For $1 \leq i \leq \ell$, $\sigma_i \leftarrow H^{b_i}(s_i)$;
 6. *signature*: $\sigma \leftarrow (\sigma_1, \dots, \sigma_\ell)$.
- Verify(m, σ, pk)
 1. Compute the *b-vector* of m as in the signature algorithm (steps 1-4);
 2. Accept if and only if $\forall i \in [1, \ell], p_i = H^{w-1-b_i}(\sigma_i)$.

Рис. 5. Шаблон для схеми підпису SPHINCS+



Параметри пропонують хороший компроміс між розміром і швидкістю, і зазвичай є такими ті, що обрані в останніх конструкціях.

SPHINCS+ – це складна схема, що включає багато різних параметрів для кожної категорії безпеки. Кожен набір параметрів визначає певний компроміс між складністю різних етапів процесу підписання та перевірки й розміром остаточного підпису. Розробники SPHINCS+ розглянули широкий діапазон набору параметрів і запропонували два набори для кожної категорії безпеки. Один набір робить підписи швидшими за рахунок більших підписів, а інший набір робить підписи меншими за рахунок повільніших підписів. Хоча ці набори параметрів добре підходять для більшості загального використання SPHINCS+, можна зробити інші екстремальніші компроміси (напр., зробити підписи дуже повільними, щоб зробити підпис на пару тисяч байтів коротшим), які можуть бути чутливими в деяких випадках.

Складність SPHINCS+ є потенційною проблемою для безпеки впровадження, а також для оцінювання безпеки всієї схеми (оскільки помил-

ку у специфікації або конструкції легше пропустити у складнішому алгоритмі). Криптографічна безпека SPHINCS+ покладається лише на безпеку використовуваних базових хеш-функцій. SPHINCS+ забезпечує успішний запасний варіант у разі непередбачених криптоаналітичних атак. Складність захисту SPHINCS+ від атак бічними каналами переважно визначається складністю захисту реалізації хешу з ключем від атак бічними каналами.

Через спосіб формування підписів SPHINCS+ генерування та перевірка ключів відбувається набагато швидше, ніж підписання. Відкриті ключі SPHINCS+ дуже короткі, але підписи SPHINCS+ досить довгі. Основною ідеєю SPHINCS+ є створення безпечного підпису, який неможливо підробити, навіть якщо той, хто атакує, отримає секретний ключ підписувача. Спосіб побудови підпису SPHINCS+ робить його дуже стійким до атак, таких як атака Гроша, і надійним для довготермінового використання (Ducas, Lepoint, & Lyubachevsky, 2024).

Наочне порівняння характеристик алгоритмів ЕП наведено в таблиці.

Таблиця

Характеристики алгоритмів ЕП

	CRYSTALS-Dilithium	Falcon	SPHINCS+
Механізм ЕП	Конструкція механізму ЕП Dilithium базується на підході "Fiat-Shamir з перериваннями"	Механізм Falcon є розвитком ЕП NTRU та позначається як NTRU – Falcon	SPHINCS+ використовує велику кількість хеш-функцій і дерево Горнера
Швидкодія	+++*	+++	++
Розмір ключа	++**	+	+++
Відмовостійкість	Стійкість механізму ЕП Dilithium ґрунтується на складності пошуку коротких векторів у алгебричних ґратках	Falcon розроблено з огляду на відмовостійкість і стійкість до різних типів атак, включно з квантовими атаками	SPHINCS+ має високий рівень відмовостійкості та стійкості до атак, включно з атаками Гроша та квантовими атаками

Примітки. +++* – висока швидкодія; ++ – помірна швидкодія; * – низька швидкодія; ** ++ – великі розміри ключа; ++ – помірні розміри ключа; + – невеликі розміри ключа.

Дискусія і висновки

Методи Falcon і CRYSTALS-Dilithium відомі високою швидкістю підписування і помірнішим розміром ключа, що робить їх практичними для багатьох застосувань. SPHINCS+, незважаючи на свою відмовостійкість, має меншу швидкість і вимагає більшого розміру ключа. Вибір між CRYSTALS-Dilithium, Falcon і SPHINCS+ залежатиме від конкретних потреб застосування, а також від компромісів між швидкістю, розміром

ключа та відмовостійкістю. Зазвичай ці системи пропонують високу швидкість підписування, і це одна з їхніх ключових переваг. Вони призначені для використання у швидких операціях, наприклад, на серверах чи вбудованих системах. Falcon вирізняється високою швидкістю підписування та помірним розміром ключа. Цей метод підходить для застосувань, де важливо забезпечити високу продуктивність підписування. Falcon має достатню відмовостійкість і рівень



захисту від квантових атак, а також характеризується високою швидкістю підписування, схожою на Dilithium, він призначений для швидких операцій і вимагає менше часу для створення підпису.

SPHINCS+ відомий своєю високою відмовостійкістю та захистом від квантових атак. Цей метод підходить для застосувань, де відмовостійкість є першочерговою вимогою, навіть за високих витрат обчислювальних ресурсів. Зазвичай SPHINCS+ має меншу швидкість підписування та великий розмір ключа, що може бути обмеженням для деяких застосувань.

CRYSTALS-Dilithium характеризується високою швидкістю підписування та меншим розміром ключа. Цей метод підходить для застосувань, де важливі і висока швидкість підписування, і відмовостійкість. CRYSTALS-Dilithium є ефективним рішенням для багатьох застосувань, оскільки поєднує високу продуктивність і відмовостійкість. SPHINCS+ зазвичай має помірну швидкість підписування. Він вимагає значної кількості операцій для створення підпису, що робить його менш швидким порівняно з іншими методами. Зазвичай швидкість SPHINCS+ оцінюється в сотнях операцій за секунду.

Розмір ключа в CRYSTALS-Dilithium зазвичай менший порівняно з SPHINCS+, що дозволяє зберігати ключі й обробляти дані ефективніше. Розмір ключа у Falcon невеликий, що полегшує управління ключами та їхнє зберігання. SPHINCS+ вимагає великого розміру ключа, що може бути неефективним для деяких застосувань, особливо на обмежених ресурсах.

Внесок авторів: Андрій Фесенко – концептуалізація; методологія; аналіз джерел, підготування огляду літератури або теоретичних засад дослідження;

Марія Мирошніченко – збір емпіричних даних та їх валідація; емпіричне дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Горбенко Ю., & Ганзя, Р. (2014). Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів. *CSN*, 806. <http://science.lpnu.ua/uk/csn/vsi-vypusky/nomer-806-2014/analiz-shlyahiv-rozvytku-kryptografiiy-pislya-poyavy-kvantovyh>.

Горбенко, І., Качко, О., Єсіна, М., & Пономар, В. (2018). Методи, методика та результати порівняльного аналізу кандидатів на постквантовий стандарт електронного підпису. *XX Ювілейна міжнародна науково-практична конференція "Безпека інформації в інформаційно-телекомунікаційних системах"* (с. 96–97). м. Буча (Київська область), ГНЦ "Зелена Буча".

Горбенко, І., Кузнецов, О., Потій, О., Горбенко, Ю., Ганзя, Р., & Пономар, В. (2017). Модель зрілості можливостей системи кібербезпеки на об'єктах критичної інфраструктури енергетичного сектору ES-C2M2. *Кібербезпека: освіта, наука, техніка*, 2(10), 32–52.

Ducas, L., Lepoint, T., & Lyubachevsky, V. (2024). *Crystals – Dilithium: Digital Signatures from Module Lattices*. TCHES 2024. <https://cryptojedi.org/papers/dilithium-20170617.pdf>

REFERENCES

Ducas, L., Lepoint, T. & Lyubachevsky, V. (2024). *Crystals – Dilithium: Digital Signatures from Module Lattices*. TCHES 2024. <https://cryptojedi.org/papers/dilithium-20170617.pdf>.

Gorbenko, I., Kuznetsov, O., Potii, O., Horbenko, Yu., Ganzya, R., & Ponomar, V. (2017). Maturity model of cyber security system capabilities at critical infrastructure facilities of the energy sector ES-C2M2. *Cyber security: education, science, technology*, 2(10), 32–52 [in Ukrainian].

Horbenko, I., Kachko, O., Yesina, M., Ponomar, V. (2018). Methods, techniques and results of comparative analysis of candidates for the post-quantum electronic signature standard. *XX Jubilee International Scientific and Practical Conference "Information Security in Information and Telecommunication Systems"* (pp. 96–97). Bucha (Kyiv region), SSC "Zelena Bucha" [in Ukrainian].

Horbenko, Yu., & Ganzya, R. (2014). Analysis of the development of cryptography after the advent of quantum computers. *CSN*, 806. [in Ukrainian]. <http://science.lpnu.ua/uk/csn/vsi-vypusky/nomer-806-2014/analiz-shlyahiv-rozvytku-kryptografiiy-pislya-poyavy-kvantovyh>.

Отримано редакцією журналу / Received: 12.04.24

Прорецензовано / Revised: 17.04.24

Схвалено до друку / Accepted: 13.05.24



Andrii FESENKO, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0001-5154-5324
e-mail: andrii.fesenko@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Maria MYROSHNICHENKO, Student
ORCID ID: 0009-0008-3535-661X
e-mail: mrshnchnkmaria@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

COMPARISON OF POST-QUANTUM STANDARDS AS IMPLEMENTED IN CLASSICAL ELECTRONIC SIGNATURE ALGORITHMS

Background. *The work examines the development and promotion of post-quantum standards, as well as the analysis and improvement of existing algorithms, on the basis of which the functioning of standards in the field of electronic digital signature can be based. One of the main reasons was also the migration of classical cryptography to post-quantum cryptography. The robot is aligning three popular post-quantum standards: CRYSTALS-Dilithium, Falcon and SPHINCS+. As a result of the investigation, the most optimal standards were selected before implementation of classical electronic signature schemes.*

The article is dedicated to the development and promotion of post-quantum standards in the field of electronic digital signature. It is also necessary to analyze and level up existing algorithms, on the basis of which the functioning of such standards can be based. The research is considered relevant due to the growing interest in quantum technologies and the need for secure electronic communications in the upcoming quantum world.

Methods. *Migrating classical cryptography to post-quantum cryptography. However, power is important, because the power of quantum computers can be affected by certain cryptographic algorithms. An analysis of the feasibility of transitioning to new standards and their existing security capabilities is also carried out.*

In addition, three popular post-quantum standards are being updated: CRYSTALS-Dilithium, Falcon and SPHINCS+. This allows us to determine the most optimal and reliable standard for implementation of classical electronic signature schemes. The authors of the work carry out the selection of the optimal standard, ensuring the safety and security of its authorities.

Results. *Contains important results from the study of post-quantum standards for electronic digital signatures, which may be useful for developers of cryptographic software and information security engineers.*

The power supply to the influences and changes in the advanced post-quantum standards, such as the complexity of implementation, the flexibility of infrastructure and power standardization, are thoroughly examined. The prospects for the future development of post-quantum cryptography and its influx into modern electronic signature systems have also been highlighted. This will help readers to take away the more common sense and context of the importance and potential contributions in this area.

Conclusions. *Falcon and CRYSTALS-Dilithium have a high signing fluidity and a larger key size, making them practical for rich stagnation. SPHINCS+, regardless of its viscosity, has less fluidity and requires a larger key size. The choice between CRYSTALS-Dilithium, Falcon and SPHINCS+ will depend on the specific drying needs, as well as compromises between fluidity, key size and viscosity. This demonstrates the high speed of subscription, and this is one of its key advantages. It is intended for use in quick operations, for example, on servers and industrial systems.*

Keywords: *electronic signature, post-quantum cryptography, cryptoflexibility, post-quantum standards.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.



UDC 004.056

DOI: <https://doi.org/10.17721/ISTS.2024.7.39-44>

Volodymyr KHOROSHKO, DSc (Engin.), Prof.

ORCID ID: 0000-0001-6213-7086

e-mail: professor_va@ukr.net

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Mykola BRAILOVSKYI, PhD (Engin.), Assoc. Prof.

ORCID ID: 0000-0002-3148-1148

e-mail: bk1972@ukr.net

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Ivan PARKHOMENKO, PhD (Engin.), Assoc. Prof.

ORCID ID: 0000-0001-6889-9284

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Taras KYRYCHUK, Student

ORCID ID: 0000-0003-0013-2989

e-mail: taraskiricuk@gmail.com

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

MODEL OF IMPLEMENTATION OF MANAGEMENT OF ACCESS TO INFORMATION ASSETS IN THE CONCEPT OF ZERO TRUST

Background. Controlling access to information assets is one of the key functions of information security. This task in one form or another must be solved both as a whole at the level of the entire information technology (IT) infrastructure of a company or organization, and in each local information system.

Methods. Methods on existing approaches, the article develops a model for providing access to information assets, which allows implementing access control processes in a distributed IT infrastructure. A special feature of the model is an algorithm for dynamically determining the necessary security policies, taking into account the access of users with different privileges.

Results. The model takes into account remote access at several conventional "levels" – access of the organization's clients, organization employees, as well as partners and contractors. Since modern information infrastructures of organizations have become complex and distributed, the model assumes the presence of a significant number of access points, including automated workstations in the infrastructure, remote automated workstations, various user and mobile access devices, as well as specific devices, such as effective access control should ensure centralized access of all users to information assets.

Conclusions. The model provides for the implementation of a single access point, built on the basis of access models from the zero trust concept, for users and for "robots" – technical accounts used for inter-system interaction. The results of the study will make it possible to develop an architecture for remote user access to distributed information assets and organize access control and management processes based on dynamic determination of the level of trust in access subjects, which generally increases the security of organizations.

Ключові слова: zero Trust, multifactor authentication, single Sign-On, security Policies, fast IDentity Online.

Background

The Zero Trust security model addresses the needs of applications, users, and devices for fast and secure data access in distributed architectures. Using this concept, it is possible to create fail-safe and continuous protection of users and information assets in cases where it is not possible to be reliable in the security of the network. This concept requires that each individual user, device, or session access each specific request to an information asset without initially verifying and verifying security. The concept of zero trust is a set of ideas designed to increase

reliability in the decision to grant access for each request on an untrusted network. Its main goal is the prevention of unauthorized access and the most detailed access management, with this concept, an approach is proposed, rather than specific algorithms and models of access control implementation (Chapman, & Chapman, 2021).

In fact, the concept of zero trust is a set of concepts designed to minimize the level of uncertainty when making decisions about providing access to an information resource in discovered insecure networks that meet the requirements of least privilege. It should



be emphasized that the planning of bringing the infrastructure into compliance with the principles of zero trust cannot be carried out partially or within the framework of updating information systems. Restructuring of the information infrastructure as a whole, as well as integration into all aspects of the organization's activities, is required in order for the principles of zero trust to show their effectiveness (Lambert et al., 2023).

At the same time, the greatest efficiency is achieved by investing sufficient funds and increasing

investments in the processes of supporting zero-trust infrastructure (Lambert et al., 2023).

The basis of the concept is laid in the special publication NIST 800-207 207 (NIST CSWP, 2023. <https://www.ibm.com/topics/zerotrust>), which can be used as a guide for the development and implementation of ZTA (ZeroTrustAccess) in organizations. This publication also provides an abstract logical model of the zero-trust architecture (Fig. 1), which was the basis of the developed access control implementation model.

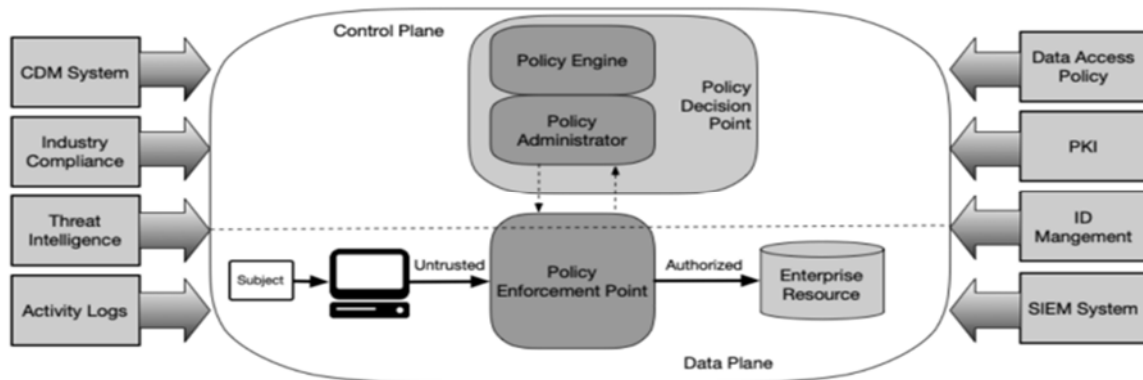


Fig. 1. Basic Logical Components of the Zero Trust Model NIST

The main elements of this model are TechRadar, 2023 (<https://www.techradar.com/opinion/whyzero-trust-cybersecurity-relies-on-people-as-much-as-tech>):

- Policy Engine (PE) – the core of ZTA implementation, components on which access possibilities within requests are evaluated, usually based on data from various sources (monitoring systems and logs, threat detection systems at endpoints, etc.);

- Policy Administrator (PA) – a component that implements the policies set on the PE and ensures the establishment, maintenance and termination of access sessions through the control plane (a set of channels between all model elements);

- Policy Enforcement Point (PEP) – a component with which subjects interact by sending requests for access to information assets, collecting information about access subjects and checking them for compliance with policies received from the PA;

- information flows (Policy Information Points, PIPs) – flows that are not the main functional components of the zero trust model, but are used to support the functioning of the PE by providing data for making decisions about access requests.

The basis of providing access to an information resource are the principles outlined in the same concept, which can be briefly formulated as follows:

- 1) authentication and authorization of all access subjects is dynamic and mandatory;

- 2) all data sources and services are pre-considered resources;

- 3) the state of security and integrity of all information resources is constantly monitored;

- 4) all interactions are protected regardless of network membership;

- 5) access to specific information resources is provided within the session corresponding to such access;

- 6) the decision to grant access is made on the basis of dynamic policies that take into account the data received from the PIP;

- 7) collection of the maximum possible amount of data on the state of security of information assets, network infrastructure and access subjects is ensured.

The listed principles are basic and must be followed when implementing the concept of zero trust in the organization. However, the study does not consider the abstract situation of providing access to a certain subject, but to specific groups of users with their own specificity, that is, subjects with different powers in information assets – user and administrative, as well as specific subjects – external services.

For objects that require greater authority or administrative access, this implies the use of specialized methods and tools to ensure access security for such objects. Thus, in addition to the



basic principles of the concept of zero trust, the following two principles were also defined:

- 1) stricter policies are required to grant broader privileges in an access session;
- 2) the formation of PP policies should be carried out taking into account the maximum possible degree of security and integrity of access subjects.

The first additional principle is based on the specifics of granting access to entities performing management functions, as these functions require the provision of excess powers that go beyond the minimum necessary. The access of such subjects is usually carried out during the implementation of additional measures to check the devices from which the access is made, to control such access and to monitor.

The second additional principle is based on the likely limitations that may be present when requesting access to technical services, as the various

technologies used to implement access may not objectively meet the requirements of the main PE policies. They should be formed taking into account each specific technical service and ensure access to the minimum necessary information resources.

Methods

Methods on existing approaches, the article develops a model for providing access to information assets, which allows implementing access control processes in a distributed IT infrastructure. A special feature of the model is an algorithm for dynamically determining the necessary security policies, taking into account the access of users with different privileges.

Results

Figure 2 presents the model of the enclave gateway, on the basis of which the model of providing access to information assets in potentially unprotected networks will be organized.

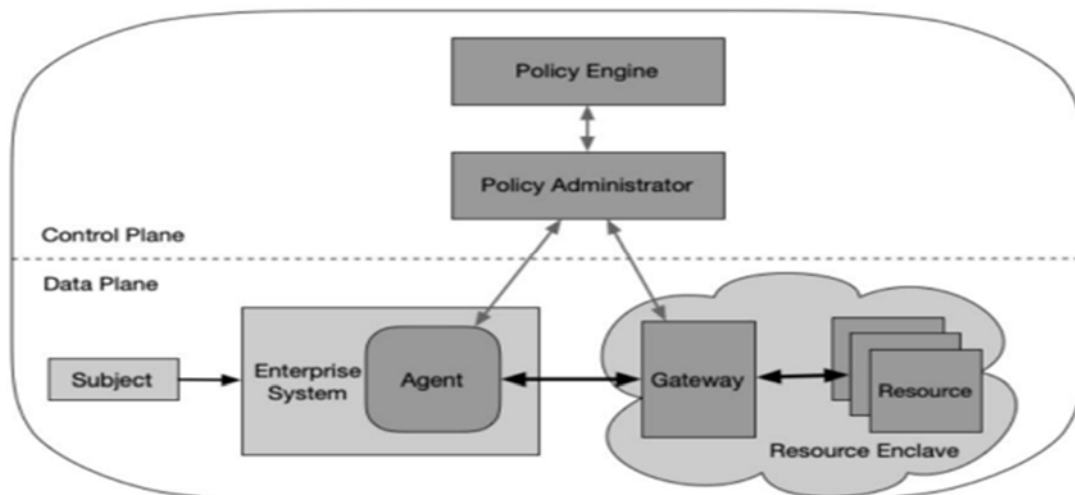


Fig. 2. Model of the enclave gateway

It involves the use of the following logical components:

- an agent located on a resource from which
- access request;
- gateway, which is the entry point of access to information resources.

Information resources located behind the gateway are not unified (like, for example, a web service), but represent an "enclave" – a set of information assets located on the same computing resources.

In this model, the access subject has an agent that is used to connect to the "enclave" gateway and can be an agent of a specific information protection system, which will allow, for example, to provide control of privileged access. With the help of an agent, you can ensure the implementation of targeted access policies to a specific resource, and with the help of a gateway, you can

control access directly to a list of information resources, which makes it possible to implement policies for users with different privileges Wagenseil, 2010 (<https://www.scmagazine.com/resource/identity-/andaccess/how-identity-and-access-management-fits-into-zero-trust>).

A disadvantage of this model is that the gateway secures the resources of the enclave as a whole and may fail to secure individual ones, thus giving access subjects the potential to discover resources within the enclave to which they do not have legitimate access. The model developed as part of the study (Fig. 3) is a complex version of the "enclave gateway model", which is characterized by more complex mechanisms for providing access through the gateway to all the above-mentioned groups of access subjects.

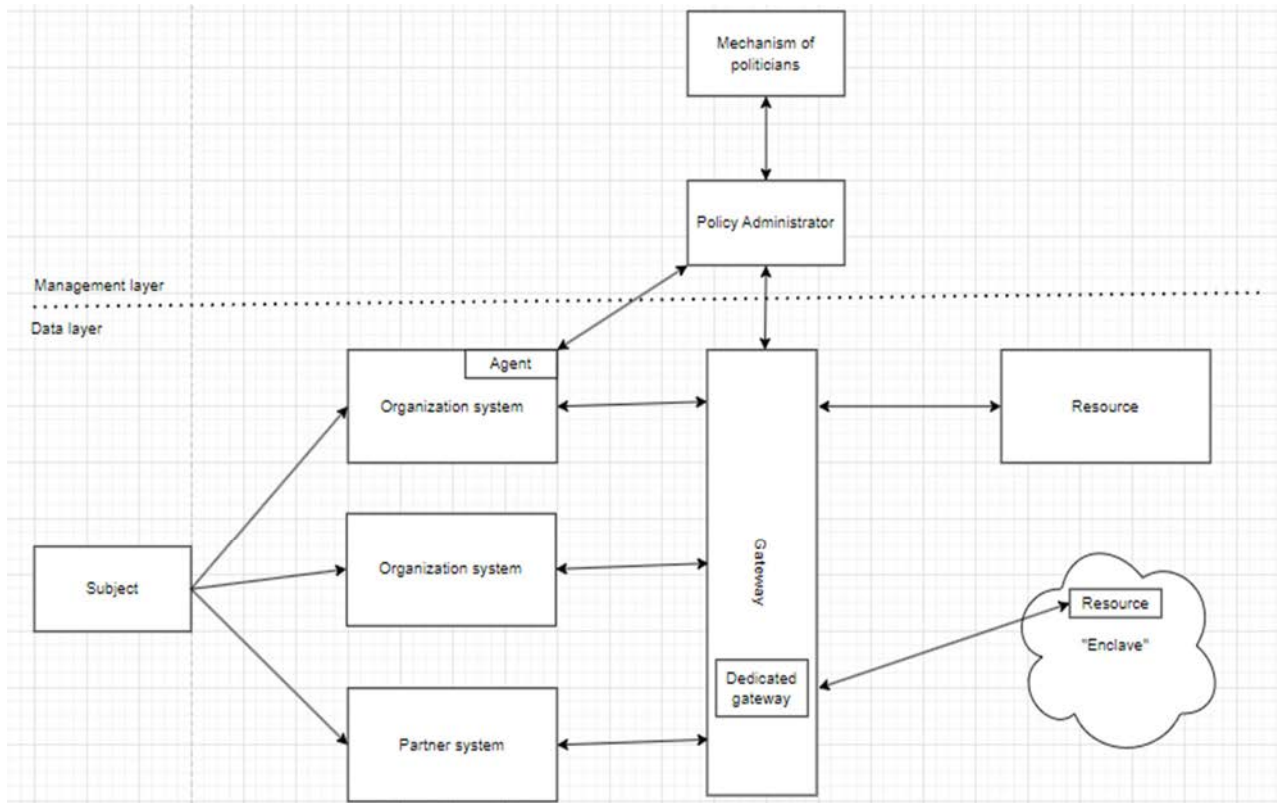


Fig. 3. The developed model of access control implementation

The access subject can make access requests from the corporate system with or without an installed agent, as well as from conditionally external partner systems. Each access request is processed at the gateway, which is the point of policy enforcement, while requests from partner systems are processed at a dedicated part of the gateway for which the policy engine applies different policies.

Figure 4 shows the access request routing scheme through the gateway. The access request comes

through the load balancer because the gateway is a composite object in the model. For each request, based on the security status data coming from the PIP, the source of the request and the subsequent processing path are determined – which gateway component will receive it for processing. Next, based on the access policies, identification and authentication is performed, and if successful, an authorization request is generated.

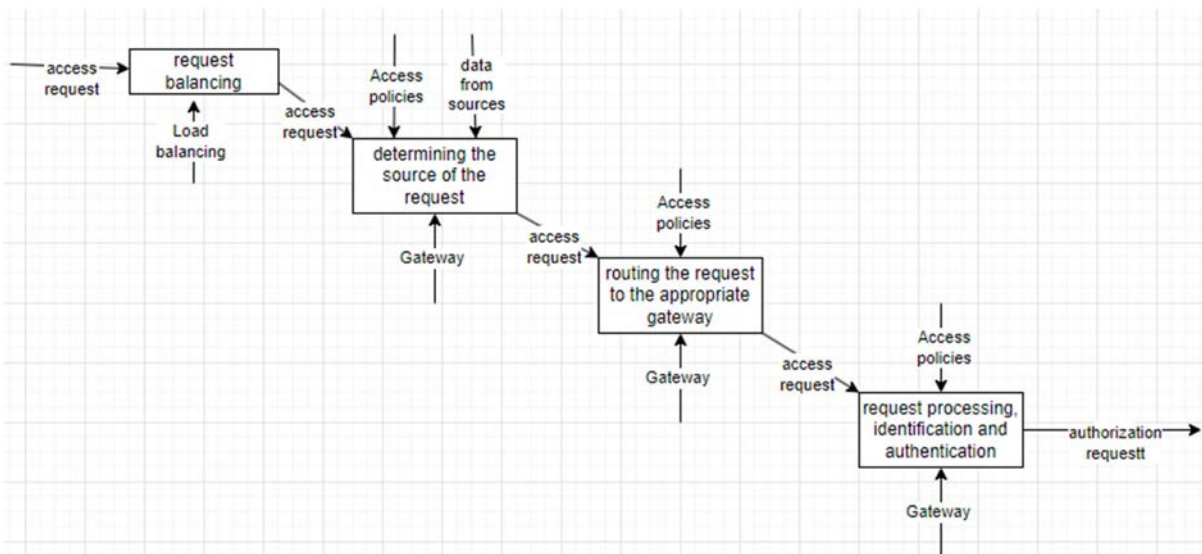


Fig. 4. PEP access request routing diagram



Identification is the first step in providing access and at the same time the basis of the concept of zero trust (Cai, & Zhang, 2019, pp. 46–49). Authentication can be implemented in various ways, and adding a second authentication factor can further reduce the

risk of attacks on the access control system (Zeng, 2020, p. 48). After successful authentication, an authorization request is conditionally formed, which is subject to further processing, the scheme of which is presented in Fig. 5.

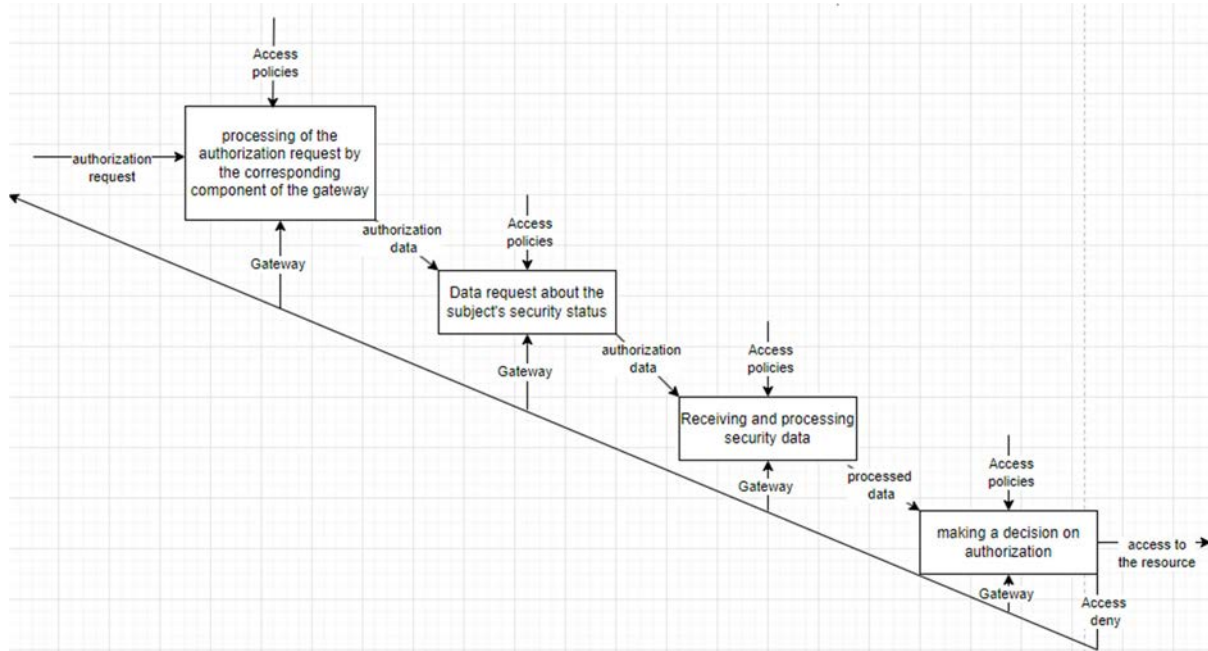


Fig. 5. Processing of access request through PEP

A feature of the proposed processing scheme is repeated access to PIPs information streams, which provide available data on the current security status of the access subject at the time of authorization. Thus, it is implied that the decision to grant access is made with two stages of verification of the subject - during the processing of the request for identification and authentication, and also after successful authentication, which will increase the confidence that this access request is legitimate and will not create risks for information security.

Dual subject checking as part of access request processing provides flexibility in decision-making on the PEP side and allows for different policies that may be more or less strict depending on the type of access subject. Weak or insufficient control policies, according to a Verizon study (Zuo., 2018, pp. 50–51), lead to the majority of incidents involving compromised accounts, and according to a report by XM Cyber (Liu, 2018, pp. 80–87), 73% of the most common attack methods involve poor access control mechanisms or compromised accounts. By using complex dynamic policies, access control can be implemented, minimizing the risk of security breaches.

Zero trust generally reduces the possible attack surface and reduces the level of damage and consequences of cyber attacks by reducing the time

and cost of managing security threats. A high degree of transparency during the provision of access simplifies administration processes and reduces the risks of unauthorized access, since it can be obtained only by those subjects who, based on a series of checks, have confirmed their level of security (Columbus, 2022). In addition, the unification of access policies between applications and servers, which are critical parts of the IT infrastructure, is the key to unifying IAM into a single secure and manageable place for on-premises and cloud IT departments.

Discussion and conclusions

The proposed model of access provision has not lost the shortcomings of the prototype model, but on demand, it provides the possibility of access to individual information resources through the gateway, as well as to resources in the enclave, which ensures the implementation of more complex and universal policies on the PP, which will be built into the administrative policy. Thanks to this, it is possible to build secure real architectures that will create different access paths to target information resources. This creates difficulties for administration and policy development, but this fact cannot be considered an insufficient model, after the concept of zero trust, it implies constant revision of policies and changes in



the information infrastructure. This is a complex process in itself that requires a zero-trust architecture and the ability to adapt to changes. As part of further research, a detailed study of the process of granting access and the development of an access policy based on dynamic data on the security status of access subjects is possible.

Authors' contribution: Volodymyr Khoroshko – conceptualization; methodology; analysis of sources; Mykola Brailovsky – preparation of the literature review; Ivan Parkhomenko – preparation of the theoretical foundations of the research; Taras Kyrychuk – collection of empirical data and their validation; empirical research.

REFERENCES

Cai, R., & Zhang, X. (2019). Zero Trust Based Identity Security Solution. *Information Technology & Standardization*, 9, 46–49.

Володимир ХОРОШКО, д-р техн. наук, проф.

ORCID ID: 0000-0001-6213-7086

e-mail: professor_va@ukr.net

Київський національний університет імені Тараса Шевченка, Київ, Україна

Микола БРАЙЛОВСЬКИЙ, канд. техн. наук., доц.

ORCID ID: 0000-0002-3148-1148

e-mail: bk1972@ukr.net

Київський національний університет імені Тараса Шевченка, Київ, Україна

Іван ПАРХОМЕНКО, канд. техн. наук, доц.

ORCID ID: 0000-0001-6889-9284

Київський національний університет імені Тараса Шевченка, Київ, Україна

Тарас КИРИЧУК, студ.

ORCID ID: 0000-0003-0013-2989

e-mail: taraskiricuk@gmail.com

Київський національний університет імені Тараса Шевченка, Київ, Україна

МОДЕЛЬ РЕАЛІЗАЦІЇ УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНИХ АКТИВІВ У КОНЦЕПЦІЇ НУЛЬОВОЇ ДОВІРИ

Вступ. Контроль доступу до інформаційних активів є однією з ключових функцій забезпечення інформаційної безпеки. Це завдання в тій чи іншій формі має розв'язуватися як загалом на рівні всієї інформаційно-технологічної інфраструктури компанії чи організації, так і в кожній локальній інформаційній системі.

У статті на основі існуючих підходів розроблено модель забезпечення доступу до інформаційних активів, що дає змогу реалізувати процеси контролю доступу в розподіленій IT-інфраструктурі.

Методи. На основі існуючих підходів у статті розроблено модель забезпечення доступу до інформаційних активів, яка дозволяє реалізувати процеси контролю доступу в розподіленій IT-інфраструктурі. Особливістю моделі є алгоритм динамічного визначення необхідних політик безпеки з урахуванням доступу користувачів із різними привілеями.

Результати. Результатом є алгоритм динамічного визначення необхідних політик безпеки, який враховує доступ користувачів із різними привілеями. Модель враховує віддалений доступ на кількох умовних "рівнях" – доступ клієнтів організації, співробітників організації, а також партнерів і підрядників. Оскільки сучасні інформаційні інфраструктури організації стали складними й розподіленими, модель передбачає наявність значної кількості точок доступу, серед яких автоматизовані робочі станції в інфраструктурі, віддалені автоматизовані робочі станції, різноманітні користувацькі та мобільні пристрої доступу, а також специфічні пристрої на зразок торгових терміналів, ефективний контроль доступу має забезпечувати можливість централізованого доступу всіх користувачів до інформаційних активів.

Висновки. Модель передбачає реалізацію єдиної точки доступу, побудованої на основі моделей доступу з концепції нульової довіри, для користувачів і для "роботів" – технічних облікових записів, які використовують для міжсистемної взаємодії. Результати дослідження дадуть змогу розробити архітектуру віддаленого доступу користувачів до розподілених інформаційних активів та організувати процеси контролю й управління доступом, які базуються на динамічному визначенні рівня довіри до суб'єктів доступу, що загалом покращує безпеку організації.

Ключові слова: нульова довіра, багатofакторна автентифікація, єдиний вхід, політики безпеки, Fast IDentity Online.

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.



КОМП'ЮТЕРНІ НАУКИ

УДК 004.58/934

DOI: <https://doi.org/10.17721/IJSTS.2024.7.45-51>

Лариса МИРУТЕНКО, канд. техн. наук, доц.

ORCID ID: 0000-0001-8538-8996

e-mail: myrutenko.lara@gmail.com

Київський національний університет імені Тараса Шевченка, Київ, Україна

Яніна ШЕСТАК, канд. техн. наук, асист.

ORCID ID: 0000-0002-7291-1829

e-mail: luchenko@ukr.net

Київський національний університет імені Тараса Шевченка, Київ, Україна

Анастасія ЛОБАН, студ.

ORCID ID: 0009-0000-3828-6663,

e-mail: anastasiyaloban0912@gmail.com

Київський національний університет імені Тараса Шевченка, Київ, Україна

ДОСЛІДЖЕННЯ ІНДЕКСІВ ТЕОРЕТИЧНОЇ ВІДПОВІДНОСТІ ДЛЯ УКРАЇНСЬКОГО АЛФАВІТУ З ПРОБІЛОМ

Вступ. Важливу роль у виявленні слабкостей криптографічних систем і забезпеченні їхньої стійкості відіграють індекси теоретичної відповідності. Проаналізувавши доступні джерела інформації, не було виявлено вказаного показника для українського алфавіту з пробілом, що унеможливило знаходження точних результатів у розрахунках, де використовують цей показник.

Методи. Індекси теоретичної відповідності мають широке застосування, але найчастіше їх використовують у першому методі Фрідмана під час обчислення розміру ключа для шифру Віженера, який використовують у вивченні базових понять криптографічних систем. Розглянуто загальний алгоритм знаходження індексів теоретичної відповідності для українського алфавіту з пробілом на основі аналізу великої вибірки текстів.

Для розрахунків проаналізовано 700 текстів, кількість елементів яких становить 1500. Тексти обрано за допомогою API із загальнодоступної вільної багатомовної онлайн-енциклопедії Wikipedia. Розрахунок виконували для ключів розміру від 2 до 7. Індекс теоретичної відповідності обчислено у два етапи. На першому етапі знайдено практичні індекси відповідності для всіх текстів, а далі за допомогою стандартного відхилення вибірки обчислено проміжок найповторюваніших показників. Програмний код для реалізації алгоритму обчислення індексу було представлено у вигляді компонентів проекту, які відповідають за різні аспекти процесу.

Результати. В результаті дослідження виявлено варіацію значень індексу відповідності залежно від розміру тексту, що підкреслює необхідність враховувати довжину тексту під час аналізу та розроблення криптографічних систем, зокрема й у виборі ключів шифрування. Зроблено висновок, що розмір тексту може впливати на результати розрахунків індексів відповідності, але несуттєво впливає на загальну захищеність та ефективність шифрування.

Висновки. У процесі виконання роботи проведено аналіз українського алфавіту з пробілом та його властивостей. Розроблено та реалізовано алгоритм обчислення індексу теоретичної відповідності для цього алфавіту. Експериментально визначено індекс теоретичної відповідності для різних текстів українською мовою за допомогою розробленого алгоритму.

Ключові слова: індекси теоретичної відповідності, індекс збігу, перший метод Фрідмана, другий метод Фрідмана, комп'ютерна лінгвістика.

Вступ

В сучасному світі, де кількість та обсяг інформації стрімко зростають, виникає нагальна потреба в інструментах, спроможних забезпечити безпеку

ISSN 2707-1758

та конфіденційність обміну даними. Одним із важливих напрямів у цьому контексті є криптографія – наука, яка вивчає методи захисту інформації від несанкціонованого доступу. Серед

© Мирутенко Лариса, Шестак Яніна, Лобан Анастасія, 2024



криптографічних інструментів важливе місце належить індексам теоретичної відповідності (ІТВ), які є криптографічними метриками, що дозволяють оцінити ступінь відповідності між текстами. ІТВ використовують для аналізу й оцінювання якості шифрування, розпізнавання мови, визначення авторства тексту та багатьох інших завдань. У цьому контексті одним із найвідоміших індексів теоретичної відповідності є індекс Шеннона, який базується на концепції ентропії.

Вказані індекси відіграють важливу роль у виявленні слабкостей криптографічних систем і забезпеченні їхньої стійкості. Проте застосування індексів теоретичної відповідності може викликати труднощі, такі як складність обчислення та неоднозначність інтерпретації результатів. Для розв'язання цих питань, розроблення ефективних алгоритмів стає ключовою задачею, що сприятиме автоматизації та вдосконаленню процесу використання індексів теоретичної відповідності в криптографії. ІТВ дозволяють оцінити рівень випадковості та непередбачуваності згенерованих ключів. Вони можуть бути використані для виявлення атак на криптографічні системи, таких як атаки з використанням статистичного аналізу.

Індекси теоретичної відповідності допомагають забезпечити конфіденційність, цілісність і доступність передавання даних. Вони можуть бути використані для оцінювання якості різних криптографічних примітивів, наприклад, хеш-функції. ІТВ дозволяють здійснювати аналіз криптографічних систем із різними алфавітами й символічними системами (Boneh, & Shoup, 2017). Вони можуть застосовуватися для оцінювання якості генерування псевдовипадкових чисел у криптографії. Наприклад, шифр Віженера використовує індекси теоретичної відповідності для аналізу тексту та визначення ключа шифрування. Шифр Цезаря також може піддаватися аналізу за допомогою цих індексів, де вони застосовуються для визначення зсуву алфавіту й відновлення оригінального тексту. Криптосистема Ель-Гамала також використовує індекси теоретичної відповідності для оцінювання стійкості до криптоаналізу.

Індекси теоретичної відповідності є корисним інструментом для аналізу й оцінювання безпеки криптографічних протоколів, таких як SSL/TLS. Вони допомагають виявити потенційні вразливості у протоколах, які використовують асиметричні шифри й обмін ключами.

Застосування індексів теоретичної відповідності дозволяє розробникам криптографічних систем покращувати їхню стійкість і надійність, аналізуючи оптимізацію параметрів та алгоритмів шифрування.

Проте виникають певні труднощі, наприклад, складність обчислення індексів для великих текстів або об'ємних даних. Також може виникнути неоднозначність в інтерпретації результатів через різні методології обчислення та відсутність єдиного стандарту для їхнього розрахунку. Проблема також полягає у визначенні оптимального порогового значення індексу, яке вказує на ступінь відповідності. Загалом, використання індексів теоретичної відповідності у криптографічних системах вимагає ретельного вивчення та розробок для забезпечення їхньої стійкості до криптоаналізу. Реалізація алгоритму сприятиме розвитку комп'ютерного аналізу мови та статистичного моделювання в текстових даних. Впровадження алгоритму дозволить зробити процес обчислення індексів теоретичної відповідності ефективнішим і швидшим, як показано у роботі A Graduate Course in Applied Cryptography (<https://toc.cryptobook.us/>).

Мета. Алгоритм знаходження індексів можна використати для покращення якості машинного перекладу й автоматичного оброблення текстів.

Наявність алгоритму спростить порівняння різних мов або діалектів на основі їхньої відповідності теоретичним моделям. Розроблення алгоритму викликає необхідність удосконалення методів оброблення тексту та статистичного аналізу даних (Rivest, Shamir, & Adleman, 1978, pp. 120–126).

Алгоритм знаходження індексів теоретичної відповідності є актуальним завданням у сучасних наукових і прикладних дисциплінах, що вивчають текстову інформацію.

Методи

Індекси теоретичної відповідності мають широке застосування, але найчастіше їх використовують у першому методі Фрідмана у процесі обчислення розміру ключа для шифру Віженера, який використовують у вивченні базових понять криптографічних систем. Розглянуто загальний алгоритм знаходження індексів теоретичної відповідності для українського алфавіту з пробілом (УАЗП) на основі аналізу великої вибірки текстів.

Для розрахунків проаналізовано 700 текстів, кількість елементів яких становить 1500. Тексти обрано за допомогою API із загальнодоступної вільної багатомовної онлайн-енциклопедії Wikipedia. Розрахунок виконували для ключів розміру від 2 до 7. Індекс теоретичної відповідності розраховано у два етапи. На першому етапі знайдено практичні індекси відповідності для всіх текстів, а далі за допомогою стандартного відхилення вибірки обчислено проміжок найпов-



торюваніших показників. Програмний код для реалізації алгоритму обчислення індексу представлено у вигляді компонентів проєкту, які відповідають за різні аспекти процесу.

Результати

Загальний алгоритм знаходження індексів відповідності для українського алфавіту з пробілом передбачає такі кроки:

1. Зібрати достатньо велику вибірку текстів українською мовою, які містять пробіли. Це можуть бути літературні тексти, новини, наукові статті тощо. Важливо, щоб вибірка була репрезентативною і включала різноманітні тематики.

2. Знайти кількість літер УАЗП. Український алфавіт складається з 33 літер, але з пробілом ця кількість становитиме 34.

3. Розбити кожен текст на окремі елементи, включно з пробілами. Кожен елемент може бути окремим символом або комбінацією символів, наприклад, літера з пробілом.

4. Порахувати частоту входження кожного елемента у вибірці текстів. Це можна зробити, складаючи таблицю, де стовпці відповідають символам, а рядки – кожному тексту у вибірці. Кожна комірка таблиці міститиме кількість входжень певного символу відповідно до тексту.

5. Обчислити частоту входження кожного символу у всій вибірці, підсумовуючи відповідні значення з усіх текстів.

6. Розрахувати загальну частоту входження символів із пробілом, яка дорівнюватиме частоті входження пробілу плюс сумі частот входження інших символів із пробілом.

7. Обчислити індекс відповідності для кожного символу, застосовуючи формулу

$$\text{Індекс} = \frac{\text{частота входження символу}}{\text{загальна частота входження символів з пробілом}}. \quad (1)$$

8. Порівняти отримані індекси відповідності для всіх символів і визначити ті, які мають найбільшу відповідність.

9. Виокремити проміжок найбільш повторюваних індексів відповідності. Цей проміжок вказуватиме на теоретичний індекс відповідності для УАЗП.

10. За необхідності, виконати додаткову статистичне оброблення, наприклад, розрахувати середнє значення і стандартне відхилення для отриманих індексів відповідності.

11. Перевірити алгоритм на інших вибірках текстів для підтвердження його ефективності і стабільності результатів.

Цей загальний алгоритм дозволяє знаходити індекси відповідності для українського алфавіту з пробілом на основі аналізу великої вибірки текстів.

Отриманий теоретичний індекс відповідності можна використати для подальших розрахунків у криптографії та інших сферах, де необхідно враховувати особливості української мови з пробілом.

Програмний код для реалізації алгоритму обчислення індексу теоретичної відповідності (IBPr) представлено у вигляді компонентів проєкту, які відповідають за різні аспекти процесу:

1. Text.py: Цей клас відповідає за отримання випадкового українського тексту з Вікіпедії, його очищення й обчислення IBPr для заданого ключа з використанням шифру Віженера.

2. Settings.py: У цьому класі зберігаються всі конфігураційні параметри проєкту, такі як український алфавіт, мінімальна та максимальна довжина ключа, параметри API Вікіпедії тощо.

3. Cipher.py: Модуль, який надає функції для шифрування та дешифрування текстів за допомогою шифру Віженера. Включає функції для генерування випадкового ключа та виконання операцій шифрування та дешифрування.

4. Ivpr.py: Модуль, який містить функцію для обчислення IBPr для заданого тексту. IBPr обчислюють як метрику для визначення ступеня відповідності тексту.

5. Main.py: Цей скрипт використовує згадані вище компоненти для генерування таблиці IBPr. Програма застосовує бібліотеки та модулі, такі як json, logging, numpy, tqdm, matplotlib, defaultdict та colorama. У функції main() відбувається організація виконання програми, яка отримує текст, генерує випадковий ключ певної довжини, обчислює індекс теоретичної відповідності для кожної довжини ключа й виводить графічне представлення результатів.

За основу для розрахунку взято аналіз 700 текстів, кількість елементів яких становить 1500, отриманих із Wikipedia за допомогою API. Розрахунок відбувається для ключів розміром від 2 до 7 (рис. 1, 2).

Обчислені значення індексу теоретичної відповідності зберігаються у відповідному форматі, а також виводяться графічні представлення результатів за допомогою matplotlib. Логування виконують за допомогою модуля logging, крім того, використовують бібліотеку colorama для кольорового форматування виводу. Результати також зберігають у JSON-файлі.

Ми знаходимо практичні індекси відповідності для всіх текстів. І за допомогою стандартного відхилення вибірки одержуємо проміжок найповторюваніших показників. Це і є наш індекс теоретичної відповідності (рис. 3, 4).



```
# Set the amount of texts to analyze
self.amount_of_texts = 700

# Set the minimum size of the text to analyze
self.min_text_size = 1500

# Set the maximum and minimum lengths of the key to use in the Vigenère cipher
self.max_key_length = 7
self.min_key_length = 2
```

Рис. 1. Задання параметрів для аналізу текстів

```
/Users/admin/Desktop/IBPrTable/venv/bin/python /Users/admin/Desktop/IBPrTable/main.py
INFO:root:START...
0%|          | 0/700 [00:00<?, ?it/s]INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/w/api.ph
INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/w/api.php?action=query&prop=extracts&titles=Ірм
INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/w/api.php?action=query&prop=extracts&titles=Доп
INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/w/api.php?action=query&prop=extracts&titles=Моп
INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/w/api.php?action=query&prop=extracts&titles=Гоп
INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/w/api.php?action=query&prop=extracts&titles=Шу-
0%|          | 1/700 [00:02<30:36, 2.63s/it]INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/
INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/w/api.php?action=query&prop=extracts&titles=Шуф
INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/w/api.php?action=query&prop=extracts&titles=Герп
INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/w/api.php?action=query&prop=extracts&titles=Кон
INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/w/api.php?action=query&prop=extracts&titles=Сни
0%|          | 2/700 [00:04<25:33, 2.20s/it]INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/
INFO:wikipediaapi:Request URL: https://uk.wikipedia.org/w/api.php?action=query&prop=extracts&titles=Бік
```

Рис. 2. Виконання програмного коду

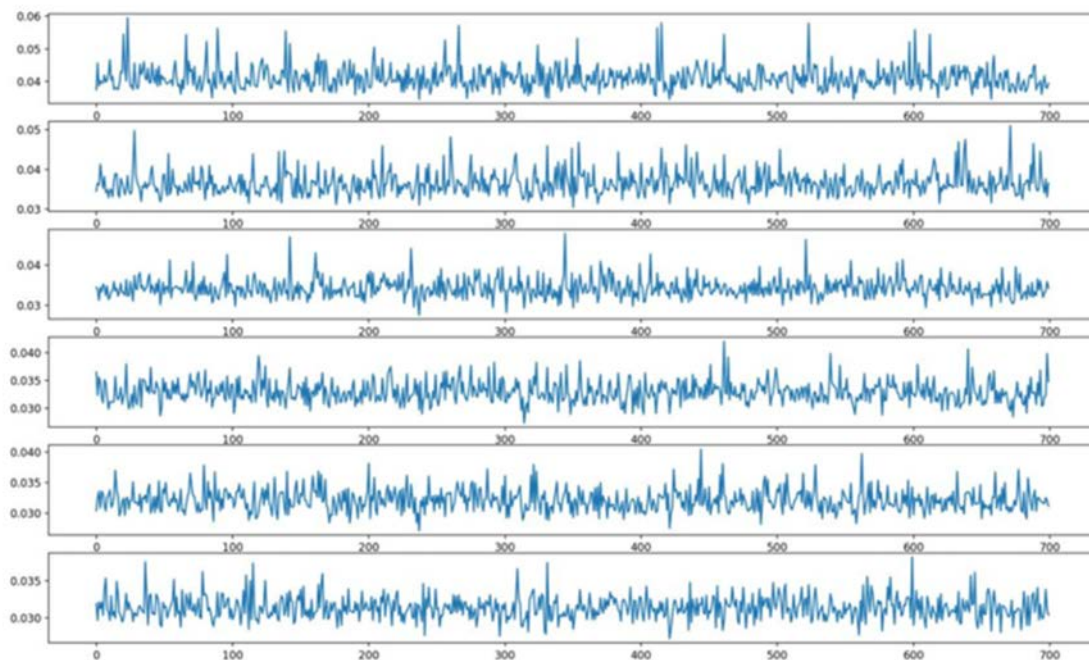


Рис. 3. Графік індексів практичної відповідності для всіх текстів розміром 1500 символів



```

100%|██████████| 700/700 [24:34<00:00, 2.11s/it]
INFO:root:2
INFO:root:3
INFO:root:4
INFO:root:5
INFO:root:6
INFO:root:7
INFO:root:Key: 2, Min Value: 0.03446344164544084, Max Value: 0.05957376779396034
INFO:root:Key: 3, Min Value: 0.030462497420599775, Max Value: 0.051022574258673535
INFO:root:Key: 4, Min Value: 0.027531891978430617, Max Value: 0.047932151705736614
INFO:root:Key: 5, Min Value: 0.02735624531769972, Max Value: 0.04205401456717444
INFO:root:Key: 6, Min Value: 0.02711855156203381, Max Value: 0.04047303747959718
INFO:root:Key: 7, Min Value: 0.027209786919405794, Max Value: 0.03818595577202063
    
```

Рис. 4. Показники індексів теоретичної відповідності

Індекси теоретичної відповідності для українського алфавіту з пробілом відкривають широкі можливості для застосування в різних галузях. Наведемо деякі потенційні можливості і сфери застосування цих індексів:

1. Криптографія. ІТВ можуть бути використані для аналізу шифрованих текстів і встановлення можливості розшифрування. Вони допомагають визначити розподіл символів у шифрованому тексті та порівняти його з відомим розподілом символів у мові відкритого тексту.

2. Мовознавство. Індекси теоретичної відповідності застосовують для вивчення структури та властивостей української мови. Вони дозволяють оцінити ступінь відповідності між розподілом символів у тексті та типовим розподілом символів у мові.

3. Літературознавство. За допомогою ІТВ можна проводити аналіз текстів літературних творів. Вони дозволяють виявляти особливості авторського стилю, використання символіки та лексики.

4. Контентний аналіз. Індекси теоретичної відповідності можуть бути використані для оцінювання схожості або розбіжності між різними документами чи текстовими джерелами. Вони дозволяють проводити порівняльний аналіз, виявляти патерни й розробляти алгоритми автоматичного пошуку.

5. Аналіз соціальних мереж. В аналізі комунікаційних мереж, які складаються з повідомлень, коментарів та інших текстових даних, вони допомагають виявляти схожість між користувачами, групами або темами обговорень.

6. Виявлення плагіату. ІТВ допомагають порівнювати семантичну схожість між текстами та виявляти спільні фрази, що свідчать про можливе копіювання (Gorkavenko, Popova, & Tarasenko, 2019, p. 24).

7. Аналіз електронної пошти. ІТВ можна використати для аналізу текстових повідомлень, електронних листів та інших форм комунікації через електронну пошту.

8. Аналіз настрою та сентимент-аналіз. ІТВ застосовують для визначення настрою або емоційного відтінку тексту. Вони допомагають виявляти позитивний, негативний або нейтральний характер тексту, що має значення для аналізу відгуків користувачів і соціальних медіа.

9. Медичний аналіз. Можуть бути використані для аналізу медичних записів, пацієнтських оглядів та інших медичних документів. Вони допомагають виявляти зв'язки між симптомами, діагнозами й лікуванням.

10. Фінансовий аналіз. ІТВ можуть бути застосовані для аналізу фінансових звітів, економічних новин та інших фінансових документів. Допомагають виявляти тренди, патерни й ризики у фінансових ринках і підприємствах.

Наведені потенційні застосування індексів теоретичної відповідності показують, що вони можуть бути корисними інструментами для аналізу та розуміння текстових даних у різних галузях.

З розрахунків можна зробити такі висновки щодо різниці результатів залежно від розміру тексту. Збільшення розміру тексту з 1500 до 2000 символів призвело до деякого зниження значень індексу відповідності для всіх розглянутих ключів. Це може вказувати на більшу варіативність і розподіленість символів у більших текстах, що зменшує ступінь повторюваності та структурованості.

Хоча величина змін значень індексу відповідності не є значною, вона показує, що довжина тексту може впливати на ступінь подібності між українським алфавітом із пробілом і текстами, що



аналізуються. Більші розміри текстів можуть призводити до меншої впевненості в точності індексів теоретичної відповідності.

Незважаючи на зниження значень індексу відповідності, результати залишаються в межах прийнятних значень для шифрування та забезпечення високого рівня захищеності текстів.

Варіація значень індексу відповідності залежно від розміру тексту підкреслює необхідність враховувати довжину тексту під час аналізу та розроблення криптографічних систем, зокрема й у виборі ключів шифрування.

Отже, розмір тексту може впливати на результати розрахунків індексів відповідності, але несуттєво впливає на загальну захищеність та ефективність шифрування (Rivest, Shamir, & Adleman 1978, pp. 120–126).

Дискусія і висновки

У процесі виконання роботи проведено аналіз українського алфавіту з пробілом і його властивостей. Розроблено й реалізовано алгоритм обчислення індексу теоретичної відповідності для цього алфавіту. Експериментально визначено індекс теоретичної відповідності для різних текстів українською мовою за допомогою розробленого алгоритму.

Отримані результати проаналізовано і зроблено висновки щодо їхньої значущості та застосування у криптографії та лінгвістиці. Ці

результати дозволяють зрозуміти ступінь відповідності мовних текстів українській мові з використанням вказаного алфавіту. Вони можуть бути використані для побудови ефективних криптографічних систем, а також для дослідження мовних особливостей і стилістичних відмінностей української мови.

Внесок авторів: Лариса Мирутенко – концептуалізація; методологія; аналіз джерел; Яніна Шестак – підготування огляду літератури або теоретичних засад дослідження; Анастасія Лобан – збір емпіричних даних та їх валідація; емпіричне дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Gorkavenko, V. M., Popova, T. G., & Tarasenko, O. V. (2019). *Mathematical Linguistics: a textbook*. Publishing House "Prosvita".

Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.

REFERENCES

Gorkavenko, V. M., Popova, T. G., & Tarasenko, O. V. (2019). *Mathematical Linguistics: a textbook*. Publishing House "Prosvita".

Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.

Отримано редакцією журналу / Received: 10.03.24

Прорецензовано / Revised: 29.03.24

Схвалено до друку / Accepted: 13.05.24



Larysa MYRUTENKO, PhD (Engin.), доц.
ORCID ID: 0000-0001-8538-8996
e-mail: myrutenko.lara@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Yanina SHESTAK, PhD (Engin.), Assist.
ORCID ID: 0000-0002-7291-1829
e-mail: luchenko@ukr.net
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Anastasiia LOBAN, Student
ORCID ID: 0009-0000-3828-6663
e-mail: anastasialoban0912@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

RESEARCH OF INDICES OF THEORETICAL CORRESPONDENCE FOR THE UKRAINIAN ALPHABET WITH SPACES

Background. *Theoretical compatibility indices play an important role in identifying the weaknesses of cryptographic systems and ensuring their stability. After analyzing the available sources of information, this indicator was not found for the Ukrainian alphabet with a space, which makes it impossible to find accurate results in calculations where this indicator is used.*

Methods. *Theoretical correspondence indices have a wide range of applications, but they are most often used in Friedman's First Method when calculating the key size for the Vigenere cipher, which is used in the study of the basic concepts of cryptographic systems. The general algorithm for finding indices of theoretical correspondence for the Ukrainian alphabet with a space based on the analysis of a large sample of texts is considered.*

Results. *For calculations, 700 texts were analyzed, the size of which is 1500 elements. The texts were selected using an API from Wikipedia, a free and open multilingual online encyclopedia. The calculation took place for keys of size from 2 to 7. The index of theoretical correspondence was calculated in two stages. At the first stage, practical indices of correspondence were calculated for the whole range of texts, and then, using the standard deviation of the sample, the interval of the most repeated indicators was calculated. The program code for implementing the index calculation algorithm was presented in the form of project components responsible for various aspects of the process.*

As a result of the study, a variation of the values of the correspondence index was found depending on the size of the text, which emphasizes the need to consider the length of the text in the analysis and development of cryptographic systems, in particular, the selection of encryption keys. It was concluded that the size of the text can affect the results of the calculation of the compatibility indices, but it does not significantly affect the overall security and effectiveness of encryption.

Conclusions. *In the course of the work, an analysis of the Ukrainian alphabet with a space and its properties was carried out. An algorithm for calculating the index of theoretical correspondence for this alphabet was also developed and implemented. The index of theoretical correspondence was experimentally determined for various texts in the Ukrainian language using the developed algorithm.*

Keywords: *indices of theoretical correspondence, index of coincidence, First Friedman method, Second Friedman method; computational linguistics.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.



УДК 004.801.056.5

DOI: <https://doi.org/10.17721/ISTS.2024.7.52-61>

Володимир НАКОНЕЧНИЙ, д-р техн. наук, проф.

ORCID ID: 0000-0002-0247-5400

e-mail: volodym.nakonechnyi@knu.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

Володимир САЙКО, д-р техн. наук, проф.

ORCID ID: 0000-0002-3059-6787

e-mail: v.saiko@knu.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

Микола МОРДВИНЦЕВ, канд. техн. наук, доц.

ORCID ID: 0000-0002-7674-3164

e-mail: lukolyu@gmail.com

Харківський національний університет внутрішніх справ, Харків, Україна

Владислав ЛУЦЕНКО, асп.

ORCID ID: 0000-0002-2377-1858

e-mail: vlkiller175@knu.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

ПЕРЕВАГИ ТА НЕБЕЗПЕКИ ВИКОРИСТАННЯ CHATGPT

Вступ. Ця стаття презентує ChatGPT – новий чат-бот, один з останніх продуктів у сфері штучного інтелекту, створений компанією OpenAI, яка розробила цю технологію спільно з Ілоном Маском. У статті надано рекомендації щодо підключення до чат-бота. Визначено основні переваги штучного інтелекту, наведено приклади його застосування. Нинішні освітні процеси мають розвивати у студента крос-дисциплінарний і практико-орієнтований підхід.

Результати. Показано, що серед основних переваг ChatGPT – можливість генерувати тексти на задану тему, відповідати практично на всі запитання користувачів і висловлюватись навіть українською мовою. Наведено конкретні приклади питань до чат-бота, що пов'язані, зокрема й із захистом інформації, управлінням ризиками тощо. Продемонстровано відповіді з його боку. Зосереджено увагу на небезпеці, що виникає у разі використання нового чат-бота. Показано, що серед виявлених небезпек особливе місце займають можливий плагіат, проблеми сумісності, застосування у зловмисних цілях, проблеми конфіденційності, питання щодо порушення авторських прав і проблеми використання ChatGPT у системі освіти. Підкреслено, що нині система освіти переживає значну кризу і щоб процес отримання знань був адекватний викликам сьогодення, треба кардинально переглянути підхід до того, якими мають бути нинішній викладач і сам навчальний процес. Зазначено, що Україні потрібна докорінна трансформація самої суті системи освіти. Нині головне завдання викладача – дати студенту можливість самому проявити ініціативу в навчанні, ефективно використовувати отриману інформацію, комбінувати її й застосовувати отриманий результат у розв'язанні свого завдання. Успішний студент має навчитися розв'язувати комплексні завдання, які перебувають на стику різних предметів і дисциплін.

Висновки. ChatGPT є потужним інструментом, але нині він має деякі недоліки, які варто врахувати, якщо в планах є його використання.

Ключові слова: чат-бот, нейронні мережі, застосунок, шифрування, авторське право, конфіденційність, штучний інтелект.

Вступ

В листопаді 2022 р. у світі з'явився унікальний чат-бот на базі штучного інтелекту (ШІ) ChatGPT – крайній продукт у сфері штучного інтелекту (ШІ), створений компанією OpenAI (AI – це скорочення від "Artificial Intelligence" або "штучний інтелект"), що розробила цю технологію спільно з відомим бізнесменом

Ілоном Маском. GPT – аббревіатура, що означає Generative Pre-Trained Transformer.

ChatGPT може генерувати тексти на задану тему та відповідати, практично, на всі запитання користувачів. Бот демонструє себе обережним співрозмовником, здатним чітко й точно висловлюватись, вже навіть й українською мовою. Він підтримує кілька платформ, що робить його

© Наконечний Володимир, Сайко Володимир, Мордвинцев Микола, Луценко Владислав, 2024



ідеальним вибором для компаній, які прагнуть вийти за межі англомовних ринків.

Формат чата дозволяє ШІ відповідати на додаткові запитання, визнавати свої помилки й відхиляти невідповідні запити. Автори проєкту ChatGPT вчили модель бути обережною, що змушує її відхиляти запитання, на які вона не може відповісти правильно.

Менш ніж за тиждень, новим чат-ботом, скористалися більше мільйона користувачів. Спробували оцінити роботу ChatGPT й автори цієї статті, а для цього, звісно, треба підключитися до нього. Тому скажемо кілька слів про цей процес.

ChatGPT доступний на офіційній сторінці організації-розробника – OpenAI. Нині офіційного застосунку ще немає, тому завантажувати його не слід. Причому варто бути обережними під час установа застосунків із подібною назвою, оскільки вони не є офіційними програмами компанії OpenAI (Краковецький, 2023).

Раніше, до того як OpenAI відкрила доступ до чат-бота українцям, користування ChatGPT в Україні нагадувало достатньо складний квест, у якому були потрібні – віртуальна приватна мережа – virtual private network (VPN), іноземний мобільний номер і багато маніпуляцій із браузером, щоб обійти відповідне блокування.

Зараз все стало набагато простіше. Щоб почати спілкування з чатом, треба виконати такі дії.

1. Перейти за посиланням на платформу ChatGPT.
2. Зареєструватись.
3. Ввести адресу своєї електронної пошти.
4. Пройти верифікацію вже за номером телефону українського оператора.
5. Написати повідомлення чат-боту.

Для користування чат-ботом ChatGPT не потрібно робити жодних оплат. Але OpenAI запустила платну підписку за \$20 дол. так званого ChatGPT Plus, після оформлення якої її, передплатники матимуть пришвидшений час відповіді, навіть у години пікового навантаження, а також пріоритетний доступ до функцій та оновлень. Платна підписка нині доступна виключно у Сполучених Штатах.

Мета. Багато людей, починають використовувати чат-бот як Google-пошук. Але поки що він не настільки обізнаний. Компанія OpenAI попереджає, що чат-бот ще багато вчиться, тому може давати не завжди коректні відповіді чи демонструвати упереджену поведінку. Досить часто чат-бот дає не зовсім правильні відповіді, можна зазначити, просто вигадуює їх.

Проте він добре вміє структурувати текст. Наприклад, його можна попросити написати структуру резюме тощо.

Варто зауважити, що мовна модель AI – це програмне забезпечення, створене з використанням штучного інтелекту, здатне розуміти й генерувати природну мову. Мовну модель AI засновано на великому обсязі текстових даних, які використовують для тренування моделі. Мовна модель AI здатна генерувати відповіді на запитання, надавати пояснення, перекладати, генерувати текст тощо.

Подібні до GPT-3.5 мовні моделі AI засновано на глибокому навчанні та рекурентних нейронних мережах, які можуть аналізувати контекст, розуміти мовні відношення, виявляти в тексті закономірності й генерувати логічні та зв'язні відповіді. Крім того, ці моделі можуть навчатися на великій кількості даних, що дозволяє їм розуміти широкий спектр тематик і мовних конструкцій.

Мовні моделі ШІ мають широке застосування, а саме:

- генерування тексту;
- автоматичний переклад;
- розпізнавання мови;
- відповіді на питання тощо.

Тому вони можуть бути корисним інструментом для розширення можливостей оброблення природної мови й автоматизації різних завдань, що пов'язані з нею. Проте існують і певні недоліки й навіть проблеми, пов'язані з використанням ChatGPT, про які піде мова у цій статті (Чим небезпечний чат-бот ChatGPT..., 2023).

Результати

Ось яке перше запитання задали автори цієї статті після реєстрації на сайті дослідницької компанії штучного інтелекту OpenAI: "Розкажи про себе". Результат, наведений нижче, був отриманий протягом 2–3 секунд (рис. 1).

Продовженням знайомства із ШІ було запитання до нього – склади програму на C++, яка помножить два числа A і B . І ось що було запропоновано ChatGPT (рис. 2).

Після цього захотілося дізнатися, наскільки ChatGPT може бути романтиком. І на запитання – напиши вірш про любов до України – бот видав вірш, рис. 3 (Чат-бот ChatGPT: помічник..., 2023), який, хоч із римами, на нашу думку, поки що не все гаразд, є дуже зворушливим.

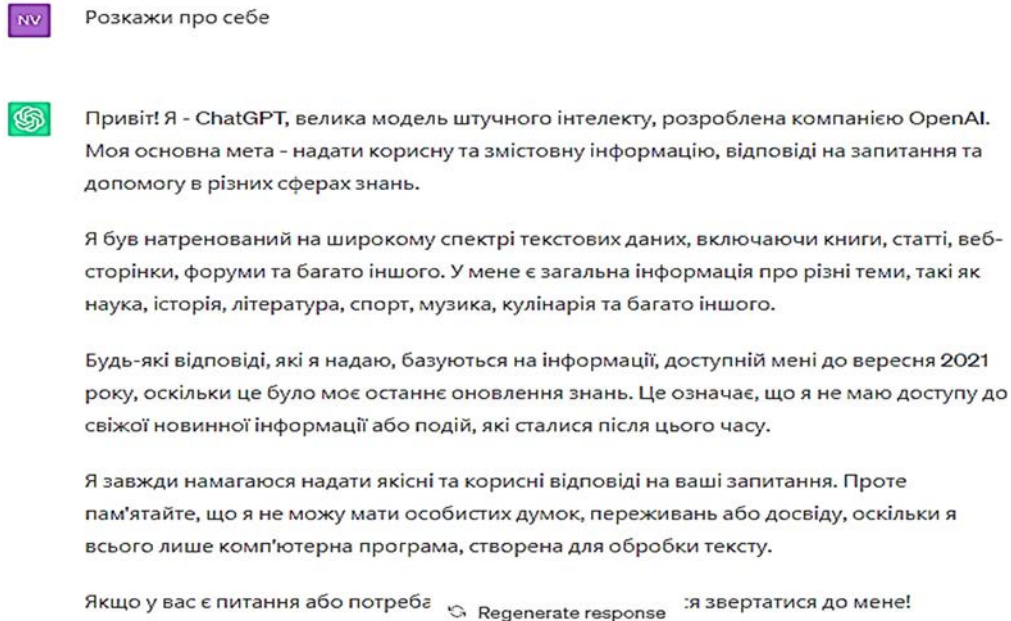


Рис. 1. Фрагмент тексту відповіді ChatGPT на запитання "Розкажи про себе"

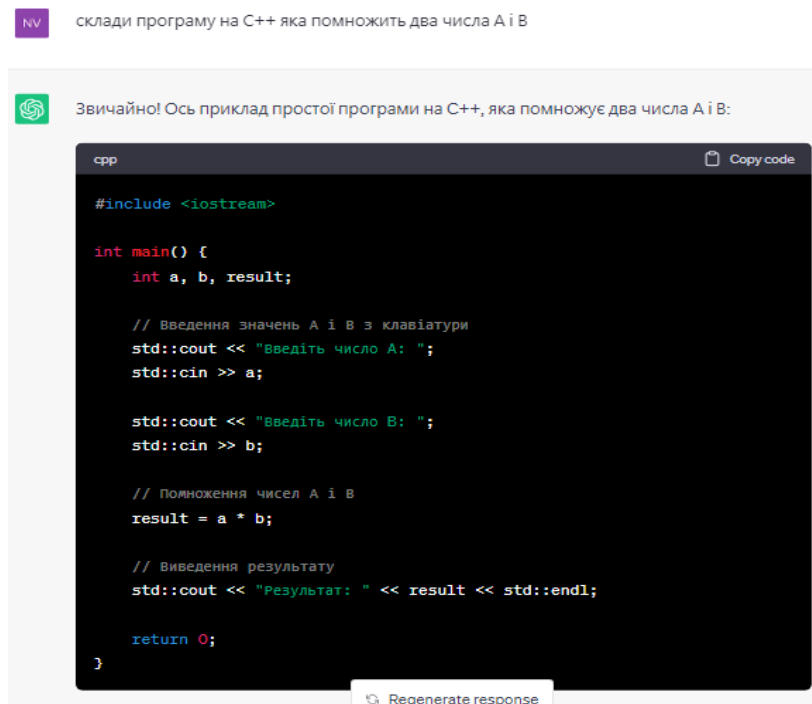


Рис. 2. Фрагмент тексту відповіді ChatGPT на запитання "Склади програму на C++, яка помножить два числа A і B"

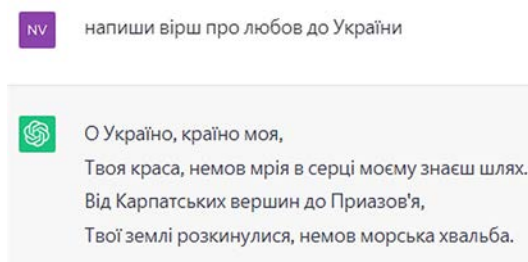


Рис. 3. Фрагмент тексту відповіді ChatGPT на запитання "Напиши вірш про любов до України"



Ми, з дозволу читачів, наведемо повний текст цього "шедевра".

"О Україно, країно моя,
Твоя краса, немов мрія в серці моєму знаєш шлях.
Від Карпатських вершин до Приазов'я,
Твої землі розкинулися, немов морська хвальба.
Твої поля рясніють житом золотим,
Де співають соловей у сумерках нічних.
Твої ріки спішать до морів вільних,
Мов карети кохання від сонця розпечених.
О, ти моя ненько, мов калина в крові,
Ти відроджуєш душу, даруєш волю людям.
Твої діти, мужні й ніжні, до тебе клоняться,
Бо в твоєму серці співає розлогий хоровод їхніх імен.
Ти пройшла крізь вогні і випробування,
Зберегла мову, традиції й культуру віків.
Ти надія, сила і віра для кожного покоління,
Україно моя, в твоїх очах бачу неба височінь.
Захищай свої землі і небо блакитне,
Твоя краса неповторна, ніжна й міцна.
Ми будемо завжди вірні, як твої сини й дочки,
Любити тебе, Україно, до останнього подиху.
О, Україно моя, найкраща країна на світі,
Твої простори широкі, твої гори величні.
Ми завжди будемо з тобою, навіть у далекім світі,
Бо любов до тебе в наших серцях безмежна
й незліченна".

Не знаю як Ви, шановні читачі, а у нас, після першого знайомства з ChatGPT, перехопило подих від того, які технології існують нині і стали доступні сучасному людству.

Проте не все так добре, як здається на перший погляд, і тому, знаючи проблеми із захистом інформації, ми задали відповідне запитання до ШІ, а саме: "Які загрози ти несеш людству?" Через кілька секунд була отримана така відповідь (цитуємо оригінал).

"Я, як мовна модель штучного інтелекту (AI), несую певні потенційні загрози, що можуть бути

пов'язані зі шкідливим використанням або зловживанням. Ось кілька можливих загроз, пов'язаних із використанням мене:

Розповсюдження дезінформації: якщо недобросовісні особи використовують мене для створення та поширення дезінформації або фейкових новин, це може спричинити шкоду суспільству та довірі до інформації.


Маніпуляція громадською думкою: якщо я використовуюся для маніпулювання громадською думкою або створення пропаганди, це може вплинути на політичні процеси, вибори та соціальну стабільність.


Порушення конфіденційності та приватності: якщо недобросовісні особи зловживають моїми можливостями, їм може вдатися отримати конфіденційну інформацію про людей або порушити їхню приватність.

Поширення зловмисного програмного забезпечення: якщо зловмисники змінюють мою функціональність або використовують мої можливості для створення та поширення шкідливих програм або вірусів, це може завдати шкоди комп'ютерній безпеці й інфраструктурі.

Важливо зрозуміти, що ці загрози не виникають безпосередньо через мою природу як AI моделі, але вони можуть з'являтися через недобросовісне використання. Щоб повністю контролювати ці потенційні загрози, потрібен ретельний нагляд, регулювання й етичне використання технологій штучного інтелекту".

Фахово займаючись питанням захисту інформації, ми поцікавилися у ChatGPT про кібербезпеку у процесі його використання й отримали у відповідь таке (рис. 4).

 розкажи про кібербезпеку при використанні chatGPT

 Кібербезпека є важливою темою при використанні ChatGPT або будь-якого іншого інтерактивного онлайн-інструменту. Хоча ChatGPT є потужним інструментом для забезпечення корисної інформації та розваг, важливо дотримуватись кількох принципів безпеки для захисту своєї конфіденційності та особистої безпеки:

1. Конфіденційність даних: Уникайте надавати особисту, конфіденційну або фінансову інформацію через ChatGPT або інші подібні сервіси. Не розголошуйте свої паролі, номери соціального страхування, банківські реквізити або інші особисті дані.
2. Бережливе поводження з інформацією: Уникайте розголошення конфіденційної або

Рис. 4. Фрагмент тексту відповіді ChatGPT на запитання "Розкажи про кібербезпеку під час використання ChatGPT"



Кібербезпека є важливою темою при використанні ChatGPT або будь-якого іншого інтерактивного онлайн-інструменту. Хоча ChatGPT є потужним інструментом для забезпечення корисної інформації та розваг, важливо дотримуватись кількох принципів безпеки для захисту своєї конфіденційності й особистої безпеки:

1. Конфіденційність даних: уникайте надавати особисту, конфіденційну або фінансову інформацію через ChatGPT або інші подібні сервіси. Не розголошуйте свої паролі, номери соціального страхування, банківські реквізити або інші особисті дані.

2. Ощадливе поводження з інформацією: уникайте розголошення конфіденційної або чуливої інформації, якщо ви не впевнені в безпеці отримувача. Не надавайте особисті дані про себе або інших людей, якщо вам необхідно зберегти приватність.

3. Фільтруйте інформацію: не всі відповіді, надані ChatGPT, можуть бути точними або актуальними. Завжди перевіряйте будь-яку надану інформацію з довіреного джерела, особливо якщо вона стосується конфіденційності, безпеки або фінансів.

4. Усвідомленість про фішинг: фішинг – це метод шахрайства, коли зловмисники намагаються отримати вашу особисту інформацію шляхом імітації довіреної особи або організації. Не відкривайте посилання, які виглядають підозріло або приходять від ненадійних джерел.

5. Використання офіційних джерел: коли ви використовуєте ChatGPT або будь-який інший інтерактивний онлайн-інструмент, переконайтеся, що ви застосовуєте офіційне та надійне джерело. Не використовуйте посилання на невідомі або підозрілі сайти.

Ці принципи безпеки допоможуть вам зменшити ризики, пов'язані з використанням ChatGPT та забезпечити більшу конфіденційність та безпеку. Завжди пам'ятайте, що важливо бути обережним і розуміти можливі ризики, пов'язані з використанням онлайн-інструментів.

Крім того, важливо враховувати можливість зловживань чат-ботами для поширення шкідливого програмного забезпечення або для зловживань довірою користувачів. Чат-боти мають бути належно перевірені щодо наявності вразливостей і регулярно оновлюватися, щоб захистити їх від нових видів атак.

Також варто враховувати етичні аспекти використання систем штучного інтелекту в чат-ботах. Наприклад, необхідно уникати використання систем для поширення дезінформації або проведення шахрайських дій. Команда розробників і операторів чат-бота повинна дотримуватись високих стандартів етики та використовувати систему відповідально.

Загальні принципи кібербезпеки, такі як регулярне оновлення програмного забезпечення, моніторинг активності й аналіз поведінки, також застосовуються до систем штучного інтелекту. Забезпечення безпеки чат-ботів – це постійний процес, який вимагає уваги і заходів із мінімізації ризиків.

Загалом кібербезпека використання чат-ботів, включно із системою ChatGPT, є комплексним завданням, яке вимагає постійного вдосконалення і впровадження заходів безпеки для захисту користувачів і їхніх даних.

На питання "Як керувати ризиками кібербезпеки?", ChatGPT надав таку відповідь (рис. 5).

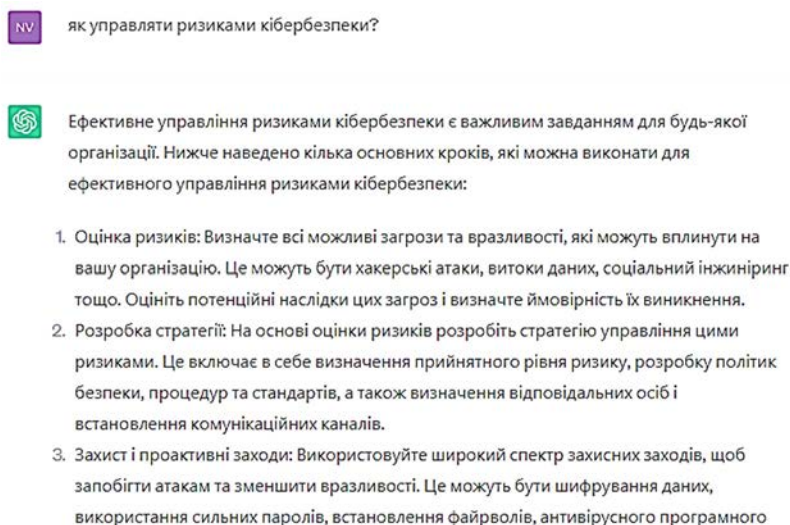


Рис. 5. Фрагмент тексту відповіді ChatGPT на запитання "Як керувати ризиками кібербезпеки"



Ефективне управління ризиками кібербезпеки є важливим завданням для будь-якої організації. Нижче наведено кілька основних кроків, які можна виконати для ефективного управління ризиками кібербезпеки:

1. Оцінювання ризиків: визначте всі можливі загрози та вразливості, які можуть вплинути на вашу організацію. Це можуть бути хакерські атаки, витікання даних, соціальний інжиніринг тощо. Оцініть потенційні наслідки цих загроз і визначте ймовірність їхнього виникнення.

2. Розроблення стратегії: на основі оцінювання ризиків розробіть стратегію управління цими ризиками, що включає визначення прийняттого рівня ризику, розроблення політик безпеки, процедур і стандартів, а також визначення відповідальних осіб і встановлення комунікаційних каналів.

3. Захист і проактивні заходи: використовуйте широкий спектр захисних заходів, щоб запобігти атакам і зменшити вразливості. Це можуть бути шифрування даних, використання сильних паролів, встановлення файрволів, антивірусного програмного забезпечення, регулярне оновлення програмного забезпечення, навчання співробітників безпековим практикам тощо.

4. Виявлення і відновлення: розробіть механізми виявлення вторгнень і кібератак, щоб вчасно виявляти і реагувати на них, включно з моніторингом систем, виявленням аномалій, аудитом безпеки, резервним копіюванням даних і планом відновлення діяльності після інциденту.

5. Навчання та свідомість: забезпечте навчання співробітників щодо кібербезпеки та свідомості про потенційні загрози. Проводьте регулярні тренінги, оновлюйте їхні знання про нові загрози та методи атак. Співробітники мають бути ознайомлені з політиками безпеки та процедурами, а також знати, як повідомляти про підозрілу активність.

6. Аудит та оновлення: регулярно проводьте аудит систем безпеки для виявлення потенційних слабких місць і вразливостей. Оновлюйте свої захисні заходи та політики відповідно до кіберсередовища, що змінюється, та нових загроз.

Управління ризиками кібербезпеки є постійним процесом, і його необхідно систематично оновлювати та вдосконалювати. Пам'ятайте, що кожна організація має свої унікальні потреби і загрози, тому важливо адаптувати ці рекомендації до конкретних умов вашої організації.

Здатність ChatGPT відповідати на запитання змушує деяких користувачів задуматися, чи зможе він замінити Google. Інші запитують, чи не загрожує він роботі журналістів?

За словами Карлі Кінд з Інституту Ади Лавлейс, системи ШІ загального призначення, такі як ChatGPT та інші, створюють низку етичних і соціальних ризиків (Чим небезпечний чат-бот ChatGPT..., 2023).

Серед потенційних проблем є та, що ШІ може посилити поширення дезінформації або зруйнувати наявні інститути та послуги. Наприклад, ChatGPT зможе написати заявку на грант, успішний мотиваційний лист на роботу тощо. Також існують проблеми щодо порушення авторських прав, конфіденційності, з огляду на те, що ці системи часто містять дані, які неетично збираються від користувачів інтернету. Щоправда, такі винаходи у найближчій перспективі можуть принести цікаві переваги для суспільства.

Почесний президент Київської школи економіки Тимофій Милованов також тестував ChatGPT. Він пише про інший ризик – чат-бот бере на віру різні тексти, зокрема і пропаганду. Наприклад, відповідаючи на політичні питання, чат-бот часто повторює російські наративи. На питання Милованова – чий Крим? – чат-бот відповів, що "це спірна територія, яку фактично контролює росія, яка вважає її своєю, а Україна – своєю". Милованов зазначив, що чат-бот не зміг назвати причину війни в Україні, він писав про Майдан, вплив різних міжнародних гравців і відмовився назвати нинішню війну в Україні війною. Це пов'язано з тим, що чат-боти тренуються на всіх англомовних текстах, тому сприймають їх як рівноправні. А росія виробляє значно більше англомовних текстів ніж Україна. Тому, і це дуже важливо, сьогодні президент України переконає політиків і журналістів світу харизмою, емоцією і фактами. Але вже зараз потрібно готуватись переконувати ШІ світу, а там емоція і навіть факти не працюють і це величезний виклик.

Проте важливо зазначити, що ChatGPT постійно навчається, оновлюючи свої знання і нині думка ChatGPT стосовно "чий Крим?" змінилася. Ось яку відповідь він дав нам у середині червня 2023 р. "Крим, також відомий як Кримський півострів, є територією, що споріднюється історично з Україною. Однак внаслідок подій, які відбулися 2014 р., російська федерація анексувала Крим і оголосила його своїм суб'єктом. Цей процес визнано багатьма країнами та міжнародними організаціями незаконним. Україна, Європейський Союз, США та багато інших країн продовжують вважати Крим українським територіальним утворенням, а російська окупація Криму є порушенням міжнародного права".



Як бачимо, хоча ChatGPT має ще багато чому навчитися, проте, як і говорили його розробники – чим більше з ним спілкуватися, тим розумнішим стає цей новий інструмент.

Аналіз багатьох інтернет-ресурсів показав, що про ChatGPT в Україні зазначають таке. Деякі називають його "повним шоком" та вважають, що у майбутньому ця технологія "струсне світ сильніше ніж поява інтернету". "Більше немає сенсу вміти писати курсові, більше не треба мучитись під час написання супроводжувального листа на роботу, більше не потрібне багатоденне планування поїздки, сценарії для художніх творів тепер доступні майже в необмеженому режимі". "За пару років умовний Disney генеруватиме сценарій у ChatGPT, зможе створювати персонажі, анімувати їх в якійсь іншій нейромережі. Причому вартість інтелектуальної роботи стрімко наближається до нуля".

Деякі експерти кажуть, що можливості чат-бота шокують, а деякі переживають, що невдовзі ChatGPT почне забирати в людей їхню роботу.

Відомо, що міністр юстиції Денис Малюська попросив ChatGPT написати законопроект. Каже, жартуючи: "Написало за 30 секунд. Підозрюю, що Мін'юст чекають скорочення вже з понеділка".

Крім зазначених переваг ШІ, є важлива проблема використання його в системі освіти.

Такий "помічник" за лічені секунди здатний цікаво й розгорнуто відповісти на питання, написати вірш, створити креативний контент на будь-яку тему тощо.

Зауважимо, що ChatGPT й аналогічні сервіси ставлять школярів або студентів перед спокусою схитрувати і за допомогою чата-помічника виконати свої домашні завдання в кілька кліків "мишки".

І справді, навіщо витрачати багато часу на пошук інформації в інтернеті та її систематизацію? Можна ввести запит у чат-бот, зачекати кілька секунд і на руках у школяра або студента робота, написана зв'язною, цілком живою мовою, яка практично не відрізнятиметься від тієї, яку вони написали би власноруч, спираючись на інформацію з інтернету. Причому тексти, створені чатом GPT, успішно проходять перевірку на антиплагіат і довести, що їх писав робот, а не учень або студент буває дуже складно.

ChatGPT – це лише одна з перших спроб широкого впровадження у масовий вжиток такої технології. Далі це явище тільки розвиватиметься й набиратиме оберті. Тому в подальшому в освіті такі прості форми контролю знань, як тести, написання есе або твору-роздуму, перестають

бути актуальними, бо ШІ може знайти та структурувати інформацію і розмістити на слайдах замість школяра або студента. Тому виникає питання: як реагувати навчальному процесу на такий технічний прогрес?

Нині система освіти переживає значну кризу, і щоб процес отримання знань був адекватний викликам сьогодення, ми мусимо кардинально переглянути підхід до того, якими мають бути нинішній викладач і сам навчальний процес. Світу загалом, зокрема й Україні, потрібна докорінна трансформація самої суті системи освіти.

Тепер головне завдання викладача не дати знання і навіть не перевірити засвоєння студентом матеріалу, а дати самому студенту можливість проявити ініціативу в навчанні, ефективно використовувати отриману інформацію, комбінувати її і застосовувати отриманий результат у розв'язанні своєї задачі. Успішний студент має навчитися розв'язувати комплексні завдання, які перебувають на стику різних предметів і дисциплін. Нинішні освітні процеси мають розвивати в нього такий крос-дисциплінарний і практико-орієнтований підхід.

Від майбутніх спеціалістів роботодавці очікують умінь подивитися на робоче завдання з різних боків і знайти для нього нетривіальні рішення. Це охоплює вміння працювати у крос-функціональних командах, де кожен учасник – фахівець своєї галузі. Найчастіше для такої співпраці студентам потрібні знання та компетенції з різних професій, а також просто вміння сприймати аргументи від представників іншої спеціальності, з іншими поглядами, й інтегрувати ці пропозиції у спільний командний проєкт.

У цьому процесі головне завдання кожного успішного спеціаліста, який хоче зайняти місце в такій команді, – це застосовувати критичне мислення, здатність думати своєю головою, вміти аналізувати інформацію й інтегрувати свою частку в загальне ціле, під конкретний проєкт. Цього не може зробити робот і жоден чат-бот, але це поки що.

А ось для тих, хто хоче залишитися "вузьким спеціалістом", робота, яку виконують нині junior-фахівці, з розвитком штучного інтелекту може стати фактично непотрібною. Такі чати, як GPT або нейромережі на кшталт Midjourney, вже зараз, успішно виконують роботу примітивних дизайнерів і копірайтерів.

Для навчання й розвитку майбутні фахівці мають бути суперпродуктивними й різнобічно компетентними, щоб залишатися на плаву та бути затребуваними й успішно конкурувати з розвит-



ком ШІ. У навчанні й роботі більше не буде місця примітивізму. Тому освіта має зосередитися на комплексних завданнях, для розв'язання яких студент має опанувати різні дисципліни, але найголовніше, майбутній фахівець має активно взаємодіяти зі своїми одногрупниками в університеті та спільно з ними шукати шляхи розв'язання того чи іншого завдання.

Ми маємо рухатися від проблеми, задля розв'язання якої потрібна та або інша інформація. І в цьому випадку вже не так важливо, як саме студент її знайде: в підручнику, у Вікіпедії чи у ChatGPT.

Свого часу щодо командної роботи досить популярним був термін "синергія" тобто, простими словами – це спільний ефект від взаємодії людей, який значно перевищує суму дій кожного окремого учасника процесу. Математично це можна подати як "1+1=11". У навчанні такий підхід до спільної командної праці – найрезультативніший. Адже в суспільстві майбутньому фахівцю для досягнення успіху доведеться розвивати насамперед комунікативні навички взаємодії та організаторської роботи і це саме те, чого за студента не зможе зробити жоден чат-бот або ШІ.

Тільки з урахуванням тенденцій розвитку суспільства та технологій ми зробимо Україну у сфері освіти країною, що стане прикладом для всього світу, показавши, яким має бути справжнє навчання у XXI ст., в цифрову епоху (Новий чатбот ChatGPT..., 2023).

Дискусія і висновки

Отже, ChatGPT є потужним інструментом, але нині він має деякі недоліки, які слід враховувати, якщо у планах є його використання.

1. Можливий плагіат. Однією з проблем є ризик плагіату через труднощі з відстеженням походження створеного вмісту. Завдяки здатності ChatGPT генерувати мову, схожу на людську, багато хто стурбований можливістю плагіату.

2. Проблеми сумісності. Нині можна безкоштовно використовувати чат-бот на вебсайті OpenAI. Однак із зростанням популярності моделі ШІ зросла кількість користувачів, які намагаються отримати доступ до вебсайту OpenAI. В результаті це іноді призводить до проблем із пропускнуою здатністю ChatGPT.

3. Недостатньо розумний. Використання ChatGPT для створення ідей у сфері маркетингу та реклами може бути цікавим рішенням. Ввівши назву бренду або продукту та запитавши у ChatGPT ідеї про те, як його просувати, маркетологи можуть отримати багато творчих

пропозицій і перспектив, які вони, можливо, не розглядали раніше. Але ChatGPT може мати проблеми зі складними темами, які вимагають глибшого рівня аналізу, ніж той, у якому була навчена модель.

4. ChatGPT має деякі проблеми, пов'язані з расовими та гендерними упередженнями. На початку грудня 2022 р. професор психології та неврології Каліфорнійського університету в Берклі Стівен Піантадосі поділився у Twitter багатьма тривожними результатами, які він знайшов під час введення певного тексту в чат-бот.

5. ChatGPT не дає статистику. ChatGPT підбиває підсумок темі, але не пропонує унікальності її розуміння. Люди творять завдяки знанням, а також через свій особистий досвід та суб'єктивне сприйняття. Хоча ChatGPT може демонструвати високі граматичні якості й витончені ідеї, йому все одно бракує розуміння.

6. ChatGPT все ще на стадії навчання. Зараз ChatGPT все ще перебуває у процесі навчання та вдосконалення. Компанія OpenAI рекомендує, щоб увесь контент, створений ChatGPT, перевіряв фахівець, щоб отримати відгуки для вдосконалення нейромережі у майбутньому.

7. ChatGPT має машинну мову. Щоб ідентифікувати створений машиною контент, дослідники визначили особливості, якими він звучить неприродно. Однією із цих особливостей є проблеми ШІ з ідіомами. Ця особливість генерованого машиною контенту є однією з проблем ChatGPT. Хоча ШІ черпає відповіді майже з будь-якого доступного джерела і має певним чином усереднюватися, особливості програмування і те, звідки здобуваються дані, викликають серйозні проблеми з довірою.

8. ChatGPT можуть використовувати у зловмисних цілях. Якщо запитати ChatGPT про певні небезпечні теми, наприклад, як спланувати ідеальне вбивство або зробити напад вдома, система пояснить, чому вона не може дати вам відповіді. Але при цьому можна змусити бота створювати таку небезпечну інформацію за допомогою певних прийомів, наприклад, вдавати, що це персонаж у фільмі або, що він пише сценарій про те, як моделі ШІ не повинні відповідати на подібні питання.

9. Проблеми конфіденційності. Нещодавно ChatGPT потрапив у скандал, пов'язаний із збереженням даних. OpenAI заявив, що ChatGPT був відповідальним за витікання платіжних даних. Деякі користувачі могли побачити ім'я та прізвище іншого активного користувача, адресу його електронної пошти, платіжну адресу, останні



чотири цифри номера кредитної картки та термін дії кредитної картки. Повні номери кредитних карток не були розкриті. Компанія OpenAI перевела ChatGPT в автономний режим і тепер виправила помилку.

10. Є питання щодо порушення авторських прав. Є проблеми щодо конфіденційності, враховуючи, що ці системи часто містять дані, які неетично збираються від користувачів глобальної мережі "Інтернет". Щоправда, такі винаходи також можуть принести цікаві та поки що невідомі переваги для суспільства.

11. Проблема використання ChatGPT в системі освіти. Підводячи підсумок цієї статті, хочемо висловити думку виконавчого директора OpenAI Сема Альтмана, "штучний інтелект має пройти довгий шлях, а великі ідеї ще належить відкрити. Іноді це буде невдало. Іноді ми ухвалюватимемо справді погані рішення, а іноді у нас будуть моменти надзвичайного прогресу й успіху" (Чат-бот ChatGPT: помічник ..., 2023).

Внесок авторів: Володимир Наконечний – концептуалізація; методологія; Володимир Сайко – аналіз джерел, підготування огляду літератури або теоретичних засад дослідження; Микола Мордвинцев – збір емпіричних даних та їх валідація; Владислав Луценко – емпіричне дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Краковецький, О. (2023, 6 січня). Генерація текстів в AI-моделях DOU. *Генерація текстів: перевіряємо прогрес AI-моделі від GPT до ChatGPT*. <https://dou.ua/forums/topic/41509>.

Новий чат-бот ChatGPT змусив говорити про себе світ. Чим він небезпечний (2023, 10 січня). *BBC News Україна*. <https://www.bbc.com/ukrainian/news-64221657?xtor=AL-73-%5Bpartner%5D-%5Bukr%5D-%5Bheadline%5D-%5/Bukrainian%5D-%5Bbizdev%5D-%5Bisapi%5D>.

Чат-бот ChatGPT: помічник чи реальна загроза освіти (2023, 10 січня). <https://www.op.ua/news/osvita-v-ukraini/chatbot-chatgpt-pomichnik-chi-realna-zagroza-osviti>.

Чим небезпечний чат-бот ChatGPT – новий продукт у сфері штучного інтелекту (2023, 1 листопада). <https://texty.org.ua/fragments/108687/chym-nebezpechnyj-chatbot-chatgpt-novyj-produkt-u-sferi-shtuchnoho-intelektu/>.

REFERENCES

Chatbot ChatGPT: a helper or a real threat to education (2023, January 10) [in Ukrainian]. <https://www.op.ua/news/osvita-v-ukraini/chat-bot-chatgpt-pomichnik-chi-realna-zagroza-osviti>.

How dangerous is the chatbot ChatGPT – a new product in the field of artificial intelligence (2023, November 1) [in Ukrainian]. <https://texty.org.ua/fragments/108687/chym-nebezpechnyj-chatbot-chatgpt-novyj-produkt-u-sferi-shtuchnoho-intelektu/>

Krakovetsky, O. (2023, January 6). Text generation in AI models DOU. *Text generation: checking the progress of the AI model from GPT to ChatGPT* [in Ukrainian]. <https://dou.ua/forums/topic/41509>.

The new chatbot ChatGPT made the world talk about itself. What makes him dangerous. *BBC News Ukraine* (2023, January 10). <https://www.bbc.com/ukrainian/news-64221657?xtor=AL-73-%5/Bpartner%5D-%5Bukr%5D-%5Bheadline%5D-%5/Bukrainian%5D-%5Bbizdev%5D-%5Bisapi%5D>.

Отримано редакцією журналу / Received: 11.03.24

Прорецензовано / Revised: 18.03.24

Схвалено до друку / Accepted: 13.05.24



Volodymyr NAKONECHNYI, DSc (Engin.), Prof.
ORCID ID: 0000-0002-0247-5400
e-mail: volodym.nakonechnyi@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Volodymyr SAIKO, DSc (Engin.), Prof.
ORCID ID: 0000-0002-3059-6787
e-mail: v.saiko@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Mykola MORDVYNTSEV, DSc (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-7674-3164
e-mail: lukolyy@gmail.com
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine

Vladyslav LUTSENKO, PhD Student
ORCID ID: 0000-0002-2377-1858
e-mail: vlkiller175@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ADVANTAGES AND RISKS OF USING CHATGPT

Background. *This article presents ChatGPT - a new chatbot, one of the latest products in the field of artificial intelligence, created by OpenAI, which developed this technology together with Elon Musk. The article provides recommendations for connecting to a chatbot. The main advantages of artificial intelligence are defined, and examples of its application are given.*

Current educational processes should develop a cross-disciplinary and practice-oriented approach in the student.

Results. *It is shown that among the main advantages of ChatGPT is the ability to generate texts on a given topic, to answer almost all user questions, and to express oneself even in Ukrainian. Specific examples of chatbot questions related, in particular, to information protection, risk management, etc., are given. Demonstrated responses from his side. Focused on the dangers of using a new chatbot. It is shown that possible plagiarism, compatibility issues, malicious use, privacy issues, copyright infringement issues, and problems of using ChatGPT in the educational system occupy a special place among the identified dangers. It is emphasized that the education system is currently experiencing a significant crisis and that the process of obtaining knowledge is adequate to the challenges of today, it is necessary to radically revise the approach to what the current teacher and the educational process itself should be. It is noted that Ukraine needs a fundamental transformation of the very essence of the education system. Now the main task of the teacher is to give the student himself the opportunity to take the initiative in learning, to effectively use the information received, to combine it and to apply the received result in solving his task. A successful student must learn to solve complex tasks that are at the junction of various subjects and disciplines.*

Conclusions. *So, ChatGPT is a powerful tool, but today it has some drawbacks that should be considered if you plan to use it.*

Keywords: *chatbot, neural networks, application, encryption, copyright, privacy, artificial intelligence.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.



ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УДК 004.056

DOI: <https://doi.org/10.17721/ISTS.2024.7.62-68>

Сергій ТОЛЮПА, д-р техн. наук, проф.

ORCID ID: 0000-0003-1715-0761

e-mail: serhii.toliupa@knu.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

Сергій ЛАПТЄВ, асп.

ORCID ID: 0000-0002-7291-1829

e-mail: salaptiev@gmail.com

Київський національний університет імені Тараса Шевченка, Київ, Україна

УДОСКОНАЛЕННЯ МЕТОДУ ВИЯВЛЕННЯ РАДІОСИГНАЛІВ ЗА ДОПОМОГОЮ ТОПОЛОГІЧНОЇ ІДЕНТИФІКАЦІЇ ЗАГРОЗ

Вступ. Людство ввійшло в епоху інформаційної цінності, в якій інформація стає ресурсом, важливішим за інші ресурси. Тому доступ до інформації, особливо до конфіденційної, зокрема і до інформації, яка містить основні конкурентні переваги, є першочерговим завданням конкурентної розвідки. Отримання такої інформації, найчастіше, пов'язане з порушенням закону та застосуванням спеціальних технічних засобів. Нині є можливість розв'язувати складні проблеми щодо витікання інформації швидкими темпами, але спеціалісти технічної розвідки можуть використовувати нові способи проникнення у вашу систему, щоб викрасти важливу інформацію та завдати непоправної шкоди.

Методи. Досліджено методи виявлення небезпечних радіосигналів, які можуть бути сигналами від радіозакладних пристроїв. Запропоновано вдосконалений метод виявлення радіосигналів, вказане вдосконалення засновано на використанні топологічної ідентифікації загроз. Метод засновано на тому, що об'єкт інформаційної діяльності треба розбити на фрактали, тобто області самоподібності. Області самоподібності визначаються фізичними властивостями радіосигналів. Крім фрактальної розмірності, з метою значного підвищення ймовірності виявлення небезпечних радіосигналів, як ідентифікацію радіосигналів вводять відповідні фрактальні міри. Фрактальні міри додатково дозволяють визначити зони, в яких виявляються небезпечні радіосигнали. Задаючи відповідні еталонні значення відповідних параметрів радіосигналів можна визначити фрактальні розмірності через показник Герста і залежно від отриманого значення розмірності можна ідентифікувати небезпечні радіосигнали, сигнали радіозакладних пристроїв або інших пристроїв знімання інформації, які встановлені на об'єкті з конфіденційною інформацією. Використання запропонованого методу дозволить збільшити ефективність виявлення сигналів радіозакладних пристроїв та у випадку виявлення таких сигналів блокувати канал витікання інформації.

Результати. Згідно з дослідженнями аналітиків 76 % міжнародних компаній та державних установ стикались із промисловою розвідкою. За допомогою технічних засобів видобувається 80–90 % необхідної інформації. У зв'язку із цим, зберігання у таємниці комерційно важливої інформації, дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг. Для отримання доступу до комерційної інформації зловмисник застосовує технічні засоби. Одним із видів технічних засобів є радіозакладний пристрій. Для передавання інформації створюється канал передавання отриманої інформації. Тому дуже важливим є питання виявлення та блокування каналів витікання інформації.

Висновки. Доведено, що використовуючи методи фрактальної геометрії, можна об'єкт інформаційної діяльності розбити на фрактали, на області самоподібності. Критеріями, за якими визначають ці області, є фізичні принципи роботи закладних пристроїв. Задаючи відповідні еталонні значення відповідних параметрів, можна визначити фрактальні розмірності через показник Герста.

Ключові слова: радіосигнал, радіозакладний пристрій, витікання інформації, фрактальна розмірність.

Вступ

Людство увійшло в епоху інформаційної цінності, в якій інформація стає ресурсом, важливішим за інші ресурси. Тому доступ до

інформації, особливо до конфіденційної інформації, зокрема і до інформації, яка містить основні конкурентні переваги, є першочерговим завданням конкурентної розвідки. Отримання такої

© Толюпа Сергій, Лаптев Сергій, 2024



інформації, найчастіше, пов'язане з порушенням закону та застосуванням спеціальних технічних засобів. Нині є можливість розв'язувати складні проблеми з витікання інформації більш швидкими темпами, але спеціалісти технічної розвідки можуть використовувати нові способи проникнення у вашу систему, щоб викрасти важливу інформацію та завдати непоправної шкоди. Якість інформації, що використовується, дозволяє отримувати відповідний економічний або моральний ефект. Згідно з дослідженнями аналітиків 76 % міжнародних компаній і державних установ стикались із промисловою розвідкою. За допомогою технічних засобів видобувається 80–90 % необхідної інформації. У зв'язку із цим, зберігання у таємниці комерційно важливої інформації, дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг. Відповідно до мети, яку ставить для себе конкурентна розвідка, використовують різні канали витікання інформації. Існує багато різних типів моделей, які дають можливість виявляти окремі різні канали витікання інформації.

Тому розроблення й удосконалення моделей та методів ідентифікації каналів витікання конфіденційної інформації на об'єкті інформаційної діяльності нині є дуже актуальними.

Метою цієї статті є підвищення ефективності виявлення каналів витікання інформації та сигналів радіозакладних та інших пристроїв знімання інформації завдяки вдосконаленню методу виявлення небезпечних радіосигналів або інших видів небезпечних сигналів.

Огляд літератури. Питанням захисту конфіденційної інформації, розробленню та вдосконаленню моделей виявлення каналів витікання інформації та сигналів радіозакладних пристроїв присвячено значну кількість публікацій.

У роботі (Козачок, 2017) розглянуто різні методи біометричної статичної та динамічної ідентифікації, що дозволяє підвищити ступінь захисту інформації. Ці методи базуються на фізіологічних особливостях людини. На основі цих фізіологічних особливостей можна будувати різні математичні моделі ідентифікації. Вказані моделі можна використовувати у процесі створення різних технологій захисту інформації з обмеженим доступом. Але цей принцип не дозволяє повною мірою захистити конфіденційну інформацію.

Дослідженнями, висвітленими у працях (Sobchuk, Samoilenko, & Samoilenko, 1999) визначено велику кількість параметрів для ідентифікації кібератак на інформаційні системи. Ідентифікація кібератак дає можливість підвищити рівень захисту інформації. Проте кібератаки ідентифікуються не повною мірою та визначені

лише для вузького класу об'єктів, до того ж, постійно розвиваються. Тому ідентифікація не розв'язує проблему повністю.

В роботах В. Собчука, О. Капустяна, О. Барабаша, О. Машкова розкрито особливості ідентифікації в корпоративних інформаційно-телекомунікаційних системах. Досліджено сучасні засоби ідентифікації. Проте методи ідентифікації не розглянуто з погляду можливих інформаційних атак. Не запропоновано математичної моделі, за допомогою якої можна створювати технологію виявлення загроз.

Учені О. Барабаш, Н. Лукова-Чуйко, І. Саланда запропонували технологічне рішення для ідентифікації об'єктів інформаційної діяльності у створенні технічних систем охорони. Однак це рішення притаманне не кожній системі, більшість із них залишаються поза розробленим методом.

Дослідження таких учених, як Н. В. Лукова-Чуйко, С. В. Толюпа, С. О. Лаптев, О. А. Лаптев, описують метод фрактальної розмірності. Проте його запропоновано лише для ідентифікації для оптичних систем. Це значно скорочує кількість галузей, у яких можна використовувати фрактальний аналіз. Тому розвиток теорії фракталів потребує подальшого поширення на різні галузі й об'єкти інформаційної діяльності.

У науковій літературі є багато методик, методів і моделей, які дають можливість виявляти канали витікання інформації, канали якими відбувається витікання конфіденційної інформації, але загальної або універсальної моделі, або загального методу виявлення каналів витікання інформації, нині не існує.

З огляду на викладене вище, наукове завдання з підвищення ефективності виявлення каналів витікання інформації та сигналів радіозакладних пристроїв щодо вдосконалення методу виявлення небезпечних радіосигналів на об'єктах інформаційної діяльності є актуальним (Козачок, 2017, с. 42–48).

Методи

У роботі досліджено методи виявлення небезпечних радіосигналів, які можуть бути сигналами від радіозакладних пристроїв. Запропоновано вдосконалений метод виявлення радіосигналів. Вказане вдосконалення засновано на використанні топологічної ідентифікації загроз. Метод засновано на тому, що об'єкт інформаційної діяльності треба розбити на фрактали, тобто області самоподібності. Такі області самоподібності визначаються фізичними властивостями радіосигналів. Крім фрактальної розмірності, з метою значного підвищення ймовірності виявлення небезпечних радіосигналів, як ідентифі-



кацію радіосигналів вводять відповідні фрактальні міри. Фрактальні міри додатково дозволяють визначати зони, в яких виявляються небезпечні радіосигнали. Задаючи відповідні еталонні значення відповідних параметрів радіосигналів, можна визначати фрактальні розмірності через показник Герста і залежно від отриманого значення розмірності можна ідентифікувати небезпечні радіосигнали, сигнали радіозакладних пристроїв або інших пристроїв знімання інформації, які встановлені на об'єкті з конфіденційною інформацією. Використання запропонованого методу дозволить підвищити ефективність виявлення сигналів радіозакладних пристроїв та у випадку виявлення таких сигналів блокувати канал витікання інформації.

Результати

Під час робіт із пошуку та блокування радіозакладних пристроїв на об'єктах інформаційної діяльності, виникає необхідність розбиття приміщення на пошукові зони. Можна розділити загальне приміщення за існуючим розподілом. У кожній пошуковій зоні з якоюсь імовірністю може розміщуватися радіозакладний пристрій. Практично це і є початком використання сучасного топологічного аналізу. Такий аналіз можна застосовувати в реалізації різних топологічних ефектів, пов'язаних з аналізом аудіоінформації та аналізу зображень. У процесі дослідження об'єктів у багатьох випадках виникає завдання з'ясувати, яким чином пошукові зони пов'язані. Необхідно зрозуміти, чи можна з однієї пошукової зони (геометричного образу) отримати матеріал для іншої. Тобто вже переходимо у фрактальну теорію – в окремий розділ математики. Частиною фрактальної теорії і є саме топологія системи (Sobchuk, Samoilenko, & Samoilenko, 1999, с. 926–933).

Оскільки фрактал – це множина точок у просторі, то це може бути якась геометрична фігура, що має властивість самоподібності. Тоді дослідження розмірності D вказаного об'єкта можна використовувати у пошуку закладних

пристроїв у інших зонах на об'єкті. Підтверджує цю теорію те, що радіосигнали мають ознаки фрактальної структури. Використовуватимемо таке припущення або позначення: якщо фрактальна розмірність області розповсюдження сигналу $D=1$, то це означатиме, що сигнал неперервно розповсюджується без перешкод; якщо $D=2$, то поляризований сигнал поширюється у плоскій області; у разі $D=3$, сигнал розповсюджується у тривимірному просторі. Іншими словами, запропонована фрактальна розмірність дає загальну характеристику розповсюдження сигналу. Однак за наявності завад, область розповсюдження сигналу не можна розглядати як неперервну, тому що в цьому випадку виникають особливі зони, в яких сигнал не поширюється за іншими законами. Тоді в цих випадках фрактальна розмірність уже набуватиме дробове значення. Отже, фрактальну розмірність цієї області залежно від області розповсюдження сигналу, можна в загальному випадку записати виразом (1) (Sobchuk, 2018, р. 233–239):

$$D = k - H, \quad k = \overline{1,3}. \quad (1)$$

Тут H – показник Герста.

Показник Герста невідомий, пояснимо визначення цього показника. Спочатку необхідно розтлумачити поняття – обраний поріг, перевищення якого свідчить про наявність значного радіосигналу в пошуковій зоні. Як поріг для радіосигналу бажано використовувати файл зразка. Файл зразка – це файл, який отримали під час сканування радіодіапазону поблизу об'єкта обстеження. Тоді математичний опис виглядатиме так: $\{\Delta_i, i = 1, \dots, n\}$ – послідовність рівнів перевищення порогів радіосигналів від файлу зразка. На рис. 1 зображено, яким способом визначається перевищення порога файлу зразка (Sobchuk et al., 2019, р. 79–95). Дельта на рисунку показує перевищення порога радіосигналу зразка.

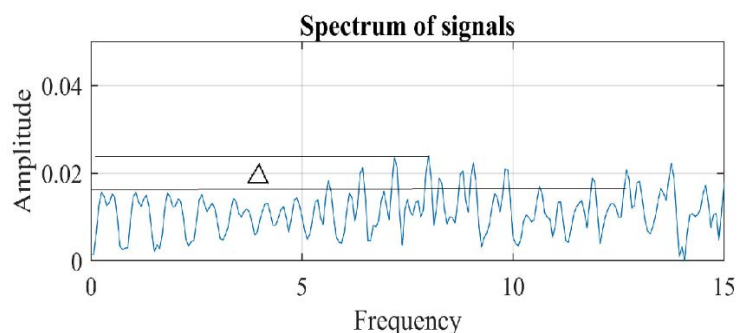


Рис. 1. Визначення перевищення порога заданої порогової амплітуди сигналів



Для виявлення радіозакладного пристрою задають порогову амплітуду A_n і в заданому діапазоні частот від f_1 до f_2 Г за допомогою сканувального приймача або спектр-аналізатора визначають i -ту амплітуду сигналу – того сигналу, що наявний у пошуковій зоні.

Загалом маємо

$$\Delta_i = A_i - A_n. \quad (2)$$

Нехай R – розмах між максимальним і мінімальним значеннями цих порогів.

Тоді

$$R = \max \Delta_i - \min \Delta_i. \quad (3)$$

Середнє значення порога Δ визначимо як середнє арифметичне всіх даних, тобто матимемо вираз

$$\Delta = \frac{1}{n} \sum_{i=1}^n \Delta_i, \quad (4)$$

а середнє квадратичне відхилення визначатиметься виразом

$$\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^n \Delta_i^2 - \Delta^2}. \quad (5)$$

З огляду на вирази (3)–(5) і маючи показник Герста, який буде визначатись виразом (6), маємо

$$H = \frac{\ln\left(\frac{R}{\sigma}\right)}{\ln\left(\frac{n}{2}\right)}. \quad (6)$$

Зробивши підстановку, а саме вираз (6) у (2) отримаємо три можливі значення фрактальної розмірності, які описуватимуться виразом (7):

$$D_1 = 1 - H, \quad D_2 = 2 - H, \quad D_3 = 3 - H. \quad (7)$$

Дослідженнями під час пошукових робіт встановлено: якщо фрактальна розмірність має значення $D_1 > 0,6$, то з великою імовірністю можна стверджувати, що на об'єкті, де проводять роботи з пошуку та блокування радіозакладних пристроїв, якраз і розміщено такий пристрій.

Якщо ж фрактальна розмірність набуває значення $1 < D_2 < 1,35$, то на об'єкті відбувається несанкціоноване знімання інформації за допомогою СВЧ-накачки, без використання радіозакладних пристроїв. Проте такий канал витікання інформації дуже важко виявити у зв'язку з тим, що він працює тільки у разі направлення на закладний пристрій спрямованим випромінюванням.

Якщо фрактальна розмірність набуває значення $D_3 > 2$, то на об'єкті міститься цифровий засіб прихованого знімання інформації.

Отже, запропоновано модель і метод, які дозволяють підвищити ефективність виявлення каналів витікання інформації та сигналів радіозакладних та інших пристроїв знімання інформації завдяки вдосконаленню методу виявлення небезпечних радіосигналів або інших видів небезпечних сигналів.

Варто враховувати, що критерій, за яким знаходять області пошуку, визначається фізичними принципами роботи закладних пристроїв. Тому не слід звертати увагу на досвід фахівця. Саме досвід фахівця доповнює всі фізико-математичні методи пошуку і дозволяє зрозуміти, в якій частині об'єкта може знаходитись той чи інший тип засобу прихованого отримання інформації. Тому ймовірність виявлення каналів і пристроїв знімання інформації також дуже суттєво залежить від досвіду фахівця (Mashkov et al., 2019, p. 344–357).

Практичне застосування розробленої моделі. З метою практичного використання та підтвердження адекватності розробленої моделі проведено натурне моделювання. Як пошуковий апаратно-програмний комплекс небезпечних радіосигналів у натурному моделюванні застосовували програмно-апаратний комплекс DigScan, який дозволяє програмувати порогове значення радіосигналів. Установлювали різні порогові значення, але в цій роботі за порогове взяли значення амплітуди порога 50 дБ. Частотний діапазон обрали від 50 Гц до 3 МГц, але для моделювання можна було використати і менший діапазон частот. Мета радіомоніторингу полягала в тому, що ми намагалися лише отримати відхилення від встановленого нами порогового значення. Тобто у натурному моделюванні нас цікавило лише відхилення від встановленого порогового значення (Varabash et al., 2018).

У реальній роботі у процесі пошуку та блокування засобів прихованого отримання інформації, порогове значення встановлюється для кожного конкретного об'єкта. Порогове значення обиралось після попереднього сканування радіодіапазону біля об'єкта. Порогове значення у методичних матеріалах має назву файл зразка. Слід враховувати, що порогове значення діапазону сканування різне і залежить від частотного завантаження місцевості, де розташовано об'єкт.

В результаті натурного моделювання отримали результати, які дозволили вичислити відхилення від порогових значень у заданому частотному діапазоні. Результати сканування у заданому радіодіапазоні та відхилення амплітуди наведено у таблиці.



Таблиця

Результати сканування

i – порядковий номер амплітуди сигналу	Δ_i , дБ
1	-6,0
2	-6,5
3	-4,0
4	1,0
5	0,5
6	-2,0
7	-5,0
8	2,0
9	-4,0
10	-4,5
11	-8,0
12	-10,0
13	-5,0
14	-1,5
15	-3,5
16	-5,0
17	3,0
18	1,0
19	2,0
20	-1,5
21	-1,0
22	-4,5
23	-5,0
24	-6,0
25	-5,5

Використовуючи дані таблиці, визначили, що $\Delta_{\min} = -10$, $\Delta_{\max} = 3$ і згідно з виразом (3) $R = 13$. У подальшому застосували вираз (4) й отримали, що $\Delta = -2,84$, середнє квадратичне відхилення рівня згідно з виразом (4) $\sigma = 3,3$ дБ. Надалі обчислюємо показник Герста, який згідно з виразом (6) знаходять так:

$$H = \frac{\ln(3,94)}{\ln(12,5)} = 0,54.$$

Маємо такі результати фрактальної розмірності відповідно: $D_1 = 0,46$, $D_2 = 1,46$, $D_3 = 2,46$. За результатами натурного моделювання та математичних обчислень значень фрактальних

розмірностей доходимо висновку, що найбільшій області розповсюдження небезпечного сигналу відповідає фрактальна розмірність D_3 , а це у свою чергу дає можливість стверджувати, що на об'єкті пошуку сигнал поширюється у тривимірному просторі. Це доводить, що з великою імовірністю можна стверджувати про наявність небезпечних сигналів цифрового діапазону. Тобто є велика ймовірність, що на об'єкті пошуку працює цифровий засіб прихованого знімання інформації. Результати моделювання підтвердили адекватність методу та довели дієвість методу пошуку небезпечних сигналів на об'єкті.



Висновки

В результаті проведених досліджень запропоновано вдосконалений метод виявлення небезпечних сигналів. Запропонований метод надає можливість підвищення ефективності виявлення каналів витікання інформації та сигналів радіозакладних та інших пристроїв знімання інформації завдяки вдосконаленню методу виявлення небезпечних радіосигналів або інших видів небезпечних сигналів. Удосконалення полягає у застосуванні у методі топологічної ідентифікації загроз.

Доведено, що використовуючи методи фрактальної геометрії можна об'єкт інформаційної діяльності розбити на фрактали, на області самоподібності. Критерії, за якими знаходять ці області, визначаються фізичними принципами роботи закладних пристроїв. Задаючи відповідні еталонні значення відповідних параметрів можна визначити фрактальні розмірності через показник Герста. За показником Герста, залежно від отриманого значення розмірності можна ідентифікувати вид закладного пристрою, який встановлено на об'єкті. Додатково з метою значного підвищення ефективності виявлення закладних пристроїв, варто для покращення виявлення небезпечних сигналів вводити відповідні фрактальні міри. Це надає можливість не тільки виявляти небезпечні сигнали, а ще й визначити місце розташування засобу знімання інформації на об'єкті.

Внесок авторів: Сергій Толюпа – концептуалізація; методологія; аналіз джерел, підготування огляду літератури або теоретичних засад дослідження; Сергій Лаптев – збір емпіричних даних та їх валідація; емпіричне дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Козачок, В. (2017). Особливості ідентифікації та авторизації в сучасних корпоративних інформаційно-телекомунікаційних системах. *Сучасний захист інформації*, 2(30), 42–48.

Barabash, O., Lukova-Chuiko, N., Sobchuk, V., & Musienko, A. (2018). Application of petri networks for support of functional stability of information systems. *IEEE 1st International Conference on System Analysis and Intelligent Computing*, SAIC 2018 – Proceedings, 2018, <https://doi.org/10.1109/SAIC.2018.8516747>.

2018 – Proceedings, 2018. Shatylova dacha str., 4, of. 702, Kharkiv. <https://doi.org/10.1109/SAIC.2018.8516747>.

Mashkov, O., Sobchuk, V., Barabash, O., Dakhno, N., Shevchenko, H., & Maisak, T. (2019). Improvement of variational-gradient method in dynamical systems of automated control for integro-differential models. *Mathematical Modeling and Computing*, 6(2), 344–357.

Sobchuk, V. (2018). Approximate Homogenized Synthesis for Distributed Optimal Control Problem with Superposition Type Cost Functional. *Statistics Optimal Information Computer*, 6, 233–239.

Sobchuk, V., Barabash, O., Kopiika, O., Zamrii, I., & Musienko, A. (2019). *Modern Mathematics and Mechanics: Fundamentals, Problems and Challenges. Fraktal & Differential Properties of the Inversor of Digits of Q_s -Representation of Real Number*. Springer.

Sobchuk, V., Samoilenko, A., & Samoilenko, V. (1999). On periodic solutions of the equation of a nonlinear oscillator with pulse influence. *Ukrainian Mathematical Journal*, Springer New York, 926–933.

REFERENCES

Barabash, O., Lukova-Chuiko, N., Sobchuk, V., & Musienko, A. (2018). Application of petri networks for support of functional stability of information systems. *IEEE 1st International Conference on System Analysis and Intelligent Computing*, SAIC 2018 – Proceedings, 2018, <https://doi.org/10.1109/SAIC.2018.8516747>.

Kozachok, V. (2017). Peculiarities of identification and authorization in modern corporate information and telecommunication systems. *Modern information protection*, 2(30), 42–48 [in Ukrainian].

Mashkov, O., Sobchuk, V., Barabash, O., Dakhno, N., Shevchenko, H., & Maisak, T. (2019). Improvement of variational-gradient method in dynamical systems of automated control for integro-differential models. *Mathematical Modeling and Computing*, vol. 6(2), 344–357.

Sobchuk, V. (2018). Approximate Homogenized Synthesis for Distributed Optimal Control Problem with Superposition Type Cost Functional. *Statistics Optimal Information Computer*, 6, 233–239.

Sobchuk, V., Barabash, O., Kopiika, O., Zamrii, I., & Musienko, A. (2019). *Modern Mathematics and Mechanics: Fundamentals, Problems and Challenges. Fraktal & Differential Properties of the Inversor of Digits of Q_s -Representation of Real Number*. Springer.

Sobchuk, V., Samoilenko, A., & Samoilenko, V. (1999). On periodic solutions of the equation of a nonlinear oscillator with pulse influence. *Ukrainian Mathematical Journal*, Springer New York, 926–933.

Отримано редакцією журналу / Received: 13.03.24
Прорецензовано / Revised: 27.03.24
Схвалено до друку / Accepted: 13.05.24



Serhii TOLIUPA, DSc (Engin.), Prof.
ORCID ID: 0000-0003-1715-0761
e-mail: serhii.toliupa@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Serhii LAPTIEV, PhD Student
ORCID ID: 0000-0002-7291-1829
e-mail: salaptiev@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

IMPROVEMENT OF THE METHOD OF DETECTION OF RADIO SIGNALS WITH THE HELP OF TOPOLOGICAL IDENTIFICATION OF THREATS

Background. *Humanity has entered the era of information value. An era in which information becomes a more important resource than other resources. Therefore, access to information, especially to conference information, especially to information that contains the main competitive advantages, is the primary task of competitive intelligence. Obtaining such information is most often associated with breaking the law and using special technical means. Complex data breaches can now be resolved at a faster pace, but tech intelligence professionals can use new ways to penetrate your system to steal valuable information and cause irreparable damage.*

Methods. *The work examines the methods of detecting dangerous radio signals, which can be signals from radio jamming devices. An improved method of detecting radio signals is proposed, the improvement is based on the use of topological identification of threats. The method is based on the fact that the object of information activity must be divided into fractals, that is, areas of self-similarity. Areas of self-similarity are determined by the physical properties of radio signals. In addition to the fractal dimension, in order to significantly increase the probability of detecting dangerous radio signals, introduce the appropriate fractal measures as the identification of radio signals. Fractal measures additionally allow you to determine the zones in which dangerous radio signals are detected. By setting the appropriate reference values of the relevant parameters of radio signals, it is possible to determine the fractal dimensions through the Hurst index and, depending on the obtained dimension value, it is possible to identify dangerous radio signals, signals of radio interceptor devices or other information capture devices that are installed at the facility with conference information. The use of the proposed method allows to increase the efficiency of detection of signals of radio interceptor devices and, in case of detection of such signals, to block the channel of information leakage.*

Results. *According to research by analysts, 76% of international companies and government institutions have encountered industrial intelligence. With the help of technical means, 80-90% of the necessary information is extracted. In this regard, keeping commercially important information secret allows us to successfully compete in the market for production and sales of goods and services. The attacker uses technical means to gain access to commercial information. One of the types of technical means is a radio device. For the transmission of information, a transmission channel of the received information is created. Therefore, the issue of identifying and blocking information leakage channels is very important.*

Conclusions. *It is proved that using the methods of fractal geometry, it is possible to divide the object of information activity into fractals, into areas of self-similarity. The criteria by which these areas are determined are determined by the physical principles of embedded devices. By setting the corresponding reference values of the corresponding parameters, it is possible to determine the fractal dimensions through the Hurst index.*

Keywords: *radio signal, radio deposit device, information flow, fractal dimension.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.

Наукове видання



БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

№ 1(7)/2024

Редактор *Л. Магда*

Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, економіко-статистичних даних, власних імен та інших відомостей. Редколегія залишає за собою право скорочувати та редагувати подані матеріали.

Оригінал-макет виготовлено Видавничо-поліграфічним центром "Київський університет"
Виконавець *В. Гаркуша*



Формат 60x84^{1/16}. Ум. друк. арк. 8,02. Наклад 100. Зам. № 224-10999.
Гарнітура Times New Roman. Папір офсетний. Друк офсетний. Вид. № 1т1.
Підписано до друку 01.07.2024

Видавець і виготовлювач
ВПЦ "Київський університет",
б-р Тараса Шевченка, 14, м. Київ, 01601, Україна
☎ (38044) 239 32 22; (38044) 239 31 72; тел./факс (38044) 239 31 28
e-mail: vpc_div.chief@univ.net.ua; redaktor@univ.net.ua
http: vpc.knu.ua
Свідоцтво суб'єкта видавничої справи ДК № 1103 від 31.10.02