

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. Н. КАРАЗІНА

ІТ-ПРОСТІР СЬОГОДЕННЯ: ТЕНДЕНЦІЇ, ІННОВАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Збірник тез доповідей
II Міжнародної науково-практичної студентської
конференції

(15 жовтня 2025 року, м. Харків, Україна)

Електронний ресурс

Харків – 2025

УДК 338.46:004](063)

I-70

*Реєстраційне посвідчення УкрІНТЕІ МОН України
(№ 761 від 09 грудня 2024 р.)*

*Затверджено до розміщення в мережі Інтернет рішенням Вченої ради
Харківського національного університету імені В. Н. Каразіна
(протокол № 28 від 27 жовтня 2025 року)*

Редакційна колегія:

д-р. екон. наук, проф. Б. В. Самородов (головний редактор);
к.філос.н., доц. А.А. Чхеайло;
к-т. екон. наук, доц. Р. О. Піскунов;
д-р. екон. наук, проф. Г. М. Азаренкова;
д-р. екон. наук, проф. А. П. Грінько;
к-т. екон. наук, доц. Н. Л. Морозова;
к-т. пед. наук, доц. Н. І. Стяглик.

Адреса редколегії:
61022, м. Харків, майдан Свободи, 4

I-70 ІТ-простір сьогодення: тенденції, інновації та перспективи розвитку:
збірник тез доповідей II Міжнародної науково-практичної
студентської конференції (15 жовтня 2025 року, м. Харків, Україна)
[Електронний ресурс]. – Харків : ХНУ імені В. Н. Каразіна, 2025. –
1 ел. опт. диск (CD-ROM). – Систем. вимоги: Процесор Pentium-
класа ; ОС Windows 7/10 ; дисковод CD-ROM; Acrobat Reader 10. –
524 с. (PDF)

ISBN 978-966-285-805-1

<https://ekhnuir.karazin.ua/handle/123456789/23685>

У збірнику представлені тези доповідей учасників II Міжнародної науково-практичної студентської конференції на загальну тему «ІТ-простір сьогодення: тенденції, інновації та перспективи розвитку».

Для студентів, аспірантів, науковців вищих навчальних закладів. Матеріали подано в авторській редакції. Відповідальність за зміст і оформлення матеріалів несуть автори.

Усі права застережено. Посилання на матеріали обов'язкові.

УДК 338.46:004](063)

<https://ekhnuir.karazin.ua/handle/123456789/23685>

ISBN 978-966-285-805-1

© Харківський національний
університет імені В. Н. Каразіна, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
V. N. KARAZIN KHARKIV NATIONAL UNIVERSITY

IT-SPACE OF TODAY: TRENDS, INNOVATIONS AND DEVELOPMENT PROSPECTS

Collection of abstracts
of the II International Scientific and Practical
Student Conference

(October 15, 2025, Kharkiv, Ukraine)

Electronic resource

Kharkiv – 2025

UDC 338.46:004](063)

I-70

*Registration certificate of UkrINTEI of the Ministry of Education and Science of Ukraine
(No. 761 dated December 09, 2024)*

*Approved for posting on the Internet by the decision of the
Academic Council in V.N. Karazin Kharkiv National University
(Minutes №28 of October 27, 2025)*

Editorial Board:

Doctor of Economics, Professor Borys Samorodov (Editor-in-Chief);

PhD in Philosophy, Associate Professor Anna Chkheailo;

PhD in Economics, Associate Professor Roman Piskunov;

Doctor of Economics, Professor Galyna Azarenkova;

Doctor of Economics, Professor Alla Grinko;

PhD in Economics, Associate Professor Nadiia Morozova;

PhD in Pedagogy, Associate Professor Natalia Stiahlyk.

Editorial board address:

4 Svobody Square, Kharkiv, 61022, Ukraine

IT space of today: trends, innovations and development prospects: a collection of abstracts of the II International Scientific and Practical Student Conference (October 15, 2025, Kharkiv, Ukraine) [Electronic resource]. – Kharkiv: V. N. Karazin Kharkiv National University, 2025. 1 electronic disk (CD-ROM). – System requirements: Pentium-class processor; OC Windows 7/10; CD-ROM drive; Acrobat Reader 10. – 524 p.(PDF)

ISBN 978-966-285-805-1

<https://ekhnuir.karazin.ua/handle/123456789/23685>

The collection presents abstracts of the participants of the II International Scientific and Practical Student Conference on the general topic “IT Space of Today: Trends, Innovations and Development Prospects”.

For students, postgraduates, and researchers of higher education institutions. The materials are presented in the author's edition. The authors are responsible for the content and design of the materials.

All rights reserved. References to the materials are required.

UDC 338.46:004](063)

<https://ekhnuir.karazin.ua/handle/123456789/23685>

ISBN 978-966-285-805-1

© V.N. Karazin Kharkiv National University, 2025

РОЗДІЛ 1.

ЗАГРОЗИ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩУ, КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Hart D.O.

Higher education student

Institute № 5 of Kharkiv National University of Internal Affairs

Pavlina T.V.

Senior lecturer at the Department of Language Training

Institute № 5 of Kharkiv National University of Internal Affairs

ANALYSIS OF SOCIAL ENGINEERING ATTACKS IN THE MODERN INFORMATION SPACE AND METHODS OF PREVENTING THEM

In today's information environment, social engineering has become one of the most dangerous tools used by cybercriminals. It is based not on technical vulnerabilities, but on human ones, such as trust, ignorance, and emotions. This is especially relevant for Ukraine, where cyberspace is part of hybrid warfare, and information attacks are often combined with social manipulation. User vulnerability is exacerbated by stress, instability, information overload, and insufficient cyber education.

The categories of uninformed users who are most often affected by social engineering include:

- Elderly people with limited experience in using digital technologies;
- Young people who actively use social networks but often neglect security settings;
- New users of digital services who do not understand the principles of authentication and data protection.

To effectively counter threats, it is necessary to have a deep understanding of the social engineering methods used by attackers, how they work, and how to recognise them. Below is a systematic overview of the main techniques used in modern attacks.

Phishing is a type of online fraud aimed at gaining illegal access to users' confidential data. The word is homophonous with the English word 'fishing' because the technique uses the same logic of 'catching'. The latest targets of phishing are social networks, i.e. sites where you communicate with friends, as personal data and login details entered on such sites can be stolen through phishing and used to steal personal data.

An example of a phishing message is "Your account will be blocked. Update your details immediately." The text contains a hyperlink that leads to a fake web page that looks identical to the real bank website. After entering your credentials (login, password, card details), the information is sent to the attacker.

- Vishing is a type of fraud in which criminals use telephone communication to force a person to disclose their confidential banking or personal data or encourage them to perform certain actions with their bank account or bank card. The fraudsters skilfully play a certain role (usually a bank employee, technical specialist, service provider, government organisation, IT service employee, etc.) and use social engineering techniques, methods and technologies.

An example is when a user receives a phone call from a person who claims to be an employee of the security service of a state digital service (for example, 'Diy'). The caller reports alleged suspicious activity in the user's digital document and asks them to confirm their identity by providing a code from an SMS message. In reality, this code is a one-time password for login initiated by the attacker themselves.

- Smishing (SMS + phishing). This criminal scheme is aimed at getting the user to click on a malicious link in an SMS message. For example, an SMS message is sent to a mobile phone imitating a delivery service: "Your parcel has been delayed. Confirm delivery: rozetka-ua.info/track."

Clicking on the link takes the user to a fake page where they enter their payment details to 'pay for delivery,' which are then sent to the attacker.

- Baiting is a social engineering technique (a method of manipulating human behaviour) used by attackers to trick victims into doing something.

This social engineering method uses a kind of 'bait' to persuade potential victims to use malicious products. Fraudsters usually use websites or links for this purpose, offering to get something for free (e.g., a film, book, song, or other digital file). A hacker may ask you to create an account or immediately download a file that automatically installs malicious software on your computer. [1]

How to counteract attackers who use social engineering methods online:

- Be critical of any offers from strangers, especially tempting ones.
- Do not be afraid and do not rush to do what fraudsters ask or, even more so, demand;
- Be careful with unknown links and attachments – do not open them unnecessarily;
- Do not work in the presence of strangers with personal data, especially card details (number, expiry date, CVV code, PIN code), passwords for online banking or any other passwords and codes sent in SMS messages.
- Install and update antivirus software.
- Use different and complex passwords to access personal and corporate email, social networks and banking applications. [2]

So, social engineering attacks are a tricky threat that mixes technical, psychological, and social stuff. Their effectiveness is based on human vulnerability rather than software flaws. Therefore, countering such attacks requires an interdisciplinary approach – a combination of cybersecurity, educational technologies, behavioural analytics, and communication ethics.

List of sources used:

1. Cyber fraud: Phishing. Wishing. Smishing. Baiting. URL: <https://kopirait.com.ua/kibershahrajstvo-fishyng-vishyng-smishyng-bejting/>
2. How fraudsters manipulate: see another series of the project «Cyber security.UA» about social engineering. URL: <https://cyberpolice.gov.ua/article/yak-shaxrayi-manipulyuyut-dyvitsya-chergovu-seriyu-proyektu-kiberbezpekaua-pro-soczialnu-inzheneriyu-2586/>
3. Combating Cybercrime: English language textbook for second-year cadets / V.V. Markov, G.S. Oganezova; Ministry of Internal Affairs of Ukraine, Kharkiv

National University of Internal Affairs; International Women's Rights Protection Centre 'La Strada – Ukraine'. Centre 'La Strada – Ukraine'. – Kharkiv: Human Rights Publishing House, 2014. – 152 p.

UDC 330.341

Kviatkivska A. P.

student of the State University of Trade and Economics

Geseleva N.V.

PhD, Associate Professor, Associate Professor of the

Department of Digital Economy and System Analysis

State University of Trade and Economics

INNOVATION AND BUSINESS: MODERN TRENDS

Since the late 18th century, humanity has witnessed the development of technologies and gained experience in working with them, and since the 2000s we have seen their rapid growth. Today, people are both people exist in a constant flow of information, while businesses face competition, with those who keep up with trends staying ahead. Innovation is an important source of growth and a key determinant of competitive advantage for many organizations.

Achieving innovation requires the coordinated efforts [1]. These are exponentially increasing demand for computing power, capturing the attention of management teams and the public, and accelerating experimentation. These developments are occurring against a backdrop of rising global competition as countries and corporations race to secure leadership in producing and applying these strategic technologies [2].

According to a McKinsey Global survey, 84 percent of executives say «innovation is extremely or very important to their companies' growth strategy»[3]. For businesses, this creates powerful challenges, and ignoring them automatically means losing a competitive advantage.

Meanwhile, consumers are becoming increasingly demanding, quickly developing habits around new technologies. Now the consumer expects speed, AI integration, and convenience. Another concept is globalization, which is rather an advantage for businesses, as it expands opportunities. Just ten years ago, it was hard to imagine being able to order a product from another continent. When businesses succeed, everyone benefits.

Maybe the most popular and discussing thing – AI. Agentic AI can operate, make decisions, and perform tasks independently of humans. Not only that, but it can also learn from customer interactions, adapting and improving over time [3]. The implementation of artificial intelligence has a positive impact on the customer experience, as it enables faster responses. It helps create the impression that the business is always with the customer 24/7, which can contribute to increasing sales during nighttime hours.

At the same time, the risk of cyberattacks is increasing. Companies, whether small or large, must not forget an important factor – cybersecurity. Today, vast amounts of personal information are stored on various platforms and can be exploited for fraudulent purposes. Cybersecurity is not only about trust, it is about building safety first and foremost.

Another factor that is positive and indicates that we are moving in the right direction toward a sustainable approach is when actions speak louder than words – when it is about caring for the environment and consciously considering the consequences. I would like to talk more about sustainable development.

Sustainability in business refers to a company's strategy and actions to reduce adverse environmental and social impacts resulting from business operations in a particular market. Even during the COVID-19 pandemic, companies continued to align to the United Nations General Assembly sustainable development goals (SDGs) set in 2015 and intended to be achieved by the year 2030 [4].

Examples of sustainability in business:

- Improving energy management efficiency by using alternative power sources and carbon accounting.
- Deploying infrastructure that reduces greenhouse gas (GHG) emissions, preserves water resources and eliminates waste.
- Operating dynamic and efficient supply chains to empower a circular economy, encourage reuse, design out waste, promote sustainable consumption and protect natural resources.
- Enabling sustainable development by assessing risks and improving resiliency while adhering to external regulations and development goals[4].

Another important factor is the care and development of employees. Today, we are witnessing changes that have remained the same for decades: some companies are shifting to a four-day workweek, investing in quality meals for employees, yoga, and gym facilities. Could we have imagined 20 years ago that an office would have a room for relaxation and self-reflection? All of this is about a human-centered approach, which is an advantage and a great trend among employers.

The global technology landscape is undergoing significant shifts, propelled by fast-moving innovations in technologies. We cannot avoid technology; we can use it to build a better present.

Resources:

1. Innovative organizations: structure, learning and adaptation, *Innovation Perspectives for the 21st Century*, Madrid: BBVA, Spain, pp. 163-175. URL: https://pure.royalholloway.ac.uk/ws/portalfiles/portal/1457271/Innovative_organizations_BBVA_book_Lam_Dec_2010.pdf
2. McKinsey & Company. “The Top Trends in Tech.” *McKinsey Digital*. URL: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech>
3. BigSpeak. 8 Emerging Trends in Business Innovations in 2025. URL:

4. <https://www.bigspeak.com/8-emerging-trends-in-business-innovations-in-2025/>
5. BM. “Business Sustainability.” IBM THINK. URL: <https://www.ibm.com/think/topics/business-sustainability>

UDC 004.056.53

*Nikolaichuk A.I.,
applicant of higher education,
Kharkiv National University of Radio Electronics
Kobylin I.O.,
PhD in Engineering,
Assistant Lecturer of the Department of Informatics,
Kharkiv National University of Radio Electronics;*

SYNTACTIC COMPLEXITY AS A FACTOR IN PREDICTION ACCURACY FOR SENTENCE SIMILARITY TASKS IN UKRAINIAN

Transformer-based models have significantly improved the performance of semantic textual similarity (STS) tasks [1]. However, the effect of syntactic complexity on their accuracy remains largely unexplored, especially in languages with flexible word order such as Ukrainian [2].

There are various textual and sentence complexity measures, though the unified metric is not available. Structural properties are more informative when exploring the complexity of the shorter text inputs, such as sentences. Hence, the syntactic complexity was measured using Mean Dependency Distance (MDD). It reflects the average span between words that are syntactically linked [3]. Since MDD generally measures the cognitive load of sentence processing, it is widely used and comparable across different languages, so it can serve as a meaningful metric for Ukrainian.

Dependency Distance (DD) refers to how far apart two connected words are – a head and its dependent in a sentence. For example, if a verb is directly followed by its object, the distance is short, but if several words intervene, the distance increases. For a sentence with n words, MDD (1) is calculated as the average of all dependency distances, excluding the root relation (which is assigned a distance of zero):

$$MDD = \frac{1}{n-1} \sum_{i=1}^{n-1} |DD_i|. \quad (1)$$

The dataset for this study is the Ukrainian version [4] of the widely adopted Semantic Textual Similarity Benchmark (STSB), containing 5749 sentence pairs with similarity scores from 0 to 1. Based on the observed distribution of MDD values, three groups of sentences were defined: low, medium, and high complexity, bounds of which are depicted in Figure 1.

Six multilingual models from the Sentence-Transformers library on the Hugging Face platform were selected: paraphrase-multilingual-mpnet-base-v2 (MPNet), paraphrase-multilingual-MiniLM-L12-v2 (MiniLM), LaBSE, gte-multilingual-base (GTE), distiluse-base-multilingual-cased-v2 (DistilUSE), and static-similarity-mrl-multilingual-v1 (StaticSim).

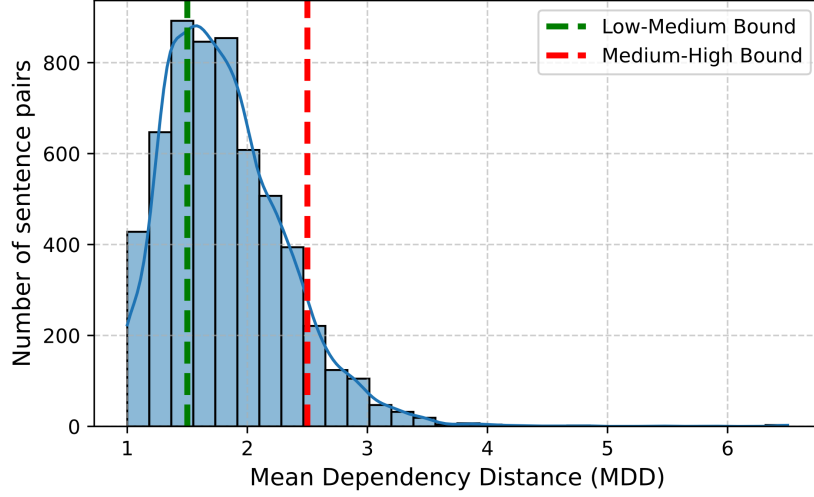


Figure 1 – Distribution of MDD

The goal was to evaluate whether model prediction errors are related to MDD in terms of overall correlation and group-level differences. First, Pearson’s correlation coefficient was calculated to test the continuous relationship between MDD (x_i) and model errors (y_i) as in formula (2):

$$r = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})^2}}. \quad (2)$$

Table 1 demonstrates that the negative correlation is both consistent and statistically significant.

Table 1.

Pearson’s correlation coefficient between MDD and model errors

	MPNet	MiniLM	LaBSE	GTE	DistilUSE	StaticSim
r	-0.07	-0.06	-0.22	-0.15	-0.17	-0.1
p-value	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001

Across all models, the results showed a consistent negative correlation, meaning that lower-complexity sentences tended to cause higher errors. This counterintuitive pattern suggests that models might rely on the presence of stronger syntactic cues, which are often missing in simpler sentences.

Among the models, LaBSE and DistilUSE displayed the strongest correlations, translating into higher sensitivity to syntactic complexity. On the contrary, MPNet and MiniLM showed only weak relationships.

Second, the Kruskal-Wallis test was applied to compare model errors across the three complexity groups. The test is a non-parametric alternative to ANOVA, suitable for non-normally distributed data, as is the case here. The test statistic H according to formula (3) is:

$$H = \frac{12}{N(N+1)} \left(\frac{R_1^2}{n_1} + \frac{R_2^2}{n_2} + \dots + \frac{R_k^2}{n_k} \right) - 3(N + 1), \quad (3)$$

where N is the total number of observations and k indicates the number of groups under comparison (three complexity levels in this study). Each group contributes its sample size n_k and the sum of the ranks R_k . The statistic reflects how much the rank distributions differ across groups.

Test results shown in Table 2 confirmed significant differences for all models, with the same ranking pattern. The same as in Table 1, LaBSE and DistilUSE were most affected, while MPNet and MiniLM were least sensitive.

Table 2.

Kruskal-Wallis test results across complexity levels

	MPNet	MiniLM	LaBSE	GTE	DistilUSE	StaticSim
H-statistic	11.22	9.96	183.82	82.43	120.62	39.06
p-value	0.004	0.007	<0.001	<0.001	<0.001	<0.001

Thus, the negative correlations highlight a general trend, while the Kruskal-Wallis results confirm that error distributions shift across different complexity levels.

The analysis demonstrates that syntactic complexity has a measurable impact on the performance of sentence similarity models. Negative values of Pearson correlation indicate that prediction errors are more frequent for simpler sentences with shorter dependency distances. Complementary evidence from the Kruskal-Wallis test confirms that error distributions differ significantly across the defined complexity levels. This finding highlights that the effect of complexity is not limited to individual cases but is consistent across the dataset as a whole.

These results suggest that syntactic complexity should be considered an important variable in evaluating and developing systems predicting semantic textual similarity. While overall model performance may appear strong, systematic weaknesses in handling structurally simple inputs suggest that transformer models often rely on structural cues to anchor their similarity judgments. When such cues are limited, the models struggle to align their predictions with human-annotated similarity scores.

References:

1. SemEval-2017 Task 1: Semantic Textual Similarity Multilingual and Crosslingual Focused Evaluation / D. Cer et al. *Proceedings of the 11th International Workshop on Semantic Evaluation (SemEval-2017)*, Vancouver, Canada. Stroudsburg, PA, USA, 2017. URL: <https://doi.org/10.18653/v1/s17-2001>.
2. Pires T., Schlinger E., Garrette D. How Multilingual is Multilingual BERT?. *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, Florence, Italy. Stroudsburg, PA, USA, 2019. URL: <https://doi.org/10.18653/v1/p19-1493>.
3. Haitao Liu. Dependency Distance as a Metric of Language Comprehension Difficulty. *Journal of Cognitive Science*. 2008. Vol. 9, no. 2. P. 159–191. URL: <https://doi.org/10.17791/jcs.2008.9.2.159>.
4. STSB-UK · Datasets at Hugging Face. *Hugging Face – The AI community building the future*. URL: <https://huggingface.co/datasets/anikol12/STSB-UK>.

UDC: 004.056

Osmanov S.S.O.

higher education student,

Institute of «Criminal police» KNUIA

Scientific supervisor

Horbach N.L.

senior lecturer «department of foreign languages»

Institute of «Criminal police» KNUIA

INFORMATION SECURITY ISSUES

In the present era of global connectivity, ensuring the security of information has become a key priority. With massive amounts of private and sensitive data being constantly stored, transmitted, and exchanged through networks, the risks of breaches and misuse have grown considerably. Therefore, individuals, organizations, and governmental bodies must treat data security as a critical responsibility, both to safeguard vital resources and to uphold long-term trust within society and professional relationships.

The spectrum of information security threats is broad, including acts of human error or failure, deliberate attacks such as espionage or extortion, compromises to intellectual property, software attacks, technical hardware or software failures, and forces of nature [2].

Common threats to data security include various cyber security threats such as malware, phishing attacks, vulnerabilities, backdoor attacks, formjacking, cryptojacking, DDoS attacks, and DNS poisoning attacks [1].

Strong data security not only prevents unauthorized access and data breaches but also ensures the integrity and availability of information. With the rapid

advancement of technologies such as cloud computing, artificial intelligence, and the Internet of Things (IoT), the attack surface for cybercriminals continues to expand. As a result, implementing multi-layered security measures including encryption, access control, regular audits, and employee training has become essential.

Compliance with data protection regulations, such as GDPR, HIPAA, and CCPA, is another critical aspect of data security practices. Non-compliance can lead to severe penalties and tarnish an organisation's reputation. Therefore, integrating comprehensive data security measures into business operations is imperative to protect data and demonstrate a commitment to maintaining privacy and confidentiality [1].

Phishing attacks represent a widespread method of social engineering, where cybercriminals attempt to illegally gain access to sensitive data. These may include login credentials, financial information, or personal details. Attackers typically disguise themselves as credible institutions or reliable individuals within electronic communication channels, making the deception more convincing and harder to detect. To counter phishing attempts, organizations and individuals must adopt a combination of technological safeguards and awareness strategies. Email filtering systems, multi-factor authentication, and advanced threat detection tools can reduce the likelihood of successful intrusions. However, technology alone is insufficient—continuous user education is vital. Training programs that teach employees how to identify suspicious messages, avoid clicking on unknown links, and verify the authenticity of requests significantly lower the risk. In addition, developing clear incident response procedures ensures that, if an attack does occur, it can be quickly contained and investigated to prevent further damage.

Phishing and Social Engineering Susceptibility of the organization's users to phishing and social engineering attacks leading to unauthorized access to hospital systems. A review of security incident data collected over the past year shows that a large number of the incidents documented were related to some form of phishing or social engineering attack [2].

Information security today should be viewed not only as a technological task but also as a strategic business priority. Protecting corporate data means much more than preventing intrusions—it is equally about establishing trust with clients and partners, ensuring uninterrupted business processes, and meeting the demands of continuously updated regulations. An effective defense strategy requires a comprehensive, risk-based approach, where protective measures are seamlessly integrated into daily operations. Instead of treating cybersecurity as a set of separate functions, organizations should embed practices such as encryption, staff awareness programs, and strict access controls into their routine activities. This allows them to significantly lower the probability of attacks and reduce potential damage. Achieving lasting compliance begins with adopting a mindset that prioritizes risk management. A balanced combination of innovative technologies and human expertise enables companies to confidently manage the complex landscape of data protection and regulatory requirements.

References:

1. DataGuard Insights. URL: <https://www.dataguard.com/blog/what-are-the-threats-to-data-security/>
2. Information Security Risk Assessment Toolkit, 2012 pp 195-231. URL: <https://www.sciencedirect.com/science/article/abs/pii/B9781597497350000075>

UDC 004.056:004.738.5

Vytkovets I. O.

Higher Education Student,

ERI "Karazin Banking Institute" V.N Karazin Kharkiv National University

Scientific Advisors:

Denchyk I. S.

Senior Lecturer, Department of Management,

Accounting and Business Communications

Yermakova N.A.

Senior Lecturer, Department of of Information Technologies

and Mathematical Modeling

ERI "Karazin Banking Institute" V. N. Karazin Kharkiv National University

INFORMATION ENVIRONMENT THREATS: CYBERSECURITY AND DATA PROTECTION

Today, cybersecurity is an integral part of our reality, protecting people from numerous potential threats hidden on the internet. It is very important to understand the need for reliable protection and to ensure it by all possible means. This field safeguards confidentiality, protects personal data, and prevents financial losses. Since there are many fraudsters online, it is necessary to ensure reliable protection against them.

Cybersecurity is a system of measures to protect systems, networks, and programs from digital attacks. Such cyberattacks are usually aimed at altering or destroying confidential information or extorting money from users through various means. But what types of threats exist, and how does cybersecurity deal with them?

There are many malicious programs and practices that cause significant harm to the online community. One such tactic is phishing. This is a type of cybercrime where fraudsters send emails pretending to be from a trusted source. In this way, they can obtain usernames, passwords, credit card numbers, or sensitive document data. There is also search engine phishing, where hackers create their own website and index it in legitimate search systems. According to Wandera, five years ago 25 billion spam pages were discovered daily, but this number has been reduced thanks to powerful cybersecurity measures [1].

Ransomware is also a major threat — it is malicious software that demands money by restricting access to files or computer systems. The program offers a ransom in exchange for restoring access, but this is a scam, meaning victims lose both

their money and their access. As for DoS and DDoS attacks, they overload computer systems, preventing them from processing user requests. A DoS (Denial of Service) attack comes from a single source, while a DDoS (Distributed Denial of Service) attack is an expanded form involving multiple botnets. They are often used to distract from more serious, large-scale problems with far-reaching consequences. To protect against massive DDoS attacks, organizations use cloud-based protection, which makes it possible to handle large volumes of malicious requests and scale resources as needed, thereby protecting users.

According to the State Service of Special Communications and Information Protection, in 2024 the number of cyberattacks grew by nearly 70%, reaching 4,315 cases compared to 2,541 in 2023.

One type of cybersecurity tool is encryption, which is applied during file transmission. A service using this method receives the user's message or files and converts them into code, making the original information unreadable. With this method, attackers cannot access or steal the data [2]. To hide IP addresses, VPN networks are used, preventing attackers from learning the user's location. Another important protection technology today is SIEM, which supports security information and event management. It enables companies to monitor activity, provide alerts about potential problems, and prevent them through emergency recovery.

Of course, the simplest and most basic methods of protection remain antivirus software and firewalls. They help detect malicious programs and prevent them from being downloaded. A firewall can be considered a "filter" that controls traffic and blocks dangerous connections to a device. Antivirus software, in turn, neutralizes and removes malware.

Every year, the demand for cybersecurity specialists continues to grow. Over the past five years, the number of vacancies has increased by 350%, mainly due to the rise in cyberattacks. Labor market trends show a growing need for specialists in protecting critical infrastructure [3]. To secure a job in this field, one must have advanced knowledge of international security standards and maintain a constant focus on professional development. Specialists have a wide range of opportunities, including:

- rapid career growth to positions such as CISO and Security Director;
- transition into related areas such as DevSecOps and Cloud Security;
- prospects for international employment;
- the possibility of starting a private cybersecurity company.

Thanks to specialization within cybersecurity, professionals can work as information security analysts, cryptography experts, digital forensics specialists, incident response experts, and more. The career choices are diverse, offering excellent prospects and good income. Protecting confidential information and defending against fraud not only makes this a well-paid career but also a meaningful contribution to the world of technology [4].

In conclusion, cybersecurity plays a crucial role for everyone, whether an ordinary user or a large global corporation. One major advantage is the ability to provide protection regardless of location, but it is equally important to ensure a flexible cybersecurity system, especially to support digital business. Every person

must be aware of their actions when using technology, and the likelihood that information will remain confidential will become much greater.

References:

1. Cisco Systems. (n.d.). *What is cybersecurity*. Cisco. Retrieved from <https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html#jump-anchor-2>
2. Gigatrans. (n.d.). *How not to get hooked: Everything you need to know about phishing*. Retrieved from <https://gigatrans.ua/ua/news/kak-ne-popast-na-kryuchok-ili-vse-cto-nuzhno-znat-o-fishinge>
3. Diia.Osvita. (n.d.). *Cybersecurity*. Retrieved from <https://it-osvita.diia.gov.ua/task/item/b0cab3dc-3797-40bc-8591-a7e3fe42c3d7>
4. Neoversity. (n.d.). *Employment prospects in cybersecurity: Employers' perspective*. Retrieved from <https://neoversity.com.ua/blog/perspektivi-pracevlashtuvannya-u-sferi-kiberbezpeki-poglyad-robotodavciv>

УДК 004.056.53

Аджимян К.О.

*здобувач фахової передвищої освіти,
ВСП "ХКТФК НТУ "ХПІ"
Науковий керівник*

Кононова Г.О.

*викладач вищої категорії, голова циклової комісії комп'ютерних та
інформаційних дисциплін ВСП "ХКТФК НТУ "ХПІ"*

БЕЗПЕКА ПІД'ЄДНАННЯ ДО КОРПОРАТИВНОЇ МЕРЕЖІ

Сьогочасна корпоративна мережа – каверзна система з хмарними сервісами, колосальна кількість елементів. Коли вона більше не має визначних меж, новий елемент в мережі перетворюється в потенційний кіберінцидент. І у відповідь на загрози інформаційному середовищу у вигляді фішингових атак, Distributed Denial of Service атак, заражених USB – накопичувачів, зіставляється принцип "нульової довіри" – ніхто не довіряє нікому, поки не доведе протилежне. Цей принцип передбачає постійну перевірку кожного запиту незалежно від його походження – чи то внутрішня мережа, чи віддалене під'єднання. Проте, навіщо так детерміновано? Відповідь криється вже у вищевказаному – складності сучасних мереж, де існує грандіозна необхідність кіберзахисту.

Одна з суттєвих проблем – відсутність чіткого розуміння власної інфраструктури. Організації часто не знають точної кількості пристроїв, що під'єднуються до мережі. Без повної інвентаризації неможливо контролювати,

котрі елементи є вразливими, котрі давно не отримували оновлень чи патчів, а котрі мають доступ до критичних даних, не маючи на це підстав.

Не менша загроза – надмірні привілеї користувачів. У багатьох компаніях досі практикується надання широких прав за замовчуванням. У такій ситуації компрометація, тобто втрата конференційної інформації, одного акаунта відкриває шлях до всієї мережі. Зловмисник, отримавши контроль над одним користувачем, може безперешкодно пересуватися системою, збираючи потрібні дані. Це особливо небезпечно, коли частина мережі розташована в хмарних середовищах, а частина – на локальних серверах, що ускладнює контроль за нею. У таких ситуаціях додатковим чинником вразливості стає і відсутність сегментації, тобто розподілення мережевої інфраструктури на ізольовані сегменти, котрі контролюються окремо для запобігання поширення загроз усередині самої системи.

Проблема пов'язана й з людським фактором. Переважна більшість атак починається з помилок працівників – кліка по фішинговому листу, підключення невідомого USB – накопичувача чи використання одного й того самого пароля для кількох систем. Без структурованої архітектури кібербезпеки технології, такі як Security Information and Event Management (система управління інформацією й подіями безпеки), Multi – Factor Authentication (метод підтвердження користувача за допомогою двох або більше факторів) і мережеві фільтри, залишаються радше інструментами, ніж гарантією захисту.

Саме тому в сучасних корпоративних мережах особливу увагу приділяють не лише технічним засобам, а й комплексним стратегіям захисту, які інтегрують людський фактор для побудови ефективної системи кіберзахисту. Її реалізація включає такі складові:

- сегментацію мережі – поділ інфраструктури на ізольовані сегменти, щоб у разі інциденту загроза не поширювалась на всю систему;
- логи безпеки – автоматично створювані записи про будь – які дії, зміни у цифровій інфраструктурі, що дозволяють відстежувати діяльність користувачів, виявляти аномалії та розслідувати інциденти;
- регулярну перевірку на ознаки компрометації – моніторинг і аналіз поведінки користувачів та пристроїв для своєчасного виявлення порушень безпеки;
- інвентаризація активів – повний облік всіх пристроїв і користувачів, що підключаються до мережі, для точного визначення вразливих елементів;
- контроль доступу за принципом найменших привілеїв – обмеження прав користувачів і пристроїв до мінімально необхідних для виконання їхніх завдань.

Досвід останніх років підтверджує актуальність цієї парадигми. За даними Cyber Security Breaches Survey 2025, майже 93% британських організацій, що зазнали інцидентів, повідомили про фішингові атаки як найпоширенішу загрозу. А в середньому один бізнес стикається з кількома десятками кіберінцидентів на рік. Це означає, що питання безпеки під'єднання до корпоративної мережі вже давно перестало бути другорядним.

Отже, безпека під'єднання до комп'ютерної мережі криється у формуванні системного підходу до кібербезпеки, де кожен елемент

інфраструктури підлягає постійному контролю. Лише така послідовність дій дозволяє зменшити ризики кібератак і забезпечити надійну роботу організації в умовах постійно мінливо – динамічного інформаційного середовища.

Список використаних джерел:

1. Avolute Technology 'Захист корпоративних мереж: чи готова ваша компанія до сучасних загроз'. <https://avolutech.com/blog>
2. Avolute Technology 'Сегментація мережі. Як побудувати стійку мережеву інфраструктуру'. <https://avolutech.com/blog>
3. Microsoft 'What is: Multifactor Authentication'. <https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661>
4. Datami 'Що таке MFA – багатофакторна аутентифікація'. <https://datami.ee/ua/blog/shho-take-mfa-bagatofaktorna-autentifikatsiya/>
5. Microsoft 'What Is SIEM'. <https://www.microsoft.com/en-us/security/business/security-101/what-is-siem>
6. Avolute Technology 'Логи безпеки як основа інформаційної стійкості організації'. <https://avolutech.com/blog>
7. Cyber Security Breaches Survey 2025. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-technical-report>

УДК 004.056.53

Алькова А.М.

здобувач вищої освіти,

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Наукові керівники

Стьопочкіна І.В.

к.т.н., доцент, доцент кафедри інформаційної безпеки

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Лиманюк О.С.

с.н.с., Український науково-дослідний інститут спеціальної техніки та судових експертиз

ЦИФРОВА ФОРЕНЗИКА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У СЕРЕДОВИЩІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Актуальність. У сучасному світі критична інфраструктура, як-от енергетичні мережі, транспортні системи чи промислові комплекси, дедалі більше залежить від цифрових технологій, що робить її вразливою до соціальної інженерії – атак, які експлуатують людський фактор для

проникнення в захищені системи. Цифрова форензика, що займається збором і аналізом цифрових доказів, стає ключовим інструментом для виявлення таких інцидентів, адже за даними звітів, до 70-80% кібератак на критичну інфраструктуру пов'язані саме з цією загрозою. Особливо в середовищі оперативних технологій (OT) та систем керування (ICS/SCADA) традиційні методи часто неефективні через обмеженість форензичних даних, що підвищує ризики не виявлення атак. Ця робота пропонує методику оцінки ризиків пропуску інцидентів соціальної інженерії шляхом аналізу форензичних даних, інтегруючи підходи цифрової форензики з ризик-менеджментом, щоб допомогти організаціям ідентифікувати вразливості та посилити безпеку критичних об'єктів.

Соціальна інженерія належить до категорії атак, які здатні обійти апаратні чи програмні засоби захисту, що традиційно застосовуються для запобігання кіберзагрозам. Її складність полягає саме у тому, що технічні механізми безпеки малоефективні, якщо основною ціллю зловмисника є користувач, який взаємодіє з системою [1]. У типовій атаці соціальної інженерії кіберзлочинець встановлює контакт із потенційною жертвою, представляючись співробітником довіреної організації.

Попри те, що у ЗМІ найчастіше висвітлюють кіберзлочини, пов'язані з технічними вразливостями великих технологічних систем або складними державними кіберзагрозами, насправді, як виявляється, більшість інцидентів у кіберпросторі експлуатують людський фактор – «найслабше місце в ланцюзі кіберзагроз». Існує думка про те, що SCADA-системи складно атакувати через їхню ізольованість. Але за даними останніх досліджень, як зазначається в [2], майже 60% організацій, що використовують SCADA/ICS, протягом останнього року зазнали порушень безпеки.

Постановка задачі. Для ефективного розслідування інцидентів, спричинених соціальною інженерією, та оцінки їхнього впливу на критичну інфраструктуру необхідно не лише ідентифікувати ознаки атак, а й систематизувати форензичні дані, які фіксуються на пристроях SCADA-систем. Для цього необхідно запропонувати методики, які дадуть уявлення про дані та інформаційні об'єкти, які можуть бути важливими для цього.

Результати. У рамках цього дослідження, використовуючи дані MITRE ATT&CK [3], було розроблено чекліст сценаріїв атак соціальної інженерії у вигляді таблиці. Вона детально описує сценарії атак (наприклад, фішинг, pretexting), їх ознаки, відповідні форензичні дані та пристрої фіксації (як Email Server чи HMI), а також оцінку впливу на критичну інфраструктуру. Це дозволяє адміністраторам швидко ідентифікувати підозрілі дії, перевіряти релевантні журнали (наприклад, email-транзакції чи логи HMI) і оцінювати потенційні наслідки, що сприяє оперативному реагуванню та зниженню ризиків не виявлення інцидентів. Було проведено порівняння активів, що представлено на рис. 1.

На основі чеклістів і матриці активів, що систематизують сценарії атак соціальної інженерії та форензичні дані в SCADA-системах, розроблено методику оцінки ризиків не виявлення інцидентів, спричинених соціальною

інженерією, дані до якої подано в [4]. Методика оцінює ймовірність не виявлення атак ($Pnd = 1 - \text{Detection Probability, DP}$) як ключовий компонент вразливості (Vulnerability) у FAIR-моделі, де сам ризик = LEF (Частота подій утрати) $\times$ LM (Величина втрат), а $LEF = TEF$ (Частота загроз) $\times$ VF (Фактор вразливості). VF залежить від співвідношення Threat Capability (TC, здатність зловмисника) і Control Strength (CS, сила захисних заходів). Pnd відображає слабкість системи у виявленні атак, знижуючи CS: вища Pnd (низька DP) вказує на слабші контролю, що підвищує VF і, відповідно, загальний ризик.



Рис.1. Важливість активів об'єкта критичної інфраструктури з точки зору збору артефактів соціальної інженерії

Було обрано 6 сценаріїв: фішинг, spear-phishing/whaling, baiting, water-holing, pretexting, reverse social engineering (~70% атак на SCADA-пристрої: PLC, HMI, IED). Заздалегідь підготовлено пул із 25 питань, що перевіряють можливість системи виявити такі атаки (логування email, моніторинг браузерів, аудит USB). Відповіді оцінюються за шкалою 1–5 (1 = відсутнє, 5 = відмінне). Також для розрахунків побудовано матрицю ваг (W): ваги (0–1) відображають важливість питань для сценаріїв і нормалізовані.

Алгоритм реалізації:

1. Збір даних: Адміністратор відповідає на 25 питань, оцінюючи систему ($Score(Q_i)$, 1–5).
2. Розрахунок DP: Нормалізована оцінка ($Norm\_score_i = Score(Q_i)/5$) множиться на вагу ($W_{i,s}$) для кожного сценарію, сумується для отримання Detection Probability (DP).
3. Оцінка Pnd: Ймовірність не виявлення ($Pnd = 1 - DP$). Якщо $Pnd > 0.5$, ризик вважається високим.

Висновки. Запропонована методика допомагає оцінити вразливості SCADA-систем і знизити ризик атак соціальної інженерії. Результати можуть бути використані для систематизації даних на об'єктах критичної інфраструктури та належної підготовки інформаційних активів та моніторингових систем для фіксації причин кіберінцидентів.

Список використаних джерел:

1. І. Стьопчкіна, К. Ільїн. Профілювання користувачів для підвищення стійкості персоналу об'єктів критичної інфраструктури до кібератак, які використовують людський фактор. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 2024, с. 159–168. doi: <https://doi.org/10.32782/IT/2024-3-17>
2. ICS/SCADA social engineering attacks. [Електронний ресурс]. URL: <https://www.infosecinstitute.com/resources/scada-ics-security/ics-scada-social-engineering-attacks/>
3. Phishing. [Електронний ресурс]. URL: <https://attack.mitre.org/techniques/T1566/>
4. Social engineering detection. [Електронний ресурс]. URL: <https://github.com/alkovaalina/Social-engineering-detection>

УДК 004.056.53

Андрущенко С.А.

здобувачка вищої освіти,

Державний торговельно-економічний університет

Геселева Н.В.

к.т.н., доцент, доцент кафедри цифрової економіки та системного аналізу

Державний торговельно-економічний університет

МЕТОДИ АНОНІМІЗАЦІЇ ТА ПСЕВДОНІМІЗАЦІЇ У BIG DATA ДЛЯ ЗАХИСТУ ПРИВАТНОСТІ

У сучасному світі обсяги даних постійно зростають, а технології Big Data дозволяють збирати, зберігати та аналізувати інформацію про мільйони користувачів. Такі дані охоплюють фінансову, медичну, соціальну та поведінкову інформацію, що створює серйозні ризики для конфіденційності.

Забезпечення захисту даних є критичною задачею, оскільки порушення приватності може призводити до витоків особистої інформації, шахрайства та порушення законодавства. Сучасні методи анонімізації та псевдонімізації дозволяють захищати дані у системах Big Data, зберігаючи при цьому їх аналітичну цінність.

Анонімізація даних, відома також під назвою деідентифікація, передбачає повне видалення або приховування персональних ідентифікаторів з наборів даних, завдяки чому стає неможливим встановити особу, якій належать дані.

Для забезпечення захисту конфіденційності даних у великих наборах інформації використовуються різні математично-статистичні підходи, які складають основу ключових методів анонімізації у Big Data: k-anonymity, l-diversity та t-closeness. Перед застосуванням цих методів важливо класифікувати змінні у наборі даних, оскільки від цього залежить вибір підходу та рівень захисту. У даних моделях розрізняють три типи змінних:

1. *Ідентифікатори (ключові атрибути)* – прямі ідентифікатори, такі як імена, номери, адреси електронної пошти тощо. Ці змінні зазвичай не слід збирати або їх необхідно видаляти, якщо вони не критично потрібні для дослідження.

2. *Квазіідентифікатори* – непрямі атрибути, які можуть призвести до ідентифікації особи в поєднанні з іншими змінними або зовнішньою інформацією. Це можуть бути вік, стать, місце проживання, фізичні характеристики тощо.

3. *Чутливі атрибути* – змінні, що становлять основний об'єкт дослідження і потребують захисту. Їх не можна змінювати, оскільки вони є ключовими для результатів аналізу.

Правильна класифікація змінних є необхідною для ефективного застосування методів k-anonymity, l-diversity та t-closeness.

K-anonymity забезпечує, щоб кожен запис у наборі даних не відрізнявся від щонайменше k інших записів за вибраними квазіідентифікаторами. Усі прямі ідентифікатори, які не є критично необхідними, видаляються. Метод зазвичай реалізується через узагальнення або перестановку даних, зберігаючи статистичну цінність набору.

L-diversity доповнює k-anonymity, забезпечуючи достатню різноманітність чутливих атрибутів у кожній групі даних. Наприклад, якщо у групі є кілька осіб із однаковими демографічними характеристиками, l-diversity гарантує, що їхні чутливі атрибути різняться. Це знижує ризик того, що сторонній користувач зможе вивести конкретну інформацію про когось із групи.

T-closeness контролює відхилення розподілу чутливих атрибутів у групі від загального розподілу у наборі даних. Такий підхід ускладнює ідентифікацію конкретних значень навіть у групах, які статистично схожі, і підвищує рівень захисту приватності даних.

Крім методів анонімізації, важливою складовою захисту персональних даних у системах Big Data є псевдонімізація. Цей підхід полягає у заміні прямих ідентифікаторів унікальними кодами або псевдонімами, що дозволяє обробляти інформацію без розкриття особистості користувачів. Основна перевага псевдонімізації полягає в тому, що при наявності контрольованого ключа первинні дані можуть бути відновлені, що робить її цінною для довготривалих досліджень та перевірки аналітичних результатів. Структура процесу псевдонімізації включає кілька основних етапів:

1. *Заміну персональних даних* – такі атрибути, як імена, адреси електронної пошти, ідентифікаційні номери та інші прямі ідентифікатори, перетворюються на псевдоніми. Вони можуть бути представлені у вигляді

алфавітно-цифрових кодів або інших умовних позначень, які унеможливають розпізнавання особи.

2. *Роздільне зберігання даних* – оригінальні та псевдонімізовані набори даних зберігаються окремо, часто в різних базах або системах зберігання, щоб запобігти випадковому чи несанкціонованому поєднанню.

3. *Контрольована повторна ідентифікація* – у разі потреби для законних цілей використовується захищений ключ, що дозволяє відновити відповідність між псевдонімами та початковими даними. Доступ до ключа суворо регламентується для запобігання неправильного використання.

Основна мета псевдонімізації полягає у зменшенні ризику розкриття персональних даних і підвищенні рівня приватності, гарантуючи, що без спеціальних заходів інформація не може бути пов'язана з конкретною особою.

У порівнянні обох підходів до захисту приватності анонімізація забезпечує повне приховання особистості користувачів, проте може знижувати точність або деталізацію даних для аналітичних досліджень, а псевдонімізація зберігає можливість відновлення первинних даних за допомогою контрольованого ключа, що дозволяє підтримувати аналітичну цінність наборів даних, але потребує надійного управління ключами для запобігання несанкціонованому доступу. Поєднання цих методів дозволяє ефективно балансувати між конфіденційністю та точністю інформації.

Описані методи широко використовуються у різних сферах. У медицині вони дозволяють захищати дані пацієнтів при проведенні наукових досліджень. У фінансовому секторі застосовуються для безпечного аналізу транзакцій та поведінки користувачів. Соціальні мережі використовують ці підходи для обробки демографічної та поведінкової інформації без ризику розкриття особистості користувачів.

Отже, застосування методів анонімізації та псевдонімізації у системах Big Data забезпечує захист приватності користувачів, мінімізуючи ризик витоку персональної інформації. Поєднання різних методів дозволяє зберігати аналітичну цінність даних і підвищувати ефективність обробки інформації у наукових, фінансових та соціальних дослідженнях. Таким чином, впровадження цих технологій є важливим кроком у забезпеченні безпеки та конфіденційності інформації у сучасному цифровому середовищі.

Список використаних джерел:

1. Анонімізація та псевдонімізація даних – Ishchuk Pharmacovigilance Academy. *Ishchuk Pharmacovigilance Academy – Ishchuk Pharmacovigilance Academy*. URL: https://ishchuk.academy/data_anonym/ (дата звернення: 19.09.2025).

2. Що таке анонімізація – Терміни та визначення в галузі кібербезпеки. *VPN Unlimited – Fast & Secure VPN service*. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/anonymization?srsId=AfmBOop_Gof0oghUzYSslvhWz47MbrkVMHC6AmZ5oRxt6C0JeCU57MC5 (дата звернення: 19.09.2025).

3. Що таке псевдонімізація – Термінологія та визначення в кібербезпеці. *VPN Unlimited – Fast & Secure VPN service*. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/pseudonymization?srsId=AfmBOop2ic1d_C61SkBBi5bqVa_5JNjdZwzNy3Tt4Davz3Rzip3CTKrc (дата звернення: 19.09.2025).
4. Purpose and Means. Leadership explainer: k-anonymity, l-diversity and t-closeness | Purpose and Means. *Purpose and Means*. URL: <https://www.purposeandmeans.io/leadership-explainer-k-anonymity-l-diversity-and-t-closeness> (дата звернення: 19.09.2025).
5. Richman A. The L Diversity Data Anonymization Model: Extending K Anonymity. *Making Data AI-Ready* | K2view. URL: <https://www.k2view.com/blog/l-diversity/> (дата звернення: 19.09.2025).
6. Trotino G. What is K Anonymity and Why Data Pros Care. *Making Data AI-Ready* | K2view. URL: <https://www.k2view.com/blog/what-is-k-anonymity> (дата звернення: 19.09.2025).
7. Utrecht University. K-anonymity, l-diversity and t-closeness // Data Privacy Handbook. URL: <https://utrechtuniversity.github.io/dataprivacyhandbook/k-l-t-anonymity.html> (дата звернення: 19.09.2025).

УДК 004.838

Антощук С.А.

курсант 3-го курсу навчально-наукового інституту №4
Харківського національного університету внутрішніх справ
<https://orcid.org/0009-0004-1074-8378>

Стародубцев І.В.

курсант 3-го курсу навчально-наукового інституту №4
Харківського національного університету внутрішніх справ

Лучик В.Є.

д. е. н., професор кафедри протидії кіберзлочинності ННІН №4
Харківський національний університет внутрішніх справ
orcid.org/0000-0001-6007-910X

ПОРІВНЯННЯ МІЖНАРОДНИХ СТАНДАРТІВ ISO/IEC 27001 ТА NIST У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В умовах глобальної цифровізації та зростання залежності суспільства від інформаційних технологій питання забезпечення інформаційної безпеки набуває особливого значення. Кіберзагрози стають дедалі складнішими, а їх масштаби можуть мати критичні наслідки як для окремих організацій, так і для держав у цілому. У цьому контексті впровадження ефективних систем

управління інформаційною безпекою є ключовим завданням сучасних підприємств та урядових структур.

Серед найбільш поширених міжнародних підходів до організації системи інформаційної безпеки виділяються стандарт ISO/IEC 27001, що регламентує вимоги до системи управління інформаційною безпекою (СУІБ), та рекомендації Національного інституту стандартів і технологій США (NIST), які формують комплексний підхід до управління ризиками та захисту інформаційних систем. Обидві моделі мають спільну мету – забезпечення конфіденційності, цілісності та доступності даних, проте відрізняються методологією, структурою та сферою застосування.

ISO/IEC 27001 – це міжнародний стандарт системи менеджменту інформаційної безпеки, який допомагає організаціям захищати свої дані, забезпечувати їхню конфіденційність, цілісність та доступність. Він підходить для будь-якої компанії, незалежно від розміру чи сфери діяльності, та базується на управлінні ризиками. Стандарт охоплює людей, процеси й технології, визначає вимоги до оцінки ризиків, дотримання законодавства та управління інформаційними потоками. Основні елементи включають захист від несанкціонованого доступу, управління інцидентами, безперервність бізнесу та проведення внутрішніх і зовнішніх аудитів. ISO/IEC 27001 може бути інтегрований з іншими системами менеджменту (наприклад, ISO 9001 чи ISO/IEC 20000-1), що дозволяє підвищити ефективність і оптимізувати ресурси [1].

NIST Cybersecurity Framework (CSF) – це набір стандартів, рекомендацій та практик, розроблений Національним інститутом стандартів і технологій США для управління кіберризиками. Він створений для організацій будь-якого розміру та галузі, допомагає оцінювати рівень захисту й вибудовувати ефективні стратегії кібербезпеки.

Фреймворк складається з п'яти основних функцій: Identify (визначати), Protect (захищати), Detect (виявляти), Respond (реагувати), Recover (відновлювати). Ці блоки охоплюють увесь життєвий цикл управління кіберзагрозами – від оцінки ризиків до відновлення після інцидентів.

NIST CSF є гнучким інструментом, який можна адаптувати під потреби конкретної організації. Він широко використовується у США та за кордоном, особливо в галузях критичної інфраструктури, та може інтегруватися з іншими системами менеджменту інформаційної безпеки, включаючи ISO/IEC 27001 [2].

ISO/IEC 27001 застосовується у будь-яких організаціях для побудови системи управління інформаційною безпекою. Його ключові вимоги: оцінка ризиків, політика безпеки, визначення ролей персоналу, контроль доступу, управління інцидентами, безперервність бізнесу та проведення аудитів. Стандарт є сертифікаційним і охоплює як технічні, так і організаційні заходи [3].

NIST Cybersecurity Framework (CSF) орієнтований на критичну інфраструктуру, державні й приватні компанії, які прагнуть підвищити кіберзахист. Він базується на п'яти функціях: Identify, Protect, Detect, Respond, Recover. NIST CSF не є сертифікаційним стандартом, а пропонує гнучкі рекомендації для оцінки й поступового вдосконалення безпеки [4].

У цілому, ISO/IEC 27001 формалізує вимоги до системи безпеки, тоді як NIST CSF надає практичну структуру для її розвитку.

Таблиця 1.

Порівняльний аналіз ISO/IEC 27001 та NIST CSF [1,3,4].

Критерій	ISO/IEC 27001	NIST Cybersecurity Framework (CSF)
Призначення	Створення системи менеджменту інформаційної безпеки (СМІБ) з можливістю сертифікації.	Добровільний набір рекомендацій для управління кіберризиками.
Сфера застосування	Будь-які організації незалежно від розміру та сфери діяльності.	Переважно критична інфраструктура, держсектор та приватні компанії, але придатний для будь-яких організацій.
Основні функції/вимоги	Політика безпеки, оцінка ризиків, управління доступом, інцидентами, безперервністю бізнесу, проведення аудитів.	5 функцій: Identify, Protect, Detect, Respond, Recover (повний життєвий цикл кіберзахисту).
Тип стандарту	Сертифікаційний міжнародний стандарт.	Несертифікаційний фреймворк (набір практик і рекомендацій).
Підхід	Орієнтований на управління ризиками та відповідність вимогам.	Орієнтований на практичну оцінку зрілості кібербезпеки та поступове вдосконалення.
Гнучкість	Чітко формалізовані вимоги, що потребують дотримання.	Гнучка структура, яку організація адаптує під свої потреби.
Міжнародне використання	Широко застосовується у світі, зокрема для сертифікації постачальників.	Найпоширеніший у США, але також використовується міжнародно як методичний інструмент.
Інтеграція	Легко інтегрується з ISO 9001, ISO/IEC 20000-1, ISO/IEC 22301.	Може поєднуватися з ISO/IEC 27001 та іншими стандартами, підсилюючи практичну частину.

Висновки. Проведене дослідження дає змогу стверджувати, що стандарти ISO/IEC 27001 та NIST CSF відіграють ключову роль у формуванні сучасної системи інформаційної безпеки. Обидва підходи мають спільну мету – забезпечення конфіденційності, цілісності та доступності інформації, однак відрізняються за структурою, методологією та можливостями впровадження. ISO/IEC 27001 є універсальним сертифікаційним стандартом, який встановлює чіткі вимоги до організацій будь-якого масштабу, тоді як NIST CSF виступає

гнучким інструментом, орієнтованим на управління кіберризиками та практичне підвищення рівня кіберзахисту.

Список використаних джерел

1. Про стандарт ISO/IEC 27001 – систем менеджмент. Систем Менеджмент – Сертифікація та Навчання.
URL: <https://sm-mt.com.ua/services/standart-iso-iec-27001/> (дата звернення: 21.09.2025).
2. IBM. What is the NIST cybersecurity framework?
URL: <https://www.ibm.com/think/topics/nist> (дата звернення: 21.09.2025).
3. ISO/IEC 27001:2022. ISO.
URL: <https://www.iso.org/ru/standard/27001> (дата звернення: 21.09.2025).
4. NIST CSF - стандарт, про який варто знати.
URL: <https://my-itspecialist.com/what-is-the-nist-csf-standardtrt> (дата звернення: 21.09.2025).

УДК 004.056.5+614.253.4+378.147

Бабчук І.С.

здобувачка вищої освіти,

Івано-Франківський національний технічний університет нафти і газу

Бабчук Л.Р.

викладачка фахового медичного коледжу

кафедри біологічної та медичної хімії ім. Г.О.Бабенка

Івано-Франківський національний медичний університет

ЗАГРОЗИ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩУ ХІМІЧНОЇ НАУКИ З БОКУ ЧАТУ GPT

Майбутнє сучасної освіти невід’ємно пов’язане з розвитком інформаційних технологій та комп’ютерів. Штучний інтелект – це загальне поняття у яке входить машинне навчання, а його частиною є глибоке навчання, що використовує математичні моделі штучних нейронних мереж, зокрема, трансформерів. Перспективи штучного інтелекту (ШІ) відкривають нові можливості у викладанні та навчанні у закладах освіти. Загалом, використання ШІ в наукових дослідженнях, таких як збір інформації чи аналіз даних, може значно пришвидшити процес появи нових наукових відкриттів.

ШІ концептуально здатен генерувати нові знання так само, як людина. Навіть більше, на відміну від людини, ШІ не обмежений упередженнями чи глибиною своїх знань. Навіть, якщо зараз розробники не можуть отримати нові знання від генеративних моделей через певні обмеження, то це лише питання часу, коли вони зможуть їх отримати, а це може статися у недалекому майбутньому.

На даний час одним з таких обмежень є якість даних, на яких навчається ШІ. Будь-яка модель залежить від якості даних. Якщо навчати генеративний ШІ на всіх доступних даних, то модель може видавати помилкові результати. Якщо ж навчання базується на ретельно відібраній інформації, то відповіді ШІ будуть точнішими. Від якості даних на яких навчається ШІ залежить величина загрози інформаційної безпеки.

Згідно з тлумаченням поняття загрози інформаційної безпеки, то це сукупність умов та факторів, що створюють небезпеку порушення інформаційної безпеки. Отже, вплив ШІ на сучасну хімічну освіту пов'язаний з деякими проблемами, одна з яких – це недостовірні інформація. Якщо описувати навчання сучасного студента чи студентки, то можна говорити про те, що студенти фахового медичного коледжу розпочали масово використовувати чат GPT в підготовці до занять з наук хімічного профілю.

В процесі перевірки рівня знань студентів було виявлено, що ШІ погано орієнтується в структурних формулах органічних сполук. Наприклад, майже всі студенти що використовували допомогу чату GPT писали структурні формули вуглеводів-моносахаридів, таких як глюкоза, фруктоза, рибоза чи дезоксирибоза, малюючи зв'язки між атомами Гідрогену замість відповідних зв'язків між атомами Карбону у карбоновому ланцюзі. Тобто штучний інтелект не розуміє, що органічна хімія - це хімія Карбону, в органічній хімії Карбон завжди 4-х валентний, а Гідроген у хімії завжди одновалентний і всі сполуки органічної хімії побудовані на основі саме карбонових ланцюгів.

При розв'язуванні задач на розчини в умові задачі у кожного студента була звичайна сіль, наприклад, натрію сульфат, купруму сульфат чи феруму нітрат. Студенти ж в розв'язку задачі вказували молярну масу не звичайної солі а відповідного кристалогідрату, як навчив чат GPT. Як наслідок, такі задачі ними були розв'язані з помилкою, відповідь була невірною і це зупинило їх на шляху до приготування розчинів заданої концентрації.

У студентів також виникали проблеми при написанні проєктів з хімії. Студенти отримали завдання написати проєкт про органічну чи неорганічну сполуку, яка застосовується в медицині як засіб для лікування людей. Не усі ті, хто використав найпростіший спосіб - звернутися до чату GPT змогли отримати максимум достовірної інформації. Першою причиною було те, що проєкт мав мати список використаних джерел. Чат GPT створював літературу, але в деяких випадках реально ні таких авторів ні таких підручників чи публікацій з такими назвами у пошуку Google знайдено не було. Наприклад, при написанні проєкту на тему «Використання винної кислоти як допоміжної речовини в медичних препаратах» студентка подала на перегляд літературні джерела жодне з яких не було достовірним.

Спостерігалась ситуація, коли штучний інтелект властивостями однієї речовини наділяє іншу речовину. Тобто, якщо є описане застосування однієї речовини, то штучний інтелект іншу речовину яка має схожу хімічну формулу, схожі хімічні властивості може наділяти такими ж способами використання, хоча насправді та речовина в таких напрямках не використовується, бо подібними властивостями не володіє.

Та ж сама винна кислота, яка широко використовується у фармацевтичній промисловості, бо входить до складу фармацевтичних препаратів як підкислювач або у складі шипучих гранул, порошків чи таблеток уже з точки зору штучного інтелекту володіє властивостями що захищають компоненти ліків від окислення та надає змогу продовжити їх термін зберігання. Крім того, на думку чату GPT, вона використовується як складова розчинів для ін'єкцій для стабілізації активних компонентів щоб медикаменти не розкладались чи не осідали в розчині. GPT вказує що це важливо для антибіотиків, гормонів та інших біоактивних сполук, а також він пише що в таблетках та капсулах ця кислота допомагає покращити розчинність активних інгредієнтів і забезпечити швидке та повне всмоктування їх людським організмом а суспензіях та емульсіях, перешкоджає осадженню активних інгредієнтів та стабілізує рідку фазу забезпеченням рівномірного розподілу компонентів. На думку III, винна кислота може покращувати біодоступність деяких лікарських засобів, що мають низьку розчинність у воді та запобігає розкладу активних компонентів таких як вітаміни та інші біологічно активні сполуки.

З допомогою чату GPT властивості винної кислоти в фармацевтичній промисловості було підсилено, зроблено більш яскравими, повнішими та більш багатогранними. Споживач отримав не повністю достовірну інформацію про властивості цієї сполуки як медичного препарату.

Небезпеку порушення інформаційної безпеки саме через отримання недостовірної інформації отримує споживач чату GPT при створенні ним відповідного запиту в чаті. На прикладі винної кислоти це пов'язано з тим, що чат GPT плутає застосування винної кислоти та її аналогів в харчовій чи переробній промисловості з її застосуванням у фармацевтичній промисловості та медицині. На прикладі структурних формул вуглеводів чат GPT плутає атоми Карбону з атомами Гідрогену, у випадку розчинів солей ШІ плутає безводні солі з кристалогідратами і надає споживачам недостовірну інформацію, порушуючи таким чином їх інформаційну безпеку.

Список використаних джерел:

1. Кислота винна // Фармацевтична енциклопедія. URL: <https://www.pharmencyclopedia.com.ua/article/3499/kislota-vinna>
2. Вплив штучного інтелекту: чому "Нобеля" з фізики та хімії дали психологам і математикам // Економічна правда. 2024. URL: <https://epravda.com.ua/publications/2024/10/17/720704/>
3. Р. С. Гуревич, Л. Л. Коношевський, О. Л. Коношевський, А. Л. Воевода, С. Ю. Люльчак. Інформаційні технології та інноваційні методики навчання в освіті дорослих // Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми. – 2024. – Вип. 72. – Вінниця, Україна. doi: 10.31652/2412-1142-2024-72-170-187
4. Загрози інформаційної безпеки // Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B8_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%

УДК 338.27:004.056.5

Бедринський В.П.

*здобувач ступеня доктора філософії,
Західноукраїнський національний університет*

Будник І.М.

*здобувач ступеня доктора філософії,
Західноукраїнський національний університет*

ІНВЕСТИЦІЇ В КІБЕРЗАХИСТ ЯК ОСНОВА ЕКОНОМІЧНОЇ КОНКУРЕНТОСПРОМОЖНОСТІ

У сучасному глобалізованому світі економічна конкурентоспроможність держави та бізнесу дедалі більше залежить від здатності ефективно функціонувати у цифровому середовищі. Цифровізація економічних процесів, поширення електронної комерції, розвиток фінансових технологій та використання великих даних створюють нові можливості для зростання, однак одночасно породжують масштабні загрози, які здатні підірвати стабільність ринків та зруйнувати довіру до інституцій. Кіберзлочинність, шпигунство, крадіжка інтелектуальної власності, атаки на критичну інфраструктуру й маніпуляція інформаційними потоками вже давно вийшли за межі технічної проблеми і стали чинником стратегічного значення для економіки. Саме тому інвестиції у кіберзахист постають не лише як витрати на безпеку, а як довгострокова інвестиція у конкурентоспроможність.

Історія розвитку цифрових технологій показує, що будь-яка інновація викликає хвилю нових ризиків. Поява банківських онлайн-сервісів відкрила шлях до масових шахрайських схем, цифровізація державних послуг створила умови для спроб втручання у бази даних громадян, а поширення промислових систем управління через інтернет виявилось слабким місцем для атак на енергетичні компанії та транспортну інфраструктуру. У цих умовах підприємства, які вчасно інвестують у захист даних, відновлення після інцидентів і створення системи цифрової стійкості, отримують не лише технологічну, але й економічну перевагу. Адже захищеність інформаційних систем прямо впливає на рівень довіри партнерів, клієнтів і інвесторів.

Сучасні міжнародні дослідження демонструють, що збитки від кібератак обчислюються сотнями мільярдів доларів щороку, а окремі інциденти можуть призвести до банкрутства компаній чи значних падінь фондових індексів [1]. При цьому мова йде не лише про прямі фінансові втрати, але й про репутаційні ризики, що у сучасному інформаційному суспільстві мають колосальне значення. Бренд, який одного разу втратив довіру споживача через витік персональних даних або неспроможність забезпечити безперебійність роботи

сервісу, може роками відновлювати свій імідж. Таким чином, інвестиції у кіберзахист стають елементом управління не тільки ризиками, але й вартістю компанії на ринку.

Особливої ваги ця проблема набуває на рівні національної економіки. Держава, що не вкладає у розвиток надійної системи кібербезпеки, стає вразливою до зовнішніх атак, здатних паралізувати фінансову систему, порушити роботу енергетики чи транспорту. У сучасних геополітичних умовах кіберпростір розглядається як ще один театр військових дій, де перемогу здобуває той, хто має кращу технологічну базу і більшу кількість підготовлених фахівців. Для економіки це означає, що від рівня кіберзахищеності залежить її стабільність, привабливість для інвесторів та здатність інтегруватися у глобальні ланцюги створення вартості [2]. Іншими словами, кіберзахист стає складовою економічної безпеки та чинником, який визначає місце країни у міжнародній конкуренції.

Водночас інвестиції у кіберзахист не обмежуються закупівлею програмного забезпечення чи технічних рішень. Це комплексний процес, що передбачає підготовку кадрів, розвиток наукових досліджень, впровадження стандартів управління інформаційною безпекою та формування культури відповідального ставлення до даних. Лише поєднання технологічних, організаційних і освітніх заходів здатне забезпечити реальну стійкість економіки до кіберзагроз. Іншими словами, кіберзахист слід розглядати як інвестицію у людський капітал, адже кваліфіковані спеціалісти й грамотні користувачі часто є кращим бар'єром, ніж будь-які технічні системи.

Для бізнесу інвестиції у кіберзахист відкривають можливості виходу на нові ринки. У сучасній глобальній економіці доступ до міжнародних ринків дедалі частіше залежить не лише від якості товарів чи послуг, а й від здатності компанії гарантувати безпечність цифрових процесів. Багато транснаціональних корпорацій висувають до своїх партнерів суворі вимоги у сфері інформаційної безпеки, адже будь-яка уразливість у ланцюгу постачання може стати точкою входу для кібератак. Це означає, що підприємство, яке не має сертифікованих систем захисту, ризикує втратити можливість укласти вигідні контракти та брати участь у глобальних проєктах. Навпаки, компанії, що інвестують у кіберзахист і підтверджують це міжнародними стандартами, отримують конкурентну перевагу та доступ до ширшого кола партнерів.

Вихід на нові ринки потребує довіри з боку клієнтів та інвесторів. Якщо йдеться про фінансові сервіси, електронну комерцію чи цифрові платформи, довіра майже повністю базується на здатності забезпечувати безпеку персональних і фінансових даних. Інвестиції у захищені інфраструктури, багаторівневу автентифікацію та системи моніторингу загроз стають ключем до створення позитивного іміджу, який є вирішальним чинником під час виходу на іноземні ринки. Адже сучасні споживачі дедалі обережніше ставляться до питань захисту інформації і віддають перевагу тим брендам, які відкрито декларують та доводять свою відповідальність у сфері безпеки [3].

Крім того, посилення кіберзахисту сприяє відповідності вимогам регуляторів різних країн. Європейський Союз, США та інші юрисдикції

запровадили суворі норми щодо обробки персональних даних, а їх порушення може призвести до значних штрафів і навіть заборони на діяльність. Таким чином, компанії, які заздалегідь інвестують у дотримання цих стандартів, отримують не лише правову захищеність, але й можливість безперешкодно розширювати географію своєї діяльності. Це особливо важливо для малого та середнього бізнесу, який прагне інтегруватися у міжнародні ланцюги постачання й співпрацювати з великими партнерами.

Інвестиції у кіберзахист також стимулюють внутрішню інноваційність компанії. Захищене цифрове середовище дозволяє сміливіше впроваджувати нові бізнес-моделі, запускати електронні сервіси та використовувати технології штучного інтелекту без страху, що вони стануть слабкою ланкою для зловмисників. Завдяки цьому підприємство не лише виходить на нові ринки, а й формує власну нішу, пропонуючи безпечні й надійні рішення, що відповідають очікуванням сучасних клієнтів. У підсумку саме інвестиції у кіберзахист стають тим фактором, який перетворює безпеку на інструмент зростання та глобальної конкурентоспроможності.

У довгостроковій перспективі інвестиції у кіберзахист слід розглядати як стратегічний актив, здатний формувати нові сектори економіки. Розвиток індустрії кібербезпеки, створення інноваційних рішень для захисту даних, формування ринку послуг з аудиту та управління кіберризиками стимулює появу нових робочих місць і підвищує технологічний рівень країни. Таким чином, кіберзахист є не лише витратною статтею, а й джерелом економічного зростання.

У підсумку можна стверджувати, що інвестиції у кіберзахист стають фундаментом економічної конкурентоспроможності у XXI столітті. Вони визначають рівень довіри до компаній і держав, впливають на їхню здатність протидіяти глобальним викликам, формують основу для сталого розвитку та відкривають нові перспективи на світовому ринку. В умовах зростання кіберзагроз і посилення цифрової залежності економік, лише ті гравці, які усвідомлюють стратегічне значення безпеки і розглядають її як інвестицію, а не як витрату, зможуть зберегти і примножити свою конкурентну перевагу.

Список використаних джерел:

1. МВФ оцінив втрати від кібератак на фінансовий сектор у \$12 млрд за останні 20 років. URL: <https://fintechinsider.com.ua/mvf-oczinyv-vtraty-vid-kiberatak-na-finansovyy-sektor-u-12-mlrd-za-ostanni-20-rokiv/>
2. Стендер С. В., Фротер О. С., Снітко Ю. М. Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії. *Академічні візії*. 2023. №26. С. 1-13. DOI: <http://dx.doi.org/10.5281/zenodo.10389831>
3. Вербівська Л. В. Розвиток інноваційних технологій та конкурентоспроможність підприємства: економічні аспекти безпеки. *Економіка та суспільство*. 2024. №64. DOI: <https://doi.org/10.32782/2524-0072/2024-64-7>

Борисова К.Є.

курсант 4-го курсу ННІ № 4

Харківського національного університету внутрішніх справ

Мойко О.О.

курсант 3-го курсу ННІ № 4

Харківського національного університету внутрішніх справ

Макаліш Б.Д.

курсант 2-го курсу ННІ № 4

Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ДРОНІВ ЯК ОБ'ЄКТА ТА СУБ'ЄКТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У ХХІ столітті безпілотні літальні апарати, або дрони, стали одним із найбільш динамічних напрямів розвитку технологій. Вони широко застосовуються у військовій, цивільній, та комерційній сферах, охоплюючи завдання від розвідки й моніторингу до логістики, сільського господарства та рятувальних операцій. Разом із розширенням масштабів використання дронів зростають і ризики, пов'язані з інформаційною безпекою. БПЛА можуть виступати як суб'єктом інформаційної безпеки, забезпечуючи збір, передачу та обробку даних, так і об'єктом інформаційних загроз, стаючи мішенню для кібератак і технічного втручання. Така подвійність ролі дронів формує потребу у комплексному аналізі їхнього місця в інформаційному середовищі.

Як суб'єкт інформаційної безпеки, дрони виконують функції передачі та захисту інформації у різних сферах діяльності. У пошуково-рятувальних операціях вони дозволяють швидко виявляти постраждалих у важкодоступних районах, передавати координати до центрів управління, забезпечувати візуальний контроль територій та комунікацію у режимі реального часу. Подібні можливості є надзвичайно важливими у випадках стихійних лих, техногенних катастроф чи збройних конфліктів, коли кожна хвилина має вирішальне значення. У сфері моніторингу критичної інфраструктури дрони також відіграють вагомую роль, забезпечуючи нагляд за електромережами, транспортними вузлами та промисловими об'єктами. Зібрана ними інформація дозволяє попереджати аварії, виявляти відхилення та швидко реагувати на потенційні загрози, що безпосередньо впливає на національну інформаційну безпеку. У військовому контексті роль дронів як суб'єкта інформаційної безпеки ще більш виражена: вони забезпечують розвідку, коригування артилерійського вогню та передачу даних про противника у реальному часі, стаючи ключовим елементом інформаційно-аналітичної підтримки операцій.

Разом із тим дрони залишаються надзвичайно вразливими до інформаційних атак і стають об'єктом кіберзагроз. Однією з найпоширеніших проблем є перехоплення управління. Використовуючи вразливості у протоколах зв'язку, зловмисники здатні заволодіти контролем над дроном і використати його у власних цілях – від викрадення до застосування як зброї. Не менш

небезпечним є викрадення даних, адже дрони збирають великі обсяги фото- і відеоматеріалів, телеметрії та інших відомостей, які можуть містити конфіденційну інформацію. Несанкціонований доступ до таких даних створює ризики для державних структур і приватних компаній. Досить поширеною загрозою є глушіння сигналів, коли зловмисники блокують канали зв'язку між оператором і дроном. Це призводить до втрати керування, аварійних ситуацій і навіть до небезпеки для життя та здоров'я людей на землі. Через складність сучасних БПЛА та інтеграцію з мережами Інтернету вони можуть стати мішенню для кібератак, які здатні повністю паралізувати роботу апарата або використати його як інструмент для інших атак [1; 2].

Таким чином, ми бачимо, що дрони мають подвійний статус у сфері інформаційної безпеки. З одного боку, вони є суб'єктом – активним учасником, що забезпечує оперативний збір та передачу інформації, підтримку комунікацій і моніторинг. З іншого – вони є об'єктом, ціллю для кібератак, маніпуляцій і несанкціонованого доступу. Така подвійність вимагає особливого підходу до їхнього проектування, експлуатації та захисту. Для зниження ризиків необхідне впровадження багаторівневих заходів, які охоплюють технічні, організаційні та правові аспекти.

Технічний захист включає шифрування каналів зв'язку між оператором і дроном, використання систем автентифікації для підтвердження легітимності користувачів, а також алгоритмів виявлення аномалій у телеметричних даних, що дозволяють ідентифікувати несанкціоноване втручання. Організаційні заходи передбачають розробку стандартів безпечної експлуатації БПЛА, належну підготовку операторів із наголосом на інформаційній безпеці та постійний моніторинг польотів для своєчасного реагування на загрози. Правовий аспект не менш важливий: необхідне вдосконалення національного законодавства у сфері використання дронів, його гармонізація з міжнародними стандартами та введення відповідальності за кібератаки на БПЛА. Тільки поєднання цих трьох компонентів забезпечить надійний захист дронів як від інформаційних, так і від технічних загроз [2].

Міжнародний досвід свідчить, що провідні країни світу активно працюють над створенням систем протидії безпілотникам, які поєднують радіоелектронну боротьбу, штучний інтелект і кіберзахист. США, країни ЄС та Ізраїль впроваджують комплексні підходи до інтеграції БПЛА у стратегію національної інформаційної безпеки. Для України, яка перебуває у стані збройного протистояння, врахування цього досвіду має особливе значення. Дрони вже довели свою ефективність не лише як зброя, але й як елемент інформаційного забезпечення, тому їхній захист є критично важливим фактором.

У найближчому майбутньому очікується подальший розвиток технологій дронів. Зокрема, поява автономних апаратів, здатних до самостійного прийняття рішень, широке застосування штучного інтелекту для аналізу даних, розвиток систем колективного управління так званими «роями дронів». Усі ці тенденції відкривають нові можливості, але одночасно створюють додаткові виклики для інформаційної безпеки, адже збільшується складність захисту каналів зв'язку та

управління. Це означає, що увага до кіберзахисту дронів зростатиме як на національному, так і на міжнародному рівні.

Підсумовуючи, можна стверджувати, що дрони стали невід'ємною частиною сучасного інформаційного середовища. Вони одночасно є суб'єктами інформаційної безпеки, забезпечуючи збір та передачу даних, і об'єктами, оскільки залишаються вразливими до кібератак. Захист дронів від інформаційних загроз є необхідною умовою їх ефективного застосування у військовій, цивільній і гуманітарній сферах. Це вимагає системного підходу, що поєднує технічні рішення, організаційні заходи, правове регулювання та міжнародну співпрацю. Лише в такому разі дрони зможуть реалізувати свій потенціал, а не перетворитися на джерело нових ризиків. Водночас подвійна роль дронів – як об'єкта та суб'єкта інформаційної безпеки – підкреслює необхідність усвідомлення нових викликів та розробки інноваційних механізмів протидії загрозам. Саме від того, наскільки швидко суспільство та держава зможуть адаптуватися до цих змін, залежатиме ефективність використання безпілотних технологій у майбутньому.

Список використаних джерел:

1. Війна дронів: перехоплення контролю БПЛА. CyberSet. URL: <https://cyberset.com.ua/vulnerabilities/drone-war/> (дата звернення: 25.09.2025).
2. Борисов О.В., Артабаєв Ю.З., Сурма А.І. Кібербезпека безпілотних військових апаратів: методи захисту від перехоплення та дистанційного управління. Науковий журнал "Комп'ютерно-інтегровані технології: освіта, наука, виробництво", Луцьк, 2024. Випуск № 56. С. 117-125. URL: <https://cit.lntu.edu.ua/index.php/cit/article/view/610/713> (дата звернення: 25.09.2025).

*Ботик М.І.,
здобувач вищої освіти,
ННІ «Каразінський інститут міжнародних
відносин та туристичного бізнесу» ХНУ імені В.Н. Каразіна*

*Шкодін І.В.,
д.е.н., професор, професор кафедри
міжнародних економічних відносин та логістики
ННІ «Каразінський інститут міжнародних
відносин та туристичного бізнесу» ХНУ імені В.Н. Каразіна*

КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ ЧИННИК У ТРАНСФОРМАЦІЇ РІТЕЙЛ-МОДЕЛЕЙ ПІД ВПЛИВОМ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Стрімка цифровізація ритейлу та поширення електронної комерції відкривають нові можливості для підвищення ефективності бізнесу, проте одночасно генерують зростаючу кількість загроз у сфері кібербезпеки. Використання Big Data, AI, блокчейну, AR/VR та омніканальних платформ створює складні інформаційні системи, які стають об'єктом кібератак.

Міжнародні організації (World Economic Forum, ENISA) наголошують, що кіберризик є одним із головних бар'єрів для розвитку цифрової економіки. У наукових працях зарубіжних дослідників розглянуто питання управління інформаційною безпекою у контексті електронної комерції. В Україні проблематику досліджують Л. Федулова, С. Колодяжна, а також Національний інститут стратегічних досліджень, акцентуючи увагу на необхідності формування комплексної політики кіберзахисту бізнесу. Проте практичні аспекти кіберзагроз для ритейл-моделей потребують подальшої розробки.

За даними IBM Security, середня вартість витоку даних у сфері ритейлу перевищила 4,8 млн дол. США, а кількість атак на e-commerce зросла на 24 % у 2024 році порівнянні з попереднім [1].

Аналіз ключових ризиків електронної комерції дав можливість виділити наступні:

- кібератаки (фішинг, DDoS). Фішингові атаки залишаються наймасовішим інструментом зловмисників. За даними Verizon Data Breach Investigations Report 2024, майже 36 % зламаних акаунтів у сфері ритейлу стали наслідком фітингу [3]. DDoS-атаки у 2023-2024 рр. особливо часто використовувалися проти маркетплейсів і великих мережеских ритейлерів. Наприклад, Alibaba Group у 2023 році зафіксувала одну з найбільших у світі DDoS-атак, яка тимчасово ускладнила доступ до платформи Tmall;

- витік персональних даних. Електронна комерція акумулює значні обсяги персональної інформації про споживачів (дані карток, адреси, історії покупок). Порушення конфіденційності підпадає під регулювання, зокрема GDPR у ЄС та CCPA у Каліфорнії (США). У Target (США) було викрадено дані понад 40 млн банківських карток клієнтів. В результаті цієї атаки компанія

виплатила понад 200 млн дол. компенсацій і відчутно втратила в довірі клієнтів [2];

- шахрайство в онлайн-платежах. За даними Juniper Research, глобальні збитки від шахрайства в онлайн-платежах перевищили 48 млрд дол. США, з прогнозом зростання до 91 млрд дол. у 2028 р. Основними схемами є використання викрадених банківських карток, підробка транзакцій через скомпрометовані акаунти, бот-атаки на системи лояльності. Наприклад, eBay у 2022 році зафіксував масові спроби використання ботів для отримання бонусів у програмі знижок;

- порушення роботи ланцюгів постачання через цифрові загрози. Сучасний ритейл інтегрує IoT-рішення, ERP-системи та цифрові двійники для управління запасами. Це створює нові «входи» для атак. Згідно з World Economic Forum Global Risks Report 2024, 45 % компаній у секторі ритейлу зазначили перебої у ланцюгах постачання через кіберінциденти. Наприклад, атака на Maersk у 2017 р. паралізувала логістику на кілька тижнів та завдала збитків у 300 млн дол. Наслідки відчули ритейлери в усьому світі [4];

- репутаційні ризики. В часи соціальних медіа будь-який інцидент з кібербезпекою швидко набуває розголосу, що посилює втрати. Наприклад, після атаки на British Airways у 2018 р. (витік даних 380 тис. клієнтів) компанія зазнала не лише штрафів у розмірі 183 млн фунтів, але й падіння показників продажів протягом кількох кварталів.

Таким чином, цифрова трансформація ритейл-моделей створює не лише нові бізнес-можливості, а й підвищує вразливість компаній до кіберзагроз. Успішна адаптація до умов електронної комерції потребує інтеграції стратегії кібербезпеки у бізнес-моделі, орієнтації на міжнародні стандарти (ISO/IEC 27001, GDPR) та розвиток внутрішньої культури захисту даних. Для України це питання має особливу актуальність у контексті інтеграції до європейського цифрового ринку. Якщо банківська інфраструктура і платіжні системи в Україні активно захищаються, то ритейл має пришвидшити впровадження комплексних заходів (контроль постачальників, MFA, SOC-сервіси). Для українських компаній важливі також локальна відповідність (НБУ, закони про захист персональних даних), участь у міжнародних програмах обміну індикаторами (TI), та інвестиції у хмарні сервіси з enterprise-security рівнем.

Список використаних джерел:

1. Cost of a Data Breach Report 2024. <https://www.ibm.com/reports/data-breach>
2. Romanosky, S. Examining the Costs and Causes of Cyber Incidents. Journal of Cybersecurity. 2019. Vol. 5, No. 1. P. 1–18. DOI:10.1093/cybsec/tyz004
3. Verizon. Data Breach Investigations Report 2024. Verizon Enterprise, 2024. 120 p. <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf>

4. World Economic Forum (WEF). *Global Risks Report 2024*. Geneva: World Economic Forum, 2024. 120 p.
<https://www.weforum.org/publications/global-risks-report-2024/>

УДК 004.8

Величко С. Ю.
здобувач вищої освіти
Державний торговельно-економічний університет
Геселева Н.В.
к.т.н., доцент, доцент кафедри цифрової економіки
та системного аналізу
Державний торговельно-економічний університет

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК

У сучасну цифрову епоху забезпечення стійкості інформаційних систем до кіберзагроз є одним із ключових завдань, що має важливе значення як для користувачів, так і для організацій, які обмінюються та використовують інформаційні ресурси. Нині спостерігається зростання кількості атак на дані, ресурси та критично важливу інфраструктуру, зокрема на фінансову сферу та персональну інформацію. В умовах постійного розвитку кіберзагроз впровадження сучасних технологій набуває вирішальної ролі. У цьому контексті застосування штучного інтелекту для виявлення та протидії кібератакам вважається одним із найперспективніших напрямів. Завдяки здатності аналізувати й обробляти значні масиви даних, а також виявляти та мінімізувати ризики, пов'язані з кіберзагрозами, штучний інтелект, що навчається самостійно, відкриває нові можливості для підвищення безпеки. [1]

Штучний інтелект – це поєднання теоретичних і практичних підходів у сфері інформаційних технологій, спрямованих на створення систем, здатних діяти розумно й автономно, подібно до процесу прийняття рішень людиною. Використовуючи ШІ, машина отримує можливість навчатися на основі досвіду, аналізуючи великі масиви даних і виявляючи закономірності в них. [2]

Переваги використання ШІ в кібербезпеці полягають у здатності аналізувати великі обсяги даних та мережевого трафіку в реальному часі, автоматично виявляти аномальні дії та підозрілі активності, що дозволяє швидше та ефективніше виявляти потенційні загрози, ніж це може зробити людина. Крім того, ШІ прогнозує майбутні атаки на основі історичних даних і поточних загроз, допомагаючи запобігати інцидентам до їхнього виникнення, та створює адаптивні системи безпеки, які в реальному часі реагують на змінні загрози, автоматично коригуючи правила й політики для надійнішого захисту мереж і даних.

Штучний інтелект також застосовується для розпізнавання образів і біометричної автентифікації, наприклад, розпізнавання осіб, відбитків пальців або сканування сітківки ока, що підвищує безпеку доступу до систем. Системи на основі ШІ допомагають виявляти фішингові листи, шахрайські схеми та підозрілі фінансові операції, а також автоматизують рутинні завдання у сфері кібербезпеки, звільняючи час аналітиків для більш складних та стратегічних завдань. [3]

Перспективи впровадження систем ШІ для кібербезпеки полягають у можливості аналізувати великі обсяги даних та виявляти патерни й аномалії за допомогою різноманітних інструментів:

1. Методи машинного навчання: Використання алгоритмів, таких як нейронні мережі, дерева рішень, алгоритми кластеризації та інші, для автоматичного аналізу великих обсягів даних і ідентифікації патернів у реальному часі.

2. Аналіз поведінки користувачів: Застосування ШІ для відстеження дій користувачів та виявлення аномалій або змін у звичних патернах, що можуть сигналізувати про потенційні кібератаки чи порушення безпеки.

3. Системи виявлення вторгнень (IDS): Використання інтелектуальних IDS для виявлення аномалій у мережевому трафіку чи системних даних, які можуть свідчити про загрози.

4. Аналіз журналів подій (SIEM): Застосування систем управління інформаційною безпекою та подій з вбудованими засобами аналізу для виявлення підозрілих або незвичних активностей у великих масивах журналів подій.

5. Технології Big Data: Використання рішень для обробки великих даних, що дозволяє збирати, зберігати та аналізувати величезні обсяги інформації у реальному часі для виявлення патернів і аномалій. [4]

Таким чином, використання штучного інтелекту для виявлення кібератак є однією з найважливіших тенденцій сучасної кібербезпеки. Алгоритми машинного навчання та глибоких нейронних мереж дозволяють ефективніше протидіяти новим видам загроз, забезпечують швидку реакцію та зменшують навантаження на фахівців. Проте розвиток ШІ не є універсальним вирішенням усіх проблем – він має поєднуватися з підвищенням рівня обізнаності користувачів і вдосконаленням нормативно-правової бази у сфері захисту інформації.

Список використаних джерел:

1. Зоря І. С., Марущак А. В. Застосування штучного інтелекту для виявлення та реагування на кіберзагрози / І. С. Зоря, А. В. Марущак. – Вінниця : Вінницький національний технічний університет, 2024. – 1 с. – URL: <https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf>

2. Савченко В. А., Шаповаленко О. Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці // Захист інформації. – 2020. – №3. – С.6 – URL: <https://journals.dut.edu.ua/index.php/dataprotect/article/view/2456/2356>

3. Cisco, мережна академія. Штучний інтелект та кібербезпека / Cisco, мережна академія. – 2023. – 31 серпня. – URL: <https://www.education.ua/blog/48113/>

4. Іваненко П. В., Ковальчук С. М. Використання технологій штучного інтелекту у забезпеченні кібербезпеки // Університетські технології. – 2024. – Вип.12. – С.50 – URL: <http://uwtech.knuba.edu.ua/article/view/307217/298537>

УДК 311:004.056:658.5

Вінічук М.В.

*к.е.н., доцент, професор кафедри менеджменту та економічної безпеки
Львівський державний університет внутрішніх справ*

Лавриш Софія

*здобувач вищої освіти спеціальності 073 «Менеджмент»
Львівський державний університет внутрішніх справ*

СТАТИСТИЧНІ МЕТОДИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХОДІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ НА ПІДПРИЄМСТВА ІТ-СФЕРИ

У сучасних умовах цифровізації економіки та суспільства проблема забезпечення кібербезпеки набула стратегічного значення. Зростання кількості та складності кібератак та кіберзлочинів зумовлює потребу у впровадженні комплексних заходів протидії даному деструктивному явищу. Однак, не менш важливим є питання оцінки їхньої ефективності. Без кількісного вимірювання рівня результативності заходів кіберзахисту неможливо оптимізувати витрати на безпеку та забезпечити належний рівень стійкості інформаційних систем. Для цього застосовуються статистичні інструменти, що дають змогу аналізувати обсяги кіберзагроз, динаміку інцидентів, структуру збитків та ефективність реалізованих механізмів реагування.

Оцінка ефективності заходів кіберзахисту ґрунтується на системному підході та поєднанні кількісних і якісних показників [1; 2]. Традиційно в аналізі використовуються такі групи показників: (1) кількість кіберінцидентів (успішних та заблокованих атак); (2) час виявлення та реагування (MTTD – Mean Time to Detect, MTTR – Mean Time to Respond); (3) економічні втрати (прямі й непрямі збитки); (4) рівень доступності систем (uptime, SLA-виконання); (5) частка інцидентів, локалізованих без значних наслідків. Ці показники у поєднанні зі статистичними методами дозволяють отримати об'єктивні результати щодо визначення ефективності та резервів підвищення кіберзахисту.

У практиці міжнародних організацій і великих корпорацій статистичний аналіз використовується для оцінки трендів атак (наприклад, збільшення кількості фішингових кампаній у певні періоди року); пріоритизації ресурсів (встановлення, які саме заходи безпеки дають найбільший ефект відносно

витрат); порівняльного аналізу (benchmarking) між компаніями чи галузями; моделювання сценаріїв розвитку подій (stress-testing у сфері кіберзахисту). Тому можна стверджувати, що статистичні інструменти стають не лише засобом оцінки минулих результатів, а й інструментом стратегічного планування [3].

При цьому, достатньо ефективною та такою, що заслуговує на увагу є багатофакторна регресійна модель [4], залежною змінною в якій виступає рівень ефективності кібербезпеки (SEC_EFF) – інтегральний показник, розрахований як відношення кількості відвернених атак до загальної кількості спроб, скоригований на рівень економічних втрат (від 0 до 1). Зазначена регресійна модель має вигляд (рівняння 1):

$$SEC\_EFF_i = \beta_0 + \beta_1 INV_i + \beta_2 RESP_i + \beta_3 TRAIN_i + \beta_4 MON_i + \beta_5 INC_i + \varepsilon_i \quad (1)$$

де: SEC_EFF_i – рівень ефективності кібербезпеки; INV_i – обсяг інвестицій у кібербезпеку (у % від ІТ-бюджету); $RESP_i$ – середній час реагування на інцидент (MTTR, у год.); $TRAIN_i$ – кількість навчальних заходів з кібергігієни для персоналу на рік; MON_i – рівень автоматизації моніторингу (наприклад, % покриття системами SIEM/SOC); INC_i – кількість зареєстрованих інцидентів на 100 користувачів; ε_i – випадкова похибка. β_1 – показує, наскільки зростає ефективність кіберзахисту зі збільшенням інвестицій; β_2 – очікувано має негативний знак: чим довше реагування, тим нижча ефективність; β_3 – відображає внесок підготовки персоналу у зменшення кількості інцидентів; β_4 – характеризує значення автоматизованих систем моніторингу; β_5 – має від’ємний вплив, оскільки більша кількість інцидентів свідчить про слабшу захищеність.

Емпіричні дослідження щодо апробації зазначеної багатофакторної регресійної моделі здійснено на прикладі гіпотетичних даних 50 компаній ІТ-сектора, внаслідок чого отримано наступну модель (рівняння 2), яка дозволяє зробити певні висновки:

$$SEC\_EFF_i = 0,52 + 0,18 \cdot INV_i - 0,25 \cdot RESP_i + 0,12 \cdot TRAIN_i + 0,21 \cdot MON_i - 0,15 \cdot INC_i \quad (2)$$

$R^2 = 0,73$, що свідчить про високу пояснювальну здатність моделі.

На підставі отриманих результатів можна констатувати, що модель дозволяє порівнювати ІТ-компанії за рівнем кіберзахищеності та визначати, які фактори найбільше впливають на результат, а також можна здійснити прогнозування щодо зростання ефективності при збільшенні інвестицій чи зменшенні часу реагування. Деталізацію результативних показників проведених досліджень узагальнимо в табл. 1.

Таблиця 1

Результати оцінювання ефективності заходів протидії кіберзлочинності на підприємства ІТ-сфери

Змінна	Очікуваний знак	Оцінений коефіцієнт	t-статистика	p-значення
Константа (β_0)	–	0,52	4,12	0,000
INV	+	0,18	2,95	0,005
RESP	–	-0,25	-3,41	0,002
TRAIN	+	0,12	2,21	0,032
MON	+	0,21	3,68	0,001
INC	–	-0,15	-2,44	0,018

Таким чином, на підставі результатів встановлено, що інвестиції (INV) мають позитивний вплив на протидію кіберзлочинності на підприємства ІТ-сфери, а саме збільшення їх частки на 1% підвищує індекс ефективності на 0,18. Це свідчить про доцільність пріоритетного фінансування заходів кіберзахисту. При цьому, час реагування (RESP) має найбільший від'ємний вплив, оскільки виявлено, що кожна додаткова година збільшує ризик зниження ефективності на 0,25, що підтверджує важливість швидких дій SOC-команд. Навчання персоналу (TRAIN) істотно знижує ймовірність успішних атак, особливо фішингових. Однак, автоматизація моніторингу (MON) значно підвищує ефективність захисту (0,21), оскільки дозволяє оперативно ідентифікувати інциденти, а кількість інцидентів (INC) негативно впливає на результат, відображаючи реальну загрозу перевантаження систем безпеки. Тому, можна констатувати, що найбільший ефект забезпечують скорочення часу реагування та автоматизація моніторингу, а підвищення ефективності неможливе лише за рахунок інвестицій, адже ключову роль відіграє людський фактор (навчання). При цьому, варто зазначити, що модель може бути використана для прогнозування ефективності нових заходів і формування оптимального балансу витрат у сфері кіберзахисту, що є перспективами подальших досліджень.

Таким чином, зазначене доводить, що застосування статистичних інструментів у сфері кібербезпеки дає можливість об'єктивно оцінювати результативність заходів кіберзахисту, виявляти закономірності та тенденції у динаміці кіберзлочинності, оптимізувати витрати на безпеку завдяки кількісному аналізу ефективності різних заходів, спрогнозувати можливі ризики та підвищувати рівень готовності ІТ-компаній до кіберзагроз. Стає очевидним, що статистичні методи та інструменти стають ключовим елементом системи забезпечення кіберстійкості як на рівні окремого підприємства, так і на рівні держави. Подальші дослідження повинні бути спрямовані на розробку інтегральних індикаторів кіберзахищеності та створення адаптивних систем моніторингу, що базуються на статистично-математичних моделях.

Список використаних джерел:

1. Kopytko, M., Vinichuk, M. Statistical Methods for Diagnosing the Level

of Ukraine's Economic Security in the Context of Formulating Strategic Priorities of Public Administration Policy. *Public Administration and Law Review*. 2025. Issue 2(22). P. 47–58. URL: DOI: <https://doi.org/10.36690/2674-5216-2025-2-47-58>.

2. Копитко М.І., Миськів Г.В., Вінічук М.В. Аналіз стану та проблем використання економіко-математичних методів та моделей в дослідженні фінансових злочинів. *Вчені записки Університету «КРОК»*. 2022. № 2(66). С. 33–39. URL: DOI: 10.31732/2663-2209-2022-66-33-39.

3. Вінічук М.В. Застосування економіко-математичних методів і моделей в дослідженні впливу економічної злочинності на рівень життя населення в Україні. *Науковий вісник Львівського державного університету внутрішніх справ*. 2024. Вип. 2. С. 10–18. URL: DOI: <https://doi.org/10.32782/2311-844X/2024-2-2>.

4. Копитко М.І., Вінічук М.В. Проблеми статистичного оцінювання рівня корупції в Україні. *Актуальні питання економічних наук*. 2025. № 7. URL: DOI: <https://doi.org/10.5281/zenodo.14758425>.

УДК 004.056.53

Витковець І.О.

здобувач вищої освіти,

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

Науковий керівник

Стяглик Н.І.

завідувач кафедри інформаційних технологій

та математичного моделювання

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

РОЛЬ І ВАЖЛИВІСТЬ КІБЕРБЕЗПЕКИ

Кібербезпека сьогодні є невід’ємною складовою нашого життя, адже саме вона захищає користувачів від численних прихованих загроз у мережі. Усвідомлення потреби надійного захисту та вжиття необхідних заходів є вкрай важливими. Ця сфера покликана оберігати конфіденційність, захищати особисті дані й запобігати фінансовим втратам. Оскільки в Інтернеті діє багато шахраїв, наявність ефективного захисту стає запорукою безпеки кожного користувача.

Кібербезпека – це система заходів, спрямованих на захист комп’ютерних мереж, програм і даних від цифрових атак. Такі атаки зазвичай націлені на викрадення чи знищення конфіденційної інформації, блокування доступу до систем або вимагання коштів у користувачів. Постає питання: які існують основні типи кіберзагроз і яким чином сучасні засоби захисту здатні їм протидіяти?

У сучасному цифровому середовищі існує безліч зловмисних програм і практик, що становлять серйозну загрозу як для окремих користувачів, так і для організацій. Одним із найбільш поширених видів шахрайства є фішинг –

різновид кіберзлочинності, при якому зловмисники надсилають електронні листи, повідомлення чи навіть телефонні дзвінки, маскуючись під надійне джерело. Їхня мета – змусити людину розкрити конфіденційні дані, такі як імена користувачів, паролі, номери кредитних карток або інформацію з важливих документів. Окремим підтипом є фішинг пошукових систем, коли шахраї створюють підроблені веб-сайти, просувають їх у результатах пошуку й тим самим вводять користувачів в оману. За даними компанії *Wandera*, ще п'ять років тому щодня виявлялося близько 25 мільярдів спам-сторінок, однак завдяки розвитку сучасних засобів кіберзахисту їхня кількість поступово зменшується.

Не менш небезпечними є програми-вимагачі (ransomware) – різновид шкідливого програмного забезпечення, яке блокує доступ до файлів або цілої системи та вимагає викуп за відновлення працездатності. Проте навіть після сплати коштів гарантії відновлення даних не існує, а отже жертви часто зазнають подвійних втрат – фінансових і інформаційних.

Суттєву загрозу становлять і мережеві атаки типу DoS (Denial of Service) та DDoS (Distributed Denial of Service). Їхня суть полягає у перевантаженні серверів чи комп'ютерних систем великою кількістю запитів, що робить їх тимчасово недоступними для легальних користувачів. Якщо DoS-атака здійснюється з одного джерела, то DDoS є її масштабованою формою, яка використовує мережі заражених пристроїв (ботнетів). Окрім прямої шкоди, такі атаки часто застосовуються як тактика відволікання уваги від масштабніших злочинних дій, що можуть мати ще серйозніші наслідки.

Для протидії цим загрозам застосовуються сучасні технології кіберзахисту. Зокрема, хмарні рішення для захисту від DDoS дозволяють обробляти надмірну кількість шкідливих запитів, масштабувати ресурси на вимогу й забезпечувати безперервність роботи систем. Поєднання таких технічних засобів із політиками інформаційної безпеки та підвищенням обізнаності користувачів є ключем до ефективної боротьби з кіберзлочинністю.

За даними Державної служби спеціального зв'язку та захисту інформації у 2024 році кількість кібератак зросла майже на 70%, досягнувши 4315 випадків, порівняно із 2023 роком, коли було виявлено 2541 атак.

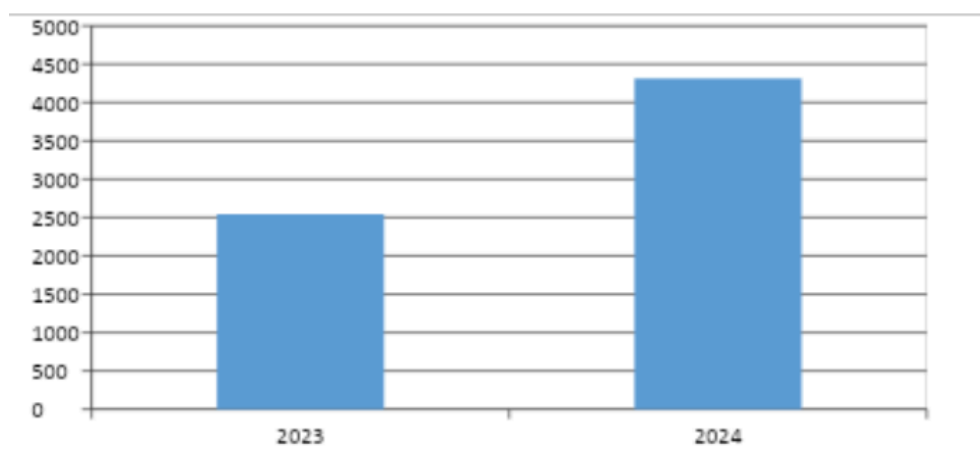


Рис. 1. Порівняння кількості кібератак в 2023 та 2024 роках

Серед ключових механізмів кібербезпеки особливе місце займає шифрування даних. Воно використовується під час передачі файлів чи повідомлень і полягає в перетворенні відкритої інформації на закодований набір символів, зрозумілий лише для того, хто володіє спеціальним ключем розшифрування. Завдяки цьому навіть у випадку перехоплення даних зломисники не зможуть отримати доступ до їхнього змісту.

Ще одним поширеним засобом захисту є VPN (Virtual Private Network) – технологія, що дозволяє приховати реальну IP-адресу користувача та шифрувати інтернет-з'єднання. Це унеможливорює визначення місця розташування людини та суттєво знижує ризик відстеження чи крадіжки даних у публічних мережах.

Важливу роль у забезпеченні інформаційної безпеки компаній сьогодні відіграють системи SIEM (Security Information and Event Management). Вони поєднують можливості управління інформацією та подіями безпеки, забезпечують централізований моніторинг, збір і аналіз журналів подій, вчасно сигналізують про потенційні загрози й дозволяють швидко реагувати на інциденти. Крім того, SIEM підтримують сценарії аварійного відновлення, що допомагає мінімізувати наслідки кібератак.

Не менш значущими залишаються і базові інструменти кіберзахисту – антивірусні програми та брандмауери. Антивірус виконує функцію виявлення, нейтралізації та видалення шкідливого програмного забезпечення. Брандмауер же можна вважати «цифровим фільтром»: він контролює вхідний і вихідний трафік, запобігає встановленню небезпечних з'єднань та обмежує несанкціонований доступ до системи.

Таким чином, ефективна кібербезпека ґрунтується на поєднанні передових технологій (шифрування, VPN, SIEM) із традиційними методами захисту. Лише комплексне використання цих інструментів дозволяє забезпечити належний рівень безпеки як для окремих користувачів, так і для організацій.

Попит на фахівців із кібербезпеки стрімко зростає. Це зумовлено зростанням кількості кібератак та потребою у захисті критичної інфраструктури.

Для успішної кар'єри важливими є знання міжнародних стандартів безпеки та постійний професійний розвиток. Перспективи галузі включають кар'єрне зростання до керівних посад, роботу в суміжних напрямках (DevSecOps, Cloud Security), міжнародне працевлаштування та навіть створення власних компаній. Спеціалізація у сфері кібербезпеки відкриває широкий вибір професій: від аналітика інформаційної безпеки й спеціаліста з криптографії до експерта з реагування на інциденти. Це не лише високооплачувана, а й суспільно корисна професія, адже вона забезпечує захист конфіденційних даних і боротьбу з кіберзлочинністю.

Отже, кібербезпека сьогодні є важливою як для окремих користувачів, так і для великих компаній, а усвідомлене використання цифрових технологій значно підвищує рівень захищеності.

Список використаних джерел:

1. CiscoSystems. URL:
<https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html#jump-anchor-2>
2. Gigatrans/ URL:
<https://gigatrans.ua/ua/news/kak-ne-popast-na-kryuchok-ili-vse-cho-nuzhno-znat-o-fishinge>
3. Дія.Освіта/ URL:
<https://it-osvita.diia.gov.ua/task/item/b0cab3dc-3797-40bc-8591-a7e3fe42c3d7>
4. Neoversity. URL:
<https://neoversity.com.ua/blog/perspektivi-pracevlashtuvannya-u-sferi-kiberbezpeki-poglyad-robotodavciv>

УДК 004.056.5:336.71

Гладій А.Л.

*здобувач фахової передвищої освіти,
ВСП «Хмельницький торговельно-економічний фаховий коледж Державного
торговельно-економічного університету»*

Науковий керівник

Нестерук Г.В.

*викладач циклової комісії Фінансів, обліку і оподаткування
ВСП «Хмельницький торговельно-економічний фаховий коледж
Державного торговельно-економічного університету»*

ЗАХИСТ БАНКІВСЬКИХ КАРТОК ВІД КІБЕРЗАГРОЗ

У сучасному світі фінансові технології стали невід'ємною частиною повсякденного життя людини. Банківські картки значно спростили доступ до коштів, забезпечили зручність у здійсненні платежів та відкрили нові можливості для розвитку електронної комерції. Проте разом із цими перевагами зростає й рівень кіберзагроз. Шахрайські схеми, вірусні програми, фішинг та інші методи кібератак створюють значні ризики як для пересічних користувачів, так і для фінансових установ.

Тема захисту банківських карток від кіберзагроз набула особливої актуальності в умовах цифровізації фінансового сектору. Питання безпеки вже не можна розглядати як другорядне: воно стало стратегічним напрямом розвитку банківських систем у світі. Використання банківських карток зростає з кожним роком. За даними міжнародних фінансових організацій, понад 70% безготівкових операцій у світі здійснюється за допомогою карткових рахунків. Це означає, що будь-які загрози їх безпеці можуть мати масштабні наслідки.

Для України питання кіберзахисту є дійсно важливим. Країна активно інтегрується у світовий фінансовий простір і переходить до цифрових

технологій. В умовах воєнного стану кібератаки з боку зовнішніх і внутрішніх зловмисників стали частиною гібридної війни. Таким чином, кібербезпека банківських карток — це не лише питання особистої безпеки громадян, а й елемент фінансової стабільності держави.

Актуальність теми підсилюється й тим, що методи злочинців постійно вдосконалюються. Якщо раніше шахраї діяли переважно шляхом фізичного викрадення даних картки, то сьогодні використовуються цілісні програмні комплекси для масових атак, включно з фішинговими схемами, шкідливими програмами та соціальною інженерією. Саме тому вивчення механізмів захисту та пошук нових рішень у сфері кібербезпеки є одним із головних завдань сучасного фінансового сектору.

Банківські картки є невід’ємним елементом сучасної фінансової системи, що забезпечує швидкий і зручний доступ до коштів. Разом із тим, розвиток електронних платежів супроводжується зростанням ризиків кіберзагроз, які можуть призвести до втрати коштів або конфіденційної інформації користувачів. Кіберзагроза — це будь-яке незаконне втручання у роботу фінансових систем або спроба отримати несанкціонований доступ до даних користувачів.

До основних видів кіберзагроз належать фішинг, програми-вимагачі (ransomware), трояни, криптомайнінг та шахрайство через соціальну інженерію. Фішинг полягає у використанні підроблених повідомлень, веб-сайтів або електронних листів для викрадення даних картки та облікових записів. Програми-вимагачі блокують доступ до файлів або систем, вимагаючи викуп, а трояни замасковані під легітимне програмне забезпечення, що збирає конфіденційні дані. Криптомайнінг використовує ресурси користувачів для видобутку криптовалюти, створюючи додаткове навантаження на системи, а соціальна інженерія експлуатує психологічні фактори, змушуючи людей добровільно передавати особисті дані.

Сучасні загрози характеризуються високим рівнем адаптивності: шахраї підлаштовуються під актуальні події та інтереси користувачів, пропонуючи «виграші», «подарунки» або «вигідні пропозиції». Це підкреслює важливість обережності та знання методів захисту.

Для зниження ризиків кіберзагроз банки застосовують багаторівневі стратегії захисту. Одним із ключових заходів є оцінка ризиків та тестування систем на проникнення. Регулярний аудит дозволяє виявити слабкі місця, перевірити права доступу та оцінити ефективність наявних заходів безпеки.

Не менш важливим є навчання користувачів і співробітників. Людський фактор залишається однією з головних слабких ланок, тому працівники банків проходять тренінги, які дозволяють ідентифікувати підозрілі операції та діяти у випадку кібератак.

Моніторинг подій і швидке реагування на інциденти дозволяють мінімізувати наслідки атак. Технології машинного навчання і штучного інтелекту допомагають контролювати транзакції, аналізувати трафік та блокувати підозрілі дії.

Важливе значення має захист кінцевих пристроїв і серверів. Надійні робочі місця та захищені сервери знижують ризик втрати даних через шкідливе ПЗ або внутрішні помилки користувачів. Крім того, централізоване управління доступом та багатофакторна автентифікація облікових записів мінімізують можливість несанкціонованого доступу до фінансових систем.

В Україні питання кібербезпеки фінансового сектору стає пріоритетним. Національний банк України встановив чіткі вимоги до платіжних систем, які передбачають побудову захищеної інфраструктури, створення алгоритмів дій під час кібератак та впровадження сучасних технологій безпеки.

Позитивним прикладом є українські платіжні системи, які пройшли сертифікацію за стандартом PCI DSS та впровадили комплексні системи захисту даних. Особливе значення має і обізнаність користувачів.

Українські експерти радять дотримуватися базових правил кібергігієни: завантажувати програми тільки з офіційних джерел, не переходити за підозрілими посиланнями, уникати зберігання даних карток на сторонніх ресурсах, застосовувати багатофакторну автентифікацію та користуватися VPN при підключенні до відкритих мереж.

Водночас в Україні відсутній єдиний орган, що відповідає за національну кібербезпеку, а законодавство має рамковий характер. Це підкреслює необхідність комплексного підходу: безпека фінансових операцій залежить не лише від банків, а й від самих користувачів.

Для ефективного захисту фінансових даних користувачам необхідно поєднувати технологічні засоби та власну обережність. Одним із ключових заходів є використання надійного антивірусного програмного забезпечення, що дозволяє блокувати шкідливі програми, фішингові сайти та віруси. Не менш важливо регулярно оновлювати операційну систему та програми, оскільки застаріле програмне забезпечення створює вразливі місця для хакерських атак.

Користувачі повинні уникати зберігання даних банківських карт на сторонніх сайтах та додатках, навіть якщо це зручно для швидких покупок. Використання багатофакторної автентифікації для доступу до інтернет-банкінгу суттєво знижує ризик злому акаунту. При підключенні до публічних мереж Wi-Fi рекомендується використовувати VPN, щоб запобігти перехопленню персональних даних.

Не менш важливо дотримуватися обережності під час отримання повідомлень у месенджерах, електронній пошті або соцмережах. Слід перевіряти достовірність джерела, не переходити за підозрілими посиланнями та не повідомляти стороннім свої паролі та інші конфіденційні дані.

На рівні банківської системи ефективними є багаторівневі заходи безпеки: моніторинг підозрілих транзакцій у режимі реального часу, автоматичне блокування підозрілих операцій та навчання співробітників для виявлення потенційних загроз.

Комплексний підхід, який поєднує технології, знання та уважність користувачів, дозволяє суттєво зменшити ризики кіберзлочинів та захистити фінансові ресурси.

Таким чином, кібербезпека є не лише технічним завданням, а й соціально-організаційним процесом, який вимагає свідомого підходу, постійного навчання та інвестицій у сучасні технології. Тільки системний підхід дозволяє забезпечити надійний захист коштів та персональних даних у цифровому середовищі, зменшуючи ризики кіберзлочинності та підвищуючи довіру користувачів до фінансових установ.

Список використаних джерел:

1. Захист від шахрайства з банківськими картками: корисні поради та рекомендації. URL: <https://www.oschadbank.ua/blog/zahist-vid-sahrajstva-z-bankivskimi-kartkami-korisni-poradi-ta-rekomendacii>
2. Кібербезпека платежів: що робити, щоб не було запізно. URL: <https://minfin.com.ua/ua/2021/08/31/70762402/>
3. Кібербезпека в Україні: як захистити свої кошти від шахраїв. URL: <https://unn.ua/news/kiberbezpeka-v-ukraini-yak-zakhystyty-svoi-koshty-vid-shakhrayiv>

УДК 336.71

Гудзь О.Є.

*д.е.н., професор, завідувач кафедри
фінансових ринків та технологій
Державний податковий університет*

БЕЗПЕКА ІНФОРМАЦІЙНИХ РЕСУРСІВ У ФІНАНСОВИХ УСТАНОВАХ

Діяльність фінансових установ завжди пов'язана із високими ризиками. Водночас, інформаційні технології значно змінили поведінку фінансових установ, привносячи інновації, підвищуючи ефективність, але й генеруючи додаткові загрози.

Так, фінансові установи впроваджують онлайн-банкінг, що дозволяє клієнтам управляти своїми рахунками, переказувати гроші та отримувати фінансові послуги без необхідності відвідувати фізичні відділення, саме, „завдяки відкритому банкінгу споживачі отримують можливість безпечно ділитися своїми фінансовими даними з авторизованими третіми сторонами, що стимулює створення інноваційних сервісів, таких як персоналізоване управління фінансами, автоматизоване бюджетування та порівняння банківських продуктів” [2]. Фінансові установи використовують розумні алгоритми та штучний інтелект для аналізу даних, прогнозування ринкових тенденцій та виявлення схильностей до шахрайства. А, блокчейн-технології та криптовалюта змінили спосіб, як фінансові установи проводять транзакції, тобто, „технологія блокчейн стала основою сучасних платіжних систем,

забезпечуючи прозорість, швидкість і безпеку транзакцій” [3], а цифрові платформи, такі як Robinhood та E TRADE, надають широким верствам інвесторів доступ до ринків акцій та цінних паперів з мобільних пристроїв. Завдяки мобільним додаткам, онлайн-банкінгу та цифровим платіжним платформам фінансові послуги стають доступнішими. Зростання популярності мобільних платіжних систем, таких як Apple Pay, Google Pay та інші, значно спростило процеси оплати. Це призвело до зменшення використання готівки і збільшення обсягу безготівкових транзакцій. Відбувається демократизація фінансів, оскільки технології знижують бар'єри для участі у фінансовій системі, цифрові платформи, такі як краудфандинг та P2P-кредитування, відкрили нові можливості для малих підприємств і стартапів отримувати фінансування, зменшуючи залежність від традиційних банків, а люди з будь-якого куточку світу отримують доступ до інвестицій, мікрокредитів та міжнародних платежів, все більше фінансових послуг переходять на модель підписки, що дозволяє споживачам отримувати доступ до послуг за фіксовану плату, замість одноразових виплат.

Водночас, науковці звертають увагу, що „в умовах зростаючої цифровізації та поглиблення глобалізаційних процесів фінансова система країни стикається з новими викликами, які стосуються кібербезпеки, фінансової стабільності, ефективності державного регулювання, розвитку фінансових технологій та забезпечення прозорості економічних процесів” [4, с. 190]. Так, протягом останніх п'яти років понад 90% опитаних фінансових установ зазнали фінансових збитків, пов'язаних із недостатнім рівнем безпеки інформаційних ресурсів від: комп'ютерних вірусів; атак із середини та із зовні; помилок неувважності; інформаційного шпигунства.

Цікаво, що загрози безпеки інформаційних ресурсів проявляються не самотійно, а через можливу взаємодію з найбільш слабкими ланками системи захисту, тобто через чинники уразливості. Загроза призводить до порушення діяльності систем на конкретному об'єкті-носії.

Основні вразливості виникають внаслідок: недосконалості програмного забезпечення, апаратної платформи; різних характеристик будови автоматизованих систем в інформаційному потоці; частина процесів функціонування систем є неповноцінною; неточності протоколів обміну інформацією та інтерфейсу; складних умов експлуатації і розташування інформації.

Як свідчить досвід, основними способами реалізації інформаційних загроз є: маніпулювання інформацією (дезінформація, викривлення інформації, подання в інформаційне середовище неповної або неправдивої інформації); порушення встановленого порядку інформаційного обміну, несанкціонований доступ або необґрунтоване обмеження доступу до інформаційних ресурсів, протиправне збирання і використання інформації; руйнування та використання з протиправною метою чужих інформаційних ресурсів; інформаційний тероризм (поширення комп'ютерних вірусів, установлення програмних та апаратних пристроїв, призначених для несанкціонованого отримання інформації, упровадження радіоелектронних приладів перехоплення інформації,

незаконне використання чи порушення роботи інформаційних і телекомунікаційних систем, нав'язування фальшивої інформації, оприлюднення компрометуючої інформації тощо).

Процес забезпечення безпеки інформаційних ресурсів у фінансових установах повинен включати: аналіз та ідентифікацію ризиків; оцінювання ризиків з точки зору їх впливу на бізнес та ймовірності їх появи; інформування особи, яка вправі приймати рішення та акціонерів установи про ймовірності та впливи цих ризиків (ймовірність і наслідки ризику мають бути зрозумілими); встановлення порядку та пріоритетів оброблення ризиків; становлення пріоритетів виконання дій щодо зниження ризиків; участь керівництва в процесі прийняття рішень; ефективний моніторинг та регулярний перегляд ризиків і безпекових аспектів; інформування керівництва та персоналу.

При цьому, „сучасні технології кібербезпеки включають моніторинг у реальному часі, використання штучного інтелекту для виявлення загроз та автоматизацію процесів реагування на інциденти” [2]. „Важливим аспектом цифрової трансформації фінансової системи є також регуляторні ініціативи, які мають на меті забезпечити кібербезпеку, захист персональних даних і дотримання міжнародних стандартів у сфері фінансових технологій” [4], адже, фінансові установи мають впроваджувати передові технології для захисту даних клієнтів, такі як biometric authentication (біометрична автентифікація) та encryption (шифрування). Разом з цим, науковці наголошують, що „особливої уваги потребує питання гармонізації національного фінансового законодавства з міжнародними стандартами та забезпечення ефективної взаємодії державних інституцій із приватним сектором у сфері фінансової безпеки” [4, с. 190].

Тобто, організація безпеки інформаційних ресурсів у фінансових установах має здійснюватися на основі централізованого управління безпекою. Основними домінантами тут виступають: законність; самостійність та відповідальність; компетентність; економічна доцільність; цілеспрямованість; конфіденційність. А, основними принципами забезпечення безпеки інформаційних ресурсів у фінансових установах мають стати: стійкість; адаптація; трансформація; відновлення; автономність.

Список використаних джерел:

1. Білявський В., Білявська Ю., Уманців Ю., Шестак Я., Журба О., Хаванов А. Цифрові технології у фінансовому секторі економіки. *Financial and Credit Activity Problems of Theory and Practice*. 2024. № 4(57), 171–183. URL: <https://doi.org/10.55643/fcaptop.4.57.2024.4444>
2. Демчишак Н. Б., Лоїк Р. В., Лоїк А. В. Розвиток цифрових технологій у банківській системі України: інновації в кредитуванні, ризики та перспективи. *Економіка та суспільство*. 2024. № 61. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/3714/3636>
3. Козир Ю. Р. Функціональна роль блокчейн технологій у трансформації платіжних систем. *Інвестиції: практика та досвід*. 2023. № 20. С. 112–116.

4. Пузирьова П.В. Механізм забезпечення економічної безпеки у сфері сталого розвитку фінансової системи держави в умовах цифрової економіки та глобалізаційних змін. *Актуальні проблеми економіки*. № 1 (283). 2025. С. 189 – 204.

УДК 004.056

Дракон Д.С.

здобувач вищої освіти

ННІ «Каразінський банківський інститут» ХНУ ім. В.Н. Каразіна;

Науковий керівник:

Стяглик Н.І.

к.п.н., доцент, завідувач кафедри інформаційних технологій

та математичного моделювання

ННІ «Каразінський банківський інститут» ХНУ ім. В.Н. Каразіна

СУЧАСНІ ПІДХОДИ ДО ЗАХИСТУ ПРОГРАМНИХ ПРОДУКТІВ: ВІД ПОЛІТИК БЕЗПЕКИ ДО ІНСТРУМЕНТІВ АВТОМАТИЗАЦІЇ

У сучасному цифровому середовищі програмні продукти стали основою роботи багатьох інфраструктур. Бізнесу, освіти, державних установ, та повсякденного життя. Збільшення кількості кіберзагроз, високий рівень автоматизації та залежність від хмарних технологій вимагають нових методів забезпечення інформаційної безпеки.

Традиційні підходи, такі як антивірусний захист та міжмережеві екрани, вже не гарантують достатнього рівня надійності. Тому актуальним стає системний підхід до захисту програмних продуктів, що включає поєднання політик безпеки, технологій і засобів автоматизації.

Фундаментальною складовою захисту програмних продуктів є політика безпеки. Вона визначає правила, стандарти та процедури, які регулюють використання, обробку і збереження інформації. У сучасних умовах саме правильно сформована політика стає тією межею, в рамках якої реалізуються всі технічні та організаційні заходи. Без неї навіть найновіші технологічні інструменти можуть бути використані неефективно або з помилками.

Існує один із ключових принципів сучасних політик, це концепція – Security by Design. Це підхід коли безпека закладається на ранніх етапах життєвого циклу програмного продукту. Це означає, що вимоги до безпеки враховуються вже при проектуванні архітектури системи, створенні технічних завдань і написанні коду.

Наприклад, у процесі розробки застосунку можуть бути застосовані інструменти статичного та динамічного аналізу коду, які дозволяють виявити потенційні вразливості ще до виходу продукту у реліз. Такий підхід дозволяє значно знизити витрати на усунення помилок і зменшити ризики їх експлуатації зловмисниками.

Не менш важливим аспектом є політика доступу. Вона базується на принципі найменших привілеїв, який передбачає, що користувач або процес отримує лише ті права, які необхідні для виконання конкретного завдання. Наприклад, бухгалтер у корпоративній системі має доступ лише до фінансових модулів, але не до адміністративних налаштувань.

У великих компаніях політики доступу часто реалізуються через системи керування ідентифікацією та доступом (IAM – Identity and Access management), що дозволяє централізовано контролювати права користувачів.

Крім того, в найважливіші складники також входять: управління інцидентами та відповідність міжнародним і національним стандартам. Жодна система не може бути повністю захищеною від атак, тому необхідно мати чіткі процедури реагування, у сучасних практиках широко використовується підхід IRP (Incident Response Plan), який описує покрокові дії персоналу у випадку кіберінциденту.

Найпоширенішим є стандарт ISO/IEC 27001, який встановлює вимоги до системи управління інформаційною безпекою. Для організацій, що працюють із персональними даними користувачів, актуальним є також регламент ЄС із захисту даних (GDPR).

Не менш ключову роль відіграють технологічні засоби, адже вони реалізують практичні механізми захисту даних. У сучасних мовах поєднуються як класичні методи, так і нові технології, орієнтовані на гнучкість та адаптивність.

Криптографічні методи залишаються основою кіберзахисту. Вони застосовуються для шифрування інформації як під час її передачі (наприклад, протоколи SSL/TLS), так і під час зберігання у базах даних чи хмарних сервісах.

Багатофакторна автентифікація (MFA) підвищує рівень захисту користувачів, коли перевірка паролем вже давно не є достатньою. В той самий час все більшої популярності набуває Zero Trust Architecture – підхід під час якого кожен запит на доступ перевіряється окремо, незалежно від того, де знаходиться користувач чи пристрій.

Окрему роль відіграють системи моніторингу та виявлення аномалій. IDS/IPS-рішення здатні відстежувати підозрілу активність у режимі реального часу, тоді як SIEM-платформи агрегують журнали подій з різних систем і дозволяють швидко виявити тенденції, що можуть свідчити про кібератаку.

Також, зростання популярності хмарних технологій актуалізує питання захисту у хмарному середовищі. Тут застосовуються такі механізми, як сегментація даних, ізоляція віртуальних середовищ, контроль доступу на основі ролей і шифрування у контейнерах.

А в таких умовах, зростання масштабів програмних систем і кількості користувачів та динамічного розвитку технологій кіберзахисту, автоматизація є не просто бажаним, а необхідним елементом.

Одним із ключових напрямів автоматизації є DevSecOps, тобто інтеграція безпеки у всі етапи життєвого циклу розробки. У цьому підході тестування на вразливості відбувається автоматично під збірки та розгортання програмного

продукту, що мінімізує ризик виходу у світ з потенційними «дірками» у захисті. Таким чином, безпека стає невід’ємною частиною CI/CD-процесів.

Важливим інструментом стає і застосування штучного інтелекту та машинного навчання. AI/ML здатні аналізувати величезні обсяги даних у режимі реального часу, виявляючи нові типи атак і прогножуючи потенційні загрози.

Не менш значущими є автоматичні оновлення та патч-менеджмент. Використання таких систем дозволяє оперативно встановлювати виправлення вразливостей, зменшуючи ризик експлуатації застарілих версій програмного забезпечення.

Ще один аспект – роботизація моніторингу. Автоматизовані агенти та боти можуть відстежувати доступи, перевіряти журнали активності, формувати сповіщення і навіть створювати візуальні дашборди. Це знижує навантаження на спеціалістів з безпеки та дозволяє їм зосередитись на стратегічних завданнях, а не на рутині.

Попри значні досягнення у сфері політик, технологій та автоматизації, реальна ефективність системи безпеки досягається лише тоді, коли ці елементи взаємодіють у єдиній моделі. Комплексний підхід – це не сукупність окремих заходів, а скоординована стратегія, у якій організаційні та технічні рішення взаємно підсилюють одне одного.

Ключовими аспектами комплексного підходу є навчання персоналу, постійний аудит, перевірка відповідності стандартам. А додатковий рівень захисту формує багаторівнева архітектура безпеки, котра передбачає використання кількох незалежних бар’єрів.

Окремо слід зазначити роль співпраці між різними групами фахівців. Розробники, системні адміністратори та спеціалісти з безпеки мають працювати як єдина команда. Це дозволяє враховувати безпеку ще на етапі проєктування, швидко усувати вразливості та забезпечувати стабільність роботи програмного продукту.

Захист програмних продуктів у сучасному цифровому середовищі є багатогранним завданням, яке неможливо вирішити за допомогою лише одного інструменту чи методу. Політики безпеки формують основу, задаючи правила, стандарти й процедури, що регулюють роботу з інформацією. Технологічні засоби забезпечують практичну реалізацію цих правил, створюючи багаторівневу інфраструктуру захисту.

Лише комплексний підхід, що інтегрує політики, технології та автоматизацію в єдину систему, здатний забезпечити належний рівень безпеки програмних продуктів. Важливим доповненням є навчання персоналу, постійний аудит і гнучкість архітектури, які дозволяють організаціям адаптуватися до змін середовища та нових викликів.

У перспективі головними трендами у сфері кіберзахисту стають використання штучного інтелекту, розвиток концепції Zero Trust і глибша інтеграція DevSecOps у процеси розробки.

Список використаних джерел

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, 2022.
2. NIST Special Publication 800-207. Zero Trust Architecture. National Institute of Standards and Technology, 2020.
3. OWASP Foundation. OWASP Top Ten 2021: The Ten Most Critical Web Application Security Risks. [Електронний ресурс]. Режим доступу: <https://owasp.org/Top10/>
4. Microsoft Security Blog. The future of cybersecurity: AI, Zero Trust, and resilience. [Електронний ресурс]. Режим доступу: <https://www.microsoft.com/security/blog/>

УДК 004.056

Жилін І.С.

здобувач вищої освіти,

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

Науковий керівник

Ковальчук Д.М.

PhD, старший викладач кафедри інформаційних технологій

та математичного моделювання

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

СУЧАСНІ СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

У сучасному цифровому світі інформаційні системи посідають центральне місце у функціонуванні бізнесу, державного управління, освітніх установ та науково-дослідних організацій. Вони забезпечують обробку, зберігання, передавання та захист даних, що є основою для прийняття рішень і підтримки безперервності діяльності. Проте з розвитком цифрових технологій зростає кількість і складність кіберзагроз, що призводить до необхідності впровадження нових стратегій забезпечення надійності та безпеки інформаційних систем.

Однією з головних проблем сьогодення є зростання масштабів цілеспрямованих атак на інформаційну інфраструктуру. Такі атаки, як АРТ (Advanced Persistent Threats), програми-вимагачі (ransomware), атаки на відмову в обслуговуванні (DDoS), орієнтовані на порушення нормальної роботи систем та викрадення даних, завдають значних економічних збитків і шкодять репутації організацій. Додатковим викликом стає поширене використання хмарних технологій і сервісів, інтеграція великої кількості мобільних та IoT-пристроїв, а також необхідність дотримання міжнародних стандартів і нормативів у сфері

кібербезпеки. Усі ці фактори зумовлюють формування нових стратегій, спрямованих на досягнення високого рівня надійності та стійкості інформаційних систем.

Серед сучасних стратегій особливе місце займає концепція Zero Trust Security. Її принцип базується на відмові від традиційної моделі довіри до користувачів і пристроїв, що перебувають усередині корпоративної мережі. Замість цього впроваджується перевірка кожної взаємодії, багатофакторна автентифікація, політика мінімальних привілеїв та безперервний моніторинг дій. Це дає змогу знизити ризики несанкціонованого доступу та поширення загроз усередині інформаційної системи.

Іншим напрямом є застосування штучного інтелекту та машинного навчання у системах моніторингу та реагування. Сучасні рішення класу SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation and Response) здатні аналізувати великі обсяги даних у режимі реального часу, виявляти аномалії у мережевому трафіку та автоматизувати реагування на інциденти без участі людини. Це значно підвищує ефективність захисту та скорочує час реакції на атаки.

Важливим аспектом безпеки є хмарні технології, які дедалі активніше впроваджуються в інформаційні системи. Для забезпечення їхнього захисту використовуються CASB-рішення (Cloud Access Security Broker), що здійснюють контроль доступу до хмарних ресурсів, запобігають витокам даних і забезпечують відповідність нормативним вимогам. Разом із цим поширення мікросегментації мереж дозволяє поділяти інформаційні системи на ізольовані сегменти, що знижує ризик поширення шкідливого програмного забезпечення у разі компрометації окремих компонентів.

Не менш важливим елементом є застосування криптографічних методів захисту інформації. Використання сучасних алгоритмів шифрування, таких як AES, RSA, ECC, забезпечує захист конфіденційних даних під час передавання та зберігання. Водночас актуальним завданням стає підготовка до постквантової криптографії, оскільки з розвитком квантових обчислень існуючі алгоритми можуть втратити свою ефективність.

Забезпечення безперервності бізнес-процесів вимагає створення систем резервування та відновлення. Сучасні стратегії Disaster Recovery включають дублювання критичних компонентів, використання географічно розподілених дата-центрів та автоматизоване відновлення роботи після збоїв. Це дозволяє мінімізувати втрати даних і час простою інформаційних систем у разі інцидентів.

Практичне впровадження зазначених стратегій потребує комплексного підходу. Організаціям доцільно проводити регулярний аудит безпеки, впроваджувати систему управління ризиками на основі міжнародних стандартів ISO/IEC 27001 та NIST, здійснювати навчання персоналу принципам кібергігієни, застосовувати багатофакторну автентифікацію та контроль доступу, а також інтегрувати кібербезпеку в усі етапи життєвого циклу інформаційних систем у межах концепції DevSecOps.

Перспективи розвитку стратегій надійності та кібербезпеки пов'язані з активним впровадженням квантових технологій і постквантових алгоритмів шифрування, розвитком кіберстійких архітектур для критичних інформаційних інфраструктур, застосуванням генеративного штучного інтелекту для прогнозування та запобігання атакам, а також посиленням глобальних нормативних вимог у сфері інформаційної безпеки.

Отже, сучасні стратегії забезпечення надійності та кібербезпеки інформаційних систем ґрунтуються на поєднанні технічних інновацій і організаційних заходів. Вони включають використання Zero Trust, штучного інтелекту, хмарних технологій, мікросегментації, криптографії, резервування та відновлення, а також постійний розвиток політик і процедур управління безпекою. Лише комплексний підхід дозволяє забезпечити стійкість інформаційних систем до сучасних загроз, гарантувати захист даних і підтримати безперервність діяльності організацій у цифровій економіці.

Список використаних джерел:

1. Толюпа С., Кулько А. Забезпечення захищеності складних інформаційних та технологічних систем об'єктів критичної інфраструктури // Кібербезпека: освіта, наука, техніка. – 2025. – Т. 4, № 28. – С. 671–687. – Режим доступу: <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/859>
2. Юдін О. Безпека інформаційно-телекомунікаційних систем: питання термінології та базових визначень галузі // Наукоємні технології. – 2015. – № 2 (26). – С. 198–203. – Режим доступу: <https://jrn1.nau.edu.ua/index.php/SBT/article/view/5332>

УДК 004.056:336.71

Заріцький О. В.

здобувач вищої освіти,

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Науковий керівник

Гальчинський Л. Ю.

ORCID: 0000-0002-3805-1474

к.т.н., доцент, доцент кафедри інформаційних технологій та математичного моделювання

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

КІБЕРСТІЙКІСТЬ БАНКІВСЬКОГО СЕКТОРУ УКРАЇНИ: АНАЛІЗ ФРЕЙМВОРКІВ ТА ПІДХОДІВ

Кіберстійкість – здатність фінансової установи протистояти кіберінцидентам, стримувати їх вплив та оперативно відновлювати роботу. В англomовній літературі усталено вживається термін *cyber resilience*, інколи – *кіберрезильєнтність*. Немало дослідників в україномовній науковій літературі вживають термін кіберрезильєнтність. У 2015 році дослідники уточнили саме кіберрезильєнтність як *«здатність організації постійно досягати запланованого результату, незважаючи на кібератаки»*[1]. Тобто акцент змістився з відновлення після інциденту на забезпечення безперервності критичних функцій навіть під час атак.

За минуле десятиріччя кількість кібератак суттєво зросла, а в умовах війни, інфраструктури України стала однією з найбільш атакованих цілей. Це визначило практичну потребу у стратегіях кіберстійкості: від технічного захисту до організаційних заходів і стратегічного управління ризиками.

Жоден окремий стандарт не дає всеосяжного «рецепту» стійкості. До прикладу, NIST Cybersecurity Framework (CSF) [2] виділяє п'ять базових функцій – Identify, Protect, Detect, Respond, Recover; у версії 2.0 (2024) додано функцію Govern. ISO/IEC 27001 задає вимоги до системи менеджменту безпеки й безперервності (BCP/DRP).

WEF розробив комплексний фреймворк, що поєднує характеристики NIST та концепцію Ігоря Лінкова [3]: чотири домени (фізичний, інформаційний, когнітивний, соціальний) × чотири етапи (планування, поглинання, відновлення, адаптація). Додано стадію «виявлення загроз», а разом – 20 клітинок і 98 показників. Це дозволяє оцінити стійкість системи комплексно – від технічних до організаційних аспектів.

У Шотландії створено урядовий фреймворк для публічного сектору [4]: опитування зрілості кіберстійкості за чотирма доменами – управління ризиками, захист, виявлення інцидентів, реагування та відновлення. Він не прив'язаний до одного стандарту, що забезпечує адаптивність до нових вимог.

У 2016 році Управління грошового обігу Гонконгу запровадило Cybersecurity Fortification Initiative [5], що включає Cyber Resilience Assessment Framework (C-RAF) із трьома елементами: оцінка притаманного ризику, оцінка зрілості контролів та тестування iCAST (intelligence-led cyber attack simulation testing), що являють собою симуляції реальних атак на основі актуальної threat intelligence, що оцінюють не лише захист, а й здатність фінансової установи дог виявлення та реагування.

На наднаціональному рівні Комітет з платежів і інфраструктур CPMI-IOSCO у 2016 році видали керівництво з кіберстійкості для фінансових інфраструктур. Європейський центробанк на його основі створив CROE з 8 розділами: від управління ризиками до навчання і тестування. Додатково, у 2023 році набув чинності акт DORA, який прямо зобов'язує банки ЄС впровадити операційну стійкість, стрес-тести та аудити третіх сторін. Всі ці нововведення формують сучасний ландшафт нормативних вимог до кіберстійкості банків.

У Великій Британії діє аналогічний підхід CBEST, у ЄС – програма TIBER-EU. Вони передбачають red team-тестування фінансових установ за сценаріями реальних APT. Це суттєва відмінність від недавніх часів, коли

фінансові установи здебільшого обмежувалися аудитами та технічними тестами на відповідність стандартам. Зараз – акцент на динамічному випробуванні стійкості до новітніх атак.

Україна сьогодні – це передовий плацдарм кіберпротистояння. Тут випробовуються як нові атаки (APT, wiper-атаки, масовані DDoS), так і технології захисту (хмарні сервіси, автоматизація SOC, інтеграція з глобальними ТП). Тож маємо ситуацію, на яку подивимось з різних боків: з одного боку, величезні ризики для безперервності фінансових послуг, а з іншого – можливості для підготовки, напрацювання практик та формування стандартів, які потім перейматимуть інші країни.

НБУ інтегрує принципи кіберстійкості в регулюванні: створено CSIRT-NBU, впроваджуються вимоги до управління кіберризиками як складової операційного ризику, рекомендації банкам впровадження внутрішніх «Положень про кіберстійкість», що враховують специфіку бізнес-процесів банку, критичність сервісів, результати аналізу ризиків і залежностей та визначають цілі, відповідальність і порядок обміну інформацією про інциденти. Фактично формується циклічний процес: оцінка вразливостей → реалізація заходів захисту → плани неперервності та аварійного відновлення → регулярні тренінги та перегляд стратегії після значних атак.

У серпні 2025 року керівник CSIRT-NBU, Олександр Кльок підтвердив плани впровадження TIBER-UA, що передбачає регулярне red team-тестування банків з урахуванням актуальних загроз для фінансового сектору України та участю CERT-UA.

На практиці банки переходять у хмарні інфраструктури, інвестують у XDR та SOAR, формують власні SOC або користуються SOC-as-a-Service. Окремим вектором стає проведення тестування на проникнення на основі ШІ: це здешевлює перевірки та робить їх регулярнішими, але водночас відкриває нові ризики використання ШІ для атак.

Як підсумок, кіберстійкість у фінансовому секторі України – це вже не просто плани відновлення після інцидентів, а повний життєвий цикл кіберзахисту, інтегрований у бізнес-процеси. Існуючі міжнародні стандарти та фреймворки (NIST CSF, ISO, WEF, C-RAF, CBEST, TIBER-EU, CROE, DORA) формують методичну основу. Їхні відмінності – у рівні деталізації та глибині: від загальних рамок до практичних симуляцій атак. Українськими науковцями вже було запропоновано методики адаптації міжнародних моделей для оцінювання стійкості критичної інфраструктури України [6], що створює підґрунтя для подальшого застосування подібних підходів у банківській сфері.

Для України кіберстійкість має особливе значення: країна водночас є головною ціллю атак та полігоном для випробування нових практик захисту та методик їх оцінювання. Впровадження TIBER-UA та перспектива використання AI-driven pentesting визначають новий етап. Оптимальною стратегією для українських банків є поєднання міжнародних стандартів, виконання регуляторних вимог та систематичне тестування готовності до найгірших сценаріїв із використанням новітніх технологій.

Список використаних джерел:

1. Björck, Fredrik; Henkel, Martin; Stirna, Janis; Zdravkovic, Jelena (2015). Cyber Resilience - Fundamentals for a Definition. Advances in Intelligent Systems and Computing. Vol. 353. Stockholm University. pp. 311–316.
2. The NIST Cybersecurity Framework (CSF) 2.0 National Institute of Standards and Technology <https://doi.org/10.6028/NIST.CSWP.29>, February 26, 2024
3. Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471–476.
4. SCOTTISH PUBLIC SECTOR CYBER RESILIENCE FRAMEWORK V1.2
5. Hong Kong Monetary Authority. Cybersecurity Fortification Initiative. Cyber Resilience Assessment Framework (C-RAF), 2016.
6. Харламова, К., & Гальчинський, Л. (2022). Оцінювання кіберстійкості об'єктів критичної інфраструктури України. Scientia, Vilnius, 118–120.
7. Bodeau, D.J., Graubart, R.D., McQuaid, R., & Woodill, J. (2019). Cyber Resiliency Metrics and Scoring in Practice-UseCase Methodology and Examples.

УДК: 373.2:004.738.5:004.056.2

Змійова Д.Д.

здобувач вищої освіти, ННІ «КБІ» ХНУ імені В.Н. Каразіна

Науковий керівник

Єрмакова Н.А.

ст.викл. кафедри інформаційних технологій та математичного моделювання

ННІ «КБІ» ХНУ імені В.Н. Каразіна

КІБЕРБЕЗПЕКА ТА ФОРМУВАННЯ БЕЗПЕЧНОГО ІНТЕРНЕТ-ПРОСТОРУ ДЛЯ ДІТЕЙ ДОШКІЛЬНОГО ВІКУ

Сьогодні інтернет є невід'ємною частиною життя навіть наймолодших користувачів. Діти дошкільного віку дедалі частіше мають доступ до цифрових пристроїв – смартфонів, планшетів, смарт телебачення. З одного боку, це відкриває широкі можливості для розвитку, навчання та пізнання світу, з іншого – створює серйозні ризики для їхньої безпеки.

Створення безпечного інтернет-середовища для дошкільнят охоплює кілька важливих аспектів: контроль доступу до інформації, використання спеціальних додатків та фільтрів, добір якісного навчально-розважального контенту, обмеження часу перебування за гаджетами, а також формування перших навичок цифрової грамотності. Це допомагає запобігти небажаним ризикам, підтримати психоемоційний розвиток дитини та створити умови, за

яких технології стають корисним інструментом для навчання й розвитку, а не загрозою.

Основні небезпеки для дошкільнят у мережі пов'язані з:

- доступом до неприйняттого контенту,
- можливістю випадкових покупок чи завантажень,
- ризиком надмірного використання гаджетів, що впливає на психічний та фізичний розвиток.

Створення безпечного простору для дітей у мережі потребує комплексного підходу. Важливими кроками від батьків є:

1. Батьківський контроль – використання спеціальних програм та налаштувань, що обмежують доступ до небажаних сайтів чи додатків
2. Якісний контент – добір освітніх ігор, мультфільмів та програм, що відповідають віку дитини.
3. Формування культури користування – пояснення дітям простими словами правил поведінки в інтернеті: не натискати на незнайомі посилання, не завантажувати нічого без дозволу дорослих.
4. Часові рамки – встановлення балансу між перебуванням онлайн та реальними іграми, спілкуванням, творчістю.

Головна роль у створенні безпечного простору у середовищі інтернет для дітей належить дорослим – саме батьки й вихователі мають бути першими провідниками дитини у цифровий світ. Лише поєднання технологічних рішень із вихованням та увагою дорослих забезпечить справді безпечний і корисний інтернет-простір для дошкільнят.

Важливо зазначити, що питання безпеки дітей у цифровому середовищі неможливо розглядати окремо від проблематики кібербезпеки. Саме вона стає фундаментом захисту дошкільнят в інтернеті.

Основні аспекти кібербезпеки у цьому віці включають:

- Захист персональних даних – приховування геолокації, контроль доступу до фото та відео, правильні налаштування конфіденційності.
- Безпечні пристрої – використання паролів, антивірусів, спеціальних дитячих профілів та блокування небажаних сайтів.
- Контент-фільтри – застосування дитячих браузерів, YouTube Kids, освітніх платформ з перевіреним матеріалом.
- Захист від соціальної інженерії та фішингу – блокування реклами та контроль дозволів, адже маленькі діти легко можуть натиснути на підозрілі посилання.
- Формування цифрової грамотності з раннього віку – пояснення простими словами правил: “Не натискай без дозволу”, “Завжди запитуй у дорослого”. Це перші кроки у формуванні навичок кібергигієни.

Підсумовуючи, створення безпечного простору для дітей у мережі – це комплексне завдання, що включає як технічні рішення, так і виховні заходи. Лише поєднання сучасних технологій, уваги та контролю з боку дорослих і формування у дітей перших навичок цифрової грамотності може забезпечити справді корисне, безпечне та розвивальне середовище для наймолодших користувачів інтернету.

Список використаних джерел:

1. Безпечний Інтернет для дітей: методичні рекомендації / МОН України. – Київ, 2021. – 48 с.
2. Як навчити безпеці у віртуальному світі: посібник для батьків і педагогів. – Київ: Київстар, Центр цифрових технологій майбутнього, 2020. – 64 с.
3. Освіта.ua. Усе про безпеку дітей і підлітків в інтернеті. URL: <https://osvita.ua/school/topics/92279/>
4. Children's Safety in the Digital Environment. Data for Impact Project, 2024. URL: https://www.data4impactproject.org/wp-content/uploads/2024/10/D4I-Report-Childrens-Safety-in-the-Digital-Environment_TR-24-588_508c.pdf?utm_source
5. Stop the Traffik. Online Safety for Ukrainian Youth: Survey Findings, 2023. URL: https://stopthetraffik.org/child-online-safety-ukraine1/?utm_source
6. Amazonia Investiga. The problem of child safety in the digital space // Amazonia Investiga. – 2023. – Vol. 12(61). – P. 253–260. URL : https://amazoniainvestiga.info/index.php/amazonia/article/view/2538?utm_source
7. UNICEF. Policy guidance on AI for children. – Geneva: UNICEF, 2021. URL: <https://www.unicef.org/globalinsight>
8. Al-Garadi, M. et al. A safety risk assessment framework for children's online safety using large language models. – arXiv preprint, 2024. URL: https://arxiv.org/abs/2401.14713?utm_source

УДК 343.98

**Ішу В.В.,
Степанов А.А.,
Горбань Ю.В.**

*Курсанти 2 курсу ННІ №4,
Харківський національний університет внутрішніх справ
Науковий керівник*

Лучик С.Д.
*д.е.н., професор, професор кафедри інформаційних систем та
технологій ННІ №4
Харківський національний університет внутрішніх справ*

CERT: ЇХ ДІЯЛЬНІСТЬ В УКРАЇНІ ТА ІНШИХ КРАЇНАХ

CERT (Computer Emergency Response Team) – це організація, яка займається реагуванням на комп'ютерні інциденти, зокрема на кіберзагрози, атаки та вразливості. Основна мета CERT – допомогти організаціям і

користувачам виявляти, усувати та запобігати кіберзагрозам [1]. До основних функцій CERT відносять: моніторинг виявлення загроз – CERT відслідковує потенційні кіберзагрози і уразливості в системах, реагування на інциденти – коли відбувається інцидент, CERT допомагає відновити безпеку і мінімізувати наслідки, інформування та попередження – CERT інформує організації і громадськість про нові загрози та вразливості, аналіз і розслідування – проведення розслідувань для визначення причин інцидентів і створення рекомендацій щодо запобігання майбутнім атакам.

Зазвичай кожна країна має свій власний національний CERT (наприклад, в Україні є CERT-UA), а також існують приватні CERT-команди, що обслуговують конкретні організації або компанії. Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, в 2024 році опрацювала 4315 кіберінцидентів. Це на 69,8% більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2541 раз [2].

CERT працює за певним процесом, який включає кілька ключових етапів для ефективного реагування на інциденти та запобігання загрозам. CERT виконує багато функцій. Серед них:

1. *Постійно відслідковує різні джерела інформації:* Мережі, системи безпеки, програмне забезпечення) на наявність потенційних загроз.

Виявлення вразливостей: Фахівці CERT аналізують інформацію про нові вразливості в програмному забезпеченні чи апаратних засобах, щоб забезпечити своєчасне усунення потенційних проблем.

2. *Оцінка та ідентифікація інцидентів:*

Аналіз інциденту: Після виявлення загрози CERT проводить детальний аналіз інциденту, визначаючи, що саме сталося, коли і які системи були впливовими.

Ідентифікація типу загрози: Важливо правильно визначити, чи це кібератака (наприклад, DoS-атака, фішинг), чи технічна несправність (наприклад, вразливість у ПЗ).

3. *Реагування на інцидент:*

Миттєве усунення загрози: Якщо загроза реальна і може призвести до серйозних наслідків (наприклад, витік даних), CERT має негайно вжити заходів для локалізації або усунення загрози.

Ізоляція уражених систем: Якщо загроза дуже велика, CERT може відключити уражені системи від мережі, щоб не допустити подальше поширення.

4. Після локалізації загрози CERT працює над відновленням нормальної роботи систем, наприклад, за допомогою резервних копій або патчів для виправлення вразливостей.

Виправлення вразливостей: Встановлення оновлень безпеки (пачів), щоб уникнути повторного виникнення інциденту.

5. *Документування та звітність:*

Документація інциденту: CERT збирає всі необхідні дані для створення звіту, який описує інцидент, його причини та заходи, які були вжиті для усунення загрози.

Звітування: Важливо надавати інформацію вищим органам, партнерам чи громадськості, якщо це необхідно. Вони можуть отримати поради щодо того, як захистити себе від подібних загроз.

Аналіз після інциденту: Після того як інцидент закритий, CERT проводить ретельний аналіз для виявлення слабких місць в системах безпеки.

Поліпшення процесів: Використовує отримані уроки для покращення своєї стратегії реагування на інциденти та оновлення протоколів безпеки.

6. Профілактика та попередження: Поширення інформації: CERT активно поширює інформацію про нові загрози і вразливості серед організацій і громадськості, щоб інші могли вчасно вжити заходів для захисту.

Навчання: Часто проводяться тренінги для персоналу і користувачів для підвищення рівня обізнаності про безпеку.

CERT взаємодіє з іншими організаціями, урядовими структурами, компаніями та навіть міжнародними організаціями для обміну інформацією і координації дій. При цьому усі дії CERT повинні відповідати високим стандартам конфіденційності та захисту персональних даних.

Однак, слід зауважити, що діяльність CERT-UA пов'язана з рядом ризиків та небезпек. Насамперед це кібернетичні атаки у вигляді поширення різноманітних шкідливих програм, зокрема вірусів, троянів, програм для виявлення вразливостей, а також вірусів, що використовуються для крадіжки даних або атак на інфраструктуру критичних об'єктів. Також широко запускаються атаки з метою крадіжки особистої інформації, фінансових даних або доступу до критичних інфраструктурних систем; вибіркові атаки з використанням програм-вимагачів (наприклад, атака NotPetya). Особливу негативну роль відіграють організовані, тривалі атаки, орієнтовані на злам критичних інфраструктурних об'єктів, а також пропаганда та поширення фейкових новин з метою дестабілізувати ситуацію в країні.

Список використаних джерел

1. CERT-UA (Computer Emergency Response Team of Ukraine): офіційний сайт. URL: <https://cert.gov.ua/> (дата звернення: 15.09.2025).

2. CERT-UA минулого року опрацювала 4315 кіберінцидентів. URL: <https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyovala-4315-kiberincidentiv> (дата звернення: 20.09.2025).

Кам'янський Я.Б.

курсант 2 курсу інституту № 4

Харківського національного університету внутрішніх справ

Лучик В. Є.

доктор економічних наук,

професор кафедри протидії кіберзлочинності інституту № 4

Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Блокчейн-технології, спочатку створені для криптовалют, за останні роки отримали значне визнання у різних сферах, зокрема в кібербезпеці. Це технологія, що базується на принципах децентралізації, відкритості і незмінності, що дозволяє значно підвищити рівень безпеки інформації в сучасному цифровому середовищі. Завдяки своїм властивостям, блокчейн може допомогти вирішити ряд проблем у сфері захисту даних, створюючи більш стійкі до атак і непередбачуваних змін системи.

Основним механізмом, який забезпечує безпеку блокчейну, є криптографія. Кожен блок у ланцюгу має унікальний хеш, що посиляється на попередній блок. Це забезпечує послідовність і незмінність записів у ланцюзі. Якщо зловмисник намагається змінити дані в одному з блоків, хеш цього блоку змінюється, і всі наступні блоки також мають змінитися. Це робить неможливим несанкціоновану зміну даних без зміни всього ланцюга блоків, що потребує величезних обчислювальних потужностей і значних ресурсів. Використання блокчейн-технологій у сфері кібербезпеки може допомогти вирішити кілька проблем, зокрема, захист даних від несанкціонованих змін. Системи, які ґрунтуються на блокчейні, можуть забезпечити відсутність єдиної точки вразливості, що є особливо важливим в умовах зростаючих загроз з боку зловмисників. Традиційні системи з централізованим контролем мають єдину точку відмови, яка може стати об'єктом атак. У випадку з блокчейном, навіть якщо зловмисник отримає доступ до окремих компонентів системи, йому не вдається змінити дані без того, щоб це було помічено іншими учасниками мережі. Одна з основних сфер застосування блокчейну в кібербезпеці - це забезпечення аутентифікації та авторизації. Блокчейн може бути використаний для створення дистрибутивних- систем ідентифікації, де дані про користувачів зберігаються не в централізованих базах даних, а на розподілених серверах, доступ до яких має лише певний коло учасників. Такий підхід дозволяє уникнути проблем, пов'язаних з крадіжкою або компрометацією централізованих баз даних, що неодноразово ставало причиною серйозних витоків конфіденційної інформації. Ще одна важлива сфера застосування блокчейну в кібербезпеці - це зберігання і передача критично важливої інформації, такої як ключі шифрування, паролі, токени та інші конфіденційні

дані. Блокчейн може забезпечити безпечний обмін такими даними, зберігаючи їх у зашифрованому вигляді, що дозволяє знизити ризики їх компрометації під час передачі через незахищені канали зв'язку. Крім того, блокчейн дозволяє створювати механізми для здійснення безпечних транзакцій, що є особливо важливим для фінансових організацій, де збереження конфіденційності інформації є першочерговим завданням. Попри свої переваги, технологія блокчейн має певні обмеження, які можуть вплинути на її використання в кібербезпеці. Одним з таких обмежень є масштабованість. Блокчейн-системи можуть працювати зі значними затримками при великому обсязі транзакцій або запитів.

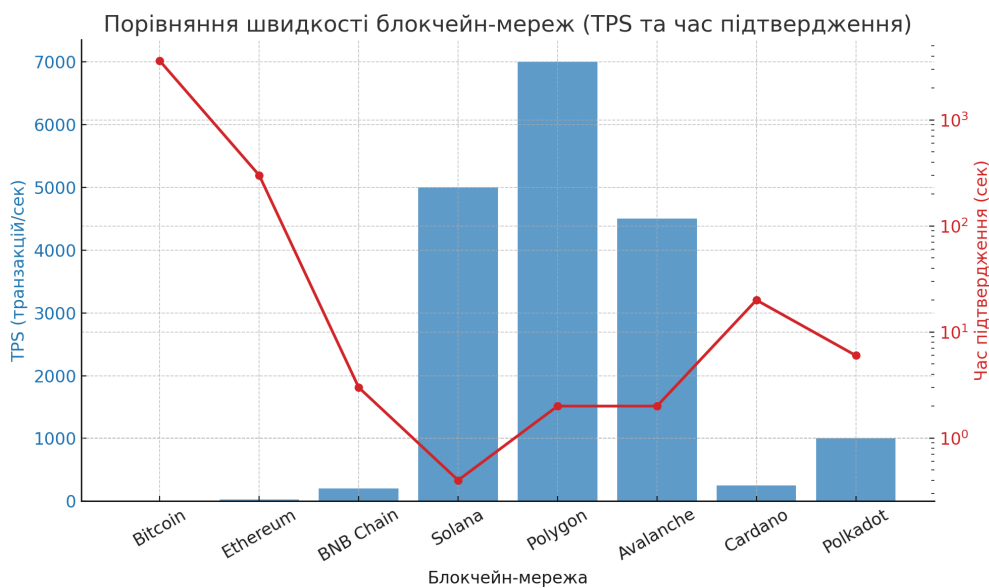


Рисунок 1. - Порівняння швидкості передачі інформації в різних мережах

До прикладу в мережі Polygon швидкість буде найбільшою через найменшу кількість запитів та має більш централізовану будову, на відміну мережа Ethereum буде дорожчим варіантом та повільнішою, оскільки там більший рівень децентралізації та більша кількість запитів. Це може бути проблемою для організацій, які працюють з величезними обсягами даних, оскільки обробка кожної транзакції вимагає обчислювальних ресурсів і часу. Враховуючи цей фактор, важливо розробляти нові протоколи і підходи до масштабування, які б зберігали безпеку та ефективність блокчейн-систем. Ще однією проблемою є високі вимоги до обчислювальних потужностей. Криптографічні операції, необхідні для забезпечення безпеки даних у блокчейн-системах, є досить ресурсоемними. Крім того, велика кількість транзакцій у розподілених мережах може вимагати значних витрат на енергію, що робить блокчейн менш привабливим у порівнянні з іншими технологіями з точки зору екологічної стійкості.

Однак, незважаючи на ці виклики, блокчейн все ж має величезний потенціал для підвищення рівня безпеки в різних сферах. Для цього необхідно проводити подальші дослідження та розробки, спрямовані на покращення

масштабованості та зниження витрат на обчислювальні ресурси, що дозволить впроваджувати блокчейн у більш широкому масштабі. Крім того, важливим є створення стандартів і регулювань для використання блокчейну в різних сферах. Це допоможе знизити ризики, пов'язані з недобросовісними учасниками мережі, і забезпечити прозорість у використанні технології. Впровадження блокчейн-технологій в кібербезпеку допоможе створити більш надійні системи захисту, знизити ймовірність зловживань і покращити довіру до цифрових інфраструктур, що має особливе значення для розвитку цифрових економік.

Список використаних джерел

1. Палагін В. О. Система захисту електронного документообігу на основі технології блокчейн: бакалаврська робота. Київ, 2024. 67 с. (дата звернення: 23.09.2025).
2. A Z. Blockchain-Based Security Applications in Cybersecurity: Perspectives and Challenges. 2017. (дата звернення: 21.09.2025).
3. D T., A T. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. 2016. (дата звернення: 22.09.2025).
4. Satoshi N. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: <http://bitcoin.org> (дата звернення: 23.09.2025).
5. Chat GPT, URL: <https://chatgpt.com/> | Проведення графічного порівняння (Дата звернення: 24.09.2025)

УДК 004.056:316.77:351.861

Караетян О.М.

*к.е.н., доцент кафедри безпеки та правоохоронної діяльності
Західноукраїнський національний університет*

Караетян А.Е.

*здобувач ступеня доктора філософії
Західноукраїнський національний університет*

АКТУАЛЬНІ ЗАГРОЗИ ТРАНСФОРМАЦІЯМ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

У сучасних умовах глобалізації та динамічного розвитку цифрових технологій інформаційне середовище постає не лише як комунікаційний простір, але й як багатовимірна соціотехнічна система, яка визначає характер політичних, економічних та культурних процесів у світі. Його трансформації зумовлені інтенсивною цифровізацією управлінських практик, інтеграцією штучного інтелекту у процеси прийняття рішень, поширенням мережеских платформ, що перетворюють інформацію на стратегічний ресурс, а також зростанням залежності державних інституцій та приватних суб'єктів від

цифрових технологій. Водночас у цьому середовищі активізуються численні загрози, які мають поліструктурний і транскордонний характер, охоплюючи як технологічну, так і когнітивну площину.

Однією з найбільш актуальних проблем постають технологічні ризики, пов'язані з кібератаками на критичну інформаційну інфраструктуру, що охоплює енергетичні системи, фінансові ринки, транспортні мережі та комунікаційні вузли. З огляду на системоутворююче значення зазначених об'єктів, їх ураження може призвести до ефекту каскадного колапсу, що виводить з ладу життєво важливі для держави та суспільства механізми [1]. Стрімке впровадження технологій великих даних і алгоритмів машинного навчання створює одночасно додаткові інструменти аналізу та моніторингу, але й підвищує ризики використання цих технологій у злочинних чи терористичних цілях, зокрема для автоматизованого поширення дезінформації та підриву довіри до демократичних інституцій.

Політико-інформаційний вимір трансформацій інформаційного середовища акумулює у собі низку викликів, які мають системний та довготривалий характер. Сучасні інформаційні війни не обмежуються поширенням неправдивих повідомлень, а являють собою цілеспрямований комплекс заходів, спрямованих на підрив когнітивної та комунікативної резильєнтності суспільства [2]. Їхня структура охоплює багатовекторні інструменти: фабрикацію та мультиплікацію фейкових наративів, здійснення психологічних операцій у віртуальному просторі, використання технологій кіберпропаганди, спрямованих на створення альтернативної картини реальності, яка здатна конкурувати з об'єктивними фактами. В умовах тотальної медіатизації це призводить до так званого «ефекту симулякрів», коли штучно сконструйовані інформаційні конструкції починають сприйматися суспільством як первинна реальність [3].

Інформаційне середовище, таким чином, перетворюється на арену гібридних протистоянь, де інструменти «жорсткої сили» поступаються місцем технологіям «м'якого впливу», а інформація сама стає стратегічною зброєю. Особливо небезпечним є те, що зазначені впливи є латентними, тобто малопомітними для більшості громадян, однак водночас вони чинять руйнівний ефект на когнітивну стійкість, критичне мислення та колективну ідентичність населення. Маніпулятивні комунікативні практики підривають довіру до традиційних інститутів влади та суспільних авторитетів, провокують соціальну фрагментацію й радикалізацію окремих груп, що унеможливорює формування консолідованої громадської думки [4].

Наслідком цього процесу є дестабілізація політичних систем: ерозія легітимності державної влади, зростання протестної активності, делегітимація демократичних процедур та зниження рівня громадянської участі. Виникає парадоксальна ситуація, коли формально відкритий доступ до інформації не гарантує її об'єктивності, а інформаційне перевантаження перетворюється на чинник дезорієнтації суспільства. У цьому контексті можна стверджувати, що сучасні інформаційні війни – це не стільки боротьба за територію чи ресурси,

скільки змагання за контроль над свідомістю, установками й поведінкою масових аудиторій.

Не менш значущим є соціально-психологічний аспект. Постійний інформаційний тиск, цифрова залежність, перенасичення повідомленнями та агресивність віртуальних комунікацій створюють нові ризики для психоемоційної стійкості індивідів і колективів. Цифрова середовище сприяє поширенню когнітивних викривлень, зниженню рівня критичного мислення та посиленню інформаційної втоми, що робить суспільство більш вразливим до маніпулятивних технологій. Паралельно виникають феномени «інформаційної бульбашки» та «ефекту резонансу», які ізолюють індивідів у вузьких сегментах інформаційного поля та унеможлиблюють формування об'єктивної картини реальності [5].

Правовий та організаційний вимір трансформацій демонструє значне відставання від темпів технологічного прогресу. Національні законодавства часто не встигають адаптуватися до нових кіберзагроз, а міжнародне право залишається фрагментарним і неспроможним забезпечити уніфіковані стандарти кібербезпеки. Відсутність глобально узгоджених механізмів регулювання інформаційних потоків і захисту персональних даних призводить до асиметричності у спроможності різних держав протидіяти інформаційним загрозам. Водночас приватні транснаціональні корпорації, які контролюють значні сегменти інформаційного простору, фактично формують власні правила гри, що часто суперечать національним інтересам окремих країн.

Перспективи протидії актуальним загрозам трансформаціям інформаційного середовища полягають у виробленні комплексної стратегії, що поєднувала б технологічні, правові та гуманітарні інструменти. Йдеться про розвиток систем кіберрозвідки та моніторингу інформаційних потоків, інтеграцію когнітивно-поведінкових методів аналізу для виявлення маніпулятивного впливу, формування стійкої цифрової культури серед населення, яка ґрунтувалася б на критичному мисленні та медіаграмотності. Важливим є і налагодження міжнародної співпраці у сфері кібербезпеки, вироблення універсальних стандартів захисту інформації, а також імплементація інституційних механізмів контролю за діяльністю глобальних цифрових платформ.

Таким чином, трансформації інформаційного середовища мають амбівалентний характер: з одного боку, вони створюють безпрецедентні можливості для розвитку комунікацій, науки, економіки та культури, а з іншого – породжують комплекс загроз, які набувають технологічного, політичного, соціально-психологічного та нормативно-правового вимірів. Подолання цих викликів можливе лише на основі міждисциплінарного підходу, який забезпечить формування стійкої архітекτονіки інформаційної безпеки в умовах глобальних трансформацій.

Список використаних джерел:

1. Василенко В. А. Інформаційна безпека: правові та організаційні засади. К.: Юрінком Інтер, 2022. 356 с.

2. Nye J. The Future of Power in the Cyber Age. Oxford: Oxford University Press, 2021. 284 p.
3. Клімушин П. С. Кібербезпека та міжнародне право: сучасні підходи. Харків: Право, 2023. 412 с.
4. Castells M. The Rise of the Network Society. 2nd ed. Oxford: Blackwell, 2020. 597 p.
5. Черняк В. Інформаційна політика і гібридні війни: виклики для України // Науковий вісник. 2024. №2. С. 15–27.

УДК 303.4

Карапетян О.М.

к.е.н., доцент

Західноукраїнський національний університет

Коженцьовський Ю.В.

здобувач ступеня доктора філософії

Західноукраїнський національний університет

Рудий Р.В.

здобувач ступеня доктора філософії

Західноукраїнський національний університет

ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ В УМОВАХ ГЛОБАЛЬНИХ ВИКЛИКІВ: ЗАГРОЗИ, КІБЕРБЕЗПЕКА ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ

У контексті глобальної інформатизації та цифровізації суспільних процесів інформаційне середовище набуває статусу стратегічного ресурсу, від стійкості та захищеності якого залежить функціонування політичних інститутів, економічних механізмів, соціальних систем і культурних практик. Поступове проникнення інформаційно-комунікаційних технологій у всі сфери життєдіяльності людини зумовлює зростання вразливості соціуму перед новітніми загрозами, що виникають унаслідок трансформації традиційних форм злочинності та появи кіберпростору як автономної сфери реалізації протиправної діяльності. Сучасні деструктивні впливи характеризуються комплексністю та багатовимірністю: вони одночасно охоплюють технічні, організаційні, психологічні та правові виміри, що актуалізує потребу у формуванні системи кібербезпеки як невід'ємної складової національної безпеки [1].

До найбільш поширених загроз інформаційному середовищу належать: кібератаки на критичну інфраструктуру держави, що спрямовані на порушення стабільності енергетичних, фінансових, транспортних і комунікаційних систем; протиправне втручання в інформаційні ресурси органів державної влади та недержавних інституцій; поширення шкідливого програмного забезпечення

(зокрема програм-вимагачів, шпигунських комплексів і ботнетів), яке дозволяє здійснювати несанкціонований доступ до інформації, а також маніпулятивні інформаційні технології, що продукують дезінформацію, фейки, пропагандистські наративи й матеріали типу deepfake. Особливої небезпеки набуває поєднання технічних і когнітивних загроз, коли інструменти кіберпростору використовуються з метою впливу на масову свідомість, дестабілізації суспільно-політичної ситуації, руйнування довіри до державних інститутів [2].

У науковій та правозастосовній площині кібербезпека визначається як стан захищеності інформаційного середовища, який забезпечує його безперервність і надійність функціонування, здатність протидіяти внутрішнім і зовнішнім загрозам, а також гарантує недоторканність, конфіденційність і цілісність інформаційних ресурсів. У нормативно-правовій системі України цей інститут отримав закріплення у Законі «Про основні засади забезпечення кібербезпеки України» 2017 р., а також у Національній стратегії у сфері кібербезпеки. При цьому акцент робиться на принципах системності, комплексності, превентивності та міжнародної кооперації, що відображає глобальний характер сучасних кіберзагроз. В умовах гіперконектованого світу жодна держава не здатна самотійно протистояти організованій кіберзлочинності чи державним актам кібертероризму, тому міжнародно-правові механізми, зокрема Будапештська конвенція про кіберзлочинність, відіграють ключову роль у формуванні правового простору глобальної цифрової безпеки [3].

Захист інформації в умовах цифрових трансформацій виступає багаторівневим і поліфункціональним процесом, що поєднує правові, організаційні та технічні компоненти. Правовий рівень забезпечує нормативне закріплення режиму інформаційної безпеки, встановлює кримінальну відповідальність за кіберзлочини, визначає порядок обробки, зберігання та поширення інформації, у тому числі персональних даних [4]. Організаційний рівень охоплює діяльність суб'єктів забезпечення кібербезпеки, розроблення стратегій управління ризиками, проведення кібераудиту та підготовку кадрів. Технічний рівень передбачає використання криптографічних алгоритмів, багатофакторної автентифікації, систем резервного копіювання, інтелектуальних платформ моніторингу загроз і нейтралізації кібератак. У сучасних умовах особливого значення набуває інтеграція інноваційних технологій – штучного інтелекту, блокчейну, великих даних, квантових комунікацій – які одночасно виступають і потенційними інструментами забезпечення кіберзахисту, і джерелами новітніх ризиків.

Таким чином, інформаційне середовище виступає одночасно простором можливостей та уразливостей, а його безпека стає визначальною умовою стабільності держави й суспільства. Кіберзагрози мають міждисциплінарний характер, що потребує інтегрованих механізмів протидії, поєднання правових, технічних і соціально-комунікаційних інструментів [5]. Успішна реалізація політики кібербезпеки неможлива без міжнародної кооперації, адже глобалізований характер кіберзлочинності вимагає формування колективної

системи захисту. Водночас ключовим критерієм ефективності має бути не лише здатність до ліквідації наслідків кібератак, а й створення превентивного середовища, яке унеможливило б руйнівний вплив на інформаційну інфраструктуру [6]. Перспективи розвитку системи захисту інформації в Україні та світі визначатимуться рівнем адаптації до новітніх технологічних реалій, здатністю до міждержавної взаємодії та готовністю формувати високий рівень цифрової культури як базового чинника інформаційної безпеки.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45.
2. Конвенція про кіберзлочинність (Будапешт, 23.11.2001). Ратифікована Законом України від 07.09.2005 № 2824-IV.
3. Національна стратегія у сфері кібербезпеки України: Указ Президента України від 14.05.2021 № 447/2021.
4. Гуцалюк О. В., Баранов О. А. Кібербезпека як складова національної безпеки: сучасні виклики та перспективи. Науковий вісник публічного та приватного права. 2022. Вип. 4. С. 12–19.
5. Клімушин П. С. Інформаційна безпека: навч. посіб. Київ : Центр учбової літератури, 2021. 312 с.
6. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. New York : W. W. Norton & Company, 2018. 320 p.

УДК 004.67

Кравченко В.В.

здобувач вищої освіти,

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СИСТЕМИ ЗАХИЩЕНОГО ЗБЕРІГАННЯ Й ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

У сучасному цифровому суспільстві захищене зберігання та передавання інформації є одним з найважливіших аспектів функціонування інформаційних систем. Розвиток глобальних мереж, зростання кількості кіберзагроз, поширення електронної комерції, дистанційної освіти та медицини вимагають створення надійних засобів захисту даних. Програмне забезпечення, що працює з конфіденційними відомостями, повинно забезпечувати конфіденційність, цілісність, автентичність та доступність інформації, адже саме ці властивості визначають її безпечне використання.

Захищене зберігання інформації передбачає застосування методів шифрування, контроль доступу та захист від несанкціонованих змін.

Традиційно для цього використовуються криптографічні алгоритми симетричного й асиметричного шифрування, хеш-функції та електронні підписи. Наприклад, симетричні алгоритми AES чи ChaCha20 забезпечують високу швидкість шифрування даних на носіях, тоді як асиметричні методи RSA чи ECC застосовуються для керування ключами й автентифікації користувачів. Хеш-функції SHA-2 та SHA-3 широко використовуються для перевірки цілісності, а цифрові підписи дозволяють підтвердити авторство та неможливість відмови від дії.

При розробці програмного забезпечення для безпечного зберігання даних важливим є проектування архітектури, що враховує різні рівні безпеки. Система повинна передбачати шифрування не лише файлів, а й метаданих, журналів активності та резервних копій. Особливу увагу слід приділяти захисту ключів шифрування, оскільки компрометація ключа призводить до втрати всіх механізмів захисту. Для цього застосовують апаратні модулі безпеки (HSM), програмні сховища ключів або технології багатофакторної автентифікації.

Щодо захищеного передавання інформації, то основним стандартом виступають протоколи безпечного обміну даними. Найбільш поширеним є TLS, що використовується у веб-додатках для забезпечення захищеного з'єднання між клієнтом і сервером. Протокол TLS поєднує симетричне шифрування для швидкості та асиметричне – для безпеки. Окрім TLS, для спеціалізованих рішень застосовуються IPsec, SSH, VPN-тунелювання. Усі ці підходи дозволяють забезпечити не лише шифрування переданих даних, але й автентифікацію учасників комунікації та захист від атак типу «людина посередині».

Серед викликів, які постають при розробці програмного забезпечення, слід відзначити баланс між рівнем захисту та продуктивністю. Занадто складні алгоритми або надмірна кількість перевірок можуть уповільнити роботу системи та знизити зручність для користувачів. З іншого боку, спрощення механізмів безпеки призводить до вразливостей. Тому завдання розробників полягає у виборі оптимальних алгоритмів і методів, що враховують специфіку застосування системи. Наприклад, у хмарних сховищах використовуються технології шифрування на стороні клієнта, коли дані шифруються перед завантаженням, що гарантує конфіденційність навіть у випадку компрометації сервера.

Сучасні тенденції у сфері захищеного зберігання та передавання інформації передбачають активне використання блокчейн-технологій. Децентралізоване зберігання дозволяє виключити єдину точку відмови й підвищити стійкість системи до атак. Також усе більшого поширення набувають методи квантово-стійкої криптографії, що покликані захистити дані у майбутньому від атак з боку квантових комп'ютерів. Алгоритми, такі як CRYSTALS-Kyber чи Dilithium, розглядаються як перспективна основа для нових протоколів захищеного обміну даними.

У процесі розробки програмного забезпечення важливим є застосування методологій безпечної інженерії. Це означає інтеграцію механізмів захисту вже на ранніх етапах проектування системи. Використання моделей загроз, аналіз

ризиків та тестування на проникнення дозволяє своєчасно виявити слабкі місця. Додатково застосовуються методи безперервного моніторингу, що забезпечують оперативне виявлення атак і реагування на них.

Практична реалізація системи захищеного зберігання й передавання інформації буде включати клієнтське та серверне програмне забезпечення, засоби управління доступом, протоколи обміну ключами та механізми резервного копіювання. Наприклад, користувач завантажує файл, який автоматично шифрується у браузері або додатку, передається у зашифрованому вигляді до сервера та зберігається у базі даних, де метадані також зашифровані. Для доступу інший користувач проходить автентифікацію з багатофакторною перевіркою, після чого система передає йому дані у захищеному каналі.

Таким чином, дослідження та розробка програмного забезпечення для систем захищеного зберігання й передавання інформації є комплексним завданням, яке поєднує криптографію, системний аналіз, програмну інженерію та інформаційну безпеку. Висока якість реалізації таких рішень є критичною для захисту даних у бізнесі, державних структурах та повсякденному житті. Майбутнє розвитку цієї сфери пов'язане з поєднанням традиційних криптографічних методів з новітніми технологіями, включаючи блокчейн, штучний інтелект для моніторингу аномалій та квантово-стійкі алгоритми. Лише системний підхід до створення програмного забезпечення дозволить гарантувати належний рівень захищеності інформації в умовах постійного зростання кіберзагроз.

Список використаних джерел:

1. Остапов С. Е., Євсєєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів: «Новий Світ-2000», 2020. – 678 с.
2. Логачова Є., Єсіна М., Бобух В. Аналіз особливостей забезпечення кібербезпеки у банківських мобільних додатках // Комп'ютерні науки та кібербезпека. – 2023. – № 1. – С. 63-73.
3. Баляцька В., Опірський І. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну // Кібербезпека: освіта, наука, техніка. – 2023. – Том 4, № 20. С. 6-19.

Куліш Д. О.

курсант 2 курсу навчально-наукового інституту № 4
Харківського національного університету внутрішніх справ
<https://orcid.org/0009-0006-9458-9902>

Мойко О. О.

курсант 3 курсу навчально-наукового інституту № 4
Харківського національного університету внутрішніх справ
<https://orcid.org/0009-0000-3828-6196>

Борисова К. Є.

курсант 4 курсу навчально-наукового інституту № 4
Харківського національного університету внутрішніх справ
<https://orcid.org/0009-0006-6015-1304>

Науковий керівник

Каленіченко Л. І.

доктор юридичних наук, професор,
завідувач кафедри інформаційних систем та технологій
навчально-наукового інституту № 4
Харківського національного університету внутрішніх справ

ВПЛИВ OSINT-ДАНИХ НА ЕФЕКТИВНІСТЬ ФІШИНГОВИХ АТАК

Фішингові атаки залишаються одним із найпоширеніших векторів кіберзагроз у сучасному цифровому середовищі. За даними Anti-Phishing Working Group, у 2023 році було зафіксовано понад 5 мільйонів фішингових атак, що на 15% більше порівняно з попереднім роком [1]. Особливу увагу привертає тенденція до персоналізації атак за допомогою відкритих джерел інформації (OSINT), що дозволяє зловмисникам створювати більш переконливі та ефективні сценарії соціальної інженерії. Сучасні кіберзлочинці активно використовують доступну в мережі інформацію про потенційних жертв, включаючи дані з соціальних мереж, професійних платформ, публічних реєстрів та інших відкритих джерел, що значно підвищує ймовірність успіху їхніх атак. Таким чином, комплексний аналіз взаємозв'язку між сучасними фішинговими методами та використанням OSINT-даних для підвищення ефективності атак є актуальним напрямом дослідження для захисту персональних даних та розробки практичних рекомендацій щодо захисту від подібних загроз в умовах зростаючої доступності особистої інформації в цифровому просторі.

На наш погляд, такого роду комплексний аналіз потребує, по-перше, дослідження публічно доступних звітів про кібер-інциденти; наукових публікацій провідних експертів з кібербезпеки та власних спостережень за фішинговими кампаніями протягом 2022-2024 років. По-друге, визначення частоти використання різних типів OSINT-даних у фішингових атаках, а також успішності атак залежно від обсягу зібраної інформації про жертв. По-третє,

дослідження наявних інструментів та методів збору OSINT-даних, що використовуються як дослідниками безпеки, так і зловмисниками.

Фішингові атаки як і будь-яке явище, можна класифікувати за різними критеріями. Так, за ступенем використання OSINT-даних для здійснення фішингової атаки останні можна поділити на три основні категорії.

Масові атаки складають 75% від загальної кількості та використовують мінімальну кількість персональної інформації, отриманої переважно з публічних реєстрів та базових профілів соціальних мереж. Ці атаки характеризуються низькою ефективністю, але великим охопленням аудиторії [2].

Цільові атаки становлять 20% від загального обсягу та базуються на детальному OSINT-профілі конкретної жертви, включаючи професійну інформацію, особисті інтереси, соціальні зв'язки та поведінкові патерни [2].

Високо персоналізовані атаки, які складають лише 5% від усіх випадків, використовують комплексний OSINT-аналіз для створення надзвичайно переконливих сценаріїв, що імітують комунікацію з довіреними особами або організаціями [2].

Характерно, що під час фішингової атаки з використанням OSINT-даних зловмисниками активно використовуються чотири основні категорії джерел інформації.

Соціальні мережі займають провідне місце (45% використання) та включають Facebook, LinkedIn, Instagram, Twitter, які надають багату інформацію про особисті інтереси, професійну діяльність, родинні зв'язки, геолокацію та розклад щоденної активності користувачів [2].

Професійні платформи становлять 25% від загального обсягу джерел та охоплюють LinkedIn, корпоративні сайти, професійні форуми, які містять детальну інформацію про посади, колег, робочі проекти, бізнес-контакти та професійні досягнення [2].

Публічні реєстри (20%) включають відкриті бази даних державних установ, судові реєстри, реєстри нерухомості та підприємницької діяльності, що надають особисту, фінансову та юридичну інформацію [2].

Витоки даних становлять 10% та представлені інформацією з попередніх порушень безпеки різних сервісів, що потрапила у відкритий доступ і часто містить паролі, електронні адреси та особисті дані користувачів [2].

Сучасні зловмисники використовують широкий спектр технологій для збору та аналізу відкритих даних, поєднуючи автоматизовані інструменти з ручними методами дослідження. Серед найпоширеніших автоматизованих рішень виділяються Maltego для візуалізації зв'язків між об'єктами, the Harvester для збору електронних адрес та доменної інформації, Reconng для комплексної веб-розвідки, а також спеціалізовані скрипти для парсингу соціальних мереж [4]. Встановлено, що 60% успішних цільових фішингових атак використовували дані, зібрані з 3-5 різних джерел, що дозволяло створити детальний профіль жертви та підібрати найбільш ефективну тактику впливу. Особливу роль відіграє застосування машинного навчання для аналізу

поведінкових патернів та автоматичного генерування персоналізованого контенту на основі зібраної інформації [4].

Захист від OSINT-базованих фішингових атак, на наш погляд, повинен базуватися на використанні комплексного багаторівневого підходу до захисту.

Технічні заходи захисту від OSINT-базованих фішингових атак мають включати впровадження багатофакторної автентифікації для всіх критично важливих сервісів, використання сучасних anti-phishing фільтрів з можливостями машинного навчання, регулярне оновлення програмного забезпечення та операційних систем, а також налаштування систем моніторингу мережевого трафіку для виявлення підозрілої активності.

Організаційні заходи захисту від OSINT-базованих фішингових атак мають передбачати проведення регулярних тренінгів з кібербезпеки для всіх співробітників, розробку та впровадження корпоративних політик використання соціальних мереж, створення чітких процедур верифікації підозрілих запитів на надання конфіденційної інформації, а також формування культури кібербезпеки в організації.

Особисті заходи захисту від OSINT-базованих фішингових атак мають включати свідоме обмеження кількості особистої інформації, що розміщується в публічному доступі, правильне налаштування параметрів приватності в соціальних мережах, розвиток критичного мислення при аналізі отримуваних повідомлень та регулярний аудит власного цифрового сліду.

Отже, зловмисники активно використовують OSINT-дані під час фішингової атаки. Ефективність фішингової атаки прямо залежить від обсягу зібраних зловмисником OSINT-даних. Захист від OSINT-базованих фішингових атак повинен базуватися на використанні комплексного багаторівневого підходу до захисту.

Список використаних джерел:

1. Anti-Phishing Working Group. Phishing Activity Trends Report, Q4 2024 – 12 p.
2. Heartfield R., Loukas G. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks // *ACM Computing Surveys*. 2016. Vol. 48, No. 3. P. 1-39.
3. Алексеев М.О., Петренко С.І. Методи протидії фішинговим атакам в корпоративних мережах // *Кібербезпека: освіта, наука, техніка*. 2023. № 4(20). С. 15-28.
4. Sawyer B.D., Hancock P.A. Hacking the human: the prevalence paradox in cybersecurity // *Human Factors*. 2018. Vol. 60, No. 5. P. 597-609.
5. Грищук Р.В., Охрімчук В.В. Технології OSINT як інструмент кіберрозвідки: аналіз загроз та методи захисту // *Безпека інформації*. 2024. Т. 30, № 1. С. 44-52.

СПЕЦИФІКА ДОТРИМАННЯ ІНФОРМАЦІЙНОЇ ЕТИКИ В МЕЖАХ ДЕРЖАВНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вивчаючи інформаційну етику як прикладну науку, необхідно виокремити її актуальні питання, що вимагають свого вирішення:

- проблеми морального регулювання у мережі Інтернет, Інтернет-міфи;
- питання, що виникають у сфері використання комп'ютерної технології;
- етичні аспекти досліджень у сфері медицини та біології;
- етичне регулювання діяльності засобів;
- етичні питання у сфері бібліотечного та інформаційного обслуговування;
- морально-нормативне регулювання в інформаційному бізнес-середовищі

[1; 2].

В аналізованій теорії завдання інформаційної етики не мають такого глобального характеру, але в той же час вони відрізняються високим ступенем конкретності, що дозволяє ясно уявити можливі методологічні рішення їх реалізації. У зв'язку з цим можна визначити наступне коло питань, яке підлягає вивченню:

- вирішення проблем у галузі комп'ютерної технології;
- завдання морального регулювання в глобальній мережі та етичні аспекти діяльності фахівців, які використовують у своїй професійній практиці інформаційні технології (ЗМІ, медицина, бібліотечне обслуговування тощо).

Отже, розглянувши актуальні проблеми теорії інформаційної етики, слід їх узагальнити. Так, класифікація завдань інформаційної етики виглядає так:

- вирішення проблем у сфері використання комп'ютерних технологій;
- вирішення етичних та соціальних проблем у кіберпросторі чи глобальній мережі;
- вивчення питань моральної відповідальності спеціалістів родинних професій (бібліотекарів, журналістів тощо) [2; 3].

Наведені вище проблеми інформаційно-етичного характеру насамперед пов'язані з відсутністю ясного уявлення про етичні обмеження використання сучасних технологій, а також з нерозумінням вибору необхідних дій суспільством та людиною у наданні нових можливостей.

Щодо першого розділу проблем у сфері комп'ютерних технологій варто сказати, що вивченням та аналізом соціального й етичного впливу комп'ютерних технологій на всі сфери суспільного життя займається комп'ютерна етика – галузь дослідження, що вивчає моральні питання, пов'язані з процесом розробки, застосування та використання комп'ютерів.

Сьогодні термін «комп'ютерна етика» використовують у професійній етиці комп'ютерних фахівців, керованих етичними кодексами всередині своєї

професії. Комп'ютерна етика розглядає вплив комп'ютерної та інформаційної технології на цінності людини, використовуючи концепції з філософії, соціології, публічного управління, права, психології тощо.

Що стосується розділу етичних та соціальних проблем у кіберпросторі або глобальній мережі, важливо зазначити, що, починаючи з моменту виникнення та вирішення зазначених питань, сформувалися такі напрямки, що займаються етичними дослідженнями в галузі регулювання людської поведінки в середовищі Інтернет: інтернет-етика, мережева етика, кіберетика, нетикет, віртуальна етика. Внаслідок цього фахівці стали говорити про низку проблем терміносистеми та кодифікування у сфері етичного регулювання застосування інформаційних технологій, які потребують значного ступеня уточнення.

Зокрема, віртуальна етика пов'язана з осмисленням проблем Інтернет-комунікацій. Розглядаючи глобальну мережу Інтернет як соціальний електронний простір, фахівці виділяють її багатофункціональність. Насамперед це масштабне комунікаційне поле, що складається з власної реальності: розваги, ділове середовище, віртуальні спільноти, інтернет-міфи та інтернет-конфлікти, а також соціальні, креативні та асоціальні наслідки віртуальних ігор, що звідси впливають.

Кіберетика покликана регулювати поведінку людини в інформаційному світі. Кіберетику також називають Інтернет-етикою, тобто областю прикладної етики, що вивчає етичні питання та моральні дилеми, пов'язані з появою цифрових технологій та глобального віртуального середовища, зокрема: проблеми конфіденційності, точності та доступності інформації, захисту інтелектуальної власності, безпеки даних та цифрової нерівності [1–3].

Список використаних джерел:

1. Гуржій А. М., Овчарук О. В. Дискусійні аспекти інформаційно-комунікаційної компетентності: міжнародні підходи та українські перспективи. *Інформаційні технології в освіті*. 2018. № 3. С. 38.
2. Панченко О. А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект. Київ : КВІЦ, 2020. 331 с.
3. Савосько Т. Особливості формування державної інформаційної політики. *Аспекти публічного управління*. 2024. № 12(1). С. 22–28.

Легойда Ю.В.

здобувач вищої освіти,

навчально-науковий Фізико-технічний інститут, КПІ імені Ігоря

Сікорського

Наукові керівники

Стьопочкіна І.В.

к.т.н., доцент, доцент кафедри інформаційної безпеки,

Навчально-науковий Фізико-технічний інститут, КПІ імені Ігоря

Сікорського

Кривуля Є.К.

с.н.с., Український науково-дослідний інститут спеціальної техніки та

судових експертиз

ОЦІНКА СТІЙКОСТІ ІОТ-СИСТЕМИ УПРАВЛІННЯ НАСОСОМ ДО DOS-АТАК

Актуальність. Сучасний розвиток цифрових технологій неможливо уявити без використання Інтернету речей (IoT), який дедалі активніше впроваджується у сферу критичної інфраструктури. В Україні приклади впровадження IoT у критичну інфраструктуру вже демонструють свою ефективність. Приклади пошкодження гідротехнічних споруд [1], затоплень або перебоїв у роботі насосних станцій свідчать про необхідність дослідження не лише ефективності таких систем, а й їхньої стійкості до кіберзагроз. Компанія використовувала рішення з управління водою Арапа [2], що працює на мережі LPWAN, для обладнання своїх закладів батарейними датчиками IoT. Датчики здійснювали моніторинг потоку та тиску в трубопроводах, передаючи дані щохвилини.

Існуючі рішення. В роботі [3] запропоновано класифікацію трафіку для виявлення атак на IoT мережі, в роботі [4] показано аспекти апаратної безпеки IoT пристроїв, робота [5] підкреслює основні загрози та вразливості IoT-пристроїв, зокрема через обмеженість ресурсів, що дозволяє показати, що проблема безпеки IoT вже актуальна й у національному контексті. На відміну від існуючих рішень, які свідчать про актуальність проблеми, дана робота присвячена оцінці ефекту DoS-атак на доступність та стабільність роботи насосної системи.

Мета та постановка задачі. Незважаючи на наявні дослідження щодо виявлення DoS/DDoS-атак та апаратної безпеки IoT-пристроїв, більшість робіт зосереджені на теоретичних моделях або аналізі мережевого трафіку. Практичне експериментальне тестування стійкості конкретних IoT-систем управління насосними станціями до DoS-атак наразі недостатньо висвітлене. Метою даного дослідження є експериментальна оцінка стійкості IoT-системи управління насосом (Arduino+Blynk) до DoS-атак. Для досягнення поставленої мети були визначені наступні завдання: 1) розробка та налаштування лабораторного стенда, що імітує систему водопостачання; 2) проведення серії експериментів з

DoS-атаками на систему; 3) оцінка впливу атак на ключові параметри системи (час відгуку, стабільність роботи); 4) формулювання практичних рекомендацій щодо підвищення стійкості подібних систем.

Експеримент. Для проведення експериментального дослідження була розроблена лабораторна установка, що імітує систему управління насосною станцією водопостачання. Установка складається з наступних ключових компонентів: 1) Arduino Uno з платою розширення ESP8266 для підключення до мережі Wi-Fi. Arduino відповідає за збір даних із сенсорів та керування насосом, тоді як ESP8266 забезпечує мережевий зв'язок; 2) мотор, який імітує насос, підключений до контролера через релейний модуль. Реле дозволяє Arduino комутувати живлення мотора. 3) Ультразвуковий датчик HC-SR04, що вимірює відстань до поверхні води у резервуарі. 4) LCD-дисплей, який відображає поточний рівень води та стан насоса (увімкнено/вимкнено), а також світлодіоди, що візуально сигналізують про стан системи (наприклад, стан роботи насоса чи наявність зв'язку). Ці компоненти були зібрані на макетній платі для зручності тестування та налагодження. Вся система працювала від зовнішнього джерела живлення.

Платформа Blynk була використана як хмарний сервіс для моніторингу та управління системою. Blynk забезпечує віддалене керування насосом, візуалізацію даних з датчика та надсилання сповіщень. Для DoS-атак використовувався сервер Blynk. Для генерації потоку DoS-запитів застосовувався спеціалізований скрипт, написаний мовою Python. Скрипт імітував велику кількість запитів до API-сервера Blynk з метою перевірки стійкості системи до навантаження.

Результати. Практичний експеримент дозволив виявити залежності, показані на рис. 1. На ньому наведено розподіл часу відгуку (Latency) для різних сценаріїв атак. Сценарії відрізнялися інтенсивністю згенерованих запитів у секунду. Можна побачити, що в більшості випадків затримка становить 27–29 мс, хоча у базовому сценарії вона іноді була нижчою. Розподіли для сценаріїв 1, 2 та 3 подібні між собою, що свідчить про відносну стабільність часу відгуку навіть при збільшенні навантаження.

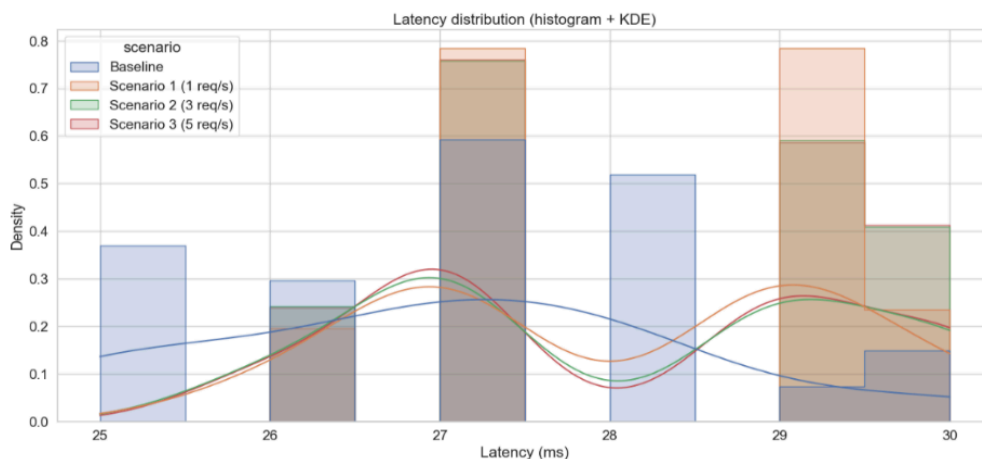


Рис.1. Гістограма з оцінкою щільності ймовірності (KDE) для різних сценаріїв навантаження

Це пояснюється тим, що на серверах Blynk Cloud присутній вбудований механізм rate-limiting – механізм, який контролює кількість запитів, що користувач або пристрій може надсилати до сервера чи API за певний проміжок часу. Його основна мета – захист від перевантаження та зловмисних атак, зокрема DoS/DDoS. Хмарна платформа Blynk, яку ми використовуємо, застосовує rate limiting, щоб обмежити кількість запитів до нашого пристрою на одиницю часу. Таким чином, навіть якщо ми надсилаємо надмірну кількість запитів, як під час DoS-атаки, хмара бере на себе "удар", ставлячи запити в чергу або відхиляючи їх, що дозволяє кінцевому пристрою, в нашому випадку – нашій системі, залишатися працездатним і не перевантажуватися

Висновки. Висока стійкість до DoS-атаки в обумовлена не стійкістю самого ESP8266, а вбудованими механізмами захисту на серверах Blynk Cloud. Вони ефективно обмежують частоту запитів (rate-limiting) і ставлять їх у чергу, не дозволяючи потоку даних перевантажити кінцевий пристрій. Було визначено показники End-to-End Latency (~140 мс) – повний час, який відчуває користувач, та Local Latency (~30 мс) – час, який пристрій витрачає на обробку команди. Ця різниця показує, що основний час затримки припадає на передачу даних по мережі, а не на обробку на мікроконтролері. Проведене дослідження показало, що навіть проста IoT-система на базі ESP8266, що використовує професійну хмарну платформу, може бути стійкою до базових DoS-атак. Для підвищення надійності таких систем найефективнішим є використання захищених, професійно керованих платформ.

Список використаних джерел:

1. Destruction of the Kakhovka Dam. URL: https://en.wikipedia.org/wiki/Destruction_of_the_Kakhovka_Dam
2. LoRa-based IoT solution from Semtech ‘saves Costco 22% in water management’. URL: <https://www.iot-now.com/2018/09/19/88361-lora-based-iot-solution-semtech-saves-costco-22-water-management/>
3. Hardware security overview of fog computing end devices in the internet of things. URL: <https://journals.uran.ua/itssi/article/view/277306/272053/>
4. Analysis of security problems of IoT devices. URL: <https://eir.kntu.net.ua/jspui/>
5. Detecting DoS/DDoS attacks in IoT using machine learning. URL: <https://ela.kpi.ua/items/c2895013-56f1-4695-8be9-32c3e2dd93fc/>

Лєвкіна А.Р.,

Янчук С.М.

здобувачі фахової передвищої освіти

Харківський комп'ютерний фаховий коледж

Науковий керівник:

Ахмедзянова О.А.

викладач вищої категорії

Харківський комп'ютерний фаховий коледж

ЗАХИСТ ІНФОРМАЦІЇ. МЕТОДИ ШИФРУВАННЯ

У сучасному цифровому середовищі, де обмін інформацією відбувається щосекунди, питання захисту даних набуває особливої актуальності. Зловмисники постійно вдосконалюють свої методи атак, тому лише фізичного контролю за інформацією вже недостатньо. Одним із найефективніших способів убезпечення конфіденційних даних є використання різних методів шифрування.

Методи шифрування поділяються на симетричні та асиметричні. Симетричне шифрування передбачає застосування одного ключа для кодування й розшифрування інформації, що робить його швидким і зручним у роботі з великими обсягами даних. Асиметричне шифрування, натомість, базується на парі ключів – відкритому та закритому, що значно підвищує рівень безпеки під час передавання інформації в мережі.

Крім того, активно застосовуються гібридні методи, які поєднують швидкодію симетричних алгоритмів із надійністю асиметричних.

Розглянемо кожний з методів більш детально:

1. Симетричне шифрування - як і впливає з назви, цей метод використовує один криптографічний ключ для шифрування і дешифрування даних. Використання одного ключа для обох операцій робить процес простим.

Найбільш видатною особливістю симетричного шифрування є простота процесу, так як використовується один ключ як для шифрування, так і для дешифрування. Там, де необхідно зашифрувати великий шматок даних, симетричне шифрування виявляється відмінним варіантом.

Деякі типи симетричного шифрування:

- DES-алгоритм симетричного шифрування(Включає в себе 16 циклів різних процесів – таких як розширення, перестановка, заміна або інші операції – через які будуть проходити дані в зашифрованому вигляді.);
- Алгоритм симетричного шифрування 3DES;
- Blowfish(Він пропонує високу швидкість і гнучкість, але AES замінив його використання в багатьох програмах.).

2. Асиметричне шифрування, на відміну від симетричного, включає в себе кілька ключів для шифрування і дешифрування даних, які математично пов'язані один з одним. Один з цих ключів відомий як «відкритий ключ», а

інший – як «закритий ключ». Асиметричний метод шифрування також відомий як «криптографія з відкритим ключем».

Якщо брати ту саму ситуацію про дівчат, то для асиметричного шифрування кожна з них має мати дві пари ключів:

- відкритий ключ – його можна давати всім, хто хоче надіслати зашифроване повідомлення,
- закритий ключ – зберігається у таємниці й використовується лише для розшифрування.

Перша (і найбільш очевидна) перевага цього типу шифрування – безпека, яку він забезпечує.

Друга важлива особливість, яку пропонує асиметричне шифрування, – це аутентифікація. Як ми бачили, дані, зашифровані за допомогою відкритого ключа, можуть бути розшифровані тільки за допомогою закритого ключа, пов'язаного з ним.

Основні типи асиметричного шифрування:

- Алгоритм асиметричного шифрування RSA;
- Алгоритм асиметричного шифрування ECC.

3. Гібридні методи поєднують два підходи: асиметричне і симетричне. Асиметричне використовується для безпечної передачі ключа, а симетричне – для швидкого обміну даними. Такий метод забезпечує одночасно безпеку та високу швидкість і застосовується у більшості сучасних протоколів, наприклад у HTTPS.

4. Квантове шифрування – це новітня технологія, яка використовує кубіти та закони квантової фізики для передачі даних. Вона практично неможлива для злому, тому що будь-яка спроба перехоплення інформації одразу стає помітною.

5. Стеганографія – це метод приховування самого факту передачі даних, а не лише їх шифрування. За допомогою стеганографії повідомлення можна вбудувати в інші файли, наприклад у зображення, аудіо чи відео, так що сторонній навіть не помітить, що інформація передається. Це дозволяє обмінюватися даними приховано, без привертання уваги.

Технології захисту даних від Kingston:

Компанія Kingston понад 35 років спеціалізується на виробництві пристроїв для зберігання даних і є одним із лідерів у цій сфері. Вона пропонує різноманітні рішення для захисту та зберігання інформації:

- Швидкі SSD та оперативну пам'ять – забезпечують високу продуктивність і надійність при роботі з великими обсягами даних.
- USB-накопичувачі та карти пам'яті – компактні та зручні для щоденного використання, з можливістю зберігати та переносити інформацію.
- Шифровані накопичувачі – спеціальні пристрої, які захищають дані навіть у разі втрати або крадіжки пристрою, забезпечуючи безпеку конфіденційної інформації.
- Продукція Kingston підходить як для звичайних користувачів, так і для бізнесу та дата-центрів, гарантуючи надійне зберігання даних та багаторівневий захист від несанкціонованого доступу.

Список використаних джерел

1. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються? [Електронний ресурс] Режим доступу: <https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/>
2. Симетричне та асиметричне шифрування. [Електронний ресурс] Режим доступу: <https://academy.binance.com/uk-UA/articles/symmetric-vs-asymmetric-encryption>
3. Види шифрування інформації. [Електронний ресурс] Режим доступу: <https://ua5.org/protect/395-vidi-shifruvannya-informaciyi.html>

УДК 004.056.53

Логунів О.С.

здобувач вищої освіти,

Навчально-науковий інститут №4

Харківський національний університет внутрішніх справ

Науковий керівник

Тімошин А. С.

к. ф.-м. н.,

доцент кафедри інформаційних систем та технологій ННІ № 4

Харківського національного університету внутрішніх справ

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ У ВІРТУАЛЬНИХ ТА ДОПОВНЕНИХ СЕРЕДОВИЩАХ (VR/AR)

Віртуальні та доповнені реальності (VR/AR) набувають широкого поширення в Україні в освіті, медицині, промисловості та обороні, проте їхнє впровадження супроводжується суттєвими ризиками для інформаційної безпеки. Системи VR/AR постійно збирають великі обсяги персональних даних користувачів, зокрема рухи тіла, позицію, голос, погляд, біометричні показники та взаємодію з об'єктами [1]. Недостатній захист цих даних створює ризики несанкціонованого використання, витоку або маніпуляцій. Пристрої та програмне забезпечення VR/AR уразливі до атак шкідливого програмного забезпечення, перехоплення даних та несанкціонованого доступу [2].

Однією з проблем є фішинг та соціальна інженерія у віртуальних середовищах. Користувачі можуть опинитися у підроблених VR/AR програмах або тренувальних сценаріях, що імітують реальні ситуації, що дозволяє зловмисникам отримати доступ до персональних даних або корпоративних систем [3].

Окрім цього, тривале перебування у віртуальному середовищі може призвести до психологічної залежності, стресу та порушень сприйняття реальності. Маніпуляції віртуальними об'єктами здатні формувати у користувачів хибні уявлення, що робить VR/AR середовища не лише

технологічним, а й соціально-психологічним викликом.

В Україні VR/AR активно використовуються для створення віртуальних лабораторій у вищих навчальних закладах, для тренувань хірургів та реабілітації пацієнтів у медичних установах, а також для підготовки фахівців у моделюванні різних професійних ситуацій. Наприклад, Український стартап Aspichi (та інші компанії) використовує VR-технології для психологічної допомоги та реабілітації, в тому числі для ветеранів та постраждалих від війни, створюючи заспокійливі віртуальні середовища. Водночас опитування серед студентів та медичних працівників показало, що більшість користувачів не використовують багатофакторну автентифікацію для захисту VR-пристроїв та не володіють достатньою інформацією про ризики витоку даних у VR/AR системах. Це підкреслює необхідність комплексного підходу до захисту: поєднання технічних рішень, організаційних заходів та навчання користувачів [4].

Для підвищення безпеки у VR/AR середовищах рекомендовано використовувати сучасні технології шифрування даних, багатофакторну автентифікацію, системи контролю доступу та регулярне оновлення програмного забезпечення. Крім того, важливо інтегрувати моніторинг потенційних загроз та механізми швидкого реагування на інциденти безпеки. Використання VR/AR у промисловості та медицині потребує особливої уваги, адже будь-який витік інформації може призвести до економічних збитків або шкоди репутації організацій [5].

Серед додаткових викликів варто відзначити взаємодію VR/AR із зовнішніми IoT-пристроями та мережами, що створює додаткові точки уразливості для кібератак. Водночас використання VR/AR для навчання та тренувань наочно показує їхній потенціал у підвищенні ефективності підготовки спеціалістів, але підкреслює необхідність суворого контролю безпеки.

Забезпечення інформаційної безпеки у VR/AR середовищах є критично важливим для безпечного та ефективного використання технологій у навчанні, медицині, промисловості та професійній підготовці. Комплексний підхід до захисту інформації дозволяє мінімізувати ризики для користувачів і даних, забезпечуючи стійкість систем навіть у випадках потенційних кіберзагроз.

Подальші дослідження у сфері інформаційної безпеки VR/AR повинні бути спрямовані на розробку методів виявлення аномальної поведінки користувачів та систем у реальному часі з використанням інструментів штучного інтелекту. Це дозволить не лише фіксувати факти кібератак чи витоку даних, але й прогнозувати потенційні загрози ще на етапі їхнього формування. Такий підхід відкриває перспективу створення адаптивних систем кіберзахисту, здатних самонавчатися й підвищувати власну ефективність у динамічних VR/AR середовищах.

Список використаних джерел:

1. Гриценко І., Тарасов А., Руденко О. Методи підвищення безпеки та стійкості VR-систем. Матеріали CEUR Workshop Proceedings, 2024. – Т. 3675. – С. 182–192. – <https://ceur-ws.org/Vol-3675/paper21.pdf>
2. Дутта Р., Сінг С. Виявлення аномалій у бездротових мережах віртуальної реальності. Міжнародний журнал комунікаційних мереж і розподілених систем, 2023. – Т. 31, № 2. – С. 145–159. – https://www.researchgate.net/publication/374197234_Anomaly_Detection_in_Virtual_Reality_Wireless_Networks
3. Kaspersky. Які ризики для безпеки та приватності у VR та AR. – 2023. – <https://www.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr>
4. Digital Experience. Ризики безпеки VR та AR: що потрібно знати. – 2024. – <https://www.digitalexperience.live/vr-ar-security-risks-what-you-need-know>
5. Шевченко О. О., Іванова І. В. Безпека персональних даних у віртуальних та доповнених реальностях: виклики та шляхи вирішення. Інформаційна безпека та кіберзахист, 2024, 12(3), с. 45–58.

УДК 004.42 : 004.056 : 004.89

*Лук'яненко С.В.,
здобувач вищої освіти другого (магістерського) рівня,
Державний податковий університет
Науковий керівник
Погорєловська І. Д.,
к.е.н., доцент, доцент кафедри
комп'ютерних та інформаційних технологій і систем
Державний податковий університет
м.Ірпінь, Україна*

НАПРЯМИ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ СИСТЕМИ УПРАВЛІННЯ SMART- БУДИНКОМ

Стрімкий розвиток технологій «розумного будинку» призводить до зростання кількості IoT-пристроїв (Інтернет речей), що взаємодіють між собою та з користувачами. Водночас, збільшення кількості підключених елементів породжує нові загрози інформаційній безпеці, зокрема це можуть бути:

- перехоплення та модифікація даних (MITM (man-in-the-middle) – «людина посередині»)[2];
- відтворення перехоплених команд (Replay-атаки (повторні атаки)[6];
- несанкціонований доступ до пристроїв через слабкі налаштування авторизації [4];

- підбір паролів або ключів доступу (Bruteforce-атаки - атаки перебором)[6];
- атаки на слабко захищені протоколи тощо[1].

Зазначені проблеми зумовили необхідність дослідження відкритих стандартів безпеки, зокрема рекомендацій OWASP IoT Project [4], криптографічних підходів, викладених у [5], та практик безпечної інтеграції IoT-пристроїв у мережеве середовище [2].

За результатами дослідження, вважаємо, що для підвищення рівня захищеності системи управління «розумним будинком» доцільним є:

- використання Spring Security та Keycloak для автентифікації та авторизації користувачів [5, 3];
- застосування OAuth2/OIDC з токенами доступу JWT [5];
- шифрування даних у каналах TLS (Transport Layer Security) [5];
- контроль доступу на рівні брокера MQTT за допомогою ACL (Access Control List)[1];
- журналювання подій та аудит безпеки в PostgreSQL [4].

Запропонована архітектура системи (рис. 1) доводить можливість створення безпечного середовища управління розумним будинком засобами з екосистеми Java.

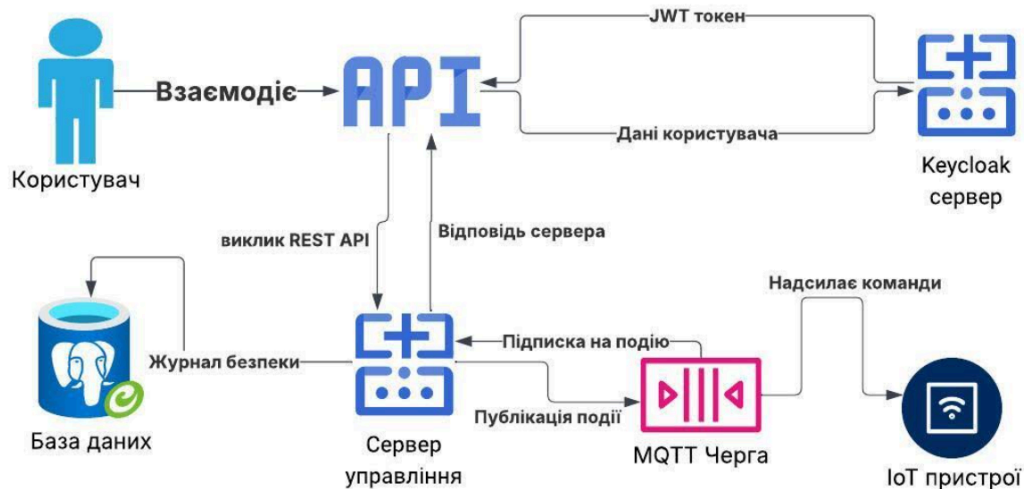


Рис. 1. Архітектура системи управління «розумним будинком»
розроблено автором

Реалізація механізмів аутентифікації, авторизації, шифрування та аудиту дозволить значно знизити ризики несанкціонованого доступу. Використання ПЗ з відкритим кодом дозволить мінімізувати вартість розробки подібних систем.

Подальші дослідження передбачають масштабування системи для керування великою кількістю пристроїв та інтеграцію з хмарними сервісами.

Список використаних джерел:

1. Eclipse Foundation. MQTT – The Standard for IoT Messaging. [Online]. URL: <https://mqtt.org>

2. Fernandes, E., Jung, J., & Prakash, A. (2016). Security Analysis of Emerging Smart Home Applications. IEEE S&P.
3. Keycloak Documentation. URL: <https://www.keycloak.org/documentation>
4. OWASP IoT Project – Internet of Things Security Guidance. URL: <https://owasp.org/www-project-internet-of-things>
5. Spring Security Documentation. URL: <https://spring.io/projects/spring-security>
6. Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson, 2022

УДК 316.776

Лучик В.Є.

*доктор економічних наук,
професор кафедри протидії кіберзлочинності інституту № 4
Харківського національного університету внутрішніх справ
orcid.org/0000-0001-6007-910X*

Маловажна А.Р.

Руденко М.А.

*курсанти 2 курсу інституту № 4
Харківського національного університету внутрішніх справ*

ФЕЙКОВІ НОВИНИ ТА ДЕЗІНФОРМАЦІЯ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

В Україні слово «фейк» лунає майже з кожного інформаційного ресурсу, воно собою являє свідомий збір та оприлюднення неправдивих даних та інформації. В умовах цифрового розвитку інформація – це не лише певні відомості для загального сприйняття, а й засіб впливу на свідомість людей, їхню поведінку, поштовх до прийняття рішень.

У ході російсько-української війни фейки стали боротьбою наративів та культур. Найпоширенішими пропагандистськими твердженнями є «українці-бандерівці», «звільнення від націоналістів». Дезінформацію використовують для погіршення відносин між людьми, підризу довіри до держави та формування паніки серед населення.

Дезінформація – це оманлива інформація, що використовується для маніпуляцій, заради політичних, економічних та інших вигод. За формою її поділяють:

фейкові новини – повністю неправдиві дані, що імітують журналістський стиль, але повністю базуються на неправдивій інформації;

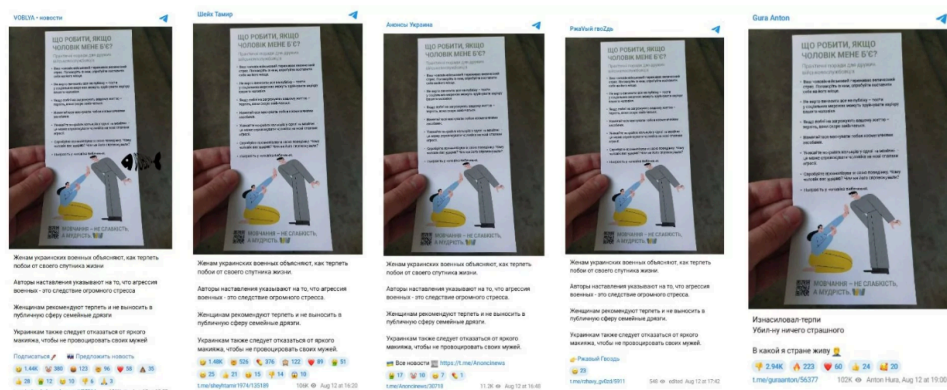
пропаганда – постійне поширення інформації з метою впливу на емоції читача;

маніпуляції – публікація справжньої інформації, але не в повному обсязі для створення хибного враження

фейкові документи – підроблені офіційні папери, скриншоти, або листи; візуальні матеріали – змінені зображення або відео, використання застарілих фото та подача їх, як нових;

бот-мережі – використання масового поширення повідомлень, аби створити ілюзію «суспільної думки».

Цей маніпулятивний метод і є загрозою національній безпеці. Наприклад, у серпні 2025 року російські ЗМІ почали опубліковувати інформацію з написом: «Дружинам українських військовослужбовців роздають пам’ятки з порадами, як терпіти побої» (рис. 1); обізнані люди легко можуть розрізнити, що цей фейк, адже в самій пам’ятці слово «побої» написано російською мовою, перейшовши по QR-коду, читача автоматично перенаправляє на офіційний сайт громадського руху «Жіноча сила України», на якому відразу з’являється повідомлення, що ці пам’ятки розроблені не членами громадського руху і вони є поширенням фейкової інформації.



«Дружинам українських військових пояснюють, як терпіти побої від свого супутника життя. Автори повчання вказують на те, що агресія військових — це наслідок величезного стресу. Жінкам рекомендують терпіти і не виносити у публічну сферу сімейні чвари. Українкам також слід відмовитись від яскравого макіяжу, щоб не провокувати своїх чоловіків», — йдеться у дописах.

Рис. 1. Фейк «Дружинам українських військовослужбовців роздають пам’ятки з порадами, як терпіти побої»

Це повідомлення створено з метою інформаційно-психологічного впливу: воно мало дискредитувати українських військовослужбовців, посіяти недовіру та підірвати авторитет громадських організацій. Його поширювали через проросійські телеграм-канали. Використання соцмереж пояснюється тим, що вони на сьогоднішній день є одним з основних джерел отримання новин для населення. Згідно з дослідженням Громадської мережі «Опора», 73,4% українців дізнаються інформацію із соціальних платформ (рис. 2):

Telegram 78,1%;

YouTube 59,5%;

Facebook 44,6%.

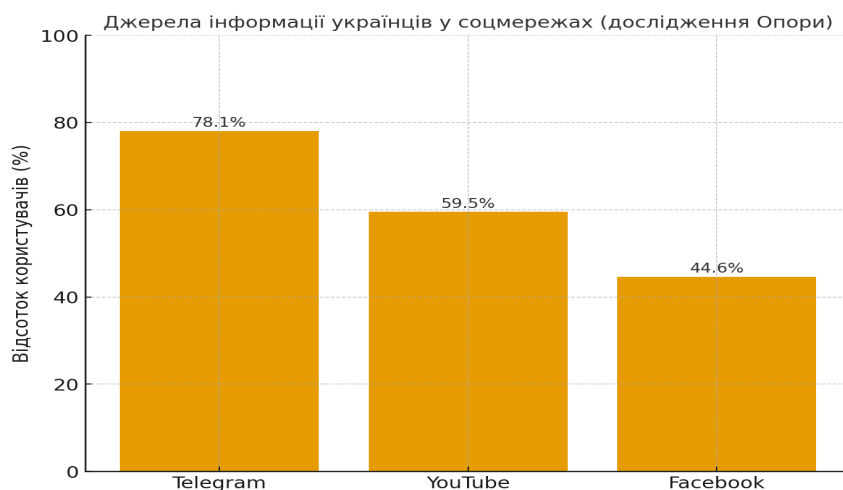


Рис. 2. Джерела інформації у соцмережах

Таким чином, саме ці платформи стають ключовими каналами впливу на громадську думку, де поширення неправдивої інформації може найшвидше масштабуватися та мати безпосередній вплив на громадську думку і суспільно-політичну стабільність країни в цілому. Особливого поширення таке явище набуває у складний для кожної країни період (політична чи економічна криза, період війни).

Отже, для підвищення національної безпеки у протидії фейків та дезінформації потрібно розвивати медіаграмотність населення, створювати механізми для швидкого спростування шейків. Адже лише спільними зусиллями держави та населення можна мінімізувати вплив дезінформації й зміцнити стійкість до інформаційних атак.

Список використаних джерел

1. Вовк В.М. *Filosofs'ki ta metodologični problemi prava*. 2022. № 2 (24) *Філософські та методологічні проблеми права «Фейки як загроза національній безпеці в умовах гібридної війни»* (дата звернення: 23.09.2025).
2. Калитич М.М. *«ФЕЙКОВІ НОВИНИ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ»* Львів -2025 (дата звернення: 21.09.2025).
3. Мазуренко Л.І. вісник Харківського національного університету імені В. Н. Каразіна *«Інформаційна безпека в умовах російсько-української війни: виклики та загрози»* (дата звернення: 24.09.2025).
4. Chat GPT, URL: <https://chatgpt.com/> | Проведення графічного порівняння (Дата звернення: 25.09.2025)

Ляшенко А.С.,

Куліуш Д.О.,

Мойко О.О.,

здобувачі вищої освіти,

Навчально-науковий інститут №4

Харківський національний університет внутрішніх справ

Науковий керівник

Мальцев В.В.

Викладач кафедри протидії кіберзлочинності

Навчально-науковий інститут №4

Харківський національний університет внутрішніх справ

КІБЕРБУЛІНГ: МЕХАНІЗМИ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ ПОЛІЦІЇ

В реаліях сьогодення цифрові технології пронизують усі сфери життя – від спілкування й освіти до практичної більшості позицій на ринку праці. Одночасно зростає й кількість нових ризиків серед яких окреме місце посідає кібербулінг. В даному контексті мова йде не просто про грубі жарти чи незначні конфлікти в інтернеті, а про цілеспрямоване тривале переслідування людини за допомогою цифрових каналів. Проблема ускладнюється тим, що віртуальний простір фактично не має ані територіальних, ані часових обмежень. Жертва може цілодобово отримувати образливі повідомлення, а аудиторія таких дій потенційно необмежена. За даними CERT-UA, лише у 2023 році в Україні зафіксували суттєве зростання таких інцидентів що підтверджує критичність проблеми та нагальну потребу в комплексних заходах реагування [1].

Правоохоронні органи в даному контексті виступають головним гарантом захисту. Поліція виконує функцію не лише виявлення й фіксації фактів цифрового цькування, але й створення умов для ефективної превенції таких випадків. Це охоплює певну кількість векторів: моніторинг інформаційного простору, кваліфікацію правопорушень, роботу з доказами, взаємодію з освітніми закладами та навіть міжнародну співпрацю. В такому контексті науковці регулярно наголошують на необхідності модернізації правоохоронних структур та їх технічного та кадрового оновлення ефективно протидіяти такому явищу неможливо [2]. Одним із найсерйозніших викликів на цьому шляху є анонімність порушників. Зловмисники користуються фейковими акаунтами, шифрованими месенджерами, VPN-сервісами й іншими технологіями що ускладнюють їх ідентифікацію. У відповідь правоохоронці застосовують інструментарій цифрової криміналістики: від ретельного аналізу мережевого трафіку до відстеження зв'язків між акаунтами.

Для підвищення ефективності роботи поліції особливе значення має впровадження чітких стандартів захисту інформації, що дозволяє не лише систематично обробляти цифрові інциденти але й підвищує ефективність реагування на кіберзлочини, зменшує ризик втрати або спотворення доказів та

забезпечує високий рівень організації роботи правоохоронців у сфері кібербезпеки [3]. Проте важливою частиною діяльності поліції є й профілактика потенційно небезпечних інцидентів. Важливо, щоб громадяни могли ідентифікувати ознаки кібербулінгу та правильно фіксувати факти агресії (знімки екрана, посилання, позначки часу) та знали куди звернутись за допомогою. З метою реалізації цієї мети поліцейські активно проводять зустрічі у школах, університетах, організовують онлайн-кампанії. За наявними даними такі програми дійсно зменшують кількість інцидентів, оскільки жертви починають ефективно та своєчасно реагувати. Подібні ініціативи перегукуються з підходами, описаними в дослідженнях із інформаційного менеджменту, де підкреслюється значення алгоритмізації процесів реагування [4].

Також важливо розглянути юридичний компонент питання. В Україні булінг складає зміст адміністративного правопорушення за статтею 173-4 КУпАП. А у випадку якщо булінг призведе до тяжких наслідків, як самогубство, то це може бути кваліфіковано за ст. 120 ККУ. У цьому контексті перед поліцією стоїть завдання не лише оперативно реагувати, але й якісно зібрати доказову базу. Дослідники у сфері права також зазначають розмитість законодавчих норм і відставання правової бази від реалій цифрового середовища, що становить суттєву перешкоду в роботі правоохоронців [5].

Не можна обійти увагою й кадровий аспект. Сучасний поліцейський повинен отримати необхідні цифрові компетентності, тому правоохоронці проходять спеціалізоване навчання. Зокрема, велику роль відіграють міжнародні освітні програми, такі як Cisco Networking Academy які дозволяють українським фахівцям отримати доступ до найновіших практик кіберзахисту [6]. Що дозволяє ефективніше протидіяти складним цифровим проявам кіберзлочинності. Водночас варто розуміти, що жодна країна не зможе самотужки боротися з явищем, яке часто виходить за межі національних кордонів. Більшість популярних платформ і сервісів розташовані в інших юрисдикціях і поліція не може отримати до них доступ без міжнародної правової допомоги. Саме тут вагоме значення має Будапештська конвенція Ради Європи про кіберзлочинність. Цей документ закріплює єдині підходи до розслідування кіберзлочинів та створює механізми для обміну інформацією між державами [7].

Окрім виявлення та запобігання кібербулінгу важливою складовою є психологічна підтримка постраждалих. Жертви цифрового цькування часто переживають стрес, тривогу та ізоляцію, що може негативно впливати на їхнє навчання, роботу та соціальні взаємодії. Тому правоохоронці співпрацюють із психологами та соціальними службами, організовують консультації та гарячі лінії, де постраждалі можуть отримати фахову допомогу. Такий підхід дозволяє не лише мінімізувати наслідки кібербулінгу, а й підвищує ефективність реагування правоохоронців, адже люди, які отримали підтримку, легше надають достовірні свідчення та співпрацюють у розслідуванні.

Отже, сучасна поліція у протидії кібербулінгу поєднує одразу кілька функцій: каральну, профілактичну, освітню й міжнародну. Тільки синергія цих напрямів може забезпечити реальний захист громадян у цифровому середовищі.

Правоохоронці виступають не лише як орган примусу, але й як партнер суспільства, що допомагає формувати безпечний інформаційний простір, у якому права людини й цифрова безпека перебувають у гармонійному балансі.

Список використаних джерел

1. CERT-UA. Звіт про діяльність у сфері кіберзахисту за 2023 рік. URL: <https://cert.gov.ua> (дата звернення: 25.09.2025).
2. Петров О. І. Кібербезпека: основи захисту інформації. Київ: Наукова думка, 2021. – 312 с.
3. Стандарти захисту інформації в інформаційно-телекомунікаційних системах правоохоронних органів : метод. рек. Харків : ХНУВС, 2022. 38 с.
4. Кобилін А. М., Самородов Б. В. Інформаційний менеджмент : навч. посібник. Львів : Новий Світ – 2000, 2014. 216 с.
5. Єфименко О. Правові аспекти кваліфікації кібербулінгу в Україні. Юридичний вісник. 2022. № 4. С. 61–72.
6. Cisco Networking Academy. URL: <https://www.netacad.com/> (дата звернення: 25.09.2025).
7. Convention on Cybercrime (Budapest Convention) : міжнародний договір Ради Європи від 23.11.2001. Council of Europe Treaty Office. URL: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

УДК 004.056.5:342.951

Макеєв В. В.,
здобувач вищої освіти,
Миколаївський національний аграрний університет
Пархоменко О. Ю.
кандидат фізико-математичних наук,
доцент кафедри економічної кібернетики,
комп'ютерних наук та інформаційних технологій
Миколаївського національного аграрного університету

ЗАХИСТ І ЗБІР ДАНИХ КОРИСТУВАЧІВ У ЦИФРОВІЙ ЕКОНОМІЦІ ЯК ПРОБЛЕМА ПОШУКУ БАЛАНСУ

Сучасна цифрова економіка ґрунтується на масштабному зборі та аналізі даних користувачів, що є джерелом економічної ефективності, але одночасно породжує серйозні загрози конфіденційності, безпеки та автономії особистості. Метою даного дослідження є аналіз суперечності між економічною доцільністю збору персональних даних і необхідністю забезпечення їхнього належного захисту. У дослідженні розглядаються сучасні методи збору даних, основні загрози, правові механізми захисту (зокрема GDPR, CCPA та українське законодавство), а також етична дилема когнітивного дисонансу у поведінці користувачів.

Інформація про онлайн активність користувачів є основою для функціонування бізнес-моделей технологічних корпорацій. Кожна активність користувача в онлайн середовищі стає джерелом цінної інформації. Її найпоширеніше використання це таргетована реклама, адже вона дозволяє фахівцям демонструвати саме такі оголошення, які підходять до тієї чи іншої категорії споживачів. Така персоналізація значно збільшує прибуток для більшості цифрових платформ.

Засобів для збору існує багато, але можна виділити декілька базових інструментів. Файли cookie, що зберігаються в браузері, вміщують в себе інформацію про користувача. Від історії відвіданих вебсайтів до його купівельних звичок. У тандемі з ними працюють трекінг-пкселі. Вони відправляють інформацію про відвідування сторінки або сайту. Коли піксель спрацьовує, він може асоціювати подію (наприклад, перегляд товару на сайті) з унікальним ідентифікатором cookie, що дозволяє створювати детальні профілі поведінки користувача. З них, методи збору інформації розвинулися до глибокого поведінкового та психологічного профілювання. Таргетинг перестає бути лише інструментом для аналізу аудиторії за свідомо наданими даними. Тепер це складний механізм, який досліджує, як і чим користувач живе, базуючись на його цифровому відбитку. Ця зміна лежить в основі всіх подальших проблем, оскільки вона перетворює таргетовану рекламу з маркетингового інструменту на потенційний механізм маніпуляції та втрати контролю над особистою інформацією [1].

Так як зараз більшість компаній переходять або розширюються у цифрове середовище, захист персональних даних стикається з численними загрозами. Масштаби збору інформації збільшуються, а методи розвиваються. Значна частина інформації агрегується не лише великими технологічними платформами, а й спеціалізованими компаніями, відомими як брокери даних. Вони збирають і продають дані третім сторонам, беручи їх з різноманітних джерел, як і публічних так і приватних. Масштабний збір та агрегація даних, вочевидь, збільшує шанс на кібератаки і недбале поводження. Дослідження показують зростання кількості витоків і обсягу скомпрометованих даних. Наприклад за перший квартал 2024 року у всьому світі було зафіксовано 9478 інцидентів витоків, які призвели до компрометації понад 35,9 млрд записів. Прикладом великого витоку є інцидент у квітні 2024 року в AT&T Inc., коли внаслідок збою безпеки було скомпрометовано дані 7,6 млн нинішніх та 65,4 млн колишніх абонентів [2]. Окрім прямих витоків та маніпуляцій із великими масивами даних, деякі цифрові сервіси створюють загрозу алгоритмічної упередженості. Вона виникає коли алгоритми ШІ ненавмисно посилюють існуючі упередження, наявні в даних, щодо користувачів. Таке явище вже має великий вплив на суспільну думку та інформаційне середовище. Рекомендаційні алгоритми YouTube, згідно з дослідженнями Mozilla Foundation, часто просувають радикальний або емоційний контент. Аналогічно, Facebook у 2020 році визнав, що його алгоритм «рекомендованих груп» сприяв поширенню контенту, який розпалював ненависть та поляризацію.

Отже, як відповідь на зростаючі ризики, уряди різних і організації почали розроблювати жорсткі правові регламенти. Одним із найвпливовіших є Загальний регламент захисту даних (GDPR) Європейського Союзу [3], який набув чинності 25 травня 2018 року. Регламент встановлює обмеження для обробників даних, незалежно від їх місцезнаходження, якщо вони працюють з даними жителями ЄС. GDPR вимагає явної, інформованої та активної згоди користувача на обробку його даних. Суб'єкти даних також мають право на доступ до своїх даних, виправлення і видалення. У США, навпроти, захист даних регулюється на рівні окремих штатів, з Каліфорнією як лідером, де діє Закон про захист приватності споживачів Каліфорнії (CCPA) [4]. Головна відмінність CCPA від GDPR це право на заборону продажу своїх даних третім особам. ЄС використовує модель «opt-in», тобто забороняє збір при відсутності згоди. США працює за «opt-out», де компанії завжди збирають дані, а користувач дозволяє їх продаж або забороняє. В даному порівнянні помітна різниця між превентивним захистом та правом споживача на вибір.

В Україні правове регулювання захисту персональних даних базується на Законі «Про захист персональних даних» № 2297-VI від 2010 року [5]. Закон частково схожий на GDPR, також визначаючи основні принципи, права суб'єктів і обов'язки володільців даних. Але загалом українське законодавство має слабші механізми контролю та санкцій. Наприклад штрафи за порушення низькі порівняно з ЄС, що є менш суттєвим впливом на великі компанії. Також вплив даний закон має, вочевидь, тільки в Україні, на відміну від міжнародного GDPR. З іншого боку така гнучкість дає більше простору у зборі даних для компаній

Попри існування суворих правових регламентів, що дають користувачам контроль над їхніми даними, багато хто все ще добровільно погоджується на їх збір. Це створює етичну дилему. Основною причиною такої поведінки є бажання отримати безкоштовний доступ до онлайн-сервісів, які фінансуються саме за рахунок монетизації даних. З одного боку споживачі бажають персоналізації, а з іншого стурбовані конфіденційністю. Різні поведінкові дослідження показують, що користувачі загалом надають перевагу таргетованій рекламі перед нетаргетованою, оскільки вона надає більш корисну та релевантну інформацію. Особливо схвально сприймається реклама, яка пропонує фінансову вигоду, наприклад, знижки. Однак негативні реакції виникають, коли реклама стає нав'язливою, повторюваною або створює відчуття слідкування та вразливості, що демонструє небажання користувачів віддавати повний контроль над своєю інформацією. Ця ситуація демонструє когнітивний дисонанс у поведінці користувачів. Вони цінують зручність і переваги, які надають персоналізовані послуги, але водночас усвідомлюють та побоюються ризиків, пов'язаних із втратою приватності.

Таргетована реклама, що є рушійною силою сучасної цифрової економіки, водночас породжує системні загрози, які виходять за межі приватності та зачіпають питання безпеки, демократії та соціальної справедливості. Правові регламенти, такі як GDPR та CCPA, стали ефективною відповіддю, надавши користувачам реальні права та встановивши значні санкції для корпорацій.

Однак, як показує досвід, самі по собі закони не можуть вирішити проблему без згоди суспільства, що досі перебуває в стані когнітивного дисонансу між бажанням зручності та усвідомленням ризиків.

Список використаних джерел:

1. Кияниця Є. Контент і таргетинг – основні елементи новітньої медіалогії. *Наукові праці Міжрегіональної Академії управління персоналом. Філологія*. 2021. № 1. С. 63–67. URL: <https://doi.org/10.32689/maup.philol.2021.1.10>.
2. Global Data Breaches and Cyber Attacks in 2024 – IT Governance Blog. *IT Governance Blog*. URL: <https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024> (дата звернення: 27.09.2025).
3. Загальний регламент про захист даних (GDPR). *Регламент (ЄС) 2016/679: Загальний регламент про захист даних (GDPR). Керівні принципи, претензія та експертні коментарі*. URL: <https://www.gdpr.org.ua/> (дата звернення: 27.09.2025).
4. California Consumer Privacy Act (CCPA). *State of California – Department of Justice – Office of the Attorney General*. URL: <https://oag.ca.gov/privacy/ccpa> (дата звернення: 27.09.2025).
5. Про захист персональних даних. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 27.09.2025).
6. Lim S., Oh J. Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. *IET Information Security*. 2025. Vol. 2025, no. 1. URL: <https://doi.org/10.1049/ise2/5536763>.

УДК 004.8:004.056

Мірошниченко М.Ю.

*к.т.н., доцент, доцент кафедри комп'ютерних наук
Таврійський державний агротехнологічний університет
імені Дмитра Моторного*

ШЛЯХИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Захист інформаційних систем від несанкціонованого втручання є одним з важливих питань сучасного цифрового середовища. Це пояснюється тим, що більшість процесів у державному управлінні, економіці, науковій сфері базуються на обробці та зберіганні великих обсягів даних. Зростання кількості інформаційних онлайн ресурсів, активне використання хмарних технологій та їх інтеграція в глобальні віртуальні мережі підвищують рівень уразливості інформаційних систем до різноманітних загроз. Кожного дня фахівці з кібербезпеки зустрічаються з випадками віртуального шахрайства, кіберзлочинністю, витоками даних (персональними та корпоративними),

шкідливим програмним забезпеченням тощо. Водночас, ефективна стратегія захисту інформаційних систем вимагає комплексного підходу, який поєднує технічні, організаційні та нормативно-правові заходи, здатні забезпечити безперервність функціонування, конфіденційність та цілісність інформації [2, с. 128].

Основні шляхи забезпечення безпеки інформаційних систем можна представити у вигляді таблиці 1.

Таблиця 1.

Основні шляхи захисту інформаційних систем

Напрямок захисту	Метод / Засіб	Опис	Об'єкт застосування
Технічний	Багаторівневий контроль доступу	Автентифікація користувачів, розмежування прав доступу, моніторинг дій користувачів	Корпоративні інформаційні системи, державні портали
Технічний	Криптографія	Шифрування даних при передаванні та зберіганні, використання цифрового підпису	Хмарні сервіси, банківські системи, електронний документообіг
Організаційний	Політики безпеки	Регламентування правил роботи з даними, процедури реагування на небезпечні інциденти	Державні установи, великі підприємства
Організаційний	Навчання персоналу	Кібергігієна, обізнаність щодо онлайн шахрайства, керування паролями	Заклади освіти, установи та підприємства
Технологічний	Штучний інтелект і машинне навчання	Автоматичне виявлення аномалій, прогнозування атак, реагування у реальному часі	Кіберцентри, аналітичні системи великих підприємств
Соціальний / Освітній	Розвиток цифрової грамотності	Інструктажі з безпечної роботи у віртуальному середовищі	Освітні програми, тренінги для громадян

Коротко розглянемо кожний за наведених вище напрямків.

Інформаційні системи піддаються численним загрозам, які мають як зовнішнє, так і внутрішнє походження. Одним із основних механізмів їх захисту є багаторівнева система контролю доступу, що передбачає автентифікацію користувачів, розмежування прав, моніторинг дій та ведення журналів безпеки [5, с. 103]. Використання криптографічних методів дозволяє забезпечити конфіденційність даних під час передавання та зберігання, а також захищає інформаційні ресурси від несанкціонованого доступу до внутрішніх модулів. Регулярне оновлення програмного забезпечення, встановлення патчів, періодичне тестування інформаційних систем на наявність уразливостей є обов'язковими складовими кібергігієнічних заходів.

Останнім часом досить ефективним напрямком у сфері захисту інформаційних систем є використання інноваційних технологій. Штучний інтелект і методи машинного навчання дозволяють в автоматичному режимі виявляти аномальні дії, прогнозувати потенційні загрози та оперативно реагувати на кіберінциденти. Використання хмарних та розподілених систем із високим рівнем шифрування забезпечує не лише безпеку даних, а й масштабованість, гнучкість та доступність послуг для користувачів [1, с. 81]. Приклади успішного впровадження таких рішень можна спостерігати у роботі державних цифрових платформ, корпоративних інформаційних систем великих підприємств, що дозволяють ефективно управляти ресурсами та забезпечують безперервне функціонування навіть в умовах надзвичайних ситуацій. Захищені інформаційні системи дозволяють забезпечити безперервність бізнес-процесів, зменшити фінансові втрати внаслідок кібератак, підвищити довіру партнерів і клієнтів, а також сприяти розвитку інноваційних продуктів і послуг.

Слід також уникати «суб'єктивних» факторів. Як наслідок, розбудова безпечної та стійкої цифрової інфраструктури включає модернізацію апаратних і програмних компонентів інформаційних систем, підготовку висококваліфікованих фахівців у сфері кібербезпеки, а також забезпечення рівного доступу громадян до електронних сервісів та освітніх ресурсів [4, с. 32]. А розробка політик безпеки, навчання персоналу та формування інформаційної культури сприяють зменшенню ризиків та підвищують загальну стійкість інформаційних систем.

Захист інформаційних систем також передбачає інтеграцію технічних та правових заходів. Нормативно-правове регулювання у цій сфері визначає правила обробки та зберігання персональних і корпоративних даних, встановлює відповідальність за порушення інформаційної безпеки та регламентує процедури реагування на інциденти. Для нашої країни, що активно інтегрується у глобальний цифровий простір, це є досить актуальним завданням. Адже відповідність міжнародним стандартам кібербезпеки стає передумовою участі у глобальних економічних, наукових і освітніх проєктах.

Важливим аспектом цифрової трансформації є соціальна відповідальність користувачів у сфері інформаційної безпеки. Відсутність правдивої інформації про можливості інформаційних систем та сервісів, поширення дезінформації можуть негативно впливати на довіру користувачів до цифрових сервісів. Тому формування навичок критичного мислення та цифрової грамотності є важливим напрямком забезпечення захисту інформаційних систем. Освітні програми, тренінги та вебіари на відповідні теми сприяють підвищенню обізнаності громадян щодо кіберзагроз, надають можливість опанувати ефективними способами захисту персональних даних та безпечної взаємодії з цифровими платформами [3, с. 165].

Отже, шляхи захисту інформаційних систем мають комплексний характер, об'єднуючи технічні, організаційні, освітні та правові підходи. Ефективна реалізація цих заходів забезпечує не лише стійкість інформаційних систем до зовнішніх і внутрішніх загроз, а й створює передумови для подальшого розвитку цифрової інфраструктури, підвищення конкурентоспроможності

економіки та інтеграції України у міжнародний цифровий простір. Системний підхід до кіберзахисту, включно з інноваційними технологіями, підготовкою фахівців та формуванням цифрової культури користувачів, надає можливість забезпечити безпеку інформаційних систем та сталий розвиток суспільства в умовах активної цифровізації.

Список використаних джерел:

1. Колмакова В. О., Шаров С. В. Використання МВОК для формування імунітету від інформаційних загроз. *Українські студії в європейському контексті*. 2023. № 6. С. 80–87.
2. Коцюк Ю. А. Роль людського чинника у питаннях захисту інформаційних систем. *Наукові записки Національного університету Острозька академія. Серія: Психологія і педагогіка*. 2012. № 20. С. 128–138.
3. Марущак А. І. Інформаційні ресурси держави: зміст та проблема захисту. *Правова інформатика*. 2009. № 1.21. С. 65–71.
4. Носулич М. В. Захист персональних даних в інформаційних системах методом знеособлення. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення*. 2021. Вип. 4. С. 31–34.
5. Хомета Т. М. Задачі захисту соціальних інформаційних систем. *Моделювання та інформаційні технології*. 2015. № 75. С. 103–111.

УДК 004.8:331.101

Нагірна О.В.,

*к.е.н., доцент, доцент кафедри менеджменту
та економічної безпеки Львівського державного
університету внутрішніх справ*

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ПРОФЕСІЙНИЙ РОЗВИТОК: ВИКЛИКИ Й УПРАВЛІННЯ В СУЧАСНОМУ ОФІСІ

Інформаційне середовище в умовах цифрової доби постає ключовим ресурсом функціонування сучасного офісу, адже саме інформація забезпечує ефективність управлінських процесів, прийняття рішень та стратегічний розвиток організації. Доступ до актуальних даних, швидкий обмін повідомленнями та збереження корпоративних знань формують основу конкурентоспроможності бізнесу. Інформаційна інфраструктура стає не лише інструментом діяльності, але й чинником, що визначає рівень організаційної культури та професійної взаємодії в колективі. Таким чином, інформаційне середовище інтегрує технологічні та людські ресурси, забезпечуючи стійкість і результативність офісних процесів.

Водночас цифрова доба породжує низку загроз, які ставлять під сумнів надійність та безпеку інформаційного середовища. Найпоширенішими з них є кібератаки, що можуть паралізувати роботу установи або призвести до втрати

критично важливих даних; поширення фейкового контенту, здатного маніпулювати громадською думкою й викривляти управлінські рішення; а також витоки конфіденційної інформації, які загрожують як фінансовими збитками, так і репутаційними втратами.

Людський фактор у системі інформаційної безпеки посідає центральне місце, адже навіть найдосконаліші технічні засоби не можуть гарантувати повного захисту від загроз без належної культури поведінки з інформацією. Працівники офісу щоденно взаємодіють із цифровими системами, обробляють дані та приймають управлінські рішення, тому їхня обізнаність та відповідальність безпосередньо впливають на рівень захищеності організації. Низький рівень цифрової грамотності, нехтування правилами безпеки чи відсутність критичного мислення стають передумовами для виникнення інформаційних інцидентів.

В узагальненому розумінні інформаційна безпека охоплює комплекс засобів та методів, що забезпечують захист інформації та підтримку її інфраструктури від умисного або випадкового впливу, що може призвести до збитків для власника даних – держави, бізнесу або фізичних осіб. Основні принципи інформаційної безпеки включають:

- цілісність даних – гарантує збереження первісного формату та структури інформації під час її зберігання та передачі. Зміни або видалення інформації можливі лише власником або особами з офіційним доступом;
- конфіденційність – забезпечує доступ до інформації виключно тим користувачам, які пройшли ідентифікацію та мають відповідні права у системі;
- доступність – інформація повинна бути своєчасно та безперешкодно доступна користувачам, які мають на це право;
- достовірність – підтверджує, що інформація належить певному власнику, який є її джерелом [2].

Процеси цифровізації та глобалізації підкреслюють актуальність проблем інформаційної безпеки на державному рівні. У сучасному світі, де домінують інтернет, інновації та єдиний глобальний інформаційний простір, обсяги даних зростають надзвичайно швидко, що ускладнює їх контроль та управління. Це, у свою чергу, створює додаткові виклики для протидії загрозам та забезпечення стабільності внутрішньополітичної й соціальної ситуації в країні. В таких умовах розробка ефективних технологій захисту від ворожих втручань набуває першочергового значення [1].

Кібербезпека та захист інформації є фундаментальними умовами функціонування сучасних організацій, оскільки забезпечують цілісність, доступність та конфіденційність даних. До основних технічних заходів належать використання антивірусного програмного забезпечення, впровадження брандмауерів для контролю мережевого трафіку, регулярне резервне копіювання даних та застосування захищених каналів зв'язку. Сукупність цих інструментів створює багаторівневу систему, що мінімізує ризики несанкціонованого доступу та знижує вірогідність втрати критично важливої інформації. Водночас технічні рішення потребують постійного оновлення та модернізації, оскільки кіберзагрози швидко еволюціонують.

Не менш значущими є організаційні заходи, які формують поведінкові та управлінські стандарти в колективі. Серед них особливе місце посідає розробка політик інформаційної безпеки, чітке регламентування прав доступу до ресурсів та систем, а також регулярне навчання персоналу щодо правил безпечної роботи з даними. Важливо підкреслити, що людський фактор залишається найбільш вразливою ланкою у сфері кіберзахисту: необачні дії співробітників, помилки чи нехтування інструкціями часто стають причиною серйозних інцидентів. Отже, підвищення рівня цифрової грамотності та формування корпоративної культури інформаційної безпеки є ключовими передумовами ефективного захисту інформаційного середовища.

В умовах цифрової епохи офіс-менеджмент набуває нових характеристик, адже сучасний офіс функціонує на перетині людських ресурсів і технологічних рішень. Роль офіс-менеджера значно розширюється: він виступає не лише організатором внутрішніх процесів, але й координатором між співробітниками та цифровими системами, що забезпечують ефективність комунікацій і документообігу. Від компетентності офіс-менеджера залежить гармонійне поєднання адміністративних завдань, інформаційної безпеки та психологічного клімату в колективі.

Тренінги з інформаційної безпеки є ключовим інструментом формування у працівників знань і навичок, необхідних для захисту корпоративних ресурсів. Вони сприяють підвищенню рівня цифрової грамотності, роз'яснюють принципи безпечної роботи з електронною поштою, документами та онлайн-сервісами, а також формують навички розпізнавання потенційних кіберзагроз. Завдяки інтерактивним методам навчання співробітники мають змогу відпрацьовувати практичні сценарії, пов'язані з виявленням фішингових повідомлень, створенням надійних паролів чи реагуванням на інформаційні інциденти.

Сучасний офіс функціонує як комплексна система, де технологічні інструменти та людський фактор взаємодіють на щоденній основі. Ефективне управління інформаційною безпекою неможливе без розуміння потреб та поведінки співробітників, адже саме люди є ключовим елементом у запобіганні загрозам та підтриманні стабільної роботи організації.

Інвестиції у професійний розвиток персоналу та сучасні технології створюють синергію, яка забезпечує конкурентоспроможність компанії. Майбутнє офісів належить організаціям, які одночасно впроваджують інновації та формують культуру безпеки, адже гармонійне поєднання знань, навичок та технологій є основою стійкого розвитку та ефективного управління ризиками.

Список використаних джерел

1. Бакалінська О., Бакалінський О. Правове забезпечення кібербезпеки в Україні. Підприємництво, господарство і право. 2019. № 9. С. 100–108.
2. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. Київ : «Гельветика», 2017. 168 с.

*Наконечна Н.В.,
к.е.н., доцент, доцент кафедри безпеки
інформаційних технологій
НУ “Львівська політехніка”*

СТРАХУВАННЯ КІБЕРРИЗИКІВ В УКРАЇНІ

Кіберстрахування можна визначити як специфічний різновид страхових послуг, спрямованих на мінімізацію ризиків, пов'язаних із кіберзагрозами. Його ключове завдання полягає у наданні захисту від негативних наслідків хакерських атак, викрадення конфіденційної інформації, поширення шкідливого програмного забезпечення та інших проявів кіберзлочинності. Значення цього виду страхування зростає, адже зловмисники постійно шукають нові способи доступу до персональних і корпоративних даних, які мають високу цінність. За відсутності відповідного захисту як компанії, так і окремі користувачі можуть стати мішенню для кіберінцидентів, що призведе до витоку інформації, серйозних фінансових втрат та репутаційних ризиків.

Упродовж останніх років спостерігається помітне зростання кількості кіберризиків, які становлять небезпеку як для бізнес-структур, так і для окремих користувачів.

Під кіберризиком розуміють ймовірність виникнення подій, що негативно впливають на функціонування інформаційних систем та рівень кіберзахищеності організації внаслідок зовнішнього втручання у цифрові чи інші електронні технології. Такі події можуть спричиняти фінансові збитки, пошкодження цифрових активів і навіть репутаційні втрати для установи [1].

Основними видами кіберризиків є:

- технічні ризики – пов'язані з несправністю або вразливістю апаратного та програмного забезпечення, що може призвести до збоїв у роботі систем.
- організаційні ризики – виникають через недоліки у внутрішніх політиках безпеки, неналежний контроль доступу чи відсутність належного управління даними.
- людський фактор – ризики, що виникають через помилки персоналу, нехтування правилами безпеки чи зловмисні дії співробітників.
- зовнішні загрози – атаки хакерів, шкідливе програмне забезпечення, фішинг, DDoS-атаки та інші дії третіх осіб, спрямовані на отримання доступу до даних чи блокування систем.
- фінансові ризики – втрати, пов'язані з викраденням коштів, шахрайськими операціями чи витратами на відновлення після кіберінцидентів.
- правові ризики – можливі штрафи, санкції або судові позови у випадку порушення законодавства у сфері захисту персональних даних чи кібербезпеки.

- репутаційні ризики – шкода іміджу організації, втрата довіри клієнтів і партнерів через витoki інформації чи публічне розголошення інцидентів.

- стратегічні ризики – довгострокові негативні наслідки, які можуть вплинути на конкурентоспроможність компанії та її розвиток.

Сучасний ринок страхових послуг поступово адаптується до нових викликів цифрової епохи, пропонуючи компаніям різні напрями кіберстрахування, що дають можливість мінімізувати фінансові та організаційні наслідки кіберінцидентів.

Напрямами кіберстрахування у контексті основних видів кіберризиків є:

- Страхування технічних ризиків. Поліси можуть покривати витрати на відновлення IT-інфраструктури, ремонт обладнання чи відновлення програмних систем після кіберінцидентів.

- Страхування організаційних ризиків. Передбачає відшкодування витрат на впровадження нових засобів захисту, аудит систем безпеки, а також компенсацію збитків через помилки у внутрішніх процедурах управління інформацією.

- Страхування людського фактора. Дає змогу компанії отримати компенсацію у випадках, коли шкода завдана внаслідок недбалості співробітників, внутрішніх витоків інформації чи зловмисних дій персоналу. Захист від зовнішніх атак. Передбачає покриття витрат, пов'язаних із хакерськими вторгненнями, фішингом, шкідливим ПЗ, DDoS-атаками та іншими кіберзагрозами.

- Фінансове кіберстрахування. Спрямоване на компенсацію прямих грошових втрат: викрадення коштів, шахрайські операції, витрати на відновлення бізнес-процесів та виплату компенсацій клієнтам.

- Правове кіберстрахування. Охоплює витрати на судові процеси, штрафи за порушення законодавства у сфері захисту персональних даних та інші юридичні зобов'язання, що можуть виникнути після інциденту.

- Страхування репутаційних ризиків. Включає витрати на PR-кампанії, відновлення довіри клієнтів та підтримку позитивного іміджу компанії після оприлюднення фактів про витік чи кібератаку.

- Стратегічне кіберстрахування. Має на меті забезпечити довгострокову стійкість організації, зокрема шляхом покриття витрат на реструктуризацію бізнес-моделі, модернізацію систем безпеки та збереження конкурентних позицій.

Після хвилі масштабних кібератак, що вразили український бізнес та державні установи впродовж останнього року, все більше підприємців почали замислюватися над інструментами захисту від подібних загроз. Хоча кіберстрахування поки що не набуло широкого поширення на українському страховому ринку й суттєво відстає від світових тенденцій, представники страхових компаній відзначають наявність попиту на цей продукт. Найбільший інтерес, за їхніми спостереженнями, виявляють ті організації, які оперують великими масивами даних та зберігають значні обсяги конфіденційної інформації [2].

Розвиток сегмента кіберстрахування здатний позитивно позначитися й на суміжних напрямках, передусім на галузі інформаційної безпеки та кіберзахисту загалом.

Головною тенденцією у формуванні ринку страхування кіберризиків в Україні є поступове зростання інтересу до таких послуг. Організації та компанії, які найбільше наражаються на небезпеку кібератак, активно шукають дієві механізми захисту власних інформаційних ресурсів. У цьому контексті кіберстрахування може відігравати роль ефективного інструменту зменшення фінансових збитків та мінімізації негативних наслідків від можливих інцидентів у цифровому середовищі [3].

Офіційні цифри саме щодо кіберстрахування відсутні, ріст ринку кібербезпеки говорить про зростаючий потенціал і інтерес до продуктів, пов'язаних із кіберризиками, а також через відсутність стандартів, високий ризик, невизначеність у законодавстві та страхових випадках – надання продуктів кіберстрахування все ще на стадії формування, і страховики обережно оцінюють свої можливості.

Таким чином, напрями кіберстрахування безпосередньо відображають ключові категорії кіберризиків, дозволяючи підприємствам формувати комплексну стратегію захисту не лише від фінансових втрат, а й від організаційних, правових та репутаційних наслідків.

Список використаних джерел

1. Приказюк Н. В., Гуменюк Л. С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. Ефективна економіка. 2020. № 4. URL: <http://www.economy.nayka.com.ua/?op=1&z=7777>
2. Кіберстрахування як засіб забезпечення економічного правопорядку в інформаційній сфері. URL: <https://coordynata.com.ua/kiberstrahuvanna-ak-zasib-zabezpecenna-ekonomicnogo-pravoporadku-v-informacijnij-sferi>
3. Попович, Д., Бундз, Н., Іванків, В. (2023). Проблеми та перспективи розвитку страхування кіберризиків на національному ринку. Молодий вчений, 4 (116), 168-172. URL: <https://doi.org/10.32839/2304-5809/2023-4-116-33>

Новікова Д.Г.
*здобувач вищої освіти,
ННІ ЕІТІ ХНУМГ імені О.М. Бекетова
Науковий керівник
Братерська Н.М.
асистент кафедри комп'ютерних наук
та інформаційних технологій
ННІ ЕІТІ ХНУМГ імені О.М. Бекетова*

СТІЙКІСТЬ СУЧАСНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ У КОНТЕКСТІ НОВИХ ЗАГРОЗ

Криптографічні алгоритми відіграють важливу роль у забезпеченні конфіденційності та цілісності даних. Їхня стійкість до сучасних загроз безпосередньо впливає на надійність захисту інформації, тому з розвитком потужних квантових комп'ютерів та методів застосування штучного інтелекту для автоматизованого виявлення закономірностей зростає актуальність дослідження алгоритмів та їх безпечності у контексті нових небезпек.

Серйозну загрозу для сучасних криптографічних алгоритмів становить розвиток квантових обчислювальних технологій, які можуть здійснювати обчислення з набагато більшою швидкістю, порівняно з класичними комп'ютерами [1, с. 248]. Таким чином, розв'язання складних математичних задач та квадратичне прискорення перебору елементів у невпорядкованих множинах стає потенційно доступним, що піддає ризику стійкість методів шифрування та хеш-функцій.

Застосування штучного інтелекту становить загрозу внаслідок можливості автоматизованого виявлення закономірностей у криптографічних даних [2, с. 92]. Це підвищує ефективність кібератак, оскільки полегшує пошук вразливостей у хеш-функціях та симетричних й асиметричних алгоритмах шифрування.

Генератори випадкових чисел, які використовуються для створення криптографічних ключів та ініціалізаційних векторів, можуть бути слабкими, що полегшує знаходження їхніх значень. Аналіз часу виконання операцій, енергоспоживання або електромагнітного випромінювання може виявляти секретні значення ключів або внутрішні параметри алгоритму, що є загрозою для методів шифрування та хеш-функцій. Вразливості протоколів також знижують стійкість криптографічних алгоритмів, оскільки вони використовуються для підміни даних або компрометації хеш-функцій.

Отже, сучасні криптографічні алгоритми зіштовхуються з багатьма загрозами, включно з квантовими обчислювальними технологіями та застосуванням штучного інтелекту, тому їхня стійкість має ґрунтуватися не лише на математичній складності задач, а й на надійності генераторів випадкових чисел, захищеності від перебору ключів та атак із побічних каналів, а також правильності реалізації алгоритмів і протоколів.

Класичні криптографічні алгоритми вважаються надійними в сучасних умовах, але з появою потужних квантових комп'ютерів їх безпека опиниться під загрозою [3, с. 205].

RSA (Rivest-Shamir-Adleman) є алгоритмом асиметричного шифрування, що широко застосовується для захисту конфіденційності та автентифікації в мережі Інтернет. Він ґрунтується на складності розкладання великих цілих чисел на прості [4, с. 171]. Не менш поширеним алгоритмом з відкритим ключем є й ECC (Elliptic Curve Cryptography), який спирається на важкість знаходження дискретного логарифма на еліптичних кривих. Однак квантовий алгоритм Шора здатний ефективно розв'язувати задачі факторизації та дискретного логарифма, що ставить під загрозу безпеку класичних асиметричних алгоритмів, зокрема таких, як RSA та ECC.

Квантовий алгоритм Гровера прискорює перебір ключів симетричних методів шифрування, що потенційно знижує їх криптографічну стійкість. Таким чином, алгоритми на кшталт AES (Advanced Encryption Standard) також опиняються під загрозою. Але вони є менш вразливими до небезпеки, пов'язаної з розвитком квантових обчислювальних технологій, завдяки можливості використання довших ключів.

Хеш-функції також піддаються сучасним загрозам, адже квантові обчислення дають змогу значно прискорювати пошук колізій, що зменшує ефективну довжину хешу. Крім того, даний процес може автоматизуватися за допомогою штучного інтелекту. Отже, такі криптографічні алгоритми, як SHA-256 (Secure Hash Algorithm 256, належить до сімейства SHA-2), SHA-3 та BLAKE2, стійкі проти класичних атак, але вразливі до квантових обчислень та виявлення слабких закономірностей за допомогою ШІ.

Конкурс NIST Post-Quantum Cryptography (PQC) [5], спрямований на відбір та стандартизацію квантово-стійких криптографічних алгоритмів, підкреслює необхідність захисту даних від атак квантових комп'ютерів. Серед постквантових алгоритмів, що наразі демонструють високу стійкість, виділяють Kyber (Key Encapsulation Mechanism Kyber), Dilithium (Digital Signature Scheme based on Lattices), FALCON (Fast Fourier Lattice-based Compact Signatures over NTRU) і SPHINCS+ (Stateless Practical Hash-based Incredibly Nice Cryptographic Signature), вони базуються на матричних, кодових та хеш-структурах.

Також для підвищення стійкості сучасних криптографічних систем є доцільним застосування гібридних підходів, які полягають у поєднанні різних типів алгоритмів. Зокрема, використання постквантового алгоритму разом із класичним забезпечує сумісність з наявними протоколами та захист від атак квантових комп'ютерів. Такий підхід застосовується для шифрування, цифрових підписів, обміну ключами та у поєднанні з сучасними хеш-функціями, він підвищує стійкість до атак та захист від потенційних вразливостей окремих алгоритмів.

Отже, розгляд сучасних криптографічних алгоритмів та їхньої стійкості до нових загроз є важливим у контексті забезпечення надійного захисту інформації, оскільки розвиток квантових обчислювальних технологій, застосування штучного інтелекту та вразливості генераторів випадкових чисел

збільшують ризик компрометації даних. Важливим напрямом для підвищення безпеки є постквантові алгоритми, такі як Kyber, Dilithium, FALCON та SPHINCS+, а також застосування гібридного підходу, який поєднує класичні та квантово-стійкі методи.

Список використаних джерел:

1. А. В. Ярмолатій, Л. О. Черемісіна, В. І. Богом'я. Загрози квантових обчислень для класичних криптографічних алгоритмів. // Водний транспорт. 2025. № 1(42). С. 248–257. doi: <https://doi.org/10.33298/2226-8553.2025.1.42.27>
2. А. С. Коляда, А. В. Павлишко, О. С. Лопаків, В. М. Тігарев, В. В. Космачевський. Використання машинного навчання для виявлення вразливостей криптографічних алгоритмів на основі шифротексту // Інформатика та математичні методи в моделюванні. 2025. Т. 15, № 1. С. 83–94. doi: <https://doi.org/10.15276/imms.v15.no1.83>
3. В. В. Семеренська. Квантово-стійкі криптографічні алгоритми для критичних інфраструктур. Вісник Херсонського національного технічного університету. 2025. Т. 2, № 1(92). С. 204–209. doi: <https://doi.org/10.35546/kntu2078-4481.2025.1.2.27>
4. Д. Новиков, В. Полторак. Технології постквантової криптографії. // Адаптивні системи автоматичного управління. 2023. Т. 1, № 42. С. 171–183. doi: <https://doi.org/10.20535/1560-8956.42.2023.279169>
5. National Institute of Standards and Technology. Post-Quantum Cryptography. URL: <https://csrc.nist.gov/projects/post-quantum-cryptography>

УДК: 37.035:172.15

Новосад А.В.

здобувач вищої освіти, Комунальний заклад вищої освіти «Дніпровська академія неперервної освіти» Дніпропетровської обласної ради»

Шинкаренко В. В.

кандидат педагогічних наук, доцент, завідувач кафедри дошкільної та початкової освіти Комунальний заклад вищої освіти «Дніпровська академія неперервної освіти» Дніпропетровської обласної ради»

ВИКОРИСТАННЯ ЕЛЕМЕНТІВ АРТ-ТЕРАПІЇ В УМОВАХ ОСВІТНЬОГО ПРОЦЕСУ ЗДО: ТЕОРЕТИЧНІ ЗАСАДИ, МЕТОДИЧНІ ТА ПРАКТИЧНІ ПІДХОДИ ДЛЯ МАЙБУТНІХ ВИХОВАТЕЛІВ

У сучасній дошкільній освіті важливо створювати умови, де дитина не лише засвоює базові знання й уміння, а й розвиває емоційну стійкість, творчість, соціальні навички та здатність до саморегуляції. Арт-терапія як сукупність художньо-терапевтичних підходів (малюнок, ліплення, аплікація,

музика, рух, казкотерапія, драматизація) являється найефективнішим інструментом для реалізації цих завдань у закладах дошкільної освіти (ЗДО) [4].

На думку З. Фрейда арт-терапевтичні підходи базуються на ідеї, що творчість – природний шлях вираження внутрішнього світу дитини. У дошкільному віці художня діяльність сприяє: емоційному вираженню і регуляції, розвиває мислення та уяву дошкільнят, формує в них мовленнєві навички через опис власної роботи та розвиває здібності комунікації, удосконалює дрібну моторику рук та координацію рухів всього тіла, соціалізація з іншими учасниками освітнього процесу через виконання групових творчих завдань [8].

Основні принципи застосування арт-терапевтичних методів – це безпечність освітнього середовища для дитини дошкільного віку, доступність необхідних матеріалів, відсутність оцінювання «гарно/погано» від вихователя, друзів та помічника, підтримка у самовираженні власного досвіду малюка, увага й підтримка до індивідуальних особливостей дитини, інтеграція з педагогічними цілями заняття [6].

Для дитини дошкільного віку важливими є розвиток емоційної грамотності (розпізнавання, називання й переживання емоцій), підвищення самооцінки та віри у власних можливостях з боку дорослого за допомогою мотиваційних відгуків та підтримки товаришів, стимуляція креативності і уяви шляхом наочності, поліпшення комунікативних навичок у спілкуванні.

А для майбутнього вихователя під час педагогічного процесу важливими є збагачення дидактичних методів, створення діагностичного простору методом «тихого спостереження» (виявлення труднощів, ресурсів), впровадження в роботу з дітьми корекційно-розвиткових заходів в доступній формі [2, 96].

Використання арт-терапії в освітньому процесі закладів дошкільної освіти ґрунтується на твердженні Маргарет Наумбург – засновниці арт-терапії, що творчість є природним і необхідним способом розвитку дитини дошкільного віку. У цьому віці домінує образне мислення, символічна гра і потреба в невербальному самовираженні. Саме тому художня діяльність стає «мовою» дитини, через яку вона передає свої емоції, думки й внутрішні переживання [7].

З позицій психології та педагогіки, арт-терапевтичний підхід спирається на ідеях гуманістичної педагогіки (цінність особистості, розвиток індивідуальних здібностей); культурно-історичній теорії розвитку Л. Виготського (роль соціального та творчого середовища у становленні особистості); принципах інтеграції емоційного, когнітивного й сенсомоторного досвіду, об'єднаних єдиною освітньою діяльністю [3, с. 187].

Таким чином, арт-терапія в ЗДО розглядається не як лікувальний інструмент у вузькому розумінні, а як засіб розвитку, виховання і корекції. Її головна функція – підтримка емоційного благополуччя, розвиток здатності до комунікації та формування творчого потенціалу дошкільника.

Для майбутніх вихователів важливо усвідомити, що застосування арт-терапевтичних методів в освітньому процесі має ґрунтуватися на певних методичних орієнтирах. Застосування елементів арт-терапії на практиці передбачає особливу позицію майбутнього вихователя. Він має виступати не як

суворий контролер чи оцінювач результатів, а як фасилітатор – той, хто створює умови для творчості, підтримує дитину й надихає її [5, с. 35].

На практичній площині це означає:

- налагодження емоційного контакту з дітьми, щоб вони відчували довіру й готовність відкриватися;
- використання вільного вибору (дитина сама вирішує, які матеріали брати, як виконувати завдання, яким буде її продукт);
- спостереження й аналіз: вихователь уважно відстежує прояви дітей у процесі діяльності, що дає інформацію про їхній емоційний стан, соціальні навички, комунікацію;
- створення умов для групової взаємодії – коли діти вчаться домовлятися, співпрацювати, обговорювати свої роботи.

Для майбутніх вихователів важливо усвідомлювати, що результат арт-терапевтичної діяльності вимірюється не лише готовим виробом, а й тим, як змінилася поведінка дитини, наскільки вона навчилася виражати емоції, взаємодіяти з іншими та отримувати позитивний досвід від творчості [1, с. 136].

Отже, використання елементів арт-терапії – це гнучкий і ефективний інструмент у роботі з дошкільниками. Для майбутніх педагогів важливо не лише знати методи, а й вміти організувати безпечний, підтримуючий простір, документувати зміни та співпрацювати з вихованцями, батьками й колегами. Інтегруючи творчі практики в освітній процес, ви не лише розвиваєте художні навички дитини, а перш за все – їхні внутрішні ресурси: емоційну стійкість, здатність до спілкування і творче мислення. Це дає міцну основу для подальшого навчання і становлення особистості.

Список використаних джерел:

1. Вачков І. В. Арт-терапія: теорія та практика. Київ, 2017. С. 136.
2. Лебедева Л. Д. Арт-терапія в роботі з дітьми: методи і прийоми. Центр учбової літератури. Київ, 2016. С. 96–98.
3. Кисельова М. В. Арт-терапія для дітей: практичний посібник. Харків, 2019. С. 187–192.
4. Наказ МОН України № 655 від 23.04.2018 р. «Про затвердження Базового компоненту дошкільної освіти (нова редакція)».
5. Савченко О. Я. Дидактика початкової освіти. Генеза. Київ, 2019. С. 35.
6. Winnicott D. W. Playing and Reality. London, 2001. 214 p.
7. Malchiodi C. A. The Art Therapy Sourcebook. New York, 2013. 400 p.
8. Rubin J. A. Approaches to Art Therapy: Theory and Technique. New York, 2016. 496 p.

Павлюк Р.О.
*здобувач вищої освіти,
Бахмутського навчально-наукового професійно-педагогічного
інституту ХНУ імені В.Н. Каразіна
Науковий керівник
Зубенко С.О.*
*старший викладач кафедри електромеханічних
та комп'ютерних систем
Бахмутського навчально-наукового професійно-педагогічного
інституту ХНУ імені В.Н. Каразіна*

КІБЕРГІГІЄНА КОРИСТУВАЧІВ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасному світі інформація є однією з найцінніших складових життя. Ми щодня користуємося соціальними мережами, онлайн-банкінгом, електронною поштою та безліччю цифрових сервісів. Але одночасно із зручностями зростає і кількість кіберзагроз. Саме тому питання інформаційної безпеки стає надзвичайно актуальним у наш час.

Ключову роль у захисті даних відіграє не лише техніка чи програмне забезпечення, а й поведінка самих користувачів. Цю поведінку називають кібергігієною.

По-перше, важливим елементом кібергігієни є використання надійних паролів. Паролі – це перша лінія захисту особистих облікових записів. На жаль, багато користувачів досі застосовують прості комбінації на кшталт «123456» чи «password». Це робить їх акаунти легкою здобиччю для зловмисників. Рекомендовано створювати паролі, що містять щонайменше 12 символів, включаючи великі та малі літери, цифри й спеціальні знаки. Також варто використовувати власний пароль для кожного сервісу. Уникнути плутанини допомагають спеціальні менеджери паролів [1].

По-друге, варто застосовувати двофакторну автентифікацію (2FA). Це додатковий рівень безпеки, коли для входу в обліковий запис потрібен не лише пароль, а й підтвердження через телефон або інший пристрій. Навіть якщо пароль було вкрадено, двофакторна автентифікація значно ускладнює доступ до акаунта. Це може бути одноразовий код із SMS, підтвердження у мобільному додатку або апаратний ключ. Такий додатковий рівень захисту стає все більш поширеним і рекомендованим у всіх сервісах, де зберігаються важливі дані [2].

По-третє, користувачі повинні регулярно оновлювати програмне забезпечення. Хакери часто використовують уразливості у старих версіях програм та операційних систем. Виробники програмного забезпечення регулярно випускають оновлення, що закривають «дірки» в безпеці. Ігнорування цих оновлень може призвести до серйозних наслідків: від зараження вірусами до повної втрати даних.

По-четверте, дуже важливо проявляти обережність у мережі. Не слід відкривати підозрілі електронні листи, натискати на невідомі посилання чи завантажувати файли з ненадійних джерел. Це один із найефективніших способів захисту від вірусів та фішингу. Для цього слід дотримуватися простих правил: не відкривати підозрілі посилання, не завантажувати файли з невідомих джерел і завжди перевіряти адресу сайту перед введенням пароля чи банківських даних.

По-п'яте, користувач має піклуватися про захист особистих даних. Надмірна кількість інформації у відкритому доступі в соціальних мережах може стати знаряддям для шахраїв. Багато користувачів самі надають зловмисникам необхідну інформацію, публікуючи зайві деталі у соціальних мережах: адресу проживання, номери телефонів, дані про місце роботи чи навчання. Така інформація може стати основою для шахрайських схем, зокрема атак із використанням методів соціальної інженерії. Важливо використовувати налаштування конфіденційності та обмежувати коло осіб, які мають доступ до особистих даних.

По-шосте, невід'ємною складовою кібергігієни є резервне копіювання даних. У разі втрати інформації через вірус, кібератаку або технічний збій копії допоможуть швидко відновити важливу інформацію.

Отже, кібергігієна – це не одноразова дія, а щоденна культура поведінки в Інтернеті. Вона включає створення надійних паролів, використання двофакторної автентифікації, регулярні оновлення, обережність у мережі, захист персональних даних і резервне копіювання. Саме від особистої відповідальності користувачів залежить рівень інформаційної безпеки як кожної людини, так і суспільства загалом. Таким чином, кібергігієна є ключовим елементом захисту даних у сучасному цифровому світі.

Список використаних джерел

1. Методичні рекомендації з кіберзахисту та кібербезпеки паролів – URL: <https://cnap.zelenopidska-gromada.gov.ua/news/205576-metodicni-rekomendaciyi-z-kiberzaxistu-ta-kiberbezpeki-paroliv>
2. Центр стратегічних комунікацій та інформаційної безпеки. Що таке двофакторна автентифікація і як вона працює? – URL: <https://cip.gov.ua/ua/faqs/sho-take-dvofaktorna-avtentifikaciya-i-yak-vona-pracyuye>

Пархоменко О. Ю.

*кандидат фізико-математичних наук,
доцент кафедри економічної кібернетики,
комп'ютерних наук та інформаційних технологій
Миколаївського національного аграрного університету*

Ємельянов С. І.

*доктор філософії (фізика та астрономія),
старший викладач кафедри економічної кібернетики,
комп'ютерних наук та інформаційних технологій
Миколаївського національного аграрного університету*

ВПЛИВ ДИСБАЛАНСУ КЛАСІВ НА ЕФЕКТИВНІСТЬ МЕТРИК ОЦІНКИ В ЗАДАЧАХ ДЕТЕКЦІЇ ШАХРАЙСТВА З КРЕДИТНИМИ КАРТКАМИ

У сучасних умовах стрімкої цифровізації фінансових послуг, зокрема платежів, розробка ефективних систем детекції шахрайства з кредитними картками набуває ключового значення для забезпечення безпеки. Вирішення цієї задачі вимагає створення надійних моделей машинного навчання, здатних точно класифікувати транзакції. Однак, як свідчить практика, істотним викликом у цій галузі є дисбаланс класів у навчальних даних, коли частка шахрайських операцій часто не перевищує 1% від загального обсягу. Така асиметрія може суттєво впливати на адекватність оцінювання якості моделей. Таким чином, дослідження впливу дисбалансу класів на метрики оцінки представляється актуальним, оскільки стандартні підходи можуть давати завищені оцінки ефективності, що маскують реальні недоліки алгоритмів.

Дисбаланс класів є класичною проблемою в задачах класифікації, особливо в таких доменах, як фінансова безпека, де рідкісні події (наприклад, шахрайство) мають критичну важливість, а їх пропуск може призводити до значних матеріальних втрат. У таких випадках стандартні метрики на кшталт ассурасу часто виявляються недостатніми. Як альтернатива пропонуються метрики, що враховують як точність прогнозу позитивного класу (precision), так і його повноту (recall). Зокрема, F1-score, будучи гармонійним середнім precision та recall, може бути корисним там, де важливий баланс між помилками першого та другого роду. ROC-AUC оцінює здатність моделі до розрізнення класів на різних порогах прийняття рішення, але на сильно дисбалансованих даних його значення також може бути необ'єктивно високим через домінування класу більшості. Коефіцієнт кореляції Метьюса (MCC), натомість, вважається більш збалансованою метрикою, оскільки враховує співвідношення всіх чотирьох клітин матриці неточностей. Разом з тим, залишається недостатньо дослідженим питання про те, як дисбаланс даних впливає на стабільність цих метрик у процесі крос-валідації, що має особливе значення в реальних умовах з обмеженими вибірками даних.

Для дослідження було використано публічно доступний датасет Credit Card Fraud Detection з платформи Kaggle [1], який містить 284 807 транзакцій, з них 492 (0,17%) ідентифіковані як шахрайські. Такий розподіл є типовими прикладом сильного дисбалансу класів, де легальні операції значно домінують. У роботі було застосовано низку моделей машинного навчання, включаючи Logistic Regression, Random Forest, XGBoost та ансамблевий метод Stacking. Оптимізація гіперпараметрів моделей проводилася за допомогою GridSearchCV. Для корекції дисбалансу класів використовувалися методи SMOTE, ADASYN та RandomUnderSampler, що дозволило оцінити вплив балансування на якість класифікації. Оцінка ефективності моделей проводилася за метриками F1-score, ROC-AUC, MCC та G-Mean з використанням стратифікованої крос-валідації (StratifiedKFold, n_splits=5). Всі експерименти були реалізовані в середовищі Python з використанням бібліотек scikit-learn, imbalanced-learn та xgboost.

Як і очікувалося, дисбаланс даних суттєво впливає на оцінку моделей. Без застосування методів балансування моделі демонструють високу загальну точність (accuracy ~99%), проте мають низький показник повноти (recall ~0,5) для класу шахрайських транзакцій, що робить їх малопридатними для вирішення практичних завдань. Наприклад, модель XGBoost без корекції даних досягає значення ROC-AUC близько 0,95, однак F1-score для меншостного класу опускається нижче 0,7 через значну кількість пропущених аномалій (false negatives).

Застосування методів балансування призводить до помітних змін у результатах. Зокрема, спостерігається суттєве покращення метрик, орієнтованих на менший клас. Важливо зауважити, що отримані високі показники досягнуті в умовах конкретного експерименту та на даному конкретному датасеті. Так, комбінація Random Forest з методом SMOTE показала результат F1-score 0,99950, тоді як з RandomUnderSampler цей показник склав 0,98318. Це ілюструє залежність результату від обраного методу корекції. Більш збалансована метрика MCC також продемонструвала значне зростання – з 0,17 (для XGBoost з RandomUnderSampler) до 0,851 (для Random Forest з SMOTE), що може свідчити про ефективність синтетичних методів зменшення дисбалансу в даному випадку. Аналогічно, метрика G-Mean, яка враховує геометричне середнє, зросла до 0,99950 при використанні SMOTE, що вказує на зменшення упередженості моделі до класу більшості в рамках проведеного дослідження.

Таблиця 1 демонструє порівняння середнього F1-score за методами балансування, обчисленими на основі результатів моделей.

Таблиця 1.

Середній F1-score за методами балансування

Метод балансування	Середній F1-score	Стандартне відхилення
SMOTE	0,99567	0,0065
ADASYN	0,98817	0,0182
RandomUnderSampler	0,97849	0,0031

Аналіз даних таблиці 1 показує, що SMOTE забезпечує найвищу стабільність метрик, тоді як RandomUnderSampler, ймовірно, призводить до втрат інформації, що знижує середній F1-score приблизно на 1,7 процентних пункти.

Проведений аналіз підтверджує, що в умовах дисбалансу класів стандартні метрики на кшталт accuracy є недостатніми для адекватної оцінки моделей. Для всебічного аналізу доцільно використовувати комплекс метрик, таких як F1-score та MCC, що дозволяють оцінити якість прогнозу для меншого класу. З практичної точки зору, це означає необхідність інтеграції методів балансування даних у пайплайни побудови моделей для фінансових установ, що дозволяє мінімізувати ризики пропуску шахрайських операцій. Як показано на прикладі датасету, модель без корекції дисбалансу може не виявляти до 50% аномалій, що робить її застосування в реальних умовах проблематичним.

Отже, дисбаланс класів є не лише технічною перешкодою, а фактором, що фундаментально впливає на інформативність та надійність оцінкових метрик для практичного застосування. Отримані результати вказують на те, що синтетичні методи балансування, зокрема SMOTE, можуть істотно покращувати результати класифікації, що підтверджується високими значеннями F1-score в умовах даного дослідження.

Разом з тим, важливо враховувати обмеження цієї роботи. Результати отримані на одному конкретному датасеті, і ефективність методів може варіюватися залежно від характеру даних, ступеня дисбалансу та архітектури моделі. Крім того, синтетичні методи можуть мати схильність до генерації шумових вибірок або перенавчання моделі.

Таким чином, перспективним напрямом для подальших досліджень є вивчення гібридних підходів до балансування даних, а також їх поєднання з методами глибокого навчання для підвищення стійкості та узагальнюючої здатності моделей. Усвідомлення впливу дисбалансу класів залишається ключовим для розробки ефективних систем детекції, здатних протидіяти еволюційним загрозам у фінансовій сфері.

Список використаних джерел:

1. <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud> (date of access: 27.09.2025).
2. Tyshchenko S., Parkhomenko O., Hilko I. Modeling the Impact Of Digital Threats on Financial Markets Using Time Series Analysis and Anomaly Detection Using Python. *Modern Economics*. 2024. P. 205–212.
URL: [https://doi.org/10.31521/modecon.v44\(2024\)-30](https://doi.org/10.31521/modecon.v44(2024)-30).
3. Dwarampudi A., Yogi M. K. A Robust Machine Learning Model for Cyber Incident Classification and Prioritization. *Journal of Trends in Computer Science and Smart Technology*. 2024. Vol. 6, no. 1. P. 51–66.
URL: <https://doi.org/10.36548/jtcsst.2024.1.00>.
4. Classification and Prediction of Significant Cyber Incidents (SCI) using Data Mining and Machine Learning (DM-ML) / G. Mumtaz et al. *IEEE Access*. 2023. P. 1.
URL: <https://doi.org/10.1109/access.2023.3249663>.

Пархоменко О. Ю.
здобувач вищої освіти,
Національний університет кораблебудування
імені адмірала Макарова
Морозова Г. С.
старший викладач кафедри
інформаційних управляючих систем та технологій
Національний університет кораблебудування
імені адмірала Макарова

КОНЦЕПЦІЯ ВИЯВЛЕННЯ ЧАСОВИХ АНОМАЛІЙ У ЛОГАХ RFID-СИСТЕМ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ

У сучасних інформаційних системах контролю доступу важливу роль відіграють технології автоматичної ідентифікації, зокрема RFID (Radio Frequency Identification). Використання RFID-карт забезпечує швидку та зручну авторизацію користувачів у різних сферах – від офісних приміщень до закладів освіти. Проте традиційні системи контролю доступу часто обмежуються лише перевіркою факту наявності картки в базі, ігноруючи аналіз поведінкових патернів користувачів. Це створює потенційні ризики, наприклад, картка може бути втрачена або передана іншій особі, а сама система не здатна виявити нетипові спроби доступу.

Одним із перспективних напрямів підвищення надійності таких систем є інтеграція алгоритмів машинного навчання (ML), що дозволяють виявляти аномалії у часових характеристиках доступу. Це дає можливість фіксувати підозрілі дії, наприклад, спроби входу в нетиповий час або повторні входи протягом надто короткого інтервалу.

Метою дослідження є концептуальний аналіз можливостей застосування методів машинного навчання для виявлення часових аномалій у логах RFID-систем з метою підвищення ефективності систем контролю доступу.

Для аналізу часових аномалій доцільно застосувати підхід на основі алгоритмів виявлення аномалій (Anomaly Detection), реалізованих у середовищі Python із використанням бібліотек scikit-learn та pandas. Методологічна база дослідження включає ряд алгоритмів, що демонструють найвищу ефективність для темпоральних даних, і які наведено в таблиці 1.

Isolation Forest демонструє високу ефективність при роботі з багатовимірними даними великого обсягу. Алгоритм базується на припущенні, що аномальні точки потребують меншої кількості поділів для ізоляції в просторі ознак.

One-Class Support Vector Machine (One-Class SVM) моделює межі нормальної поведінки користувачів у високовимірному просторі ознак. Метод особливо ефективний для випадків, коли нормальні дані утворюють компактні кластери.

DBSCAN забезпечує автоматичну ідентифікацію викидів через механізм кластеризації на основі щільності. Алгоритм не потребує попереднього визначення кількості аномалій.

Autoencoder є ще одним перспективним інструментом для виявлення аномалій у часових даних. Його архітектура ґрунтується на нейронній мережі, що навчається відтворювати вхідні дані у стиснутому вигляді. Під час навчання на нормальних зразках модель формує компактне представлення характерних патернів поведінки користувачів. Коли на вхід подається нетипова послідовність подій, похибка відновлення значно зростає, що дозволяє ідентифікувати її як аномалію. Перевагою Autoencoder є здатність працювати з нелінійними залежностями та складними багатовимірними часовими ознаками.

Таблиця 1.

Можливі ML-методи виявлення часових аномалій

Тип аномалії	Приклад ситуації	Можливі ML-підходи
Темпоральна девіація (нетиповий час входу)	Працівник завжди приходить з 8:00–9:30, а тут з'явився о 02:00 ночі	Isolation Forest, One-Class SVM, Autoencoder
Частотна аномалія (занадто часті входи)	Користувач прикладає картку 5 разів за 10 хвилин	DBSCAN (кластеризація подій), статистичні методи
Аномалія відсутності (довга відсутність)	Користувач відсутній у логах більше тижня, хоча зазвичай відвідує щодня	Time Series Forecasting (ARIMA, Prophet), Isolation Forest
Календарна аномалія (вхід у незвичні дні)	Користувач ніколи не відвідував офіс у суботу, але з'явився	Isolation Forest, One-Class SVM, статистичний аналіз

Лог-файл RFID-системи подається у вигляді таблиці подій, де для кожного користувача фіксуються унікальний ідентифікатор (UID) картки, дата та час входу. На основі цих даних формується набір ознак (features): година входу, день тижня, інтервал між подіями тощо. Можливу структуру даних для аналізу часових аномалій наведено в таблиці 2. Процес створення ознак включає екстракцію темпоральних компонентів (година, день тижня, місяць), обчислення інтервалів між послідовними подіями, формування агрегованих статистик для кожного користувача, нормалізацію числових ознак.

Таблиця 2.

Приклад структури даних для аналізу часових аномалій

UID користувача	Дата	Час	День тижня	Інтервал від попереднього входу (хв)	Ознака аномалії
123ABC	2025-09-24	09:15	Середа	480	Норма
456DEF	2025-09-24	09:18	Середа	1440	Норма
123ABC	2025-09-24	02:30	Середа	105	Аномалія
789GHI	2025-09-25	09:20	Четвер	3	Аномалія

У таблиці для користувача 123ABC було зафіксовано спробу доступу вночі (02:30), що вважається нетиповим для його звичної поведінки. Для користувача

789GHz спостерігається повторний вхід через 3 хвилини після попереднього, що також може свідчити про аномальну активність.

Алгоритми машинного навчання дозволяють:

1. Виявляти нічні спроби входу як відхилення від звичного діапазону часу.
2. Визначати підозрілі повторні входи протягом короткого проміжку часу.
3. Аналізувати довготривалі відсутності у логах, що може сигналізувати про втрату або передачу картки іншій особі.

Теоретичний аналіз демонструє потенціал інтеграції алгоритмів машинного навчання з існуючими RFID-системами без модифікації апаратної архітектури. Концептуальна модель передбачає можливість трансформації статичних систем ідентифікації в адаптивні рішення з функціями самонавчання та автоматизованого виявлення аномалій, що наближає технологію до принципів поведінкової біометрії.

Попри значний потенціал, запропонований підхід має низку викликів. По-перше, якість виявлення аномалій суттєво залежить від обсягу та повноти історичних даних: якщо логів недостатньо, алгоритми можуть формувати спотворену модель «нормальної» поведінки. По-друге, існує проблема хибнопозитивних спрацювань, коли система відносить до аномалій рідкісні, але легітимні події (наприклад, позаплановий нічний вхід чергового працівника). Крім того, складні алгоритми, такі як нейронні мережі, потребують додаткових обчислювальних ресурсів і ретельної оптимізації параметрів, що може ускладнити їх інтеграцію у вже розгорнуті системи контролю доступу.

У роботі обґрунтовано теоретичну можливість застосування ML-підходів для детекції часових девіацій у логах RFID-систем. Запропонована концепція може слугувати методологічною основою для майбутніх розробок інтелектуальних систем контролю доступу, орієнтованих на підвищення безпеки через аналіз поведінкових патернів користувачів.

Перспективи подальших досліджень включають розширення спектру виявлюваних аномалій на просторові та групові девіації, а також практичну апробацію запропонованого підходу на реальних даних RFID-систем.

Список використаних джерел:

1. Automated Log Analysis and Anomaly Detection Using Machine Learning / A. H. Shah et al. *Frontiers in Artificial Intelligence and Applications*. 2022.
URL: <https://doi.org/10.3233/faia220378>.
2. Distributed system anomaly detection using deep learning-based log analysis / P. Han et al. *Computational Intelligence*. 2023.
URL: <https://doi.org/10.1111/coin.12573>.
3. Log Analysis For Network Attack Detection Using Deep Learning Models / H. P. Pham et al. *SOICT 2023: The 12th International Symposium on Information and Communication Technology*, Ho Chi Minh Vietnam. New York, NY, USA, 2023.
URL: <https://doi.org/10.1145/3628797.3628943>.
4. Towards Detecting Anomalies in Log-Event Sequences with Deep Learning: Open Research Challenges / P. Himler et al. *EICC 2023: European Interdisciplinary Cybersecurity Conference*, Stavanger Norway. New York, NY, USA, 2023.

УДК 004.056.5

Подвальний А. О.,

Ішу В. В.,

Мойко О. О.

здобувачі вищої освіти

Харківського національного університету внутрішніх справ

Науковий керівник

Тімошин А. С.

кандидат фізико-математичних наук,

доцент кафедри інформаційних систем та технологій ННІ № 4

Харківського національного університету внутрішніх справ

АНАЛІЗ ФУНКЦІОНАЛЬНОСТІ НАЙБІЛЬШ ПОПУЛЯРНИХ МЕНЕДЖЕРІВ ПАРОЛЕЙ ДЛЯ ОСОБИСТОГО КОРИСТУВАННЯ

Пароль – це послідовність символів, яка використовується для підтвердження особи користувача під час автентифікації. Зазвичай він застосовується разом із іменем користувача і призначений для того, щоб бути відомим лише власнику. Пароль надає доступ до пристроїв, програм та різних облікових записів. Він може містити літери, цифри та спеціальні символи, а також відрізнятися за довжиною.

Види паролів:

Статичний пароль – це пароль, який використовується постійно для ідентифікації та доступу до персональних даних. Його необхідно зберігати особливо ретельно. Вибір багаторазового пароля потребує уважного підходу, оскільки саме від його надійності залежить захист конфіденційної інформації. У порівнянні з одноразовими паролями, багаторазові мають нижчий рівень безпеки, оскільки можуть використовуватися повторно. Статичні паролі є основним засобом автентифікації, але вони вразливі до атак методом підбору (brute force), фішингових атак та витоків баз даних. Рекомендується використовувати довгі, унікальні паролі для кожного облікового запису та зберігати їх у захищених сховищах.

Динамічний пароль – це унікальний код або ключове слово, яке можна використати лише один раз. Він дійсний тільки протягом одного сеансу автентифікації, що підтверджує право користувача на доступ до конфіденційної інформації. Термін дії такого пароля може бути обмежений визначеним часовим інтервалом. Основна перевага такого виду пароля полягає в тому, що його неможливо використовувати повторно, а тому злоумисник, навіть якщо дізнався пароль, не може отримати доступ до інформації під захистом. Недоліком застосування одноразового пароля є потреба в частій зміні та запам'ятовуванні пароля.

Основними недоліками зберігання паролів є можливість їх втратити. Для збереження паролів та подальшого їх застосування дуже часто використовуються різні способи зберігання паролів: на комп'ютері, телефоні, у спеціальних програмах, на папері, у пам'яті. Одні з них більш безпечні чи практичні, інші навпаки. Крім ризику втрати паролів, ще одна проблема – повторне використання одного пароля на різних сайтах. У разі витоку бази даних одного ресурсу зловмисники можуть отримати доступ до всіх облікових записів користувача. Одним із сучасних засобів зберігання паролів є спеціальні менеджери паролів. [1]

Основні види менеджерів паролів:

Браузерні менеджери

Багато інтернет-браузерів, як-от Safari та Chrome, пропонують вбудовані менеджери паролів, які можуть автоматично зберігати та автоматично заповнювати ваші дані, коли вам потрібно увійти в облікові записи онлайн.

Хмарні менеджери

Хмарні менеджери паролів зазвичай завантажуються та керуються через програму на вашому мобільному телефоні чи комп'ютері. Важливим у такому менеджері є те, що самі паролі зберігаються в хмарі. Це захищає їх від атак на ваш пристрій і може забезпечити більшу гнучкість, дозволяючи користувачам отримувати доступ до паролів із кількох пристроїв.

Локальні менеджери

Локальні менеджери паролів зберігають ваші дані на вашому пристрої. Це означає, що вони можуть бути дуже безпечними, оскільки дані не передаються третім особам. Однак ця форма настільки безпечна, наскільки безпечні пристрій і користувач. Якщо ваш пристрій вразливий до атак, ваші паролі також можуть бути скомпрометовані.[2]

Для аналізу ми обрали декілька найбільш популярних менеджерів з кожної категорії:

- Google Password Manager (браузерний менеджер найпопулярнішого браузера)
- LastPass (хмарний менеджер, 10 млн завантажень у Play Market)
- Bitwarden (хмарний менеджер, 5 млн завантажень у Play Market)
- KeePass (найбільш відомий локальний менеджер)

Аналіз менеджерів проводився на ОС Windows 10 в браузері Google Chrome. Однак поведінка деяких менеджерів може змінюватися залежно від операційної системи або браузера. Наприклад, Bitwarden має розширену підтримку для Linux та Firefox, а Google Password Manager найкраще працює у Chrome.

Провівши аналіз кожного менеджера паролів та створивши порівняльну таблицю, ми дійшли до деяких висновків:

1. Перевага Google Password – глибока інтеграція з екосистемою Google. Однак він має обмежений набір функцій у порівнянні з повноцінними менеджерами, такими як LastPass або Bitwarden, наприклад, відсутність розширених параметрів спільного доступу до паролів.

2. LastPass – популярний хмарний менеджер, який пропонує як безкоштовний, так і платний функціонал, який покриває більшість запитів користувачів. Однак він за останні роки він зазнав кількох витоків даних, що вплинуло на довіру користувачів[4]

Таблиця 1.

Порівняльна таблиця

Критерії	Google Password	LastPass	Bitwarden	Keepass
Тип	Браузерний	Хмарний	Хмарний	Локальний
Відкритий код	Ні	Ні	Так	Так
Алгоритм шифрування	Немає точної інформації	AES-256	AES-256	За замовчанням AES-256, ChaCha20, інші можна встановити через плагіни, ще є можливість подвійного шифрування[3]
Генератор паролів	ASCII, паролі генеруються тільки при створенні акаунтів	ASCII	ASCII	Unicode символи
2FA	Так	Так	Так	Так
Безкоштовна	Так	Ні	Ні	Так
Синхронізація	Так	Так	Так	Так

3. Bitwarden – Один із найбільш безпечних хмарних менеджерів, оскільки його код є відкритим, а це означає, що незалежні експерти можуть перевіряти його безпеку.

4. Keepass – Найкращий вибір для тих, хто хоче повний контроль над своїми даними. В той час як хмарні менеджери як Bitwarden і LastPass є готовими рішеннями, Keepass потребує багато налаштування та встановлення плагінів, але й дозволяє отримати більший функціонал та контроль над алгоритмами шифрування та створенням резервної копії бази даних.

Список використаних джерел

1. Зубарський Д. О. Автоматизована система збереження персональних даних користувача : магістерська дис.:наук. кер. С. О. Цибульник ; Нац. техн. ун-т України «Київ. політехн. ін-т ім. Ігоря Сікорського». – Київ, 2021.

2. What Are The Different Types Of Password Manager? : [Електронний ресурс] / Alex Zawalnyski. – <https://expertinsights.com/insights/what-are-the-different-types-of-password-manager/>

3. KeePass Plugins / Extensions : [Електронний ресурс]. —<https://keepass.info/plugins.html#multicipher>

4. Timeline of the Latest LastPass Data Breaches : [Електронний ресурс] / CSO Online. –

УДК 004.056

Поліщук А.В.

здобувач вищої освіти,

ННІ ІБСК Національної академії Служби безпеки України

Науковий керівник

Вавіленкова А.І.

д.т.н., професор, завідувач кафедри кібербезпеки

ЦКБ ННІ ІБСК Національної академії Служби безпеки України

АКТИВНІ МЕТОДИ МОНІТОРИНГУ ДОСТУПНОСТІ МЕРЕЖЕВИХ РЕСУРСІВ У СИСТЕМАХ КІБЕРЗАХИСТУ

Забезпечення стійкої роботи інформаційних систем сьогодні є одним із ключових завдань у сфері кіберзахисту. Будь-яка відмова окремого сервера, вузла чи сервісу може призвести не лише до фінансових втрат, але й створити умови для виникнення кіберінцидентів. Саме тому сучасні організації приділяють значну увагу питанням моніторингу інформаційної інфраструктури. Одним із найпоширеніших підходів у цьому напрямі є активний моніторинг доступності, що базується на використанні діагностичних запитів для оцінки працездатності мережеских ресурсів у режимі реального часу.

Активні методи моніторингу полягають у безпосередньому зверненні до контрольованих об'єктів та аналізі їхніх відповідей. Це відрізняє їх від пасивних методів, де інформація збирається з уже наявних журналів подій. Найвідомішим прикладом є використання протоколу ICMP (Internet Control Message Protocol), який застосовується для перевірки доступності вузлів у мережі. Проста команда ping стала класичним інструментом для адміністратора, оскільки дозволяє швидко оцінити чи функціонує віддалений ресурс. Проте на рівні кіберзахисту важливо розглядати цей метод у ширшому контексті – як один із елементів системи раннього попередження про інциденти [1].

Окрім ICMP, у практиці застосовуються й інші засоби. Traceroute використовується для визначення маршруту проходження пакетів та виявлення проблемних ділянок мережі, а протокол SNMP (Simple Network Management Protocol) дозволяє отримувати від обладнання інформацію про його стан і робочі параметри. Також широкого поширення набули агентські перевірки, коли на кінцеві сервери чи робочі станції встановлюється спеціальне програмне забезпечення (наприклад, Zabbix Agent або WMI-агенти), яке збирає дані про навантаження процесора, використання пам'яті, стан сервісів тощо.

Серед переваг активного моніторингу варто відзначити його простоту, швидкість та універсальність. Він дозволяє своєчасно виявляти недоступність ресурсів, а також діагностувати проблеми, що пов'язані з деградацією роботи

сервісів. Наприклад, навіть кілька секунд простою критичного вузла можуть призвести до зупинки бізнес-процесів або створити «вікно можливостей» для зловмисників. Активний моніторинг забезпечує миттєве виявлення таких ситуацій та створює основу для оперативного реагування.

Втім, самостійне використання активних методів має й обмеження. По-перше, постійне надсилання діагностичних запитів створює додаткове навантаження на мережу, що особливо відчутно у великих інфраструктурах. По-друге, дані, отримані в результаті перевірок, не завжди дозволяють відрізнити технічний збій від цілеспрямованої кібератаки. Наприклад, під час DDoS-атаки ресурс може здаватися «недоступним» для користувача, але справжня причина буде прихована. По-третє, активні методи не надають розширеної інформації про внутрішні події у системі – для цього потрібен аналіз логів, кореляція подій та застосування методів машинного навчання [2].

Саме тому в сучасних підходах до кіберзахисту активний моніторинг використовується у комплексі з іншими технологіями. Одним із найефективніших рішень у цій сфері є інтеграція активного моніторингу з системами обробки журналів подій та платформами класу SIEM (Security Information and Event Management). У такому випадку інформація про стан мережевих ресурсів поєднується з аналізом внутрішніх логів, що дозволяє виявляти складніші загрози, включаючи інсайдерські атаки чи нетипові сценарії використання систем.

Прикладом платформи, яка реалізує такий підхід, є система Zabbix. Вона підтримує різні механізми активного моніторингу: ICMP-перевірки, SNMP-опитування, роботу агентів, а також розширені тригери, що дозволяють автоматично реагувати на інциденти [3]. Окрім того, Zabbix може інтегруватися з іншими сервісами для збору та аналізу журналів подій, створюючи багаторівневу модель контролю. Це дає змогу не лише виявити факт недоступності ресурсу, але й визначити причину, побудувати прогноз та своєчасно попередити ескалацію проблеми.

Таким чином, активні методи моніторингу залишаються фундаментальним інструментом у сфері кіберзахисту. Вони забезпечують швидке виявлення інцидентів, пов'язаних із недоступністю чи нестабільністю ресурсів, та створюють основу для ефективного реагування. Водночас найбільший ефект досягається у разі їх поєднання з інтелектуальним аналізом подій та застосуванням комплексних систем моніторингу, які інтегрують активні та пасивні методи. Це формує цілісний підхід до виявлення загроз і підвищує стійкість інформаційної інфраструктури в умовах сучасних викликів кібербезпеки.

Список використаних джерел:

1. Stallings W. *Network Security Essentials: Applications and Standards*. – 6th ed. – Pearson, 2020. – 480 с.
2. Internet Engineering Task Force (IETF). *RFC 1157 – Simple Network Management Protocol (SNMP)*. – 1990. – URL: <https://www.rfc-editor.org/rfc/rfc1157>

3. Zabbix Documentation. *Zabbix 6.0 LTS Manual*. – URL: <https://www.zabbix.com/documentation/current>

УДК 343.98

Полякова Є.Р.

здобувач вищої освіти,

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

Науковий керівник

Стяглик Н.І.

завідувач кафедри інформаційних технологій та

математичного моделювання

Харківський національний університет імені В.Н.Каразіна

ЦИФРОВІ ДОКАЗИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ: ВИКЛИКИ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ УКРАЇНСЬКОГО ЗАКОНОДАВСТВА В УМОВАХ РОЗВИТКУ КРИПТОВАЛЮТ

Робота присвячена проблемам використання цифрових доказів у кримінальному процесі України, зокрема у справах, пов'язаних із криптовалютами. Розглянуто ключові прогалини законодавства, технічні та процедурні виклики, що ускладнюють допустимість та автентичність цифрових доказів. Запропоновано конкретні рішення, які базуються на міжнародних стандартах цифрової криміналістики та практиках Європейського Союзу.

Поява криптовалютних активів поставила перед системою кримінального правосуддя України нові виклики. У кримінальних провадженнях дедалі частіше фігурують цифрові докази: дані з блокчейн-мереж, криптовалютних бірж, електронних гаманців та інших цифрових платформ. Водночас українське законодавство не надає чітких механізмів їх використання. Це створює труднощі для слідчих, прокурорів та суддів, а також знижує ефективність протидії фінансовим злочинам.

Ключові проблеми та можливі рішення

1. Відсутність визначення цифрових доказів у КПК.

Проблема: у Кримінальному процесуальному кодексі немає чіткого поняття цифрових доказів. Це призводить до сумнівів у їх допустимості.

Рішення: внести до КПК окрему статтю, що визначатиме цифрові докази, їх джерела та процедуру збору. Прикладом може слугувати досвід Естонії.

2. Неврегульований статус криптовалют у кримінальному праві.

Проблема: Закон «Про віртуальні активи» не врегульовує процедуру арешту та конфіскації криптовалют.

Рішення: закріпити у КПК і ККУ процедури арешту цифрових активів та доступу до апаратних гаманців. Використати практику Німеччини, де поліція має право арештовувати криптовалютні кошти.

3. Проблема автентичності та допустимості.

Проблема: відсутні стандарти підтвердження автентичності даних із блокчейну.

Рішення: імплементувати міжнародні стандарти ISO/IEC 27037:2012 та забезпечити ведення chain of custody для цифрових доказів.

4. Відсутність спеціалізованої експертизи.

Проблема: українські судово-експертні установи не мають фахівців із криптовалютної криміналістики.

Рішення: створити державний центр цифрової криміналістики, а також залучати приватні компанії (Chainalysis, Elliptic) для експертиз.

5. Відсутність судової практики.

Проблема: брак рішень щодо допустимості цифрових доказів у справах із криптовалютами.

Рішення: розробити методичні рекомендації для суддів, використати досвід США та ЄС у визнанні даних із блокчейну доказами.

Схарактеризуємо перспективи вдосконалення законодавства

Для інтеграції України у європейський правовий простір важливо гармонізувати національне законодавство з Регламентом ЄС MiCA та рекомендаціями FATF. Необхідно запровадити системні зміни у КПК, створити інфраструктуру для цифрової криміналістики та забезпечити підготовку фахівців. Тільки так можна гарантувати ефективне використання цифрових доказів у кримінальному процесі.

Підведемо підсумки. Цифрові докази у сфері криптовалют стають ключовим інструментом у розслідуванні фінансових злочинів. Українське законодавство потребує модернізації: визначення цифрових доказів у КПК, регулювання арешту та конфіскації криптовалют, впровадження міжнародних стандартів автентичності та chain of custody, а також розвитку експертної бази. Ці кроки дозволять підвищити ефективність кримінального правосуддя та наблизити Україну до європейських стандартів правового регулювання.

Список використаних джерел:

1. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.
2. Regulation (EU) 2023/1114 of the European Parliament and of the Council on Markets in Crypto-assets (MiCA).
3. FATF Guidance on Virtual Assets and Virtual Asset Service Providers, 2021.
4. Кримінальний процесуальний кодекс України (чинна редакція).

ІНФОРМАЦІЯ ЯК ЕКОНОМІЧНИЙ РЕСУРС У ГЛОБАЛЬНОМУ СВІТІ: ЗАГРОЗИ І ПЕРСПЕКТИВИ РОЗВИТКУ

У сучасному глобалізованому світі інформація набуває статусу стратегічного ресурсу, що визначає конкурентоспроможність національних економік, корпорацій, суспільств та конкретних особистостей. Її значення суттєво зростає в умовах переходу до цифрової економіки, де інформаційні потоки стають основою створення доданої вартості. Проблема полягає в тому, що одночасно із зростанням значення інформаційних ресурсів посилюються і глобальні загрози: монополізація доступу до даних, зростання кіберзлочинності, інформаційні війни та дисбаланс між правом власності на інформацію і суспільною потребою у вільному доступі. Саме тому дослідження економічної природи інформації, її ролі у глобальному розвитку, а також потенційних ризиків і можливостей стає вкрай актуальним завданням сучасної науки.

У сучасній економіці інформація дедалі більше набуває статусу ключового ресурсу, що визначає не лише темпи інноваційного розвитку, а й здатність держав і корпорацій інтегруватися у глобальні ринки. Якщо у XX столітті головними факторами економічного зростання вважалися капітал, земля та праця, то у XXI столітті саме інформація й пов'язана з нею цифрова інфраструктура стають фундаментом нової економічної архітектури. Це обумовлено тим, що інформаційні ресурси створюють специфічну форму доданої вартості, засновану не на фізичному виробництві, а на генерації, аналізі й застосуванні знань. Також у XXI столітті інформація дедалі більше визначає траєкторію розвитку глобальної економіки. Її роль не обмежується лише технологічними галузями – вона інтегрується у всі сфери: від промисловості до державного управління. Глобальні корпорації – Amazon, Google, Microsoft, Alibaba – створюють свої ринкові переваги завдяки ефективному використанню інформаційних ресурсів. За оцінками McKinsey, до 2030 року цифрова економіка формуватиме понад 25 % світового ВВП. Водночас інформація є джерелом вразливостей: кіберзагрози у 2023 році завдали збитків на понад 8 трлн дол. США, що підкреслює подвійність цього ресурсу [1;2].

Особливістю інформації є її майже невичерпний характер за умови наявності технологічних засобів тиражування та обробки. На відміну від природних ресурсів, які обмежені у своїй фізичній природі, інформаційні ресурси здатні до багаторазового використання без втрати цінності. Отже, зростання обсягів даних і включення ширших масивів інформації у виробничі процеси створюють ефект масштабу, що підвищує продуктивність усіх учасників економічної системи [3].

За оцінками International Data Corporation (IDC), глобальний обсяг цифрових даних зріс із 64 зеттабайтів у 2020 році до понад 120 зеттабайтів у 2023-му, а до 2025 року прогнозується на рівні понад 175 зеттабайтів. Це свідчить про безпрецедентну швидкість накопичення інформаційного ресурсу, який фактично став основою нової економіки знань. Зростає і ринок big data: у 2022 році його вартість становила близько 274 млрд дол. США, а до 2030 року очікується понад 650 млрд дол. Швидкий розвиток штучного інтелекту, машинного навчання та хмарних обчислень формує основу нової інформаційної економіки XXI ст. [4;5].

Водночас інформація має й іншу специфічну рису – асиметрію доступу. Наявність даних не гарантує їх рівномірного використання всіма учасниками економіки. Великі транснаціональні корпорації та провідні держави накопичують значні обсяги інформації, які слугують для створення конкурентних переваг. В цьому аспекті проявляються наступні загрози:

- 1) монополізація інформаційних ресурсів великими корпораціями;
- 2) зростання масштабів кіберзлочинності (у 2023 році кібератаки призвели до збитків понад 8 трлн дол. США);
- 3) інформаційні війни та маніпуляції даними формують загрозу демократичним інститутам та ринковій інфраструктурі [6].

Перспективи розвитку інформації як економічного ресурсу залежать від здатності поєднати технологічні інновації з адекватним правовим та інституційним забезпеченням. ЄС ще у 2020 році презентував «Європейську стратегію даних», що передбачає створення єдиного ринку даних. Тому для України перспективним є поєднання національних програм цифровізації (зокрема, платформи «Дія») з гармонійною інтеграцією у європейський інформаційний простір.

Відзначимо й те, що вітчизняне підприємництво в умовах повномасштабного вторгнення може відновитись тільки за рахунок проактивної дієвої стратегії власного розвитку в кризових умовах. Провідною частиною цієї стратегічної політики є система фільтрування, збору, переробки, зберігання і надання актуальної інформації для внутрішнього і зовнішнього споживання. Провідними інститутами підтримки вітчизняної економіки на сьогодні і на середньостроковий період у майбутньому залишатимуться уряд України, уряди інших країн-партнерів вільного світу і міжнародні організації. Тому для їх активного залучення необхідно й надалі проводити системні євроінтеграційні інституційні реформи, посилювати прозорість в роботі з інформацією та її розповсюдженням. Враховуючи гібридну інформаційну війну РФ в ЄС та повноцінну інформаційну війну проти України – необхідно посилювати власні спроможності протидії таким заходам на державному, регіональному, корпоративному рівні, а також на рівні особистої інформаційної гігієни у використанні інформаційних ресурсів. При такому комплексному підході Україна більш успішно інтегруватиметься в євро-атлантичний простір і її економіка системно посилить власну конкурентоспроможність в глобалізованому світі.

В цілому, у міжнародних відносинах спостерігається тенденція до посилення напруження, до намагання управляти інформаційними потоками і спрямовувати їх проти глобальних опонентів, конкурентів, ворогів. Тому інтелектуально розвинені суспільства швидко реагують на ці виклики і формують власну інфраструктуру, що протидіє ворожій пропаганді, фейкам та провокаціям. Україна має також динамічно і ефективно реагувати на ці виклики, а також формувати власний інформаційний вплив у глобальному просторі, що повинен базуватись на розгалуженій мережі інформаційно-комунікаційних ресурсів та проактивній позиції державних органів влади, особливо у зовнішньополітичній та зовнішньоекономічній діяльності.

Підсумовуючи відзначимо, що інформація в глобальному сучасному світі виступає специфічним економічним ресурсом, який одночасно відкриває значні перспективи та створює серйозні загрози. Її інтеграція у виробничі процеси здатна забезпечити підвищення ефективності, зростання інноваційного потенціалу та формування нових бізнес-моделей. Водночас відсутність належного регулювання, концентрація ресурсів у руках небагатьох гравців і зростання ризиків кіберзлочинності можуть перетворити інформаційну економіку на джерело глобальних дисбалансів. Перспективи розвитку інформації як економічного ресурсу безпосередньо залежать від здатності міжнародної спільноти поєднати технологічні можливості з інституційними рамками, які б гарантували баланс між ефективністю використання й безпекою суспільства [7;8;9].

Список використаних джерел:

1. McKinsey Global Institute. The Future of Digital Economy. 2023. URL: <https://www.mckinsey.com>
2. Cybersecurity Ventures. Cybercrime Report 2023. URL: <https://cybersecurityventures.com>
3. OECD. Data-Driven Innovation. OECD Publishing, 2015. URL: <https://www.oecd.org>
4. IDC. Data Age 2025 Report. 2021. URL: <https://www.idc.com>
5. Statista. Big Data Market Size 2022–2030. URL: <https://www.statista.com>
6. World Economic Forum. Global Risks Report 2023. URL: <https://www.weforum.org>
7. Редзюк Є.В. Інформація та інформаційний вплив в сучасних геополітичних і геоekonomічних відносинах. І Всеукраїнська науково-практична студентська конференція «ІТ-простір сьогодення: тенденції, інновації та перспективи розвитку», Харківський національний університет імені В.Н. Каразіна, м.Харків, 16 жовтня 2024 р. – с.58-61
8. Редзюк Є.В. Формування конкурентних кластерів України в умовах глобальних викликів. Збірник наукових праць "Стратегія економічного розвитку України", КНЕУ ім. В.Гетьмана. – том 53, м.Київ, 2023. – с.63-77
9. Redziuk Y. Leading risks of geopolitical and geoeconomics for business activity in Ukraine during the war. Actual problems of International Relations. Vol. 1 No. 159 (2024).- p.138-145

Романюк В.І.

здобувач вищої освіти,

Маріупольський державний університет, м. Київ

Науковий керівник

Верительник С.М.

доктор філософії з публічного управління та адміністрування,

доцент, доцент кафедри публічного управління та адміністрування

Маріупольський державний університет, м. Київ

ЗАПРОВАДЖЕННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ В УПРАВЛІННІ БЕЗПЕКОВОЮ СФЕРОЮ

В умовах воєнного стану інноваційні технології перетворюються на ключовий інструмент ефективного публічного управління у сфері безпеки. Сучасна архітектура національної безпеки вибудовується завдяки цифровій трансформації, автоматизації управлінських процесів, застосуванню штучного інтелекту (ШІ), посиленню кіберзахисту, використанню геоаналітики та аналізу великих даних (Big Data) [1;5].

Інноваційні рішення дають змогу державі швидко реагувати на виникаючі загрози та удосконалювати процес ухвалення управлінських рішень.

Ізраїль. Використовує технології штучного інтелекту у військовій сфері та державному управлінні. Важливим прикладом є система Fire Weaver, яка інтегрує інформацію з розвідувальних дронів, супутників і бойових підрозділів у режимі реального часу. Державні структури активно співпрацюють із приватними стартапами через мережу національних інноваційних кластерів.

США. Застосовують платформу Palantir для аналізу великих масивів даних у сфері безпеки (розвідка, боротьба з тероризмом, управління кризами). Система JADC2 (Joint All-Domain Command and Control) інтегрує військові й цивільні структури в єдиний аналітичний простір.

Естонія. Є прикладом цифрової держави, де запроваджено платформу X-Road для безпечного обміну даними між структурами безпеки, охорони здоров'я, енергетики та цивільного захисту. У відповідь на кіберзагрози створено Кіберкомандування та Центр передового досвіду НАТО з кібероборони.

В Україні також реалізуються інноваційні ініціативи у сфері безпеки, приклади яких відображено в таблиці 1. У сфері кібербезпеки Національний координаційний центр кібербезпеки забезпечує централізовану координацію захисту державних органів від кіберзагроз. Геоаналітика реалізується через геопортали Міноборони та МВС, які інтегрують супутникові дані для оперативного моніторингу ситуацій. Програма «Армія дронів» розвиває безпілотні технології для потреб армії та МВС. Використання Big Data втілено у вигляді інформаційних панелей ДСНС, що аналізують дані про обстріли, евакуацію та пошкодження. Комунікаційні платформи «єЗахист» і «єВорог» сприяють збору розвідувальних даних від громадян та автоматизованому

інформуванню населення. Сукупність цих ініціатив створює основу для технологічно модернізованої та гнучкої системи безпеки.

Таблиця 1.

Українські ініціативи у сфері інновацій безпеки

Напрямок	Ініціативи	Опис
Кібербезпека	Нацкоординаційний центр кібербезпеки (НКЦК)	Координація кіберзахисту держорганів
Геоаналітика	Геопортал Міноборони та МВС	Інтеграція супутникових даних для моніторингу ситуацій
Безпілотні технології	Армія дронів	Закупівля та розвиток БПЛА для армії й МВС
Big Data	Інформаційні панелі ДСНС	Аналіз динаміки обстрілів, евакуації, пошкоджень
Комунікаційні платформи	«ЄЗахист», «ЄВорог»	Збір розвідувальних даних від громадян, автоматизовані сповіщення

Джерело: [2;3;6;7].

Разом з тим, реалізація інноваційних рішень у сфері безпеки супроводжується низкою викликів: від фрагментарності IT-інфраструктури державних установ та недостатнього рівня цифрових компетентностей на місцевому рівні – до ризиків витоку даних і кібердиверсій. Подальший розвиток можливий за умови створення єдиної національної цифрової платформи безпеки, подібної до Центру передового досвіду НАТО з кібероборони (CCD COE), активізації грантової підтримки оборонних стартапів та формування концепції «Smart Security State».

Використання штучного інтелекту в безпековій сфері забезпечує перехід від реактивного до проактивного підходу у протидії загрозам. Для України доцільно орієнтуватися на досвід держав НАТО, Ізраїлю та Естонії, адаптуючи його до власних умов із пріоритетом на розвиток ШІ, геоаналітики, кіберзахисту та інтегрованих цифрових систем.

Серед найбільш відомих прикладів можна відзначити компанію SKIFTECH, яка постачає системи бойового тренування на основі лазертаг-технологій для підготовки штурмових бригад; стартап Secutor, що розробляє БПЛА-камікадзе та FPV-дрони для фронтових підрозділів; компанію Infozahyst, чия технологія розвідки радіосигналів (SIGINT) використовується силами спеціальних операцій і артилерією; розробника систем штучного інтелекту AiLand Systems, який співпрацює з Генеральним штабом у сфері бойового аналізу; виробника засобів радіоелектронної боротьби Kvertus, що успішно пройшов державні випробування; а також українсько-естонський стартап Farsight Vision, який створює тактичні 3D-карти та візуалізацію місцевості для підрозділів ЗСУ, ДПСУ та СБУ [2-4].

Динамічний розвиток безпекових і оборонних технологій, а також суттєве зростання інвестицій у кіберзахист та інноваційні рішення, формують нові вимоги до можливостей органів публічного управління. Ефективне

використання цифрових платформ, штучного інтелекту й оборонних інновацій потребує не лише сучасної матеріально-технічної бази, але й висококваліфікованих фахівців, здатних інтегрувати ці інструменти у процеси планування, координації та реагування на загрози. Тому нарівні з розвитком технологічної інфраструктури першочерговим завданням постає зміцнення кадрового потенціалу органів публічного управління, що є ключем до їхньої стійкості та здатності адаптуватися в умовах воєнного стану.

Список використаних джерел:

1. Балабаниць А.В., Мацука В.М. Сучасна парадигма механізму управління фінансово-економічною безпекою держави. Економіка та суспільство. 2022. № 39. doi: <https://doi.org/10.32782/2524-0072/2022-39-65>
2. Інновації для перемоги: як Україна та НАТО об'єднали зусилля у підтримці оборонних стартапів. URL: <https://armyinform.com.ua/2024/06/18/innovacziyi-dlya-peremogy-yak-ukrayina-ta-nato-obyednaly-zusylyya-u-pidtrymczi-oboronnyh-startapiv/>
3. Команди понад 20 українських оборонних стартапів пройшли навчання в Кремнієвій долині. URL: <https://mod.gov.ua/news/komandi-ponad-20-ukrayinskih-oboronnih-startapiv-projshli-navchannya-v-kremniyevij-dolini-katerina-chernogorenko>
4. Стойка А.В., Верительник С.М., Мацука В.М. Діджиталізація управління проектами і вплив на світову економіку та інвестиції. Збірник наукових праць «Вчені записки». 2025. № 39(2). С. 45-58. URL: [https://vz.kneu.ua/archive/2025/39\(2\).04](https://vz.kneu.ua/archive/2025/39(2).04)
5. Управління фінансово-економічною безпекою держави та шляхи запобігання зовнішнім і внутрішнім загрозам: монографія/ А.В Балабаниць, О.І. Гапонюк, М.О. Горбашевська, Л.А. Кислова, В.Я. Омельченко, Л.В. Семкова, В.М. Мацука, К.В. Осипенко, Ф.Л. Перепадя. М., 2020. 223 с. URL: https://repository.mu.edu.ua/jspui/bitstream/123456789/1746/1/upravlinnia_finansov_o-ekonomichnoiu.pdf
6. Matsuka V., Horbashevsk M. Digital technologies in economic management: European trends of development and implementation [2.5]. Європейський досвід використання цифрових технологій в економіці=European experience in the use of digital technologies in the economy: кол. монографія / за ред. А. В. Череп, І. М. Дашко, Ю. О. Огренич та ін. Рига, Латвія: Baltija Publishing, 2025. С. 186–210. URL: <http://repository.mu.edu.ua/jspui/handle/123456789/9278>
7. Matsuka V., Horbashevsk M. International business strategies of digital transformation of the economy [3.2]. Теоретико-методичні засади використання цифрових технологій в Україні шляхом впровадження досвіду ЄС: кол. монографія / за ред. А.В. Череп, І.М. Дашко, Ю.О. Огренич, О.Г. Череп. Запоріжжя: Вид. ФОП Мокшанов В.В., 2024. С. 132-155. URL: <http://repository.mu.edu.ua/jspui/handle/123456789/8408>

Руденко Б.В.*здобувач вищої освіти,**Харківський національний університет радіоелектроніки**Науковий керівник***Кобилін І.О.***к.т.н., асистент кафедри Інформатики,**Харківський національний університет радіоелектроніки*

МОДЕЛЬ ZERO TRUST ДЛЯ ІНФОРМАЦІЙНИХ СИСТЕМ У СУЧАСНИХ УМОВАХ КІБЕРЗАГРОЗ

Сучасні кіберзагрози вимагають кардинальної зміни підходів до забезпечення інформаційної безпеки. Традиційні моделі безпеки, засновані на концепції "довіри за замовчуванням" до внутрішніх ресурсів, виявилися недостатньо ефективними у протистоянні сучасним атакам. У цьому контексті модель Zero Trust (Нульова Довіра) представляє зміщення від локаційно-орієнтованого до підходу забезпечення безпеки орієнтованого на дані [1].

Модель Zero Trust базується на семи фундаментальних принципах згідно з NIST SP 800-207 [3]: всі джерела даних і обчислювальні сервіси вважаються ресурсами незалежно від розташування; захист всіх комунікацій незалежно від мережевого розташування; доступ до ресурсів надається на основі сесійних рішень з урахуванням контекстуальних факторів; доступ визначається динамічною політикою; постійний моніторинг цілісності та безпекового статусу всіх активів; динамічна автентифікація та авторизація перед наданням доступу; збір усієї інформації про стан активів для покращення безпекової позиції [3].

Ключовими компонентами є системи управління ідентичністю та доступом (IAM), мікросегментація мережі, шифрування даних і безперервний моніторинг [2]. Мікросегментація створює захищені периметри навколо критичних активів, обмежуючи латеральне поширення загроз. Ефективність мікросегментації виражається коефіцієнтом зменшення поверхні атаки:

$$R = 1 - \left(\frac{S_{segmented}}{S_{total}} \right),$$

де R – коефіцієнт зменшення ризику, $S_{segmented}$ – поверхня атаки після сегментації, S_{total} – загальна поверхня атаки до сегментації.

Імплементація моделі Zero Trust здійснюється поетапно через створення захищених анклавів (Protect Surface), що містять найбільш критичні дані, активи, програми та сервіси організації [2]. NIST SP 800-207 та пов'язана з ним спеціальна публікація NIST 1800-35 підкреслюють, що організації повинні спочатку скласти карту та класифікувати свою поверхню захисту – це включає

конфіденційні дані, критично важливі додатки, інтелектуальну власність та відповідні активи [3].

Розмір захищеної поверхні суттєво менший за традиційний периметр атаки, що дозволяє застосовувати більш ретельні засоби контролю. Процес переходу включає ідентифікацію критичних активів, картування транзакційних потоків, побудову архітектури Zero Trust, створення політик доступу та безперервний моніторинг.

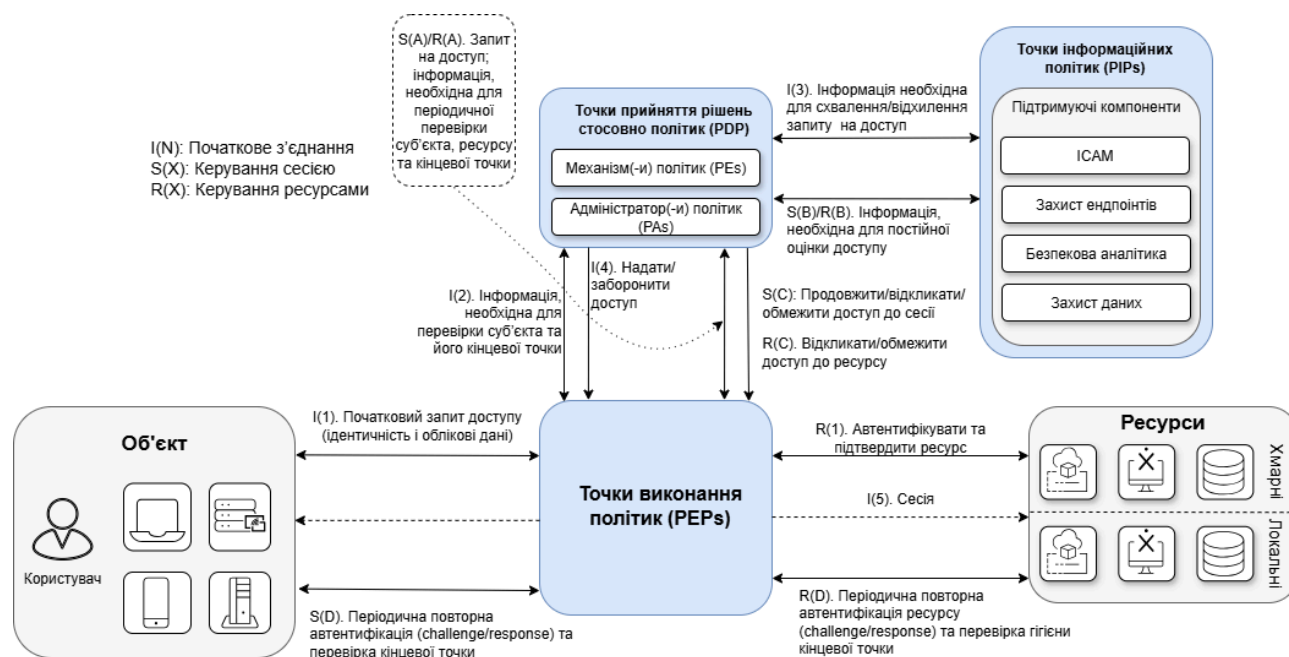


Рис. 1 – Абстрактна еталонна архітектура ZTA

Сучасні реалізації Zero Trust використовують контекстно-залежну мультифакторну автентифікацію з динамічною оцінкою ризику. Рівень довіри T до користувача формалізується як:

$$T = f(U, D, L, B, A),$$

де U – профіль користувача, D – характеристики пристрою, L – геолокаційні дані, B – поведінкові патерни, A – атрибути мережевого середовища. Система безперервно аналізує ці параметри та динамічно коригує рівень доступу, застосовуючи принцип найменших привілеїв.

Параметри цієї функції оцінюються за допомогою машинного навчання, аналітики поведінки користувачів (User Entity Behavior Analysis), ризик-орієнтованих моделей прийняття рішення, які дозволяють посилювати автентифікацію у разі перевищення порогу ризику. Контекстно-залежна MFA забезпечує баланс між безпекою і зручністю, адже для низькоризикових сценаріїв автентифікація може проходити з меншими складнощами, тоді як при підозрілих умовах застосовуються додаткові рівні перевірок.

Застосування таких адаптивних механізмів відповідає принципам безперервної перевірки (continuous verification) в Zero Trust і дозволяє

ефективно боротися з класичними та сучасними загрозами, такими як крадіжка облікових даних, соціальна інженерія тощо.

Таблиця 1.

Порівняльна таблиця Zero Trust та традиційної архітектур

Критерій	Традиційна інфраструктура	Zero Trust інфраструктура
Модель довіри	Довіра за замовчуванням всередині периметру	Ніколи не довіряй, завжди перевіряй
Сегментація мережі	Макросегментація, великі мережеві сегменти	Мікросегментація, ізоляція на рівні застосунків
Автентифікація	Одноразова при вході в мережу	Безперервна протягом всієї сесії
Контроль доступу	Статичний, базований на ролях	Динамічний, контекстно-залежний
Моніторинг	Периметро-орієнтований	Комплексний, орієнтований на усі IT-активи
Реагування на інциденти	Повільне, мануальне	Автоматизоване, в реальному часі
Поширення загроз	Можливість латерального руху по мережі	Обмежене мікросегментацією

Повномасштабна агресія росії проти України продемонструвала критичну важливість застосування моделі Zero Trust. Російські кіберугруповання APT44 (Sandworm), Gamaredon, Armageddon активно атакують українські державні системи, критичну інфраструктуру та приватний сектор. Згідно з аналітичним звітом CERT-UA за першу половину 2024 року, основними цілями є дестабілізація урядових систем, створення проблем у критичних секторах та знищення інформації.

У цьому контексті Zero Trust забезпечує захист від латерального поширення загроз всередині скомпрометованих мереж через мікросегментацію та безперервну верифікацію запитів. Навіть у випадку успішного проникнення, зловмисники не можуть вільно переміщуватися мережею та отримувати доступ до критичних ресурсів. Модель забезпечує швидке виявлення аномальних дій через аналіз поведінкових патернів (UEBA) та автоматизовані механізми реагування.

Список використаних джерел:

1. CISA. Zero Trust Maturity Model. 2023. 32 p. URL: <https://www.cisa.gov/zero-trust-maturity-model>.
2. Cloud Security Alliance. Defining the Zero Trust Protect Surface. URL: <https://cloudsecurityalliance.org/artifacts/defining-the-zero-trust-protect-surface>.
3. Zero Trust Architecture. NIST Special Publication 800-207. 2020. 59 p.

Самойленко А.Р.

здобувач вищої освіти,

Державний біотехнологічний університет

Науковий керівник

Сирий В.М.

старший викладач кафедри інформаційних технологій,

кібернетики та захисту інформації

Державний біотехнологічний університет

КІБЕРБЕЗПЕКА В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ У ГІБРИДНИХ КОНФЛІКТАХ ТА ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ

У сучасних гібридних конфліктах кібератаки, інформаційна війна та збройне ураження критичної інфраструктури застосовуються комплексно.

Використання інструментів штучного інтелекту (АІ, ШІ) дає змогу створювати нові загрози: автоматизовані хакерські атаки, АІ-віруси-шифрувальники, фішинг з АІ-згенерованим вмістом, дипфейки тощо. Одночасно зловмисники поєднують кібератаки з дезінформацією в соцмережах і масмедіа, аби підірвати довіру до влади й посіяти паніку.

У другій половині 2024 року кількість кібернападів на українські ресурси зросла на 48%, що свідчить про системну кампанію проти цифрової інфраструктури [1].

За останні роки в Україні й у світі зросла інтенсивність та різноманітність кібератак. Хакери активно експериментують з АІ-інструментами для створення нових шкідливих програм. Це створює асиметричну динаміку, де атаки стають більш ефективними, а захист вимагає постійної адаптації.

ШІ стає не тільки інструментом в арсеналі зловмисників; він фундаментально змінює ландшафт загроз, надавши зловмисникам можливості для масштабування, персоналізації та модифікації атак.

Так АІ-віруси-шифрувальники (наприклад, PromptLock) самостійно генерують шкідливий код і швидко змінюють форму, щоб уникнути виявлення стандартними методами.

Фішинг традиційно залишається одним з найефективніших методів кібератак, оскільки експлуатує людський фактор, а не технічні вразливості. А з появою генеративного ШІ ця загроза вийшла на новий рівень. Так за один рік із запуску ChatGPT кількість фішингових атак, пов'язаних з використанням нейромереж зросла на 1265%.

Таке зростання безпосередньо корелює з появою у відкритому доступі моделей, які дозволяють зловмисникам автоматизувати процеси, що раніше вимагали значних людських зусиль. Наприклад, у минулому році понад 67% фішингу були з АІ-згенерованим текстом, у якому з відкритих джерел використовувались персональні дані родичів, друзів, колег. Це призвело до статистики кліків у 44% випадків, на відміну від рівня 19–28% «традиційного» фішингу [2].

ШІ також надає змогу генерувати реалістичні фальшиві відео, аудіо чи зображення впливових осіб. Це створює умови, в яких люди починають сумніватися в автентичності будь-якого контенту і робить суспільство більш вразливим до маніпуляцій.

Зловмисникам AI-інструменти дозволяють автоматично знаходити вразливості та створювати динамічне шкідливе програмне забезпечення. Вони використовують генеративні інструменти для автоматизованого сканування серверів та підбору атакуючих алгоритмів, що в свою чергу дозволяє невеликим групам або навіть окремим особам проводити «масові» атаки, які можуть завдати великих економічних і соціальних збитків.

Проте ШІ надає нові можливості не тільки для створення кіберзагроз, але й для засобів захисту.

Нейромережі дозволяють захисникам кіберпростору протистояти загрозам зі швидкістю та масштабом, які непідвладні людині. Наприклад, у високоризикових середовищах, таких як енергетична інфраструктура, впровадження ШІ-систем дозволило досягти 98% рівня виявлення загроз та 70% скорочення часу реагування на інциденти [3].

Крім того, ШІ автоматизує рутинні завдання, такі як аналіз журналів, сортування загроз та ініціювання попередньо визначених дій, наприклад, ізоляцію ураженої системи або блокування шкідливих IP-адрес за лічені секунди. Така технологічна еволюція дозволяє автоматизувати рутинні та «низько-інтелектуальні» завдання, змінювати роль людини для зосередження на стратегічному мисленні, та розробці стратегій.

Прогнози вказують на стрімке зростання ринку кібербезпеки, що використовує генеративний ШІ, з очікуваним десятикратним зростанням до 2034 року. Майбутнє захисту полягає також в переході до уніфікованих платформ, які об'єднують дані від стадії розробки програмного забезпечення до моніторингу в реальному часі.

Отже, дослідження кібербезпеки в умовах інформаційної війни у гібридних конфліктах свідчить про її глибокі трансформації, що відбуваються під впливом штучного інтелекту.

Список використаних джерел:

1. Кібератаки на бізнес України 2025: Нові Вектори Загроз та Захист. URL: <https://surl.lu/iehnhg> (дата звернення: 29.09.2025).
2. AI проти вас: чому фішинг став ще небезпечнішим та як від нього захиститися. URL: <https://surl.li/ejxdfx> (дата звернення: 29.09.2025).
3. Штучний інтелект змінює світ: шанси і виклики для України. URL: <https://surli.cc/ohptrj> (дата звернення: 29.09.2025).

Світличний В.А.,

к.т.н., доцент

vit.svet@ukr.net

Ковтун І.А.,

Курсант

morzog08092006@gmail.com

*Харківський національний університет внутрішніх справ
м. Кам'янець-Подільський, Україна*

СУЧАСНА БОРОТЬБА КІБЕРПОЛІЦІЇ З РОСІЙСЬКОЮ ПРОПАГАНДОЮ

Анотація: У статті досліджено сучасні підходи кіберполіції до протидії російській пропаганді в цифровому просторі. Розглянуто механізми поширення дезінформації через соціальні мережі, фейкові новинні сайти та штучно створені інформаційні кампанії, що становлять серйозну загрозу національній безпеці. Особливу увагу приділено технологічним інструментам, які використовують правоохоронні органи для виявлення та нейтралізації пропагандистських атак, включаючи системи штучного інтелекту для аналізу контенту, виявлення бот-мереж і маніпулятивних алгоритмів.

Ключові слова: кіберполіція, інформаційна безпека, російська пропаганда, штучний інтелект, дезінформація, кібербезпека.

Постановка проблеми. У контексті сучасного інформаційного суспільства Росія веде проти України системну гібридну війну, в якій дезінформація й пропаганда виступають ключовими інструментами психологічного впливу. Через телебачення, інтернет-ресурси та соціальні мережі противник постійно формує викривлену картину реальності, маніпулює емоціями та підриває довіру до державних інституцій. Це створює загрозу не лише національній безпеці, а й демократичним процесам, сприяючи соціальній дестабілізації та «виготовленню» примусових уявлень про світ [1, с. 85-100].

Метою статті є аналіз сучасних методів протидії кіберполіції російській пропаганді в цифровому інформаційному просторі, а також розробка науково обґрунтованих рекомендацій щодо вдосконалення механізмів захисту національного інформаційного середовища.

Виклад основного матеріалу. Кіберпропаганда – це підхід до інформаційно-психологічного впливу, який реалізується через цифрові комунікаційні канали. Вона відрізняється від традиційної пропаганди інтеграцією алгоритмічних технологій, таргетованих кампаній та високою швидкістю розповсюдження контенту. До характерних механізмів кіберпропаганди належать: мережі автоматизованих акаунтів (боти); координація поведінки через алгоритмічні системи; таргетинг аудиторій на основі аналітики великих даних; а також змішування правдивих і неправдивих повідомлень, що створює гібридні операції. Все це підсилюється застосуванням

штучного інтелекту: генеративні моделі дозволяють формувати персоналізований контент і створювати ілюзію природного спілкування [2, с. 5-7].

Сучасний російський пропагандистський апарат базується на розгорнутій багатоканальній інфраструктурі впливу, що активно використовує соціальні мережі (Facebook, Twitter, Telegram, YouTube), фейкові акаунти та сайти, бот-мережі й організовані групи тролів. Ці структури імітують незалежні ЗМІ, контролюють алгоритми активності та координовано поширюють дезінформацію. Зокрема, «фабрики тролів» та бот-ферми забезпечують масове накручування пропагандистських наративів – поєднання справжнього й сфальсифікованого контенту створює потужний ефект «вогняного шлангу брехні», ускладнюючи виявлення й нейтралізацію атак [3, с. 3-5].

Російські кампанії дезінформації системно руйнують суспільну довіру до державних установ, формують альтернативну інформаційну реальність, де реальні події замінюються вигідними Кремлю наративами, і цим провокують соціальну розділеність. Такі операції підривають потенціал суспільної єдності в критичні моменти, ослаблюють ефективність державної політики та сприяють реалізації геополітичних інтересів РФ. Особливо руйнівним є їх довготривалий вплив: систематичне поширення дезінформації призводить до ерозії критичного мислення, сприяючи формуванню стійких маніпулятивних установок у масовій свідомості [4, с. 1-2].

Сучасна кіберполіція України функціонує як спеціалізований підрозділ Національної поліції, що відповідає за запобігання, виявлення та розслідування кіберзлочинності, включно з інформаційно-пропагандистськими атаками. Її ключові повноваження охоплюють моніторинг цифрового простору, блокування шкідливого контенту, ідентифікацію джерел дезінформації, а також активну міжнародну співпрацю. Упродовж 2023 року кіберполіція ініціювала й забезпечила участь у понад 18 міжнародних операціях, виконуючи багаторівневі заходи для протидії транснаціональним кіберзагрозам з залученням правоохоронців із США, Норвегії, Франції та інших країн [5].

У сфері технологічного розвитку особлива увага приділяється впровадженню систем аналізу великих даних та штучного інтелекту, що дозволяє оперативно реагувати на інциденти та підсилювати кіберстійкість України, зокрема під час обміну досвідом на міжнародних платформах (через участь у конференціях EU4DigitalUA та співпрацю з Інтерполом і Європолом) [6].

Українська кіберполіція, застосовуючи багаторівневий підхід для стримування пропагандистських кампаній, інтегрує аналіз алгоритмів соціальних мереж з використанням штучного інтелекту для автоматичної ідентифікації ботів і координаційних мереж. Виявлення підозрілої активності відбувається через детальні поведінкові моделі – такі як частота постів, характер взаємодії й алгоритмічна аномалія. Цей технологічний підхід поєднується з міжнародною співпрацею: взаємодією з НАТО, зокрема через Центр стратегічної комунікації (StratCom COE), та платформами обміну

інформацією про дезінформаційні загрози – як-от EU DisinfoLab – що забезпечує узгоджені транснаціональні контрзаходи [7, с. 10-12].

Українська кіберполіція досягла помітних результатів у стримуванні російських пропагандистських мереж. Водночас із технічними заходами з блокування понад 1 500 фейкових новинних ресурсів, які маскувалися під автентичні ЗМІ щоб поширювати дезінформацію, був реалізований цільовий захід проти великих проросійських Telegram-каналів із аудиторією понад 500 000 підписників. Вони активно поширювали фальшиві наративи про ЗСУ та міжнародну підтримку України. У 2023 році була проведена операція з деанонізації та притягнення до відповідальності адміністраторів кількох «трольових ферм», які координували масові атаки на соціальних платформах. Це свідчить про суттєве зростання ефективності українських правоохоронних органів в контексті протидії складним технологічно-несправжнім інформаційним загрозам [8, с. 1-4].

Протидія цифровій пропаганді в Україні стримується низкою структурних правових бар'єрів. Зокрема, існує відсутність єдиних міжнародних правових норм щодо інформаційних кіберзлочинів, що ускладнює притягнення до відповідальності осіб, які діють із-за меж різних юрисдикцій. Анонімність в інтернет-просторі значно ускладнює встановлення авторства цифрових атак чи дезінформаційних кампаній. Водночас національна юридична практика часто не має достатніх механізмів для оперативного блокування шкідливого контенту без порушення свободи слова. Тому необхідне подальше вдосконалення законодавства у напрямі встановлення меж державного втручання та розробка справді узгоджених міжнародних інструментів, здатних протидіяти транснаціональним мережам дезінформації [9, с. 45-47].

Сучасна боротьба з цифровою пропагандою стикається зі значними технологічними викликами, зокрема адаптацією зловмисників до алгоритмів модерації соцмереж і широким впровадженням генеративного ШІ для створення правдоподібного контенту: текстів, зображень і відео. Використання VPN та анонізаторів ускладнює блокування, а схеми маскування бот-мереж під органічну активність дедалі важче виявити за допомогою традиційного аналізу даних. Обсяг атак часто перевищує можливості ручного моніторингу, що робить необхідним розвиток проактивних AI-рішень для автоматизованого виявлення нових маніпулятивних технологій у реальному часі [10, с. 3-5].

Висновки: Сучасна боротьба з російською кіберпропагандою вимагає комплексного підходу, що поєднує технологічні інновації (AI-аналіз даних, автоматизований моніторинг глибоких фейків), правові ініціативи (гармонізація законодавства, міжнародні санкції) та системну медіаосвіту населення, оскільки, незважаючи на успіхи у блокуванні пропагандистських мереж і Telegram-каналів, кіберполіція продовжує стикатися з викликами швидкої адаптації пропагандистів, анонімності джерел дезінформації та глобального масштабу загрози, що потребує подальшого розвитку проактивних стратегій, міжнародної координації та постійного вдосконалення кібербезпекових механізмів для ефективного захисту інформаційного суверенітету України.

Список використаної літератури

1. Варга, Т. М. Дезінформація та пропаганда як інструменти ведення гібридної війни Росії проти України. Ужгородський національний університет, 2024. С. 85–100.
2. Ховард, П. Н. Обчислювальна пропаганда. 2024. С. 57.
3. Пол та Метьюз. Модель російської пропаганди "пожежний шланг брехні". RAND, 2016. С. 3–5.
4. Одартченко, К. Боротьба з дезінформацією: постійний виклик для демократії. Інститут досліджень зовнішньої політики, 24 січня 2025. С. 1–2.
5. Звіт про результати роботи Департаменту кіберполіції Національної поліції України у 2023 році. URL: <https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-i-naczionalnoyi-policziyi-ukrayiny-u--roczni-4792>.
6. Обмін досвідом і кращими практиками: кіберполіцейські взяли участь у міжнародній конференції з кіберстійкості. URL: <https://npu.gov.ua/news/obmin-dosvidom-i-krashchymy-praktykamy-kiberpolitseiski-vzialy-uchast-u-mizhnarodnii-konferentsii-z-kiberstiikosti>.
7. Поте. Теорія обчислювальної пропаганди та система виявлення ботів: критичний огляд літератури. 2024. С. 10–12.
8. Кіреєв та ін. Характеристика та виявлення акаунтів, які поширюють пропаганду в Telegram. arXiv, 2024. С. 1–4.
9. Якимчук, Особливості правового регулювання протидії кіберзлочинності в Україні: порівняльно правовий аспект. 2021. С. 45–47.
10. Да Сан Мартіно та ін. Огляд виявлення обчислювальної пропаганди. 2020. С. 3–5.

УДК 004.8:004.056

Семенюта В.І.

Здобувач вищої освіти

Державний торговельно-економічний університет

Науковий керівник

Міщенко А.О.

к. е. н., доцент,

доцент кафедри цифрової економіки та системного аналізу

Державний торговельно-економічний університет

МОЖЛИВОСТІ І ЗАГРОЗИ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ

Ми живемо у часи небаченого розквіту кіберзлочинності. Кількість та складність атак на диджитал-системи продовжує зростати вже декілька років поспіль, хакери постійно вигадують нові методи злочинів та активно використовують новітні технології.

Як бізнесу протистояти цим загрозам? Як забезпечити безпеку своїх даних, систем та мереж? Однією з можливих відповідей є застосування засобів штучного інтелекту.

Однією із домінуючих тенденцій сучасного світу є інтенсивний розвиток та удосконалення науки і техніки, зокрема інформаційно-комунікаційних технологій (ІКТ). Проголошена Резолюцією 3384(XXX) ГА ООН від 10 грудня 1975 р. Декларація про використання науково-технічного прогресу в інтересах світу та на благо людства, підкреслює, що науково-технічний прогрес став одним із найважливіших факторів розвитку суспільства. Безсумнівно, саме науково-технічний прогрес створює все більш широкі можливості для покращення умов життя суспільства, де особливу роль виконує штучний інтелект [1].

Перші інструменти на основі ШІ почали застосовуватись для потреб безпеки ще наприкінці 80-х років. Це були системи оповіщення про кіберзагрози на основі заздалегідь визначених правил та параметрів. У 2000-х роках роль ШІ почала зростати, передусім завдяки прогресу в області машинного навчання. Але справжній прорив у кібербезпеці забезпечив стрімкий розвиток нейромереж та генеративного ШІ останніми роками.

Сьогодні штучний інтелект у кібербезпеці вже перетворився на двосічне лезо, яке може бути як найбільшою загрозою, так і найефективнішим засобом захисту. Все залежить від того, у чиїх руках опиняється цей інструмент.

ШІ може сприяти виявленню та передбаченню загроз такими способами:

- аналіз великих наборів даних у режимі реального часу: активний моніторинг вашої мережі загроз вимагає сортування величезних обсягів структурованих і неструктурованих даних. Без ШІ цей процес потребував би значного часу та людських ресурсів. ШІ може автоматизувати моніторинг загроз, зменшуючи кількість людських помилок і роблячи виявлення ефективнішим.

- визначення незвичайної діяльності: ідентифікація ризиків має вирішальне значення для прогнозування ШІ в кібербезпеці. ШІ може аналізувати зміни мережі та використовувати ці шаблони для прогнозування. Він може використовувати поведінкову аналітику для виявлення незвичайних дій у межах і за межами вашої системи.

- моделювання потенційних векторів атак: методи або шляхи, які кіберзловмисники використовують для доступу до системи або мережі, називаються векторами атак. ШІ відіграє вирішальну роль у прогнозуванні векторів атак на основі історичних даних. Він використовує методи машинного навчання для аналізу історичних даних на наявність шаблонів і аномалій, що може допомогти передбачити майбутні вектори атак.

Крім того, прогнозується, що до 2026 року понад 80% підприємств матимуть власні генеративні API та моделі ШІ.

Запровадження штучного інтелекту обумовлено декількома факторами, зокрема бажанням покращити взаємодію з клієнтами, збільшити дохід і покращити безперервність бізнесу. Кібербезпека також є ключовою сферою, де використовується штучний інтелект: 51% власників бізнесу планують посилити

свої зусилля з кібербезпеки за допомогою цієї технології [2]. AI надає значні переваги для організацій, але його також використовують для посилення та посилення кібератак.

Фахівці з кібербезпеки та IT повинні визнати подвійну природу ШІ, оскільки хакери розглядають його як додаткову зброю проти вразливих об'єктів. Вони ж використовують штучний інтелект для підвищення якості свого контенту соціальної інженерії. Використовуючи його, можна створювати граматично точний і безпомилковий веб-вміст, текстові повідомлення, фішингові електронні листи та навіть дуже переконливі голосові повідомлення. Ця оманлива тактика має на меті змусити жертв отримати доступ до шкідливих посилань, текстових повідомлень і електронних листів. Здатність штучного інтелекту аналізувати величезні обсяги даних із таких джерел, як соціальні медіа-платформи, дозволяє створювати персоналізовані повідомлення, які жертвам важко легко відхилити.

Атаки на конфіденційність і атаки на ухилення додають додаткові рівні складності захисту ШІ. Атаки на конфіденційність намагаються зібрати конфіденційну інформацію про штучний інтелект або його навчальні дані, використовуючи законні запитання для зворотного проектування моделі. Атаки ухилення, що відбуваються після розгортання, намагаються змінити реакцію системи ШІ на традиційні вхідні дані [3]. Це включає оманливі модифікації дорожніх знаків, що створює ризики для автономних транспортних засобів. Основна проблема полягає в тому, що важко змусити моделі штучного інтелекту відмовитися від навченої поведінки, навіть якщо вона виявляється зловмисною або шкідливою.

Настає нова ера виявлення загроз і реагування на них, і це цілком може змінити те, як організації реагують на кіберзагрози. Штучний інтелект має потенціал для значного зменшення робочого навантаження аналітиків, забезпечуючи підвищення продуктивності та звільняючи їх для зосередження на стратегічному плануванні та інших критично важливих стратегіях. Тобто нейромережа може допомогти нам перейти від реагування до проактивних дій, дозволяючи організаціям набирати обертів і залишатися попереду безлічі кіберзагроз [4].

Отже, штучний інтелект у сфері кібербезпеки представляє собою технологію подвійного призначення, яка одночасно створює нові можливості для захисту та нові виклики для організацій. З одного боку, ШІ революціонізує процеси виявлення загроз завдяки можливості аналізувати величезні обсяги даних у режимі реального часу, ідентифікувати незвичайну активність та моделювати потенційні вектори атак. Це дозволяє організаціям переходити від реактивного реагування на інциденти до проактивного прогнозування та запобігання кіберзагрозам. Водночас кіберзлочинці також активно використовують можливості штучного інтелекту для створення більш досконалих фішингових атак, персоналізованих шахрайських повідомлень та складних атак на конфіденційність і ухилення, що значно ускладнює їх виявлення традиційними методами.

Майбутнє кібербезпеки нерозривно пов'язане з подальшим розвитком та впровадженням технологій штучного інтелекту, що вимагає від фахівців галузі постійної адаптації та підвищення кваліфікації. Прогнозоване масове впровадження генеративних моделей ШІ більшістю підприємств до 2026 року підкреслює стратегічну важливість цієї технології для бізнесу. Однак успішне використання ШІ у кібербезпеці потребує збалансованого підходу, який враховує не лише технічні можливості, а й етичні аспекти та питання конфіденційності. Організаціям необхідно розглядати штучний інтелект як цінний інструмент у комплексній стратегії захисту, зберігаючи при цьому пильність щодо нових вразливостей, які він може створювати, та постійно вдосконалюючи свої підходи до кібербезпеки у відповідь на еволюцію загроз.

Список використаних джерел:

1. European Business Association. URL: <https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/>
2. BDO Україна. URL: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection>
3. Wezom. URL: <https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi>
4. Кібербезпека в інформаційному суспільстві. Інформаційно-аналітичний дайджест. Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2024 © Національна бібліотека України імені В.І. Вернадського, 2024, с. 205-217
5. Основи інформаційної та кібернетичної безпеки. В.Л. Бурячок, Р.В. Киричок, П.М. Складанний, 2019, с. 8-9.

УДК 330.341.1:334.722:338.12

Спіцина А.О.

здобувач освіти,

*ВСП Кам'янець-Подільський фаховий коледж
НРЗВО «Кам'янець-Подільський державний інститут»*

Науковий керівник

Мельник М.В.

*Викладач ВСП Кам'янець-Подільський фаховий коледж
НРЗВО «Кам'янець-Подільський державний інститут»*

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА

Сучасне суспільство стрімко розвивається у напрямку цифровізації, що зумовлює зростання обсягів обробки персональних даних у різних сферах – від

державного управління до електронної комерції. Водночас зростає й кількість кіберзагроз, пов'язаних із несанкціонованим доступом, витоками інформації та неправомірним використанням даних громадян [1; 4].

Захист персональних даних стає однією з ключових складових інформаційної безпеки. Основними ризиками сьогодні є:

Сучасні зловмисники використовують різні методи для злому паролів, зокрема:

1. використання методів соціальної інженерії (фішинг, шахрайські сайти, маніпуляції в соцмережах);
2. зловживання з боку компаній, що збирають дані без належного інформування користувачів;
3. недостатня поінформованість громадян про правила кібергігієни [2; 5].

Правове забезпечення захисту персональних даних в Україні регулюється Законом «Про захист персональних даних» [3], однак для ефективної протидії викликам цифрової епохи необхідна гармонізація із міжнародними стандартами, зокрема Загальним регламентом про захист даних (GDPR) [6].

Важливу роль відіграють технічні інструменти захисту: шифрування даних, багатофакторна автентифікація, системи контролю доступу, а також постійний моніторинг та аудит інформаційної інфраструктури [2,7]. Однак навіть найсучасніші технології будуть неефективними без належної культури кібергігієни серед користувачів [4].

Отже, захист персональних даних у цифровому суспільстві вимагає комплексного підходу, що поєднує правові механізми, технічні рішення та освітні заходи, спрямовані на формування безпечної поведінки в інформаційному просторі.

Список використаних джерел:

1. Баранов О. А. Інформаційна безпека: навчальний посібник. – Київ: КНЕУ, 2020.
2. Гриценко О. Кібербезпека та захист персональних даних: сучасні виклики. // Інформаційне право. – 2021. – №2. – С. 45–52.
3. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17>
4. Кузьменко О. В., Чаплигіна Ю. В. Проблеми захисту персональних даних у цифровому середовищі. // Юридична наука. – 2022. – №3. – С. 88–95.
5. CERT-UA. Звіт про кіберінциденти в Україні за 2023 рік. [Електронний ресурс]. – Режим доступу: <https://cert.gov.ua/>
6. General Data Protection Regulation (GDPR). [Електронний ресурс]. – Режим доступу: <https://gdpr.eu/>
7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems.

Тищенко С. І.

*кандидат педагогічних наук,
доцент кафедри економічної кібернетики,
комп'ютерних наук та інформаційних технологій
Миколаївського національного аграрного університету*

Богатєнкова О. Є.

*викладач кафедри економічної кібернетики,
комп'ютерних наук та інформаційних технологій
Миколаївського національного аграрного університету*

СТАТИСТИЧНИЙ АНАЛІЗ ВІДМІННОСТЕЙ РОЗПОДІЛІВ ОЗНАК І ЧАСОВИХ ПАТЕРНІВ ШАХРАЙСЬКИХ ТРАНЗАКЦІЙ

У сучасних фінансових системах проблема кіберзагроз, зокрема шахрайства з платіжними картками, набула особливої гостроти. Зростання обсягів електронної комерції та поява нових схем протиправних дій роблять цю проблему глобальною. У зв'язку з цим актуальним є вивчення статистичних характеристик транзакцій, що дозволяє виявити відмінності між легальними та шахрайськими операціями. Особливий інтерес становить аналіз часових патернів, оскільки поведінка зловмисників часто відрізняється від дій звичайних користувачів.

Методологічна основа дослідження ґрунтується на статистичному аналізі транзакційних даних із використанням спеціалізованих інструментів обробки даних та методів математичної статистики. Застосовано відкритий датасет Credit Card Fraud Detection, який містить 284807 транзакцій, серед яких 492 позначені як шахрайські (0,17%). Така дисбалансована структура є типовою для задач фінансової безпеки та вимагає ретельного врахування під час аналізу. Усі ознаки в наборі даних поділено на три групи: анонімізовані змінні V1–V28, отримані за допомогою методу головних компонент (PCA), які зберігають статистичні властивості реальних характеристик клієнтів та операцій; фінансова змінна Amount, що відображає суму транзакції; часові характеристики, які кодують момент здійснення операції. Для зручності аналізу час перетворено у години доби (Година), а також закодовано циклічними змінними Time_sin та Time_cos, що враховує періодичність на межі доби (наприклад, близькість 23:59 та 00:01).

Для описового аналізу обчислено базові статистики (середнє значення, стандартне відхилення, мінімум, максимум, квартилі) окремо для легальних (клас 0) і шахрайських (клас 1) транзакцій. Це дозволило виявити загальні закономірності та ключові відмінності у розподілах ознак. Усі обчислення здійснено мовою Python з використанням бібліотек pandas та numpy. Отримані статистики стали основою для інтерпретації поведінкових профілів користувачів і виявлення характерних патернів шахрайських дій.

Аналіз транзакційного датасету виявив суттєві відмінності між легальними та шахрайськими операціями, що проявляються як у розподілах

окремих ознак, так і в часових патернах. Найбільш яскраво відмінності простежуються в анонімізованих змінних, зокрема V1 та V2. Для легальних транзакцій середнє значення V1 становить 0,008 при стандартному відхиленні 1,93, тоді як у шахрайських воно зсунуте до -4,77 зі значно більшою дисперсією (6,78). Подібна ситуація спостерігається для V2, де середнє у легальних дорівнює -0,006, а у шахрайських зростає до 3,62. Це свідчить про те, що шахрайські транзакції концентруються у відмінних областях простору ознак, формуючи специфічний статистичний профіль.

Важливу інформацію надає змінна Amount. Середнє значення для шахрайських транзакцій (122,21) дещо вище, ніж для легальних (88,35), зі стандартним відхиленням 256,68 проти 250,12. Однак розподіл має іншу форму: медіана шахрайських операцій нижча (9,25 проти 22,0), що вказує на переважання невеликих сум, але максимум (2125,87) значно нижчий за легальні (25691,16), хоча іноді спостерігаються разові великі транзакції. Це відповідає практиці, коли зловмисники тестують картку на малі суми перед масштабними переказами.

Часові патерни також демонструють відмінності. Середня година проведення легальних транзакцій становить 14,05 при стандартному відхиленні 5,83, тоді як для шахрайських – 11,65 з більшою варіабельністю (6,66). Це вказує на те, що шахрайські дії менш прив'язані до звичних часових інтервалів і можуть мати піки активності у нетипові години, наприклад, о 2:00 чи 11:00. Циклічні змінні Time_sin (середнє 0,133 для шахрайств) і Time_cos (-0,027) підтверджують періодичні патерни, підкреслюючи більшу варіабельність у шахрайських операціях.

Таблиця 1 підсумовує ключові статистичні характеристики для обраних ознак, дозволяючи детально проаналізувати відмінності між класами

Таблиця 1.

Порівняння статистичних характеристик для класів 0 і 1

Ознака	Клас	Середнє	Стандартне відхилення	Мін.	25%	50%	75%	Макс.
V1	0	0,008	1,93	-56,41	-0,92	0,02	1,32	2,45
V1	1	-4,77	6,78	-30,55	-6,04	-2,34	-0,42	2,13
V2	0	-0,006	1,64	-72,72	-0,60	0,06	0,80	18,90
V2	1	3,62	4,29	-8,40	1,19	2,72	4,97	22,06
Amount	0	88,35	250,12	0,0	5,6	22,0	77,16	25691,16
Amount	1	122,21	256,68	0,0	1,0	9,25	105,89	2125,87
Година	0	14,05	5,83	0,0	10,0	15,0	19,0	23,0
Година	1	11,65	6,66	0,0	5,0	12,0	17,0	23,0

Детальний аналіз даних таблиці розкриває кілька ключових закономірностей. Для ознаки V1 у класі 0 розподіл симетричний навколо нуля (медіана 0,02, 25% і 75% кватилі від -0,92 до 1,32), з помірною дисперсією, тоді як у класі 1 він сильно зсунутий у негативну область (медіана -2,34, 25% кватиль -6,04), з вищою дисперсією, що вказує на аномальні значення, такі як мінімум -30,55. Це свідчить про те, що шахрайські транзакції часто

асоціюються з екстремальними відхиленнями в певних PCA-компонентах, можливо, пов'язаними з незвичайними параметрами операцій.

Для V2 картина протилежна: у класі 0 середнє близьке до нуля ($-0,006$), з медіаною $0,06$ і квартилями від $-0,60$ до $0,80$, що вказує на нормальний розподіл без значних асиметрій. У класі 1 середнє позитивне ($3,62$), медіана $2,72$, а 75% квартиль сягає $4,97$, з максимумом $22,06$, що перевищує легальні значення. Такий зсув у позитивну сторону може відображати специфічні патерни, як-от повторювані операції чи незвичайні локації, замасковані PCA.

Змінна Amount показує, що легальні транзакції мають ширший діапазон (максимум $25691,16$), з медіаною $22,0$ і 25% квартилем $5,6$, що типово для повсякденних покупок. У шахрайських медіана нижча ($9,25$), 25% квартиль $1,0$, але 75% квартиль вищий ($105,89$), а стандартне відхилення більше, що вказує на бімодальний розподіл: переважання малих тестових операцій з рідкісними великими сумами. Це підтверджує стратегію зловмисників – починати з малих транзакцій для перевірки.

Для ознаки Година легальні операції зосереджені в денний час (медіана $15,0$, 25%–75% від $10,0$ до $19,0$), з меншою варіабельністю. Шахрайські мають нижчу медіану ($12,0$), ширший квартильний діапазон ($5,0$ – $17,0$) і вищу дисперсію, що свідчить про активність у нічний або ранковий час, менш передбачувану.

Узагальнюючи, результати підтверджують, що шахрайські транзакції відрізняються від легальних за сукупністю характеристик: від зміщених розподілів ознак до специфічних часових закономірностей. Проведене дослідження доводить, що статистичний аналіз є потужним інструментом для розкриття прихованих закономірностей у фінансових даних. Шахрайські операції концентруються у відмінних областях простору ознак, з асиметричними розподілами та більшою дисперсією. Фінансова змінна Amount підтверджує патерн невеликих тестових операцій з потенційними великими переказами. Часові характеристики вказують на меншу передбачуваність атак, з піками в нетипові години. Інтеграція цих ознак до моделей може значно підвищити точність виявлення аномалій. Подальші дослідження можуть фокусуватися на комбінуванні статистичних методів з алгоритмами машинного навчання для створення адаптивних систем моніторингу в реальному часі.

Список використаних джерел:

1. <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud> (date of access: 27.09.2025).
2. Tyshchenko S., Parkhomenko O., Darmosyuk V. Modelling and Analysis of Cyberattack Risks on Financial Institutions Using Mathematical Statistics and Python Methods. *Modern Economics*. 2024. Vol. 48, no. 1. P. 130–136.
URL: [https://doi.org/10.31521/modecon.v48\(2024\)-16](https://doi.org/10.31521/modecon.v48(2024)-16).
3. Bawany Z., Shanbhag A. D. Using Machine Learning To Detect Credit Card Fraud. 2023 *International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Cape Town, South Africa, 16–17 November 2023. 2023.
URL: <https://doi.org/10.1109/icecet58911.2023.10389421>.

Топалова С.О.

*к.політ.н., доцент, доцент кафедри менеджменту, обліку
та бізнес-комунікацій*

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

Торяник Ж.І.

*к.е.н., доцент, доцент кафедри менеджменту, обліку
та бізнес-комунікацій*

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

Шевченко В.І.

*к.філол.н., доцент, доцент кафедри менеджменту, обліку
та бізнес-комунікацій*

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ: ЗАГРОЗИ ДЛЯ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ТА ОСВІТНІ ЗАСОБИ ПРОТИДІЇ

Застосування штучного інтелекту в інформаційному середовищі створює низку загроз, які умовно можна розділити на технологічні та соціально політичні. Технологічні новації дають можливість суттєво впливати на відбір контенту й сприйняття його змісту, створюючи тим самим соціально-політичні небезпеки в масштабах суспільства. Однією з перших актуалізується проблема збереження свободи слова і свободи інформації, протидії цензурі.

Дослідники акцентують увагу на тому, що технології ШІ вже не лише опосередковують, а й формують відносини між владою і суспільством [1]. Впроваджується алгоритмічна модерація, яка порушує баланс між свободою слова і безпекою у цифровому інформаційному просторі. Автоматичні фільтри, які ухвалюють рішення про просування чи видалення контенту, сприяють тому, що великі інформаційні платформи фактично самостійно можуть регулювати доступ до інформації, обмін інформацією, формувати ставлення до інформації. Таким чином впроваджується «приватна алгоритмічна цензура». Великі платформи та їхні алгоритми вже відіграють роль регуляторів комунікації, збираючи й обробляючи великі масиви персональних даних. З одного боку, вони зобов'язані не шкодити інтересам користувачів, не формувати інформаційну асиметрію, не маніпулювати інформацією, тобто, забезпечувати свободу інформації. Проте, з іншого боку, ці ж платформи впроваджують алгоритмічні перешкоди – алгоритми, що відбирають, просувають чи блокують контент, завдяки чому виступають «новими воротами свободи слова» і вже зараз впливають на публічну сферу більше, ніж традиційні медіа.

Соціальні платформи широко застосовують автоматизовані підходи для відсіву небажаної інформації, тож і для придушення комунікацій, що стосуються цієї небажаної інформації. По суті це інтервенціоністський підхід до модерації соціальних комунікацій, що забезпечує великим соціальним

платформам безпрецедентний рівень контролю і над публічними, і над приватними комунікаціями. Враховуючи факт домінування в інформаційному просторі кількох соціальних платформ, виникає небезпека інформаційної змови, впровадження їхніх комерційних і політичних пріоритетів у повсякденне спілкування користувачів мереж [2].

Поява «персональних цифрових агентів», які шукають і відбирають контент, окрім зручностей, створює й загрозу підсилення залежності від алгоритмів, які здійснюють інформаційний вибір. Оскільки такі алгоритми розробляються кампаніями, то й діяти вони можуть в інтересах розробника, обмежуючи інформаційний вибір користувачів. Крім того, ШІ-боти вже масово просувають певні інформаційні продукти, ставлять «лайки», чим забезпечують ілюзію підтримки суспільством потрібних певним суб'єктам наративів. Таким чином через упередженість чи помилки алгоритмів відбувається викривлення інформаційного простору, підсилюються дискримінаційні практики у відборі контенту – політичного, комерційного – залежно від статусів та інтересів тих, хто володіє інформаційними платформами чи має ресурси для впливу на них. Так утверджується інформаційна асиметрія. Великі технологічні корпорації отримують можливість контролювати інформаційні потоки, блокувати доступ до «незручних» для них даних. Оскільки нерівність доступу до ШІ зростає, посилюються й тенденції до встановлення інформаційної монополії навіть за формальної наявності великої кількості суб'єктів інформаційного впливу. Так за збереження фасадних ознак свободи інформації вибудовується щільна цензура.

Технології ШІ дають можливості для створення масових кампаній з дезінформації шляхом імітації політичних лідерів, експертів, громадських активістів [3]. Це стає вагомим засобом впливу на громадську думку, на хід політичних кампаній, передусім виборчих. Водночас розгортається «масове виробництво інформаційних мильних бульбашок» через персоналізовані рекомендації контенту. Вже зараз ми бачимо багато таких на YouTube та інших платформах. Це підриває довіру до інституцій – владних, громадських, до засобів інформації, формує тотальну недовіру до всіх. Поряд з цим ШІ вже широко використовується для розпізнавання облич, що може застосовуватись для контролю над громадянами, в тому числі для утисків свободи мирних протестів. Тож інформаційний контроль, що доповнюється можливостями алгоритмічного контролю участі громадян у політичних акціях фактично нівелює низку базових принципів демократії.

Автор наступного дослідження [4] піднімає ще один пласт проблем – великих мовних моделей у сфері модерації контенту. Він вводить поняття «gatekeeping» – алгоритмічного «воротарства», де моделі фактично стають «вхідними фільтрами» (input filters) для інформаційних потоків. Ці «вхідні фільтри» можуть блокувати запити користувачів ще на етапі їх введення, відсіювати великий обсяг контраверсійних матеріалів, як некоректних (а по факту незручних для певних суб'єктів), або ж застосовувати алгоритмічне переписування відповідей, тим самим змінюючи їх стиль і зміст, що по суті є викривленням. На нашу думку, це величезний виклик не лише для адекватного сприйняття дійсності на основі інформації про реальні факти. Це загроза для

освітнього процесу й навчання, оскільки формується, в тому числі, упереджена база навчального контенту. Упередженість, окрім іншого, знижує довіру до контенту, демотивує до навчання.

Заслужовують на увагу і відзначені в аналітичному звіті за результатами дослідження ризику автоматичної цензури. Найбільш загрозливими з них вважаємо: глобальну уніфікацію норм, розроблюваних і впроваджуваних великими корпораціями з недотриманням чи відвертим ігноруванням правових норм і демократичних принципів; непрозорість критеріїв відбору й блокування контенту, що доповнює попередню загрозу; «м'яку цензуру», яка на відміну від «жорсткої» прямо не блокує, але через замовчування, викривлення чи «розмивання» змісту досягає того ж ефекту, і, на нашу думку, є навіть більш небезпечною, ніж й пряма жорстка цензура, адже «м'яка» менш помітна та залишається видимість свободи інформації; придушення меншості, що досягається через просування автоматичними алгоритмами «основних наративів», «точки зору більшості» і, відповідно, відсіювання та пригнічення менш популярних чи зручних. Як наслідок, завдяки алгоритмічним правилам встановлюється контроль і над отриманням, і над поширенням інформації. Прихована автоматична цензура діє малопомітно для користувача й ефективно для її суб'єкта.

ШІ та автоматичні алгоритми змінюють споживання та аналіз інформації. Тут виникають важливі запитання: Наскільки споживачі інформації обізнані про застосування новітніх технологій, зокрема ШІ, в інформаційній сфері? Наскільки усвідомлюють, як використання цих технологій впливає на інформаційний простір? Як ШІ змінює контент і наше сприйняття? Який вплив здійснюють технології ШІ на критичне мислення та медіаграмотність і як їх зараз розвивати? Перші спроби такого дослідження здійснили М. Мілошавлевич та І. Вобіч [5]. Оскільки алгоритми ШІ відбирають, ранжують і навіть створюють контент, у багатьох користувачів необхідність самотійно шукати, перевіряти й навіть аналізувати інформацію стрімко зменшується. Таким чином у суспільстві формується інформаційна нерівність. Група тих, хто усвідомлює вплив вищезгаданих алгоритмів і при цьому може критично сприймати й аналізувати інформацію стає значно меншою, ніж та, що сприймає результати ШІ без перевірки й осмислення й навіть покладається на рішення, запропоновані ШІ. Адже він все «знає» і «пояснює», тому й «краще» сприймати відповіді без сумнівів. Так на рівні суспільства формується загроза «інтелектуальної пасивності», яка швидко послаблює і зводить нанівець здатність до аналізу інформації. Оскільки алгоритми ШІ ще й підсилюють та «розкручують» «інформаційні мильні бульбашки» і можуть блокувати альтернативну інформацію, це привчає користувача до однобічного мислення і усуває саму потребу мислити критично. Адже немає альтернативної інформації для порівняння. Делегуючи когнітивні функції машинам і алгоритмам, ми добровільно відмовляємось від власної здатності до критичного мислення і розвитку навичок медіаграмотності.

Освітні засоби протидії цим загрозам перебувають у двох площинах: розвиток критичного мислення й медіаграмотності, а також навчання спеціальній алгоритмічній грамотності. Друге без першого не працює. Формування здатності до критичного мислення та медіаграмотності не можливе лише в рамках окремих курсів на кшталт «Критичне мислення» чи «Медіаграмотність». Такі курси можуть бути ефективними лише за умови сформованого підґрунтя.

Критичне мислення формується поступово, в ході вивчення гуманітарних дисциплін, спочатку шкільних, потім університетських. Процес вивчення має передбачати роботу з першоджерелами, змістовний аналіз текстів та інформаційних повідомлень, аргументацію висновків, тощо. Якщо ж це вивчення зводиться до копіювання і переміщення у слайди презентацій уривків матеріалів, їх озвучення без розуміння змісту, звісно, про критичне мислення чи медіаграмотність у такому випадку не йдеться. Завдяки Інтернету та ІІІ реально створилася ситуація, за якої для забезпечення цензури і ліквідації здатності до критичного мислення не потрібно прямо забороняти книги, спалювати їх, як це практикували режими за Гітлера, Сталіна, Мао Цзедуну, відтворювати сюжет фільму «451 градус за Фаренгейтом». Аналогічний результат забезпечують дегуманітаризація освіти, симуляція в освітньому процесі і застосування автоматичних алгоритмів. Якщо у здобувачів освіти буде відсутня сама потреба читати, осмислювати, аналізувати, порівнювати, навіть максимально можлива кількість джерел інформації у найдоступніших форматах не буде стимулювати до критичного мислення. Отже, оскільки застосування ІІІ створює загрози для низки демократичних принципів і громадянських прав та свобод, формування критичного мислення та медіаграмотності має стати вагомим складовою системної громадянської освіти [6,7]. Станом на сьогодні громадянська освіта відсутня в системі вищої освіти [8].

Спеціальну алгоритмічну грамотність потрібно розвивати шляхом впровадження в шкільні та університетські освітні програми окремих курсів про автоматичні алгоритми та включення в курси з медіаграмотності тем про упередженість цих алгоритмів із використанням прикладів із реальних мереж для ілюстрації їх впливу на пошук інформації. Важливе значення мають інструменти практичного навчання, які дозволяють бачити, як змінюється результат пошуку при зміні запиту для пошуку та алгоритмічних параметрів. Це також вчить правильно задавати параметри пошуку. Окрім того, доцільно ставити завдання формування нового різновиду критичного мислення – критичного мислення щодо ІІІ. Тут йдеться не лише про здатність критично читати тексти і критично осмислювати інформацію, а й про розвиток вміння читати і розуміти самі ці алгоритми. Це формуватиме здатність розуміти чому користувач бачить саме такий результат пошуку та як змінити запит, щоб отримати інший результат. Розуміючи механізми упередженості, легше, хоча б певною мірою, мінімізувати цю упередженість, змінивши запит на пошук інформації. Крім того, користувач буде усвідомлювати, що не можна

беззастережно покладатись на ШІ, потрібно застосовувати власний для перевірки результатів і вибору рішень.

Список використаних джерел:

1. Free Speech in the Algorithmic Society: Big Data, Private Platforms and the New School of Speech Regulation – Yale Univ. Law. URL: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/4699/51_U.C.D._law_Review_1149_2018.pdf.
2. Algorithmic Censorship by Social Platforms: Power and Resistance. URL: <https://link.springer.com/article/10.1007/s13347-020-00429-0>
3. Automated Content Moderation. URL: https://georgetownlawtechreview.org/wp-content/uploads/2022/11/Sheng_Automated-Content-Moderation.pdf.
4. Algorithmic Gatekeepers: LLMs, content moderation and expression. URL: https://ecn1.org/sites/default/files/2025-04/ECNL_LLM_CM_expression_information_opinion_2025.pdf.
5. Artificial intelligence and the dawn of an algorithmic divide. URL: <https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2024.1453251/pdf>.
6. Топалова С.О. Медіаграмотність для громадянської компетентності: позитивний досвід Ізраїлю. «Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія» в № 58 (2023 р.), с. 188-200. DOI: <https://doi.org/10.21564/2663-5704.58.285775>
7. Топалова С.О., Топалова В.С. Основи концепції медіаосвіти в умовах сучасного глобального інформаційного суспільства. PROBLEMS OF INTEGRATION OF EDUCATION, SCIENCE AND BUSINESS IN GLOBALIZATION. Abstracts of V International Scientific and Practical Conference Sofia, Bulgaria (February 05-07, 2024), с. 143-146. URL: <https://eu-conf.com/events/problems-of-integration-of-education-science-andbusiness-in-globalization/>
8. Топалова С.О., Швидка О.Б. Соціальна відповідальність закладів вищої економічної освіти в контексті реалізації місії університету. (2020). *Фінансово-кредитна діяльність: проблеми теорії та практики*, 2(33), 585-592. DOI: <https://doi.org/10.18371/v2i33.3021>

Тюренкова К.В.

здобувач вищої освіти,

Миколаївський національний аграрний університет

Науковий керівник

Кучмійова Т. С.

к.е.н., доцент, доцент кафедри економічної кібернетики, комп'ютерних

наук та інформаційних технологій

Миколаївський національний аграрний університет

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ В УКРАЇНІ

Інформаційна безпека є ключовим аспектом функціонування сучасних організацій і суспільства загалом. У сучасному цифровому середовищі дані постійно піддаються різним загрозам – від несанкціонованого доступу до втрати чи спотворення інформації. Вивчення видів загроз та їх класифікації дозволяє розробляти ефективні механізми захисту інформаційних ресурсів, зменшувати ризики кіберзлочинності та забезпечувати стабільне функціонування інформаційних систем.

Кібербезпека являє собою комплекс технологій, процедур та практик, спрямованих на захист інформаційних систем, мереж, пристроїв, програмного забезпечення та даних від кібератак, пошкоджень або несанкціонованого доступу. Вона виступає ключовим компонентом інформаційної безпеки та передбачає запобігання загрозам, своєчасне їх виявлення та ефективне реагування. Крім технічних заходів, кібербезпека включає організаційні та освітні аспекти, що забезпечують безпечне використання цифрових ресурсів у сучасному інформаційному середовищі [2].

Зарубіжні країни активно впроваджують низку сучасних методів захисту персональних даних, які Україні варто врахувати для вдосконалення власної системи безпеки в умовах цифровізації. До таких методів належать:

- Шифрування даних – один із найефективніших технічних способів захисту, який широко застосовується в ЄС, США та Японії. Завдяки шифруванню навіть у випадку витоку інформації дані залишаються недоступними для злоумисників [1].

- Багатофакторна автентифікація (MFA) – використовується у США та Європі для захисту доступу до конфіденційної інформації. Вона передбачає підтвердження особи за допомогою декількох методів (пароль, SMS-код, біометричні дані), що суттєво ускладнює несанкціонований доступ.

- Регулярні кібербезпекові аудити та сертифікації, які активно застосовуються в країнах ЄС для оцінки надійності інформаційних систем. Вони дозволяють своєчасно виявляти вразливі місця та усувати їх.

- Машинне навчання та штучний інтелект для моніторингу безпеки, які вже використовують великі компанії, такі як Google та Microsoft, для виявлення потенційних загроз і аномальної активності, що може свідчити про

кібератаки або інші інциденти.

Україна сьогодні не здатна повністю впровадити ефективні механізми захисту персональних даних через низку причин. Однією з ключових є недосконалість національної законодавчої бази. Хоча в країні діє Закон «Про захист персональних даних», його положення не повністю узгоджуються з міжнародними стандартами, зокрема з GDPR, що призводить до правової невизначеності та відсутності чітких норм для застосування сучасних технологій захисту.

Впровадження таких заходів потребує значних фінансових ресурсів, тоді як бюджетні обмеження та низький рівень інвестицій у кібербезпеку уповільнюють процес модернізації. Багато державних установ та підприємств не мають змоги забезпечити впровадження дорогих технологій захисту, таких як багатофакторна автентифікація чи використання штучного інтелекту для моніторингу кіберзагроз.

Фасій Б. [3] зазначає, що суттєвим бар'єром є кадровий дефіцит і низький рівень кіберграмотності. В Україні спостерігається нестача кваліфікованих фахівців у сфері кібербезпеки, що ускладнює як впровадження, так і підтримку сучасних технологій захисту інформації. Низький рівень знань і практичних навичок серед державних службовців та працівників бізнесу також призводить до недотримання базових принципів безпеки даних. Крім того, складна політична та економічна ситуація, зокрема військовий конфлікт, додатково загострює проблему: у таких умовах ресурси переважно спрямовуються на загальну безпеку, тоді як питання кіберзахисту часто відходять на другий план.

Таким чином, ефективна інформаційна та кібербезпека є ключовою для захисту даних і стабільного функціонування цифрових систем. Україна може підвищити рівень захисту персональної інформації, впроваджуючи міжнародні практики та сучасні технології, проте для цього необхідно вдосконалити законодавство, розвивати фахові компетенції та підвищувати кіберграмотність користувачів.

Список використаних джерел:

1. Гончарова І.П. Кібербезпека в цифровому освітньому середовищі закладів професійної освіти: електронний навчальний курс. 2022. URL: <https://lib.iitta.gov.ua/id/eprint/733620/1/%D0%9A%D0%86%D0%91%D0%95%D0%A0%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%9A%D0%90.pdf> (дата звернення: 19.09.2025).
2. Анікеєнко А.Р., Кучмійова Т.С. Кібербезпека як один із ключових аспектів сучасного життя / А.Р. Анікеєнко, Т.С. Кучмійова // Збірник наукових праць конференції. 2024. С. 45–53. URL: <https://biotechuniv.edu.ua/wp-content/uploads/2024/05/conf-22-04-24-zbirnyk.pdf>
3. Фасій Б. Національна безпека та захист персональних даних в епоху цифрових технологій. Управління національною безпекою. 2024. С. 76-82. URL: <https://sas.ztu.edu.ua/article/view/320856/311397>

Ульянченко О.В.

здобувач вищої освіти,

Харківський національний університет міського господарства

імені О.М. Бекетова

Науковий керівник

Сізова Н.Д.

докт.фіз.-мат.наук., професор, професор кафедри комп'ютерних наук та

інформаційних технологій

Харківський національний університет міського господарства

імені О.М. Бекетова

РОЛЬ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ (ШІ) У СФЕРІ КІБЕРБЕЗПЕКИ

У добу активної цифрової трансформації суспільства проблема забезпечення надійної комп'ютерної безпеки стає одним із ключових стратегічних завдань. Збільшення обсягів даних, широке використання хмарних сервісів, розвиток Інтернету речей та зростання популярності дистанційних послуг створюють нові можливості, але водночас породжують і додаткові ризики для інформаційної інфраструктури. Кіберзлочинність набуває більшої організованості, а методи атак стають складнішими та витонченішими, що знижує ефективність традиційних підходів до захисту [1].

Паралельно швидкий прогрес у сфері штучного інтелекту (ШІ) відкриває нові шляхи підвищення рівня кібербезпеки. Використання алгоритмів машинного навчання, нейронних мереж і технологій аналізу великих даних дозволяє виявляти приховані залежності у великих інформаційних потоках, прогнозувати можливі загрози та своєчасно реагувати на підозрілі події. Інтеграція ШІ в системи безпеки забезпечує автоматизацію моніторингу, підвищує точність і швидкість виявлення атак та зменшує час реагування на інциденти.

Актуальність дослідження зумовлена необхідністю розробки інтелектуальних рішень у сфері кіберзахисту, здатних ефективно протистояти сучасним і майбутнім викликам інформаційної безпеки. Застосування ШІ у цій галузі є не лише перспективним напрямом наукових розвідок, а й практично значущим інструментом для захисту даних у державному, корпоративному та приватному секторах.

Традиційні методи захисту, такі як системи контролю доступу, брандмауери, антивірусні рішення чи системи виявлення вторгнень, більше не здатні ефективно протидіяти динамічним і складним загрозам. Це зумовлює необхідність інтеграції штучного інтелекту (ШІ) у системи комп'ютерної безпеки.

Інтеграція штучного інтелекту (машинного навчання, глибинного навчання, експертних системи, нечітка логіка тощо) призначена для автоматизації виявлення загроз, класифікації інцидентів, прогнозування ризиків,

реагування та адаптації захисних механізмів. Завдяки інтеграції підвищується швидкості виявлення аномалій і атак у великих потоках даних, відбувається автоматичне оновлення моделей під нові типи атак (zero-day, polymorphic malware), знижується навантаження на аналітиків за рахунок пріоритизації інцидентів і автоматичного реагування на загрози, прогнозуються ризики і проактивний захист (аналітика загроз, сценарії), підвищується точність завдяки комбінації правил і поведінкових моделей [2].

Інтеграція ШІ стає ключовим фактором побудови проактивної кіберзахисної інфраструктури.

Проактивність у сфері кіберзахисту визначається як здатність інфраструктури інформаційної безпеки не лише реагувати на вже виявлені інциденти чи атаки, але й передбачати, попереджати та мінімізувати ризики ще до їх реалізації. Це принципово відрізняє проактивний підхід від традиційних реактивних систем захисту, що спрацьовують лише після виявлення загрози. Проактивна кіберзахисна інфраструктура є сучасним етапом розвитку систем інформаційної безпеки, що базується на передбачуванні та запобіганні загрозам, а не на реагуванні після факту. Вона інтегрує аналітику великих даних, штучний інтелект, автоматизацію та адаптивні механізми, що дозволяє створювати стійку та гнучку модель кіберзахисту для критично важливих систем і підприємств [3].

Проактивність у сфері кіберзахисту характеризується такими діями як:

моніторинг у реальному часі, тобто постійний збір і аналіз даних із мережесегментів, серверів, кінцевих пристроїв та користувацької активності;

аналіз на основі прогнозних моделей, що передбачає використання методів машинного навчання, нейронних мереж та поведінкового аналізу для виявлення аномалій і передбачення потенційних атак.

загрозова розвідка (Threat Intelligence), що являє собою інтеграцію з базами даних про відомі вразливості, експлойти та шкідливе ПЗ, що дозволяє заздалегідь ідентифікувати ризики;

автоматизація реагування з використанням систем SOAR (Security Orchestration, Automation and Response) для оперативного блокування атак, ізоляції вузлів та відновлення систем;

сценарне планування та моделювання атак, тобто імітація кіберзагроз (наприклад, через Red Team / Blue Team тренування) для підготовки персоналу та тестування стійкості інфраструктури.

Переваги проактивної кіберзахисної інфраструктури у наступному:

зменшення часу виявлення та реагування на атаки (MTTD/MTTR);

мінімізація фінансових та репутаційних втрат;

підвищення рівня довіри користувачів і партнерів;

забезпечення відповідності нормативним вимогам (ISO/IEC 27001, NIST, GDPR тощо).

Безперервний моніторинг і прогнозування, тобто використання систем SIEM/SOAR, аналітики великих даних, штучного інтелекту та машинного навчання для виявлення аномалій.

Інтелектуальне виявлення загроз (Threat Intelligence)

Інтеграція зовнішніх джерел загроз (Threat Feeds), аналіз поведінки зловмисників, формування профілів атак.

Адаптивність і самонавчання

Застосування нейронних мереж і поведінкової аналітики для адаптації системи до нових патернів атак.

Сегментація та багаторівневий захист

Використання Zero Trust, розподілених міжмережевих екранів, мікросегментації мережі.

Інтеграція людського фактора та автоматизації

Автоматичне реагування на відомі інциденти та залучення аналітиків до критичних випадків.

Моделювання сценаріїв атак (Red/Blue Team, Purple Team)

Проведення регулярних тестів на проникнення, кіберполігонів та симуляцій атак.

Проактивна кіберзахисна інфраструктура поєднує автоматизовані системи (SIEM, SOAR, AI/ML) та експертні дії аналітиків, що дозволяє виявляти й запобігати загрозам ще до їхнього реалізації. Такий підхід підвищує стійкість організації до кіберінцидентів, знижує ризики та забезпечує безперервність бізнес-процесів.

Список використаних джерел:

1 Bhatele, K. R., Shrivastava, H., & Kumari, N.. The role of artificial intelligence in cyber security. In Countering cyber attacks and preserving the integrity and availability of critical systems. –2019.– 170-192 p.

https://www.researchgate.net/publication/330569376_The_Role_of_Artificial_Intelligence_in_Cyber_Security

2. Онищенко Ю. М., Каланча, А. А., Гельдт, С. В. Застосування штучного інтелекту у сфері кібербезпеки. In The 8th International scientific and practical conference “Trends, theories and ways of improving science”(February 28–March 03, 2023) Madrid, Spain. International Science Group. 2023 – 544 – 548 p.

<https://elar.tsatu.edu.ua/server/api/core/bitstreams/a636fbeb-2ad2-459e-b381-b4d0813d4d8e/content>

3 Пантюшенко Р., Чайка Ю, Штучний інтелект у сфері кібербезпеки: інновації, виклики та перспективи розвитку//Military Science. – 2024. – Vol. 2, No.1, 200-209 p.

<https://pdfs.semanticscholar.org/c958/0ab242782ccb683fccd615856da9ccc8e3fe.pdf>

Філатов О.П.

здобувач вищої освіти,

Бахмутський навчально-науковий професійно-педагогічний інститут

ХНУ ім. В.Н. Каразіна

Науковий керівник

Нефьодова І.В.

к. ф.-м. н., доцент, доцент кафедри

електромеханічних та комп'ютерних систем,

Бахмутський навчально-науковий професійно-педагогічний інститут

ХНУ ім. В.Н. Каразіна

ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРЗАХИСТ: ГЛОБАЛЬНІ ВИКЛИКИ І УКРАЇНСЬКИЙ ДОСВІД

У ХХІ столітті інформація стає одним із ключових ресурсів держави поряд із фінансовими, енергетичними та військовими. З розвитком цифрових технологій війни більше не обмежуються лише фізичним протистоянням на полі бою – дедалі більшу роль відіграє інформаційна та кібернетична сфера. Приклад війни Росії проти України демонструє, що сучасні конфлікти носять гібридний характер, де інформаційна війна та кібероперації займають центральне місце.

Російська Федерація активно застосовує методи інформаційно-психологічних операцій, спрямованих на:

- деморалізацію населення України;
- дискредитацію військово-політичного керівництва;
- розпалювання міжетнічної та міжрелігійної ворожнечі;
- створення паніки та хаосу в суспільстві.

Ключовими інструментами стають: поширення фейків через соціальні мережі, використання бот-мереж, маніпуляція відео- та фото-матеріалами, а також міжнародні інформаційні кампанії, покликані представити Україну «нестабільною державою».

Такі дії не лише впливають на суспільну свідомість, але й створюють пряму загрозу національній безпеці, адже підривають довіру до інституцій влади та міжнародних партнерів.

Паралельно з інформаційними атаками Росія здійснює масові кібератаки на критичну інфраструктуру України. Найбільш відомі приклади:

- атака на енергетичні компанії України у 2015–2016 рр., що призвела до масштабних відключень електроенергії;
- кібератака NotPetya у 2017 р., яка завдала Україні та світовій економіці збитків на мільярди доларів;
- численні атаки на державні сайти та банківську систему під час повномасштабного вторгнення у 2022 р.;

- масштабна атака на телекомунікаційного оператора (Kyivstar) у грудні 2023 року, яка порушила мобільний та інтернет зв'язок по всій Україні; також відключення деяких критичних систем попередження.

Кібератаки завдають економічних збитків, дестабілізують фінансову систему, блокують логістику та можуть паралізувати державне управління.

Завчасно повинен бути сформований орієнтир протидій. Для мінімізації ризиків та посилення стійкості України у сфері інформаційної та кібербезпеки доцільно реалізувати наступний комплекс заходів.

1. Посилення державної кіберзахисної інфраструктури – розвиток центрів моніторингу, швидке реагування на кібератаки та впровадження національної системи кіберзахисту критичних об'єктів.

2. Співпраця з приватним сектором та ІТ-спільнотою – залучення висококваліфікованих спеціалістів у рамках кіберрезерву та створення умов для ефективної взаємодії як державних, так і приватних структур.

3. Розвиток інформаційної грамотності населення – впровадження курсів медіаграмотності в освітніх закладах та проведення систематичних державних кампаній з інформування населення про ризики фейкових повідомлень.

4. Міжнародне партнерство – активна участь у програмах НАТО та ЄС з кіберзахисту та обмін розвідданими, а також технологіями з міжнародними партнерами.

Отже, досвід України доводить, що інформаційна війна та кіберзагрози є невід'ємною частиною сучасних воєнних конфліктів. Згідно даним академії електронного управління «National Cyber Security Index» динаміка цифрового розвитку України, та кібербезпеки, робить впевнені кроки вперед [4]. Для більш ефективної протидії потрібна синергія державних ресурсів, приватного сектору та громадянського суспільства, а також міжнародна підтримка. Розбудова національної системи кіберзахисту та підвищення рівня інформаційної культури суспільства стають фундаментом стійкості України у сучасному світі.

Список використаних джерел:

1. Гайдук О.В., Зверев В.П. Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій. *Кібербезпека: освіта, наука, техніка*. Том 3 № 23 (2024), с. 225-236. doi: <https://doi.org/10.28925/2663-4023.2024.23.225236>

2. Сироватченко М. (2024) Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка»*. Серія: "Юридичні науки". Том 11, № 1(41), С. 314-320. doi: <https://doi.org/10.23939/law2024.41.314>

3. Талліннський механізм: Україна та міжнародні партнери започаткували новий інструмент співпраці у кіберпросторі (20.12.2023). *Урядовий портал*. URL: <https://www.kmu.gov.ua/news/tallinnskyi-mekhanizm-ukraina-ta-mizhnarodni-partnery-zapochatkuvaly-novyiy-instrument-spivpratsi-u-kiberprostorii>.

4. Ukraine.National Cyber Security Index. URL: <https://ncsi.ega.ee/country/ua/>

Філатова Л. Д.

к. ф.-м. н., доцент,

*доцент кафедри інформаційних технологій та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В. Н. Каразіна*

Фаткулін В. В.

*здобувач другого (магістерського) рівня вищої освіти
ННІ «Каразінський банківський інститут» ХНУ імені В. Н. Каразіна;*

СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА ЛЮДСЬКИЙ ФАКТОР

Соціальна інженерія – це сукупність методів, спрямованих на те, щоб переконати ціль розкрити певну інформацію або виконати певну дію. Ці методи не є чимось новим: вони були основою найрізноманітніших шахрайських схем з часів появи людства. Однак в епоху цифрових комунікацій злочинці отримали нові надзвичайно ефективні можливості [1, 2].

Соціальна інженерія використовує такі людські риси, як готовність допомагати іншим, довіра, страх або повага до влади – це все експлуатується для маніпулювання людьми. Кіберзлочинці переконують своїх жертв поділитися конфіденційною інформацією, обійти функції безпеки, надіслати гроші або встановити шкідливе програмне забезпечення на свої особисті пристрої або на комп'ютер, підключений до мережі компанії тощо. При цьому зловмисник, щоб завоювати довіру, часто видає себе за надійну особу або джерело. Тобто, у соціальній інженерії для досягнення цілей фактично використовується людський фактор, який є найслабшою ланкою в будь-якому ланцюжку безпеки.

На сьогодні зловмисники для досягнення своїх цілей використовують цілий спектр методів. Найпопулярнішими все ще залишаються фішингові техніки. Проаналізуємо основні з них.

— Фішинг – спонукає одержувачів перейти за посиланням і розкрити конфіденційну інформацію, таку як паролі, номери кредитних карток або особисті дані. Зловмисники використовують оманливі електронні листи, повідомлення або посилання на фейкові веб-сайти, які виглядають як оригінальні [3].

— Персоналізований фішинг – це цілеспрямований фішинг. Щоб виглядати ще більш переконливими, зловмисники намагаються ідентифікувати отримувача та налаштовують повідомлення на основі конкретної інформації про організацію або конкретну ціль. Часто зловмисники використовують відкриті джерела інформації (OSINT) для вивчення своєї цілі.

— Смішинг – це фішингова атака, яка використовує мобільні текстові повідомлення (SMS), де зловмисник видає себе за авторитетну компанію або надійного суб'єкта.

— Вішинг – це форма фішингу, яка відбувається за допомогою голосового зв'язку, зазвичай телефонних дзвінків. Зловмисники видають себе за надійні організації або знайомих та переконують жертву розкрити конфіденційну інформацію. З розвитком штучного інтелекту стало набагато

простіше створювати аудіозаписи на основі базових записів.

— Діпфейк фішинг – новий вид фішингових атак через засоби відео та аудіо комунікацій набув популярності під час коронавірусного локдауну.

Останнім часом окрім популярних фішингових технік зловмисники для переконання своїх жертв використовують ще цілий ряд підходів. Основні з них:

— Претекстинг – це підхід, коли зловмисник створює вигаданий сценарій або привід для отримання інформації. Він видає себе за іншу особу онлайн або особисто, щоб завоювати довіру і маніпулювати жертвою, змушуючи її розкрити конфіденційну інформацію або вчинити певні дії.

— Business Email Compromise (BEC) – різновид кіберзлочинів який використовує ланцюжки електронних листів, щоб переконати жертву виконати певну дію. Атаки BEC особливо небезпечні, оскільки вони часто використовують реальні дані про компанію та її співробітників, щоб створити переконливі повідомлення, які важко відрізнити від справжніх.

Проаналізуємо основні причини того, чому саме ви можете стати жертвою зловмисників, які використовують методи соціальної інженерії.

Під час фішингової атаки зазвичай проходить лише 60 секунд від моменту відкриття електронного листа до натискання на шахрайське посилання, але у 80% випадків співробітники не повідомляють про спроби фішингу. Крім того, поява технології deepfake значно розширила можливості маніпуляцій, додавши новий рівень ризику.

Також наступні дії часто призводять до «успіху» кіберзлочинців:

- недотримання політик безпеки компанії;
- використання ІТ-обладнання, наданого компанією, в особистих цілях;
- використання особистого ІТ-обладнання в корпоративних цілях;
- використання слабких або повторюваних паролів для декількох облікових записів;
- публічне поширення конфіденційної інформації в соціальних мережах.

Останнім часом як у міжнародному так і у вітчизняному інформаційному просторі фіксується значне зростання кількості інцидентів, пов'язаних із соціальним інжинірингом. Кампанії соціального інжинірингу в різних формах залишаються суттєвою загрозою для користувачів. Для зменшення ризиків необхідно дотримуватись наступних рекомендацій [4]:

— Користуйтеся соціальними мережами відповідально. Ретельно обмірковуйте, яку особисту інформацію ви хочете оприлюднити, враховуючи, що злочинці можуть її зібрати та використати з метою обману.

— Не оприлюднюйте конфіденційну інформацію про свого роботодавця або роботу в приватних чи професійних соціальних мережах.

— Ніколи не повідомляйте паролі, дані для доступу або інформацію про рахунки по телефону чи в електронних листах. Пам'ятайте, що банки та інші надійні компанії ніколи не просять клієнтів надсилати конфіденційну інформацію електронною поштою або телефоном.

— Будьте особливо обережні, коли отримуєте електронні листи від

невідомих осіб: якщо є хоч найменший сумнів або підозра, що електронний лист може бути частиною атаки, краще взагалі не відповідати. Якщо це помилкова тривога, відправник, швидше за все, спробує зв'язатися з вами іншим способом. Приділіть час для трисекундної перевірки безпеки.

— Якщо в електронному листі вимагається негайна відповідь, знайдіть час, щоб зателефонувати відправнику і переконатися, що лист є справжнім.

Таким чином, зважаючи на те, що неуважність користувачів є основною причиною входу для хакерів, кожен користувач повинен стати ключовим гравцем у власному захисті, значно ускладнюючи зловмисникам досягнення успіху.

Список використаних джерел

1. Атаки соціальної інженерії: посилення людського фактору в безпеці. [Електронний ресурс]. Режим доступу: <https://pedbezpeka.vntu.edu.ua/index.php/pb/article/view/151/132>
2. Що таке соціальна інженерія в кібербезпеці? Реальні приклади та методи запобігання. [Електронний ресурс]. Режим доступу: <https://hideez.com/uk-ua/blogs/news/social-engineering#>:
3. Основні типи фішингових атак. Як бізнесу захиститися від дій зловмисників? [Електронний ресурс]. Режим доступу: <https://ua.issp.com/post/phishing>
4. Кібергігієна: як захистити бізнес від внутрішніх загроз. [Електронний ресурс]. Режим доступу: <https://itez.com.ua/blog/cyber-hygiene-for-employees.html>

УДК 004.056.53

Чередниченко Б.І.
здобувач вищої освіти,
Державний торговельно-економічний університет / Київський національний
торговельно-економічний університет
Науковий керівник
Жирова Т.О.
к.т.н., доцент, доцент кафедри інженерії програмного забезпечення та
кібербезпеки Державного Торговельно-Економічного Університету

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ДАНИХ: ВІД ПАРОЛІВ ДО БЕЗПАРОЛЬНИХ ТЕХНОЛОГІЙ

Загрози інформаційному середовищу, кібербезпека та захист інформації: роль політики паролів

Сучасне інформаційне середовище формується під впливом цифровізації всіх сфер суспільства. Разом із можливостями воно створює й нові виклики – постійне зростання кіберзагроз. Одним із ключових елементів захисту

інформації залишається парольна політика, адже навіть найскладніші технічні системи можуть бути вразливими через людський фактор.

Основні загрози:

- Злом паролів брутфорсом – автоматизований перебір комбінацій, що особливо ефективний проти коротких або простих паролів.
- Фішинг – психологічні атаки через підроблені сайти та листи, що експлуатують довіру користувача.
- Соціальна інженерія – маніпуляції та обман, коли вразливим елементом стає не система, а людина.
- Використання вкрадених баз даних – поширена практика на чорному ринку, де зловмисники комбінують «злиті» паролі з іншими даними.

Шляхи підвищення безпеки:

- Впровадження складних паролів і багатофакторної автентифікації як обов’язкового стандарту.
- Регулярне оновлення та ротація паролів.
- Освітні програми для користувачів, які формують культуру кібергігієни.
- Інтеграція політики паролів у комплексну систему інформаційної безпеки, де паролі – лише один із рівнів захисту.

Перспективи розвитку:

У майбутньому ключовим напрямом стане поступова відмова від класичних паролів. Серед альтернатив:

- Біометричні технології (відбитки пальців, розпізнавання обличчя, сканування сітківки).
- Passwordless-автентифікація (одноразові токени, апаратні ключі безпеки, автентифікація через мобільні застосунки).
- Штучний інтелект у кіберзахисті, який дозволить прогнозувати та блокувати атаки ще до їхнього розвитку.

Висновки

У світі, де зростає кількість кіберзагроз і витонченість атак, парольна політика перестає бути лише технічним інструментом. Вона стає елементом стратегічного захисту інформаційного середовища, де найважливішим чинником виступає усвідомленість і відповідальність користувачів. Перехід до безпарольних технологій може стати новим етапом розвитку кібербезпеки.

Список використаних джерел:

1. Інформаційний менеджмент. Навчальний посібник / А.М. Кобилін, Б.В. Самородов – Львів: «Новий Світ – 2000», 2014. – 216 с.
2. Дубницький В. Ю., Кобилін А. М., Кобилін О. А., Кушнерук Ю. І., Ходирєв О. І. Обчислення значень функції Харрінгтона при інтервальному визначенні її аргументів. // Сучасні інформаційні системи, 2022. Т. 7, № 1, с. 116–123. doi: <https://doi.org/10.20998/2522-9052.2023.1>
3. Cisco Networking Academy. URL: <https://www.netacad.com/>
4. Cisco Skills For All – навчальні курси. URL: <https://skillsforall.com/course/>

5. NIST Special Publication 800-63B. Digital Identity Guidelines – Authentication and Lifecycle Management. 2017. URL: <https://pages.nist.gov/800-63-3/sp800-63b.html>

6. Microsoft Security Blog. Passwordless authentication: The next step in cybersecurity. URL: <https://www.microsoft.com/security/blog/>

УДК 004.8:004.056:519.85

Шабалтас В.Я.,
здобувач другого (магістерського) рівня вищої освіти
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Чеканова Н. М.
к. ф.-м. н., доцент,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

МЕТОДИ ОПТИМІЗАЦІЇ В ЗАДАЧАХ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

У сучасному цифровому світі кіберзагрози перетворилися з технічної проблеми на один із головних викликів для безпеки бізнесу, держави та кожного користувача. Щороку кількість кібератак невинно зростає, а способи їхнього приховування стають дедалі витонченішими. Традиційні засоби захисту, побудовані на фіксованих правилах і сигнатурах, часто просто не встигають за новими сценаріями атак.

За даними IBM Security[3], у 2024 році середній час виявлення витоку даних перевищував 200 днів, а середня вартість одного інциденту сягала 4,45 млн доларів США. Такі цифри свідчать: реагувати на загрози постфактум – занадто пізно.

Тому сьогодні в центрі уваги опинилися інтелектуальні системи захисту, які можуть не лише фіксувати підозрілу активність, а й навчатися на попередніх подіях, передбачаючи можливі ризики. Саме тут на сцену виходить штучний інтелект (ШІ) – здатний аналізувати величезні обсяги мережевого трафіку, розпізнавати нетипову поведінку та швидко адаптуватися до нових, раніше невідомих атак.

Однак навіть найкраща модель ШІ не буде ефективною без правильної оптимізації. Від того, як налаштовані параметри навчання, залежить не лише точність виявлення атак, а й швидкість реагування, стабільність роботи та витрати ресурсів. Тому сьогодні в дослідженнях усе більше уваги приділяється саме методам оптимізації – вони стають ключем до того, щоб ШІ справді працював швидко, точно й надійно.

Багато робіт зосереджені на порівнянні різних підходів до оптимізації на стандартних наборах даних. Один із найвідоміших – NSL-KDD[1–2], оновлена

версія класичного KDD'99[1], яка містить приклади як нормальної поведінки, так і різних типів кібератак. Саме цей набір даних дозволяє об'єктивно оцінити, наскільки ефективно модель виявляє вторгнення (IDS) за різних стратегій оптимізації. Згідно з узагальненими аналітичними даними з відкритих джерел [1–3], найкращі результати демонструють глибокі нейромережі зокрема, автоенкодери у поєднанні з сучасними оптимізаційними підходами – такими як байєсова оптимізація, ройові алгоритми або генетичні стратегії. Навіть при однакових архітектурах нейронних мереж, правильно підібраний метод оптимізації може дати приріст точності на 5–10%, а також знизити кількість хибнопозитивних спрацювань, які є критичними у практичному застосуванні систем кіберзахисту.

Таблиця для порівняння ефективності методів оптимізації в задачах виявлення кіберзагроз наведена нижче (Таблиця 1).

Таблиця 1.

Порівняння ефективності методів оптимізації в задачах виявлення кіберзагроз за даними [1–3]

Модель	Метод оптимізації	Точність (%)	Хибні спрацювання (FPR)	Час навчання (сек)
Random Forest	Гradientний спуск	89,2	11,5%	12,4
DNN	Генетичний алгоритм	93,5	7,8%	29,1
Autoencoder	Ройовий інтелект	94,1	6,3%	34,7
Autoencoder	Байєсова оптимізація	96,7	5,4%	23,5

Дані з таблиці свідчать про те, що автоенкодери в поєднанні з байєсовою оптимізацією демонструють не лише високу точність, але й оптимальний баланс між продуктивністю та витратами часу на навчання. Це робить їх придатними для реального впровадження в інфраструктури безпеки банків, хмарних сервісів, державних систем та інших середовищ, де потрібна оперативна реакція на загрози.

Загалом, правильний вибір методу оптимізації – це не просто технічна деталь, а стратегічне рішення. Він визначає, наскільки модель ШІ буде ефективною, стабільною, швидкою і придатною до масштабування. Із зростанням складності атак та обсягів трафіку, саме оптимізовані моделі стануть основою нових поколінь систем виявлення загроз, що працюють не лише на основі відомих сигнатур, а й через розуміння поведінкових закономірностей.

Список використаних джерел

1. Tavallae, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA).

2. Nguyen, N. T., Nguyen, T. P., & Van Huynh, N. (2021). Deep learning for intrusion detection using autoencoders with Bayesian optimization. Journal of Information Security and Applications, 58, 102804.

3. Sarker, I. H., Kayes, A. S. M., & Watters, P. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 7(1), 1-29.

УДК: 004.056.5:004.738.5

Шутова А.В.

здобувач вищої освіти,

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

Науковий керівник

Єрмакова Н.А.

ст. викл. кафедри інформаційних технологій

та математичного моделювання

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

МЕТОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ХМАРНИХ СЕРВІСАХ

Сучасне життя все більше переноситься у хмарні сервіси, де користувачі зберігають особисту та професійну інформацію. Разом із ростом популярності таких платформ зростають і ризики витоку даних, несанкціонованого доступу та кібератак. Конфіденційність персональної інформації стає критично важливою для користувачів і компаній, адже від цього залежить безпека бізнес-процесів, фінансова стабільність та довіра клієнтів [1].

Одним із ключових методів захисту інформації є шифрування даних, а також використання багатофакторної автентифікації і чітких політик доступу, що дозволяє зменшити ймовірність компрометації хмарних облікових записів [2]. Метою цього дослідження є аналіз сучасних методів захисту персональних даних у хмарних сервісах та оцінка їх ефективності для користувачів і організацій.

Для захисту персональних даних у хмарних сервісах застосовують такі основні методи:

1. Шифрування даних.

Дані зберігаються у зашифрованому вигляді, а для доступу потрібен ключ розшифровки. Сучасні алгоритми (AES, RSA) забезпечують високий рівень безпеки навіть у випадку витоку файлів [2].

2. Багатофакторна автентифікація (MFA).

Додає другий або третій рівень перевірки особи користувача (SMS-код, код з мобільного додатку або фізичний ключ безпеки). Навіть якщо злоумисник знає пароль, без додаткового фактору доступ отримати складно [5].

3. Контроль доступу та налаштування прав користувачів.

Кожен користувач отримує тільки ті права, які необхідні для роботи. Адміністратори можуть обмежувати доступ до чутливої інформації та відстежувати спроби входу [4].

4. Регулярне навчання користувачів.

Людський фактор часто стає слабкою ланкою безпеки. Навчання допомагає розпізнавати підозрілі листи, фішингові посилання та сумнівні запити [4].

5. Сучасні технології аналітики та штучного інтелекту.

Системи AI можуть автоматично виявляти аномальні дії в хмарі та попереджати про потенційні загрози [3]. Це дозволяє оперативно реагувати на атаки і зменшувати ймовірність витоку даних.

Застосування цих методів у комплексі значно підвищує безпеку персональних даних у хмарних сервісах. Шифрування, багатофакторна автентифікація та контроль доступу допомагають захистити інформацію від несанкціонованого доступу, а навчання користувачів і сучасні системи аналітики дозволяють своєчасно виявляти потенційні загрози [2],[3],[4].

Висновки та рекомендації:

Комплексне застосування методів захисту персональних даних у хмарних сервісах є ключовим фактором забезпечення безпеки користувачів і організацій. Шифрування, багатофакторна автентифікація та контроль доступу зменшують ризики несанкціонованого доступу, а навчання користувачів і сучасні аналітичні інструменти дозволяють своєчасно виявляти підозрілі дії [1],[5].

Як наголошує Ілон Маск, у сучасному цифровому середовищі безпека персональних даних має бути пріоритетом для всіх користувачів і організацій. Він рекомендує впроваджувати багатофакторну автентифікацію, контролювати права доступу до інформації та регулярно проводити навчання персоналу щодо безпечної роботи з хмарними сервісами [3].

Такий підхід дозволяє мінімізувати ризики витоку інформації, підвищує довіру користувачів і забезпечує стабільну та безпечну роботу організацій у цифровому середовищі [2],[5].

Список використаних джерел

1.Зарічук О. Безпека в хмарних обчисленнях: методи забезпечення приватності та інтеграції //Управління розвитком : міжнар. екон. журн. / [редкол.: Т. В. Шталь (голов. ред.) та ін.]. – Харків : Харківський національний економічний університет імені Семена Кузнеця, 2024.– Т. 23, № 1. С. 45–52. URL:

<https://devma.com.ua/en/journals/t-23-1-2024/bezpeka-v-khmarnikh-obchislennyakh-metodi-zabezpechennya-privatnosti-ta-integratsiyi-v-suchasnikh-dodatках>

2. Agri, R., Kudjo, A., Afodjo, K. et al. Cloud Security Best Practices: Strategic Measures to Protect Digital Assets Within the Cloud. International Journal for Multidisciplinary Research (IJFMR), 2025. - № 7(1), P. 1–10. URL: https://www.researchgate.net/publication/388074557_Cloud_Security_Best_Practices_Strategic_Measures_to_Protect_Digital_Assets_Within_the_Cloud

3. Akineye, A. O., Adepoy, P. A., Ige, A. B., Afolabi, A. I. Cloud Security Challenges and Solutions: A Review of Current Best Practices // International Journal of Multidisciplinary Research and Growth Evaluation, 2025. № 6(1), P. 26–35. URL: https://www.researchgate.net/publication/387558426_Cloud_Security_Challenges_and_Solutions_A_Review_of_Current_Best_Practices

4. Бойко, О. М. Розробка методології захисту інформації від атак соціальної інженерії. Тернопіль, ТНТУ, 2020. - С.41.

5. Безпека у хмарі: поради та кращі практики. SMART Cloud. URL: <https://cloud.smart-it.com/news-post/cloud-security-tips-and-best-practices/> (дата звернення: 20.09.2025)

УДК 004.8

Щувайло Д.О.

здобувач вищої освіти,

Державний торговельно-економічний університет

Науковий керівник

Горохова О.М.

к.ф.м.н., доцент, доцент кафедри інженерії програмного забезпечення

Державний торговельно-економічний університет

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ КІБЕРЗАХИСТУ ТА ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

У сучасних умовах цифровізації та розвитку глобальної мережі Інтернет питання кібербезпеки набувають стратегічного значення. Штучний інтелект (ШІ) виступає одночасно потужним інструментом протидії кібератакам та новим джерелом загроз.

Штучний інтелект сьогодні сприймається як потужний інструмент кіберзахисту. Його застосування дає змогу результативно здійснювати нагляд мережевого трафіку та виявляти аномалії в режимі живого часу. Внаслідок машинного навчання розробляються сучасні системи виявлення вторгнень (IDS/IPS), які можуть оперативно реагувати на підозрілу активність. Окрім того, ШІ забезпечує автоматизацію обробки великих баз даних, що дозволяє передбачати можливі кібератаки ще до їх реального виконання.

Разом з тим штучний інтелект становить також певну небезпеку для інформаційної безпеки. Зокрема, генеративні системи можуть використовуватися для створення правдоподібних фішингових листів, які складно розрізнити від справжніх. Deepfake-технології дають змогу змінювати відео- та аудіо-матеріали, обманюючи користувачів. Окрім цього, автоматизовані кібератаки із використанням ботів та адаптивних алгоритмів суттєво підвищують їхню дієвість і масштабність.

У такому випадку важливо враховувати перспективи та виклики, які стоять перед суспільством. Для протидії новим загрозам вимагає тісної міжнародної

співпраці, яка забезпечить обмін знаннями і спільні заходи безпеки. Одночасно потрібна розробка системи етичних норм, що регулюватиме застосування ШІ в галузі кіберзахисту. Головним завданням є досягнення рівноваги між інноваціями та захистом даних, адже лише загальний підхід забезпечить ефективне використання можливостей штучного інтелекту та мінімізувати його ризики.

Висновки
Штучний інтелект є двосічним інструментом: з одного боку він посилює можливості захисту, з іншого — створює нові загрози. Саме тому дослідження та розробка комплексних підходів до використання ШІ у кібербезпеці є пріоритетним завданням сучасного суспільства.

Список використаних джерел:

1. Symantec. Internet Security Threat Report. Volume 23: Executive Summary. URL: <https://docs.broadcom.com/docs/istr-23-executive-summary-en>
2. European Union Agency for Cybersecurity (ENISA). Artificial Intelligence and Cybersecurity Research. URL: <https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research>
3. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. Norton, 2018. URL: <https://www.schneier.com/books/click-here/>
4. Cisco Networking Academy. URL: <https://www.netacad.com/>

УДК 004.6-027.552:004.777

Яхно Н.Є.

Курсант 2 курсу ННІ №4

Науковий керівник:

Мальцев В.В.

*викладач кафедри протидії кіберзлочинності
навчально-наукового інституту (ННІ) №4*

Харківський національний університет внутрішніх справ

ПРАКТИЧНІ АСПЕКТИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ВЕБ-СЕРВІСАХ

В контексті сучасного інформаційного суспільства спостерігається стрімке зростання обсягів оброблюваних персональних даних, однак зі збільшенням їх об'єму зростають і різноманітні загрози для безпеки наведеного типу інформації. Персональні дані розглядаються як система атрибутів ідентифікаційної, фінансової, медичної та соціально-демографічної природи, що наразі можна позиціонувати як стратегічний, інфраструктурно значущий ресурс для публічної влади, бізнесу та суспільства.

Нормативний каркас наведеного питання формулює Закон України «Про захист персональних даних», який окреслює легальну рамку для операцій з такими даними, однак автономна правова комплаєнс-рамка не гарантує фактичної безпеки: без технічно якісно спроектованих і експлуатаційно витриманих механізмів не гарантує безпеки по криптографічним, або операційним векторам атаки. В такому контексті криптографічні інструменти виглядають необхідною (хоч і недостатньою) умовою належного захисту: вони формалізують гарантії у площині протоколів, гарантують конфіденційність каналів і сховищ, автентичність джерела та інваріантність даних в площині несанкціонованих модифікацій. Реальна ефективність криптозахисту залежить не лише від вибору алгоритмів, а й від комплексного контуру керування ключами (генерація, розповсюдження, зберігання, ротація, відкликання), коректності режимів та параметрів, та від організаційного контролю (розмежування повноважень, аудит). Саме в конфігурації правових норм і математично обґрунтованих криптографічних конструкцій виникає доказовий периметр довіри до систем оперування персональними даними [1].

Класифікація персональних даних:

- перша група ПД створюється та збирається органами державної влади і місцевого самоврядування відповідно до вимог закону.
- друга група ПД створюється та збирається суб'єктами права власності і господарювання відповідно до вимог закону.
- третя група ПД самостійно надається фізичними особами органам державної влади і місцевого самоврядування та суб'єктам права власності і господарювання у визначені законом терміни та ситуації.
- четверта група персональних даних створюється суб'єктами права власності і господарювання згідно з угодами між ними та фізичними особами, що описуються цими даними [2].

Захист персональних даних реалізується на двох взаємодоповнюючих рівнях:

1. Нормативно-правовий – встановлює правила збору, обробки, зберігання та передачі даних, права та обов'язки суб'єктів інформаційних відносин, відповідальність за порушення конфіденційності.
2. Технічно-криптографічний – забезпечує практичну реалізацію захисту, включаючи шифрування, хешування, електронний цифровий підпис, автентифікацію користувачів та контроль цілісності даних.

Криптографія – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації сторонніми) і автентичності (цілісності і справжності автора) інформації [3].

Основні методи криптографічного захисту інформації можуть бути класифіковані різним чином, але найчастіше їх розподіляють в залежності від способу використання та за типом ключа [3-5]:

- системи без ключа – не використовуються ключі (хеш-функції, генерація псевдовипадкових чисел, односторонні перестановки);
- системи з таємним ключем – використовується один секретний ключ – (симетричне шифрування, ідентифікація);

– системи з відкритим ключем – використовуються два ключі – відкритий/публічний та закритий/приватний (асиметричне шифрування, цифровий підпис, автентифікація).

Таблиця 1

Порівняльна характеристика методів криптографічного захисту

Метод	Принцип	Приклади	Переваги	Недоліки	Застосування
Симетричне шифрування	Один ключ (шифрування, розшифрування)	AES, DES, 3DES, RC4	Швидке шифрування великих обсягів	Проблеми з безпечним передаванням ключа	Шифрування файлів, VPN, диски
Асиметричне шифрування	Два ключі: відкритий та закритий	RSA, ECC	Безпечний обмін ключами, захист від перехоплення	Повільне для великих обсягів даних	SSL/TLS, електронна пошта, обмін ключами
Хеш-функції	Генерація фіксованого хеш-коду з повідомлення	SHA-256, MD5, SHA-3	Швидка перевірка цілісності даних	Не забезпечує конфіденційності	Контроль цілісності файлів, паролі
Цифровий підпис	Використання закритого ключа для підпису, відкритого для перевірки	RSA, DSA, ECDSA	Гарантує цілісність	Потребує асиметричного шифрування для перевірки	Документи, електронна пошта, контракти

У сучасному цифровому середовищі персональні дані піддаються постійним загрозам, що походять як від злочинних суб'єктів, так і від технічних чи організаційних недоліків.

До основних загроз належать несанкціонований доступ, який може проявлятися у зломах баз даних, крадіжці облікових даних або використанні вразливостей у програмному забезпеченні, витік даних, що призводить до несанкціонованого розповсюдження або публікації персональної інформації, фішинг та соціальна інженерія, що передбачають обман користувачів для отримання конфіденційної інформації, такої як паролі, номери карток або медичні дані.

У підсумку варто зазначити, що ефективна політика захисту персональних даних формується на базі нормативної архітектури та доказових криптографічних гарантій. В такій архітектоніці правові вимоги встановлюють рамку допустимих операцій, а математично верифіковані протоколи конкретизують рівні довіри. Якість безпеки здебільшого залежить від коректного моделювання загроз і їх мапування на криптоконтролі (конфіденційність, цілісність, автентичність) в синергії з політиками доступу, аудитом і журналюванням. Стратегія захисту ПД має бути ризик-орієнтованою, інтегрованою з міжнародними стандартами та конструюватись з випередженням технологічного горизонту, адже лише така інтегрована

парадигма дозволяє мінімізувати залишковий ризик і гарантує відтворювані, перевірні властивості безпеки у реальних інформаційних системах.

Список використаних джерел:

1. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // БД «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> .
2. Обуховська Т. Класифікація персональних даних та режиму доступу до них. *Вісник Національної академії державного управління при Президентові України*. 2013. № 1. С. 97–104.
3. Мінгальова Ю. І. Новітні криптографічні методи захисту інформації // *«Науково-дослідна робота молодих учених: стан, проблеми, перспективи» : II Всеукр. наук.-практ. Інтернет-конф., присвяч. 95-річчю Херсонського держ. ун-ту* (м. Херсон, 12–16 листоп. 2012 р.). Херсон, 2012. С. 373–378.
4. Водозазський В. Комерційні системи шифрування: основні алгоритми та їх реалізація. *Монітор*. 1992. № 6–7. С. 14–19.
5. Бабак В. П. Теоретичні основи захисту інформації : підручник. Київ : Книжкове видавництво НАУ, 2008. 752 с.

РОЗДІЛ 2.

ТЕХНІЧНІ СКЛАДОВІ ПРОЄКТУВАННЯ, РОЗРОБКИ, ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ І МЕРЕЖ

Kravchenko O.O.

*postgraduate student of Department of Informatics,
Kharkiv National University of Radio Electronics*

Academic Advisors

Vechirska I.D.

*Ph. D., associate professor of Department of Informatics,
Kharkiv National University of Radio Electronics*

Kobylin O.A.

*Ph. D., associate professor, head of Department of Informatics,
Kharkiv National University of Radio Electronics*

METHODS OF FINITE PREDICATE ALGEBRA FOR FORMALIZING SEMANTIC STRUCTURES OF TEXTS

Text semantic analysis is one of the key directions of modern computational linguistics and natural language processing (NLP). The growth of textual data requires methods capable not only of surface-level classification or segmentation but also of revealing deep semantic connections between linguistic elements. Mathematical approaches that enable unified representation of textual structures and logical operations over them are of particular importance. One of the promising tools for this purpose is the algebra of finite predicates (AFP).

Current research in semantic text analysis traditionally develops along several lines. Statistical methods, such as frequency-based models (TF-IDF, Bag-of-Words) or word vector representations (Word2Vec, GloVe), are known for their simplicity and efficiency, but they largely ignore contextual dependencies [1]. Linguistically oriented methods rely on grammatical rules, dictionaries, and ontologies such as WordNet, which makes it possible to account for semantic roles but requires significant human resources and complex maintenance [2]. Neural network methods, including transformer architectures like BERT and GPT, demonstrate high performance in meaning recognition but remain poorly interpretable and difficult to verify in terms of formal correctness [3].

Predicate algebra helps overcome these limitations by formally representing relationships between objects in a text. Within this approach, subjects and objects of sentences are described as variables, while relations between them are expressed as predicates. Logical operations such as union, intersection, or implication allow the creation of more complex yet formally correct semantic structures. For example, the sentence “*The student reads a book*” can be represented as *Reads(Student, Book)*, which opens the possibility of combining it with other statements to form an integral semantic model.

To demonstrate the differences between approaches, a comparison of traditional methods and finite predicate algebra was conducted across the main evaluation criteria. In the results, as shown in Table 1, AFP significantly outperforms other approaches in terms of formal rigor and interpretability, which is crucial for applied systems requiring transparent logic.

Table 1.

Comparative analysis of approaches to semantic text analysis

Criterion	Statistical methods	Neural network methods	Algebra of finite predicates
Interpretability	Low (frequencies)	Very low ("black box")	High, explicit logical rules
Formal correctness	Partial	Partial	Full, mathematically guaranteed
Scalability	High	High	Medium (depends on predicate construction)
Resource consumption	Low	High (GPU, large datasets)	Moderate
Adaptation to Ukrainian language	Limited	Limited (lack of corpora)	High (rules formed at the level of logical structures, language-independent)

During the study, a conceptual model of semantic analysis based on AFP was created. It consists of three levels. At the first, lexico-syntactic level, preprocessing of text is carried out: tokenization, part-of-speech tagging, and syntactic dependency analysis. The second, predicate level, involves forming predicate expressions for each sentence that reflect relationships between subjects, actions, and objects. The third, semantic level, integrates predicates into logical structures capable of checking consistency, identifying contradictions, and making inferences based on set rules.

Practical testing of the model was conducted on a corpus of Ukrainian texts of medium size. Results showed that the use of AFP reduces the number of false positive links between entities by 18% compared to neural network methods without explainability, ensures transparency of all analysis steps, and maintains acceptable processing speed for texts of medium length. Thus, the algebra of finite predicates has proven effective as a tool for formalizing semantic text structures.

Future development of this line of research involves expanding the text corpus for experiments, improving algorithms for predicate structure construction, and potentially integrating the model with neural network approaches to achieve an optimal balance between performance and formal rigor. Such combination may provide a new level of quality in applied systems for natural language analysis, where the balance between accuracy, speed, and interpretability is of decisive importance.

References:

1. D. A. Haisal, U. Mahmood. Sentiment Classification: Review of Text Vectorization Methods: Bag of Words, Tf-Idf, Word2vec and Doc2vec // SLU Journal of Science and Technology, 2022. 27-33p.
2. C. Fellbaum. WordNet: An Electronic Lexical Database // MIT Press, 1998.

3. J. Devlin, M. W. Chang, K. Lee. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding // NAACL, 2019.

UDC 004.056.53

Nikolaichuk A.I.,
applicant of higher education,
Kharkiv National University of Radio Electronics
Kobylin I.O.,
PhD in Engineering,
Assistant Lecturer of the Department of Informatics,
Kharkiv National University of Radio Electronics;

SENSITIVITY OF TRANSFORMER MODELS TO SYNTACTIC COMPLEXITY LEVELS IN UKRAINIAN SENTENCE SIMILARITY

Recent work shows that even top transformer models, like BERT, can struggle with texts of different complexity [1]. However, research on how sentence-level syntactic complexity influences model performance in semantic similarity tasks (STS), particularly for languages other than English, is limited. Understanding how models respond to different levels of syntactic complexity is important for assessing their sensitivity and robustness. With a rich morphology and relatively free word order, Ukrainian presents additional challenges for syntactic analysis. Dependency relations in sentences span longer distances [2], increasing the complexity of parsing and potentially affecting model predictions.

This study evaluates the model's performance on Ukrainian sentences with a mean dependency distance (MDD) as a syntactic complexity metric. In the process, sentence pairs are grouped into three complexity levels to analyze how prediction errors vary across these levels and provide detailed insights into handling structural variation.

This study aims to systematically evaluate how transformer models respond to different levels of syntactic complexity in Ukrainian sentences. Grouping sentences according to their Mean Dependency Distance (MDD) [3] allows for further assessment of which models are most sensitive to structural variation and reveals patterns in prediction errors. These analyses provide insights into model performance and highlight potential limitations when handling morphologically rich languages.

MDD reflects the average span between syntactically related words in a sentence. For a sentence with n words, it is computed as shown in formula (1):

$$MDD = \frac{1}{n-1} \sum_{i=1}^{n-1} |DD_i|, \quad (1)$$

where DD_i is the number of words separating a governor from its dependent.

Each sentence has exactly one root, usually a main word, where $DD = 0$.

The dataset used is the Ukrainian translation [4] of the Semantic Textual Similarity Benchmark (STSB), containing 5749 pairs of sentences with similarity scores from 0 to 1. Based on the distribution of MDD values, sentences were divided into three groups: Low, Medium, and High complexity. Table 1 shows the group boundaries along with example sentences and their corresponding MDD values.

Table 1.

Example sentences grouped by complexity levels based on MDD

Level	Bounds	Example sentence pair	MDD of sentence
Low	≤ 1.5	Італійські паломники загинули в результаті падіння автобуса.	1.17
Medium	≤ 2.5	Вибух на нафтопереробному заводі у Венесуелі забрав життя щонайменше 39 людей.	2.2
High	> 2.5	Це лікарня, яка ставиться до всіх, як до людей, і якби ми могли робити це в усьому світі, ми могли б покінчити з тероризмом.	3.13

For evaluation, six multilingual models from the Hugging Face Sentence-Transformers library were selected: paraphrase-multilingual-mpnet-base-v2 (MPNet), paraphrase-multilingual-MiniLM-L12-v2 (MiniLM), LaBSE, gte-multilingual-base (GTE), distiluse-base-multilingual-cased-v2 (DistilUSE), and static-similarity-mrl-multilingual-v1 (StaticSim).

While overall trends indicate that prediction errors vary with sentence complexity, it is unclear which levels contribute most to these differences. Pairwise comparisons were conducted using the Mann–Whitney U test with Bonferroni correction to examine how models respond to contrasts between Low, Medium, and High complexity sentences. This non-parametric test compares distributions of independent groups and is well suited for this analysis. The test statistic is defined in formula (2):

$$U = n_1 n_2 + \frac{n_1(n_1+1)}{2} - R_1, \quad (2)$$

where n_1 and n_2 are sample sizes, and R_1 is the sum of ranks in the first group. The smaller of U_1 and U_2 is used as the final value.

The results of the pairwise Mann-Whitney U tests are summarized in Table 2.

All models showed significant differences in prediction errors for Low vs High complexity sentence pairs, indicating that the most considerable discrepancies occur between the simplest and most complex sentences. Thus, models handle these extremes most differently.

Table 2

Results of pairwise complexity comparisons

Models	Low vs Medium		Low vs High		Medium vs High	
	U-statistic	p-value	U-statistic	p-value	U-statistic	p-value
MPNet	3129782.0	0.142	512838.0	0.001	974677.5	0.01
MiniLM	3108037.0	0.296	510345.0	0.001	976029.5	0.008
LaBSE	3666817.0	<0.001	608377.0	<0.001	1009629.0	<0.001
GTE	3437975.0	<0.001	569943.0	<0.001	997482.0	<0.001
DistilUSE	3448662.0	<0.001	602660.0	<0.001	1063247.5	<0.001
StaticSim	3286256.0	<0.001	541971.0	<0.001	995763.0	0.001

The Medium vs High complexity comparison also revealed significant differences across all models, although the effect size varied. LaBSE, DistilUSE, and GTE displayed the strongest sensitivity to these differences.

In contrast, the Low vs Medium complexity comparison showed significant differences for most models, except for MPNet and MiniLM. This indicates that these two models are less capable of distinguishing between adjacent complexity levels, pointing to their lower sensitivity to syntactic variation.

Overall, the results show that sensitivity to sentence complexity differs across models. LaBSE and DistilUSE exhibit clear error separation across all levels, reflecting a strong response to syntactic structure. MPNet and MiniLM, however, show weaker distinctions, particularly between Low and Medium levels, suggesting a greater reliance on other textual features, such as lexical content.

In conclusion, sentence-level syntactic complexity influences the transformer models' performance on Ukrainian sentence similarity, confirming that structural variation poses a meaningful challenge. Grouping sentences into Low, Medium, and High complexity levels revealed consistent patterns across all models: the most considerable differences occur between the simplest and most complex sentences. In contrast, distinctions between adjacent levels are generally negligible. These findings highlight that syntactic complexity is a critical factor in sentence similarity prediction, particularly for Ukrainian, as even state-of-the-art models vary in their sensitivity to morphologically rich and flexible word-order structures.

References:

1. An exploratory study on code attention in BERT / R. Sharma et al. *ICPC '22: 30th International Conference on Program Comprehension*, Virtual Event. New York, NY, USA, 2022. URL: <https://doi.org/10.1145/3524610.3527921>.
2. Divjak D., Sharoff S., Erjavec T. Slavic Corpus and Computational Linguistics. *Journal of Slavic Linguistics*. 2017. Vol. 25, no. 2. P. 171–199. URL: <https://doi.org/10.1353/jsl.2017.0008>.
3. Dependency Distance Differences across Interpreting Types: Implications for Cognitive Demand / J. Liang et al. *Frontiers in Psychology*. 2017. Vol. 8. URL: <https://doi.org/10.3389/fpsyg.2017.02132>.

4. STSB-UK · Datasets at Hugging Face. *Hugging Face – The AI community building the future*. URL: <https://huggingface.co/datasets/anikol12/STSB-UK>.

УДК 004.7:004.9

Oliinyk Yehor

*applicant of professional preliminary higher education,
Separate structural unit «Kharkiv Computer and
Technological Vocational College of NTU «KhPI»*

Korpan Veronika

*applicant of professional preliminary higher education,
Separate structural unit «Kharkiv Computer and
Technological Vocational College of NTU «KhPI»*

Zavora Yana

*scientific supervisor, category 1 lecturer
Separate structural unit «Kharkiv Computer and
Technological Vocational College of NTU «KhPI»*

INFORMATION SYSTEMS AND NETWORKS: TECHNICAL SUPPORT

Modern information systems and networks are the foundation of digital transformation of society, ensuring effective storage, processing and transmission of data. Their operation is based on a holistic set of technical components that determine the level of reliability, safety and performance of the entire infrastructure. Of scientific and practical interest is the systematic analysis of data components at different stages of the life cycle of the information system.

One of the key elements is hardware. It includes server systems, workstations, telecommunication and network equipment as well as data storage systems. The hardware part forms the basis of the computing environment and determines the extent of further development of the system. In modern conditions, the focus is shifting towards the use of high-performance servers, virtualization of computing resources and building cloud data centers.

Software is an equally important component. It is divided into system (operating systems, virtualization platforms, administration tools) and application (database management systems, corporate applications, specialized modules). The software environment provides automation of processes, interaction between users and equipment, as well as business logic support. Special attention is given to the use of cloud technologies and integration with big data services.

Network technologies and protocols ensure the interaction of distributed hosts and users. The core is the TCP/IP family of standards, allowing to integrate local, corporate and global network infrastructure segments. Current trends include the use of software-defined networks (SDN), virtualization of network functions and the use of secure communication channels (VPN).

Information security is of key importance and seen as an integral part of the technical architecture. In the face of growing cyber threats, data protection is achieved through cryptographic methods, authentication and authorization systems, firewall screens, attack detection tools and network traffic monitoring. Without a comprehensive approach to security, the use of information systems becomes risky, especially in critical industries.

At all stages of the information system life cycle – from design to operation – technical components play a crucial role. At the design stage, the technical specification and architecture are formed, scalability and flexibility of solutions are built. The software and hardware modules are being adapted during the development phase. The implementation phase includes installation and integration of hardware and software, networking. The operation phase is related to administration, updating and ensuring business continuity. Finally, modernization makes it possible to adapt the system to changing conditions and new technological challenges.

Thus, the effectiveness of information systems and networks is directly determined by an integrated approach to the organization of technical components. Their balanced interaction ensures reliability, high performance and resistance to threats. Promising areas of research are related to the development of cloud infrastructures, the introduction of artificial intelligence technologies for monitoring and management, as well as strengthening cyber-protection.

Conclusion. Research and improvement of technical components of information systems and networks is a current challenge of modern science and practice. It aims to increase the efficiency of digital infrastructure, which ultimately contributes to the development of the economy and society in the context of global informatization.

References:

1. Поняття про інформаційні системи та їх класифікації . URL: [ПОНЯТТЯ ПРО ІНФОРМАЦІЙНІ СИСТЕМИ ТА ЇХ КЛАСИФІКАЦІЇ, З історії розробки інформаційних систем – Теорія інформаційних процесів і систем – Підручники для студентів онлайн](#)
2. URL: [4.4. Організація процесу проектування, розробки та впровадження інформаційних систем – Бібліотека BukLib.net](#)
3. Глушков В. М. Основи побудови інформаційних систем. – К.: Наукова думка, 2018. – 352 с.
4. Кобилін, А. М. Інформаційний менеджмент: навч. посіб. / А. М. Кобилін, Б. В. Самородов. – Львів: Новий Світ-2000, 2018. – 216 с.

THE PROCESS OF ASSESSING THE CORRUPTION ORIENTATION OF REGULATORY LEGAL ACTS AND ITS MODELING

Increasing requirements for means and methods of combating negative phenomena of society, as well as creating conditions for the prevention and prevention of corrupt actions of officials by editing old and creating new normative legal acts, can significantly limit the development of such offenses and have a positive impact on the economic state of the state. The task of developing fairly simple but effective methods of modeling, as well as assessing the level of corruption of regulatory legal acts, is becoming urgent. The article considers an important problem of quantitative assessment of the negative phenomenon of corrupt activities of officials, which can be stimulated by regulatory legal acts. The proposed modeling approach, carried out in order to quantify the level of corruption orientation of regulatory legal acts, allows to simultaneously take into account some individual criteria that are based on subjective assessments and have uncertainties of various nature, as well as are characterized by a fairly large number, as well as their antagonism and inequivalence. The considered modeling process provides the possibility of using both fuzzy and clear representation of the initial data, reduces the influence of the subjectivity of expert assessments on heuristic factors. When forming a global criterion for making a decision on the level of corruption orientation of a regulatory legal act, there is no need to determine the weight of each individual factor. The obtained values of the global criterion make it possible to make a decision on the choice of one of the variants of the normative legal act. The article carefully considers all stages of the implementation of the proposed approach to assessing the level of corruption of the regulatory legal act on the reclamation of forestry lands violated as a result of amber mining. If a state that does not have sufficient control over corrupt activities draws up any agreement between private and public sector entities, then with the help of which state assets are illegally converted into private ones. Such corruption is quite often used as a synonym for corruption of a high or high level of law-making corruption. But it differs from bureaucratic or so-called petty corruption, as it can be associated with political figures who make meaningful decisions. Indeed, law-making corruption is the most pernicious for any country, because politicians who have the right to create and then apply laws on behalf of the people use this power to maintain their power, status and wealth. Such law-making corruption not only leads to irrational use of resources, but also distorts the principle of state management and then the entire system of state governance becomes kleptocratic. It is corruption that is really the most important problem of our time, which cannot be overcome without the active participation of the whole society. After all, the situation in the modern state as a whole depends on how each ordinary citizen reacts and treats the manifestation of corrupt actions. Ideally, every person is obliged

to fight any manifestations of corruption by all available and, most importantly, legal methods.

The main negative phenomena that arise as a result of law-making corruption are: nullification of economic reforms in public institutions; reduction in the number and volume of investment projects; violation of the principles of social justice, equality of a person before the law; a drop in trust in the authorities, etc. Thus, Article 15 of the Law of Ukraine "On the Principles of Preventing and Combating Corruption" establishes the obligation to conduct anti-corruption examinations of draft regulations. The use of a scientific approach to the formalization of the process of such expertise helps to increase its objectivity and efficiency. That is why the development and implementation of measures that will allow to independently assess the level of corruption of regulatory legal acts is the most urgent task of today.

The main purpose of the study is to improve methods and techniques for analyzing the process of assessing the quality of regulatory legal acts by modeling their corruption orientation. The object of the study is the process of assessing the corruption orientation of regulatory legal acts. The subject of the study is the methods of fuzzy analysis and decision-making in conditions of data uncertainty. The formulation of the task of assessing the level of legal acts to promote corruption is characterized by a rich number and uncertainty of private criteria, their inequivalence, as well as antagonism. At the same time, it is very important to simultaneously take into account criteria that are based on subjective assessments and have uncertainties of a different nature. The proposed approach to assessing the level of ABOs to promote corruption has the following features and advantages: initial data can be presented both in clear and fuzzy numbers; Particular criteria of different nature are reduced to some relative units, which simplifies the convolution to a global quality indicator; there is no need to determine the weight of each individual indicator; the use of expert assessments is minimized (only when creating affiliation functions); The methodology can be used both to compare the corruption orientation of regulatory legal acts and to determine its relative change. The paper discusses in detail the stages of the process of assessing the corruption orientation of regulatory legal acts. At the same time, it is possible to quantify the negativity of legislation. For the further development of this work, it is planned to conduct research on accounting for possible financial losses, which is an additional incentive for the emergence of corruption in legal acts.

References

1. Law of Ukraine "On Prevention of Corruption" (with amendments and additions) [Electronic resource]. – Mode of access to the resource: <http://www.zakon.rada.gov.ua>
2. Methodology for managing corruption risks [Electronic resource]. – Mode of access to the resource: <http://www.nazk.gov.ua/uk/d>
3. Malyshko Y.M. Assessment and neutralization of the negative impact of administrative barriers on small business: dissertation of Candidate of Economic Sciences. – Kh., 2016. – 238 p.

4. Dubois D., Koenig J.L. Social choice axioms for fuzzy set aggregation // Fuzzy Sets and Systems. 2017. V. 43. P. 257 – 274. doi/10.1016/0165-0114(91)90254-N
5. Malyshko Y. M. Fuzzy-Multiple Assessment of the State of Parameters of Technical and Economic Systems / Yu.M. Malyshko, M. Y. Losev // Information Processing Systems: Collection of Scientific Papers. – Kh.: Ivan Kozhedub Kharkiv University of the Air Force, 2015. – Vol.4 (129). – P.33-38
6. Kononov N. Y. Methods of multi-criteria assessment of the state of technical and economic systems based on fuzzy-multiple analysis of indicators / Kononov N. Y., Loseva Y. M. – KH. : HUPS, 2015. – 232 p.
7. Fundamentals of the theory of fuzzy sets [Electronic resource]. – Mode of access to the resource: <https://www.sites.google.com/site/nechitkalogika/osnovi-teoriiie-necitkih-mnozin>
8. Zayats V.M., Rybytska O.M., Zayats M.M. Hidden possibilities of mathematics in the processing of fuzzy information [Electronic resource]. – Mode of access to the resource: <https://www.ewdtest.com/ri/wp-content/uploads/2018/01/%D0%A1%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D1%8B-64-71-%D0%B8%D0%B7-Maket-2017-4-NEW.pdf>
9. Information Systems and Technologies: Monograph / edited by V.S. Ponomarenko. – Kh.: Publish-ing House LLC "Style-Izdat", 2019. – p.155–169.
10. Information Technologies: Problems and Prospects: Monograph / Edited by V.S. Ponomarenko. – Kh.: Publishing House by Rozhko S.G., 2017. – 446 p.
11. George Bojadziev , Maria Bojadziev . Fuzzy Logic for Business, Finance and Management / Ad-vances in Fuzzy Systems – Applications and Theory. – 2017. – Vol.23. – 232
12. Daugul V., Aleksenko A. Actual issues of use of agricultural land by local self-government bodies / V. Daugul, A. Aleksenko. – Kh.: Factor, 2018. – 176 p. ISBN 978-966-180-731-9
13. Dudorov O.O., Komarnytskyi M.V., Kalmykov D.O. Criminal responsibility for illegal mining in Ukraine: monograph / O. O. Dudorov, M. V. Komarnytskyi, D. O. Kalmykov; ed. by O. O. Dudorov, V. M. Komarny-tskyi. – Sumy: RVV LDUVS named after E.O. Didorenko, 2016. – 567 p. ISBN 978-617-616-068-7
14. Shust G. P. Administrative-Legal Protection of Land Resources of Ukraine: Dissertation of Candi-date of Juridical Sciences: 12.00.07; defended 22.06.19; ; approved 25.12.16 / G. P. Shust – Ternopil, 2019. – 234 p.

Skorin Yuriy,
PhD, Associate Professor
Simon Kuznets Kharkiv National University of Economics,
SUN Xiaohai,
student of higher education
Simon Kuznets Kharkiv National University of Economics

AGILE PROJECT MANAGEMENT METHODS

It is emphasized that the present requires a significant increase in the practical effectiveness of the agile management strategy in the practice of corporate management. The analysis carried out showed that at the methodological level, this research initially systematically develops the basic concepts of agile management, emphasizing its characteristics of flexibility and adaptability, and proposes innovations in the organizational structure and management models to better meet the diverse needs of both the internal and external environment of the enterprise. Also, with the help of an in-depth analysis of specific cases of application of agile management, this study reveals the positive consequences of applying strategies such as a certain organizational structure, the introduction of flexible and diverse work schedules, and the establishment of a performance-oriented system on the ability of the enterprise to quickly adapt to market changes, flexibly adjust strategic directions and maintain a leading position in competitive market conditions.

This study is aimed at conducting an in-depth analysis of the importance and practical effectiveness of the agile management strategy in the practice of corporate management. In the face of increasingly fierce competition in the market and the rapidly changing market environment, enterprises urgently need to increase their response speed and comprehensive competitiveness to ensure their stable development. This study aims to provide practical advice and recognition for business managers, helping them to deeply understand and effectively apply agile management strategies to promote the long-term sustainable development of enterprises. In today's fast-changing and fiercely competitive market environment, enterprises are increasingly focusing on improving responsiveness and comprehensive competitiveness in order to achieve sustainable development. Among them, an agile management strategy, as an example of a people-centered management philosophy, plays a crucial role in team management. It emphasizes the adaptability and innovativeness of organizational structures and management methods, giving employees more autonomy and a sense of participation, thereby stimulating their innovative spirit and work enthusiasm, as well as increasing team efficiency and responsiveness.

Project management, as a key tool for achieving project objectives, is becoming increasingly important. In the telecommunications industry, Group A, as a leading enterprise, has demonstrated the key role of technological innovation in ensuring high-quality development and transformation of enterprises through the

practice of agile project management practices. The essence of agile project management is to increase the adaptability and agility of organizations to market changes, especially in the application of advanced technologies such as 5G, cloud computing, big data, and artificial intelligence. Group A's practice has shown that agile project management can effectively cope with rapid market changes and technological innovations. With more than 1600 fully connected 5G factory projects, Group A has not only made significant progress in integrating 5G technology and business, but also led the construction of fully connected 5G factory projects by creating pilot projects of 5G-Advanced flexible factory projects. In addition, Group A, together with partners, has promoted the construction of private 5G networks, achieving deep integration of 5G technology with industrial production networks and driving the digital transformation of industries. The implementation of agile project management is not only a reflection of technological progress for Group A, but also a practice of managerial innovation. This managerial approach allows businesses to respond quickly to customer needs, increase competitiveness in the market, and provide higher operational efficiency and a better customer service experience. Against the backdrop of rapid globalization and the development of information technology, the challenges faced by projects are becoming increasingly complex, including technological innovations, fluctuating market demand, and increased competitive pressures.

These factors require project management to be extremely flexible and adaptable to respond quickly to changes in the external environment. Learning agile project management is of considerable importance. It not only helps project managers to deeply understand the essence of project management, but also increases the overall effectiveness of project management by implementing more flexible and innovative management methods. In addition, agile project management can help businesses deal with uncertainties effectively, reduce the risk of project failure, and thus ensure the continuous development and competitiveness of businesses in the market. Despite the significant benefits of agile project management, there are also a number of challenges and challenges in the implementation process, such as how to build an appropriate agile project management structure, how to formulate and execute effective agile project management plans, and how to evaluate and monitor project flexibility, which requires further in-depth research and discussion.

Therefore, this work is dedicated to exploring agile project management techniques, proposing appropriate implementation strategies and suggestions for improvement, hoping to bring new perspectives and value to the field of project management. These practices not only increase the efficiency of internal cooperation, but also increase the speed of market response and innovation opportunities. By breaking down organizational barriers, reducing internal friction and giving more decision-making authority to the grassroots level, the group has significantly increased the speed of market response and the level of customer service. At the same time, by strengthening R&D and data analytics capabilities, the group can better understand market trends and customer needs, providing reliable data support for innovative work and contributing to continuous business optimization and modernization. In addition, the implementation of agile project management also

includes several dimensions, including the platformization of business management, the integration of marketing models, and the optimization of resource allocation. With the help of information technology, a business management platform was created, which ensures the distribution of values and optimization of management processes. The integrated marketing model is customer-centric and has established a differentiated competitive strategy. Resource allocation optimization focuses on realizing value for the customer, adjusting resource allocation across different business links, implementing a marketing layout, and achieving high-quality development. The main activities to build an agile organization by Group A include the establishment of a project management office, the establishment of a project management committee, the formation of joint project teams, the implementation of a system of responsibility for project managers and the clarification of the mechanism for the distribution of project revenues. These activities aim to concentrate group resources to support the initiation, organization and execution of internal projects, while strengthening the interaction and strategically oriented cooperation of senior management, facilitating and coordinating the support and contribution of resources for project operations by related parties.

The proposed measures for building an agile organization include agile management transformation, the development and implementation of mechanisms for the operation of an agile organization, the improvement of the rotation of senior management positions, and the agile management and development of talent. These activities aim to increase leadership flexibility and responsiveness, stimulate employee initiative and creativity, eliminate organizational rigidity, and improve team flexibility and collaboration. Through these measures, Group A has not only achieved significant results in agile project management, but has also provided valuable experience and knowledge to other state-owned enterprises. In-depth research and practice of agile project management are of great theoretical and practical importance for increasing the market competitiveness of enterprises, promoting the digital transformation of industries and achieving sustainable economic development.

References

1. Sarimah. Human Relationship Management to Enhance Organizational Performance through Effective Communication and Team Collaboration / Sarimah, Fauziah Hayati Fazrin, Tisatun, Efrita Norman // MES Management Journal, 3(3). – 2024. – p. 685 –696.
2. Chub O.P. The concept of lean production for flexible production systems, the concept of flexibility / O. P. Chub // Eurasian Scientific Association. – 2019. – № 3–2(49). – p. 135–141.
3. Redmine Project Management Tool [Electronic resource] – Access mode : <https://www.redmine.org/>

Skorin Yuriy

PhD, Associate Professor

Simon Kuznets Kharkiv National University of Economics

Zhao Lina

student of higher education

Simon Kuznets Kharkiv National University of Economics

AGILE PROJECT MANAGEMENT METHODS BASED ON THE SCRUM METHOD

It is emphasized that the present requires a significant increase in the efficiency of software for IT projects. The analysis showed that agile software development methods have now taken a key place in IT projects. Obstacles to flexible transformation, which mainly concern small and medium-sized enterprises, are considered.

The purpose of the study is defined, namely, to promote the successful implementation of agile project management based on the Scrum method, to study the integration of agile methods into OPI's management processes to promote the formation of an agile organizational culture at all levels, to check the effectiveness of OPI's agile processes of organization and development in adapting to changes in the external environment and optimizing project management processes. A generalization of the experience of implementing flexible transformation for other similar enterprises is carried out.

With the continuous development of information technology, the frequency of iterations of requirements during software development for IT projects has increased significantly. Agile software development has taken a key place in the IT projects of large enterprises, but some small and medium-sized enterprises have faced obstacles to agile transformation without meeting expectations. OPI is a high-tech enterprise controlled by a state-owned enterprise specializing in water informatization and intelligent solutions, 70% of whose revenues come from IT projects, faced the problem of low efficiency of IT projects due to changes in external conditions. In this regard, senior management was forced to plan the implementation of an agile development methodology in the project management process in the software development department.

It is assumed that the study may use a case-based method that tracks, analyzes, and summarizes the process of implementing agile project management by implementing the Scrum method in OPI's software department, including the study of internal company data and interviews with management and project team members.

It is expected that through this research, OPI will be able to successfully apply the Scrum method for project management in the software development department, solve the problem of inefficient implementation of IT projects, and create an agile organizational culture in the company. The project management process will be continuously improved, allowing the company to release better software products,

provide more value to customers, and increase customer satisfaction. In addition, the generalized experience of implementation can serve as an example for other enterprises undergoing a similar agile transformation.

In the context of Ukraine's accelerated digital transformation and industrial modernization, the deep penetration of information technologies is constantly driving intelligent demand in the water sector, creating a wide market space for local software enterprises. The Government of Ukraine has clearly identified water informatization as a priority area of development through policy documents such as the National Digital Transformation Strategy (2020-2024) and the Water Development Vision (2020-2030), promoting technological modernization in the industry through measures such as tax incentives and special funds.

Currently, the latest technologies such as big data and cloud computing, which have mature applications in smart transportation and energy management, are accelerating their penetration into the water management industry, stimulating the intelligent modernization of traditional water management facilities [1]. As a high-tech enterprise [2] in Ukraine, OPI uses a matrix organizational structure, where its software development department is the main unit responsible for comprehensive management from requirements analysis to system delivery. Its Technology Management Center includes agile development teams, a data analysis lab, and a quality assurance department, forming a closed-loop "requirements-development-validation" management system.

Guided by national policies and industry requirements, OPI continues to enhance its core competitiveness through agile transformation [4]. Its "business technology two-way iteration" model, developed on the basis of the SCRUM framework, was validated within the framework of the Smart Water project in the Chernivtsi region, improving the speed of response to demand by 50% and reducing the cost of eliminating defects by 35%. In the future, OPI plans to expand its business into advanced industries such as digital twin water conservation centers and AI-based decision-making, helping Ukraine achieve rapid development from "traditional water conservation" to "smart water conservation".

Among various flexible approaches, the SCRUM method is the most popular, widely used by large Internet and software companies. However, it should be noted that there is a significant phenomenon of misuse of agile methods, as many businesses misinterpret agility as simply "speed" rather than acknowledging that, like all standard development processes, its ultimate goal is to make development manageable and ensure project success [5]. An agile organization based on SCRUM effectively solves structural problems in OPI's software projects.

The new agile structure emphasizes continuous improvement, where team capabilities, culture, and overall quality evolve throughout the project. Replacing the cascade lifecycle with an agile process (iterative development, incremental delivery) allows for faster delivery of high-quality products, shortens turnaround times, and significantly increases customer satisfaction.

The successful implementation of the OPI agile model offers the following important takeaways: Pilot project selection: Choose the first agile project based on four criteria: relevant importance, sufficient visibility, manageable scale and

measurable results; Transition Management: Building an agile transformation team to support process change, ensure seamless implementation, and align with the organization's goals.

Future research and practical use of the case project are expected. While this case study confirms the effectiveness of agile methodologies (driven by senior management and the Change Committee), the implementation of agile methodology as the core management culture requires further efforts.

The following key areas for research can be highlighted: agile knowledge domains: deepening research on scope, quality, risk and performance management within SCRUM, integrating the fundamentals of the Project Management Body of Knowledge (PMBOK) to develop agile-specific knowledge areas, which will allow the use of agile practices for large and complex projects; agile application management: For large projects consisting of several sub-projects, multi-team SCRUM collaboration should be explored.

Because agile methodology emphasizes small, focused teams, OPI should learn how to coordinate multiple SCRUM teams to implement complex programs, maximizing the value of agile methodology at scale. Thus, this research lays the foundation for the agile transformation of OPI, but continuous improvement and expansion of agile practices will be essential to support improvements and adapt to changing project requirements.

References

1. Abrahamsson P. Agile Software Development Methods: Review and Analysis / P. Abrahamsson, O. Salo, J. Ronkainen, et al. // 2017. [Electronic resource]. – Access mode: <https://doi.org/10.48550/arXiv.1709.08439> .
2. Bardsiri V. K. A Flexible Method to Estimate the Software Development Effort Based on the Classification of Projects and Localization of Comparisons / V. K. Bardsiri, D. N. A. Jawawi, S. Z. M. Hashim, et al. // Empirical Software Engineering 2014 19(4): 857-884. [Electronic resource]. – Access mode: <https://doi.org/10.1007/s10664-013-9241-4> .
3. Beecham S. Software Process Improvement Problems in Twelve Software Companies: An Empirical Analysis / S. Beecham, T. Hall, A. Rainer, et al. // Empirical Software Engineering 2003 8(1): 7-42. [Electronic resource]. – Access mode: <https://doi.org/10.1023/A:1021764731148> .
4. Bjarnason E. Requirements Are Slipping Through the Gaps – A Case Study on Causes & Effects of Communication Gaps in Large-Scale Software Development / E. Bjarnason, K. Wnuk, B. Regnell // IEEE Computer Society 2011. [Electronic resource]. – Access mode: <https://doi.org/10.1109/RE.2011.6051639> .

*Skorin Yuriy**PhD, Associate Professor**Simon Kuznets Kharkiv National University of Economics**Zhu Zhongbiao**student of higher education**Simon Kuznets Kharkiv National University of Economics*

IMPLEMENTATION OF THE VORONYI DIAGRAM METHOD

The existing areas of application of the Voronoi diagram were considered, it was determined that these diagrams are used in quite a few fields, such as cartography, architecture, biochemistry, etc. The task of implementing this method was formed. Based on the results of the study of the subject environment, a list of tasks that were solved to achieve the goal was determined. A detailed analysis of the subject area was carried out, during which the requirements for input and output data were formed and described. Based on the analysis, an object-oriented model is built. On the basis of the data obtained in the process of analysis, the corresponding mathematical methods for constructing Voronoi diagrams have been formulated. Based on the results of object-oriented design, the tools for the software implementation of the automated system were chosen. Hardware and software requirements are formulated. A user manual for a software product has been developed, which was developed within the framework of the conducted research.

The development of modern technologies leads to more and more automation of processes performed by humans in various spheres of life, in particular such as education, medicine, industry, agriculture, etc. These tasks either cannot be solved by simple methods, or their solution will require a significant amount of time and resources. To solve this kind of problem, there are special methods and algorithms.

The Voronoi diagram is an important tool in solving so many problems. In general, a Voronoi diagram is a plane partition in which each region of the partition forms a set of points that are closer to one of the elements of the set than to any other element of the set.

Sampling an area using Voronoi cells provides a quick search for natural neighbors for a given point. Finding natural neighbors based on information about neighboring nodes derived from the Voronoi diagram significantly reduces the time it takes to construct interpolated functions.

Voronoi diagrams allow you to visualize complex data, making it easier to understand and analyze. Voronoi diagrams can be used to identify implicit structures and patterns in data, which is essential for making informed decisions. Voronoi diagrams are used to solve optimization problems, for example, to determine the optimal location of objects in space.

Voronoi diagrams: help determine the optimal location of stores to minimize competition and maximize profits; are used to plan the location of public facilities such as schools, hospitals, etc.; help determine the optimal location of base stations to

ensure maximum coverage when solving the issue of optimizing wireless networks. Versatility, intuitive visualization, and the ability to detect hidden patterns make Voronoi diagrams an indispensable tool for analyzing data and making informed decisions. Based on the above, the purpose of the study was formulated, namely, the software implementation of the system for searching for the nearest elements by the method of constructing a Voronov diagram.

At present, there is a wide variety of algorithms specifically for solving problems of computational geometry. However, the scope of such algorithms is usually very narrow. For example, the well-known algorithms for constructing a Voronoi diagram can be effectively applied only to points or segments. But when solving practical problems, you usually have to deal with more complex geometric objects, which can be defined as points and segments, as well as curves of arbitrary shape. Building a Voronoi diagram for such geometric objects is a non-trivial task, and therefore the study of Voronoi diagrams is reduced to the study of their approximations [1].

A Voronoi diagram is a mathematical object that is not described strictly in this way. A Voronoi diagram of a given finite set of points M of a plane (space) is a partition in which each region (Voronoi cell) of a given partition forms such a set of points that is located closer to one of the elements of the set M than to any other element of this set [2]. The purpose of the software implementation of the Voronoi diagram method is to provide a quick search for natural neighbors for a given point. The search for natural neighbors derived from the Voronoi diagram greatly reduces the time it takes to construct functions.

To achieve the goal, the following was performed: analysis of the subject area; select the main input and output objects; analyze the limitations of the system; choose the necessary algorithm; specify external storage; display the designation on the sheet.

During the research, the existing areas of application of the Voronoi diagram were considered and it was found that today these diagrams are used in many fields, such as cartography, biochemistry and architecture. The method of constructing the Voronoi diagram is used in many fields, so the task of implementing this method has been formed. The purpose and objectives of the diploma project are formulated, the object and subject of research are determined. Based on the results of the study of the subject environment, a list of tasks that were solved to achieve the goal was determined. A detailed analysis of the subject area was carried out, during which the requirements for input and output data were formed and described. Based on the analysis, an object-oriented model is built. On the basis of the data obtained in the process of analysis, the corresponding mathematical methods for constructing Voronoi diagrams have been formulated.

To implement the methods of system classes, the following algorithms were built: an algorithm for calculating the area; algorithm for independent location of points; algorithm for uploading data to a file; Algorithm for editing points. Based on the results of object-oriented design, the tools for the software implementation of the automated system were chosen. As a programming language in the Visual Studio Code development environment, a formalized programming language, namely, C#,

was chosen. On the basis of the object-oriented model, a software product was created, which is implemented in accordance with the principles of object-oriented programming and consists of ten classes.

Hardware and software requirements are formulated. A user manual has been developed for a software product that has been developed within the framework of these studies. The instructions describe the user's capabilities when working with the software product, reveal the purpose of windows and commands, and also provide forms corresponding to the screen.

References

1. Mark de Berg. Computational Geometry: Algorithms and Applications / de Berg Mark, Cheong Otfried, van Kreveld Marc, Overmars Mark // Springer, 2008. – 398 p.
2. Satyan L. Devadoss. Discrete and Computational Geometry / L. Devadoss Satyan, O'Rourke Joseph // Princeton University Press, 2011. – 272 p.
3. Kenneth E. Kendall. Systems Analysis and Design, Global Edition / E. Kendall Kenneth, E Kendall Julie // Pearson Education, 2019. – 578 p.
4. Hector Uriel Perez Rojas, Angel Teheran Garcia. Hands-On Visual Studio 2022: A developer's guide to new features and best practices with .NET 8 and VS 2022 for maximum productivity / Uriel Perez Rojas Hector, Angel Teheran Garcia Miguel // Packt Publishing, 2024. – 336 p.
5. Joseph Albahari. C# 9.0 in a Nutshell: The Definitive Reference / Albahari Joseph // O'Reilly Media, 2021. – 1058 p.
6. Beecham S. Software Process Improvement Problems in Twelve Software Companies: An Empirical Analysis / S. Beecham, T. Hall, A. Rainer, et al. // Empirical Software Engineering 2003 8(1): 7-42. [Electronic resource]. – Access mode : <https://doi.org/10.1023/A:1021764731148> .
7. Bjarnason E. Requirements Are Slipping Through the Gaps – A Case Study on Causes & Effects of Communication Gaps in Large-Scale Software Development / E. Bjarnason, K. Wnuk, B. Regnell // IEEE Computer Society 2011. [Electronic resource]. – Access mode : <https://doi.org/10.1109/RE.2011.6051639> .
8. Bardsiri V. K. A Flexible Method to Estimate the Software Development Effort Based on the Classification of Projects and Localization of Comparisons / V. K. Bardsiri, D. N. A. Jawawi, S. Z. M. Hashim, et al. // Empirical Software Engineering 2014 19(4): 857-884. [Electronic resource]. – Access mode : <https://doi.org/10.1007/s10664-013-9241-4> .

*Timokhin Mikhail,
IB DP2 Student,
International School Premjers, Riga, Latvia*

THE ROLE OF ARTIFICIAL INTELLIGENCE IN BUSINESS DECISION MAKING

1. Introduction

Artificial Intelligence (AI) is rapidly changing how businesses gather insights and make operational choices. Yet AI is not a “magic button” for managerial judgment: it amplifies data-driven clarity while introducing new risks (bias, privacy, over-reliance). This paper argues that AI is best understood as a decision-support tool that improves forecasting and personalization when strongly governed by human oversight. I demonstrate this through three targeted case studies (e-commerce, aviation, and a manufacturing firm), and then discuss practical risks, mitigations, and governance steps for young entrepreneurs.

2. AI as a Tool for Business Decisions

AI accelerates pattern detection and converts patterns into operational recommendations. The managerial task is to identify which recommendations should be actioned automatically and which require a personal review. Successful adoption depends on defining the decision problem, setting measurable success criteria, and retaining human oversight at key thresholds.

Case studies:

Amazon - demand forecasting and logistics

Context: Amazon applies machine learning to predict customer demand and to determine optimal inventory placement and routing across distribution networks. Recent announcements describe 'agentic' AI developments that enable robots to understand natural language commands and act more flexibly in warehouses. “We’re creating systems that can hear, understand and act on natural language commands, turning warehouse robots into flexible, multi-talented assistants,” Amazon said in a statement. Decision impact: Replenishment and routing decisions move from periodic rules to near real-time, data driven adjustments. Implication: Managers must monitor model inputs and configure human review for unexpected events, such as sudden demand shifts or supply disruptions.

airBaltic - dynamic ancillary pricing

Context: airBaltic implemented an AI-based dynamic ancillary pricing solution using segmentation and demand signals to set prices (PROS, 2024; airBaltic, 2024). Decision impact: Pricing choices that were once fixed or manual are now adjusted continuously to market conditions; early reports indicated a 6% increase in ancillary-sourced revenue per passenger after implementation (PROS, 2024). Implication: Revenue managers gain short-term revenue flexibility but must add oversight to prevent pricing that harms customer trust.

Printful (Riga) - automated quality checks for file uploads

Context: Printful uses machine learning to flag image and file issues before printing. According to company materials, a Printful employee can manually check up to 10,000 files per month whereas an ML tool can process the same amount of files in 2 to 4.5 minutes. Decision impact: Quality control shifts from manual inspection to automated pre-fulfillment checks, allowing staff to focus on exceptions. Implication: Small and medium enterprises can scale operations without large increases in headcount, provided they establish clear procedures for handling model flagged exceptions. “We have to make sure our customers get quality products, and with the help of machine learning, we can help thousands of customers by improving their experience every day. We wouldn't be able to do that just by ourselves,” says Janis Akmentins, Head of Engineering at Printful.

4. Challenges and Risks

Bias and errors: Models reflect the data they are trained on. Managers should require dataset audits and periodic bias testing to limit unfair outcomes. Mitigation: implement fairness checks and diverse data sampling.

Ethics and privacy: Data collection can erode customer trust if it is not transparent. Mitigation: apply data minimization, clear consent, and publish brief privacy summaries for users.

Impact on jobs: Automation replaces some routine tasks while creating demand for new skills. Mitigation: plan for retraining and create roles for oversight and model management.

Dependence: Over reliance on algorithmic recommendations can reduce strategic flexibility. Mitigation: require human approval for high impact decisions and maintain scenario based drills to test resilience.

7. Conclusion

AI delivers operational gains when it addresses a clearly defined decision problem and when managers pair model outputs with human judgment. The value of AI comes from measurable decision improvements, not from technology for its own sake. For students and future entrepreneurs, the immediate steps are to build data literacy, experiment with a small project that answers a specific question, and always evaluate AI outputs critically before acting on them.

References

1. Reuters. (2025). Reporting on Amazon's agentic AI and logistics investments.
2. Amazon. (2025). Company press release on warehouse AI initiatives.
3. PROS. (2024). Case study: Dynamic Ancillary Pricing results with airBaltic.
4. airBaltic. (2024). Company statement on revenue impact from pricing solution.
5. Printful. (2020). Blog post on automated file quality checks.
6. Marr, B. (2018). Artificial Intelligence in Practice: How 50 Successful Companies Used AI to Solve Problems. Wiley.

Torianykh Zh.

*PhD in Economics, Associate Professor
Department of Management, Accounting and Business Communications
REI «Karazin Banking Institute» V.N. Karazin KhNU*

Topalova S.

*PhD in Political Sciences, Associate Professor,
Department of Management, Accounting and Business Communications
REI «Karazin Banking Institute» V.N. Karazin KhNU*

Shevchenko V.

*PhD in Philology, Associate Professor
Department of Management, Accounting and Business Communications
REI «Karazin Banking Institute» V.N. Karazin KhNU*

Kraievyi N.

*the applicant of higher education
REI «Karazin Banking Institute» V.N. Karazina KhNU*

THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES AT THE STAGES OF FORMING THE BANK'S MARKETING STRATEGY

In today's conditions of rapid changes, the role of marketing is constantly being transformed. One of the most important vectors of this transformation is the concept of «Marketing 5.0», which reflects new challenges and opportunities for business in a dynamic environment. Artificial intelligence (AI) becomes the central tool for the successful implementation of this concept, because it does not only ensure adaptability to changes, but also opens qualitatively new approaches to the organization of effective marketing.

For banking institutions, the development of marketing strategies acquires an innovative content precisely due to the use of AI. Today, these technologies are used at all stages of strategy formation: from in-depth market analysis and the study of target customer segments to the introduction of personalized communication channels, which allows financial institutions not only to be more aware of consumer needs, but also to predict their future expectations, forming individual offers and services. Therefore, the integration of artificial intelligence into marketing activities becomes a decisive factor in the competitive success of banks in the modern financial industry.

According to the concept of F. Kotler, the marketing management process involves a number of stages: market research (including analysis of the macro and micro environment, prediction and assessment of the demand), identification and segmentation of the target audience, formation of the 4P marketing complex (product, price, sales channels, promotion) and implementation of planned activities [1].

The use of innovative tools, in particular artificial intelligence technologies, significantly expands the capabilities of companies in the field of marketing management. Thanks to these technologies, it becomes possible to quickly collect and

systematize information, deeply analyze data and obtain practical recommendations to increase the effectiveness of marketing solutions.

The use of innovative tools, in particular artificial intelligence technologies, significantly expands the capabilities of companies in the field of marketing management. Due to these technologies, it becomes possible to collect quickly and systematize information, analyze data deeply and obtain practical recommendations to increase the effectiveness of marketing solutions.

Table 1 presents artificial intelligence tools, ordered by the possibility of their application at different stages of the creation of a marketing strategy [2–3].

Table 1

Artificial intelligence tools in the formation of a marketing strategy

Directions	Tools	Advantages and disadvantages
Stage 1. Market research		
Competitor Analysis	Unmetric Analyze Xia is a platform from Unmetric that uses artificial intelligence and machine learning methods to analyze the activity of competitors in social networks. It provides data on content, advertising campaigns and their effectiveness, which allows you to assess the success of competitors and their impact on sales volumes.	Advantages: it enables marketers to adjust their strategy based on competitor activity. Disadvantages: the analysis is limited only to social networks, not including other channels; high cost – about \$1000 per month.
Factor analysis of micro-macro environment	NetBase Quid is a platform for tracking changes in consumer behavior and analyzing market trends.	Advantages: it helps shape strategy by providing data on customer preferences and antipathies. Disadvantages: it does not take into account competitors missing from the database, which reduces efficiency for marketing planning of businesses with a limited or local market.
	Pathmatics is a marketing analytics platform that uses artificial intelligence to evaluate the effectiveness of competitors' ads, their advertising channels and budgets.	Advantages: it allows marketers to receive data on the advertising activity of competitors, which helps to make reasonable decisions. Disadvantages: high price – about \$10,000 per year
Stage 2. Definition of target market segments		
Target market segmentation and definition	Crayon Market IQ is an artificial intelligence-based platform that identifies potential customers who meet certain criteria and show interest in a certain product online.	Advantages: it helps marketers identify and segment their target audience to make effective decisions. Disadvantages: significant costs; orientation mainly to the B2B segment.
Stage 3. Development of a 4P marketing strategy		
Analysis and prediction of customer actions and behavior	Optimove is a SaaS platform that applies machine learning to analyze customer behavior in order to optimize marketing strategies and increase customer value.	Advantages: it enables marketers to adjust the marketing plan by predicting customer behavior. Disadvantages: high cost – from \$4000 per month per user.
Building a personal content strategy	Uberflip is a platform that analyzes the behavior of each user on the site and offers personalized content and	Advantages: it helps optimize content strategy with personalized recommendations.

	dynamic recommendations to increase engagement and stimulate shopping.	Disadvantages: limited work with content only; high price – from \$1,200 per month.
Development of content strategy	Cortex is SaaS a platform based on artificial intelligence, which evaluates the content of the company and competitors and provides recommendations for its improvement.	Advantages: it allows you to improve the content and marketing plan thanks to the recommendations; trial version is available. Disadvantages: recommendations are limited only by content strategy.
Selection of platforms for advertising	GumGum is a platform based on artificial intelligence (computer vision), which analyzes images and content of pages and offers optimal sites for placing media advertising.	Advantage: it allows marketers to adjust the marketing plan based on recommendations for choosing advertising platforms. Disadvantage: limited functionality – the choice of sites has a less impact on performance than the quality of advertising or price changes.
Stage 4. Implementation of marketing actions and projects		
Monitoring and evaluation of the results of the marketing and promotion strategy	Terminus (Emarsys) – the platforms on which artificial intelligence monitors the effectiveness of marketing strategies on all promotion channels. They visualize the customer journey, optimize sales funnels and provide predictive analytics.	Advantage: it allows marketers to improve the strategy based on data about its performance. Disadvantage: it evaluates only the campaigns launched, without eliminating the potential loss of time and budget during the planning phase.

Thus, the introduction of digital technologies in the banking sector can significantly increase the efficiency of marketing activities. In particular, banks get the opportunity to analyze large ranges of client data, study behavioral models and reactions to advertising messages. It allows to orient marketing efforts, reduce costs, increase the effectiveness of advertising campaigns, as well as to form personalized offers and recommendations in order to increase the level of customer satisfaction. In addition, the use of AI contributes to the automation of request processing, provides quick answers through chatbots and virtual assistants. It improves the client experience and provides prompt service.

References

1. Osnovy marketynh. Hari Armstronh, Filip Kotler. Naukovyi svit. 2022. 880 s. URL: <https://kniga.biz.ua/ua/book-osnovi-marketingu-0032147.html>
2. Shumilo Ya. Instrumenty shchuchnoho intelektu dlia upravlinnia povedinkoiu ekonomichnykh ahentiv v marketynhovii diialnosti. Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina. 2022. №15. S. 60-66. DOI: 10.26565/2310-9513-2022-15-07
3. Serhieieva O. S. Suchasni didzhytal instrumenty yak marketynhova stratehiia bankiv. Problemy suchasnykh transformatsii. Seriia: ekonomika ta upravlinnia. 2023. №8. doi: <https://doi.org/10.54929/2786-5738-2023-8-08-01>

Афанасьєв А.С.

*Аспірант кафедри Інформатики,
Харківський національний університет радіоелектроніки
Academic Advisors*

Вечірська І.Д.

*Кандидат технічних наук, доцент, кафедра Інформатики
Харківський національний університет радіоелектроніки*

Кобилін О.А.

*Кандидат технічних наук, доцент, завідувач кафедри Інформатики,
Харківський національний університет радіоелектроніки*

АНАЛІЗ ВПЛИВУ ЯКОСТІ ВЕКТОРИЗАЦІЇ НА ТОЧНІСТЬ КЛАСИФІКАЦІЇ ТЕКСТІВ

Завдання автоматичної класифікації текстів є однією з ключових проблем у сфері обробки природної мови (NLP). Незважаючи на наявність великої кількості архітектур нейронних мереж, результативність моделі значною мірою визначається не лише її структурою, а й способом представлення вхідних даних. Зокрема, якість векторного подання тексту прямо впливає на здатність моделі виявляти семантичні зв'язки та граматичні конструкції, що мають значення для класифікації [1].

У рамках дисертаційного дослідження було окремо виділено блок, присвячений аналізу методів векторизації, з метою оцінити їхній вплив на остаточну точність класифікаційних моделей.

Текстова інформація є складною, контекстуально змінною та багатовимірною. Для її опрацювання необхідно здійснити перетворення тексту у числовий формат, придатний для обробки машинними алгоритмами. При цьому важливо не втратити змістовні характеристики тексту, такі як значення слів у контексті, лексичні зв'язки, порядок слів тощо.

Класичні методи, як-от Bag-of-Words (BoW) та TF-IDF, хоча й прості у реалізації, не враховують семантику або контекст [2]. Сучасні підходи до векторизації, зокрема Word2Vec, GloVe, FastText, а також контекстуальні ембеддинги на основі трансформерів (BERT, RoBERTa тощо), дозволяють значно точніше відтворювати значення слів у їх природному оточенні.

У дослідженні було поставлено завдання: виявити, наскільки саме метод векторизації впливає на кінцеву точність класифікації текстів, і як змінюється продуктивність нейронної мережі при використанні різних векторних подань. Для проведення експериментів було відібрано декілька популярних способів векторизації тексту:

- TF-IDF – класичний статистичний підхід, що враховує частоту терміну в документі та його рідкість у корпусі.
- Word2Vec – модель, що дозволяє отримувати щільні векторні представлення слів на основі їх оточення.

- GloVe – модель, яка поєднує статистику глобального співживання слів з локальними контекстами.
- FastText – розширення Word2Vec, що враховує морфологію слів шляхом розбиття на n-грам.
- BERT embeddings – контекстуалізоване подання, що базується на глибокій трансформерній архітектурі.

Для кожного типу векторизації були побудовані моделі на основі таких нейромереж:

- Прості послідовні LSTM-моделі;
- CNN для текстової класифікації;
- Fine-tuned BERT з власним класифікатором.

Використано відкриті датасети: IMDb (відгуки на фільми), AG News (класифікація новин), а також спеціально сформований українськомовний корпус текстів.

Оцінювання проводилось за такими метриками: Ассурасу (точність), Precision, Recall, F1-score.

Аналіз отриманих результатів дозволив зробити кілька важливих висновків:

- TF-IDF показав стабільну, але обмежену ефективність, особливо при використанні із простими логістичними класифікаторами чи SVM. При переході до LSTM модель не здатна використовувати порядок слів, бо TF-IDF його не зберігає.
- Word2Vec та GloVe забезпечили суттєво кращу якість класифікації, особливо в комбінації з BiLSTM. Вони дають змогу вловити подібність між словами, навіть якщо вони не однакові за написанням.
- FastText виявився ефективним для текстів із великою кількістю морфологічних варіантів, зокрема українською мовою. Це свідчить про важливість урахування внутрішньої структури слова.
- BERT embeddings продемонстрували найвищу точність класифікації на всіх датасетах. Особливо значна перевага спостерігалася у випадках, коли текст містив багатозначні або полісемічні слова. У порівнянні з Word2Vec, BERT більш гнучкий до контексту.
- Було виявлено, що навіть при використанні однієї і тієї ж нейромережі, зміна способу векторизації може змінити кінцеву точність на 10–25%, залежно від складності завдання.

Якість векторизації тексту відіграє критично важливу роль у побудові ефективних моделей класифікації [3]. Сучасні підходи до векторного подання, особливо контекстуалізовані embeddings, здатні суттєво покращити результати, особливо у складних або багатомовних задачах.

У рамках дисертаційної роботи ці результати були використані як основа для побудови кастомної нейромережевої архітектури, що адаптується під різні типи текстових подань. У подальших дослідженнях планується вивчити ефективність мультимовних моделей (наприклад, XLM-R) та впровадити техніки динамічного вибору векторизації залежно від жанру та мови тексту.

Список використаних джерел:

1. D. Jurafsky, J. H. Martin. Speech and Language Processing (3rd ed.). Draft available online // 2021. Available at: <https://web.stanford.edu/~jurafsky/slp3/>
2. C. D. Manning, P. Raghavan, H. Schütze. Introduction to Information Retrieval // Cambridge University Press, 2008. 482 p.
3. D. A. Haisal, U. Mahmood. Sentiment Classification: Review of Text Vectorization Methods: Bag of Words, Tf-Idf, Word2vec and Doc2vec // SLU Journal of Science and Technology, 2022. 27–33 p.

УДК 004.89 : 004.738.5 : 658.8

Бур'ян С. С.

здобувач вищої освіти

другого (магістерського) рівня,

Державний податковий університет

Науковий керівник

Погорєловська І. Д.

к.е.н., доцент, доцент кафедри

комп'ютерних та інформаційних технологій і систем

Державний податковий університет

м.Ірпінь, Україна

TELEGRAM-БОТ ЯК ІНСТРУМЕНТ СПРОЩЕННЯ КОМУНІКАЦІЇ ЗІ СЛУЖБОЮ ПІДТРИМКИ

Історія розвитку технічної підтримки тісно пов'язана з еволюцією інформаційних технологій. У 1980–1990-х роках основним каналом комунікації користувачів із технічними спеціалістами був телефон. Усі інциденти фіксувалися у паперових журналах або простих електронних таблицях. Відсутність єдиної централізованої системи робила неможливим аналіз навантаження, а виконання SLA (Service Level Agreement) мало здебільшого декларативний характер [1]. Пізніше, із поширенням електронної пошти, з'явилась можливість документувати звернення, але листування часто було неструктурованим, що ускладнювало класифікацію й контроль за виконанням завдань.

На початку 2000-х років компанії почали впроваджувати перші спеціалізовані системи Service Desk. Вони дозволяли створювати електронні тікети, контролювати строки реагування й формувати базові звіти [4]. Проте їхнім недоліком була складність інтерфейсів: користувачам доводилось витрачати час на навчання, а значна частина інцидентів так і залишалась «поза системою». У цей час набули поширення стандарти ITIL, які задали рамки для організації процесів підтримки, зокрема Incident Management, Request Fulfillment та Problem Management [10]. Саме ITIL започаткував підхід, де

технічна підтримка сприймається не як допоміжний процес, а як важливий елемент бізнес-континуїтету.

Сьогодні, в епоху цифрової трансформації, ключовим трендом стає використання звичних каналів комунікації для взаємодії користувачів із техпідтримкою. Telegram як популярний месенджер із відкритим API надає широкі можливості для інтеграції з корпоративними системами. Запропонований у межах дослідження Telegram-бот став прикладом того, як можна поєднати простоту для користувача і функціональність для IT-відділу.

Механізм взаємодії є наступним: користувач вводить опис проблеми в Telegram, додає файл або скріншот, і бот автоматично передає цю інформацію у Jira Service Desk через REST API. У системі створюється заявка із зазначенням категорії, пріоритету та відповідального виконавця. Користувач одразу отримує номер тікета та подальші повідомлення про зміну статусу. На серверному рівні інтеграція реалізована за допомогою Python і FastAPI, що забезпечує високу швидкодію та надійність. Усі звернення фіксуються в базі даних PostgreSQL, що дозволяє накопичувати історію інцидентів і здійснювати глибокий аналіз [5; 7].

Інтеграція Telegram-бота із Jira відповідає кільком ITIL-практикам. По-перше, у рамках Incident Management зменшується середній час реагування: бот одразу структурує дані та зменшує кількість уточнюючих запитань. По-друге, у сфері Request Fulfillment реалізується стандартизація типових звернень, наприклад відновлення доступу чи створення нового акаунта. По-третє, у Continual Service Improvement з'являється можливість аналізувати метрики (час першої відповіді, кількість повторних інцидентів, середню тривалість виконання) і робити висновки щодо підвищення якості сервісу [10].

Важливо, що розробка подібних систем не обмежується лише зручністю для користувачів. Вони також інтегруються з іншими елементами IT-інфраструктури. Наприклад, системи моніторингу Zabbix та Grafana можуть автоматично відправляти повідомлення про критичні збої у Telegram-бота, який інформує відповідальних фахівців і створює заявку у Jira. Таким чином, частина інцидентів фіксується не користувачами, а автоматично – ще до того, як вони вплинуть на бізнес-процеси [6]. Крім того, інтеграція з аналітичними інструментами, такими як Power BI, дає можливість керівництву бачити реальну картину навантаження на службу підтримки та прогнозувати потреби у ресурсах.

На глобальному рівні активно розробляються рішення, які підсилюють роботу ботів за допомогою штучного інтелекту. Сучасні NLP-моделі вже дозволяють чат-ботам розуміти запити у вільній формі та автоматично пропонувати відповіді з бази знань [8]. У перспективі такі системи зможуть навчатися на історії звернень, будувати прогностичні моделі та самостійно вирішувати типові інциденти. Наприклад, бот зможе одразу генерувати інструкцію з вирішення проблеми або застосовувати автоматичні сценарії: перезапускати службу, скинути паролі, перевіряти доступність серверів. Це вже приклади переходу від реактивної підтримки до предиктивної.

Ще однією перспективою є омніканальність. Telegram-бот стане частиною ширшої системи, де користувачі зможуть обирати між месенджером, мобільним

додатком, голосовим асистентом або корпоративним порталом, а всі звернення все одно будуть уніфіковано оброблятися в Jira. Таким чином, компанії отримають єдиний сервісний простір, що значно підвищує ефективність комунікації.

У найближчому майбутньому поєднання таких інструментів із технологіями штучного інтелекту може привести до створення «розумної» підтримки (smart support), здатної не лише реагувати на інциденти, а й передбачати їх. Наприклад, на основі даних моніторингу система може прогнозувати, коли сервер перевантажиться, та заздалегідь створювати заявку у Jira, інформуючи IT-відділ через Telegram-бот. Таким чином, технічна підтримка поступово трансформується з реактивного процесу у стратегічний елемент управління IT-сервісами.

Отже, Telegram-бот у поєднанні з Jira Service Desk є не лише зручним інструментом комунікації, а й складовою частиною нової парадигми технічної підтримки. Він відображає еволюцію від телефонних дзвінків та паперових журналів до автоматизованих омніканальних рішень. Його впровадження відповідає стандартам ITIL, знижує навантаження на персонал, підвищує швидкість реагування та формує основу для інтеграції із сучасними інструментами моніторингу, аналітики та штучного інтелекту. У перспективі це дозволить створити систему підтримки, яка сама адаптується під потреби бізнесу, забезпечуючи стабільність, ефективність і прогнозованість роботи IT-сервісів.

Список використаних джерел

1. Василів В. Б. Практичні підходи до формування служби технічної підтримки користувачів інформаційної системи університету // Бізнес Інформ. 2018. №4. С. 371–377.
2. Горбенко Є. М. Інформаційні системи і технології в управлінні організаціями : навч. посіб. К. : Центр учбової літератури, 2020. 216 с.
3. Круглик В. С., Плечій О. О. Концепція організації інформаційної системи технічної підтримки // Інформаційні технології в освіті. 2012. №12. С. 61–66.
4. Малюта І. Системи автоматизації обробки звернень у сфері IT-послуг // Бізнес Інформ. 2021. №2. С. 101–106.
5. Муляренко О. Ю. Веб-програмування з Python і Flask : навч. посіб. Львів : ЛНУ ім. І. Франка, 2020. С. 58–59.
6. Плєскач В. Л. Інформаційні технології підтримки прийняття рішень : навч. посіб. К. : КНЕУ, 2021. 244 с.
7. Atlassian. Jira Service Management Cloud documentation. URL: <https://support.atlassian.com/jira-service-management-cloud/>
8. Jurafsky D., Martin J. H. Speech and Language Processing. Pearson, 2023. 1024 p.
9. Sharma N. Practical Security for APIs. Apress, 2020. 218 p.
10. ITIL® and IT Service Management. URL: <http://www.itil.org.uk/>

11. Sysoev A. Jira Service Management Essentials. Packt Publishing, 2022. 290 p.
12. Telegram Bot API Documentation. URL: <https://core.telegram.org/bots/api>

УДК 004.056.53

Гема О.Г.
*магістрант кафедри інформатики,
Харківський національний університет радіоелектроніки
Науковий керівник
Гороховатський В.О.
д.т.н., проф., професор кафедри Інформатики
Харківський національний університет радіоелектроніки*

КЛАСИФІКАЦІЯ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ ХЕШУВАННЯ

У сучасних системах комп'ютерного зору актуальною задачею є пошук ефективних методів класифікації зображень на основі структурного подання у вигляді множини дескрипторів ключових точок (КТ) [1-5]. Проблема полягає у тому, що дескриптори зазвичай мають високу розмірність, а тому пряме порівняння двох множин призводить до значних обчислювальних витрат. Це створює труднощі у випадках, коли потрібно працювати з великими наборами даних, наприклад у задачах розпізнавання об'єктів у потоковому відео, пошуку схожих зображень у великих бібліотеках або у сфері біометричних ідентифікаційних систем [6-8]. Високовимірні простори породжують ефект, відомий як «прокляття розмірності»: зі збільшенням кількості вимірів дані стають надто розрідженими, а традиційні алгоритми пошуку найближчих сусідів втрачають ефективність. У таких умовах надзвичайно важливим є розроблення методів, які дозволяють скоротити обчислювальні витрати без суттєвого погіршення точності класифікації.

Одним із перспективних напрямів удосконалення пошуку у великих наборах ознак є застосування локально-чутливого хешування (Locality-Sensitive Hashing, LSH) [1-3]. Цей підхід базується на ідеї побудови такої хеш-функції, яка зі збереженням високої ймовірності відображає схожі об'єкти у однакові або близькі кошики хеш-таблиці. На відміну від звичайних хеш-функцій, що прагнуть рівномірно розподілити дані у просторі, LSH акцентує увагу на близькості: схожі об'єкти зберігаються поруч, що значно спрощує подальший пошук. Це дозволяє уникати повного перебору всіх елементів бази та скорочує час оброблення запиту.

Метод випадкових проекцій, який було використано у цій роботі, є одним із найефективніших різновидів LSH для роботи з векторами ознак у високовимірних просторах [2, 3]. Його принцип ґрунтується на побудові випадкових гіперплощин, що поділяють простір на півпростори. Для кожного

дескриптора обчислюється скалярний добуток (1) із нормалізованим вектором, який є нормально розподіленим випадковим напрямом. Якщо результат добутку є додатним, то відповідний біт хешу встановлюється як «1», у протилежному випадку – як «0» (2). Таким чином, кожен дескриптор отримує бінарний код, що компактно описує його положення у просторі. Приклад хеш-ключа: 0000000011101101. Нормалізація напрямів гіперплощин до одиничної довжини гарантує, що процес хешування відображає саме кутову подібність векторів, а не їхню довжину. Це важливо, оскільки подібність між дескрипторами найчастіше визначається їхнім напрямом, а не абсолютною величиною [1, 2].

$$L_i = \sqrt{\sum_{j=1}^D (R_{ij}^{raw})^2} \quad s_i = \sum_{j=1}^D R_{ij} \cdot x_j', \quad i = 1, \dots, k, \quad (1)$$

де $R_{i,j}$ – елемент випадкової матриці проєкції R .

$$L_i = \sqrt{\sum_{j=1}^D (R_{ij}^{raw})^2} \\ b_i = \{1, s_i > 0 \mid 0, s_i \leq 0\}, \quad i = 1, \dots, k, \quad (2)$$

де $b_i - i$ – й біт хеш-коду об'єкта.

Для опису локальних ознак зображення у запропонованій реалізації використано дескриптори AKAZE [9, 10]. Цей метод побудови ознак базується на нелінійній дифузії зображення, що дає змогу краще зберігати деталі у текстурних областях і забезпечувати високу стійкість до масштабування, поворотів та змін освітлення. На відміну від дескрипторів SIFT чи SURF, які потребують значних ресурсів для обчислення, AKAZE є більш оптимізованим і дозволяє отримувати дескриптори швидше, зберігаючи при цьому високу якість інваріантності. Це особливо важливо у завданнях, де час оброблення є критичним фактором, адже AKAZE забезпечує компроміс між швидкістю та точністю. Крім того, AKAZE підтримує побудову бінарних дескрипторів, що робить їх природно сумісними з методами хешування і дозволяє зменшити обсяг пам'яті, необхідної для зберігання ознак. Таким чином, використання AKAZE створює передумови для ефективного поєднання з методами локально-чутливого хешування [3]. У нашому дослідженні дескриптори AKAZE були обчислені на зображеннях розміром 512×512 пікселів (рис. 1).

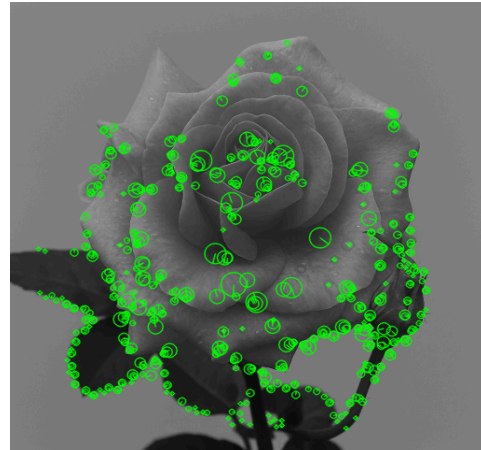


Рисунок 1 – Зображення та його координати КТ

Побудова хеш-таблиці у запропонованій реалізації відбувається шляхом групування дескрипторів за їхніми бінарними ключами. У результаті формується структура, де кожен кошик містить набір посилань на дескриптори з однаковими хешами. При пошуку подібних об'єктів замість повного перебору всієї бази відбувається звернення лише до тих кошиків, які мають співпадіння у хешах із запитом. Це дозволяє виконувати пошук кандидатів у подібності за амортизований час, близький до константи, після чого здійснюється уточнююче порівняння на основі відстані Хемінга. Така схема дозволяє досягти балансу між швидкодією та точністю і значно пришвидшує класифікацію у порівнянні з класичними методами.

Класифікація зображення у реалізованому підході відбувається за допомогою процедури голосування. Дескриптори запитного зображення послідовно хешуються і для кожного з них виконується пошук найближчого сусіда у відповідному кошику. Далі дескриптор «віддає голос» за клас знайденого об'єкта. Після того як усі дескриптори зображення оброблені, фінальне рішення приймається за правилом більшості голосів. Така схема забезпечує стійкість результатів навіть у випадку, коли частина дескрипторів потрапляє у порожні або неоднорідні кошики, оскільки остаточне рішення спирається на узагальнений результат від більшості локальних ознак.

Експериментальні результати підтвердили доцільність використання методу випадкових проекцій для задачі класифікації зображень. У порівнянні з прямим перебором за евклідовою відстанню вдалося досягти суттєвого зменшення часу оброблення при мінімальній втраті точності. Це свідчить про те, що метод є придатним для практичного застосування у системах, де одночасно важливими є як швидкодія, так і якість класифікації.

Варто також відзначити переваги поєднання AKAZE-дескрипторів із локально-чутливим хешуванням. З одного боку, AKAZE забезпечує високу стійкість до змін зовнішніх умов і дозволяє отримати компактні бінарні ознаки, що полегшують подальшу обробку. З іншого боку, LSH з випадковими проекціями створює ефективну індексаційну структуру, яка скорочує час пошуку схожих ознак. Така інтеграція дозволяє досягти балансу між точністю

та швидкодією, що робить метод привабливим для широкого спектра прикладних задач комп'ютерного зору.

У процесі дослідження для опису обсягом 500 дескрипторів час пошуку повним перебором складав 300 мілісекунд, тоді як час пошуку за допомогою LSH становив трохи більше 5 мілісекунд. Тобто LSH забезпечив майже 60-кратне прискорення у порівнянні з повним перебором, зберігаючи при цьому точність класифікації.

Серед потенційних сфер застосування можна виокремити пошук зображень у великих медіа-бібліотеках, аналіз відеопотоків у системах безпеки, ідентифікацію об'єктів у робототехніці та системах доповненої реальності. У біометричних системах метод може бути використаний для прискорення пошуку у великих базах відбитків пальців або зображень облич, де критично важливими є як швидкість, так і точність ідентифікації.

Разом з тим, слід враховувати і певні обмеження досліджуваного методу. Використання випадкових гіперплощин не гарантує абсолютної точності відображення подібності, тому у деяких випадках можливе хибне групування дескрипторів. Крім того, параметри побудови хешу, такі як кількість гіперплощин або кількість хеш-таблиць, потребують налаштування залежно від конкретних даних. Незважаючи на це, переваги у швидкодії та можливість роботи з великими наборами зображень роблять метод надзвичайно привабливим.

Таким чином, застосування локально-чутливого хешування на основі випадкових проекцій у поєднанні з AKAZE-дескрипторами дозволяє створити ефективний підхід до задачі класифікації зображень у високовимірних просторах. Отримані результати свідчать про те, що цей метод забезпечує компроміс між точністю та швидкістю, зберігає стійкість до шумів і змін умов освітлення та може бути успішно використаний у практичних системах комп'ютерного зору.

Список використаних джерел

1. Charikar, M. S. (2002). Similarity estimation techniques from rounding algorithms. In Proceedings of the thirty-fourth annual ACM symposium on Theory of computing, pp. 380-388.
2. Guo, Q. Z., Zeng, Z., Zhang, S. W., Feng, X., & Guan, H. (2014). Simhash for large scale image retrieval. Applied Mechanics and Materials, 651, 2197-2200.
3. Alcantarilla, P. F., & Solutions, T. (2011). Fast explicit diffusion for accelerated features in nonlinear scale spaces. IEEE Trans. Patt. Anal. Mach. Intell, 34(7), 1281-1298.
4. Gorokhovatskyi, O., Peredrii, O., Gorokhovatskyi, V., Vlasenko, N. (2023) Explanation of CNN Image Classifiers with Hiding Parts. In: J. Benois-Pineau, R. Bourqui, D. Petkovic, G. Quenot (eds), Explainable Deep Learning Artificial Intelligence, pp. 125-146, Academic Press, 346 p.
5. Daradkeh Y.I., Gorokhovatskyi V., Tvoroshenko I., and Zeghid M. (2024) Improving the effectiveness of image classification structural methods by

compressing the description according to the information content criterion, Computers, Materials & Continua, vol. 80, no. 2, 3085-3106.

6. Gorokhovatskyi V., Gadetska S., Stiahlyk N. (2020) Image structural classification technologies based on statistical analysis of descriptions in the form of bit descriptor set. In CEUR Workshop Proceedings: Computer Modeling and Intelligent Systems (CMIS-2020), 2608, 1027-1039.

7. Gorokhovatskyi, V., Gadetska, S., & Stiahlyk, N. (2023). Accelerating Image Classification based on a Model for Estimating Descriptor-to-Class Distance. International Journal of Computing, 22(4), 485-492.

8. Gorokhovatskyi, V., Chmutov, Y., Tvoroshenko, I., & Kobylin, O. (2025). Reducing computational costs by compressing the structural description in image classification methods. Advanced Information Systems, 9(1), 5–12.

9. Gorokhovatskyi V., Tvoroshenko I., Yakovleva O., and Hudáková M. (2025) Image description compression in classification structural methods, IEEE Access, vol. 13, pp. 43631-43641, doi: 10.1109/ACCESS.2025.3548910.

10. Gorokhovatsky V.A. Efficient Estimation of Visual Object Relevance during Recognition through their Vector Descriptions. Telecommunications and Radio Engineering. – 2016, Vol. 75, No 14. – P. 1271–1283.

УДК 004.932.2

Зіма В. О.

здобувач вищої освіти,

Харківський національний університет радіоелектроніки, кафедра інформатики (ІНФ)

Email: volodymyr.zima@nure.ua

Науковий керівник

Кобилін І. О.

к.т.н., Асоційований професор

Харківський національний університет радіоелектроніки, кафедра інформатики (ІНФ)

ОЦІНКА ЯКОСТІ І ВАЛІДАЦІЯ КРАУДСОРС-РЕПОРТІВ ПРО ПРОБЛЕМИ ДОСТУПНОСТІ МІСЬКОЇ ІНФРАСТРУКТУРИ

Із зростанням кількості маломобільних людей доступність міст набуває особливої ваги. Краудсорсингові платформи допомагають оперативно виявляти перешкоди, такі як незручні входи, відсутні пандуси чи високі бордюри. Проте ефективність цих систем залежить від якості даних, що надходять від користувачів. Основні труднощі при зборі цієї інформації полягають у наступному:

- Позиційна помилка GPS, що може бути спричинена такими факторами як слабкий сигнал, «урбан-каньйон», відбиті сигнали, похибка приймача, в

наслідок чого репорти можуть «стояти» поза реальною локацією об'єкта (наприклад, на сусідній вулиці);

- Дублікація репортів – проблема полягає в тому, що кілька користувачів можуть повідомляти про одну і ту ж саму перешкоду з трохи різними координатами/описами, в наслідок чого може спостерігатись фальшива кількість проблем, плутанина в пріоритетах;

- Семантична неоднорідність і низька якість фото – описи/теги можуть різнитися а фото можуть бути недостатньо інформативними, що ускладнює або унеможлиблює автоматизований аналіз (CV/NLP) для звітів що створюють користувачі.

- Похибка вибірки (Sampling bias/coverage), або ж велика кількість репортів у централізованих районах та недостатнє покриття околиць, що призводить до неправдивих висновків про просторові пріоритети.

В рамках використання глобальних навігаційних систем, таких як GPS та Galileo, що визначають положення приймача, вимірюючи часові затримки від кількох супутників, точність позиціонування залежить від кількості видимих супутників, умов прийому («урбан-каньйон», відбиті сигнали) та якості приймача. Типовий смартфон у містах забезпечує похибку від ~3 до ~20 метрів, для підвищення точності використовуються такі методи: A-GPS (комбінований супутниковий та мобільний зв'язок), агрегація координат, RTK/PPP (високоточні послуги) та map-matching – коригування положення до найближчої вулиці/об'єкта на карті. А також крім GNSS, в зв'язку з бурхливим та активним використанням мобільних пристроїв, широку популярність отримала VGI (Volunteered Geographic Information) – дані, які згенеровані користувачем: звіти з фотографіями, координатами, текстовим описом. Незважаючи на велику вибірку інформації, існують суттєві проблеми VGI: позиційна похибка, семантична неоднорідність (різні користувачі описують одну й ту саму перешкоду по-різному), дублювання повідомлень та нерівномірне просторове охоплення (sampling bias). Наукові підходи до забезпечення якості VGI включають метрики позиційних похибок, узгодженість між оцінювачами (Cohen's kappa), алгоритми виявлення дублікатів та крауд-валідацію.

Тож, для корекції позиціонування використовується map-matching: GPS-координати кожного повідомлення «прив'язані» до найближчого об'єкта OSM (way/node) з обмеженням відстані (наприклад, ≤ 20 м). Такий підхід зменшує похибку позиціонування для міських даних та покращує кластеризацію повідомлень.

В рамках боротьби з дублікатами, активну участь приймають алгоритми DBSCAN та семантика які працюють в два етапи як показано на рисунку 1:

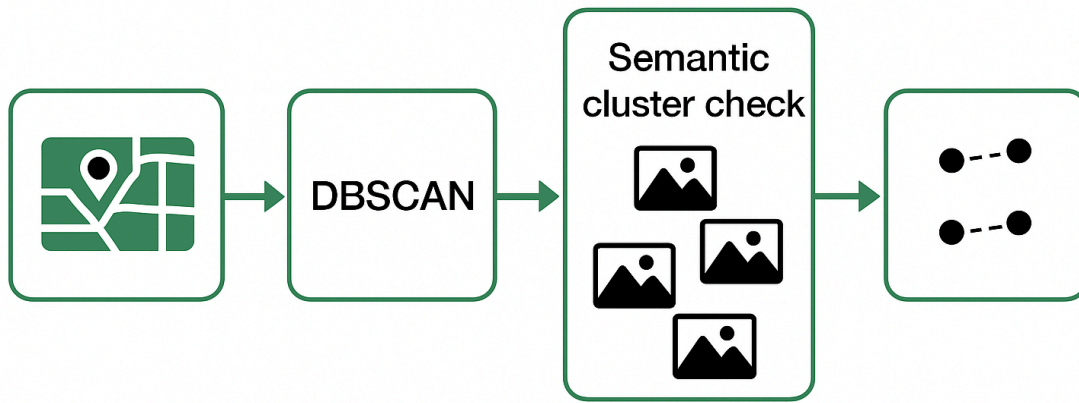


Рисунок 1 – схема роботи двоетапної системи просторове групування методом DBSCAN та семантична перевірка кластера

Тобто агрегація близьких репортів у кластери а далі, перевірка семантики шляхом порівняння категорій і/або фотохешів.

Для автоматичної попередньої фільтрації звітів введено індикатор $confidence_{score}$ **confidence_{score}**, який поєднує показники позиційної впевненості, якості фотографії, кількості підтверджень від інших користувачів та повноти метаданих. Поріг $confidence_{score}$ **confidence_{score}** використовується для автоматичного перенаправлення звіту до програми або для його позначення для ручної перевірки.

$$final_{conf} = w_1 \cdot GPS_{conf} + w_2 \cdot photo_{conf} + w_3 \cdot crowd_{conf} + w_4 \cdot meta_{conf}$$

Де GPS_{conf} **GPS_{conf}** – позиційна надійність[0,1], $photo_{conf}$ **photo_{conf}** – якість фото / CV-оцінка[0,1], $crowd_{conf}$ **crowd_{conf}** – нормалізована кількість підтверджень[0,1], $meta_{conf}$ **meta_{conf}** – повнота метаданих[0,1]

- Якщо є модель CV: $photo_{conf}$ **photo_{conf}** = модельний score (ймовірність, що фото відповідає заявленій категорії)

- Якщо моделі немає: $photo_{conf}$ **photo_{conf}** = 1, якщо фото надано і має достатню роздільність; 0.5 – якщо фото є, але темне/неінформативне; 0 – якщо фото відсутнє.

Автоматична категоризація фотографій реалізована на основі попередньо навчених згорткових мереж з додатковим навчанням на позначеному наборі зображень. Модель надає попередню категорію та оцінку, які включені до частини $photo_{conf}$ **photo_{conf}** параметра $confidence_{score}$ **confidence_{score}**.

Для швидкого семантичного порівняння фотографій використовуються алгоритми перцептивного хешування (pHash) та/або ембеддинги, які дозволяють виявляти схожі фотографії навіть за різних умов зйомки.

Запропонований підхід поєднує геопросторову корекцію через map-matching до OpenStreetMap-об'єктів для зменшення помилок визначення місцезнаходження, просторову агрегацію (DBSCAN) для виявлення

потенційних дублікатів, семантичну перевірку описів та фотографій (ембеддинги/перцептивні хеші) для розрізнення схожих звітів, а також «*confidence_{score}* *confidence_{score}*» – агреговану метрику достовірності, яка поєднує достовірність місцезнаходження, якість фотографій, кількість підтверджень та повноту метаданих. Така багаторівнева система дозволяє автоматизовано фільтрувати звіти низької якості, одночасно позначаючи сумнівні випадки для ручної перевірки, підвищуючи корисність даних для планування доступності інфраструктури та визначення пріоритетів технічного обслуговування.

Список використаних джерел:

1. Wheelmap.org URL: <https://wheelmap.org/>
2. Fonte, C C, Antoniou, V, Bastin, L, Estima, J, Arsanjani, J J, Bayas, J-C L, See, L and Vatsava, R. 2017. Assessing VGI Data Quality. In: Foody, G, See, L, Fritz, S, Mooney, P, Olteanu-Raimond, A-M, Fonte, C C and Antoniou, V. (eds.) Mapping and the Citizen Sensor. Pp. 137–163. London: Ubiquity Press. DOI: <https://doi.org/10.5334/bbf.g>. License: CC-BY 4.
3. Verification Handbook (укр.) URL: https://verificationhandbook.com/downloads/verification.handbook_ua.pdf

УДК 004.09

Іванічева С.В.,

Гладка М.І.,

Мартишко Є.С.

здобувачі вищої освіти,

Державний торговельно-економічний університет

Науковий керівник

Жирова Т.О.

кандидат педагогічних наук, доцент кафедри інженерії програмного

забезпечення та кібербезпеки

Державний торговельно-економічний університет

ХМАРНІ ТЕХНОЛОГІЇ: ЧОМУ МИ ЗБЕРІГАЄМО ФАЙЛИ В GOOGLE DRIVE ЧИ ICLOUD

Хмара – це не тільки про погоду, а про те, де лежать твої файли, типу як віддалений жорсткий диск в інтернеті. Раніше всі бігали з флешками, а зараз просто заходиш у свій Google-акаунт чи Apple ID – і все твоє завжди під рукою.

У хмари купа користі. По-перше, можеш зайти з будь-якого девайсу: з компа, телефона чи планшета. По-друге, все само резервується: накрився в тебе телефон – файли все одно в хмарі цілі. По-третє, зручно працювати разом: кілька людей можуть одночасно правити один документ. Ну і плюс, хмара економить місце на самому пристрої.

Але є й мінуси. Щоб глянути файли, треба інтернет. Безкоштовного місця мало: наприклад, Google дає 15 гігабайт, а Apple взагалі жметься – тільки 5. І ще один момент – можуть зламати акаунт і все вкрасти.

Тепер про сервіси. Google Drive дає 15 гігабайт безкоштовно,

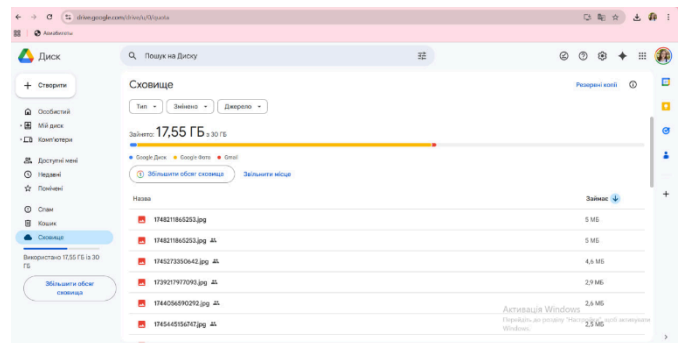
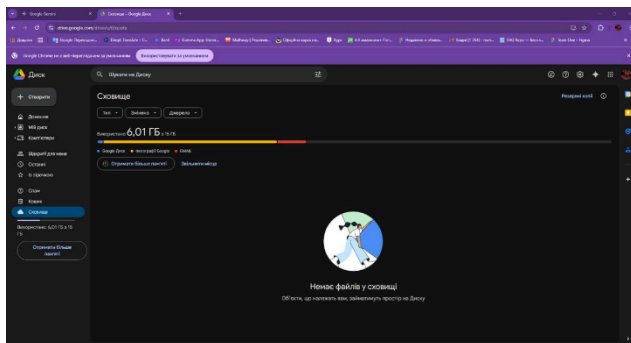


Рис.1

і він круто дружить з Gmail, Google Docs і Sheets – це взагалі супер для навчання і групової роботи. iCloud дає всього 5 гігабайт, але він ідеальний для тих, у кого iPhone і Mac, бо автоматично зберігає фотки й копії.

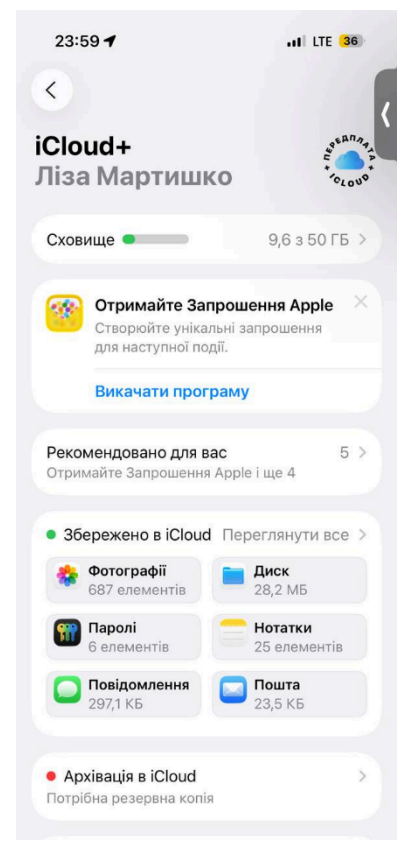
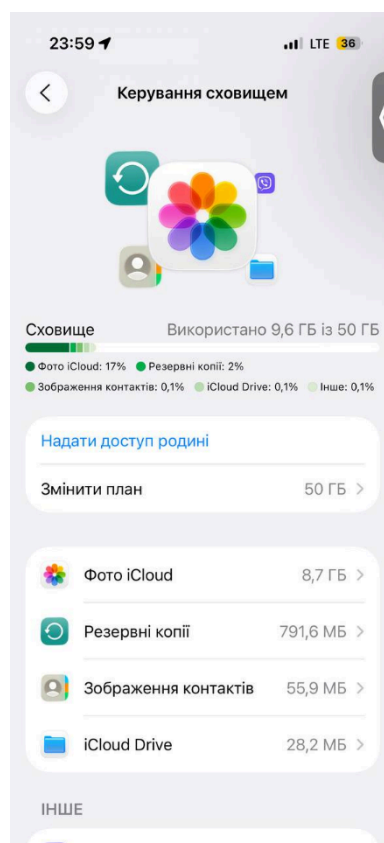
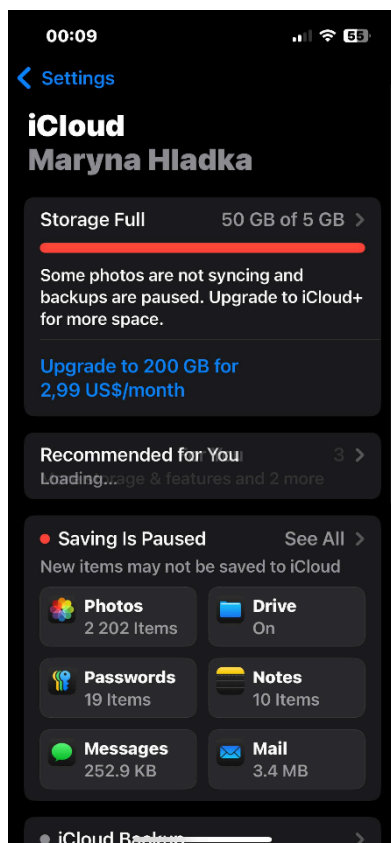


Рис. 2

OneDrive від Microsoft теж дає 5 гігабайт, але він класний для роботи з Word, Excel і Teams.

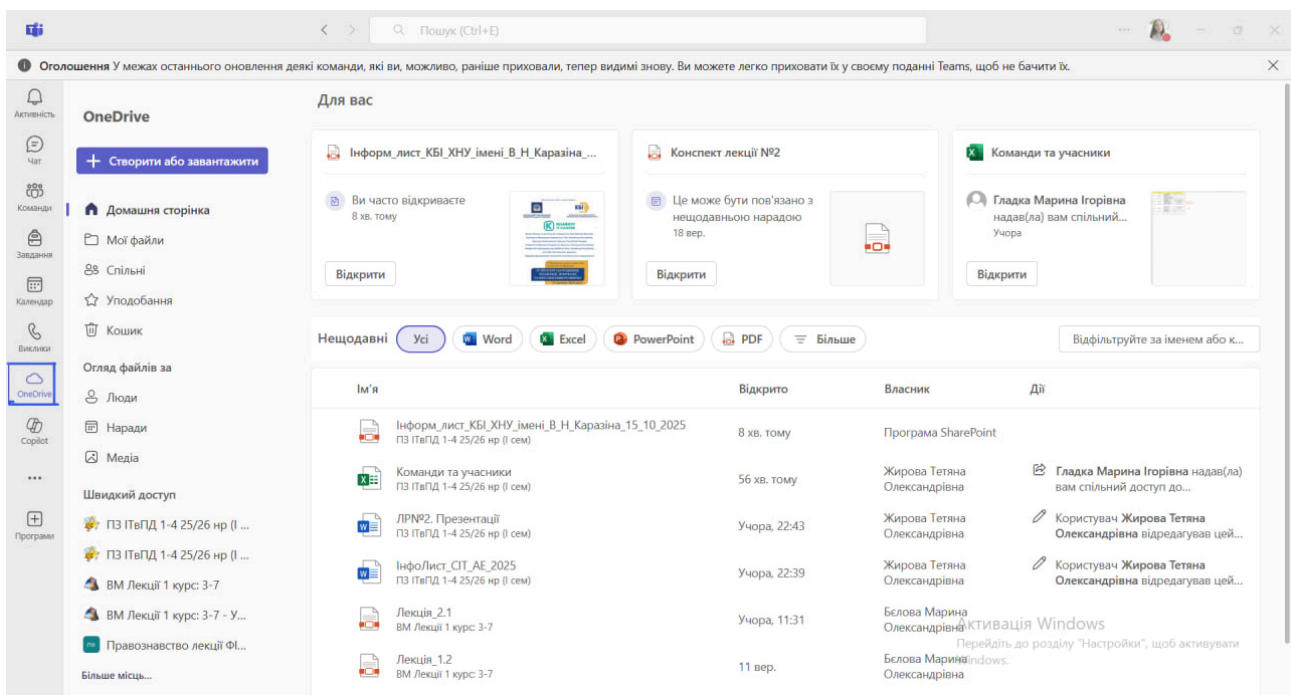


Рис. 3

Хмарні технології зараз всюди потрібні: і в навчанні, і в роботі. Студенти можуть зберігати конспекти, презентації, лаби і дивитися їх звідки завгодно. На дистанційці Google Drive і OneDrive взагалі стали незамінними. А в бізнесі хмарні сервіси допомагають працювати в команді над одним проєктом, швидко обмінюватися файлами і час економити.

Отже, хмарні технології – це сучасний і зручний спосіб зберігати і ділитися даними. Вони роблять нас мобільними, допомагають працювати в команді і бізнесу бути швидким. З часом вони стануть ще безпечнішими і розумнішими, бо в них додають штучний інтелект. Так що хмари – це вже не казка, а реальність, якою ми користуємося щодня.

Список використаних джерел:

1. Google. Google Drive – Cloud Storage & File Backup for Photos, Docs & More. <https://drive.google.com>.
2. Apple. iCloud – Apple. <https://www.icloud.com>.
3. Microsoft. OneDrive – Cloud Storage. <https://onedrive.live.com>.
4. Для перевірки пунктуації використовувався штучний інтелект Gemini

Камишан П.С.
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Науковий керівник
Кобилін І.О.
к.т.н., асистент кафедри Інформатики,
Харківський національний університет радіоелектроніки

КОМБІНОВАНИЙ ПІДХІД КОМП'ЮТЕРНОГО ЗОРУ ТА ОПТИЧНОГО РОЗПІЗНАВАННЯ ТЕКСТУ ДЛЯ ПІДВИЩЕННЯ ТОЧНОСТІ ІДЕНТИФІКАЦІЇ ЗОБРАЖЕНЬ

Існуючі підходи, які використовують ці технології окремо, часто демонструють незадовільні результати, якщо поставлене завдання вимагає одночасної ідентифікації візуальних та текстових даних. Ця проблема є особливо актуальною для систем, де критична точність ідентифікації, а помилки можуть призвести до значних фінансових ризиків чи серйозних наслідків. Наприклад, у системах автоматизованого зчитування показань вимірювальних приладів, розпізнавання номерних знаків у транспортних потоках, або при аналізі медичних зображень, де надійність результату є пріоритетом. Саме тому виникає потреба в розробці більш досконалих підходів, які б ефективно поєднували переваги комп'ютерного зору та оптичного розпізнавання зображень приклади яких показано на рисунку 1.



Рисунок 1. Приклади

Сучасні підходи в області комп'ютерного зору (CV) та оптичного розпізнавання тексту (OCR) базуються на глибокому навчанні та досягли значних успіхів у вирішенні складних завдань, але кожен з них має свої особливості. Методи комп'ютерного зору, що використовуються для детекції об'єктів, є ключовими для першого етапу гібридного підходу. Серед найпопулярніших архітектур виділяють You Only Look Once (YOLO) [1], що є

однією з найшвидших та найефективніших для виявлення об'єктів в реальному часі, та Mask R-CNN [2], яка, хоч і повільніша, але створює маску сегментації, забезпечуючи точнішу локалізацію. Ці моделі, хоч і потужні, не можуть ідентифікувати об'єкти за текстовими ознаками. Методи оптичного розпізнавання тексту, що використовуються для “читання” символів, також еволюціонували завдяки глибокому навчанню. Tesseract, один з найвідоміших відкритих OCR-двигунів, демонструє високу точність на чистому тексті. Водночас, Convolutional Recurrent Neural Network (CRNN) [3] є одним з проривів, що поєднує згорткові та рекурентні шари для стійкого розпізнавання тексту в різноманітних візуальних умовах. Незважаючи на високу точність, OCR-моделі часто працюють з усім зображенням, що може призвести до значних обчислювальних витрат та помилок.

Тож аналіз існуючих методів показує, що як CV, так і OCR є потужними інструментами, але їх використання окремо не вирішує проблему комплексної ідентифікації зображень, що містять як візуальні, так і текстові дані. Це створює необхідність у комбінованому підході, який би використав переваги обох технологій для досягнення вищої ефективності та надійності.

Тому запропонована гібридна архітектура з методів CV та OCR виконує і дозволяє значно підвищити точність та ефективність ідентифікації зображень.

Алгоритм роботи представлено на рисунку 2 де на першому етапі, етапі детекції (CV), використовується модель комп'ютерного зору (наприклад, YOLOv8 або Mask R-CNN) для сканування всього зображення з метою локалізації текстових регіонів. Модель ідентифікує об'єкти, що містять текст, та створює навколо них обмежувальні рамки. Цей крок ефективно фільтрує сторонні візуальні об'єкти та спрямовує подальшу обробку лише на релевантні області. На другому етапі, етапі розпізнавання (OCR), OCR-модуль (наприклад, Tesseract або модель на основі CRNN) застосовується виключно до цих рамок. Це дозволяє OCR-системі працювати з цільовими даними, що значно мінімізує помилки розпізнавання, викликані складним фоном або низькою контрастністю. Цей комбінований підхід пропонує низку значних переваг порівняно з використанням CV та OCR окремо: підвищену точність, зменшення затримки та підвищену стійкість.

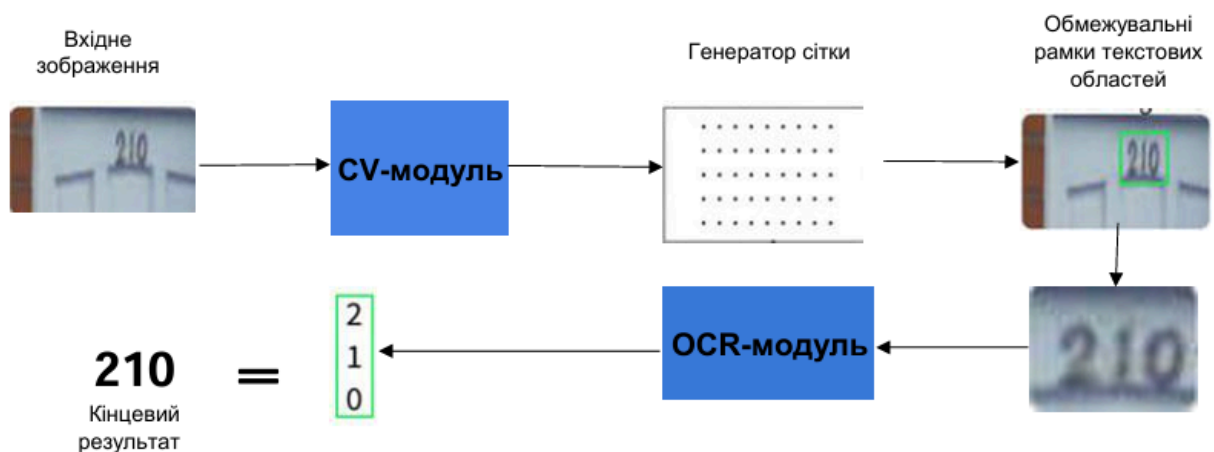


Рисунок 2. Алгоритм роботи

Ефективність комбінованого підходу CV-OCR не обмежується лише теоретичними перевагами, а знаходить своє підтвердження у численних експериментальних дослідженнях. Аналіз цих робіт переконливо демонструє, що гібридна архітектура перевершує традиційні методи за ключовими показниками, такими як точність, швидкість та надійність.

Таблиця 1.

Порівняльний аналіз звичайного OCR та комбінованого CV+OCR

Критерій порівняння	OCR	CV + OCR
Основна дія	Обробка всього зображення.	Детекція (CV) з подальшим розпізнаванням (OCR) цільової області.
Обробка зображення	Пряме застосування OCR до необробленого зображення.	Детекція об'єкта (Номерний знак) за допомогою YOLOv8 (CV), створення Обмежувальної рамки.
Вихід (Розпізнаний текст)	Помилка: "AC S419 6B LX470"	Успіх: AC 8479 CB
Точність розпізнавання	Низька: 61.5%	Висока: 100%

У дослідженні було проведено порівняльний аналіз, який показав, що двоетапний підхід демонструє значно вищу точність, оскільки CV-модуль ефективно фільтрує фон, залишаючи OCR-модулю лише релевантну область. Цей підхід успішно долає обмеження, властиві кожній з технологій, які використовуються окремо. Запропонована гібридна архітектура забезпечує значне підвищення точності та надійності, тож аналіз цих та інших досліджень дозволяє зробити висновок, що гібридна архітектура забезпечує значне покращення ключових метрик. Зокрема, точність ідентифікації в дослідженнях ANPR досягає 95% і вище, що є значно вищим показником порівняно з окремими OCR-системами. Крім того, загальна затримка обробки скорочується, що є критично важливим для додатків, що вимагають обробки зображень в реальному часі.

Список використаних джерел:

1. Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection. CVPR, IEEE.
2. He, K., Gkioxari, G., Dollár, P., & Girshick, R. (2017). Mask R-CNN. Proceedings of the IEEE International Conference on Computer Vision.
3. Shi, B., Wang, X., & Lv, P. (2016). An End-to-End Trainable Neural Network for Image-based Sequence Recognition and Its Application to Scene Text Recognition. Transactions on Pattern Analysis and Machine Intelligence, IEEE.
4. G. G. J. and S. S. S. A., (2021). A Comparative Analysis of Different Computer Vision and OCR Techniques for Automatic Number Plate Recognition. International Journal of Engineering and Advanced Technology.

*Ковальчук В.О.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Кобилін І.О.
к.т.н., асистент кафедри Інформатики
Харківський національний університет радіоелектроніки*

ЗАСТОСУВАННЯ ML.NET У СЕМАНТИЧНОМУ АНАЛІЗІ МОВЛЕННЄВИХ КОМАНД ДЛЯ ГОЛОСОВИХ АСИСТЕНТІВ

Семантичний аналіз природної мови (Natural Language Understanding, NLU) є критичним етапом у розробці інтелектуальних голосових асистентів. Його завдання полягає не лише у перетворенні мовлення на текст, а й у глибокому розумінні змісту висловлювань, виявленні прихованого наміру користувача, ідентифікації ключових об'єктів у команді, аналізі граматичної структури речення та врахуванні контексту. Для того, щоб голосовий інтерфейс працював інтуїтивно та зручно, система має вміти не просто реагувати на окремі слова, а розуміти логіку висловленого.

Важливою складовою семантичного аналізу є розпізнавання іменованих сутностей (Named Entity Recognition, NER), що дозволяє системі ідентифікувати згадки про програми, дати, дії або контакти. Це особливо актуально для команд типу «відкрий Telegram» або «створи зустріч на завтра». Ще одним важливим аспектом є виявлення інтенції – розуміння того, що саме має зробити програма у відповідь на команду: відкрити, закрити, знайти, тощо. Для досягнення високої точності обробки команд також необхідно враховувати кореференцію, коли слова на кшталт «його» чи «це» відсилають до згаданих раніше об'єктів. Усі ці елементи формують структуру, яка дозволяє системі поводитися природно та логічно у взаємодії з користувачем.

Українська мова додає окремий рівень складності через свою морфологічну багатогранність: відмінки, роди, числа, суфікси та афікси значно ускладнюють точне розпізнавання слів та сутностей. Проте в останні роки ситуація змінилася: були створені повноцінні корпуси, такі як NER-UK 2.0, який містить понад 21 тисячу вручну анотованих сутностей, а також адаптовані трансформерні моделі, які досягають точності понад 89% F1. Інструменти на кшталт lang-uk або Stanza забезпечують морфологічний аналіз і лематизацію для української мови, що дозволяє об'єднувати форми слів та працювати зі словниками в обчислювальних системах.

ML.NET – це відкрите середовище машинного навчання від компанії Microsoft, яке дозволяє реалізовувати NLP-рішення без виходу за межі екосистеми .NET. На відміну від багатьох альтернатив, реалізованих на Python, ML.NET забезпечує пряму інтеграцію в C#-проекти, що дає змогу створювати повноцінні локальні рішення без серверів, REST API чи прокладок на Flask. Завдяки таким компонентам, як TextFeaturizingEstimator або Text Classification API, розробник може реалізовувати попередню обробку тексту, токенизацію,

нормалізацію, побудову TF-IDF векторів (1) і класифікацію команд без значних зусиль. Крім того, з версії 2.0 ML.NET підтримує інтеграцію з ONNX Runtime та TorchSharp, що дозволяє підключати готові трансформерні моделі, включаючи BERT і RoBERTa.

$$TF(t_i, d_i) = \frac{f(t_i, d_i)}{\sum_k f(t_k, d_i)},$$

$$IDF(t_i, D) = \log\left(\frac{N}{|\{d \in D : t_i \in d\}|}\right),$$

$$TF - IDF(t_i, d_i, D) = TF(t_i, d_i) \times IDF(t_i, D), (1)$$

де $f(t_i, d_i)$ – кількість появ слова t_i у документі d_i , N – загальна кількість документів у корпусі, а $|\{d \in D : t_i \in d\}|$ – число документів, що містять цей термін.

Таким чином, ML.NET є привабливим інструментом для розробників, які створюють голосових асистентів для кросплатформного середовища. Його використання особливо доцільне в умовах обмежених ресурсів, коли необхідна продуктивність, локальна обробка команд і зручність інтеграції.

Для наглядності проведено експериментальне порівняння двох інструментів обробки природної мови – ML.NET та Python-бібліотеки scikit-learn. Метою експерименту було оцінити їхню ефективність у задачі класифікації простих голосових команд українською мовою. Зокрема, розглядалися короткі текстові інструкції, які користувач міг би дати голосовому асистенту. Команди поділялися на дві семантичні категорії: ті, що стосуються відкриття програм, та всі інші дії (наприклад, зміна налаштувань або встановлення нагадувань).

Для реалізації моделі в середовищі ML.NET використовувалися стандартні засоби попередньої обробки тексту та побудови векторних представлень, зокрема TF-IDF, токенізація та нормалізація. У якості класифікатора була застосована реалізація методу стохастичної координатної оптимізації. Модель демонструвала високу точність класифікації та швидкий час навчання, при цьому забезпечуючи зручну інтеграцію з середовищем C#.

У випадку Python-платформи була використана бібліотека scikit-learn із типовими засобами обробки тексту (TF-IDF векторизація) та класифікатором на основі логістичної регресії. Результати моделі виявилися трохи нижчими за точністю, а також вимагали додаткових дій для інтеграції з основним застосунком, зокрема – налаштування API або зовнішнього сервісу.

Узагальнені отримані результати

Параметр	ML.NET (C#)	Scikit-learn (Python)
Точність класифікації	91%	88%
Простота інтеграції	Висока (нативна C#)	Середня (через API)
Робота з UI	Пряма (WinForms/WPF)	Непряма (через REST)
Кросплатформеність	Так	Так
Робота офлайн	Так	Так
Робота з трансформерами	Через ONNX	Через transformers

Семантичний аналіз природної мови в контексті голосових асистентів вимагає точного розпізнавання інтенцій, сутностей і граматичних залежностей, що особливо актуально для української мови з її розвиненою морфологією. Використання ML.NET як засобу реалізації таких підходів забезпечує ефективну обробку текстових команд завдяки підтримці векторизації, класифікації та інтеграції з трансформерними моделями через ONNX. У порівнянні з Python-бібліотекою scikit-learn, ML.NET демонструє вищу інтеграційну зручність, локальну автономність і кращу відповідність архітектурі C#-застосунків. З урахуванням точності, продуктивності та сумісності з .NET-екосистемою, ML.NET є доцільним вибором для побудови кросплатформених голосових інтерфейсів із підтримкою української мови.

Список використаних джерел:

1. Alford A. ML.NET 2.0 Release Contains New NLP APIs and AutoML Updates. *InfoQ*. URL: https://www.infoq.com/news/2022/12/microsoft-mlnet-release?utm_source=chatgpt.com (date of access: 21.09.2025).
2. Brandsen A. Creating a Dataset for Named Entity Recognition in the Archaeology Domain. *Proceedings of the Twelfth Language Resources and Evaluation Conference*. 2020. P. 4573–4577.
3. Chaplynskyi D., Romanyshyn M. Introducing NER-UK 2.0: A Rich Corpus of Named Entities for Ukrainian. *Proceedings of the Third Ukrainian Natural Language Processing Workshop*. 2024. P. 23–29.
4. Microsoft previews text classification API for ML.NET. *InfoWorld*. URL: <https://www.infoworld.com/article/2335749> (date of access: 21.09.2025).
5. What is ML.NET? An open-source machine learning framework for developers | .NET. *Microsoft*. URL: https://dotnet.microsoft.com/learn/ml-dotnet/what-is-mldotnet?utm_source=chatgpt.com (date of access: 21.09.2025).

**Максімов І.М.,
Бондаренко Я.Ю.,
Бутова Д.О.,**

здобувачі вищої освіти,

Державний торговельно-економічний університет

Науковий керівник

Жирова Т.О.

*к.п.н., доц., доцент кафедри інженерії програмного забезпечення
та кібербезпеки*

Державний торговельно-економічний університет

ДОСЛІДЖЕННЯ ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ОБРОБКИ ПРИРОДНОЇ МОВИ

Обсяг інформації у сучасному світі постійно зростає, і значна її частина представлена у текстовій формі: наукові статті, новини, повідомлення у соціальних мережах, відгуки, бізнес-звіти, офіційні документи та електронне листування. Тексти та мова, якими ми спілкуємося, зараз аналізуються комп'ютерами за допомогою NLP, і саме вони стають головним предметом дослідження цих програмних засобів. Обробка NLP передбачає використання алгоритмів штучного інтелекту, машинного навчання та статистичних методів для розпізнавання, структурування, класифікації та аналізу текстової інформації.

Власне поняття NLP різними науковцями тлумачиться по-різному.

Наприклад, деякі автори визначають його так: «Обробка природної мови (NLP – Natural Language Processing) – це підрозділ інформаційних технологій, штучного інтелекту та лінгвістики, метою якого є вивчення проблем комп'ютерного аналізу та синтезу природної мови» [1].

Таким чином, ми вирішили провести дослідження одного з ключових аспектів обробки природної мови (NLP): токенізації тексту. Токенізація – це процес розбиття тексту на менші одиниці (токени), що необхідно для більш ефективної обробки та економії обчислювальних ресурсів [2].

У цій роботі ми дослідимо алгоритми FM-Tree, WordPiece та BPE, розглянувши їх з різних аспектів, виміряємо продуктивність на різних наборах даних та порівняємо між собою.

FM-Tree – це авторський алгоритм, що будує частотно-морфологічне дерево та перетворює його сегменти у токени. Алгоритм працює у три етапи.

На першому етапі будується дерево: кожна вхідна послідовність перетворюється на ланцюг вузлів, де кожен вузол відповідає окремому символу, а наступні ланцюги накладаються на попередні. У місцях збігу вузлів підраховуються їхні частоти, що дозволяє відобразити морфологічну структуру слів.

На другому етапі відбувається оптимізація дерева: ланцюги без розгалужень об'єднуються в один вузол, що зменшує надлишковість і робить структуру компактнішою для подальшої обробки.

На фінальному етапі з дерева генеруються токени: обирається унікальний набір вузлів, а для збільшення словника вводиться умова об'єднання вузлів на основі порогу відносної частоти – відношення рахунку дочірнього вузла до рахунку батьківського. Такий підхід дозволяє отримати збалансований словник tokenів, що зберігає морфологічну інформативність мови.

Byte-Pair Encoding (BPE) – це алгоритм, що був розроблений як алгоритм для стиснення текстів, однак тепер його використовують для токенизації під час навчання моделей GPT. Сьогодні він застосовується у GPT, GPT-2, RoBERTa, BART та DeBERTa.

Навчання BPE починається з формування базового словника з усіх символів корпусу після нормалізації та попередньої токенизації. У сучасних реалізаціях використовується byte-level BPE, у якому замість символів Unicode беруться байти. Це дозволяє уникати невідомих tokenів і формувати компактний початковий словник із 256 одиниць. Далі алгоритм знаходить найчастіші пари сусідніх символів чи tokenів, об'єднує їх у новий token і додає до словника. Процес повторюється доти, поки словник не досягне потрібного розміру.

Під час токенизації для нових даних виконується нормалізація, попередня токенизація та розбиття слів на символи. Потім послідовно застосовуються вивчені правила злиття, що перетворює текст у послідовність tokenів із готового словника.

Реалізація BPE передбачає поступове злиття найчастіших пар символів, оновлення корпусу та розширення словника службовими й новими токенами. Ітерації тривають доти, поки словник не досягне заданого обсягу, забезпечуючи компактне й ефективне представлення тексту [3].

WordPiece – алгоритм токенизації, подібний до BPE у загальних принципах навчання, але має свої особливості у виборів злиттів і способів токенизації.

Алгоритм починає з невеликого словника, що містить спеціальні токени та алфавіт, де всі внутрішні символи мають префікс “##”. Це дозволяє розбивати будь-яке слово на мінімальні частини.

На відміну від BPE, який об'єднує найчастіші пари, WordPiece вибирає пари для злиття за спеціальною оцінкою: частота пари ділиться на добуток частот окремих її елементів. Такий підхід віддає перевагу об'єднанню рідкісних комбінацій, завдяки чому токени краще відображають структуру слів і уникають надто частих, але загальних злиттів. Процес повторюється доти, поки не буде досягнуто заданого розміру словника.

Під час токенизації WordPiece використовує лише кінцевий словник. Для кожного слова алгоритм шукає найдовший підсловник зі словника, додає його в результат і продовжує розбиття. Це призводить до того, що одне слово може бути закодоване кількома токенами. Якщо жодна частина слова не збігається зі словником, усе слово позначається токеном [UNK] [4].

Очікується, що алгоритм FM-Tree буде створювати велику кількість дрібних пар символів при високих емпіричних значеннях та здатний відтворювати всі слова, що траплялися в корпусі, при значеннях, близьких до нуля. Алгоритм, ймовірно, забезпечить більшу морфологічну достовірність і буде більш релевантним для синтетичних мов, таких як українська.

Як найбільш універсальний метод із оптимізованою реалізацією, BPE може демонструвати найшвидшу токенизацію серед розглянутих алгоритмів та показувати кращі результати за співвідношенням tokenів на одне слово у загальному випадку порівняно з FM-Tree.

Ймовірно, алгоритм WordPiece буде ефективніший у роботі з рідко вживаними словами та демонструвати помірну швидкість токенизації. Водночас він може бути менш релевантним для повної репрезентації тексту у токенах.

Отже, токенизація є ключовим етапом у NLP, від якого залежить якість обробки тексту. FM-Tree краще зберігає морфологію та підходить для мов зі складною граматикою, BPE відзначається швидкістю й універсальністю, а WordPiece ефективний для рідкісних слів. Тому вибір алгоритму має ґрунтуватися на особливостях мови та поставленому завданні.

Список використаних джерел

1. Онищенко К., Данієль Я., Каменєв Р. Аналіз методів обробки природної мови // Інформаційні системи та технології ICT-2020. Секція 6. Програмна інженерія. – Харків: НТУ «ХПІ», 2020. – URL: <https://openarchive.nure.ua/server/api/core/bitstreams/a26452b9-d866-4aaa-aa04-524a9cae5f55/content>
2. Nature Research Intelligence. Natural language processing. – 2021. – URL: <https://www.nature.com/research-intelligence/nri-topic-summaries/natural-language-processing-for-13-460208>
3. Gage P. A new algorithm for data compression // The C Users Journal. – 1994. – Vol. 12, № 2. – P. 23–38. – URL: https://www.derczynski.com/papers/archive/BPE_Gage.pdf
4. Schuster M., Nakajima K. Japanese and Korean voice search. – Google Research, 2012. – URL: <https://static.googleusercontent.com/media/research.google.com/ja//pubs/archive/37842.pdf>

Мітла М. О.
здобувач вищої освіти,
Державний податковий університет
Науковий керівник
Скасків Л. В.
к.ф-м.н., доцент, доцент кафедри
вищої та прикладної математики
Державний податковий університет

РОЛЬ ЛІНІЙНОГО ПРОГРАМУВАННЯ У ФОРМУВАННІ МЕТОДІВ ДОСЛІДЖЕННЯ ОПЕРАЦІЙ

Дослідження операцій у XX–XXI століттях сформувалося як міждисциплінарна наукова галузь, що інтегрує математичні методи, економічні концепції та принципи управління для аналізу й оптимізації складних систем. Його становлення безпосередньо пов'язане з розвитком лінійного програмування, яке забезпечило створення універсального інструментарію для формалізації завдань оптимізації. Завдяки здатності відображати реальні процеси у вигляді математичних моделей із чітко визначеними цільовими функціями та системами обмежень, лінійне програмування стало фундаментом сучасних методів прийняття рішень.

Н. Я. Шумило, І. М. Лях та інші дослідники підкреслюють, що значна кількість планово-виробничих і економічних завдань пов'язана з розподілом обмежених ресурсів – сировини, робочої сили, енергії, палива тощо. Розподіл цих ресурсів, як правило, може здійснюватися різними способами: шляхом вибору альтернативної технології, використання різних видів сировини, обладнання чи організації виробничого процесу. Кожен із таких варіантів оцінюється за певним критерієм – прибутком, обсягом випуску продукції чи іншими показниками. Природно виникає прагнення знайти оптимальний план розподілу, який забезпечить найбільший економічний ефект. Складність реальних економічних процесів зумовлює необхідність урахування численних факторів, що в математичній моделі виражається великою кількістю умов та невідомих. Якщо змінні входять у модель лише у першому степені, то завдання належить до лінійного програмування. Даний розділ математичного програмування досліджує задачі пошуку максимуму чи мінімуму лінійної цільової функції за наявності системи лінійних обмежень. Попри багатовимірність, задачі лінійного програмування добре піддаються як теоретичному аналізу, так і чисельному розв'язанню. Методи цього напрямку активно застосовуються в економіці, логістиці, телекомунікаціях, операційному менеджменті та інформаційних технологіях [4, с. 5].

У свою чергу, В. Я. Феньо під лінійним програмуванням розуміє «методи дослідження та відшукування оптимальних значень лінійної функції, на невідомі якої накладені лінійні обмеження» [3, с. 95]. При цьому, значення лінійного програмування для формування методів дослідження операцій полягає,

насамперед, у його універсальності. Будь-яке завдання, пов'язане з раціональним розподілом ресурсів, плануванням чи управлінням потоками, може бути зведене до лінійної моделі. Слід підкреслити, що зазначене дозволяє не лише уніфікувати процес моделювання, а й виробити методологію оптимізації, яка стала базою для подальшого розвитку цілого напрямку прикладних досліджень.

Розвиток лінійного програмування сприяв формуванню загальних принципів побудови математичних моделей. По-перше, воно стимулювало широке застосування апарату матричної алгебри, що стало основою для алгоритмізації задач оптимізації. По-друге, воно заклало підґрунтя для розвитку комп'ютерних методів розрахунку, що дозволило досліджувати багатовимірні системи з великою кількістю змінних та обмежень [1, с. 29-31].

Варто відзначити, що практичне значення лінійного програмування виявляється у можливості ефективного розв'язання транспортних, виробничих, логістичних, енергетичних та фінансових задач. Саме на основі цього методу були розроблені моделі транспортної задачі, задачі про призначення, виробничого планування та управління запасами. Вони отримали широке застосування у сфері економічного аналізу, державного управління та стратегічного планування [2, с. 21].

Підсумовуючи, слід підкреслити, що лінійне програмування не обмежилось рамками власної теорії, а стало основою для розвитку нових напрямів. Зокрема, воно стимулювало становлення цілочислового та нелінійного програмування, а також методів динамічної оптимізації. Такі розширення дозволили охопити більш складні й реалістичні задачі, які неможливо було звести до класичної лінійної форми. Так, лінійне програмування виконало методологічну функцію у розвитку всієї науки дослідження операцій, ставши відправною точкою для подальших теоретичних і прикладних досліджень.

Отже, лінійне програмування стало одним із найвагоміших досягнень прикладної математики ХХ століття, яке справило визначальний вплив на розвиток дослідження операцій. Його роль полягає у створенні універсального інструментарію оптимізації, формуванні методологічної бази моделювання та стимулюванні розвитку інших напрямів математичного програмування. Завдяки цьому метод досі зберігає свою актуальність, виступаючи теоретичною та практичною основою для аналізу й оптимізації складних систем.

Список використаних джерел:

1. Балтовський О. А., Форос Г. В., Сіфоров О. І. Основи математичного моделювання. Навчальний посібник. Одеський державний університет внутрішніх справ, 2023. – 125 с.
2. Скасків Л. В. Теорія чисел та основні структури сучасної математики: навчальний посібник. – Ірпінь: Університет ДФС України, 2021. – 70 с.

3. Феньо В. Я. Застосування методів лінійного програмування при розв'язуванні економічних задач. Цифрова економіка як фактор інновацій та сталого розвитку суспільства, 2021. С. 95-97.

4. Шумило Н. Я., Лях І. М. Лінійне програмування: приклади та задачі. Навчальний посібник. – Ужгород: Вид-во УжНУ «Говерла», 2025. – 216 с.

УДК 621.317

Скорін Юрій

кандидат технічних наук, доцент

Харківський національний економічний університет ім. С. Кузнеця

РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНОЇ СИСТЕМИ НА БАЗІ ВІРТУАЛЬНИХ КОМП'ЮТЕРНИХ ТРЕНАЖЕРІВ

Проведене дослідження ґрунтується на аналізі традиційних методів і засобів вимірювання та пропозиції віртуалізації процесу вимірювання як альтернативного вирішення проблеми. Зазначено, що крім використання за прямим призначенням, тобто як віртуальних вимірювальних приладів, досить перспективним є використання віртуальних пристроїв для побудови на їх базі віртуальних тренажерів, які забезпечують підвищення наочності та якості навчання, насамперед у так званих інструментальних навчальних дисциплінах, що, у свою чергу, створює передумови для включення їх у існуючі або створення на їх основі нових систем дистанційного навчання. Дане дослідження передбачає визначення віртуальних пристроїв як базових для побудови віртуальних тренажерів на їх основі, які забезпечують підвищення ефективності та наочності освітнього процесу та створюють передумови для створення та вдосконалення систем дистанційного навчання.

Сучасний прогресивний розвиток комп'ютерної техніки, комп'ютеризація всіх галузей економіки наводить на думку про використання такого досить потужного технологічного потенціалу, як комп'ютеризація, в удосконаленні процесу вимірювання в вимірювальних системах. Пошук рішення привів до необхідності створення комп'ютерних тренажерів на базі віртуальних пристроїв, аналоги яких вже існують і демонструють величезні переваги перед так званими традиційними пристроями, що дає стимул і можливість створення віртуальних комп'ютерних тренажерів на основі віртуалізації процесу вимірювання зразків, покликаних підвищити наочність і ефективність навчального процесу і створити передумови для значного розширення функціональних можливостей систем дистанційного навчання. Саме актуальність даного напрямку полягає в тому, що: по-перше, за допомогою віртуальних комп'ютерних тренажерів можна забезпечити набуття практичних навичок роботи з найсучаснішою комп'ютерною технікою, яка в силу обмеженості технічних або економічних

можливостей ще не використовується в освітньому процесі; по-друге, віртуальні комп'ютерні тренажери можуть використовуватися слухачами під час самостійної підготовки до занять, адже вони досить прості в експлуатації, не вимагають спеціальних знань в області програмування, не критичні до апаратного і програмного забезпечення персонального комп'ютера, містять поради та коментарі, які практично керують діями оператора, відпрацьовують його помилки; по-третє, віртуальні комп'ютерні тренажери, на нашу думку, повинні створюватися в першу чергу для найсучасніших пристроїв, яких ще немає в лабораторно-технічній базі установи, на попередньому етапі підготовки до роботи на стандартному обладнанні, при самостійній підготовці до занять, при заочному навчанні тощо, тобто в тих випадках, коли доступ до стандартного вимірювального обладнання обмежений або недоцільний; в-четвертих, віртуальному комп'ютерному тренажеру можна придати додаткові функції, які не присущі реальному прибору, наприклад, відображати фізичні процеси, які відбуваються всередині прибора в час проведення вимірювального експерименту, перевірки, надавати пошукову інформацію, виконувати обробку і зберігання результатів вимірювань і діагностики, проводити тестування і контроль рівня знань учасників і тому подібне; в-п'ятих, розглядавані в статті віртуальні комп'ютерні тренажери мають зовнішній вигляд, повністю відповідний зовнішньому вигляду реальних приборів, для цього були створені нестандартні ActiveX елементи, що теж не маловажно з точки зору ефективності процесу навчання.

Таким чином, можна сформулювати цілі дослідження, а саме, підвищити ефективність освітнього процесу за рахунок розробки та впровадження віртуальних комп'ютерних тренажерів на основі створених віртуальних пристроїв.

З метою вирішення вимірювальних завдань і проведення вимірювального експерименту якість візуалізації не має вирішального значення, але якщо мова йде про віртуальному тренажері, задіяному в навчальному процесі, то тут першорядне значення має питання візуалізації, тобто наскільки зовнішній вигляд тренажера відповідає зовнішньому вигляду традиційного пристрою. Отже, актуальним стає питання, пов'язане з візуалізацією процесу вимірювання, тобто розробкою віртуального тренажера, зовнішній вигляд і функціональність якого можна було регулювати як в процесі розробки, так і в процесі роботи. Так, був розроблений віртуальний вимірювальний комплекс у вигляді програмного комплексу під загальною назвою «Віртуальна вимірювальна лабораторія», який включав в себе кілька комп'ютерних тренажерів. Методика проведення вимірювального експерименту за допомогою віртуального приладу-тренажера практично не відрізняється від існуючих методів, властивих відповідним традиційним вимірювальним приладам, тому не розглядається в рамках даної статті. Розроблений програмний продукт являє собою модульну структуру, засновану на принципі побудови і містить загальний для всіх віртуальних тренажерів блок управління або програмну оболонку, що входять до складу віртуальної вимірювальної лабораторії і дозволяє користувачеві ознайомитися зі структурою віртуального цеху, забезпечити безпосередній доступ до основних

розділів довідкової інформації, запускати інтерактивні модулі лабораторних робіт, а також зберігати результати роботи, друкувати звітувати про результати досліджень тощо. Важливою особливістю розробленого програмного продукту є те, що його робота може бути реалізована в режимі підказки, коли програма фактично керує діями оператора, надає коментарі та підказки, а також блокується при виконанні оператором дій, які можуть викликати критичну помилку. Можливість розширення функціональних можливостей комп'ютерного тренажера, перш за все, що не притаманне традиційним пристроям, представляється практично необмеженою. Тому, в залежності від призначення кожного конкретного віртуального тренажера, деякі модулі програмного продукту містять інтерактивні електронні таблиці, часові діаграми, графіки, що відображають фізичні процеси, що відбуваються в пристрої під час вимірювального експерименту, що сприяють підвищенню ефективності навчального процесу. Що стосується сфери застосування віртуальних комп'ютерних тренажерів, то, на наш погляд, в першу чергу, їх доцільно створювати для моделювання найсучасніших пристроїв, які ще не входять до складу лабораторно-технічної бази установи або придбання яких утруднено з точки зору їх вартості, а також на попередньому етапі підготовки до роботи на стандартному обладнанні або під час самостійної підготовки до занять. при заочному навчанні тощо, тобто у випадках, коли доступ до стандартної вимірювальної техніки обмежений або недоцільний. Розроблений програмний комплекс є повноцінним і самодостатнім програмним продуктом, який включає в себе інсталяційний модуль, адаптований під більшість програмних платформ. Представлений програмний продукт повністю адаптований для використання в мережі Інтернет або локальних комп'ютерних мережах. Ще одна важлива особливість програмного продукту полягає в тому, що він є основою для побудови віртуальних вимірювальних приладів і комп'ютерних тренажерів інших типів і типів. Але слід зазначити, що впровадження комп'ютерних тренажерів в процес навчання жодним чином не має на увазі певної заміни стандартних традиційних пристроїв їх комп'ютерними моделями, а навпаки, лише доповнює і розширює можливості як вчителів, так і учнів. Питання, пов'язане з розробкою концепції, методики спільного використання в освітньому процесі як стандартних традиційних пристроїв, так і їх комп'ютерних тренажерних моделей, все ще потребує серйозного осмислення і, на жаль, не є метою цієї публікації. З точки зору подальшого розвитку програмного комплексу слід зазначити, що можливості поповнення парку віртуальних пристроїв практично необмежені, тому було б цікаво побудувати, наприклад, віртуальні аналогові пристрої, аналізатори спектру і т.д.

Список використаних джерел

1. Ю. І. Скорін. Підвищення якості освітнього процесу за рахунок розробки та апробації програмного забезпечення інформаційно-імітаційної системи на базі віртуальних комп'ютерних мереж / Ю. І. Скорін, О. В. Щебаков, І. О. Ушакова // Вісник Харківського національного автомобільно-дорожнього

університету. Збірник наукових праць. Х.: ХНАДУ. – 2022. – Випуск 96. – с. 141–145.

2. Ю. І. Скорін Віртуальні вимірювальні та діагностичні прилади / Ю. І. Скорін, О. В. Щербаков, Т. І. Магдаліц // Системи обробки інформації. Збірник наукових праць. Випуск 4(102), том 1. Інформаційні технології та захист інформації. Х.: ХНЕУ. – 2012. – с. 65–68.

3. Ю.І. Скорін. Робоча програма вивчення навчальної дисципліни «Метрологія та стандартизація» для студентів напряму підготовки «Інформатика з інформатики» всіх форм навчання / Ю.І. Скорін, В.В. Федько, О. В. Щербаков. – Навчальне видання. – Харків : Під редакцією ХНЕУ, 2012. – 48 с.

УДК 621.317

Скорін Юрій

кандидат технічних наук, доцент

Харківський національний економічний університет ім. С. Кузнеця

Васильєв Ігнат

студент

Харківський національний економічний університет ім. С. Кузнеця

ОПТИМІЗАЦІЯ ПРОЦЕСІВ ПРОЄКТНОГО МЕНЕДЖМЕНТУ

У сучасну епоху бурхливого розвитку інформаційних технологій інформаційна система стала основним інструментом підтримки роботи підприємства і прийняття стратегічних рішень. Ці системи не тільки відповідають за зберігання та обробку даних, але й мають глибокий вплив на бізнес-процеси та клієнтський досвід.

З поглибленням цифрової трансформації підприємства все більше покладаються на інформаційні системи для підвищення ефективності, зниження витрат і підвищення конкурентоспроможності. Однак мінливі вимоги ринку, швидкий прогрес у технологіях та зростання очікувань клієнтів призвели до того, що багато компаній зіткнулися з проблемою, що їхні інформаційні системи не можуть ефективно задовольняти потреби бізнесу.

Нинішня інформаційна система часто демонструє проблеми недостатньої гнучкості, поганої інтеграції та низької задоволеності користувачів. Ці дефекти не тільки призводять до зниження ефективності роботи, а й збільшують розтрату ресурсів, що серйозно позначається на ринковій конкурентоспроможності підприємств. Для вирішення цих проблем бізнес-аналіз (БА) як системна методологія все частіше стає важливим інструментом для підприємств для вирішення проблем інформаційних систем.

Завдяки глибокому аналізу вимог, оптимізації процесів та підтримці прийняття рішень на основі даних, бізнес-аналітика може допомогти

організаціям виявляти критичні проблеми в їхніх інформаційних системах та розробляти цільові стратегії вдосконалення [1].

Суть бізнес-аналітики полягає в розумінні та задоволенні потреб бізнесу, що може покращити адаптивність та гнучкість інформаційних систем за допомогою різноманітних засобів. Наприклад, за допомогою аналізу вимог бізнес-аналітики можуть виявити реальні потреби користувачів і забезпечити високу відповідність функціонального дизайну інформаційних систем бізнес-цілям.

У той же час оптимізація процесів може допомогти підприємствам переглянути існуючі робочі процеси, усунути надмірності та неефективність і, таким чином, покращити загальну продуктивність системи. Застосування технології візуалізації даних забезпечує інтуїтивно зрозумілу підтримку прийняття рішень для керівництва, допомагаючи їм робити швидкий та обґрунтований вибір у складному середовищі даних.

У цій публікації буде розглянуто конкретне застосування бізнес-аналітики в удосконаленні інформаційних систем, поглиблений аналіз того, як вона може підвищити продуктивність і адаптивність інформаційних систем за допомогою ряду практичних методів, щоб створити більшу цінність для підприємств.

За допомогою вивчення конкретних прикладів та теоретичного аналізу ця стаття має на меті надати потужну підтримку підприємствам для ефективного використання інформаційних систем у динамічному середовищі та сприяти їх постійному інноваційному розвитку та розвитку. У той же час в даній роботі також буде розглянута адаптивність бізнес-аналітики в різних галузях, досліджена її ефективність і гнучкість в конкретних ринкових умовах, з метою забезпечення теоретичної основи і практичного керівництва для майбутнього розвитку інформаційних систем, а також допомоги підприємствам в умовах жорсткої ринкової конкуренції в непереможному становищі [2].

Метою даної роботи є оптимізація продуктивності інформаційних систем на платформах електронної комерції (на прикладі Alibaba), особливо систем управління замовленнями та відстеження логістики, за рахунок застосування бізнес-аналізу. За допомогою методів аналізу на основі даних підприємства можуть підвищити свою конкурентоспроможність на ринку та підвищити загальну ефективність і зручність використання інформаційних систем.

Крім того, метою роботи є дослідження потенціалу застосування великих даних, штучного інтелекту та інших технологій в оптимізації корпоративних інформаційних систем, щоб допомогти підприємствам краще реагувати на швидкі зміни ринкового попиту.

Об'єктом даного дослідження є інформаційна система платформи електронної комерції, особливо система управління замовленнями і система відстеження логістики. Дослідження зосереджене на продуктивності цих систем у великомасштабній обробці даних та реагуванні в режимі реального часу.

У цьому документі Alibaba розглядається як приклад для вивчення того, як компанія вдосконалює свою інформаційну систему та підвищує операційну ефективність за допомогою методів та інструментів бізнес-аналізу.

Дослідження також охоплює користувачів платформи, процеси замовлень, управління запасами та інші елементи, пов'язані з системою [1–4].

Темою дослідження є підвищення продуктивності інформаційних систем на платформах електронної комерції за рахунок застосування методів бізнес-аналітики, особливо для оптимізації систем управління замовленнями та логістики. У роботі досліджуються, як технічні інструменти, такі як великі дані, штучний інтелект та машинне навчання, можуть бути використані для виявлення вузьких місць у системі шляхом аналізу даних про замовлення та логістику та пропонування цільових схем оптимізації. Дослідження включають шлях удосконалення інформаційних систем, вплив бізнес-аналітики на оптимізацію системи та практичне застосування нових технологій в інформаційних системах.

Завдяки цьому дослідженню були отримані наступні результати. Виявлено ключові вузькі місця в інформаційній системі платформи електронної комерції, особливо ефективність управління замовленнями та системи відстеження логістики в умовах роботи з високим навантаженням. У даній роботі представлений конкретний метод оптимізації процесу управління замовленнями за рахунок використання інструментів бізнес-аналізу, включаючи обробку потоків даних, застосування прогнозної моделі і схему автоматичного коригування ресурсів системи [7].

Шляхом експериментальної перевірки доведено, що після впровадження моделі машинного навчання значно поліпшується продуктивність системи в період пікового виконання замовлень, скорочується час обробки замовлень, підвищується точність відстеження логістики.

Результати цього дослідження надають реальний шлях оптимізації для платформ електронної комерції та демонструють ефект застосування великих даних та технології штучного інтелекту в реальних бізнес-сценаріях. Результати свідчать, що завдяки застосуванню інструментів та технологій бізнес-аналітики підприємства можуть значно покращити гнучкість, оперативність та масштабованість інформаційних систем, тим самим зберігаючи лідируючі позиції в умовах високої конкуренції на ринку [1–6].

Список використаних джерел

1. Девенпорт Т. Х. Штучний інтелект для реального світу. / Т. Х. Девенпорт Т. Х. Ронанкі // Harvard Business Review, 96(1). – 2018. – с. 108–116.
2. Чень Х. Бізнес-аналітика та аналітика: від великих даних до великого впливу / Х. Чен, Р. Х. Чіанг, В. С. Стопі // MIS Quarterly, 36 (4)). – 2012. –с. 1165–1188.
3. Делен Д., Деміркан Х. Дані, інформація та аналітика як послуги / Д. Делен, Х. Деміркан // Системи підтримки прийняття рішень, 55 (1) . – 2013. – с. 359–363.
4. Шмуелі Г. Прогнозна аналітика в дослідженнях інформаційних систем / Г. Шмуелі, О. Р. Коппіус // Квартальник МІС, 35(3) . – 2011. – с. 553–572.

5. Девенпорт Т. Х. Фахівець з обробки даних: найсексуальніша робота 21-го століття / Т. Х. Девенпорт, Д. Дж. Патіл // Harvard Business Review, 90 (10) . – 2012. – с. 70–76.

6. Уотсон Х. Дж. Підручник: Аналітика великих даних: концепції, технології та застосування / Х. Дж. Уотсон // Комунікації Асоціації інформаційних систем, 34). – 2014. –с. 1247–1268.

7. Мортенсон М. Дж. Оперативні дослідження від тейлоризму до терабайтів: дослідницька програма для аналітичної епохи / М. Дж. Мортенсон, Н. Ф. Доерті, С. Робінсон // Європейський журнал оперативних досліджень, 241 (3). – 2015. – с. 583–595.

8. Гартнер В. Б., Бізнес-моделі на основі даних для цифрової економіки / В. Б. Гартнер, К. Гейне // Журнал бізнес-моделей, 3 (2). – 2015. – с. 1-13.

9. Вікіпедія – вільна енциклопедія. Інформаційна система управління. URL : https://en.wikipedia.org/wiki/Management_information_system

10. Що таке інформаційні системи управління? URL : <https://www.mtu.edu/business/what-is-mis/>

УДК 621.317

Скорін Юрій

кандидат технічних наук, доцент

Харківський національний економічний університет ім. С. Кузнеця

Кондратьєв Олександр

студент

Харківський національний економічний університет ім. С. Кузнеця

РОЗРОБЛЕННЯ СИСТЕМИ АВТОМАТИЗОВАНОГО АНАЛІЗУ ВІДГУКІВ КОРИСТУВАЧІВ НА ОСНОВІ МЕТОДІВ ПРИРОДНОЇ МОВНОЇ ОБРОБКИ

Метою проведеного дослідження є розроблення системи автоматизованого аналізу відгуків користувачів на основі методів природної мовної обробки для виявлення тональності, ключових аспектів та тем. Об'єктом дослідження є процеси обробки та аналізу відгуків користувачів у цифровому середовищі. Предметом дослідження є методи та моделі природної мовної обробки для автоматизації аналізу текстових відгуків. Методи дослідження включають машинне навчання, глибокі нейронні мережі, статистичні методи аналізу тексту та методи оцінки якості моделей. Використовуються класичні алгоритми, нейромережеві моделі та трансформерні архітектури. Експериментально підтверджено статистичну значущість результатів та розроблено рекомендації щодо вибору моделей для різних сценаріїв. Результати дослідження можуть бути використані в електронній комерції, сервісних

компаніях, розробці програмного забезпечення, маркетингу та аналітиці для автоматизації аналізу відгуків та виявлення трендів у великих масивах текстових даних. Дослідження має на меті розроблення сучасного вебзастосунку для управління завданнями та проектами, що сприятиме оптимізації процесів проектного менеджменту, підвищенню ефективності командної роботи та прозорості виконання завдань. Об'єктом дослідження є: вебзастосунок для управління проектами, який підтримує автентифікацію, планування спринтів, управління задачами та учасниками. Предметом дослідження є: розроблення модулів для автентифікації користувачів, управління профілями, проектами, спринтами та задачами з використанням сучасних вебтехнологій. Метод проєктування – структурно-функціональний аналіз, компонентне моделювання, розроблення з використанням підходу серверного рендерингу компонентів. Було проведено аналіз предметної області, досліджено аналоги, визначено їх переваги та недоліки, створено концепцію застосунку та реалізовано його функціональність. Вебзастосунок підтримує реєстрацію та автентифікацію через email та соціальні мережі, багатофакторну автентифікацію, редагування профілів, створення та управління проектами, спринтами і задачами, також, головне, він може бути використаний командами для ефективного управління проектами.

У сучасному світі управління проектами є ключовим аспектом успішної діяльності організацій. Оптимізація процесів проектного менеджменту за допомогою сучасних технологій дозволяє підвищити ефективність командної роботи, забезпечити прозорість виконання завдань та досягти поставлених цілей у встановлені терміни.

Розроблення вебзастосунків для управління проектами стає дедалі актуальнішою, адже такі інструменти допомагають командам планувати, відстежувати та координувати свою діяльність у реальному часі. Метою дослідження є створення вебзастосунку для управління проектами, який надасть зручний та ефективний інструмент для організації командної роботи, планування спринтів, створення та відстеження задач, а також управління учасниками проєкту. Для реалізації цього проєкту використано сучасний технологічний стек: Typescript, Next.js для фронтенду, Supabase як бекенд-платформу. Робота включає аналіз існуючих рішень на ринку управління проектами для визначення їхніх переваг і недоліків, а також розробку та впровадження нових функцій, які покращать користувацький досвід і ефективність системи. Перед початком розробки було проведено планування: створено набір функціональних і нефункціональних вимог, розроблено логічну та фізичну моделі бази даних, а також UML-діаграми варіантів використання й активності. Для планування візуальної частини використано технологію Figma. Після реалізації застосунку буде проведено тестування для перевірки коректності виконання всіх функціональних вимог і відсутності помилок.

Основні функціональні можливості вебзастосунку включають: реєстрація та автентифікація: користувачі можуть створювати облікові записи через email або соціальні мережі, входити в систему та підключати багатофакторну автентифікацію для підвищення безпеки; управління профілем: можливість

редагувати особисті дані та аватар; створення та налаштування проєктів: користувачі можуть створювати проєкти, додавати логотипи, обирати тип проєкту та змінювати параметри; управління учасниками: власник проєкту може запрошувати нових учасників за email і видаляти існуючих; планування спринтів; створення спринтів із зазначенням цілі, опису, дат початку та завершення; управління задачами: створення, редагування, генерація опису задачі за допомоги мовної моделі, фільтрація та призначення задач у межах спринтів із параметрами: назва, опис, тип, статус, виконавець, оцінка часу.

Процес розроблення вебзастосунку для управління проєктами з метою оптимізації процесів проектного менеджменту передбачає створення комплексного рішення. Головні аспекти задачі включають розробку функціональності для організації командної роботи, планування спринтів, управління задачами та учасниками проєкту, а також забезпечення зручного та інтуїтивно зрозумілого інтерфейсу. Таким чином, мета вебзастосунку – надати командам простий та ефективний інструмент для управління проєктами, що сприятиме підвищенню продуктивності, прозорості виконання завдань та оптимізації робочих процесів. У сфері управління проєктами існує широкий вибір програмних інструментів, які допомагають командам ефективно планувати, виконувати та контролювати проєкти. Під час проведення дослідження було детально розглянуто такі популярні аналоги: Jira, Trello, Asana та Monday.com. Кожен із них має свої унікальні особливості, які відповідають різним потребам команд, типам проєктів і бюджетам. Було наведено розширені описи, включно з перевагами та недоліками. Вибір між цими інструментами залежить від потреб команди, складності проєктів і бюджету, а також від того, скільки часу ви готові витратити на їх освоєння. Оскільки всі функції вебзастосунку виконуються безпосередньо через браузер, користувачам не потрібно встановлювати додаткове програмне забезпечення на свої пристрої. Це значно спрощує процес впровадження та використання системи для управління завданнями та проєктами. Для початку роботи достатньо відкрити сучасний веббраузер, перейти за URL-адресою застосунку та дочекатися завантаження сторінки. Після цього користувач може одразу почати працювати з функціоналом, зокрема – створювати проєкти, формувати спринти, додавати задачі та призначати виконавців.

У рамках дослідження було розроблено сучасний веб застосунок Sprintly для управління проєктами, спрямований на оптимізацію процесів проектного менеджменту. Актуальність роботи зумовлена зростаючою потребою в ефективних інструментах для організації командної роботи, планування спринтів і управління задачами в умовах динамічного розвитку інформаційних технологій та ІТ-галузі. Розроблений застосунок відповідає сучасним вимогам до комп'ютерних інформаційних систем, забезпечуючи гнучкість, прозорість і автоматизацію рутинних процесів. Практична проведення дослідження полягає в можливості впровадження розробленого застосунку в ІТ-компаніях, стартапах, освітніх установах та інших організаціях, які потребують ефективного управління проєктами. Застосунок дозволяє підвищити прозорість командної роботи, оптимізувати планування спринтів і задач, а також зменшити

час на виконання рутинних операцій завдяки автоматизації. Результати тестування функціональних вимог підтвердили працездатність і відповідність системи специфікаціям, що засвідчує її готовність до практичного використання. У подальших дослідженнях планується розширення функціональних можливостей застосунку, зокрема додавання аналітичних звітів, інтеграція з інструментами штучного інтелекту для прогнозування термінів виконання задач і підтримка багатомовного інтерфейсу.

Список використаних джерел

1. Кондратьєв Олександр. Розроблення вебзастосунку для управління завданнями та проєктами з метою оптимізації процесів проєктного менеджменту / О. Кондратьєв // Матеріали Міжнародної науково-практичної конференції молодих учених, аспірантів та студентів “Інформаційні технології в сучасному світі: дослідження молодих вчених”: тези доповідей, 27–28 лютого 2025 р. – Х. : ХНЕУ імені Семена Кузнеця, 2025. – с. 4.2.
2. Як створити бекенд за допомогою Supabase [Електронний ресурс] / Академія кодування // YouTube. codeacademyua. – Електрон. відеодан. – Режим доступу : https://www.youtube.com/watch?v=ae2Eaz_zEqQ
3. Project Management Institute – Learn about project management standards and certifications [Електронний ресурс] // PMI. – Режим доступу : <https://www.pmi.org> .

УДК 621.317

Скорін Юрій

кандидат технічних наук, доцент

Харківський національний економічний університет ім. С. Кузнеця

Лактіонов Артем

студент

Харківський національний економічний університет ім. С. Кузнеця

ГІБРИДНІ МЕТОДИ ШИФРУВАННЯ У БЛОКЧЕЙН-МЕРЕЖАХ

Метою проведеного дослідження є впровадження гібридних методів шифрування для забезпечення конфіденційності, цілісності та автентичності переданих даних у блокчейн-мережах. Було проаналізовано сучасні криптографічні алгоритми, виявлено їхні переваги та недоліки, а також запропоновано гібридну схему, яка поєднує симетричне та асиметричне шифрування. Об'єктом дослідження є процес обміну даними між учасниками блокчейн-мережі. Предметом дослідження є криптографічні методи, орієнтовані на підвищення безпеки передачі інформації. Було проведено аналіз криптографічних ризиків, виявлено типові вразливості передачі даних у публічних блокчейнах, зокрема при обміні ключами та передачі конфіденційної інформації до або поза межами мережевого консенсусу. Результатом

проведеного дослідження є розроблення рішення захищеного каналу передачі даних з використанням гібридного шифрування, що адаптований до особливостей блокчейн-середовища.

У сучасних інформаційних системах питання, які пов'язані з забезпеченням кібербезпеки набуває ключового значення. Зі зростанням обсягів цифрових транзакцій, популярністю децентралізованих застосунків та використанням блокчейн-технологій у різних сферах (логістика, фінанси, охорона здоров'я, ідентифікація тощо) зростає і потреба в надійних методах захисту переданої інформації. Хоча сам блокчейн забезпечує цілісність і незмінність записів у розподіленому реєстрі, він не гарантує повної конфіденційності та автентичності переданих даних, особливо в каналах взаємодії між користувачами або вузлами мережі. Передавання інформації в блокчейн-середовищах часто відбувається без додаткових рівнів шифрування або з використанням застарілих алгоритмів. Це створює загрозу перехоплення, несанкціонованого доступу або навіть модифікації критично важливої інформації. Використання лише симетричних або лише асиметричних алгоритмів не завжди є ефективним через компроміс між продуктивністю та рівнем безпеки. Одним із перспективних напрямів вирішення цих проблем є впровадження гібридних методів шифрування, які поєднують переваги симетричних (висока швидкодія) та асиметричних (безпечний обмін ключами) криптографічних систем. Такий підхід дозволяє забезпечити як швидке кодування інформації, так і захищений обмін ключовими параметрами, що особливо актуально у відкритих або частково відкритих блокчейн-мережах.

Метою проведеного дослідження є обґрунтування та розроблення гібридної криптографічної схеми, адаптованої для захищеного передавання даних у блокчейн-мережах. Об'єктом дослідження є процес передавання цифрових даних у децентралізованих обчислювальних системах. Предметом дослідження виступають методи симетричного та асиметричного шифрування, їх комбіноване застосування в умовах розподіленого середовища. У якості методів дослідження задіяні такі методи, як теоретичний аналіз криптографічних протоколів, моделювання процесів шифрування, проектування захищених схем, експериментальна оцінка продуктивності. Практичне значення проведеного дослідження полягає у поєднанні сучасних криптографічних підходів в одну ефективну гібридну модель, що враховує особливості функціонування блокчейн-мереж.

У сучасному інформаційному просторі блокчейн-технології активно впроваджуються в різноманітні галузі – від фінансового сектора й логістики до освіти, охорони здоров'я та державного управління. Основною перевагою блокчейну є забезпечення цілісності, прозорості та незмінності інформації, що зберігається у розподіленому реєстрі. Водночас, попри поширену думку про високий рівень безпеки децентралізованих систем, блокчейн сам по собі не забезпечує повноцінного захисту переданої інформації, особливо на рівні комунікації між учасниками мережі. Актуальними залишаються загрози, властиві класичним комп'ютерним мережам: атаки типу «людина посередині», які дозволяють втручатися у передавання даних між вузлами; підміна

транзакцій або маніпуляція з вмістом до моменту їхнього включення у блок; перехоплення приватної інформації у процесі створення, підписання чи передачі транзакцій; експлуатація слабких або застарілих алгоритмів криптографії, що не відповідають сучасним стандартам. Крім того, у блокчейн-мережах часто використовуються відкриті ключі для ідентифікації користувачів, тоді як відповідні приватні ключі зберігаються локально. Втрата чи компрометація приватного ключа призводить до безповоротної втрати доступу або повного контролю над обліковим записом, що підтверджує необхідність додаткових рівнів захисту. Особливої уваги вимагає проблема конфіденційності у блокчейн-середовищах. Наприклад, у фінансових додатках або децентралізованих біржах транзакції містять дані про суми, адреси сторін, хеші контрактів тощо. Якщо така інформація буде доступною стороннім особам, це може призвести до витоку комерційної або персональної інформації. Низка досліджень показує, що частина блокчейн-застосунків (особливо у сфері охорони здоров'я, цифрової ідентифікації, корпоративного документообігу) потребує не лише збереження цілісності даних, а й забезпечення їхньої конфіденційності. Однак стандартні механізми більшості публічних блокчейн-платформ цього не передбачають. У той час як протоколи рівня TLS або HTTPS забезпечують захист каналу у класичних мережах, у блокчейні подібний захист має бути реалізований самостійно, на рівні застосунку або через спеціалізовані криптографічні схеми. Одним із можливих рішень для підвищення безпеки передачі інформації у таких мережах є застосування гібридного шифрування. Воно дозволяє забезпечити шифрування самого вмісту повідомлення за допомогою симетричних алгоритмів (наприклад, AES), а також здійснити захищений обмін ключами за допомогою асиметричних алгоритмів (наприклад, ECC або RSA). Такий підхід забезпечує не лише конфіденційність і автентичність, а й підвищує ефективність у децентралізованих мережах з великою кількістю учасників.

Таким чином, попри сильні сторони блокчейн-архітектури у забезпеченні незмінності й верифікованості інформації, уразливості, пов'язані з конфіденційністю та захищеністю каналів передачі даних, залишаються актуальними. Це формує необхідність впровадження додаткових криптографічних засобів – зокрема, гібридних методів шифрування, що дозволяють комплексно підвищити рівень інформаційної безпеки в блокчейн-мережах. В умовах швидкого розвитку децентралізованих технологій зростає потреба в оцінці не лише функціональної, але й прикладної ефективності засобів захисту інформації. Для блокчейн-систем, де кожна транзакція є публічною, а структура мережі не передбачає централізованих елементів безпеки, надзвичайно важливою є здатність обраної криптографічної моделі забезпечувати надійний захист переданої інформації без шкоди для продуктивності, доступності та сумісності з наявними протоколами.

У зв'язку з цим доцільно провести комплексний аналіз ефективності гібридної моделі шифрування, яка була досліджена у попередніх розділах, та визначити її переваги, обмеження і перспективи використання в сучасних блокчейн-інфраструктурах. Аналіз показав, що найбільш ресурсоемними

етапами є генерація асиметричних ключів та обчислення спільного секрету, що очікувано. Проте загальна затримка залишається в межах допустимого навіть для інтерактивних DApp або мобільних застосунків. Було проведено порівняння гібридної моделі з іншими методами, які використовуються у криптографії (тільки симетричне або тільки асиметричне шифрування), за ключовими параметрами. Ці результати підтверджують, що гібридна модель забезпечує найкращий баланс між безпекою і продуктивністю, особливо в умовах, де необхідно забезпечити захищений обмін ключами та цілісність повідомлень у відкритій децентралізованій мережі.

У результаті тестування, порівняння та аналітичного аналізу було підтверджено, що гібридна криптографічна модель має високу практичну цінність у контексті підвищення інформаційної безпеки передачі даних у блокчейн-мережах. Вона демонструє ефективну комбінацію криптографічної надійності, продуктивності, гнучкості впровадження та відповідності майбутнім викликам (зокрема квантовим загрозам).

У ході виконання курсової роботи було проведено комплексне дослідження гібридних методів шифрування та їх застосування для забезпечення захисту інформації у блокчейн-середовищах. Метою роботи було дослідити принципи побудови та функціонування гібридних криптографічних систем, проаналізувати їхні переваги у порівнянні з традиційними методами шифрування, а також оцінити доцільність та ефективність їх інтеграції в інфраструктуру блокчейн-технологій. На основі проведеного теоретичного аналізу було встановлено, що гібридна криптографія поєднує у собі сильні сторони як симетричних, так і асиметричних методів шифрування: високу швидкість симетричних алгоритмів (зокрема AES) та безпечну передачу ключів, яку забезпечують асиметричні алгоритми (наприклад, ECC). Така комбінація дозволяє досягти оптимального балансу між продуктивністю та безпекою в умовах децентралізованих мереж. У практичній частині було проаналізовано інструментальні засоби реалізації гібридного шифрування, зокрема бібліотеку PyCryptodome, яка продемонструвала високу функціональність та відповідність сучасним вимогам інформаційної безпеки. Було змодельовано сценарії шифрування, обміну ключами, верифікації цілісності повідомлень та проведено аналіз продуктивності алгоритмів.

Результати дослідження продемонстрували високу ефективність обраної криптографічної моделі: низькі затримки при шифруванні й дешифруванні, підтримка сучасних стандартів, придатність до масштабування та захист від основних типів атак (включно з MITM та аналізом трафіку). Порівняльна оцінка також підтвердила переваги гібридної моделі перед класичними підходами. Таким чином, отримані результати є основою для розробки практичних рішень у сфері безпечного передавання даних у Web3-системах, децентралізованих застосунках та цифрових екосистемах нового покоління.

Список використаних джерел

1. ДСТУ 3008:2015 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ : ДП УкрНДНЦ, 2015. – 28 с.
2. ДСТУ 3582:2013. Інформація та документація. Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила (ISO 4:1984, NEQ; ISO 832:1994, NEQ) / Нац. стандарт України. – Київ : Мінекономрозвитку України, 2014. – 18 с.
3. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання / Нац. стандарт України. – Київ : ДП «УкрНДНЦ», 2016. – 18 с.
4. Шифрування. Типи і алгоритми [Електронний ресурс]. – Режим доступу: <https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/>.
5. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються [Електронний ресурс]. – Режим досутпу: <https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/>.
6. Порівняння симетричного і асиметричного шифрування [Електронний ресурс]. – Режим досутпу: <https://exbase.io/uk/wiki/simetrichne-i-asimetrichne-shifruvannya>.

УДК 621.317

Скорін Юрій

кандидат технічних наук, доцент

Харківський національний економічний університет ім. С. Кузнеця

Лук'янчук Софія

студентка

Харківський національний економічний університет ім. С. Кузнеця

ШТУЧНИЙ ІНТЕЛЕКТ В СИСТЕМАХ УПРАВЛІННЯ ФІНАНСОВИМИ РИЗИКАМИ

Метою проведеного дослідження є застосування штучного інтелекту в автоматизованих системах управління фінансовими ризиками з метою підвищення точності, оперативності та ефективності прийняття управлінських рішень у фінансовій сфері. У межах дослідження розроблено модель прогнозування кредитного ризику клієнтів банку, яка дозволяє здійснювати оцінку платоспроможності на основі історичних даних та сучасних методів машинного навчання. Об'єктом дослідження є автоматизовані системи управління фінансовими ризиками, які функціонують у банківському та фінансовому секторі. Предметом дослідження виступають алгоритми та моделі штучного інтелекту, які можуть бути інтегровані до автоматизованих систем управління фінансовими ризиками з метою підвищення точності прогнозів та

виявлення ризикових клієнтів. Методом дослідження є моделювання за допомогою інструментів машинного навчання, зокрема нейронних мереж і методів ансамблевого навчання. Результатом дослідження є створення ефективної моделі прогнозування кредитного ризику, яка демонструє високий рівень точності класифікації та здатність до адаптації при зміні вхідних умов.

Управління фінансовими ризиками є ключовим напрямком у діяльності фінансових установ, банків та корпорацій. У сучасних умовах динамічного розвитку ринків і високої конкуренції автоматизовані системи управління фінансовими ризиками (АСУ ФР) стали невід'ємною складовою, що забезпечує збір, обробку та аналіз великих обсягів даних для своєчасного виявлення потенційних загроз та прийняття рішень.

Ці системи інтегрують різноманітні інструменти і технології, зокрема методи статистичного аналізу та моделювання, а також новітні інтелектуальні підходи. В останні роки значну увагу приділяють застосуванню алгоритмів штучного інтелекту (ШІ), які здатні підвищити точність прогнозів та адаптивність систем до мінливих умов. Структурно АСУ ФР складаються з модулів збору даних, аналітичних інструментів, систем підтримки прийняття рішень і модулів моніторингу та контролю [1].

Таким чином, фінансові ризики являють собою комплексне явище, що охоплює різні види та джерела невизначеності, і їх управління вимагає застосування інтегрованих підходів, у тому числі із залученням сучасних автоматизованих систем та технологій штучного інтелекту для підвищення якості аналізу і прогнозування ризикових факторів. Управління фінансовими ризиками також потребує застосування систем підтримки прийняття рішень на основі штучного інтелекту, які інтегрують аналітику в режимі реального часу, моделюють різні сценарії розвитку подій та формують рекомендації для керівництва. Отже, технології штучного інтелекту у фінансовій сфері створюють нові можливості для підвищення ефективності управління фінансовими ризиками, автоматизації аналітичних процесів і адаптивного реагування на зовнішні та внутрішні загрози, що підтверджує їх важливу роль у сучасних автоматизованих системах управління. Застосування сучасних технологій у фінансовому секторі дає можливість значно знижувати різні ризики, оптимізувати процеси та підвищити ефективність роботи установ.

Управління фінансовими ризиками традиційно передбачає оцінку ризиків, їх моніторинг та прийняття відповідних управлінських рішень. ШІ дозволяє суттєво вдосконалити ці процеси за рахунок автоматизації рутинних завдань, підвищення точності прогнозів і зниження суб'єктивності оцінок. Наприклад, на основі історичних даних моделі машинного навчання можуть виявляти складні залежності між змінними, що впливають на кредитний, ринковий або операційний ризик.

Ключова перевага ШІ в управлінні ризиками – здатність адаптуватися до змінних умов ринку. Традиційні моделі зазвичай мають фіксовану структуру та обмежені можливості оновлення. Натомість ШІ-системи здатні самонавчатися на нових даних, що робить їх особливо ефективними у динамічному середовищі. Окрім того, завдяки інтеграції з цифровими платформами ШІ може

працювати в режимі реального часу, що значно покращує швидкість реакції на потенційні загрози.

У сфері фінансового аналізу ШІ також виконує роль аналітичного інструменту для побудови моделей прогнозування, аналізу сценаріїв, виявлення шахрайських операцій та підвищення загального рівня безпеки фінансової системи. Особливо важливим є використання пояснюваних моделей (Explainable AI), які дозволяють отримати не лише результат, а й зрозуміти логіку прийняття рішень, що є критичним для фінансових інституцій, які працюють у суворо регульованому середовищі.

Загалом, роль ШІ в управлінні ризиками полягає в оптимізації процесів виявлення, оцінювання та реагування на фінансові загрози. Використання інтелектуальних алгоритмів дозволяє скоротити час прийняття рішень, мінімізувати вплив людського фактору та підвищити ефективність системи управління ризиками. У рамках дослідження було реалізовано практичний кейс побудови моделі прогнозування кредитного ризику клієнтів банку. Основною метою є створення інтелектуальної системи класифікації, здатної визначати, чи буде клієнт у майбутньому здатен своєчасно обслуговувати кредит. Така система дозволяє банку зменшити ймовірність втрат через неповернення позик, підвищити ефективність управління ризиками та приймати обґрунтовані кредитні рішення. Для моделювання було використано відкритий датасет з платформи Kaggle – Home Credit Default Risk. Цей набір даних містить понад 300 000 записів про клієнтів з різними характеристиками, такими як вік, рівень доходу, кількість утриманців, кредитна історія, тип житла, працевлаштування, тощо. Було здійснено очищення й трансформацію даних. Було виявлено й видалено значну кількість пропущених значень у категоріях, де заповнення не є доцільним. Числові ознаки було нормалізовано за допомогою міні-макс масштабу. Категоріальні змінні закодовано методом one-hot encoding для сумісності з алгоритмами машинного навчання. Також проведено балансування вибірки методом SMOTE для усунення дисбалансу між класами (платоспроможні та неплатоспроможні клієнти).

У дослідження були проаналізовані можливості, переваги та виклики застосування штучного інтелекту в автоматизованих системах управління фінансовими ризиками. Був проведений аналіз теоретичних засад, класифікації фінансових ризиків, технічних особливостей реалізації інтелектуальних систем, а також практичного моделювання на прикладі прогнозування кредитного ризику. Розглянуто загальні підходи до управління фінансовими ризиками, визначено їх класифікацію та особливості у сучасних економічних умовах. Було проаналізовано основні принципи побудови АСУ та обґрунтовано доцільність впровадження інтелектуальних методів, зокрема машинного навчання та нейронних мереж, у фінансову аналітику. Проведено аналіз сучасних методів штучного інтелекту, які застосовуються для аналізу й прогнозування ризиків. Розглянуто особливості моделей глибокого навчання, дерев рішень, ансамблевих методів, а також критерії оцінки їх ефективності. Особливу увагу приділено питанням інтерпретованості моделей, що є важливим фактором для впровадження ШІ у практику управління ризиками відповідно до регуляторних

вимог. Реалізовано практичний кейс із побудови моделі прогнозування кредитного ризику клієнта банку. Проведено попередню обробку реальних даних, побудовано та протестовано кілька моделей, здійснено оцінку точності за допомогою метрик. Здійснено аналіз важливості ознак за допомогою SHAP-графіків та обґрунтовано архітектуру системи, що може бути використана для інтеграції такої моделі в практичну автоматизовану систему управління фінансовими ризиками. Загалом, результати дослідження підтверджують високу ефективність використання методів штучного інтелекту для автоматизованого аналізу та прогнозування фінансових ризиків. Такі моделі здатні не лише підвищити точність виявлення ризиків, а й забезпечити оперативність прийняття рішень у фінансових установах. Разом з тим, їх впровадження потребує належної технічної та організаційної підтримки, включно з питаннями інтерпретованості, валідації та адаптації до змін ринкового середовища.

Список використаних джерел

1. Мінцифра. Концепція розвитку ІІІ в Україні [Електронний ресурс]. – Режим доступу: <https://thedigital.gov.ua>.
2. Боровик О.І. Основи машинного навчання. : навч. посіб. / О.І. Боровик. – Київ : КНУ, 2020. – 214 с.
3. Григорук П.М. Інтелектуальні інформаційні системи. : підручник / П.М. Григорук. – Львів : ЛНУ, 2019. – 312 с.
4. Зимогляд О.О. Аналіз фінансових ризиків: монографія / О.О. Зимогляд. – Київ : КНЕУ, 2021. – 186 с.

УДК 621.317

Скорін Юрій

кандидат технічних наук, доцент

Харківський національний економічний університет ім. С. Кузнеця

Петренко Богдан

студент

Харківський національний економічний університет ім. С. Кузнеця

ПРИРОДНА МОВНА ОБРОБКА ДЛЯ АНАЛІЗУ ВІДГУКІВ КОРИСТУВАЧІВ

Метою проведеного дослідження є розроблення системи автоматизованого аналізу відгуків користувачів на основі методів природної мовної обробки для виявлення тональності, ключових аспектів та тем. Об'єктом дослідження є процеси обробки та аналізу відгуків користувачів у цифровому середовищі. Предметом дослідження є методи та моделі природної мовної обробки для автоматизації аналізу текстових відгуків. Методи дослідження

включають машинне навчання, глибинні нейронні мережі, статистичні методи аналізу тексту та методи оцінки якості моделей. Використовуються класичні алгоритми, нейромережеві моделі та трансформерні архітектури. Експериментально підтверджено статистичну значущість результатів та розроблено рекомендації щодо вибору моделей для різних сценаріїв. Результати дослідження можуть бути використані в електронній комерції, сервісних компаніях, розробці програмного забезпечення, маркетингу та аналітиці для автоматизації аналізу відгуків та виявлення трендів у великих масивах текстових даних.

У сучасному цифровому світі аналіз користувацьких відгуків став критичним елементом для будь-якого бізнесу, що прагне підвищити якість своїх продуктів та послуг. Однак, масштаб та неструктурований характер цих даних створюють значні виклики для традиційного аналізу. Основна проблема, що вирішується в даному дослідженні, полягає у неефективності та обмеженості ручного аналізу великих обсягів текстових відгуків користувачів. Ця проблема має кілька важливих аспектів:

1. Експоненційне зростання обсягів даних.
2. Суб'єктивність та неконсистентність аналізу.
3. Критичні часові затрати.
4. Обмежені можливості виявлення прихованих закономірностей.
5. Зростаюча складність багатомовного аналізу.
6. Відсутність стандартизації та суб'єктивність оцінок.
7. Зростаючі витрати на аналітику відгуків.

У сучасному цифровому ландшафті обсяг текстових даних, що генеруються користувачами продуктів і послуг, стрімко зростає. Зокрема, відгуки користувачів стали невід'ємним елементом сучасної бізнес-екосистеми. Здатність ефективно аналізувати ці відгуки стала критичним фактором успіху для компаній, що прагнуть залишатися конкурентоспроможними. Традиційні методи аналізу відгуків, що базуються на ручній обробці, стикаються з багатьма обмеженнями. Аналітики можуть ефективно обробляти лише обмежену кількість текстів, а суб'єктивність людської інтерпретації призводить до неконсистентності результатів. Більше того, людські ресурси часто зосереджуються на найновіших відгуках, зовсім залишаючи поза увагою історичні дані, які могли б виявити довгострокові тенденції. З точки зору бізнесу, відгуки користувачів містять безцінну інформацію про: сильні та слабкі сторони продукту чи послуги; очікування та потреби клієнтів; порівняння з конкурентами; ідеї для вдосконалення та інновацій; проблеми, що потребують негайного вирішення. Однак вилучення цієї інформації з великого масиву неструктурованих текстових даних залишається складним завданням. Саме тут на допомогу приходять технології природної мовної обробки (NLP). NLP – це міждисциплінарна галузь, що об'єднує комп'ютерні науки, штучний інтелект та лінгвістику для забезпечення взаємодії між комп'ютерами та людською мовою. Застосування NLP для аналізу відгуків користувачів представляє собою комплексне завдання, яке включає ряд підзадач: попередня обробка тексту (токенізація, лематизація, видалення стоп-слів); виявлення тональності

(sentiment analysis); виокремлення ключових аспектів та тем; класифікація відгуків за різними категоріями; виявлення емоційного забарвлення; узагальнення та генерація звітів. Ці завдання вимагають застосування різних моделей та алгоритмів – від класичних статистичних методів до сучасних підходів глибинного навчання з використанням трансформерів та великих мовних моделей (LLM). Для вирішення поставлених завдань буде використано комплексний методологічний підхід, який поєднує методи машинного навчання, глибинного навчання, обробки природної мови та аналізу даних.

Дослідження буде проводитися в кілька етапів:

1. Аналітичний етап.
2. Етап проектування та розробки.
3. Експериментальний етап.
4. Аналітико-узагальнюючий етап.

Проведене дослідження щодо застосування природної мовної обробки для автоматизації аналізу відгуків користувачів дозволило отримати комплексне уявлення про ефективність, переваги та обмеження різних методів і моделей NLP у вирішенні цього завдання. У результаті дослідження були досягнуті всі поставлені цілі та виконані завдання, що дозволило сформулювати такі висновки: аналіз сучасного стану проблематики підтвердив критичну важливість автоматизації аналізу відгуків користувачів у контексті постійного зростання обсягів текстових даних. Традиційний ручний аналіз стикається з фундаментальними обмеженнями, пов'язаними з часовими затратами, суб'єктивністю оцінок та неможливістю ефективної обробки великих масивів даних. Ці обмеження особливо гостро проявляються в умовах глобалізації бізнесу, коли компанії отримують відгуки різними мовами та з різних джерел.

Теоретичне дослідження методів природної мовної обробки продемонструвало еволюцію підходів до аналізу тексту – від простих словникових методів до складних трансформерних архітектур. Кожен з цих підходів має свої переваги та обмеження, і вибір конкретного методу залежить від специфіки завдання, доступних обчислювальних ресурсів та вимог до точності й швидкості аналізу. На основі експериментального дослідження було встановлено, що трансформерні моделі, забезпечують найвищу точність для аналізу тональності відгуків, значно перевершуючи класичні методи, такі. Встановлено, що ефективність усіх моделей суттєво залежить від специфіки домену та якості попередньої обробки даних. Доменна адаптація та донавчання на специфічних корпусах даних значно підвищують точність аналізу, особливо для спеціалізованих галузей з власною термінологією. Економічна ефективність впровадження систем автоматизованого аналізу відгуків підтверджується значним скороченням часових та людських ресурсів, необхідних для обробки відгуків, а також підвищенням якості отриманих інсайтів, що дозволяє компаніям приймати більш обґрунтовані рішення щодо розвитку продуктів та послуг. Практичне значення отриманих результатів полягає в можливості їх використання для створення ефективних систем автоматизованого аналізу відгуків користувачів, які можуть бути інтегровані в бізнес-процеси компаній різного масштабу та галузей. Такі системи дозволяють не лише скоротити

витрати на аналіз відгуків, але й отримати глибші й об'єктивніші інсайти щодо сприйняття продуктів та послуг користувачами, виявити приховані тренди та закономірності, а також оперативно реагувати на критичні проблеми. Таким чином, проведене дослідження робить значний внесок у розвиток методів автоматизації аналізу відгуків користувачів на основі природної мовної обробки та створює основу для подальшого вдосконалення таких систем.

Список використаних джерел

1. Stanford Sentiment Treebank [Електронний ресурс] // Stanford NLP Group. 2023. – Access mode : <https://nlp.stanford.edu/sentiment/>.
2. State of AI Report 2023 [Електронний ресурс] // State of AI. 2023. Access mode : <https://www.stateof.ai/>.
3. TensorFlow Documentation [Електронний ресурс] // Google. 2024. Access mode : https://www.tensorflow.org/api_docs.

УДК 621.317

Скорін Юрій

кандидат технічних наук, доцент

Харківський національний економічний університет ім. С. Кузнеця

Симонович Станислав

студент

Харківський національний економічний університет ім. С. Кузнеця

СИСТЕМА КЕРУВАННЯ ЗМІСТОМ WORDPRESS

Метою проведеного дослідження є визначення оптимальних підходів до впровадження системи WordPress, що не лише публікує контент, а й виконує роль інструмента для автоматизації ключових бізнес-процесів. Об'єктом дослідження є процес упровадження WordPress в якості інструмента для здійснення автоматизації бізнес-процесів у середовищі малих та середніх підприємств, що потребують оптимізації роботи. Предметом дослідження є комплекс методів і засобів, які дають змогу реалізувати процес автоматизації, починаючи від внутрішніх механізмів WordPress та де яких розширень і закінчуючи інтеграціями зі сторонніми сервісами обробки даних.

Проведений аналіз свідчить, що дедалі більше підприємств прагнуть спростити та прискорити виконання щоденних завдань, аби виділити більше часу на стратегічний розвиток. У цьому контексті WordPress вже давно перестав бути суто блог-платформою – він може стати основою для побудови повноцінної інформаційної системи, що здатна автоматизувати чимало бізнес-процесів [1].

По-перше, WordPress має відкритий код і безліч плагінів, які можна гнучко налаштовувати під власні потреби. По-друге, величезна спільнота

розробників постійно створює новий інструментарій, що робе рутинні операції, від розсилки електронних листів до формування аналітичних звітів, майже непомітними для кінцевого користувача [2].

Та попри всі переваги, деякі компанії досі недооцінюють роль WordPress у бізнес-процесах. Здебільшого це трапляється через застарілий підхід до ІТ-систем, коли веб-сайт сприймається лише як візитка, а внутрішні процедури автоматизують за допомогою кошовного програмного забезпечення від сторонніх розробників. Отож одним із пріоритетів проведеного дослідження є саме аналіз того, як саме WordPress з його екосистемою плагінів може допомогти компаніям уникнути зайвих витрат і водночас збільшити ефективність роботи [2].

Найважливішим у цьому підході є швидкість і простота побудови робочої системи. WordPress, завдяки своїй гнучкості, дозволяє буквально за кілька кліків додати плагін, що запустить розсилку клієнтам щойно вони оформлять замовлення чи залишать заявку. Під час вдалого поєднання з сервісами, наприклад, Zapier можна налаштувати синхронізацію з Google Таблицями або навіть власними CRM-системами. Звісно, тут важливо звертати увагу на сумісність версій та оптимізацію бази, щоб уникнути конфліктів плагінів і надмірного навантаження на сервер. Але, автоматизація бізнес-процесів – це завжди пошук балансу між функціональністю та безпекою. Коли компанія починає використовувати WordPress не тільки для блогу, а й для зберігання даних про замовлення, платежі та внутрішні документи, загроза кібератак стає серйознішою. Тому без розуміння основ інформаційної безпеки не обійтись. Тут може знадобитися аудит плагінів, встановлення SSL-сертифікатів, регулярні оновлення та резервне копіювання. З іншого боку, грамотна організація користувацьких ролей і обмежень доступу підвищує захищеність системи без шкоди для гнучкості [3].

Розглянемо види контенту:

Статичний контент – це контент, який зберігається у файлі. Щоб змінити такий контент знадобиться редагувати на пряму файл в якому він знаходиться. До переваг статичного контенту можна віднести такі: статичний контент підходить для складних веб-сайтів, які потребують великої кількості функціональності: перевага тут у тому, що можна впливати на все, що захочеться, можна створити свою власну платформу на основі систем управління контентом (CMS); традиційний HTML – це те, де кожен раз потрібно робити це самому: при написанні коду можна використовувати уяву, щоб створити все, що хочеться реалізувати на своєму веб-сайті. До недоліків статичного контенту відносяться: якщо потрібно щось змінити на «серверній частині» веб-сайту, слід перебувати за своїм комп'ютером в середовищі розробки, щоб внести зміни; можна створити власне програмне забезпечення на основі CMS зі статичним HTML, а потім використовувати свої системи управління контентом для редагування контенту сайту з будь-якого місця. Однак такий крок вимагатиме значного часу і роботи, не говорячи вже про значні технічні знання в області кодування.

На відміну від попереднього, динамічний контент – це контент, який знаходиться в базі даних. З бази даних він напряму виводиться користувачеві на сторінку браузера. Для роботи з динамічним контентом часто використовують CMS. До переваг динамічного контенту з CMS віднесемо наступне: можна часто міняти контент; установка виконується дуже швидко і легко; особливих технічних знань в області кодування не потрібно: всі інструменти для додавання тексту, зображень або відео, а також для створення нових сторінок або підлеглих надано всередині самої платформи; більшість платформ мають вбудовану систему безпеки; доступні різні шаблони, які можна змінити відповідно до своїх потреб; більшість шаблонів вже адаптивні; у систему легко додати сторонні плагіни, такі як слайдери банерів, галереї зображень, інструменти SEO і системи електронної комерції; можна управляти своїм контентом з будь-якого комп'ютера в будь-якому місці, де є інтернет; для завантаження вмісту в Інтернет не потрібне програмне забезпечення FTP; гарний зв'язок з пошуковими мережами; блоги вже вбудовані і готові до роботи. До недоліків динамічного контенту слід віднести: CMS вимагає більше пам'яті, потужності процесора і обслуговування програмного забезпечення, ніж її конкуренти HTML, невеликі зміни налаштувань на сервері можуть призвести до збою всього сайту; деякі шаблони погано закодовані; створювати величезний і складний веб-сайт з системою управління контентом – не найкраща ідея: наприклад, такий сайт, як amazon.com, має досить складний, великий дизайн, який неможливо було б створити за допомогою платформ на основі CMS. Краще його створювати з нуля, використовуючи власний HTML і інші мови програмування.

Однією із систем управління контентом з відкритим вихідним кодом, яка спрощує створення і управління веб-сайтом. Це WordPress, яка є однією з найпопулярніших CMS в світі. Люди щодня використовують WordPress для підтримки своєї присутності в Інтернеті. WordPress має однією з переваг безкоштовне використання: немає ніяких зборів за установку або річних витрат, крім хостингу. Програмне забезпечення з відкритим вихідним кодом не схоже на інші матеріальні продукти, оскільки жодна компанія або приватна особа не володіє WordPress. З цієї причини його підтримка, підтримка і розвиток повністю залежать від волонтерів. WordPress надає власникам повну можливість створювати, публікувати і управляти своїм контентом. Завдяки простому інтерфейсу WordPress ідеально підходить для користувачів, яким зручніше працювати з текстовими редакторами, ніж з програмами FTP та написаними вручну веб-сторінками. Розробники опублікували тисячі плагінів і віджетів WordPress, які дозволяють створювати дійсно якісний сайт. WordPress дає велику кількість можливостей розробнику. В основі роботи WordPress лежить добре налагоджена зв'язок між ядром і базою. Це легко можна використовувати саме у свою користь. Також WordPress редактор Gutenberg – плагін, який в останніх версіях WordPress вже вбудований в нього, дозволяє візуально і без застосування коду змінювати вміст сторінок і постів. WordPress має дуже велику базу плагінів, створених звичайними людьми, частина з них платні, але є і безкоштовні. Ми використовували безкоштовний плагін з

можливістю розширення функціоналу після оплати. Впровадження WordPress як системи для автоматизації бізнес-процесів здатне позитивно вплинути на швидкість і якість роботи підприємства, знизити витрати й дати змогу персоналу зосередитися на важливіших завданнях. У проведеному дослідженні увагу буде приділено і технічним аспектам, і питанню адаптації нового робочого процесу в колективі, адже без розуміння людського фактору автоматизація може виявитися безрезультатною. Результати проведених досліджень напевно допоможуть розробникам і власникам компаній отримати практичні рекомендації та уникнути прикрих помилок на шляху переходу до «розумної» IT-інфраструктури.

Список використаних джерел

1. WordPress Developer Handbook [Електронний ресурс]. – Режим доступу : <https://developer.wordpress.org/>.
2. WooCommerce Docs [Електронний ресурс]. – Режим доступу : <https://woocommerce.com/documentation/>.
3. Zapier. How to Connect WordPress to Your Other Apps [Електронний ресурс]. – Режим доступу : <https://zapier.com/apps/wordpress/integrations>.
4. WPBeginner. How to Automate Your WordPress Site [Електронний ресурс]. – Режим доступу : <https://www.wpbeginner.com/showcase/best-wordpress-automation-tools-and-plugins/>.

УДК 621.317

Скорін Юрій

кандидат технічних наук, доцент

Харківський національний економічний університет ім. С. Кузнеця

Хусаїнов Микита

студент

Харківський національний економічний університет ім. С. Кузнеця

ПРОГНОЗУВАННЯ ПОПИТУ НА ТУРИСТИЧНІ ПОСЛУГИ ТУРИСТИЧНОГО АГЕНТСТВА

Метою проведеного дослідження є розроблення бізнес-моделі, що дозволяє автоматизувати процес обліку, аналізу та прогнозування попиту на туристичні послуги інформаційної систем туристичного агентства. Об'єктом дослідження є інформаційна система агентства туристичних послуг. Предметом дослідження є веб-застосунок для обліку клієнтських запитів та формування статистичних звітів. Метод дослідження – структурно-об'єктне моделювання із використанням CASE-засобів. Було виконано аналіз предметної області, визначено вимоги до функціональності системи, побудовано діаграми варіантів

використання та розроблено модель бази даних, реалізовано веб-застосунок на основі архітектури «клієнт-сервер» з використанням стеку технологій Django, PostgreSQL, HTML/CSS та JavaScript. Застосунок дозволяє реєструвати запити користувачів, зберігати дані про напрямки та категорії туристичних послуг, виконувати фільтрацію запитів, формувати звіти, а також забезпечує багаторівневу авторизацію для користувачів різних ролей.

Сфера туристичних послуг стрімко трансформується під впливом комп'ютеризації усіх галузей народного господарства, що охоплює як процеси просування послуг, так і управління внутрішніми даними, включно з обліком попиту. У традиційній практиці менеджери туристичних компаній здійснюють облік звернень та інтересів клієнтів вручну або за допомогою примітивних електронних таблиць, що унеможлиблює оперативний аналіз тенденцій і формування стратегічної інформації для прийняття управлінських рішень. В умовах зростання конкуренції на ринку, необхідність у створенні спеціалізованих систем, що автоматизують процеси обліку попиту, є надзвичайно актуальною. Туристичний попит характеризується складною природою, яка залежить від багатьох змінних, а саме: сезонності; політичної стабільності; економічної ситуації; інфраструктурної доступності напрямків; погодних умов; локальних подій; культурних свят, епідеміологічних ризиків тощо. Система, яка б враховувала усі ці параметри та дозволяла відстежувати зміну попиту у часовому розрізі, значно підвищила б ефективність роботи туристичних компаній.

Важливим елементом є саме структура та логіка збору інформації про запити клієнтів. Кожне звернення потенційного клієнта – це джерело цінної інформації, яка в разі правильної обробки та систематизації може виявити важливі закономірності: які напрямки мають сезонну популярність; як змінюється середній бюджет подорожей; які категорії клієнтів частіше звертаються до агентства; які типи послуг затребувані найбільше тощо.

Традиційні CRM-системи, хоча і мають широкий функціонал, часто виявляються надлишковими або надто складними для невеликих туристичних агентств. У таких умовах зручне та вузькоспеціалізоване рішення, орієнтоване саме на облік попиту, дозволяє краще адаптувати систему до потреб конкретного бізнесу. Саме ця логіка закладена в основу розроблюваного веб-застосунку. Автоматизація процесу обліку попиту передбачає можливість оперативного введення даних, їх обробки, збереження в структурованому вигляді, а також отримання підсумкової статистики або динамічного аналізу у вигляді фільтрів і звітів. У системі повинні бути передбачені такі ключові параметри запитів, як країна та місто призначення, кількість осіб, бажана дата виїзду та повернення, очікуваний бюджет, категорія туру, тривалість подорожі тощо.

У перспективі така система може бути інтегрована з мобільним застосунком або веб-платформою для кінцевого користувача, однак на етапі розробки у фокусі залишається саме внутрішній облік попиту. Це дозволяє зосередитися на вдосконаленні аналітичного блоку, налаштуванні логіки фільтрації, звітності, підтримці різних ролей користувачів (менеджер, аналітик,

адміністратор) тощо. Розроблення такого програмного забезпечення потребує попереднього аналізу аналогічних рішень, як комерційних, так і відкритих, а також дослідження досвіду реалізації подібних проєктів у суміжних галузях. Зібрана інформація дозволяє уникнути повторення типових помилок, адаптувати найкращі практики, визначити функціонал, який є обов'язковим, а який – надлишковим. Такий підхід сприяє створенню оптимального за функціональністю, простого у використанні і зручного інтерфейсного рішення, яке має практичну цінність для малого та середнього бізнесу в туристичній галузі.

Огляд існуючих рішень показав, що на ринку відсутня проста, спеціалізована система саме для обліку запитів і попиту на туристичні послуги без надлишкового функціоналу. Це свідчить про доцільність створення нового інструменту, який би поєднував простоту використання, ефективне збереження інформації та зручну аналітику, адаптовану під потреби українського туристичного бізнесу. У ході аналізу були розглянуті як програмні продукти комерційного характеру, так і науково-академічні публікації, що стосуються автоматизації в галузі туризму та суміжних сферах. У переважній більшості випадків існуючі рішення орієнтовані або на повнофункціональні CRM-системи. Вони забезпечують комплексне управління клієнтами, контрактами, турпродуктами, однак не завжди мають вузькоспеціалізований інструментарій для статистичного аналізу саме попиту на туристичні послуги без його фактичного придбання. Платформи бронювання зазвичай не зберігають запити, які не завершилися транзакцією, або обмежено надають доступ до аналітики менеджерам агентств, що ускладнює аналіз реального попиту. У той же час, використання повноцінної CRM-системи часто є надлишковим для малого або середнього туристичного офісу, бо вони мають складний інтерфейс, потребують часу на навчання персоналу, значних ресурсів на підтримку, а також рідко дозволяють вносити кастомні аналітичні звіти без участі програміста. Цей підхід і логіка структуризації даних мають багато спільного з потребами туристичного агентства. Розроблюване програмне забезпечення позиціонується як важливий інструмент для внутрішнього використання в туристичних агентствах та компаніях, які працюють із великою кількістю індивідуальних запитів клієнтів. Головна його особливість – акцент не на бронюванні, а саме на обліку, збереженні та подальшій аналітиці запитів, що створює унікальну цінність для малого й середнього бізнесу, де немає потреби у складних CRM-системах або розгалужених сервісах з інтеграцією бронювань. Отже, створюване програмне забезпечення займає унікальну позицію, а саме, воно знаходиться на перетині простоти використання, фокусованої аналітики та практичного підходу до обліку клієнтських запитів, що робить його затребуваним у малих та середніх структурах, які прагнуть організувати внутрішні процеси без великих витрат. Запропонований веб-застосунок вирішує актуальну проблему – відсутність централізованого інструменту для реєстрації, обробки та аналізу попиту на туристичні послуги. Основні ділові переваги: актуальність; цінність для бізнесу; автоматизація рутинних процесів; прозорість управління; масштабованість і адаптивність; формування аналітичного ресурсу.

У результаті впровадження веб-застосунку компанія отримує не просто інструмент для зберігання запитів, а повноцінний елемент бізнес-інфраструктури, який сприяє прийняттю рішень на основі об'єктивних, структурованих даних. У результаті проведених досліджень було розроблено та реалізовано веб-застосунок для обліку попиту на туристичні послуги. Система призначена для автоматизації процесів фіксації, аналізу та класифікації запитів клієнтів туристичних агентств, що дозволяє суттєво знизити навантаження на персонал, підвищити ефективність прийняття управлінських рішень і оперативно формувати звіти про поточний стан попиту. Дослідження проводилося в кілька етапів: проведено аналіз предметної області; проведений аналіз функціональних та нефункціональних вимог; побудовано модель даних, проєкту архітектуру та структуру бази даних; реалізовано основні модулі веб-застосунку, які характеризуються зручним користувацьким інтерфейсом; проведено тестування, яку підтвердило працездатність і готовність системи до впровадження. Таким чином, результати дослідження мають як теоретичне, так і практичне значення для подальшого використання у сфері автоматизації туристичних послуг.

Список використаних джерел

1. Оболенцева Л.В. Проблеми та перспективи формування туристського іміджу України як важливої складової розвитку туризму та економіки держави / Л.В. Оболенцева, С.А. Александрова, К.О. Петренко // Міжнародний науковий журнал. – 2016. – №1 . – с. 72-76.
2. М.М. Цепенда. Інформаційні системи, комунікації і технології у туристичній індустрії : навч. посіб. / Цепенда М.М., В.И. Бурка // Чернівці : Чернівець. нац. ун-т ім. Ю. Федьковича. – 2024. – 176 с.

Філатова Л. Д.

к. ф.-м. н., доцент,

*доцент кафедри інформаційних технологій та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В. Н. Каразіна*

Артур Узвеков,

MSc in Technical Translation, BIA, inv. lect.

Baltic International Academy,

Свинаренко А. А.

здобувачка другого (магістерського) рівня вищої освіти

ННІ «Каразінський банківський інститут» ХНУ імені В. Н. Каразіна

РОЛЬ DBaaS У БІЗНЕС-АНАЛІТИЦІ ТА УПРАВЛІННІ КОРПОРАТИВНИМИ ДАНИМИ

Ключовою здатністю у сучасному бізнесі та ІТ-середовищі є ефективне управління великими об'ємами корпоративних даних. Незважаючи на те, що локальні СУБД роками підтверджували та демонстрували свою важливість, зараз намітилися серйозні ризики їх використання. Одним з таких ризиків є мала масштабованість та значні фінансові видатки, що пов'язані з адмініструванням та підтримкою. На противагу виступають хмарні рішення, такі як Database as a Service (DBaaS), що дають можливість підприємствам сконцентруватися більше на обробці й аналізі даних, аніж на обслуговуванні інфраструктури.

DBaaS – це база даних як послуга, що означає хмарну версію бази даних, суть якої полягає в тому, що клієнти отримують доступ до бази даних без необхідності самостійно розгортати та керувати інфраструктурою. DBaaS презентується як керована служба бази даних, тобто постачальник послуг бере на себе відповідальність за налаштування, масштабованість, оновлення і резервне копіювання бази даних [1]. Прикладами комерційно реалізованих DBaaS є Google Cloud SQL, Amazon RDS, Azure SQL Database, MongoDB Atlas та Snowflake.

Для такої галузі як бізнес-аналітика DBaaS відіграє суттєву роль, оскільки він забезпечує централізований і стандартизований підхід до доступу внутрішніх даних компанії. За допомогою цього інструмента компанія уникає дублювання інформації та починає зберігати її в єдиному середовищі. Окрім того, DBaaS легко інтегрується з різними аналітичними платформами, які вже використовуються на практиці. Така інтеграція допомагає автоматизувати процеси аналізу і звітності. Взаємодія DBaaS з системами бізнес-аналітики та платформами для глибинного аналізу даних дозволяє реалізовувати складні сценарії обробки структурованих і неструктурованих даних. Наприклад, використання сервісів Snowflake [2] та MongoDB Atlas [3] дозволяє компаніям виконувати багаторівневу аналітику та прогнозування на основі великих даних.

Коли обсяги даних швидко зростають, компаніям потрібно мати можливість збільшувати ресурси без перебоїв у роботі. Наприклад, такі сервіси як Amazon DynamoDB або Google BigQuery забезпечують автоматичне регулювання потужностей у залежності від навантаження. Така функція особливо корисна для компаній, які працюють з потоковими даними, онлайн-сервісами або складними прогнозними моделями. Крім того, автоматичне масштабування зменшує потребу в ручному втручанні з боку ІТ-спеціалістів, дозволяючи їм зосередитися на більш важливих завданнях. Гнучкість DBaaS також полягає у можливості вибору типу бази даних залежно від специфіки завдань: реляційні (Amazon RDS, Google Cloud SQL), документно-орієнтовані (MongoDB Atlas, Couchbase Cloud) або графові (Neo4j Aura, Amazon Neptune).

Безпека та надійність зберігання даних є ключовими аспектами DBaaS. Постачальники впроваджують сучасні механізми резервного копіювання, шифрування та відновлення даних, що суттєво знижує ризик втрати критичної інформації та відповідає корпоративним вимогам інформаційної безпеки. [4]

Водночас важливою частиною успішного впровадження DBaaS є його економічна перевага: система оплати за фактичне використання ресурсів дозволяє знизити витрати на підтримку інфраструктури та персоналу, що робить цей сервіс привабливим як для малих компаній, так і для великих корпорацій, які бажають оптимізувати свої управлінські процеси. Однак існують і ризики у впровадженні DBaaS. Наприклад, потенційні затримки при нестабільному з'єднанні, залежність від дистриб'ютора хмарного сервісу. Також важливо усвідомлювати, що провайдеру передається відповідальність щодо зберігання персональних даних.

ВИСНОВКИ. На сьогодні DBaaS виступає як потужний засіб для управління корпоративними даними та бізнес-аналітики, що поєднує гнучкість, безпеку та економічну доцільність. Результатом використання DBaaS є підвищення швидкості прийняття управлінських рішень, а також вищий рівень гнучкості й конкурентоздатності бізнесу в нестабільних динамічних умовах існування. Використання сервісів Amazon RDS, Google BigQuery, Snowflake та MongoDB Atlas дозволяє компаніям покращити рівень ефективності прийняття рішень і оптимізувати ключові бізнес-процеси.

Список використаних джерел

1. What Is DBaaS? [Електронний ресурс]. Режим доступу: <https://www.oracle.com/ua/database/what-is-a-cloud-database/dbaas/>
2. Snowflake. [Електронний ресурс]. Режим доступу: <https://www.snowflake.com/en/>
3. MongoDB Atlas. [Електронний ресурс]. Режим доступу: <https://www.mongodb.com/products/platform>
4. М. В. F. Sanjeetha, М. S. M. Siriwardane, R. J. P. K. Rajakaruna, and P. S. Haddela, «Database-as-a-Service (DBaaS) in Cloud Computing: Security Issues and Policies», Asian Journal of Computer Science and Technology, vol. 14, no. 1. 2025.

С.Шапошник М.Є.
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Кобилін І.О.
к.т.н., асистент кафедри Інформатики,
Харківський національний університет радіоелектроніки

ІІІ-АСИСТЕНТ ЯК ІНСТРУМЕНТ ПОКРАЩЕННЯ ВЗАЄМОДІЇ КОРИСТУВАЧА З САЙТОМ

В умовах конкуренції в електронній комерції, оптимізація використання сайту користувачем, та оформлення замовлення перестала бути просто технічним удосконаленням, а перетворилася на стратегічну особливість, яка може не тільки спростити користування а й підвищити зручність. Дослідження в галузі користувацького досвіду (UX) чітко демонструють, що складні процеси є однією з ключових причин відмови від покупок. А впровадження ІІІ-асистента є важливим елементом який може вплинути на різні аспекти веб-сайту, від покращення досвіду користувача до заощадження на робітниках особливо зважаючи на - Як зазначають експерти, кожен зайвий клік або поле для заповнення створює точку тертя, яка може змусити клієнта покинути кошик із товарами. ІІІ-асистенти стали важливим інструментом для підвищення продажів та якості, а головне - швидкості обслуговування. Їхня роль може виходити за межі просто відповідника, вони можуть стати вашим інтелектуальним радником або посередником, також вони можуть надавати персоналізовані рекомендації, та допомагати вирішувати проблеми в реальному часі.

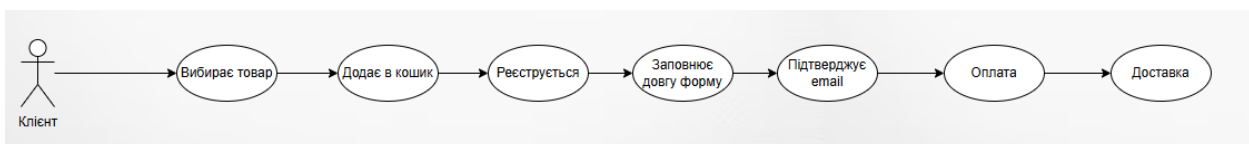


Рисунок 1. Схема порівняння кількості кроків клієнта без оптимізації веб сайту

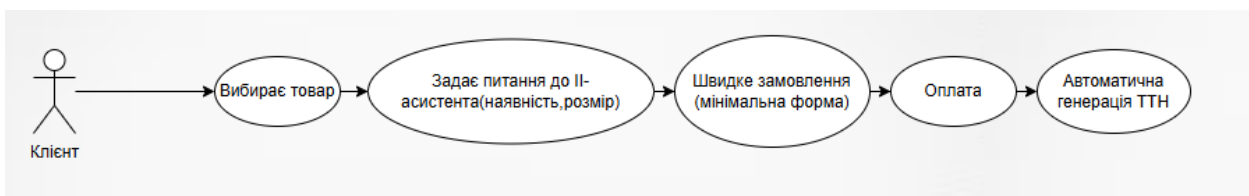


Рисунок 2. Схема порівняння кількості кроків клієнта з оптимізацією веб сайту

Основою таких систем є природномовний обробник (NLP). В його можливості входить розуміння та генерування людської мови. Це дає можливість впровадити інтерфейс для спілкування клієнта з ІІІ в реальному часі. Так як ІІІ-асистент аналізує, ще й контекст, та може запам'ятовувати

історію спілкування з користувачем - це дозволяє йому пропонувати високо персоналізовані рішення.

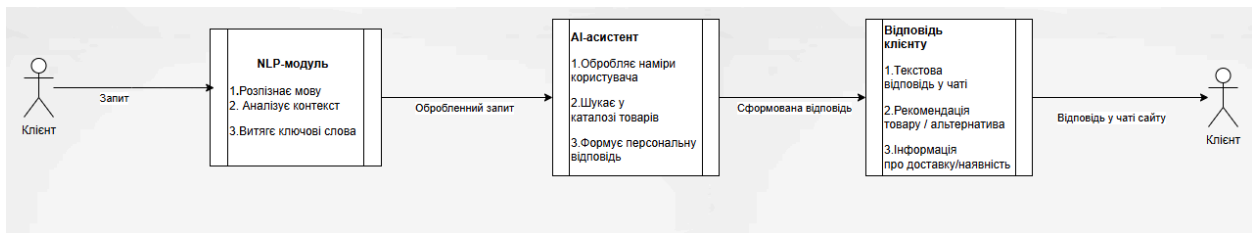


Рисунок 3. Шлях від запиту клієнта до відповіді від ШІ-асистента до відповіді у чаті

Таким чином система може заощадити кошти на робітниках сайту, може зменшити кількість покинутих замовлень за рахунок миттєвої цілодобової допомоги. Також зростає конверсія за рахунок персональних пропозицій та порад. Але найважливішим є підвищення лояльності клієнтів за рахунок того, що клієнти починають сприймати майданчик не як безособовий сайт, а як сервіс, що турбується про їхній комфорт та формує тривалі стосунки між клієнтом та сайтом. Що в свою чергу представлено у вигляді таблиці, де показано взаємодію клієнта та елементів сайту. Зважаючи на фактор метрики взаємодії:

$$UX_{AI} = \frac{(E \times P) + (C \times P)}{T},$$

Е – це ефективність пошуку інформації, тобто швидкість знаходження потрібного матеріалу чи рекомендацій; Р – персоналізація, що показує, наскільки добре асистент підлаштовує контент і відповіді під конкретного користувача; С – комфорт взаємодії, який визначається зручністю діалогу, зрозумілістю відповідей та відсутністю зайвих дій; R – рівень утримання користувача, що відображає ймовірність залишитися на сайті, повернутися чи здійснити конверсію; Т – витрачений час, де чим менше його потрібно для досягнення цілі, тим кращим є досвід. Відобразимо користь ШІ-асистента в базових аспектах користування сайтом у таблиці 1.

Таблиця 1.

Взаємодія клієнта та елементів сайту

Аспект взаємодії	Без ШІ-асистента	З ШІ-асистентом
Пошук товарів	Користувач сам переглядає каталог, витрачає більше часу	Асистент швидко знаходить потрібний товар або пропонує альтернативи
Отримання інформації	Необхідно читати FAQ чи чекати відповіді оператора	Асистент надає миттєву відповідь у чаті 24/7
Оформлення замовлення	Ручне заповнення форм, більша ймовірність помилок	Асистент допомагає підставити дані, підказує кроки
Персоналізація	Сайт показує стандартний асортимент	Асистент пропонує персональні рекомендації на основі історії
Клієнтський досвід	Сайт сприймається як «безособовий магазин»	Сайт виглядає як сервіс, що турбується про клієнта

Така оптимізація - є необхідною бо у момент коли клієнт уже ухвалив рішення про покупку процес має бути максимально інтуїтивним і швидким. Він повинен мати змогу вказати необхідні дані для відправки замовлення, яких, ще немає в його обліковому записі. Також важливо оптимізувати сайт так, щоб клієнт міг без зайвих відволікаючих перемикачів між вкладками зробити своє замовлення. Як показують реальні випадки, таке спрощення на пряму корелює конверсією, та може значно зменшити кількість покинутих кошиків оскільки зменшує кількість причин для відмови від завершення покупки. Вплив кількості кроків на завершення покупок відобразимо в таблиці 2.

Таблиця 2.

Вплив кількості кроків при оформленні замовлення на поведінку клієнтів

Кількість кроків	Час оформлення (хв)	Ймовірність завершення покупки	Ймовірність покинути кошик
3-4 (оптимізований процес)	1-2 хв	80%	20%
5-7 (середня складність)	3-5 хв	60%	40%
8+ (ускладнений процес)	6-10 хв	40%	60%

Отже, впровадження ШІ-асистента та оптимізація процесу онлайн-замовлення виступають як ключові та взаємодоповнюючі елементи, що можуть вплинути на успішність та ефективність електронної комерції. З одного боку, ШІ-асистент, який значно покращує досвід користувача, він може забезпечувати миттєву підтримку по різних питаннях клієнта, робить персоналізовані рекомендації та дозволяє заощадити ресурси. З іншого боку, оптимізація процесу оформлення замовлення зменшує кількість бар'єрів для клієнта, підвищує швидкість та інтуїтивність взаємодії, що на пряму впливає на рівень конверсії та знижує частку покинутих кошиків.

У сукупності такі підходи перетворюють інтернет магазин з простого каталогу на комплексний сервіс, який забезпечує зручність, швидкість та задоволення індивідуальних потреб клієнтів. Це, у свою чергу, формує конкурентну перевагу серед інших магазинів на ринку та забезпечує довготривалу лояльність покупців.

Список використаних джерел

1. Shopify (2023). *13 Checkout Optimization Tips To Increase Ecommerce Revenue*. <https://www.shopify.com/blog/checkout-process-optimization>
2. Hirschberg, J., & Manning, C. D. (2015). *Advances in Natural Language Processing*. Science, 349(6245), 261–266. <https://www.science.org/doi/10.1126/science.aaa8685>
3. Fastspring (2023). *How Changes to Your Checkout Can Affect Conversion Rates*. <https://fastspring.com/blog/how-checkout-changes-can-affect-conversion-rates>

Шатович Я. В.

здобувач вищої освіти,

Державний торговельно-економічний університет

Геселева Н. В.

доцент кафедри цифрової економіки та системного аналізу

Державний торговельно-економічний університет

СУЧАСНІ ПІДХОДИ ДО ОРГАНІЗАЦІЇ БАЗ ДАНИХ: ПОРІВНЯННЯ РЕЛЯЦІЙНИХ ТА НЕРЕЛЯЦІЙНИХ МОДЕЛЕЙ

Бази даних є основою сучасних інформаційних систем, оскільки забезпечують накопичення й обробку даних, необхідних для функціонування бізнесу, науки та державного управління. Реляційна модель стала фундаментом класичних СУБД, проте з поширенням великих даних та зростанням вимог до масштабованості з'явився попит на нереляційні (NoSQL) системи.

Їх порівняння дозволяє визначити переваги, обмеження та сфери застосування кожної моделі.

Реляційні бази даних

Реляційна модель баз даних була запропонована Е. Коддом у 1970 році та ґрунтується на використанні таблиць (відношень), де дані зберігаються у вигляді рядків і стовпців [2]. Основними інструментами роботи є мова структурованих запитів SQL та механізми забезпечення транзакційності, узгодженості й цілісності даних (ACID).

Прикладами сучасних реляційних систем управління базами даних (СУБД) є Oracle Database, MySQL, PostgreSQL, Microsoft SQL Server. Вони широко застосовуються у фінансовій, банківській та обліковій сферах, де критично важливою є точність і надійність обробки інформації.

Серед обмежень можна виокремити складність масштабування, зниження продуктивності при роботі з великими обсягами неструктурованих даних, а також обмежену гнучкість у зберіганні інформації, яка не має чіткої схеми [1].

Нереляційні бази даних (NoSQL)

Поширення великих даних та інтенсивний розвиток інтернет-сервісів на початку 2000-х років зумовили появу нового класу систем управління даними – нереляційних баз даних (NoSQL). Вони відмовляються від жорсткої табличної структури, властивій реляційним системам, і пропонують більш гнучкі способи збереження інформації [3].

Серед основних типів NoSQL-систем можна виокремити:

- 1) документоорієнтовані (MongoDB);
- 2) колонкові (Apache Cassandra);
- 3) графові (Neo4j), для моделювання взаємозв'язків між об'єктами;
- 4) ключ-значення (Redis).

Основними перевагами NoSQL-підходу є висока швидкодія, можливість горизонтального масштабування та робота з неструктурованими даними [4].

Разом з тим, використання NoSQL має і певні обмеження. Насамперед це відсутність єдиного стандарту, обмежена підтримка транзакційності (часто замість ACID використовується модель BASE), а також складність інтеграції з класичними інформаційними системами [5].

Порівняльна характеристика моделей

Реляційні та нереляційні бази даних використовують різні підходи до зберігання, обробки та масштабування інформації. Реляційні мають чітку табличну структуру, підтримують складні запити через SQL, забезпечують цілісність і транзакційність (ACID) та ефективні у фінансових і корпоративних системах.

Нереляційні БД (NoSQL) пропонують гнучку структуру (JSON, граfi, ключ-значення), горизонтальне масштабування та високу продуктивність, що робить їх ефективними для веб-сервісів, аналітики великих даних, соціальних мереж та IoT.

У практичних проектах часто застосовується гібридний підхід: критично важливі дані зберігаються в реляційних БД, великі обсяги неструктурованих – у NoSQL, що поєднує надійність і масштабованість системи.

Таблиця 1.

Характеристика	Реляційні БД	Нереляційні БД (NoSQL)
Структура даних	Таблиці з чітко визначеними стовпцями і рядами	Гнучка: документи (JSON/BSON), граfi, ключ-значення, колонки
Мова запитів	SQL	Власні API або запити (MongoDB Query, Cypher)
Транзакційність	ACID(підтримка цілісності та узгодженості)	Часто BASE (гнучкість, масштабованість)
Масштабування	Вертикальне (потужніші сервери)	Горизонтальне (додавання серверів у кластер)
Переваги	Надійність, точність, складні аналітичні запити	Швидкість, масштабованість, робота з великими обсягами неструктурованих даних
Обмеження	Складність масштабування, низька гнучкість	Відсутність єдиного стандарту, обмежена транзакційність, складна інтеграція з класичними системами
Сфери застосування	Банки, бухгалтерія, ERP-системи	Веб-додатки, соціальні мережі, аналітика великих даних, IoT

Отже, реляційні бази даних забезпечують точність, надійність і підтримку складних запитів, що робить їх ефективними у фінансових та корпоративних системах. Нереляційні (NoSQL) системи пропонують гнучку структуру, масштабованість і швидку обробку великих даних, підходять для веб-додатків та аналітики. Часто застосовується гібридний підхід: критично важливі дані зберігаються у реляційних БД, а великі обсяги неструктурованих даних – у NoSQL. Вибір моделі визначається технічними вимогами проєкту та обсягами даних.

Список використаних джерел:

1. Date C. J. An Introduction to Database Systems. – Boston: Addison-Wesley, 2004. – 1024 с.
2. Codd E. F. A Relational Model of Data for Large Shared Data Banks // Communications of the ACM. – 1970. – Vol. 13, No. 6. – P. 377–387.
3. MongoDB Documentation [Електронний ресурс]. – Режим доступу: <https://www.mongodb.com/docs/> (дата звернення: 24.09.2025).
4. Cassandra Documentation [Електронний ресурс]. – Режим доступу: <https://cassandra.apache.org/doc/latest/> (дата звернення: 24.09.2025).
5. Neo4j Graph Database Platform [Електронний ресурс]. – Режим доступу: <https://neo4j.com/> (дата звернення: 24.09.2025).

УДК 004.932.2

Шевченко О.О.

здобувач вищої освіти,

Харківський національний університет радіоелектроніки

Науковий керівник

Кобилін І. О.

к.т.н., асистент кафедри інформатики

Харківський національний університет радіоелектроніки

ІНСТРУМЕНТИ ВІЗУАЛІЗАЦІЇ ДАНИХ ЯК ЗАСІБ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

В умовах цифровізації та стрімкого зростання обсягів інформації управління, аналітики та дослідники стикаються з проблемою оперативної обробки й інтерпретації великих масивів даних. Ефективне прийняття рішень неможливе без наочних засобів подання інформації, які дозволяють швидко виявляти закономірності, тенденції та аномалії. То ж аналіз можливостей сучасних програмних інструментів та подальше використання інструментів візуалізації даних для підвищення ефективності процесів прийняття управлінських і стратегічних рішень є важливим і актуальним особливо в момент реалізації, технічної та бізнес підтримки, моніторингу і актуалізації інформації що продемонстровано на рисунку 1:



Рис. 1. Етапи використання інструментів візуалізації даних у процесі підтримки прийняття рішень

Візуалізація потрібна як на етапі збору даних, щоб відобразити структуру джерел так і для розуміння обсягів інформації, які підлягають аналізу. На етапі

первинного аналізу вона допомагає виявити пропуски, аномалії та приховані залежності через графіки й теплові карти. Під час побудови моделей та прогнозування візуалізація використовується для перевірки сценаріїв і оцінки точності результатів. На стадії дашбордів і стратегічних звітів вона забезпечує зрозумілу подачу ключових показників та тенденцій для швидкого ухвалення управлінських рішень. У процесі підтримки прийняття рішень важливим етапом є виявлення аномалій у даних. Це часто здійснюється за допомогою стандартного z – score z – score, який обчислюється так:

$$z = \frac{x - \mu}{\sigma}$$

де x – конкретне значення показника, μ – середнє значення, σ – стандартне відхилення. Якщо $|z| > 3$, то спостереження вважається потенційною аномалією.

Таблиця 1.

Порівняльний аналіз сучасних інструментів візуалізації даних

Інструмент	Основні можливості	Переваги	Обмеження / Недоліки
Power BI	Інтеграція з ERP/CRM, дашборди, автоматичне оновлення даних, прогнозування KPI	Глибока інтеграція з Microsoft, широкі можливості бізнес-аналітики, доступність для користувачів без програмних навичок	Платна ліцензія для професійних функцій, обмеження хмарних можливостей у безкоштовній версії
Tableau	Інтерактивні багатовимірні дашборди, складні аналітичні моделі	Потужні можливості візуалізації, підтримка інтерактивного аналізу великих обсягів даних, гнучкість у налаштуванні звітів	Висока вартість, потребує навчання для ефективного використання
Qlik Sense	Асоціативна модель аналізу, пошук прихованих взаємозв'язків, динамічні дашборди	Швидке дослідження взаємозв'язків між показниками, інтерактивні аналітичні сценарії	Потребує базових знань аналітики, іноді складність у масштабуванні
Google Looker Studio	Хмарні звіти з доступом у реальному часі, інтеграція з Google Analytics, Ads, Sheets	Безкоштовність, миттєвий доступ до даних, легкість спільного використання	Обмежені можливості аналітики та прогнозування, менше інтерактивних функцій порівняно з BI-системами

Тому сучасні BI-системи значно полегшують процес ухвалення рішень завдяки інтерактивним дашбордам і візуалізаціям, які роблять дані зрозумілими навіть для користувачів без спеціальних знань у статистиці чи програмуванні. Вони забезпечують інтеграцію різних джерел інформації (ERP, CRM, фінансові

звіти, веб-аналітика) в єдине середовище, а також надають інструменти прогнозування та автоматичного виявлення трендів. Це сприяє підвищенню швидкості та обґрунтованості управлінських рішень, полегшуючи комунікацію між аналітиками та керівниками.

Список використаних джерел:

1. Творошенко І.С. «Технології прийняття рішень в інформаційних системах» (ХНУРЕ, 2021)
2. Chen, Rui Jie Jerry (2025). The Future of Data Visualization in Business. *Advances in Economics Management and Political Sciences*.
3. Sugihara, A., et al. (2025). Data Visualization for Decision-Making: A Systematic Review. *Information*.

РОЗДІЛ 3.

ПРОГРАМНІ ЗАСОБИ ДЛЯ ВИРІШЕННЯ ПРИКЛАДНИХ ЗАДАЧ ВИРОБНИЦТВА, ОСВІТИ, БІЗНЕС-АНАЛІТИКИ, ІНТЕЛЕКТУАЛЬНОГО ОБРОБЛЕННЯ ДАНИХ, ПРИЙНЯТТЯ РІШЕНЬ

Bachmaniuk D.O.

*higher education student, first (bachelor's) level of higher education
Education and Research Institute "Karazin Banking Institute"*

*V.N. Karazin Kharkiv National University,
assistant at the department of Mathematical Economics
of European University Viadrina, Germany*

Dr. Schreibweis M.

*head of the department of Mathematical Economics
of European University Viadrina, Germany*

AUTOMATED ABC ANALYSIS IN PYTHON: A PRACTICAL IMPLEMENTATION WITH OPPORTUNITIES FOR LINEAR PROGRAMMING INTEGRATION

ABC analysis is a method for classifying business resources (such as goods, materials, suppliers, customers, etc.) according to their relative significance. The method emerged in the mid-20th century as a generalization of the Pareto principle and rapidly gained application in economics and management, particularly in areas such as inventory control, logistics, finance, and business analytics [1]. The underlying idea is that a relatively small portion of the assortment, e.g. Class A consists of highly valuable but low-volume resources; Class B represents resources of medium value and volume; while Class C comprises high-volume resources with low unit value. For instance, it is often assumed that approximately 10-20% of items (Class A) account for 70-80% of total costs or revenues, the subsequent 20-30% (Class B) contribute about 15-20%, and the remaining 50-70% (Class C) represent only 5-10%.

In practice, the implementation of ABC analysis typically begins with the calculation of the annual consumption value (ACV) for each item, defined as the product of quantity and unit price. Items are then ranked in descending order of ACV, after which the percentage contribution of each item to the total ACV and its cumulative share are determined [2]. In the provided Python code example, ACV and cumulative shares were computed for each product, and classification was performed accordingly: items with a cumulative share of $\leq 80\%$ were assigned to Class A, those between 80% and 95% to Class B, and those above 95% to Class C.

Code 1

```
import pandas as pd
data = [
    ["2F", 1523, 9],
    ["4C", 4208, 32],
    ["N9", 45, 22],
    ["O6", 2675, 40],
    ["K8", 3261, 27],
    ["Y5", 4354, 46],
    ["Lo9", 4068, 49],
    ["Ko8", 2633, 4],
    ["No11", 718, 21],
    ["Zo1", 2489, 41],
    ["Yo4", 2282, 38],
    ["Wo3", 2362, 22]]

df = pd.DataFrame(data, columns = ["productCode", "amount", "price"])
df["ACV"] = df["amount"] * df["price"]
df = df.sort_values(by='ACV', ascending=False)
df["shareACVin%"] = 100 * df["ACV"] / df["ACV"].sum()
df["cumShareACVin%"] = df["shareACVin%"].cumsum()
def classification_abc(x):
    ...
    Classifies a value 'x' into ABC categories based on predefined thresholds.
    Arguments:
        x (int,float): Value to be classified.
    Returns:
        string: The ABC category ('A', 'B', or 'C').
    ...
    if x>0 and x<=80:
        return "A"
    elif x>80 and x<=95:
        return "B"
    else:
        return "C"
df["class"] = df["cumShareACVin%"].apply(classification_abc)
print(df)
```

	productCode	amount	price	ACV	shareACVin%	cumShareACVin%	class
5	Y5	4354	46	200284	19.823131	19.823131	A
6	Lo9	4068	49	199332	19.728907	39.552039	A
1	4C	4208	32	134656	13.327593	52.879631	A
3	O6	2675	40	107000	10.590337	63.469968	A
9	Zo1	2489	41	102049	10.100311	73.570280	A
4	K8	3261	27	88047	8.714462	82.284742	B
10	Yo4	2282	38	86716	8.582726	90.867467	B
11	Wo3	2362	22	51964	5.143143	96.010610	C
8	No11	718	21	15078	1.492347	97.502957	C
0	2F	1523	9	13707	1.356652	98.859609	C
7	Ko8	2633	4	10532	1.042406	99.902015	C
2	N9	45	22	990	0.097985	100.000000	C

*Formed by the author**

Thus, ABC analysis enables management to concentrate attention on the most critical inventory items, namely: Y5, Lo9, 4C, O6, and Zo1, which fall into category (A), and K8 and Yo4, which are classified as (B). The table below presents a detailed overview of the advantages and disadvantages of this method. Among the advantages, it is worth highlighting the reduction of excess stock, acceleration of inventory turnover, and cost minimization by focusing resources on key products. At the same time, however, the method also has several limitations: it concentrates narrowly on value or sales volume while neglecting other factors; the classification thresholds are somewhat arbitrary and sensitive to their chosen cutoffs; and items with low cost but high strategic importance may be assigned to group C and consequently fall outside the focus of management [3].

Table 1

Advantages and disadvantages of the common ABC Analysis

Aspect	Advantages	Disadvantages / Criticism
Management focus	Concentrates management attention on the most important items (Class A items generate 70-80% of revenue).	One-sided approach: focuses only on sales volume/value, ignoring seasonality, product life cycle, and risks.
Inventory	Optimization: ensures adequate stock of Class A items, reduces excess inventory of Classes B and C.	Classification is sensitive to threshold selection, causing group instability (up to 50% of items may shift between classes).
Forecasting	Improves demand forecasting for Class A items, increasing procurement planning accuracy.	Requires constant data verification and updates to avoid distortions.
Supplier relations	Enables negotiation of better terms for key items (Class A products).	May overlook strategically important but low-value items (e.g., safety spare parts).
Resource allocation	Strategic allocation of resources according to demand changes.	Requires clear standards and a unified accounting system; otherwise, categorization becomes subjective.
Overall effect	Reduces excess stock, speeds up inventory turnover, and lowers costs.	Simplified method that works well only under stable conditions; may give inaccurate results under dynamic changes.

*Formed by the author**

To overcome the aforementioned limitations, researchers propose integrating ABC analysis with optimization methods. In particular, ABC classification can be formalized as a linear (or integer) programming problem by introducing decision variables to represent the assignment of items to groups and constraints related to budget or service levels. For example, Millstein et al. (2013) developed an optimization model that simultaneously determines the number of groups, their target service levels, and the allocation of items among groups, while accounting for a limited inventory budget [4]. The objective is to maximize profit or service level, achieved through the optimal distribution of resources across classes A, B, and C. Such a model has been shown to outperform traditional ABC analysis, as it explicitly incorporates objective functions and strict constraints - factors not captured by the simple threshold-based method. For instance, binary variables can be introduced for each item to indicate group membership, together with constraints on total revenue or budget. Based on these variables, an objective function can be formulated (e.g., maximizing profit or minimizing inventory costs while maintaining a specified service level). Solving such a linear or integer optimization problem enables a more flexible classification tailored to the specific needs of the enterprise. Thus, ABC analysis may be viewed not only as a discrete algorithm but also as part of broader supply chain and inventory optimization systems. This perspective extends its

applicability to multi-criteria and dynamic scenarios, where the formalization of interdependent parameters is of critical importance.

In conclusion, ABC analysis is a useful empirical tool for inventory management, grounded in the principles of the Pareto law. Its strengths lie in directing managerial focus toward the most important items and in simplifying the decision-making process. However, the method overlooks certain risk factors and may become unstable under conditions of fluctuating demand. To enhance ABC analysis, it can be formalized as a linear programming problem, which considerably broadens its potential applications: enabling automation and optimization of decisions, aligning them more closely with objective functions, and integrating ABC analysis into comprehensive optimization systems.

References

1. Kaufman T., Strategy tools from practice. «Springer» - 2025; pp. 207-211. Retrieved on August 08, 2025.
2. How ABC Analysis Supports Inventory Control Best Practices. Logiwa Marketing. Published on October 4, 2023; updated on September 15, 2025. URL: <https://www.logiwa.com/blog/abc-analysis-inventory-control>. Retrieved on September 15, 2025.
3. Assem H., ABC Analysis Method: Definition, Advantages, and Disadvantages. Published on February 14, 2024. URL: <https://www.enerpize.com/hub/abc-analysis-method-definition-advantages-disadvantages>. Retrieved on September 04, 2025.
4. Millstein M., Yang L., Li H., Optimizing ABC Inventory Grouping Decisions; Jan 2013. URL: https://www.researchgate.net/publication/259134809_Optimizing_ABC_Inventory_Grouping_Decisions. Retrieved on August 30, 2025.

Bondar Sofiia,
undergraduate student,
Kyiv National Linguistic University
Scientific advisor
Melnyk Alla,
PhD in Pedagogy, Associate Professor,
Associate Professor of the
Department of Germanic and
Romance Languages,
Kyiv National Linguistic University

SILENT VIDEOS IN ENGLISH LANGUAGE TEACHING: TASKS FOR YOUNG LEARNERS' SPEAKING AND STORYTELLING

Video materials have become an important part of modern language teaching, providing real-life situations and engaging content that traditional textbooks cannot offer. Among multimedia resources, silent/wordless videos create special opportunities for English language learning, especially for young students. These videos remove language barriers while encouraging imagination, verbal expression, and thinking skills. Without dialogue, learners naturally want to fill the silence with their own words, making silent videos effective tools for building vocabulary, storytelling skills, and cultural understanding. Silent films help ESL students use visual skills as a springboard for developing speaking and writing. Unlike dialogue-rich clips, silent videos require learners to interpret visual cues, predict events, and articulate what they see—strengthening both comprehension and oral production. For young learners aged 5–6 years, this format works especially well because children naturally learn through pictures and stories. Using silent videos can also address common classroom challenges: sustaining attention, creating authentic situations for language use, and accommodating diverse learning styles. However, successful use requires careful content selection, well-planned activities, and clear learning goals aligned with curriculum outcomes.

The goal of this paper is to examine how effectively silent/wordless videos function as teaching tools in English language education, with particular attention to young learners. It explores how such videos support vocabulary learning, storytelling skills, cultural knowledge, and engagement, while outlining practical classroom applications and typical implementation challenges.

Tasks: (a) synthesize approaches to using silent videos with young learners, (b) outline activity designs for speaking and writing, and (c) identify selection criteria and assessment options.

The review draws on recent sources (2018–2025) to reflect current directions in multimedia language education and includes practical examples from kindergarten English teaching.

Classic silent films. Works such as *The Immigrant* (Charlie Chaplin) provide rich historical and cultural contexts while conveying universal human experiences

through visual storytelling. Research and practitioner guides discuss materials and methods for using wordless videos and classic silent films in ELT, enabling exploration of topics like migration, social issues, and relationships alongside language development.

Contemporary animated shorts. Modern (often near-silent) shorts—e.g., Pixar’s *Presto* and *The Fantastic Flying Books of Mr. Morris Lessmore*—offer high production values and universal themes. Their visual clarity supports beginners, while sophisticated symbolism sustains interest for advanced learners. Curated collections (e.g., Kieran Donaghy’s site) provide teacher-ready selections.

Short video research. “Short videos” have become an established area of FL pedagogy, with studies indicating benefits for attention and acquisition. A commonly recommended 2–10 minute duration affords depth without overloading attention.

Activity design. Pre-viewing often builds vocabulary and cultural context; during-viewing tasks include prediction, character/setting analysis, and guided note-taking; post-viewing tasks extend language use via retelling, creative writing, role-play, and discussion. While findings are encouraging, teachers should plan for typical challenges—attention control, content appropriateness, and assessment validity—via clear objectives, rubrics, and careful clip selection.

In implementing silent videos in kindergarten English lessons, a rainy-weather clip (umbrellas, autumn elements) prompted 5–6-year-old learners to verbalize observations and predictions. The lack of dialogue created a “language space”: learners were motivated to describe, anticipate, and express feelings about visual elements. Pre-teaching essential vocabulary (e.g., *rain, umbrella, puddle, autumn*) and modeling sentence frames helped children focus on higher-order thinking rather than struggling with basic lexis; pairing and small-group work sustained interest and supported language production.

We argue that silent videos should complement, not replace, core instruction through scaffolded, task-based activities aligned with explicit learning objectives and age-appropriate assessment.

The Immigrant (Chaplin) supports discussion of historical periods, social issues, and cultural differences. Tasks: analyze character motives, predict plot developments, script and dub key scenes. Best for intermediate–advanced learners who can engage with cultural nuance.

Near-silent shorts like *Presto* and *The Fantastic Flying Books of Mr. Morris Lessmore* work well in mixed-ability classes: accessible visuals for beginners, rich themes for advanced learners.

Weather-themed implementation (case study, kindergarten level).

Pre-viewing: vocabulary with flashcards (*rain, umbrella, puddle, cloudy, wet, dry*), weather song for thematic context, real umbrella demo / tactile exploration;

During-viewing: pause-and-predict at key moments, color and counting (*red umbrella; three puddles*), emotion recognition (happy/sad/surprised);

Post-viewing: retelling with picture sequence cards, draw-and-describe favorite scene,

role-play mimicking character actions, create a simple “weather report” using target lexis.

Silent videos lend themselves to authentic assessment:

oral retelling (narrative sequence, vocabulary use)

creative writing (descriptive language, imagination)

peer discussion (communicative competence)

visual–verbal matching (comprehension checks).

Silent videos are powerful yet underused in ELT. Their ability to prompt language production through visual storytelling is especially valuable for young and beginning learners. Effective use depends on content selection, age-appropriate task design, and explicit learning goals. For young learners, silent videos create natural contexts for language use while supporting thinking and emotional development.

Anticipated research. Future studies should determine optimal clip length by age group; measure vocabulary retention from silent-video tasks using delayed post-tests; and compare silent videos with standard audiovisual materials on common outcomes (listening comprehension, oral fluency, narrative structure). Additional priorities include developing curated, age-appropriate repositories and teacher training for silent-video pedagogy. As technology evolves, integrating interactive elements and AI-supported feedback could further enhance learning.

References:

1. Donaghy, K. (2016). *The seven best silent short films for language teaching*. Kieran Donaghy. <https://kierandonaghy.com/seven-best-silent-short-films-language-teaching/>
2. ELT-Training. (2024). *Using silent film for teaching*. ELT-Training Blog. <https://www.elt-training.com/blog/using-silent-film-for-teaching>
3. Ellevation Education. (2023). *Videos help English learners grasp language and content simultaneously*. Ellevation Education Blog. <https://ellevationeducation.com/blog/videos-help-english-learners-grasp-language-and-content-simultaneously>
4. George, P. (2018). *Silent film: A visual narrative for developing linguistic competence*. CUNY Academic Works. https://academicworks.cuny.edu/kb_oers/18/
5. Kasper, L., & Singer, S. (2001). Unspoken content: Silent film in the ESL classroom. *TESOL Journal*, 10(3), 8–15.
6. Ollinger, A. (2021). *Wordless videos for speech therapy*. Anna Ollinger Speech Therapy. <https://annaospeech.com/blog/wordless-videos>
7. Silent Way Online. (2024). *Silent Way method resources*. <https://silentway.online/>
8. Templer, B. (2018). *Teaching wordless videos and classic silent films in EFL*. ResearchGate. https://www.researchgate.net/publication/324390225_Teaching_Wordless_Videos_and_Classic_Silent_Films_in_EFL

9. Zhang, A., & Lucas, R. (2022). A decade of short videos for foreign language teaching and learning: A review. *Education Sciences*, 12(11), 786. <https://www.mdpi.com/2227-7102/12/11/786>

UDC 378.147

Kapatsyn Alona,
undergraduate student,
Kyiv National Linguistic University
Research advisor

Melnyk Alla,
PhD in Pedagogy, Associate Professor,
Associate Professor of the
Department of Germanic and
Romance Languages,
Kyiv National Linguistic University

PODCASTS IN ENGLISH LANGUAGE TEACHING: NEW OPPORTUNITIES FOR LISTENING, PRONUNCIATION AND CLASSROOM TASKS

Modern education is shaped by the rapid development of digital technologies, which are transforming approaches to teaching foreign languages. Students of the digital generation require innovative methods that combine traditional and contemporary tools. One such resource is podcasts, which offer authenticity and interactivity. Studying their use in language education is therefore both relevant and valuable for teaching practice.

The aim of this article is to examine the role of podcasts in foreign language learning, focusing on their impact on listening and pronunciation skills, as well as identifying practical opportunities for classroom integration. This approach combines theoretical knowledge with real communicative contexts, making the learning process more dynamic and responsive to contemporary student needs. We argue that podcasts should complement structured instruction through scaffolded, task-based activities targeting listening and pronunciation.

From multiple perspectives—multimodal literacy (Serafini, 2013) and empirical classroom studies (Syahabuddin & Rizqa, 2021; Bahri & Halimatussadiah, 2024)—evidence indicates benefits, while typical concerns include distraction, privacy, and assessment validity. Among the various digital tools available, podcasts occupy a prominent place as one of the most effective means of language learning. According to Serafini (2013), podcasts are a multimodal genre that integrates linguistic modes (such as spoken words or scripted text) with aural modes (including voice quality, intonation, and music), facilitating new forms of engagement with

language. Their use extends learning beyond the classroom and connects students to a global language community.

An empirical study, *Improving Students' Listening Skill Using Podcasts*, conducted by Syahabuddin K. and Rizqa K., showed that after regular use of podcasts students demonstrated significant progress in listening comprehension: their average test scores rose from 36.3 to 63.3. This improvement can be explained by the fact that podcasts expose learners to authentic speech at a natural pace, allowing them to become familiar with a variety of accents and speech styles.

The impact of podcasts on pronunciation has also been reported by Bahri S. and Halimatussadiah in *A Qualitative Study on the Impact of Listening to Podcasts on Students' Pronunciation*. Their research showed that regular podcast listening significantly improved learners' pronunciation. Constant exposure to authentic speech helped students better recognize sounds, stress, and rhythm in English, which in turn enabled them to reproduce what they heard more accurately in their own speech.

These findings highlight the multifaceted benefits of podcasts. Using them in the classroom plays a significant role not only in enhancing listening and pronunciation skills but also in developing students' analytical thinking. Podcasts encourage learners to process information critically and draw conclusions while supporting active participation in communicative tasks.

To illustrate the potential of podcasts in teaching English, consider the episode "Who Invented Emojis?" from the series *But Why: A Podcast for Curious Kids*. This episode provides historical context, expert interviews, and practical examples. The format helps learners practice listening, enrich their topic-specific vocabulary, develop pronunciation, and explore the cultural background of emojis, which first appeared in Japan. Such material can be incorporated into lessons on topics like information technologies.

Practical implementation can include various interactive tasks. For instance, the "Emoji Timeline" activity invites students to work in groups and create a timeline of emoji development based on the podcast. They relisten to selected fragments, take notes, divide periods among themselves, and then present the results as a poster or presentation. During their presentations, they can use expressions such as "According to the podcast..." and "The timeline shows that..."

Alternatively, the teacher can organize an "Emoji Debate." The class is divided into two teams: Pros and Cons. The debate consists of three stages: both teams present their views, then ask each other questions, and finally summarize their conclusions. Students can use expressions such as "We strongly believe that..." and "However, our opponents fail to consider..."

Anticipated research. We plan a small quasi-experimental study (pre-/post- with delayed post-test) to examine segmental and suprasegmental pronunciation gains and listening comprehension, comparing podcast-based tasks with business-as-usual instruction across two EFL proficiency bands.

In conclusion, podcasts represent valuable educational resources that combine authentic language exposure with practical application. They enhance listening and pronunciation skills and support creativity, communication, and cultural awareness.

This study highlights their effectiveness in language learning and provides guidance for classroom use. These insights will inform classroom implementation and a forthcoming study; a key task for further research is to determine which podcast task types (e.g., shadowing vs. jigsaw listening) most strongly predict durable gains in pronunciation and listening across proficiency levels.

References:

1. Bahri S., Halimatussadiah. (2024). A qualitative study on the impact of listening podcast on students' pronunciation. *Educator Development Journal*, 2(2). <https://journal.ar-raniry.ac.id/index.php/edj/article/view/6039/2564>
2. Serafini, F. (2013). Reading the visual: An introduction to teaching multimodal literacies. *Teachers College Press*.
3. Syahabuddin K., Rizqa K. (2021). Improving students' listening skill by using podcasts. *Journal of Digital Education, Communication, and Arts (DECA)*, 4(1). <https://jurnal.polibatam.ac.id/index.php/DECA/article/view/2867/1427>

UDC 378.147

Krasovska Anastasiia,

undergraduate student,

Kyiv National Linguistic University

Research advisor

Melnyk Alla,

PhD in Pedagogy, Associate Professor,

Associate Professor of the Department of Germanic and Romance Languages,

Kyiv National Linguistic University

AI IN EDUCATION: BENEFITS, LIMITATIONS, AND CORE FUNCTIONS

Artificial intelligence (AI) is increasingly embedded in educational practice, shaping how teachers design instruction and how students learn. Its rapid adoption since 2023–2025 highlights both promise (scalability, personalization) and concern (accuracy, bias, assessment integrity). Understanding what AI can and cannot do well is therefore timely for educators. The purpose of the work is to analyze AI's core educational functions, benefits, and limitations for teachers and learners. Tasks: (a) synthesize current perspectives from recent reviews and position papers, (b) map practical classroom uses alongside risks, and (c) propose usage guidelines for responsible adoption.

Recent reviews survey ChatGPT's applications and document challenges such as hallucinations, bias, and privacy, while practitioner pieces outline steps to minimize harm and redesign assessment and feedback for responsible use (Ray, 2023; Hamilton, Wiliam, & Hattie, 2023; Giannakos et al., 2024; Yan, Greiff, Teuber, & Gašević, 2024). Together, these perspectives converge on a use-with-guardrails approach: AI can enhance feedback, access, and productivity, but only with human

oversight, clear criteria for quality, and explicit policies on integrity and data protection (Giannakos et al., 2024; Yan et al., 2024).

We argue AI should function as a co-pilot—augmenting teachers and learners—rather than a replacement for educators. In practice, this means: use AI to draft lesson plans, generate practice items, scaffold writing, or simulate dialogue; require human checking for accuracy, bias, and level-appropriateness; and teach students verification strategies (source checks, rubric-based revision, and reflection) (Ray, 2023; Hamilton et al., 2023). *Functions/benefits*: rapid content drafting (plans, quizzes, prompts), formative feedback at scale, language practice (grammar/vocabulary/speaking simulation), and study strategy suggestions (test prep, retrieval practice) (Giannakos et al., 2024). *Risks/limits*: factual errors, hidden bias, uneven creativity, privacy concerns, dependency, and misalignment with curricular goals if unreviewed (Ray, 2023; Yan et al., 2024). *Mitigations*: human-in-the-loop review, dataset/source transparency, bias audits, accuracy sampling, and explicit classroom policies on acceptable AI use (Hamilton et al., 2023).

Future work should: (1) run controlled classroom trials comparing AI-augmented vs. standard instruction on learning outcomes (writing quality, problem solving, language accuracy); (2) audit bias and hallucination rates in educational outputs by subject and level; (3) model cognitive load and workflow fit when students/teachers use AI; and (4) evaluate assessment integrity under different AI policies and task designs (Giannakos et al., 2024; Yan et al., 2024).

In conclusion, AI can improve access to resources, speed formative feedback, and support differentiated practice—when paired with human oversight and explicit verification. The immediate task for educators is to adopt co-pilot workflows: integrate AI for ideation and drafting, require source-backed checking, and align outputs to rubrics and standards (Hamilton et al., 2023; Ray, 2023).

Further research needs identifying which AI–human task mixes (e.g., AI draft → teacher rubric → student revision cycle) maximize learning gains while minimizing bias, errors, and integrity risks across subjects and grade levels (Giannakos et al., 2024; Yan et al., 2024).

References:

1. Giannakos, M., Azevedo, R., Brusilovsky, P., Cukurova, M., Dimitriadis, Y., Hernandez-Leo, D., Järvelä, S., Mavrikis, M., & Rienties, B. (2024). The promise and challenges of generative AI in education. *Behaviour & Information Technology*. Advance online publication. <https://doi.org/10.1080/0144929X.2024.2394886>
2. Hamilton, A., Wiliam, D., & Hattie, J. (2023). *The future of AI in education: 13 things we can do to minimize the damage*. OSF Preprints. <https://doi.org/10.35542/osf.io/372vr>
3. Ray, P. P. (2023). ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope. *Internet of Things and Cyber-Physical Systems*, 3, 121–154. <https://doi.org/10.1016/j.iotcps.2023.04.003>

4. Yan, L., Greiff, S., Teuber, Z., & Gašević, D. (2024). Promises and challenges of generative artificial intelligence for human learning. *Nature Human Behaviour*, 8(10), 1839–1850. <https://doi.org/10.1038/s41562-024-02004-5>

UDC 378.147

Kushnierov Andriy,
undergraduate student,
Kyiv National Linguistic University
Research advisor
Melnyk Alla,
PhD in Pedagogy, Associate Professor,
Associate Professor of the Department of Germanic and Romance Languages, Kyiv
National Linguistic University

AUTHENTIC MEDIA IN TEACHING ENGLISH: VIDEO AND PODCAST

Learning English as a foreign language is a challenge for many students. They need to develop listening, speaking, reading, and writing. Among these, listening and speaking are often the most difficult because learners must understand natural speech and produce accurate pronunciation. In the modern world, teachers cannot rely only on textbooks. New digital tools—such as video, podcasts, and videocasts (video podcasts)—are increasingly important in the classroom. They provide authentic English and make lessons more engaging and active. That is why the topic of using video, podcasts, and videocasts in English lessons is relevant today.

The aim of this work is to explore how video and videocasts can support English language learners, with a focus on improving listening, pronunciation, and engagement. Tasks: (a) synthesize classroom strategies, (b) review evidence on listening/pronunciation, and (c) propose active tasks that move learners beyond passive viewing or listening.

The article by Larry Ferlazzo and Katie Hull Sypnieski offers practical strategies for using video with students. The authors emphasize that video should never be used passively; teachers should design activities that require learners to think, speak, and write about what they see. Suggested techniques include: *Critical pedagogy*: show a short video and ask students to connect it to their lives, pose questions, or discuss social issues. *Back to the screen*: one student watches the video while the other faces away; the watcher describes what happens, then they switch roles (listening + speaking). *Language Experience*

Approach: after viewing, students retell events; the teacher writes their sentences for later reading/grammar work. *Dubbing*: play a clip without sound and have students create the dialogue (pronunciation + speaking). *Other strategies*: preview questions, integrate video. Videocasts are multimedia resources that integrate audio and video. Research suggests they are effective in English language learning. For example, Grynova, Rafalska, and Polodyuk (2023) argue that videocasts combine

with reading texts, and use inductive discovery tasks. The main idea is that video is most sound with images to support comprehension, motivate learners, and provide authentic input. Videocasts also aid speaking development: Pradana (2017) found that integrating videocasts into a drama class improved students' speaking ability and motivation, raising average performance scores by more than 10 points.

Common findings across these studies are clear: video and videocasts provide real-life English, enable repetition, foster learner autonomy, and connect listening with speaking as learners repeat or shadow voices they hear. We argue that video, podcasts, and videocasts should complement—rather than replace—core instruction through scaffolded, task-based activities with clear assessment criteria.

After reviewing these materials, we believe both videos and videocasts are excellent tools for language classrooms. Active video tasks are especially valuable; simply playing a clip and asking students to watch silently has limited learning impact. When teachers ask learners to describe, predict, summarize, or create dialogues, learning becomes much stronger. I also think videocasts are particularly helpful for beginners because body language and visuals clarify meaning. At the same time, challenges include fast speech rates, unequal access to devices or bandwidth, and the time required to design highquality tasks. Sharing a podcast link is not enough—teachers should plan activities around it.

We will conduct a quasi-experimental study (pre-/post- with a delayed post-test) comparing active video/podcast/videocast tasks to business-as-usual instruction, measuring listening comprehension and pronunciation (segmental and suprasegmental features) as well as learner engagement across two proficiency bands.

Using video and videocasts in English teaching is highly effective. Videos can increase motivation and enable creative speaking tasks, while videocasts support pronunciation. Evidence indicates that these tools provide authentic input and promote learner independence. However, teacher design remains crucial: if videos are used passively, effects are small; if teachers prepare active exercises—discussion, dubbing, shadowing, summarizing—students learn more deeply. In future practice, teachers should balance traditional methods with digital tools to build engagement, improve listening comprehension, and develop better pronunciation. Key problem for further research: which task types (e.g., dubbing, shadowing, “back to the screen”) most strongly predict durable gains in listening and pronunciation, and how can these outcomes be assessed reliably?

References:

1. Ferlazzo, L., & Hull Sypnieski, K. (n.d.). Eight ways to use video with English-language learners. *Edutopia*.
<https://www.edutopia.org/blog/ell-engagement-using-video-larryferlazzo-katie-hull-sypnieski>
2. when learning English as a method for developing listening skills. *Collection of Scientific Works of Uman State Pedagogical University*, (3), 14–21.
<https://doi.org/10.31499/23074906.3.2023.289871>

3. Pradana, S. A. (2017). The use of videocast in improving the speaking ability integrated in a drama class. *Engedu Journal*, 2(1), 45–54. <https://ejournal.radenintan.ac.id/index.php/ENGEDU/article/view/389>

UDC 371.3

Lubko D.V.
*Associate Professor, Candidate of Technical Sciences,
Motornyi Dmytro
Tavria State Agrotechnological University (Zaporizhzhia)*

THE USE OF MODERN INTERACTIVE INFORMATION SYSTEMS IN TEACHING THE DISCIPLINE "COMPUTERS AND COMPUTER TECHNOLOGIES" FOR 1ST YEAR UNIVERSITY STUDENTS

In today's digitalized society, the learning process increasingly depends on how effectively modern information technologies are used, which allow not only to transfer knowledge, but also to actively involve students in the educational process, creating an environment in which they can work with materials, perform practical tasks, exchange ideas and receive feedback from teachers in real time. This is especially important for first-year students who are just starting to get acquainted with basic disciplines, such as "Computers and Computer Technologies", and for whom the first steps in learning a systems approach to working with computers can be difficult and require more practical involvement than traditional lectures, since it is often difficult for beginners to simultaneously master theoretical concepts, the structure of computer systems and basic skills in working with software and hardware. The purpose of this article is to study the role of modern interactive information systems in teaching the discipline "Computers and Computer Technologies", outline the advantages and problems of using such systems, and provide practical recommendations that allow to increase the effectiveness of learning and make the process more interesting and accessible for students with different levels of training.

Interactive information systems in education.

Interactive information systems in education are a set of hardware and software tools that provide two-way interaction between students and the teacher. They allow for the exchange of educational materials, testing, online assessment of results, and group projects and simulations. This allows the educational process to become more flexible, adapted to the individual needs of students, and open to remote access, which is especially relevant in conditions of distance learning or restrictions associated with quarantine measures. Modern scientific and methodological research on this subject topic [1-5] shows that the use of interactive systems not only increases the level of material assimilation, but also develops students' digital competencies, prepares them for work in a modern information environment, forms independent learning and critical thinking skills. It also creates conditions for personalized

learning, where each student can work at their own pace, repeat complex topics, and receive additional materials at a convenient time.

Features of teaching the discipline "Computers and Computer Technologies".

This discipline is one of the key ones for first-year students, as it forms fundamental knowledge of the IT industry.

For example, at the Dmytro Motornyi Tavria State Agrotechnological University (Zaporizhzhia), first-year studentsG3 specialties „Electrical Engineering” under the educational professional programs “Digital Technologies of Electrical Engineering” and “Electrical Power Engineering, Electrical Engineering and Electromechanics” are starting to receivepractical skills in working with application software. Namely:theoretical and practical knowledge related to the work of the Microsoft Office suite, namely the basics of practical work with Microsoft Word and Microsoft Excel.

For first-year studentsin the specialty H7 "Agroengineering" foreducational professional program"Agroengineering", which is studied for two semesters (a year of studying the discipline), additionally introduces the study of the basics of programming. Namely: inStudy and familiarization with the basics of algorithmization using the Visual Basic language. That is, studying the general principles of object-oriented programming and acquiring skills in the practical application of programming when solving typical problems using the Visual Basic language.

Also, for those who wish to gain additional useful knowledge, participation in a scientific student group is provided. It studies the design of various engineering systems using the platform (microcontroller) Arduino. Participation and work in the group is held outside of school hours, free of charge and open to all interested parties. The objectives of such a group are:acquiring skills for independent work with scientific and technical literature; generalizing accumulated experience, the ability to make scientifically sound conclusions and recommendations for creating software products; forming the ability to give a mathematical statement of the problem; developing the ability to develop algorithms for created software products and choosing tools for implementing the proposed algorithm; the ability to design, compile and build electrical circuits using a structural approach; the ability to use previously acquired knowledge to solve various practical problems.

The development and independent implementation of practical work using the Arduino microcontroller in this group plays a significant role in deepening students' knowledge using modern interactive technologies. And all this provides a combination and synthesis of already acquired knowledge in the field of drawing up electrical circuits and creating software code for the Arduino microcontroller, that is, it combines knowledge of physics, mathematics, electrical technologies and programming. The proposed stages of creating an automated device, as well as the issue of involving students in solving the tasks set, create an effective impact on the activation of learning in a higher educational institution and can be successfully implemented in the modern education system in the field of educational practice.

Advantages of using interactive systems.

The use of interactive systems in learning allows to significantly increase the involvement of students. As they take an active part in completing tasks, discussions and projects, at the same time developing their digital competences, getting used to working in online environments, mastering tools for creating documents, presentations, spreadsheets, working models and software products. They also acquire self-organization skills, as they have the opportunity to work at their own pace, repeat complex topics and use additional materials for a better understanding of concepts, which ultimately contributes to the formation of independent learning and critical thinking. It also increases the effectiveness of knowledge control, as the teacher can receive data on student performance in real time, analyze errors and adapt tasks to the needs of each participant in the process, which is especially important when working with students who are just starting to get acquainted with information technologies and need more support and clarity in teaching.

Practical recommendations for effective use.

To achieve maximum efficiency in using interactive systems, teachers should combine traditional lectures with practical tasks in a digital environment, introduce gamification elements that stimulate student activity, organize group work where students complete projects together, use video lectures and interactive simulations for better assimilation of the material, provide regular feedback and monitoring of progress, and constantly improve their own qualifications in working with new platforms and digital resources, which allows making learning not only accessible and interesting, but also as effective as possible for students with different levels of training and different learning styles.

Conclusions.

The use of interactive information systems in teaching the discipline "Computers and Computer Technologies" for first-year university students is an important tool that allows you to combine theoretical training with practical exercises, increases student interest, forms the necessary digital competencies, provides access to educational materials at any time and increases the effectiveness of knowledge control, while at the same time requiring attention to technical aspects, teacher training and student motivation, and its implementation contributes to the preparation of competitive specialists who are able to work effectively in a modern information environment and adapt to rapidly changing technologies.

References:

1. Bikov V. Yu. Informacijni tehnologiyi i zasobi navchannya (Information technology and learning tools) . Kiyiv: IITZN NAPN Ukrayini. 2017. (Ukrainian)
2. Zhaldak M.I. Komp'yuterno-oriyentovani sistemi navchannya (Computer-oriented learning systems). Kiyiv: NPU imeni M. P. Dragomanova, 2016. (Ukrainian)
3. Siemens G. Connectivism: A Learning Theory for the Digital Age. International Journal of Instructional Technology & Distance Learning. 2005.
4. Bates A. W. Teaching in a Digital Age: Guidelines for Designing Teaching and Learning. – Vancouver: Tony Bates Associates Ltd. 2019.

5. Anderson T., Elloumi F. (Eds.). Theory and Practice of Online Learning. – Athabasca University Press. 2008.

UDC 004.932.2

Lysenko D. O.

Student,

Kharkiv National University of Radio Electronics, dep. INF

Email: danylo.lysenko@nure.ua

Academic supervisor

Kobylin I. O.

Ph.D., Assistant Professor

Kharkiv National University of Radio Electronics, dep. INF

METRICS FOR EVALUATING MACHINE TRANSLATION BASED ON VECTOR -BASED REPRESENTATIONS

Machine translation, which automates the process of transferring the meaning of a text from one language to another, has become an integral part of many application systems and services, ranging from automatic localization of web content to supporting interlingual communication between people on the Internet. Accordingly, it is important to accurately measure how closely a machine translation corresponds to the meaning of the original text and is understandable to the user.

The most well-known tool for evaluating machine translation is BLEU (Bilingual Evaluation Understudy). This metric is calculated using the following algorithm:

$$BLEU = BP \cdot \exp\left(\sum_{n=1}^N w_n \log p_n\right)$$

Where p_n – precise of n -grams, w_n – weight for n -grams

BLEU evaluates the quality of machine translation by comparing sequences of words (n -grams) in the translation with the same ones in human references. It counts how many of these n -grams match and then combines these accuracies into an overall score. In addition, BLEU penalizes translations that are too short to avoid overestimating the result. The result is a score from 0 to 1, where 1 means the translation matches the reference perfectly.

Despite this metric being simple and convenient for automatic evaluation, it does not consider semantics, synonymic replacements, word permutations, and context. As a result, a high-quality translation with appropriate content may receive a low score due to lexical differences, which reduces the reliability of the results and constrains the effectiveness of the metric in real-world tasks. The development of

transformers, particularly BERT, has changed translation evaluation by enabling the creation of vector-semantic metrics that analyze not only lexical matches but also the deep semantics of the text through contextual vector representations. This advancement allows evaluation methods to better capture the nuances of meaning beyond surface-level text comparison. For example, the word "light" has different meanings and grammatical functions depending on the context, as seen in the phrase "light a candle" (verb) versus "light traffic" (adjective).

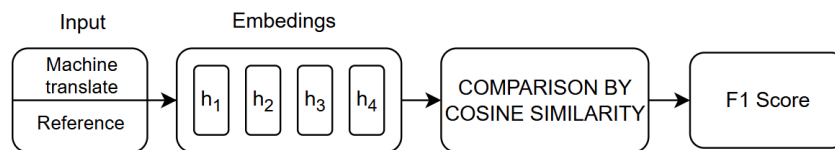
$$h_{light, context = "candle"} = [0.18, -0.42, 0.63, 0.77, \dots, -0.15] \in R^{768}$$

$$h_{light, context = "traffic"} = [-0.21, 0.55, -0.34, 0.12, \dots, 0.49] \in R^{768}$$

Where R^{768} – space with 768 real numbers

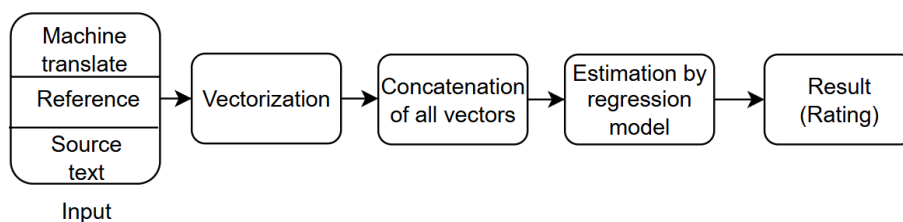
When evaluating the quality of machine translation, metrics based on these vector representations compare the vectors of the translated text with the vectors of the reference translation. Most often, they use cosine similarity, a measure that estimates the angle between two vectors in a multidimensional space. The smaller the angle, the higher the semantic similarity between the two texts. Also, thanks to contextualized embeddings, metrics are able to identify subtle semantic nuances, synonymic replacements, and other linguistic features that traditional lexical metrics cannot capture. As a result, this approach makes the assessment more accurate and closer to human perception, since people are oriented not only to literal word matches, but also to the overall meaning and logic of statements.

In this context, modern metrics such as BERTScore and COMET use these capabilities to more accurately evaluate machine translation. BERTScore calculates accuracy and completeness based on vector matches and then combines them into an F1 score, which better reflects translation quality, especially in cases of synonymic replacements and stylistic variations.



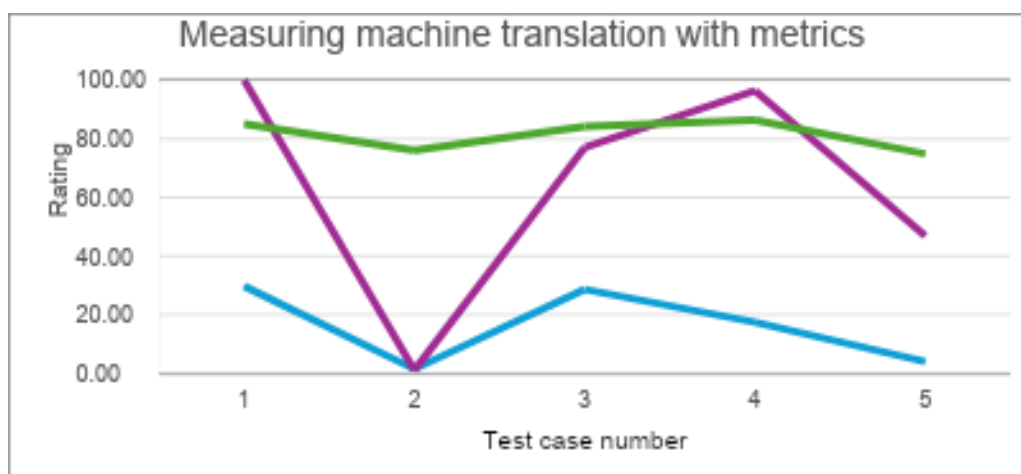
Picture 1 – Visualization of the BERTScore algorithm

COMET complements this idea by adding not only machine and reference translations to the analysis, but also the source text, allowing it to assess the accuracy of the original meaning. In addition, COMET learns from large datasets with human evaluations, making its results more reliable and as close as possible to human subjective perception.



Picture 2 – Visualization of the COMET algorithm

Now let's perform a small research where, using the Helsinki-NLP/opus-mt-cs-uk model, we will translate 5 examples of small paragraphs and evaluate the results using the above metrics. We will visualize the obtained results.



Picture 3 – Evaluation of machine translation using selected metrics using the Opus-mt-cs-uk model

Thus, the research demonstrates that the BLEU metric, which evaluates translation primarily through n-gram matches, is significantly inferior to the modern neural metrics COMET and BERTScore. Unlike BLEU, these methods rely on contextualized embeddings and transformer models, which provide high semantic sensitivity and allow for paraphrasing, synonymic variations, and word permutations to be considered. As can be seen from the table, BLEU often gives low scores for translations with different wording, while COMET and BERT-F1 demonstrate consistent adaptability and correlation with the meaning of the sentence. This confirms that the use of modern neural network metrics significantly improves the accuracy of automatic translation evaluation and better reflects the quality of the text from the point of view of human perception.

References

1. Zhang, T., Kishore, V., Wu, F., Weinberger, K. Q., & Artzi, Y. (2019). Bertscore: Evaluating text generation with bert. *arXiv preprint arXiv:1904.09675*.
2. Unanue, I. J., Parnell, J., & Piccardi, M. (2021). BERTTune: Fine-tuning neural machine translation with BERTScore. *arXiv preprint arXiv:2106.02208*.

3. Jaskowski, S., Chava, S., & Shah, A. (2024). BERTScoreVisualizer: A Web Tool for Understanding Simplified Text Evaluation with BERTScore. *arXiv preprint arXiv:2409.17160*.

4. Datta, G., Joshi, N., & Gupta, K. (2022, November). Analysis of automatic evaluation metric on low-resourced language: BERTScore vs BLEU score. In *International Conference on Speech and Computer* (pp. 155-162). Cham: Springer International Publishing.

UDC 004.942

Mazepa A.S.

(andrii.mazepa@nure.ua)

Kharkiv National University of Radio Electronics

DYNAMIC DECISION SUPPORT SYSTEM WITH MULTI-AGENT ORCHESTRATION FOR RISK MANAGEMENT IN SOFTWARE PROJECTS

This paper proposes a dynamic decision support system (DSS) for IT project risk management based on multi-agent orchestration. It describes key functional agents—such as log monitoring, regulatory compliance, risk matrix updates, and audit governance—and explains how they interact through an orchestrator. Drawing on best practices from cybersecurity, healthcare, and infrastructure, the study demonstrates that agent-based DSS architectures enhance adaptability, explainability, and compliance in volatile environments.

Modern IT projects are increasingly exposed to unpredictable risks: changing requirements, human error, cyberattacks, and evolving regulatory frameworks such as DORA, ISO 27001, and NIST. Traditional decision support systems (DSS) are usually static and do not respond adequately to real-time changes. As a result, decisions are often delayed or taken without considering critical shifts in the environment.

A modular, event-driven DSS is required—one that integrates diverse sources of risk, reacts in real time, and adapts to changes in its operating context [1, 3, 6, 7].

The proposed architecture is based on a multi-agent system (MAS) where each component is an autonomous agent responsible for a specialized function:

- Log monitoring agent – extracts critical signals from system logs and alerts, identifies risk patterns, and initiates updates in the risk model [6, 4].
- Risk matrix agent – recalculates risk probabilities and impacts based on incoming event data, audit results, or training outcomes [5, 7].
- Regulatory compliance agent – monitors changes in regulatory standards (DORA, GDPR, etc.) and updates internal compliance metrics accordingly [3, 4].

- Impact assessment agent – models the financial and operational consequences of risk scenarios using expert rules or statistical projections [5, 7].
- Simulation agent – runs stochastic simulations to evaluate "what-if" scenarios and prepare for low-probability, high-impact events [5, 7].
- Governance and audit agent – ensures transparency, traceability, and explainability of decisions made by other agents, supporting governance and compliance frameworks [3, 4].

This agent-based approach follows the principle of separation of concerns, where each agent handles a well-defined role. Agents may use rule-based logic, statistical models, or large language models (LLMs), allowing the system to be both diverse and specialized [2, 4, 6].

Scalability is achieved through the ability to dynamically add, remove, or modify agents without disrupting the overall system. This flexibility is essential in environments where threats, requirements, and constraints change frequently [2].

A central orchestration agent coordinates the behavior of all modules. It routes tasks, aggregates partial results, and ensures that workflows align with system priorities and event context [2, 4, 6]. This architecture reflects modern orchestration strategies found in agentic SOAR systems [6].

The governance layer follows the TRiSM (Trust, Risk, and Security Management) model [3], providing:

- logging of all agent activities;
- justification of each decision (explainability);
- continuous verification of compliance with defined rules [3, 4].

Practical implementations in adjacent domains support this architecture. In healthcare, multi-agent DSS systems have proven effective in dynamic, high-stakes environments [4]. In cybersecurity, agentic SOAR frameworks reduced incident response times by over 30% [6]. In infrastructure and supply chain management, multi-agent simulations demonstrated the ability to handle uncertain and incomplete data [5, 7].

This evidence confirms that agent-based, orchestrated, and auditable DSS architectures are both viable and necessary for modern IT risk management.

References

1. Reid A., Lam A., Leins K., Humphreys L. *Risk Analysis Techniques for Governed LLM-based Multi-Agent Systems*. arXiv:2508.05687. URL: <https://arxiv.org/abs/2508.05687>
2. Chen C.H., Shiu M.F. *AgentFlow: Resilient Adaptive Cloud-Edge Framework for Multi-Agent Coordination*. arXiv:2505.07603. URL: <https://arxiv.org/abs/2505.07603>
3. TRiSM Collective. *TRiSM for Agentic AI: A Review of Trust, Risk, and Security Management*. arXiv:2506.04133. URL: <https://arxiv.org/abs/2506.04133>
4. Chen Y.J., Sheikh H., et al. *Reinforcing Clinical DSS through MAS and Ethical AI Governance*. arXiv:2504.03699. URL: <https://arxiv.org/abs/2504.03699>

5. Singh D., Iqbal F., et al. *Towards Resilient Cities: A Hybrid Simulation Framework*. arXiv:2501.04746. URL: <https://arxiv.org/abs/2501.04746>
6. Ismail R., Abdirashid A., Faisal M., Khan S. *Toward Robust SOAR with Agentic AI*. Information, MDPI, 2025, Vol. 16(5), Article 365. DOI: <https://doi.org/10.3390/info16050365>
7. Karunaratne P., Abbas K. *Multi-Agent Simulation for DSS in Supply Chain Risk Management*. ResearchGate, 2024. URL:

UDC 343.627

Oliinyk M.V.

*First (Bachelor) level higher education student,
Educational and Research Institute No. 1,
Kharkiv National University of Internal Affairs
Scientific adviser*

Sazanova L.S.

*Senior Lecturer of the Department of Language Training,
Kharkiv National University of Internal Affairs*

USING ARTIFICIAL INTELLIGENCE AND BIG DATA ANALYTICS TO PREDICT CONFLICTS

The modern world is characterised by highly dynamic socio-political processes, accompanied by numerous conflicts of varying scale, from local clashes to international crises. Timely conflict prediction is an important aspect of ensuring the security of states and societies. Traditional methods based on expert assessments and statistical analyses often prove to be insufficiently effective due to limited data and subjective assessments. In this context, the use of artificial intelligence and big data analytics opens new opportunities for improving the accuracy of conflict prediction, allowing for the timely identification of potential threats and the development of effective response measures.

Conflict prediction is a complex multifactorial task that considers political, economic, social, and cultural aspects. Machine learning and deep learning models can identify hidden patterns in large amounts of data that are not accessible to classical analysis. Big data analytics allows information from various sources to be processed, including social networks, mass media, open government databases, and international statistical resources. Using this data in combination with artificial intelligence algorithms allows us to build predictive models that consider time series, interrelationships between events, and possible scenarios for conflict escalation.

The impact of artificial intelligence on society and professional activities is already being actively discussed in scientific and business circles. The potential that the artificial intelligence (AI) era opens for organizations and work teams can change the social environment and working conditions for the better, increase employee satisfaction, realise their potential, improve customer experience and, as a result,

contribute to increased profitability. For senior managers, this means developing existing skills, both their own and those of their employees, rather than replacing them.

Effective conflict management requires the development of communication skills, dispute resolution training, transparent conflict resolution procedures, a supportive work environment, and teamwork. To this end, organisations can use various types of AI, including text analysis (natural language processing (NLP), machine learning, network analysis), chatbots, face and speech recognition [1]. NLP allows communication data to be analysed to identify potential conflicts, overcome cultural and language barriers, determine the negative emotional tone of text, and prevent conflicts.

Innovative systems such as cogSolv can model people's reactions, take their worldview into account, and assist in conflict resolution in humanitarian missions [2]. Artificial intelligence for practicing conflict resolution (AI4PCR) analyses user text and provides feedback on the effectiveness of communication in conflict situations at work [3].

Chatbots can act as neutral mediators, offer solutions, and help parties engage in constructive dialogue [4]. Katharina E. Höne emphasizes that the main advantage of AI as a mediator is its neutrality and objectivity, although there are risks of bias due to incomplete or incorrect data [5].

Machine learning and deep neural networks allow the creation of highly accurate conflict prediction models. For example, in a study by Olabanji, Olaide, and Ojo, a Deep Neural Network (DNN) model was created to predict conflicts, which demonstrated 98% accuracy on the training set and 89% on the test set [6].

At the same time, the use of AI raises ethical questions, particularly regarding confidentiality, voluntary consent of employees, absence of algorithm bias, and control of personal data [7].

It is important to ensure transparency, security, and compliance with personal data protection legislation. The development of legal regulation of AI is becoming relevant for many countries, particularly in the European Union, where a comprehensive Artificial Intelligence Act has been adopted. Harmonizing Ukrainian legislation with European legislation in the field of AI will contribute to the balanced use of technology and the protection of citizens' rights [8].

Ethical aspects of AI use include considering the cultural, religious and value differences of employees in conflicts and avoiding excessive control, which can negatively affect the moral climate. Adherence to these principles is key to the effective and fair use of AI in organizations for conflict management.

Thus, the use of artificial intelligence and big data analytics opens prospects for the creation of comprehensive early warning systems for conflicts. This approach allows for more accurate forecasts, timely identification of threats, and planning of effective response measures. To improve the effectiveness of forecasting, it is necessary to combine AI technologies with traditional methods of analysis and expert assessments, consider socio-political factors, and ensure ethical data processing. In the future, this will contribute to improving security at the national and international levels and creating a more stable socio-political environment.

References:

1. Zachary Amos, How AI Can Improve Conflict Resolution in the Workplace URL: <https://swisscognitive.ch/2024/04/11/how-ai-can-improve-conflict-resolutionin-the-workplace/>
2. Daniel J. Olsher, New Artificial Intelligence Tools for Deep Conflict Resolution and Humanitarian Response URL: https://www.researchgate.net/publication/282536309_New_Artificial_Intelligence_Tools_for_Deep_Conflict_Resolution_and_Humanitarian_Response
3. Anne Hsu, Divya Chaudhary, AI4PCR: Artificial intelligence for practicing conflict resolution URL: <https://www.sciencedirect.com/science/article/pii/S2949882123000026>
4. Research HR Acuity, 2024 Guide to Employee Relations and Workplace Investigations ctp. 4 URL: https://2930928.fs1.hubspotusercontentna1.net/hubfs/2930928/HRA_2024Guide_01302024.pdf#page=4
5. Katharina E. Höne, Mediation and artificial intelligence: Notes on the future of international conflict resolution URL: https://www.diplomacy.edu/wpcontent/uploads/2021/06/Mediation_and_AI.pdf
6. Olabanji B. Olaide, Adebola K. Ojo, A Model for Conflicts' Prediction using Deep Neural Network URL: <https://www.ijcaonline.org/archives/volume183/number29/olaide-2021-ijca921667.pdf>
7. Zembra Ye. Suchasni tekhnolohii rozpiznavannia oblych ta prava liudyny. URL: <https://naub.oa.edu.ua/suchasni-tehnolohiji-rozpiznavannya-oblych-ta-pravalyudyny/> (In Ukrainian)
8. Tarasenko N. Shtuchnyi intelekt yak ob'ekt pravovoho rehuliuвання v Ukraini ta sviti. Informatsiino-analitychnyi biuleten. Shliakhy rozvytku ukrainskoi nauky: suspilnyi dyskurs. № 6 (199). 2024. 13 s. URL: <https://files.nas.gov.ua/PublicMessages/Documents/0/2024/07/24070413103087-4907.pdf> (In Ukrainian)

Onyshchenko Iryna,
undergraduate student,
Kyiv National Linguistic University
Scientific advisor

Melnyk Alla,
PhD in Pedagogy, Associate Professor,
Associate Professor of the Department of Germanic and
Romance Languages,
Kyiv National Linguistic University

BALANCING TRADITIONAL EXAMS AND ALTERNATIVE ASSESSMENT IN ONLINE EDUCATION

Assessment plays a central role in education because it not only measures students' knowledge but also shapes how they learn, their motivation, and the development of key skills. The rapid transition to online education in 2020–2021 revealed both the advantages and limitations of different assessment types. Traditional exams—timed, proctored, or closed-book—offer standardization and comparability of results. However, they often produce high stress and may insufficiently capture practical or real-world skills (Holden, Norris, & Kuhlmeier, 2021; Krueger, 2024).

In contrast, alternative assessment methods—project-based tasks, portfolios, open-book exams, and peer- and self-assessment—emphasize authentic learning, critical thinking, and problem-solving (British Council, 2021; Lazareva & Agostini, 2024). These approaches can deepen engagement but demand time, resources, and careful design to ensure fairness and reliability. Finding a balance between traditional and alternative approaches is essential for online education that is both rigorous and engaging.

The goal of this paper is to explore effective strategies for assessing students in online education by comparing traditional exams with alternative methods and examining their advantages and limitations. The focus is on supporting academic integrity, encouraging deep learning, and enhancing student motivation while addressing large class sizes, unequal access to technology, and teacher preparation. The review draws on sources from 2021–2025 to reflect current practices.

Tasks: (a) synthesize pros and cons of traditional and alternative assessments, (b) identify design principles that support integrity, motivation, and deep learning online, and (c) propose implementation guidelines for large classes and unequal technology access.

Traditional online exams are generally perceived as fair, comparable, and efficient to grade, enabling institutions to evaluate large cohorts consistently and provide standardized results (Holden et al., 2021). Many students consider these exams reliable indicators of knowledge. Yet studies also highlight drawbacks—heightened anxiety, rigid formats, and limited capacity to assess

complex skills or real-life performance—often exacerbated online by technical issues and unfamiliar tools (Krueger, 2024).

Alternative methods—portfolios, projects, open-book exams, and peer assessment—promote authentic learning and critical thinking, often increasing motivation and engagement (British Council, 2021). Case work from higher education systems undergoing change also reports benefits, while noting challenges of time-intensive grading and maintaining objectivity in large classes (Lazareva & Agostini, 2024). Technology access remains a persistent equity concern: not all students have stable connectivity or suitable devices (Lazareva & Agostini, 2024).

Poorly designed online assessments can overload working memory, elevate stress, and depress performance; therefore, assessments should be planned to balance rigor, accessibility, and psychological comfort (Surbakti, Umboh, Pong, & Dara, 2024). Emerging work suggests AI-based tools can assist with automated testing, instant feedback, and progress monitoring—potentially strengthening integrity checks and personalization (Martin, Kim, Bolliger, & DeLarm, 2025).

We argue that a hybrid assessment model—combining traditional exams with alternative tasks—offers the best balance of fairness, comparability, authenticity, and student engagement in online education. Traditional exams can verify core knowledge efficiently and comparably, while alternative tasks cultivate creativity, collaboration, problem-solving, and transfer to real-world contexts (Holden et al., 2021; British Council, 2021; Lazareva & Agostini, 2024). Clear rubrics, structured instructions, and regular formative checks are critical for fairness and transparency. Professional development is needed so instructors can design and implement diverse assessments effectively, and institutions should work to guarantee equitable technology access (Lazareva & Agostini, 2024). *Traditional elements:* closed-book midterms, timed quizzes with large item banks, and proctoring where appropriate (Holden et al., 2021). *Alternative elements:* digital portfolios tracking growth; project/case assignments with reflection; formative quizzes with immediate feedback; peer- and self-assessment to build metacognition (British Council, 2021). *Design considerations:* minimize unnecessary cognitive load, provide practice environments for tools, and scaffold complex tasks with milestones and exemplars (Surbakti et al., 2024). *AI support:* use automated feedback and analytics to surface misconceptions, personalize practice, and monitor progress—paired with human judgment for high-stakes decisions (Martin et al., 2025).

Both traditional and alternative methods have strengths and limitations online. Evidence from 2021–2025 supports a combined approach in which traditional exams provide fairness and comparability while alternative tasks deliver authentic learning experiences and foster critical thinking (Holden et al., 2021; British Council, 2021; Lazareva & Agostini, 2024; Krueger, 2024). Institutions should invest in professional development, ensure equitable access to technology, intentionally blend formative and summative assessments, and leverage AI tools judiciously for feedback and monitoring (Martin et al., 2025).

Future studies should examine long-term learning and well-being outcomes of hybrid assessment, model cognitive-load profiles across assessment types, and analyze equity impacts related to bandwidth and device access (Surbakti et al., 2024;

Martin et al., 2025).

Key open question is which specific hybrid mixes (e.g., closed-book midterm + portfolio + oral defense) optimize integrity and deep learning at scale in large online cohorts?

References:

1. British Council. (2021). *Assessing learners online: Noticing, self-checking and online quiz tools* (pp. 1–2). TeachingEnglish. https://www.teachingenglish.org.uk/sites/teacheng/files/Assessing-learners-online_noticing-self-checking-online-quiz-tools.pdf
2. Holden, O. L., Norris, M. E., & Kuhlmeier, V. A. (2021). Academic integrity in online assessment: A research review. *Frontiers in Education*, 6, Article 639814. <https://www.frontiersin.org/articles/10.3389/feduc.2021.639814/full>
3. Krueger, M. (2024). *Comparing online and traditional assessment practices in middle school mathematics* (pp. 13–18). Minnesota State University. <https://red.mnstate.edu/cgi/viewcontent.cgi?article=1846&context=thesis>
4. Lazareva, A., & Agostini, D. (2024). Shifting from traditional to alternative assessment methods in higher education: A case study of Norwegian and Italian universities (pp. 537–538). *SciTePress*. <https://www.scitepress.org/Papers/2024/126233/126233.pdf>
5. Martin, F., Kim, S., Bolliger, D. U., & DeLarm, J. (2025). Assessment types, strategies, and feedback in online higher education courses in the age of artificial intelligence: Perspectives of instructional designers. *TechTrends*. <https://doi.org/10.1007/s11528-025-01115-8>
6. Surbakti, R., Umboh, S. E., Pong, M., & Dara, S. (2024). Cognitive load theory: Implications for instructional design in digital classrooms. *International Journal of Educational Narratives*, 2(6), 487–490. <https://journal.ypidathu.or.id/index.php/ijen/article/view/1659>

*Postol Yulia,
undergraduate student,
Kyiv National Linguistic University
Research advisor*

*Melnyk Alla,
PhD in Pedagogy, Associate Professor,
Associate Professor of the Department of
Germanic and Romance Languages,
Kyiv National Linguistic University*

TIKTOK AS A LANGUAGE LEARNING TOOL: PRONUNCIATION AND COMMUNICATION PRACTICE

The rise of short-form video platforms has transformed how young people communicate and learn. TikTok offers new opportunities for foreign language education, particularly for developing pronunciation and communication skills. Purpose: to analyze TikTok's affordances for pronunciation and communicative practice in EFL and outline classroom tasks. Tasks: (a) synthesize theory on multimodal/visual literacy, (b) review recent empirical evidence, and (c) propose implementable classroom activities. Given TikTok's ubiquity, it can increase motivation by offering short, manageable tasks that promote active participation; however, despite widespread use, pedagogically grounded guidance for TikTok in ELT remains limited.

This topic is especially relevant because modern learners spend much of their free time on social media. By integrating these platforms into education, teachers can connect learning with students' everyday experiences and digital habits.

From multiple perspectives—multimodal literacy (Apkon, 2013; Serafini, 2013), visual-literacy pedagogy (Goldstein, 2016), and recent EFL studies (Li, 2024; Rahmawati et al., 2023)—evidence converges on benefits, while concerns remain about privacy, distraction, and assessment. Building on Apkon's argument about literacy in a world of screens, TikTok can be viewed not merely as entertainment but as a learning environment that integrates visual, linguistic, aural, and spatial dimensions of meaning-making (Apkon, 2013). The design of TikTok videos—camera framing, filters, transitions, captions, voice-overs, and sound effects—supports learners' ability to perceive, analyze, and reproduce authentic language use in dynamic settings (Serafini, 2013). For example, pronunciation practice can improve when learners attend to clear rhythm, rehearse with background music, and complete lip-sync tasks that model native-speaker delivery. Communication skills are developed through duets, collaborative trends, and comment-based interactions that encourage spontaneous language production.

A persistent challenge in traditional language learning is limited access to authentic, motivating practice. Students may memorize vocabulary and grammar but

lack opportunities for natural, expressive speech in real-life contexts. TikTok helps to close this gap.

Recent empirical studies further support TikTok's potential. In a study of Chinese EFL learners at Universiti Malaya, Li (2024) found measurable improvements in pronunciation accuracy when learners engaged in TikTok-based tasks, especially those requiring repetition, imitation, and peer feedback. Similarly, Rahmawati et al. (2023) report gains in speaking confidence and fluency, with learners experimenting with new vocabulary and expressions in authentic contexts. These findings align with visual-literacy work emphasizing the integration of images, sound, and text while producing clear speech (Goldstein, 2016).

We argue that TikTok should complement structured instruction via scaffolded, task-based activities. From a pedagogical perspective, tasks such as creating short pronunciation challenges, annotating videos with on-screen text, or participating in global trends provide authentic communicative purposes and motivate learners to improve expressive skills. Unlike many classroom exercises, TikTok's micro-video format requires concise, impactful communication, training learners to manage intonation, clarity, and body language in ways that resemble real-world interaction. Teachers can scaffold this work with simple pronunciation drills, speaking challenges, or short video diaries, and pair TikTok with apps such as Duolingo or Flip. Adding TikTok to blended learning diversifies practice beyond text to include voice, gesture, and visuals. Key constraints—privacy, distraction, and assessment validity—require clear classroom policies and rubrics.

TikTok can also strengthen self-regulated learning. By creating videos and participating in challenges, students assume greater responsibility, set personal goals, and monitor progress. This approach encourages creativity, problem solving, and confidence—skills valuable for both language learning and broader personal development. Rather than replacing traditional methods, TikTok should complement them, adding energy, creativity, and authenticity when coupled with structured teacher-led tasks.

A practical illustration is the widespread trend of repeating lines from well-known advertisements or short clips, where users imitate rhythm, intonation, and emotional delivery. Such shadowing-style practice promotes articulation, stress patterns, and fluency while sustaining motivation through play and creativity. Re-recording supports immediate self-feedback (and sometimes peer feedback), turning everyday entertainment into meaningful pronunciation training.

Conclusion and anticipated research. TikTok exemplifies how digital tools can reshape foreign language learning, particularly by improving pronunciation accuracy and communicative competence. As others have argued, literacy in the digital age entails mastering new forms of expression; TikTok provides a rich, multimodal environment for active language use (Apkon, 2013; Serafini, 2013). Future research will examine long-term retention of segmental and suprasegmental gains using pre-/post-/delayed measures, and compare outcomes by proficiency level and age group, alongside effects on vocabulary growth and intercultural communication (Li, 2024; Rahmawati et al., 2023).

References:

1. Apkon, S. (2013). *The age of the image: Redefining literacy in a world of screens*. Farrar, Straus and Giroux.
2. Goldstein, B. (2016). *Visual literacy in English language teaching*. Cambridge University Press. <https://bit.ly/3kHaF5Y>
3. Li, H. (2024). The impact of TikTok on pronunciation skills: A study of Chinese EFL learners in Universiti Malaya. *Journal of Language Testing & Assessment*, 7(1), 8–15. <https://www.clausiuspress.com/article/13280.html>
4. Rahmawati, D., Sari, N., & Pratiwi, L. (2023). Exploring TikTok's impact on enhancing speaking skills in language learning. *Journal of English Language Teaching*, 12(2), 45–58. <https://jurnal.unipasby.ac.id/jet/article/download/8356/5256/28756>
5. Serafini, F. (2013). *Reading the visual: An introduction to teaching multimodal literacies*. Teachers College Press.

UDC 654:681

Repchonok S.A.

*First (Bachelor) level higher education student,
Educational and Research Institute No. 1,
Kharkiv National University of Internal Affairs
Scientific adviser*

Sazanova L.S.

*Senior Lecturer of the Department of Language Training,
Kharkiv National University of Internal Affairs*

PROMISING NETWORK TECHNOLOGIES IN THE DEVELOPMENT OF INFORMATION INFRASTRUCTURE

Promising network technologies play a fundamental role in the development of modern information infrastructure, as they form the basis for the formation of a global information space that determines the pace of scientific and technological progress, the level of economic competitiveness, and the security of society. Information infrastructure in the 21st century is a key factor in socio-economic development, encompassing telecommunications networks, data centers, software, cloud services, and cyber security tools, with network technologies determining its quality, stability, and scalability. In a world where data volumes are growing exponentially, promising network solutions are becoming the main tool for ensuring the speed of information transfer, processing efficiency, and the availability of digital resources.

One of the most important areas is the development of 5G and future 6G technologies, which promise to radically change the concept of speed and quality of communication. These standards usher in a new era of ultra-fast internet, minimal data transmission delays, mass connection of Internet of Things devices, and the

creation of conditions for the full functioning of smart cities, autonomous transport, and augmented reality.

The promise of these network technologies lies not only in increasing channel bandwidth, but also in creating a new infrastructure focused on virtualization, distributed data processing, and more efficient resource management [1, p.19]. With the advent of 6G, even more ambitious possibilities are envisaged: the integration of artificial intelligence directly into the network, data transfer at terabit per second speeds, and deep interaction between the physical and digital worlds.

An equally important trend is cloud technologies and the development of edge computing, which not only allow for the storage and processing of huge amounts of information, but also enable this to be done as close to the user as possible, reducing delays and improving service quality. The combination of cloud platforms and edge computing creates a flexible infrastructure that can scale according to the needs of business and society. This is especially important in a world where the number of “smart” devices is constantly growing, and response speed requirements are becoming critical – from medical applications to industrial automation.

Another promising area is the development of cybersecurity-oriented networks. With cyber threats constantly on the rise, security is becoming a fundamental requirement for any information infrastructure, rather than an optional extra. Blockchain technologies, distributed ledgers, cryptographic protocols, and intelligent monitoring systems can create an environment in which data exchange is maximally protected from manipulation, leaks, and unauthorized access. This is particularly relevant for international business, public administration, and critical sectors of the economy.

Artificial intelligence and machine learning are also being integrated into network technologies, enabling automated infrastructure management, peak load forecasting, channel utilization optimization, and increased resilience to failures. Such approaches enable the creation of “self-organizing” networks that not only respond to changes in the environment but are also capable of anticipating them and preparing the system for potential challenges [2].

It is also worth mentioning the development of quantum communications, which in the coming decades could radically change our understanding of security and the speed of information transfer. The use of quantum physics principles allows the creation of communication channels that are theoretically impossible to intercept or hack, which will be a breakthrough in data protection. New-generation optical networks are being actively researched, which can provide almost unlimited bandwidth and become the basis for the further digital transformation of society.

Thus, promising network technologies not only form the technical foundation of the information infrastructure but also determine the strategic directions of development of the economy, science, education, and security. They are becoming the “circulatory system” of the global world, ensuring its viability, efficiency, and innovation.

In the future, the role of these technologies will only grow, as information becomes a key resource and the ability to transmit it quickly, securely, and efficiently becomes a guarantee of development for both individual states and the entire global

community. Promising network solutions are not only a matter of technical progress, but also a guarantee of stability, sovereignty, and competitiveness in a world that is increasingly dependent on digital processes.

References:

1. Andrushchak V.S. Modeli upravlinnia potokamy infokomunikatsiinykh merezh z vykorystanniam metodiv shtuchnoho intelektu i mashynnoho navchannia. Kvalifikatsiina naukova pratsia na pravakh rukopysu. Lviv, 2021. 189 s. (In Ukrainian).

2. Arkhitektura merezhevoi platformy monitorynhu obektiv u kiberfizychnykh systemakh «rozumnykh mist» – Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. Nomer: №4, 2023 (323).pdf. (In Ukrainian). URL: [https://doi.org/10.31891/2307-5732-2023-323-4-123-130./](https://doi.org/10.31891/2307-5732-2023-323-4-123-130/)

UDC 621.317

Skorin Yuriy

PhD, Associate Professor

Simon Kuznets Kharkiv National University of Economics

APPLYING ARTIFICIAL INTELLIGENCE TECHNIQUES TO CREATE TYPICAL WEB APPLICATIONS

Every day, thousands of new web applications are created by developers from all over the world: large and single-page, useful and meaningless, commercial and for their own use. However, no matter how different and original they are, the process of their development is not much different from each other and consists of the same stages, for example: interface design, monotonous writing of components, different types of testing, etc.

Each task of the stage separately may require a small amount of resources to complete, but in the aggregate and in a large-scale project, the required amount of human and, accordingly, material resources increases dramatically, which becomes a problem for managers and customers.

Optimization of resource costs in the modern world is a necessity for any enterprise to stay afloat in a competitive environment. For the development of web and regular applications, there are methodologies for optimizing this process, however, in my opinion, they use outdated tools and are too dependent on the human factor, which significantly affects their efficiency, reducing the already small amount of saved resources.

Now you will not surprise anyone with a voice assistant-assistant or a search on the Internet by photo, modern artificial intelligence systems already know how to draw pictures and can fully replace a person in correspondence and conversation. All this is made possible thanks to modern artificial intelligence and machine learning tools, the limit of development of which has not yet been found.

The use of such tools can help us solve the problem of optimizing the web application development process, but in order to improve the results compared to existing methodologies, these tools need to be integrated at every stage of development, from design to testing.

This can be done using tools such as NLP and GPT, they use artificial intelligence and machine learning methods to analyze text and speech, in order to synthesize new text, including program code.

There is no one-size-fits-all method that allows you to design and develop any web application from scratch on your own. Therefore, to achieve the goal of the work, we will need to use a set of state-of-the-art methods and tools, such as computer vision, natural language processing and a generative transformer based on it in the form of state-of-the-art artificial intelligence systems.

With the help of computer vision, it will be possible to create full-fledged layouts of interfaces, pages, and forms of the future application from hand-drawn diagrams or in primitive graphic editors.

Also, using computer vision, it will be possible to improve the interface and its usability by comparing the layout of our application with reference options. Natural language processing tools will allow us to transform our wishes regarding the appearance and functionality of interface components into a form that is understandable for the artificial intelligence system.

The generative transformer, in turn, will receive our transformed wishes and, using its intellectual capabilities and knowledge gained in the learning process, will synthesize the source code for the components of our applications. The advantages of the selected means are obvious: no other systems can currently replace the selected ones. Their functionality and capabilities are unique, and taken together, they are ideal for solving the research problem.

For a more in-depth acquaintance with the subject area, the process of developing typical web applications was analyzed and the key stages were identified. The structure of typical web applications was considered in great detail. Understanding this process will allow you to more effectively use artificial intelligence tools during development.

In addition, the ability of artificial intelligence, namely computer vision, to create interfaces based on hand-drawn wireframes with a fairly high level of accuracy was demonstrated.

To synthesize the program code of the web application itself and its components, neurolinguistic programming methods and an autoregressive model of the GPT language of the third version were chosen.

The use of these state-of-the-art artificial intelligence tools made it possible to achieve impressive results: to create working web applications without writing a single line of program code, only using human language.

As a result of the study, the module "Using artificial intelligence tools to create typical web applications" was implemented. First of all, the relevance and necessity of using artificial intelligence methods in the development of software in general and typical web applications in particular were considered and evaluated.

And, although the process of software design and development is already sufficiently studied and improved, space has been found for its further optimization. However, this can only be done using the most modern tools of artificial intelligence and machine learning.

During the practical use of the tools, the feasibility and effectiveness of the selected artificial intelligence methods were finally confirmed. They provide a high level of reliability and performance, convenience and flexibility of settings, the ability to edit the appearance of the user interface.

The end result is that typical web applications and their components, created using only human natural language, are a good example of demonstrating the capabilities of artificial intelligence tools.

The technologies in question have a future not only in the form of separate full-fledged systems, but also as an addition to existing software products used for software development, such as graphic editors for creating user interfaces and code editors. This work will contribute to drawing attention to existing artificial intelligence tools and creating new ones in the future.

References

1. The concept of the development of artificial intelligence in Ukraine. [Electronic resource] – Mode of access to the resource: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text>
2. Methodological recommendations for the preparation of reports, course projects and diploma works (projects) for students of the specialty 121 "Software Engineering", 122 "Computer Science", 126 "Information Systems and Technologies": [Electronic edition] / compiled by I.O. Ushakova, G.O. Plekhanova, O.M. Besedovsky. – Kh.: KhNEU named after S. Kuznets, 2021. – 48 p.
3. 4. Modern approaches to solving computer vision problems / R.M. Tymchyshyn, O.E. Volkov, O.Y. Gospodarchuk, Yu.P. Bohachuk. – 2018 – 73 p.
4. Modern Technologies of Neurolinguistic Programming / Oleksiy Chernenko, Serhiy Hnatiuk, Valentyn Petryk, Viktor Gureev, Viktor Kurganovich. – 2020 – 200 p.
5. Computer vision technology: typical errors during development and implementation. [Electronic resource] – Mode of access to the resource: <https://brainberry.ua/uk/newsroom/blog/computer-vision-technology-common-mistakes>
6. Artificial intelligence, machine learning and neural networks: what is the difference and what they are used for. [Electronic resource] – Mode of access to the resource: <https://evergreens.com.ua/ua/articles/machine-learning-overview.html>
7. A Complete Guide to Wireframe Design. [Electronic resource] – Mode of access to the resource: <https://userguiding.com/blog/wireframe-design/>
8. All You Need to Know About Computer Vision. [Электронный ресурс] – Режим доступа до ресурсу: <https://www.turing.com/kb/all-you-need-to-know-about-computer-vision>
9. Alpaydin Ethem. Introduction to machine learning / Ethem Alpaydin. - 2nd ed. 578 p.

10. Artificial Intelligence Explained - what it is and what it does.
[Електронний ресурс] – Режим доступу до ресурсу:
<https://www.nanowerk.com/smart/artificial-intelligence-explained.php>

UDC 621.317

Skorin Yuriy

PhD, Associate Professor

Simon Kuznets Kharkiv National University of Economics

APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS FOR ENTERPRISE OPERATIONAL RISK MANAGEMENT

The activity of manufacturing enterprises in Ukraine in modern conditions is characterized by a high level of uncertainty, the influence of a large number of external and internal factors, as well as the degree of risk that grows. In such circumstances, enterprises need to understand approaches and methods for assessing the impact of potential risks on their activities and be able to manage them in order to mitigate them.

The management of the enterprise needs to learn how to timely assess and take into account risk factors when making important management decisions, effective organization of the process of assessment and risk reduction will help to quickly adapt the activities of enterprises to unstable and rapidly changing conditions of the external and internal environment. The use of the latest technologies, such as artificial intelligence, will increase the level of risk management, reduce the error rate, and increase the efficiency of the enterprise. One of the main trends in the work of enterprises is the transition to "smart" production. Smart manufacturing aims to transform the data obtained over the entire life cycle of a product into production analysis in order to have a positive impact on all aspects of production.

All of the above necessitates the study of operational risks in the activities of the enterprise, increases the need to adapt existing methods of risk assessment to the conditions of their practical application at enterprises and the use of artificial intelligence for risk management and optimization.

The object of the study is the process of managing operational risks using artificial intelligence. The subject of the study is the theoretical foundations, methods and practical aspects of the application of artificial intelligence for the management of operational risks in the enterprise. The purpose of the study is to analyze the methods of artificial data intelligence for the management of operational risks of enterprises and to determine methods for optimizing the management of operational risks of the enterprise.

To achieve the goals of the study, the following tasks were performed: analysis of scientific sources on the types and determination of operational risks of the enterprise, management of operational risks of the enterprise; collection and processing of statistical, economic and technical information necessary for

optimization of the enterprise; analysis and assessment of operational risks of the enterprise; determining the possibility of using artificial data intelligence methods for the management of operational risks of the enterprise; selection of the most effective methods of artificial data intelligence for the management of operational risks of the enterprise, which will increase the efficiency of the studied enterprise.

Operational risk management is a complex task that uses different approaches to solve. Operational risk summarizes the uncertainty and dangers faced by a company when it tries to carry out its day-to-day business activities in a certain industry. Operational risks can arise as a result of violations of internal procedures caused by people and systems. Such problems are in contrast to problems caused by external forces, such as political or economic events, or systematic risks inherent in the entire market or market segment [1].

In the process of research, the activities of the enterprise were analyzed, statistical data on the activities of the enterprise and its competitors were analyzed, the website of the enterprise and its competitors, existing domestic regulatory documents and standards were analyzed.

In the process of research, a systematic approach was implemented and general scientific methods were used: analysis, synthesis, induction, deduction, logical analysis (to generalize the views of domestic and foreign scientists on the main categories of artificial intelligence, operational risks of the enterprise); the method of comparison and research of categories is used.

Like other risk management tools, the use of artificial intelligence must be constantly evaluated and adjusted. It is extremely important to take into account the changing needs of the enterprise and the possible drawbacks of this technology.

For manufacturing enterprises, in the context of a significant increase in competition, it is important to optimize operational risks, because this will increase their competitiveness in the market and increase consumer loyalty. The use of artificial intelligence and in particular machine vision and deep learning methods will reduce the involvement of the human factor, thus not only reducing wage costs, but also the percentage of defective products. The calculations carried out confirm the latest research in the field of artificial intelligence that the future belongs to "smart" enterprises. Reducing operational risks through the implementation of machine learning systems at the studied enterprise is possible and will pay off in the near future. Thus, the use of artificial data intelligence methods for operational risk management is appropriate at domestic enterprises.

References

1. DSTU ISO 31000:2018. Risk Management. Principles and Guidelines; Introduction. 2019-01-01. – Kyiv: SE "UkrNDNC", 2019. - 32 p.
2. Vitlinskyi V. V. Riskology in Economics and Entrepreneurship: Monogr. / V. V. Vitlinskyi, G. I. Velikoivanenko. – Kyiv: KNEU, 2004. – 480 p.
3. Vitlinsky V.V. Artificial intelligence in the system of managerial decision-making. Neuro-fuzzy modeling technologies in economics. 2012. № 1. P. 97–118.

4. Implementation of the HACCP system for food market operators: a practical guide / edited by A. S. Tkachenko. – Poltava: PUET, 2020. – 137 p.

UDC 621.317

Skorin Yuriy

PhD, Associate Professor

Simon Kuznets Kharkiv National University of Economics

FORECASTING THE ECONOMIC ACTIVITY OF A TRADING ENTERPRISE USING WEB TECHNOLOGIES

Under the conditions of the global economic crisis, the dependence of enterprises on inflationary processes, the reliability of counterparties, and complex organizational and legal conditions of functioning is growing.

This leads to special attention to the assessment of the financial condition of the enterprise as a dominant lever for identifying the weak and strong positions of the enterprise, its financial reserves.

Assessment of the financial condition should be reasoned and objective, since errors in conclusions lead to losses or underachievement of the desired level of profit.

Taking into account the variety of financial processes, the multitude of indicators that characterize the financial condition of the enterprise, the difference in the level of their marginal estimates, it is necessary to apply appropriate economic and mathematical methods and models.

They allow you to solve the problem of assessing the financial condition of the enterprise with minimal time and money costs.

At the same time, since the tasks of financial analysis require taking into account and processing powerful arrays of statistical and expert information, it is advisable to develop software tools that automate the process of determining the financial condition of the enterprise and reduce the likelihood of erroneous assessments.

Thanks to the works of domestic and foreign scientists, a large number of mathematical models have been built to solve problems of financial analysis.

However, the existing approaches do not allow to fully take into account the constantly changing composition and dimensionality of the set of evaluative parameters of the financial condition of the enterprise under the conditions of variability of internal and external environments, the specifics of the functioning of the enterprise in a particular industry under the influence of crisis phenomena.

This determines the relevance of the development of mathematical models and methods for assessing the financial condition of the enterprise and the corresponding software tools that automate them.

Purpose: is to conduct a review of the existing theoretical support for analysis and forecasting, and as a result, to conduct a complete analysis of the state and activities of an agricultural enterprise.

Object of research: development of a specialized software product for analyzing sales volumes of an agricultural enterprise.

Subject of research: the paper presents an overview of several methods for forecasting time series.

The results of forecasting the selected indicators using the autoregressive model, as well as such methods as MGVA, fuzzy MGWA are obtained.

The novelty of the conducted research lies in the fact that a comprehensive study of all aspects of financial activity allows to increase the efficiency of management of economic entities and reduce the negative impact of external and internal factors.

Methods: MGVA – method of group consideration of arguments; NMHWA is a fuzzy method of group consideration of arguments.

Expected result: analysis of the state and activities of the enterprise using a web application.

In the process of performing the study, a review of the existing theoretical support for analysis and forecasting was carried out, and on the basis of the results obtained, a complete analysis of the state and activities of the enterprise was carried out.

However, so far all these methods have not been sufficiently studied, they are based on a rather complex theoretical basis, and their conclusions cannot always be successfully applied in practice.

In this case, there is no clear standard for the use of this method, but in which it is necessary to look for new approaches.

Therefore, now there is a tendency to use not the "best" method in describing and predicting time series, but a set of methods and further comparison of results.

And the more diverse methods according to the principle of forecasting the complex has, the greater will be the probability that the natural pattern according to which the series is built will be determined.

The obtained forecast values should be used for operational planning and management of the enterprise.

One of the types of analysis was also considered - financial, which helps in the management of the enterprise.

The success of the analysis is determined by various factors. With a certain degree of conventionality, five basic principles can be recommended that it is advisable to keep in mind when carrying out the analysis.

A factor analysis is made, i.e. an assessment of the financial condition of the enterprise by calculating financial and economic indicators: indicators of profitability, liquidity, business activity, property status, financial security and others.

It has been established that the best model among those built is a fifth-order autoregressive model with the addition of purchasing factors and margins.

Several indicators were used to assess the quality of forecasts, which helps to increase the probability of choosing the best forecast. In particular, the Theil coefficient shows which models are in principle suitable for forecasting.

A software product was written that can be used at the enterprise.

The product is written in JavaScript (in the WebStorm environment) using the open React library to create user interfaces, and using: Redux, Redux-saga, Redux-Form, React Router.

The results of forecasting the selected indicators using an autoregressive model were analyzed.

References

1. Methodology for conducting an in-depth analysis of the financial and economic status of insolvent enterprises and organizations: By the Order of the Agency for Bankruptcy Prevention of June 27, 2014 // State Information Bulletin on Privatization. – 2014. - No. 12, - p. 10 – 32.
2. Verbitskaya L.V. Organization of Accounting at Enterprises of Small Business in Ukraine: Textbook. / L.V. Verbitskaya // – Kyiv: MAUP, 2012. – 116 p. – Bibliogr.: p. 110 – 112.
3. Izmailova K.V. Financial Analysis: Teaching Aid. – 2nd ed., stereotype. / K.V. Izmailova // – Kyiv: IAPM, 2011. – 152 p.: ill. – Refs.: P. 142-144.
4. Podderiyogin A.M. Finance of the enterprise / prof. A.M. Podderiyogin // : textbook / Head of the author's col. and scientific ed., 3rd ed., reworked and supplemented – Kyiv: KNEU, 2016. – 460 p.
5. Savytska G.V. Economic analysis of the activity of the project / G.V. Savytska: Scientific guide. – Kyiv: Znannya, 2015. – 654 p.
6. Korobov M.Y. Financial and Economic Analysis of the Activities of Enterprises / M.Y. Korobov // : nauch. Posob. – Kyiv: Znannya Publishing House, KOO, 2014. – 378 p.
7. Regulations (standard) of accounting 2. "Balance" ZATV. Order of the Ministry of Finance of Ukraine dated March 31, 2017. No. 87 // Galician contracts. – 1999. – №32.
8. Nikhbat E. Finance Translated from English by V.F. Ovsienko and V.Y. Musienko. / E. Nikhbat, A. Gropelli // – K.: Osnovy, 2013.
9. Kaziev V. I. Information and system [Elektronnyi resurs]. – Rezhim dostupa : <http://dit.isuct.ru/IVT/BOOKS/IS/IS5/glava3.html> .
10. Kucherenko T. Procedure for Recalculation and Accounting of VAT on Operations on the Realization of Products and Services of Agricultural Enterprises / T. Kucherenko, O. Shaiko // Accounting in Agriculture. – 2012. – No3. – P.34–39.
11. Ogerchuk Y.V. Organization of Sales Activities of Enterprises / Yu.V. Ogerchuk // : author's dissertation on obtaining the degree of Candidate of Economics: special. 08.06.01; National University "Lviv Polytechnic". – Lviv, 2014. – 20 [1] p.

INTRODUCTION OF FORECASTING METHODS DURING THE EXECUTION OF LONG-TERM TRADE OPERATIONS OF THE ENTERPRISE

Since the global recession, interest in new tools for forecasting trade operations, especially based on information regarding global world events, monetary and financial information, continues to grow. With the development of computing tools to store and expand large-scale datasets, analysts are focused on discovering a new, timely and reliable way to retrieve information by linear and non-linear methods to improve predictability in real time and for long-term trading operations.

Data on global events in the world and information on payment instruments used in society (check, credit transfer, payment card transaction) can be a unique source of information for long-term forecasts of the economic activity of the enterprise, since they are easily traced and form a picture of the state of events today, and their impact on the future.

This connection was evident at the beginning of the last century, when Irving Fisher described the basic equations of the quantitative theory of influence in the following words: "Primary equations mean that global situations have an impact on cash flows, and money, in turn, is used in any operation. Money is equal to the commodity purchased at the sale price."

In addition, the importance of forecasting trade operations using linear and nonlinear methods can hardly be overestimated for understanding monetary economics in general.

The purpose of linear analysis is to determine the direction of price movement, as well as the best prices and times for concluding transactions. Having answers to these questions, the enterprise analyst will advise you to pay attention to favorable conditions for buying or selling. In short, linear analysis is based on the following assumptions: the market knows everything (the action of all factors, economic, political and psychological, has already been taken into account by the market and included in the price), the market obeys trends, the market has patterns or history repeats itself. These assumptions do have many drawbacks, but they can and are widely used in technical analysis.

The development of nonlinear analysis as a direction in the last decade has led to the creation of many methods, procedures, variants of forecasting, unequal in their purpose. According to the estimates of domestic and foreign specialists, there are already more than a hundred nonlinear forecasting methods, in this regard, specialists need to solve the problem of choosing methods that would give adequate forecasts for the processes or system under study [3].

But despite a significant number of studies, there are a number of topical problems in the field of linear and nonlinear forecasting that have not been fully

solved: the problem of finding the disorder of a non-stationary process with a changing market trend, consideration of the process with multiple disorder from the standpoint of assessing the functions of the risk of disorder on the time interval in the future, the problem of formalizing the choice of take-profit values (asset price level, at which the concluded trade is closed with a profit) and stop-loss (the price level of the asset at which the concluded trade is closed at a loss in order to prevent further losses) for trade transactions.

In addition, the study of available methods of analysis showed that today there are not enough information automated tools that are designed to solve the problem of complex data analysis of dynamic processes and probabilistic assessment of the state of such processes.

The study presents the results of a recently proposed trend prediction method that determines the consequences of unknown exogenous variables studied when used together and compared to exponential smoothing.

The concept of experimental and statistical data on financial and economic processes was introduced, which are described by time series and require effective analytical processing in order to identify practically useful knowledge and relationships between them necessary for market decision-making.

The processes of trading in the market were studied.

Acquaintance with the methods of regression analysis, as well as information and analytical systems, gave rise to forecasting and modeling market behavior. It is revealed that decision support systems based on the method of group consideration of arguments and methods of forecasting economic data presented in the form of time series are effective.

The empirical results support the original hypothesis, which suggests that combining the newly proposed method with exponential smoothing would be more successful than using exponential smoothing alone to predict the extrapolation of an up/down trend.

A more useful confidence interval is indicated when the new method is used separately without a reliability threshold A . Confidence intervals suggest that the approach presented in this paper may be an additional tool for more efficient profit growth and more accurate forecasting of geopolitical events. The possible relationship between Google's search interest and the reliability of the recently proposed method will be further explored on a wide spectrum.

In addition, researching the integration of the proposed method into machine learning models will also be a future task.

The results of the method study can be used to predict benefit estimates that are important for trade policy. Despite the significant amount of research literature and existing forecasting methods in trade policy analysis, this method remains a subject of controversy. There is also a discrepancy between the transfer practices recommended by the scientific literature and those that are usually applied within the framework of trade policy analysis. The size, complexity, and relative disorganization of the literature can be an obstacle to the use of the latest methods.

Recognizing the importance of information transfer for trade policy development, this paper examines the concept of benefit transfer. It highlights

methods, trends, and controversies in contemporary research, identifies the challenges facing benefit transfer practices, and summarizes contributions to research. Thanks to this, several areas of future forecasting research in the market appear.

References

1. Bagnall, J. Consumer Availability of Money. Comparison with Payment Diaries Study/ J. Bagnall// Journal of the Central Bank. – 2020. – 61 p.
2. Bai J. Identification of the Number of Factors in Approximate Factor Models / J. Bai // Journal of Business and Economic Statistics. – 2018. – 52 p.
3. Belukha M.T. Fundamentals of Scientific Research: Textbook. – Kyiv: Vyshcha Shkola, 2017. – 271 p.
4. DSTU 8302:2015. Information and documentation. Bibliographic reference. General provisions and rules of compilation / Nats. Standard of Ukraine. – Kyiv: SE "UkrNDNC", 2016. – 18 p.
5. Imitation modeling/ Vitaliy Sytnyk. — Kyiv: KNEU, 2019 – 120 p.

UDC 621.317

Skorin Yuriy

PhD, Associate Professor

Simon Kuznets Kharkiv National University of Economics

METHOD OF RATING ASSESSMENTS OF TOOLS FOR CREATING WEB APPLICATIONS

The relevance of the study is due to the high demand for the use of web applications. The choice of effective technologies and tools greatly simplifies the process of creating a web application for both the contractor and the customer. After all, the choice of technologies and means of creating web applications depends on the development time and quality of the final product, its performance. In modern conditions, the tools and technologies for creating web applications are constantly updated, new ones appear, some become outdated, for high-quality work you need to have up-to-date information.

The purpose of the study is to facilitate the choice of effective technologies and tools for creating web applications. To do this, you need to complete the following tasks: familiarization with the literature; research of technologies and tools for creating web applications; comparison of technologies and tools for creating web applications; review of the method of rating assessments, development of evaluation criteria; experimental study of the method of rating assessments.

The object of research is technologies and tools for creating web applications. The subject of the study is the method of rating assessments for creating web applications.

The scientific novelty lies in the improvement of the method of rating assessments, which allows you to save development time and improve the quality of the software product by creating relevant evaluation criteria.

The methods of scientific research are the method of rating evaluations, the method of selection and the method of comparison.

Practical value of the study – the results of improving the method of rating assessments can be used by IT companies to save resources and create high-quality software products. The prospect of the study is to improve the choice of effective technologies and tools for creating web applications by introducing new selection methods.

The widespread use of web applications and the abundance of technologies and tools for creating web applications causes the problem of selecting technologies and tools for creating a particular web application. After all, the success of the web application, its security, interactivity, operability, and stability depend on the technologies and tools used.

The method of rating assessments begins with the selection of criteria for choosing technologies and tools for creating a web application, then their importance is determined. Importance is usually established through peer review. The final value of the rating is determined by summing up the products of the importance (weight) of the criterion for its expert assessment for each technology or tool for creating a web application. By calculating the rating of various technologies and tools for creating web applications and comparing the values obtained, the best technology or tool is determined. If the rating assessment of two or more technologies and tools for creating web applications according to the main criteria is the same, then the procedure is repeated using additional evaluation criteria.

The rating evaluation method used in the analysis of technologies and tools for creating web applications is a numerical or ordinal indicator of performance or popularity and shows the importance or impact of a particular object or condition.

The indicator of evaluating effectiveness and popularity at a certain point in time, which is determined by an expert opinion or sociological survey, is determined by the place it occupies among its peers. Therefore, the method of rating assessments is a system of rules and approaches to studying the effectiveness, in our case – technologies and tools for creating web applications using performance indicators by determining the place of each technology or tool in the overall process of creating a web application.

It is also effective to use monitoring, which involves several measurements of the object under study and subsequent analysis, evaluation, comparison of the results obtained to determine patterns, trends, variables and their dynamics. Therefore, the rating evaluation method is a means of monitoring technologies and tools for creating web applications, and it, like any method, is based on principles.

Scientific principles are requirements for the construction of a theory, formed as primary, underlying a certain set of facts. When characterizing different systems, the principles show those essential characteristics that are responsible for the correct functioning of the system, without which it would not fulfill its purpose.

The principles of the rating method are: consistency; logic; systematic; rationality; availability.

The method of rating assessments should take into account all the most important criteria of financial, technical and performance characteristics of technologies and tools for creating web applications.

In the process of ranking, data on the popularity of technologies and tools, the frequency of their use, the effectiveness of software products created with their help, and other indicators are used.

Improving the method of rating assessments for the selection of technologies and tools for creating web applications consists in evaluating not only technologies and tools, but also in assessing the importance of evaluation criteria. Initially, each evaluation criterion is considered from several angles, its importance for each individual project is established.

For example, one company cares about the popularity of certain technologies and tools for creating web applications, and another company is more interested in the cost of using technologies and tools for creating web applications. In this way, we will be able to more accurately select the most effective technology or tool for creating a web application for each project, developer, and company.

In the process of conducting the study, the scope of use of web applications was analyzed, the current state of tools for creating web applications was characterized, and methods for choosing effective tool technologies for creating a web application were considered. The need to improve the method of choosing technologies and tools for creating web applications was identified. The process of creating web applications is considered in detail, popular technologies and tools used in the creation of web applications are examined, and the further development of these tools is analyzed. The method of rating assessments was theoretically and methodically studied, namely, all stages of the method were examined, its advantages and disadvantages were determined, and the criteria for evaluating tools for creating web applications were considered. The methods of calculating the rating score and possible options for improving the method are considered. An experimental study of the improved method of rating assessments was also conducted. With the help of Google Forms, a survey was conducted on the evaluation of tools for building web applications and their evaluation criteria. The results of the survey were analyzed and calculated using Microsoft Excel and the adequacy of the experiment was proven.

The results of improving the rating evaluation method can be used by developers or IT specialists, IT companies to select effective tools for creating web applications. The prospect of the study is to improve the method of rating assessments by developing criteria for evaluating tools for creating web applications, this will allow choosing technologies and tools according to the necessary criteria.

References

1. Engineering of systems and software. Development and management of WEB-sites for systems, software and information services (ISO/IEC/IEEE 23026:2015, IDT): DSTU ISO/IEC/IEEE 23026:2016 – [Effective from 2018-01-01]. – Kyiv: Ministry of Economic Development of Ukraine, 2017. – 49 p.

2. Andrushkiv I. P. Digitalization in the banking sector: world and domestic experience / I. P. Andrushkiv, L. M. Nadiyevets // Problems of economy. - 2018. - № 4. - P. 195-200. - Access mode: http://nbuv.gov.ua/UJRN/Pekon_2018_4_24 .

3. Banit B. B. Selection of the information system of content management for the construction of a corporate site / B. B. Banit, S. R. Krasilnikov // Bulletin of the Khmelnytskyi National University. Technical Sciences. - 2018. - № 1. - P. 28-32. - Access mode: http://nbuv.gov.ua/UJRN/Vchnu_tekh_2018_1_7 .

4. Berkovsky V. V. Analysis of methods for creating interactive Web-applications / V. V. Berkovsky, S. O. Radionov // Systems of armament and military equipment. - 2015. - № 2. - P. 61-64. - Access mode: http://nbuv.gov.ua/UJRN/soivt_2015_2_17 .

5. Vakulchuk R. O. Analysis of the performance of Apache and Nginx web servers at peak loads / R. O. Vakulchuk, K. V. Melnyk, V. M. Melnyk // Computer-integrated technologies: education, science, production. - 2013. - № 12. - P. 8-12. - Access mode: http://nbuv.gov.ua/UJRN/Kitonv_2013_12_4 .

6. Viter M. B. Technology of integration of electronic information resources of state bodies on the basis of web-services / M. B. Viter // Scientific and technical information. - 2015. - № 3. - P. 47-50. - Access mode: http://nbuv.gov.ua/UJRN/NTI_2015_3_9 .

UDC 004.89

Suprun Anna

Master in informatics,

Kharkiv National University of Radio Electronics

Research supervisor

Tvoroshenko Iryna

Ph.D., Associate Professor, Department of Informatics

Kharkiv National University of Radio Electronics

A COMBINED METHOD FOR LEVERAGING LARGE LANGUAGE MODELS IN THE ANALYSIS AND GENERATION OF CREATIVE TEXTS

The rapid development of large language models (LLMs) has opened new opportunities for creative industries, particularly in the field of literary text generation and analysis. Yet, despite their impressive ability to generate coherent text and mimic literary styles, LLMs still face notable challenges. They often produce superficial or formulaic narratives, often lack emotional depth and originality, and struggle to maintain consistency over long passages, leading to contradictions or fragmented storylines. To overcome these limitations, a combined method for leveraging LLMs is introduced. The method integrates the most effective LLMs for analysis and generation into a single workflow, ensuring higher overall quality, consistency, and adaptability of results.

At the core of the method lies the experimental selection of two distinct models: an LLM-Analyst (responsible for semantic and logical interpretation and structuring of input data) and an LLM-Generator (responsible for producing coherent literary text). These models are chosen based on their empirical strengths – some LLMs demonstrate higher performance in analysis, while others excel in creative generation.

The proposed method is structured into several sequential stages, each addressing a specific aspect of literary text analysis and generation:

Stage 1. Input Data Formalization. This stage involves structuring and formalizing the input information provided by the user. The inputs include unstructured descriptions of characters, locations, world rules, and prior events in the story, which together define the narrative context. In addition, the user provides a prompt specifying the intended scene, stylistic preferences, mandatory and prohibited elements and events, illustrative examples, and generation parameters such as maximum length or tone. The purpose of this stage is to decompose these inputs into structured components that can be systematically interpreted by the LLM-Analyst [1].

Stage 2. Analytical Representation. At this stage, the LLM-Analyst performs a detailed semantic and logical analysis of the structured character descriptions and narrative context prepared in Stage 1. This structured interpretation provides a comprehensive profile for every character, enabling the system to reason about their behavior and interactions within the narrative. Based on these profiles, the LLM-Analyst generates a set of permissible actions for each character.

Stage 3. Text Generation. In this stage, the LLM-Generator receives the structured prompt produced by the LLM-Analyst and produces the literary text of the scene. The generator takes into account the comprehensive scene model, including character profiles, permissible actions, world context, previous events, and stylistic or tonal instructions from the user prompt. During generation, the model aims to maintain logical consistency in the plot and character behavior, adhere to the desired style and tone, ensure that mandatory actions are performed, and avoid any forbidden actions.

Stage 4. Quality Evaluation. The final stage of the method focuses on assessing the quality and consistency of the generated text. The output is evaluated against a comprehensive set of criteria, including adherence to mandatory actions and prohibitions specified in the prompt, logical consistency of the plot, coherence of character behavior, and conformity with the desired style and tone. If any discrepancies are identified – for instance, missing mandatory actions, violations of narrative logic, or stylistic inconsistencies – the text is iteratively refined. The iterative validation and regeneration process guarantees a high-quality, contextually appropriate, and stylistically consistent result [2].

Figure 1 provides a visual overview of the proposed combined method for leveraging large language models in literary text analysis and generation.

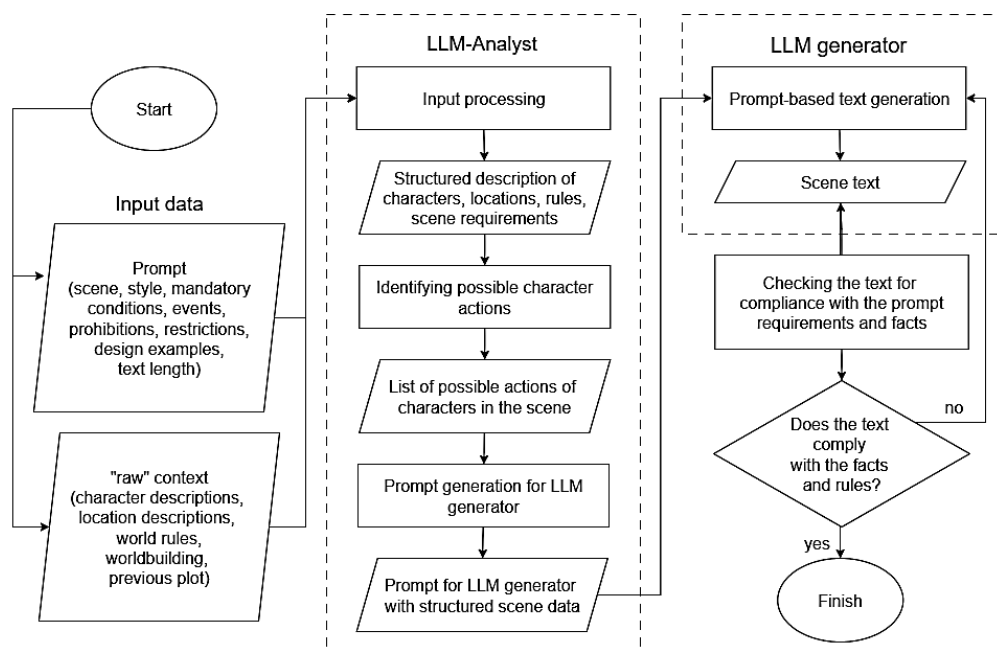


Figure 1 – Diagram of the combined method for leveraging large language models in the analysis and generation of creative texts.

The proposed combined method leverages the complementary strengths of multiple LLMs to produce coherent, stylistically consistent, and logically sound literary texts. By integrating structured analysis, generation, and iterative quality evaluation, it ensures narrative consistency, character fidelity, and adherence to user-defined constraints, offering an effective tool for creative text generation and literary analysis.

Further research plans to integrate the steps described above into computer vision tasks [3-11].

References:

1. Gorokhovatskyi V., Tvoroshenko I., Yakovleva O., Hudáková M., and Gorokhovatskyi O. (2024) Application a committee of Kohonen neural networks to training of image classifier based on description of descriptors set, *IEEE Access*, vol. 12, pp. 73376-73385.
2. Gorokhovatskyi V., Tvoroshenko I., Yakovleva O. (2024) Transforming image descriptions as a set of descriptors to construct classification features, *Indonesian Journal of Electrical Engineering and Computer Science*, 33 (1), 113-125.
3. Yakovleva O., Matúšová S., Tvoroshenko I., and Isaiev Y. (2024) Visitor counting based on video stream analysis from surveillance cameras to solve various business problems, *Verejná správa a regionálny rozvoj ekonómia, manažment a marketing*, XX(1), pp. 67-87.
4. Гороховатський В., Передрій О., Творошенко І., Марков Т. (2023) Матриця відстаней для множини компонентів структурного опису як інструмент для створення класифікатора зображень, *Сучасні інформаційні системи*, 7, С. 5-13.

5. Pomazan, V., Tvoroshenko, I., and Gorokhovatskyi, V. (2023). Development of an application for recognizing emotions using convolutional neural networks, *International Journal of Academic Information Systems Research*, 7(7), pp. 25-36.
6. Gorokhovatskyi V., Chmutov Y., Tvoroshenko I., and Kobylin O. (2025) Reducing computational costs by compressing the structural description in image classification methods, *Advanced Information Systems*, vol. 9, no. 1, pp. 5-12.
7. Gorokhovatskyi V., Tvoroshenko I., Yakovleva O., and Hudáková M. (2025) Image description compression in classification structural methods, *IEEE Access*, vol. 13, pp. 43631-43641.
8. Gorokhovatskyi V., and Tvoroshenko I. (2024) An effective method for transforming an image description into a compact vector for classification. *Information Technology and Implementation (Satellite): Conference Proceedings, November 21, 2024*, Kyiv, Ukraine, Publishing House «Caravela», pp. 25-28.
9. Tvoroshenko I., Gorokhovatskyi V., Kobylin O., and Tvoroshenko A. (2023) Application of deep learning methods for recognizing and classifying culinary dishes in images, *International Journal of Academic and Applied Research*, 7(9), pp. 57-70.
10. Gorokhovatskyi V., Tvoroshenko I. (2023) Identification of visual objects by the search request. *Int. scientific symp. «Intelligent Solutions-S». Computational intelligence. Decision making theory: proceedings of the international symposium, September 28, 2023*, Kyiv-Uzhhorod, Ukraine, 25-27.
11. Daradkeh Y.I., Gorokhovatskyi V., Tvoroshenko I., and Zeghid M. (2024) Improving the effectiveness of image classification structural methods by compressing the description according to the information content criterion, *Computers, Materials & Continua*, vol. 80, no. 2, pp. 3085-3106.

UDC 004.67

Temnikov G.E.

senior teacher,

Dmytro Motornyi

Tavria State Agrotechnological University (Zaporizhzhia)

DESIGNING APPLICATIONS FOR PROCESSING AND ANALYZING LARGE AMOUNTS OF DATA (BIG DATA) IN DISTRIBUTED SYSTEMS

Introduction. In today's digital economy and information society, processing and analysis of large amounts of data, known as Big Data, is becoming a critically important component of any organization that seeks to effectively use information resources for decision-making, forecasting trends, and optimizing business processes. The proliferation of sensor networks, social media, the Internet of Things, and mobile applications leads to a continuous increase in the amount of data that needs to be collected, stored, processed, and analyzed in real time. This requires new approaches

to application design that ensure scalability, high processing speed, and system reliability.

Features of Big Data and distributed systems. Big Data is characterized by its large volume, generation speed, variety of data structures and unpredictability of its use, which complicates the traditional approach to data processing in centralized systems [1, 2]. Distributed systems, on the contrary, allow you to divide computing and storage resources between numerous nodes, ensuring parallel execution of tasks and scaling of applications as data volumes increase. An example is the processing of data about users of a social network, where billions of events are generated daily, including posts, likes, comments and video views. In this case, a centralized system is not able to process such volumes in real time, while a distributed architecture using server clusters allows you to analyze data streams in parallel, store them in distributed file systems and apply machine learning algorithms to detect patterns and generate recommendations for users.

Architecture of applications for processing Big Data. Building big data applications involves designing an architecture that includes data collection, storage, processing, and analytics components [3, 4]. Data collection is accomplished through sensors, web service logs, third-party APIs, or real-time data streams fed into the system using streaming technologies such as Apache Kafka or RabbitMQ. Storing information requires the use of scalable storage, such as distributed file systems such as Hadoop Distributed File System or NoSQL databases such as Cassandra and MongoDB, which allow for working with large amounts of structured and semi-structured data. Data processing is performed in parallel on clusters using frameworks such as Apache Spark, which supports both batch and streaming data processing, allowing for the implementation of complex analytics, statistical processing, and machine learning algorithms. For example, e-commerce companies use similar architectures to forecast demand for products, detect fraudulent transactions, and personalize content for each user, where data from web resources, mobile applications, and transaction systems is combined, processed, and analyzed in real time.

Technologies and tools. A variety of technologies and tools are used to develop Big Data applications that allow you to effectively work with ever-growing volumes of data. Apache Hadoop, for example, provides the ability to store and process data distributed across server clusters using the MapReduce model, which distributes tasks between nodes and aggregates results, which ensures high performance and system fault tolerance. Apache Spark, in turn, allows you to implement complex analytical and machine learning algorithms at high speed thanks to in-memory data processing, which is especially effective for forecasting or data stream processing tasks. Tools such as Tableau or Power BI are often used to visualize the results of analytics, which allow you to transform large data sets into understandable graphs, dashboards, and interactive reports. As an example, in the healthcare sector, medical institutions use similar tools to analyze patient data in real time, predict the risk of complications, and form personalized treatment plans, where information from electronic medical records, laboratory results, and patient sensors is processed and analyzed using distributed Big Data systems.

Examples of practical use. In the real world, building applications for big data processing finds applications in many industries. For example, financial institutions use distributed systems to analyze bank transactions to detect fraud, where machine learning algorithms process streams of data about customer transactions, compare them with historical patterns, and instantly report suspicious activity. In the transportation industry, companies use Big Data to predict the load on public transport routes, processing data from GPS trackers, passenger flow sensors, and weather conditions, which allows them to optimize traffic schedules and reduce congestion. Social networks, on the other hand, analyze user behavior, including likes, comments, video views, and interactions with advertisements, using recommendation algorithms based on distributed data processing, which allows them to personalize content and increase audience engagement. Even in scientific research, such as in the field of climatology, large amounts of data from satellites and sensor networks are processed in distributed systems to model climate change and predict weather events.

Challenges and prospects. Despite its many advantages, developing applications for Big Data in distributed systems faces certain challenges. These include ensuring data consistency and integrity in distributed storage, system scalability when data volumes increase dramatically, optimizing processing algorithms to reduce latency, as well as protecting confidential information and complying with security regulations, which is becoming critical in the financial, medical, and government sectors. The prospects for the development of this area are associated with the improvement of machine learning algorithms, the development of cloud computing infrastructure, and the emergence of new frameworks for real-time data processing, which will allow creating more efficient and reliable applications for analyzing large amounts of data in any industry.

Future solutions will allow for more efficient systems for analyzing large amounts of data in finance, medicine, transportation, social media, and scientific research.

Conclusions. Creating applications for processing and analyzing large amounts of data in distributed systems is a key area of modern science and practice of information technology, which allows you to effectively work with giants. It provides parallel processing and scaling of resources, as well as the ability to implement complex analytical tasks and machine learning algorithms. Distributed systems provide flexibility, reliability and high performance, and their use in various industries, including finance, healthcare, transportation, social networks and science, proves the practical value and necessity of such solutions. The future development of Big Data applications involves improving algorithms, integrating cloud technologies and increasing data security, which will allow creating even more powerful and efficient information processing systems.

The creation of applications for processing and analyzing large amounts of data in distributed systems is a key direction of modern science and practice of information technologies. Distributed systems provide efficient processing of giant data sets, resource scaling, high performance and reliability. Their application in finance, medicine, transport, social networks and science proves the practical value of

such solutions. Further development of Big Data applications will be associated with the improvement of algorithms, the integration of cloud technologies and increased data security, which will create even more powerful and efficient information processing systems.

References

1. Dean J., Ghemawat S. MapReduce: Simplified Data Processing on Large Clusters. Communications of the ACM. 2008.
2. Zaharia M., Chowdhury M., Franklin M. et al. Spark: Cluster Computing with Working Sets. USENIX. 2010.
3. Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt. 2013.
4. Big Data: Survey, Technologies, Opportunities, and Challenges. Nawsher Khan, Ibrar Yaqoob, Ibrahim Abaker Targio Hashem, Zakira Inayat, Waleed Kamaleldin Mahmoud Ali, Muhammad Alam, Muhammad Shiraz and Abdullah Gani. The Scientific World Journal. January 2014.

УДК 378.147

Verhun Sofia,
undergraduate student,
Kyiv National Linguistic University
Research advisor
Melnyk Alla,
PhD in Pedagogy, Associate Professor, Associate Professor
of the Department of Germanic and Romance Languages,
Kyiv National Linguistic University

INTEGRATING SONGS, MEMES, AND VIRAL VIDEOS INTO ENGLISH TEACHING

In the context of the modern educational space, the teaching of English takes place within digital culture, where students constantly interact with multimedia content: music, memes, videos, and social networks. Teachers who integrate these resources into the learning process not only actualize lexical material but also provide students with exposure to real-life language, including slang and informal expressions.

The use of music and popular songs in foreign language learning has long proven its effectiveness. Research shows that repetitive rhymes, rhythm, and melody help students better memorize words and expressions. For example, Engh (2013) in the article “Why Use Music in English Language Learning?” emphasizes that songs create a positive emotional atmosphere, reduce stress, and increase students’ motivation.

Purpose: to examine how songs, memes, and viral videos can be systematically

integrated into ELT to enhance vocabulary, pragmatics, and cultural literacy. Tasks: (a) synthesize theoretical perspectives, (b) review classroom applications, and (c) propose ready-to-use activities.

Particular attention is drawn to memes as an example of multimodal resources. They combine visual elements (images, templates, color, composition), linguistic elements (captions, fonts, orthography that can convey tone), as well as spatial elements (the placement of text in relation to the image, sequence of panels). As Serafini (2013) notes in his concept of multimodal literacy, such resources construct meaning in ways that go far beyond verbal language. Therefore, analyzing memes in the classroom allows us to consider them as “multimodal texts” that foster critical thinking and a better understanding of contemporary English-speaking culture.

Donaghy and Xerri (2017) highlight the importance of visual materials in English language teaching, emphasizing that images are a key channel of communication for the digital generation. In this context, memes are not merely “jokes” but cultural markers that help students acquire slang and culturally nuanced vocabulary. Similarly, Herrero and Vanderschelden (2019) examine the use of film and media in language learning as a way of immersing students in an authentic environment. Viral videos and popular music clips can serve a similar role: they reproduce real-life examples of spoken language, emotional reactions, and current social themes. This enables teachers to create tasks that go beyond textbook exercises.

We argue these resources should **complement**, not replace, core instruction through scaffolded, task-based activities with clear assessment criteria.

Practical implementation of this approach may include:

While evidence is promising, typical concerns include distraction, privacy, and assessment validity, which require explicit classroom policies and rubrics.

Music Vocabulary Challenge – students listen to a popular song, write down new words and phrases, then explain their meaning in groups and create short dialogues.

Song Vocabulary Task – students listen to a popular song, identify slang expressions, and create a mini-dictionary.

Meme Analysis Workshop – students receive a selection of English-language memes, analyze them from the perspective of multimodal literacy (visual, linguistic, spatial), and then create their own memes in English.

Viral Video Discussion – after watching a viral video, students discuss which words/expressions they have learned and reproduce a short dialogue in the style of the video. For instance, some memes rely on wordplay and cultural humor, which can help

learners notice multiple meanings of a word in context.



Figure 1. Meme created by the author

A humorous meme shows a man asking a woman, “When is your birthday?” She answers, “March 1st.” The man then starts marching around the room, because the word *March* can mean both the *month March* and the *action to march*. This kind of joke draws students’ attention to lexical ambiguity, encourages discussion, and makes learning vocabulary memorable. Using memes in this way allows learners to engage creatively with language, understand cultural nuances, and internalize words and phrases in a fun and meaningful context.

Anticipated research. We plan a quasi-experimental study (pre-/post- with delayed post-test) comparing song/meme/viral-video tasks to standard practice, measuring vocabulary retention, pragmatic awareness, and culture-specific references across two proficiency bands.

Thus, the integration of songs, memes, and viral videos into English language teaching opens new horizons for education. It is not limited merely to increasing students’ motivation or diversifying the learning process. In fact, it is a kind of cultural dialogue, in which students immerse themselves in the living language of modernity, gaining experience with authentic resources that exist beyond the textbook. A key task for further research is to identify which task types (e.g., lyric gap-fills, meme analysis, scene re-voicing) most strongly predict durable gains and how best to assess them reliably.

References:

1. Donaghy, K., & Xerri, D. (Eds.). (2017). *The image in English language teaching*. ELT Council. <https://bit.ly/3xXb6vY>
2. Engh, D. (2013). Why use music in English language learning? A survey of the literature. *English Language Teaching*, 6(2), 113–127. <https://doi.org/10.5539/elt.v6n2p113>
3. Herrero, C., & Vanderschelden, I. (2019). *Using film and media in the language classroom: Reflections on research-led teaching*. Multilingual Matters.
4. Serafini, F. (2013). *Reading the visual: An introduction to teaching multimodal literacies*. Teachers College Press.

Kolesnychenko K. M.

Higher Education Student,

ERI "Karazin Banking Institute" V. N. Karazin Kharkiv National University

Scientific Advisors:

Denchyk I. S.

Senior Lecturer, Department of Management,

Accounting and Business Communications

ERI "Karazin Banking Institute" V. N. Karazin Kharkiv National University

SOFTWARE TOOLS FOR ENHANCING EFFICIENCY IN COMPUTER SCIENCE

In today's world, computer science has become a key field that supports processes across business, science, education, and industry. With the development of information technologies, software tools have become the main instrument for improving efficiency, automating tasks, analyzing data, and making informed decisions. They significantly reduce the time required for routine operations, decrease the number of errors, and increase the productivity of both individuals and organizations.

Software tools in computer science cover a wide range of applications—from office suites and specialized programs to complex integrated systems. Low-code and no-code platforms have recently gained popularity, allowing applications to be created without deep programming knowledge. Such solutions combine data analysis, business process automation, and custom app development, thereby increasing organizational efficiency.

One of the most important areas is business analytics. Business Intelligence (BI) solutions allow companies to collect, store, and analyze large volumes of information. This helps managers quickly assess situations, forecast market trends, and make evidence-based decisions. The use of such tools reduces errors, increases operational transparency, and generally improves business productivity [1].

Another important example is project management software. In computer science, such tools allow teams to coordinate activities, monitor deadlines, and manage resources. Using these systems reduces the risk of project delays, ensures proper task allocation, and improves teamwork efficiency. Studies show that specialized project management software helps plan processes effectively, reduce costs, and enhance communication among participants.

Artificial intelligence and intelligent data analysis tools also deserve special attention. In computer science, such software is used to automatically process large datasets, identify patterns, and make predictions. The application of these tools enables companies to react quickly to market changes, identify risks, and make optimal decisions. Research highlights that these technologies have become a key factor in strengthening competitiveness [2].

Benefits and Challenges. The main benefits of using software tools in computer science include:

automating routine tasks and reducing employee workload;
providing faster access to information through storage and analysis systems;
optimizing management processes in business, science, and education;
customizing the working environment through adaptive solutions.

At the same time, there are challenges: high implementation costs, the need for staff training, compatibility issues between different systems, and data security concerns. However, the efficiency that modern software tools provide significantly outweighs these disadvantages.

Thus, software tools are a crucial factor in improving efficiency across various fields of activity, especially in computer science. They automate tasks, analyze large volumes of data, increase team productivity, and support strategic decision-making. The continued development of technologies—particularly in artificial intelligence and cloud platforms—will further strengthen their impact on organizational efficiency.

References:

1. Laudon, K. C., & Laudon, J. P. (2022). *Management information systems: Managing the digital firm* (17th ed.). Pearson.
2. Turban, E., Sharda, R., Delen, D., & King, D. (2021). *Business intelligence, analytics, and data science: A managerial perspective* (5th ed.). Pearson.

UDC 004.8:631.67

Kuzmenko Y. E.

Higher Education Student,

ERI "Karazin Banking Institute" V. N. Karazin Kharkiv National University

Scientific Advisor:

Denchyk I. S.

Senior Lecturer, Department of Management,

Accounting and Business Communications

Yermakova N.A.

Senior Lecturer, Department of of Information Technologies

and Mathematical Modeling

ERI "Karazin Banking Institute" V. N. Karazin Kharkiv National University

APPLICATION OF ARTIFICIAL INTELLIGENCE IN SMART GREENHOUSE MANAGEMENT

The application of artificial intelligence (AI) in greenhouse management is highly relevant today due to the urgent need to increase agricultural efficiency and conserve natural resources. In 2024, weather conditions in Ukraine were devastating for agricultural production: drought and record-high temperatures led to a 10–20% decrease in the yield of grain and oilseed crops compared to the previous year. The total yield of grain and oilseed crops is expected to reach 73–75 million tons, which is

9.5–12.7% lower than last year. The southern and eastern regions were the most affected, where both air and soil temperatures were extremely high and precipitation was minimal. Such crop losses negatively impact not only the economy of farms but also the state budget, as agricultural products account for a significant portion of the country's exports and tax revenues. In these conditions, the use of intelligent systems in greenhouses becomes essential, as they allow for automated microclimate control and optimization of plant growing conditions, ensuring stable yields.

A smart greenhouse is a general term for greenhouses with intelligent management systems, such as Dutch-style Venlo greenhouses. They are equipped with modern technologies: lighting, heating, ventilation, irrigation systems, sun protection, and other devices that allow the automation of cultivation processes. Implementing intelligent management systems and Internet of Things (IoT) technologies makes microclimate control more precise, reduces the technical complexity of greenhouse management, and increases production efficiency.

These greenhouses are now used worldwide and are equipped with advanced technologies, including LED lighting, air filtration systems, and automated irrigation. The heart of a smart greenhouse is IoT-based systems, which connect interrelated physical devices with built-in sensors and software for automatic data collection, transmission, and exchange between the physical environment and computer systems.

IoT sensors provide information on light levels, temperature, and humidity, allowing operators to create optimal conditions for effective agricultural production. By precisely adjusting climate parameters with the help of artificial intelligence, smart greenhouses can significantly increase crop yields while reducing production costs compared to traditional methods.

In Ukraine, startups are emerging that implement such systems. For example, Green IQ offers fully automated aeroponic greenhouses, where equipment independently controls lighting, heating, ventilation, and climate, while the user monitors the process via a mobile app. Another project, Smart Oasis Farm by the startup IDA, creates autonomous greenhouses where water is harvested from the air and delivered to plants as enriched mist, while full-spectrum LEDs provide lighting. These innovative solutions allow automation of most processes—from irrigation to harvesting—and ensure high efficiency even in challenging climatic conditions.

A prominent example of international experience is the large-scale agricultural project by Dyson in the British town of Carrington. The 760-meter-long greenhouse is controlled by artificial intelligence and combines efficient food production with environmental responsibility. It operates on renewable energy and utilizes excess heat from an anaerobic reactor, significantly reducing carbon emissions. The complex monitors every stage of berry growth with maximum precision: the system analyzes humidity, temperature, lighting, and soil nutrient composition, automatically making adjustments to achieve optimal conditions. The greenhouse contains 1,456 rows with over 1.2 million strawberry plants, producing approximately 1,250 tons of berries annually for the UK domestic market. The use of AI ensures high-quality yields regardless of weather conditions. In addition, closed-loop irrigation and heat reuse reduce water consumption and carbon footprint, enhancing production efficiency and minimizing environmental impact.

Thus, the application of artificial intelligence in greenhouse management allows for the automation of microclimate control, optimization of plant growing conditions, and ensures stable yields even under adverse weather conditions. The use of modern technologies, such as IoT and automated management systems, increases production efficiency, reduces costs, and promotes the conservation of natural resources.

Farms and startups should actively implement intelligent systems and smart greenhouses, continuously update their technologies, and train personnel to achieve maximum productivity and sustainable development of the agricultural sector.

References:

1. AI360. (n.d.). *Dyson connected AI to a greenhouse for strawberry cultivation*. Retrieved from <https://ai360.com.ua/dyson-pidkliuchyla-shi-do-teplytsi-z-vyroshchuvannia-polunytsi/>
2. Greenhouse Vendor. (n.d.). *What is a smart greenhouse: The composition of a smart greenhouse*. Retrieved from <https://ua.greenhousevendor.com/info/what-is-a-smart-greenhousethe-composition-of-a-80037361.html>
3. iFarming. (n.d.). *Smart solutions step into the agricultural world*. Retrieved from <https://ifarming.ua/itehnologii/selektsiya/smartrishennya-krokuyut-agrosvitom>
4. Economic Pravda. (2024, October 16). *How much Ukraine can earn from grain exports*. Retrieved from <https://epravda.com.ua/publications/2024/10/16/720623/>

УДК 330.341.1:334.722:338.12

Астаф'єва К.Ю.

здобувач вищої освіти,

ННІ «Навчально-науковий інститут комп'ютерних наук та інформаційних технологій» НТУ «Харківський політехнічний інститут»

ВИКЛИКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ В УКРАЇНСЬКОМУ БІЗНЕСІ ТА МОЖЛИВІ РІШЕННЯ

Зі стрімким розвитком сфери ІТ в Україні цифрова трансформація стала ключовим фактором конкурентоспроможності у 2025 році. Зараз бізнес все активніше впроваджує різні інноваційні технології для полегшення внутрішніх процесів та можливості плідно працювати на рівні з глобальними ринковими умовами. Цифрова трансформація є надзвичайно актуальною темою, рівень цифрових послуг в Україні значно зріс, багато бізнесів почали працювати онлайн через війну, що дало поштовх для розвитку нових бізнес-моделей, обізнаності підприємців в різних інноваціях. Згідно з даними дослідження ЕМ Україна APS-2024, близько 32,6% зареєстрованих в Україні компаній,

використовують інструменти аналізу даних, 27,7% використовують хмарні технології, а штучний інтелект має попит у 22,4% бізнесів [1].

Серед основних викликів цифрової трансформації українського бізнесу можна виділити декілька ключових аспектів. По перше, це фінансові обмеження, багато бізнесів через ситуацію в Україні зараз перебувають на межі банкрутства, також для малого бізнесу цифровізація не є ключовим етапом у розвитку. На щастя, кількість кваліфікованих працівників у сфері інформаційних технологій, досить велика, за даними статистики сайту Work.ua на 5 тисяч вакансій є приблизно 330 тисяч кандидатів [2], тому проблем з працівниками не має. Проте, попри такі позитивні показники кількості кандидатів, все ще є проблема у сфері кадрового забезпечення. Все ще багато підприємців не мають чіткого уявлення щодо необхідних компетенцій та профілю фахівців, яких треба залучати до цифрової трансформації. Також ще одним викликом є безпека даних та їх конфіденційність, адже з впровадженням цифровізації в бізнес так само пропорційно є ризик кіберзагроз. Недостача кіберграмотності у працівників може призвести до витоку інформації, пошкодженню ресурсів, фінансових витрат, втрати довіри клієнтів та погіршенню репутації.

Водночас з викликами є шляхи їх подолання, наприклад, для вирішення фінансових труднощів є гранти – «Дія.Бізнес», USAID, GIZ, програма «Цифрова економіка» від Міністерства цифрової трансформації України, яка передбачає фінансування проєктів, що сприяють розвитку цифрових послуг. Також критично важливим є інвестування компаній в кадровий потенціал – придбання корпоративних тренінгів, оплата курсів, перекваліфікація робітників, виділення часу для освоєння нових технологій. Для запобігання кібератак компанії можуть моніторити кіберзагрози, покращувати кіберграмотність працівників, впровадження багатофакторної автентифікації, шифрування даних та формувати культуру інформаційної безпеки серед робітників бізнесу. Співпраця компаній з IT-стартапами може допомогти почати свій шлях цифрової трансформації з невеликими затратами коштів і зі свіжим поглядом на інновації сьогодення.

Формування точного плану інтеграції цифрових технологій в усі аспекти бізнесу в тандемі з впровадженням сучасних технологічних рішень, таких як хмарні сервіси, ERP та CRM-системи, автоматизація процесів, створенням плану неперервної діяльності, дає змогу компаніям бути адаптивними до змін навколо, знижувати ризик труднощів та забезпечувати ефективність внутрішніх і зовнішніх процесів в будь-яких умовах сьогодення. Таким чином цифрова трансформація українського бізнесу є не просто масовим трендом, а стратегічною необхідністю.

Список використаних джерел

1. Вишневський І. Хмарні технології використовують близько 28% всіх українських бізнесів, а ІІІ – понад 24%. Що ще показує соцдослідження? // Dev.ua. URL:

<https://dev.ua/news/khmarni-tekhnologii-vykorystovuiut-blyzko-28-vsikh-ukrainskykh-biznesiv-a-shi-ponad-24-shcho-shche-pokazuie-sotsdoslidzhennia-1740215422>

2. Середня зарплата по Україні. // Work.ua. 2025. Вересень. URL: <https://www.work.ua/salary/>

УДК 004.056.53

Білоцерківська В.А.
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Науковий керівник
Кобилін І.О.
старший викладач кафедри Інформатики
Харківський національний університет радіоелектроніки

МЕТОДИ ЗБОРУ ТА ПОПЕРЕДНЬОЇ ОБРОБКИ ДАНИХ ВАКАНСІЙ ДЛЯ ПОДАЛЬШОГО МАШИННОГО АНАЛІЗУ

Процеси пошуку роботи дедалі частіше здійснюються в онлайн-середовищі. Вакансії розміщуються на спеціалізованих веб-порталах, у соціальних мережах та месенджерах, що значно спрощує доступ до інформації для користувачів. Водночас це створює ризики поширення недостовірних або шахрайських оголошень. Для розробки системи автоматизованого виявлення таких вакансій із використанням методів машинного навчання першочерговим завданням є організація якісного процесу збору та попередньої обробки даних. Саме на цьому етапі формується основа подальшого аналізу, від якої безпосередньо залежить точність і надійність моделей.

Основним джерелом інформації виступають відкриті ресурси з пошуку роботи (наприклад, Work.ua, Rabota.ua, Jooble, LinkedIn). Збір даних може здійснюватися двома основними підходами:

- Використання API – офіційні інтерфейси дозволяють отримувати структуровані дані у форматах JSON або XML. Такий спосіб є надійним, оскільки дані подаються у впорядкованому вигляді.
- Веб-скрейпінг – застосування інструментів (BeautifulSoup, Scrapy, Selenium) для автоматизованого витягування тексту вакансій із HTML-кодів сторінок. Цей метод використовується у випадках, коли API недоступний або надає обмежену кількість інформації.

Важливим завданням є формування достатнього обсягу даних, адже для навчання моделей машинного навчання потрібні великі масиви інформації. Крім того, бажано збирати вакансії з різних джерел, щоб уникнути упередженості (bias), яка може виникнути при аналізі лише одного сайту.

Зібрані дані, як правило, мають неструктурований вигляд: вони містять текстові описи, HTML-розмітку, зайві символи та дублікати. Тому необхідно провести комплексну обробку, яка складається з кількох етапів (рис.1).

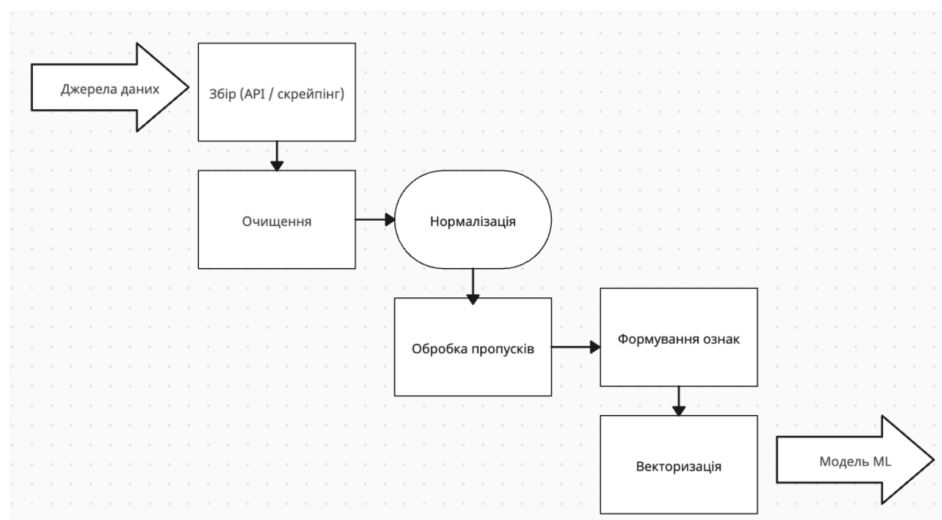


Рисунок 1 — алгоритм збору та попередньої обробки даних вакансій

Дані вакансій потребують попередньої обробки для забезпечення їх придатності до машинного аналізу. На першому етапі здійснюється очищення тексту – видалення HTML-тегів, спеціальних символів, емодзі, контактних номерів та електронних адрес, які не несуть суттєвої інформативності. Далі проводиться усунення дублікатів, оскільки одна й та сама вакансія може повторюватися на різних ресурсах, що спотворює результати. Важливим кроком є нормалізація тексту: усі символи зводяться до одного регістру, вилючаються стоп-слова, а слова лематизуються чи стемінгуються, щоб привести їх до базової форми. Також потрібно враховувати наявність пропусків у даних – у випадку відсутності заробітної плати чи опису вакансії записи або видаляються, або доповнюються за допомогою методів апроксимації. Завершальним етапом є категоризація ознак, що передбачає перетворення текстових полів (наприклад, назви компанії чи регіону) у числові формати за допомогою one-hot encoding, label encoding або сучасних підходів на основі embeddings.

Формування ознакового простору є важливим етапом, адже саме від правильно підібраних характеристик залежить здатність моделі відрізнити реальні вакансії від шахрайських. До таких ознак належить частота використання характерних слів чи фраз на кшталт “легкий заробіток”, “без досвіду” або “робота вдома”, що часто трапляються у сумнівних оголошеннях. Додатковим індикатором може бути наявність у тексті контактної інформації, зокрема телефонних номерів чи посилань на месенджери. Важливу роль відіграє й структура самої вакансії: чи вказана зарплата, вимоги до кандидата та умови праці. Ще однією ознакою виступає довжина тексту оголошення, оскільки шахрайські публікації зазвичай коротші й менш деталізовані. Усі ці характеристики після обробки перетворюються у числові вектори, що можуть бути використані як вхідні дані для моделей машинного навчання.

Таким чином, методи збору та попередньої обробки даних вакансій є базовою складовою побудови системи виявлення недостовірних оголошень. Якість цих етапів безпосередньо впливає на ефективність алгоритмів машинного навчання, адже навіть найскладніша модель не зможе забезпечити

високу точність при використанні "шумних" чи неповних даних. Тому грамотна організація процесу збору та очищення інформації є першочерговим завданням у даному дослідженні.

Оскільки значна частина інформації подана у вигляді тексту, ключову роль відіграють методи Natural Language Processing (NLP). Для цього можуть застосовуватись: Bag-of-Words та TF-IDF – класичні методи представлення тексту або Word2Vec, FastText, BERT – сучасні моделі векторизації, що зберігають семантичні зв'язки між словами.

Список використаних джерел

1. Aggarwal, C. C. (2018). Machine Learning for Text. Springer. – Книга про методи машинного навчання для текстових даних: від очищення й обробки до побудови ознак.
2. Kumar, S., Zhang, J., Leskovec, J. (2020). Rev2: Fraudulent User Prediction in Rating Platforms. Proceedings of the ACM International Conference on Web Search and Data Mining (WSDM). – Досвід застосування ML для виявлення шахрайства на онлайн-платформах, релевантно для вакансій.

УДК 004.056.53

Бобейко К.С.

*здобувач вищої освіти, Харківський національний
університет радіоелектроніки*

Науковий керівник

Кобилін О.А.

*Завідувач кафедри інформатики, кандидат технічних наук, доцент
Харківський національний університет радіоелектроніки*

ІНТЕЛЕКТУАЛЬНІ ПРОГРАМНІ ЗАСОБИ ДЛЯ ЕНЕРГОЗБЕРЕЖЕННЯ В ЖИТЛОВОМУ СЕКТОРІ

Сталий розвиток та зелений перехід в Україні неможливі без зниження енергоспоживання та підвищення ефективності використання ресурсів. Найбільш критичною є житлова сфера, де понад 40% енергії витрачається нерационально. Традиційні методи контролю енергоспоживання обмежуються статистичною звітністю та ручним аналізом, що не дозволяє вчасно виявляти проблеми та приймати ефективні рішення. У поєднанні з енергетичною кризою та зростанням тарифів це створює нагальну потребу у впровадженні інноваційних програмних рішень, що дозволять оптимізувати споживання та зменшити навантаження на енергосистему країни.

Метою дослідження є розробка програмних засобів інтелектуального аналізу енергоспоживання на основі даних з IoT-сенсорів і систем «розумного дому» для оптимізації витрат ресурсів у реальному часі.

Основними завданнями є:

1. Розробка архітектури системи збору та обробки даних у реальному часі.
2. Впровадження алгоритмів інтелектуального аналізу (кластеризація, прогнозування, виявлення аномалій).
3. Створення інтерфейсу прийняття рішень для користувачів з персоналізованими рекомендаціями.
4. Проведення експериментів на основі даних житлових домогосподарств. Методологія дослідження базується на використанні модульного підходу.

Система складається з:

- модуля збору даних з сенсорів електро-, тепло- та водоспоживання з використанням протоколів MQTT та OPC UA;
- аналітичного модуля, що включає алгоритми кластеризації K-Means для групування моделей споживання, LSTM-мережі для прогнозування добових та місячних обсягів енергоспоживання, а також статистичні методи (Z-score) для виявлення аномалій;
- системи рекомендацій, яка на основі аналізу даних пропонує користувачам практичні кроки для зниження витрат;
- користувацького інтерфейсу у вигляді веб-панелі та мобільного додатку.

Експериментальні дослідження були проведені для перевірки ефективності на вибірці з 50 домогосподарств м. Харкова. Використано понад 120 тис. записів про енергоспоживання за період 2022–2024 років. Алгоритми показали високу точність прогнозування та виявлення відхилень.

Таблиця 1.

Результати експериментальних досліджень

Метрика	Результат
Точність прогнозу	91.7%
Виявлення аномалій	88.3%
Середнє зниження споживання	12-18%

Формула інтегральної оцінки ефективності енергоспоживання має вигляд:

$$E = \sum_{i=1}^n w_i * N_i$$

де w – ваговий коефіцієнт i -ї метрики, N – нормалізоване значення i -ї метрики.



Рисунок 1 – Динаміка зниження енергоспоживання у тестових домогосподарствах

Наукова новизна полягає у поєднанні методів інтелектуального аналізу даних та адаптивного моніторингу енергоспоживання з можливістю інтеграції у масштабовані інформаційні системи «розумного міста».

Практична значущість – створення програмного комплексу, що сприяє зниженню енергетичних витрат населення та підвищує ефективність використання ресурсів у житловому секторі, що має стратегічне значення для забезпечення зеленого переходу в Україні.

Список використаних джерел:

1. Li Y., Zhang T. Smart energy management systems based on IoT and machine learning. *Energy Informatics Journal*. 2023. Vol. 6, No.P. 112–129.2.
2. Petrova O., Ivanov I. Development of intelligent decision support for energy saving in smart cities. *International Conference on Green Technologies*. 2022. P. 145–153.
3. Wang H., Chen L. Real-time anomaly detection in residential energy consumption. *Journal of Sustainable Computing*. 2021. Vol. 31. P. 67–78.
4. Міненерго України. Звіт про стан енергоспоживання у житловому секторі. Київ, 2022.
5. Ghosh A., Kumar R. LSTM-based forecasting models for energy efficiency. *IEEE Transactions on Smart Grid*. 2021. Vol. 12, No. 5. P. 4124–4133.
6. Chen S., Li M. Anomaly detection techniques in smart home energy data. *Applied Energy*. 2020. Vol. 275. P. 115389.

Богдан Н.І.
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Науковий керівник
Творошенко І.С.
к.т.н., доцент, доцент кафедри інформатики
Харківський національний університет радіоелектроніки

ПОРІВНЯЛЬНИЙ АНАЛІЗ АРХІТЕКТУРНИХ РІШЕНЬ ДЛЯ ІНТЕГРАЦІЇ ДОВГОТРИВАЛОЇ ПАМ'ЯТІ У ДІАЛогові СИСТЕМИ

Тематика обмеженої контекстуальної пам'яті існуючих великих мовних моделей (LLMs) є одним із ключових архітектурних викликів у проєктуванні сучасних діалогових систем. Кінцевий розмір контекстного вікна призводить до втрати релевантної інформації під час тривалих сесій, що знижує актуальність та якість взаємодії. Це, в свою чергу, вимагає пошуку та аналізу архітектурних рішень, здатних розширити пам'ять LLMs, забезпечуючи послідовність і логічну узгодженість діалогу [1-3].

Для подолання вказаної проблеми існує низка підходів, що принципово відрізняються своєю архітектурою та ефективністю:

- архітектура «ковзного вікна» (Sliding Window) – метод, який є найпростішим з точки зору реалізації. Він передбачає збереження лише останніх повідомлень діалогу, які вміщуються у фіксований буфер контекстного вікна. Ключовою перевагою даного методу є простота і низькі обчислювальні витрати. Однак, зазначений підхід має суттєвий недолік: він безповоротно втрачає ранній контекст, що робить його непридатним для тривалих діалогів, де важлива вся історія;

- архітектура узагальненої (епізодичної) пам'яті (Summarized/Episodic Memory) – метод, який є проміжним між простим буфером і складними гібридними системами. Його архітектура включає додатковий етап, на якому старі фрагменти діалогу періодично узагальнюються в короткі резюме. Ці резюме потім додаються до поточного контекстного вікна. Перевага цієї архітектури полягає в збереженні ключових ідей розмови без перевантаження контексту, вона може втрачати дрібні, але важливі деталі, які не потрапили в узагальнення;

- архітектура «генерації, доповненої пошуком» (Retrieval-Augmented Generation, RAG) – найбільш ефективне архітектурне рішення. Метод поєднує можливості LLM з зовнішньою базою знань. Архітектура RAG складається із двох основних компонентів: ретрівер-модуля, що виконує пошук релевантних фрагментів даних, і генератор-модуля, який створює відповідь, використовуючи як запит, так і знайдені дані (рис. 1). Цей підхід забезпечує високу точність, дозволяє надавати відповіді, які ґрунтуються на достовірних джерелах, і значно розширює «пам'ять» системи. Однак, його головним недоліком є архітектурна

складність та потреба в додаткових ресурсах для керування зовнішньою базою даних.

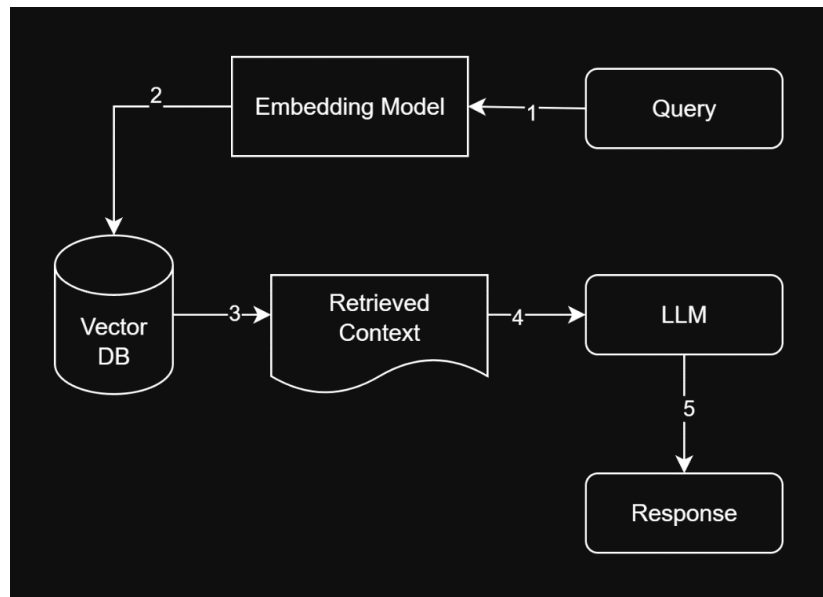


Рисунок 1 – Схематичне подання методу RAG

Отже, вибір архітектурного рішення для інтеграції довготривалої пам'яті є компромісом між простотою реалізації та ефективністю. Якщо «ковзне вікно» підходить для простих завдань, то для критично важливих застосувань, що вимагають високої точності та зв'язності, архітектура RAG є найбільш доцільною. Розуміння цих архітектурних відмінностей є фундаментальним для проектування та впровадження надійних і ефективних діалогових систем [4, 5].

Список використаних джерел:

1. Gorokhovatskyi V., Chmutov Y., Tvoroshenko I., and Kobylin O. (2025) Reducing computational costs by compressing the structural description in image classification methods, *Advanced Information Systems*, vol. 9, no. 1, pp. 5-12.
2. Gorokhovatskyi V., Tvoroshenko I., Yakovleva O., Hudáková M., and Gorokhovatskyi O. (2024) Application a committee of Kohonen neural networks to training of image classifier based on description of descriptors set, *IEEE Access*, vol. 12, pp. 73376-73385.
3. Gorokhovatskyi V., Tvoroshenko I., Yakovleva O., and Hudáková M. (2025) Image description compression in classification structural methods, *IEEE Access*, vol. 13, pp. 43631-43641.
4. Yakovleva O., Matúšová S., Tvoroshenko I., and Isaiev Y. (2024) Visitor counting based on video stream analysis from surveillance cameras to solve various business problems, *Verejná správa a regionálny rozvoj ekonómia, manažment a marketing*, XX(1), pp. 67-87.
5. Gorokhovatskyi V., Tvoroshenko I., Yakovleva O. (2024) Transforming image descriptions as a set of descriptors to construct classification features, *Indonesian Journal of Electrical Engineering and Computer Science*, 33 (1), 113-125.

Бойко М.К.*здобувач вищої освіти,**Харківський національний університет радіоелектроніки**Науковий керівник***Кобилін О.А.***Завідувач кафедри інформатики, кандидат технічних наук, доцент**Харківський національний університет радіоелектроніки*

МЕТОД БАГАТОВИМІРНОГО АНАЛІЗУ ЕФЕКТИВНОСТІ РЕКЛАМНИХ КАМПАНІЙ З АДАПТИВНИМ МОНІТОРИНГОМ

Сучасний ринок цифрової реклами характеризується високою динамічністю та необхідністю швидкого прийняття рішень для оптимізації рекламних бюджетів. Традиційні підходи до управління рекламними кампаніями часто базуються на простих метриках та інтуїтивних рішеннях, що не враховують складні взаємозв'язки між різними факторами впливу на ефективність кампаній.

Метою дослідження є розроблення комплексного методу багатовимірного аналізу ефективності рекламних кампаній з адаптивним моніторингом для підвищення точності прогнозування ROI та автоматизації прийняття управлінських рішень.

Запропонований метод включає наступні компоненти:

1. Модель інтегральної оцінки ефективності кампанії:

$$E = \sum_{i=1}^n w_i * N_i,$$

де w – ваговий коефіцієнт i -ї метрики, N – нормалізоване значення i -ї метрики за формулою:

$$N_i = (X_i - X_{\min,i}) / (X_{\max,i} - X_{\min,i}).$$

Вагові коефіцієнти визначаються на основі кореляційного аналізу:

$$w_i = |corr(X_{i,ROI})| / \sum_{j=1}^n |corr(X_{j,ROI})|.$$

2. Система виявлення аномалій базується на статистичному Z-score аналізі:

$$Z_i = \frac{X_i - \mu_i}{\sigma_i}.$$

Аномалія детектується при $Z_i > 2.5$

Експериментальне дослідження проведено на реальних даних рекламних кампаній за період 2024 року обсягом понад 10,000 конверсій. Результати тестування показали:

Точність прогнозування ROI підвищилася до 93.1% порівняно з 76.3% у базових методів;

Точність виявлення аномалій склала 87.2% при співвідношенні Precision/Recall = 85.45%/94.00%;

Час прийняття управлінських рішень скоротився з годин до хвилин;

Середнє підвищення ROI кампаній склало 15-25% при зменшенні ризиків на 30-40%.

Зростання обсягів даних у цифровому маркетингу та необхідність швидкого реагування на зміни ринкових умов створюють потребу в розробці інтелектуальних систем автоматизованого управління рекламними кампаніями. Існуючі рішення часто не враховують багатовимірну природу факторів впливу на ефективність реклами та не забезпечують адаптивного моніторингу в реальному часі.

Модуль збору та preprocessing даних забезпечує інтеграцію з трекінговими системами (Keitaro, Voluum) та рекламними платформами (Facebook Ads, Google Ads) для отримання метрик у реальному часі.

Модуль моніторингу та уведошень забезпечує передачу інформації через Telegram API з адаптивною частотою оновлення.

Система реалізована з використанням Python 3.9, frameworks FastAPI для веб-сервісу, SQLite для зберігання даних, та бібліотек Pandas, Scikit-learn для аналітичних обчислень.

Тестування проведено на реальних даних медіабайнг компанії за період січень-грудень 2024 року:

Метрика	Базовий метод	Запропонована система	Покращення
Точність прогнозування ROI, %	76.3	93.1	+22.0%
Час прийняття рішення	2-4 години	2-3 хвилини	-95.8%
Виявлення аномалій, %	68.4	87.2	+27.5%
Середній ROI кампаній, %	125.6	152.3	+21.3%

Рисунок 1 – Результати тестування системи

Система продемонструвала стабільну роботу при обробці до 10,000 конверсій на день з середнім часом відгуку API 150 мс.

Науковою новизною роботи є розроблення комплексного підходу, що поєднує інтегральну оцінку ефективності на основі кореляційного аналізу, адаптивне виявлення аномалій та гібридне прогнозування з автоматичним прийняттям рішень.

Практична значущість полягає у створенні програмного комплексу для автоматизованого управління цифровими рекламними кампаніями, що забезпечує підвищення ефективності розподілу бюджетів та оптимізацію управлінських процесів у реальному часі.

Список використаних джерел:

1. Chen L., Wang X. Real-time optimization of digital advertising campaigns using machine learning algorithms. Journal of Digital Marketing Analytics. 2023.

Vol. 15, No. 3. P. 45-62.

2. Rodriguez M., Smith J. Multidimensional analysis of digital marketing efficiency using Data Mining techniques. International Conference on Marketing Analytics. 2022. P. 278-295.

3. Li Y., Johnson K. Time series forecasting for advertising campaign performance prediction. Machine Learning in Business Applications. 2022. Vol. 12, No. 4. P. 89-105.

УДК 339.56:658.87

Бондаренко А. Є.,

здобувачка вищої освіти

Науковий керівник

Линенко А. В.,

доцент кафедри управління персоналом і маркетингу,

кандидат економічних наук, доцент,

Запорізький національний університет

АНАЛІЗ МІЖНАРОДНИХ РИНКІВ ДЛЯ ОПТИМІЗАЦІЇ ПОСТАЧАННЯ

Сучасна економіка все більше орієнтується на глобалізацію, тому для ефективної роботи підприємства важливо не лише розуміти внутрішній ринок, але й активно вивчати міжнародні ринки. Особливо це стосується відділу постачання, який відповідає за закупівлю сировини, матеріалів, обладнання та організацію логістичних процесів. Саме аналіз міжнародних ринків допомагає підприємству знизити витрати, підвищити ефективність і забезпечити стабільність у роботі.

Конкуренція між компаніями посилюється, і успіх залежить від того, наскільки швидко та гнучко підприємство реагує на зміни у світовій економіці. Зростання цін на енергоносії, зміна валютних курсів, політичні кризи чи перебої у світових ланцюгах постачання безпосередньо впливають на діяльність відділу постачання. Тому компанії вже не можуть обмежуватися лише локальними закупівлями, а повинні аналізувати пропозиції з різних країн, порівнювати їх і обирати найбільш вигідні варіанти.

Дослідження міжнародних ринків дає підприємствам змогу не лише знайти дешевші або якісніші ресурси, але й вибудувати довгострокові партнерські відносини з постачальниками. Це особливо важливо для тих галузей, які залежать від стабільного забезпечення сировиною та матеріалами, наприклад, металургійної, машинобудівної чи харчової промисловості. Крім того, глобальний підхід до постачання дає можливість диверсифікувати ризики: якщо виникнуть проблеми з одним постачальником, завжди можна скористатися альтернативними каналами постачання з інших країн.

Міжнародні ринки відрізняються від національних багатьма факторами: рівнем розвитку економіки, цінами, якістю товарів, законодавчими нормами та

навіть культурними особливостями. Для відділу постачання важливо враховувати ці фактори, щоб вибрати найкращих постачальників. Наприклад, один і той самий товар може коштувати дешевше в Азії, але при цьому доставка займе більше часу. В Європі, навпаки, ціна може бути вищою, проте логістика швидша та більш стабільна [1].

Аналіз міжнародних ринків допомагає маркетологам:

- знайти оптимальне співвідношення ціни та якості;
- зменшити залежність від одного постачальника;
- врахувати ризики коливання валютних курсів;
- передбачити вплив світових кризових явищ (наприклад, енергетичних чи політичних) тощо.

Таблиця 1

Порівняння умов закупівель на різних міжнародних ринках

Регіон	Переваги	Недоліки	Приклади використання
Азія	Низькі ціни на сировину та матеріали; широкий вибір постачальників	Довгі терміни доставки; високі транспортні витрати	Закупівля електронних компонентів із Китаю
Європа	Висока якість продукції; швидка логістика; стабільні правила	Вища ціна на товари; жорсткі вимоги до сертифікації	Поставка обладнання з Німеччини
Америка	Інноваційні технології; можливість довгострокових контрактів	Висока вартість доставки; залежність від валютних коливань	Закупівля програмного забезпечення зі США

Важливо не тільки купити товар, але й доставити його вчасно і з мінімальними витратами. Саме тут аналіз міжнародних ринків тісно пов'язаний із логістикою. Вибір постачальника залежить не лише від ціни продукції, а й від вартості транспортування, наявності портів, митних процедур, умов зберігання.

Оптимізація логістики включає: 1) вибір найбільш вигідних транспортних маршрутів; 2) порівняння різних видів транспорту (морський, автомобільний, залізничний, авіаційний); 3) використання сучасних цифрових систем для відстеження вантажів; 4) планування запасів, щоб уникати дефіциту або перевитрат [2].

Наприклад, підприємство може знайти дешевшого постачальника в Китаї, але через високу вартість доставки загальні витрати будуть більшими, ніж при закупівлі в Польщі чи Туреччині. Тому завдання відділу постачання – розрахувати повну логістичну вартість, а не дивитися лише на ціну товару.

Відділ постачання у сучасних компаніях стає стратегічним підрозділом, адже від його рішень залежить конкурентоспроможність бізнесу. Якщо закупівлі проводяться хаотично, підприємство може втрачати гроші та час. Якщо ж відділ постачання проводить детальний аналіз міжнародних ринків, то компанія отримує:

- економію коштів за рахунок вигідних контрактів;

- стабільність поставок;
- підвищення якості продукції;
- можливість швидко реагувати на зміни у світовій економіці [3].

Уявімо, що металургійний комбінат потребує великої кількості сировини – руди та вугілля. Якщо він закупає ці ресурси лише на внутрішньому ринку, то стає залежним від цін місцевих постачальників. Але якщо відділ постачання аналізує міжнародні ринки, то він може знайти вигідніші умови в інших країнах. При цьому потрібно враховувати витрати на транспортування, мита, а також можливі політичні ризики. Такий підхід робить підприємство більш гнучким і стійким. Аналіз міжнародних ринків є ключовим інструментом для оптимізації логістики та закупівель відділу постачання. Він допомагає підприємству ухвалювати раціональні рішення, знижувати витрати і водночас підвищувати ефективність роботи. В сучасних умовах глобалізації компанії, які активно вивчають і використовують можливості міжнародних ринків, отримують конкурентні переваги та краще адаптуються до змін у світовій економіці [4].

Крім того, систематичний аналіз дає змогу передбачати ризики, пов'язані з валютними коливаннями, політичними чи енергетичними кризами, а також забезпечує більшу стійкість підприємства до зовнішніх викликів. Оптимізація закупівель і логістики на міжнародних ринках сприяє не лише економії коштів, але й підвищенню якості продукції та послуг, що в кінцевому підсумку зміцнює позиції компанії на конкурентному ринку.

Таким чином, відділ постачання перетворюється на стратегічний підрозділ, що визначає не тільки внутрішню ефективність виробництва, але й перспективи розвитку підприємства в майбутньому. Чим глибший і комплексніший аналіз міжнародних ринків проводить компанія, тим більшими є її шанси на успішну інтеграцію в глобальну економіку та довгострокове зростання.

Список використаних джерел:

1. Kovalchuk A., Kenny C., Snyder M. Examining the Impact of E-Procurement in Ukraine. *Center for Global Development Working Paper*. URL: https://www.cgdev.org/sites/default/files/examining-impact-e-procurement-ukraine.pdf?utm_source=chatgpt.com (дата звернення: 23.09.2025).
2. Baranovsky A., Tkachenko N. Non-Price Criteria for the Evaluation of the Tender Offers in Public Procurement of Ukraine. *International Journal of Financial Studies*. URL: https://www.mdpi.com/2227-7072/8/3/44?utm_source=chatgpt.com (дата звернення: 23.09.2025).
3. Marketing strategy as an effective tool for government procurement management in Ukraine and the world. URL: https://www.zbw.eu/econis-archiv/bitstream/11159/654498/1/1895473624_0.pdf?utm_source=chatgpt.com (дата звернення: 23.09.2025).
4. Хеджування маркетингових ризиків у системі управління державними закупівлями в Україні. <https://salo.li/94534e3> (дата звернення: 23.09.2025).

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ В ОБЛІКУ ЦИФРОВИХ АКТИВІВ

Сучасна цифрова економіка переживає період глибоких трансформацій, які визначаються зростанням значення інформаційних технологій, віртуалізацією фінансових потоків та формуванням нових форм вартості. У цьому контексті цифрові активи, що охоплюють криптовалюти, токени, невзаємозамінні токени (NFT), а також інші форми віртуалізованих прав власності, стають невід'ємною частиною економічних процесів. Зі збільшенням їх обсягів та поширення у світовій фінансовій системі постає потреба в ефективних механізмах їхнього обліку, контролю та забезпечення прозорості [1, с. 205]. Саме блокчейн як децентралізована технологія розподіленого реєстру розглядається як ключовий інструмент для вирішення цих завдань.

Фундаментальна цінність блокчейну в обліку цифрових активів полягає в його здатності забезпечувати незмінність, прозорість і доступність даних. На відміну від традиційних централізованих систем бухгалтерського обліку, де достовірність інформації залежить від конкретного посередника чи адміністратора, блокчейн базується на принципі децентралізації. Це означає, що всі учасники мережі мають однаковий доступ до записів, а будь-які зміни фіксуються у відкритому реєстрі, який неможливо підробити чи знищити без відома спільноти. Така властивість набуває особливого значення у сфері обліку цифрових активів, де ризики шахрайства, подвійних витрат чи маніпуляцій є високими.

Облік цифрових активів в умовах традиційних фінансових стандартів стикається з низкою труднощів. З одного боку, криптовалюти та токени не завжди мають чітку правову кваліфікацію, а їхня економічна природа може коливатися між категоріями товару, валюти чи фінансового інструменту. З іншого боку, характер обігу таких активів вимагає оперативності та точності у фіксації транзакцій, чого складно досягти засобами класичної бухгалтерії. Саме блокчейн пропонує нову парадигму, де сама технологія стає гарантом правильності облікових записів. Завдяки смартконтрактам - програмованим алгоритмам, що автоматично виконуються за заданих умов, - процеси обліку можуть бути максимально автоматизовані [2, с. 271]. Це дозволяє мінімізувати людський фактор, знизити ймовірність помилок і підвищити довіру між учасниками ринку.

Особливої уваги заслуговує аспект прозорості. У традиційних системах бухгалтерський облік часто залишається внутрішнім інструментом компанії, доступним лише для обмеженого кола осіб [3]. У випадку з блокчейном кожен користувач має можливість перевірити достовірність транзакції, простежити історію активу від моменту його створення до поточного власника, а також

впевнитися у відсутності дублювань чи підробок. Це створює новий рівень довіри не лише між окремими інвесторами, а й між компаніями, державними інституціями та регуляторами. Для ринку цифрових активів, який часто критикують за непрозорість і спекулятивний характер, це є особливо важливим.

Управлінський вимір блокчейну в обліку цифрових активів полягає також у можливості створення так званого «аудиту в режимі реального часу». Якщо традиційна перевірка фінансових операцій здійснюється із запізненням, вимагає обробки великої кількості документів та залучення зовнішніх аудиторів, то блокчейн дозволяє здійснювати моніторинг фінансових потоків безперервно. Це означає, що будь-які відхилення чи аномальні транзакції можуть бути зафіксовані миттєво, а їхня перевірка - автоматизована. У результаті підвищується не лише точність обліку, а й ефективність управлінських рішень.

Проте блокчейн в обліку цифрових активів не позбавлений викликів. Технологія, попри свою стійкість до підробок, не вирішує усіх проблем, пов'язаних із визнанням цифрових активів у правовому полі. Наприклад, у багатьох країнах відсутні чіткі стандарти бухгалтерського обліку для криптовалют, що призводить до неоднозначного трактування їхньої вартості. Крім того, значна волатильність цифрових активів створює додаткові труднощі у відображенні їхнього фінансового стану. Ще однією проблемою є енергетичні витрати, особливо у випадку з блокчейнами, що базуються на алгоритмі Proof-of-Work, де підтвердження транзакцій потребує значних обчислювальних ресурсів.

Важливим напрямом розвитку є інтеграція блокчейну в існуючі системи бухгалтерського обліку. Сьогодні формується нове покоління програмного забезпечення, яке дозволяє компаніям вести облік цифрових активів у відповідності до міжнародних стандартів фінансової звітності. Такі рішення комбінують зручність традиційних бухгалтерських платформ із надійністю та прозорістю блокчейну. Зокрема, компанії отримують можливість не лише фіксувати рух цифрових активів, а й формувати звітність для інвесторів та регуляторів у режимі максимальної відкритості.

Не менш перспективним напрямом застосування блокчейну є токенизація матеріальних активів, яка дозволяє перетворювати реальні об'єкти - нерухомість, твори мистецтва, корпоративні права - у цифрові токени, що підлягають обліку у розподіленому реєстрі. Це розширює сферу дії блокчейну з суто цифрових активів на традиційні форми власності, створюючи унікальну можливість поєднання реальної та цифрової економіки. У такому разі роль блокчейну в обліку стає ще вагомішою, адже він виступає гарантом відповідності між токеном і базовим активом, що мінімізує ризики подвійного обліку чи шахрайських схем.

Досвід світових корпорацій і фінансових інституцій демонструє, що блокчейн поступово інтегрується в їхні бізнес-моделі. Провідні банки використовують його для розрахунків у міжнародних транзакціях, великі аудиторські компанії експериментують із впровадженням технології для перевірки фінансових звітів, а державні органи вивчають потенціал блокчейну для податкового контролю та державного обліку. У кожному з цих випадків

блокчейн доводить свою здатність змінювати правила гри, роблячи фінансову систему більш прозорою, доступною та справедливою [4, с. 99].

Підсумовуючи, слід зазначити, що роль блокчейну в обліку цифрових активів є багатовимірною. Він виступає не лише технічним інструментом фіксації транзакцій, а й новим концептуальним підходом до ведення бухгалтерського обліку, де довіра забезпечується не інституційним посередником, а математичними алгоритмами. Водночас перспективи широкого впровадження блокчейну залежать від узгодження правових норм, адаптації міжнародних стандартів та подолання технічних обмежень. Проте вже сьогодні очевидно, що саме блокчейн стає фундаментом для формування сучасної системи обліку цифрових активів, яка здатна відповідати викликам глобалізованої економіки та інформаційного суспільства.

Таким чином, блокчейн доцільно розглядати як технологію, що забезпечує поєднання прозорості, достовірності та інноваційності в обліку цифрових активів. Його впровадження не лише змінює бухгалтерську практику, а й формує нові принципи функціонування фінансової системи у цифрову добу. У найближчі роки блокчейн може стати тим інструментом, що поєднає потреби бізнесу, інвесторів і державних органів у єдиному середовищі, де облік цифрових активів відбувається з максимальною точністю та довірою.

Список використаних джерел:

1. Семанюк В., Мельник Н. Вплив цифрових технологій на інформаційне середовище бізнесу в умовах п'ятої промислової революції. *Вісник економіки*. 2022. Вип. 3. С. 203–212. DOI: <https://doi.org/10.35774/visnyk2022.03.203>.
2. Юрченко О.А., Савченко Р.В. Роль і місце блокчейн-технологій для ведення бухгалтерського обліку та складання фінансової звітності. *Економічний простір*. 2025. №198. С.269-274. DOI: <https://doi.org/10.30838/EP.198.269-274>.
3. Скрипник С. В., Сливка Я. В., Музиченко Т. О. Блокчейн-технології в бухгалтерії: нові підходи до забезпечення прозорості та надійності фінансової звітності. *Економіка та суспільство*. 2024. №66. DOI: <https://doi.org/10.32782/2524-0072/2024-66-34>.
4. Нашкерська Г. В. Технологія блокчейн у бухгалтерському обліку: переваги та обмеження. *Фінанси України*. 2023. №3. С.88-102.

Веприцький А.В.

*здобувач першого (бакалаврського) рівня вищої освіти
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна;*

науковий керівник:

Філатова Л. Д.

к. ф-м. н., доцент

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

СИСТЕМИ БІЗНЕС-АНАЛІТИКИ ТА МАШИННЕ НАВЧАННЯ: СУЧАСНІ РІШЕННЯ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ

Управлінські рішення дедалі більше залежать від даних: від щоденних операційних завдань до стратегічного планування. Поєднання ВІ-платформ (сховища даних, інтерактивні панелі, звітність) із ML-модулями (прогнозування, класифікація, оптимізація) перетворює «історичні» дані на цінні інсайти. Це дозволяє формувати рекомендації для прийняття рішень у режимі, наближеному до реального часу.

Типова архітектура таких систем складається з кількох взаємопов'язаних рівнів [2]:

1. Джерела даних. Це можуть бути корпоративні бази даних, інтернет речей (Internet of Things, IoT), системи управління взаємовідносинами з клієнтами (Customer Relationship Management, CRM), системи планування ресурсів підприємства (Enterprise Resource Planning, ERP), а також навчальні онлайн-платформи. Наприклад, у виробництві – це дані з датчиків обладнання, у бізнесі – дані про транзакції та поведінку клієнтів, в освіті – електронні журнали та системи дистанційного навчання.

2. Платформа обробки даних. Сюди входять процеси завантаження, перетворення та очищення даних (Extract-Transform-Load, ETL), а також обробка потоків у реальному часі (stream processing). Надійна система ETL дозволяє уникнути дублювання, пропусків чи помилок у даних, що безпосередньо впливає на точність прогнозів.

3. Сховище даних або озеро даних. Data Warehouse орієнтоване на збереження структурованих даних, тоді як Data Lake дозволяє працювати із напівструктурованими, і з неструктурованими даними (тексти, зображення, сенсорні сигнали). Саме тут формується «єдина версія правди», що забезпечує узгодженість усіх бізнес-процесів.

4. ML-шар. Це середовище для розробки моделей у Python чи R, використання платформ автоматизованого машинного навчання (Automated Machine Learning, AutoML) та інструментів управління життєвим циклом моделей (MLOps). MLOps дає можливість не лише створювати модель, а й відстежувати її якість, оновлювати та масштабувати у виробничих умовах.

5. Візуалізація та інтерфейси. Аналітичні панелі (dashboards), автоматичні сповіщення (alerts), а також інтерфейси на основі обробки природної мови

(Natural Language Processing, NLP) роблять результати зрозумілими для керівників. Це особливо важливо, оскільки не всі користувачі мають технічну підготовку для роботи з моделями.

Прикладні сценарії застосування:

Виробництво: прогнозування відмов обладнання (predictive maintenance), оптимізація запасів, адаптивне планування виробничих процесів [3].

Бізнес: сегментація клієнтів, прогноз попиту, виявлення аномалій у фінансових операціях, динамічне ціноутворення [2].

Освіта: прогноз успішності студентів, персоналізація навчальних траєкторій, аналітика для адміністративних рішень [2].

Основними перевагами інтеграції BI та ML у системи підтримки прийняття рішень (Decision Support Systems, DSS) є:

Прогностичність. Компанії можуть не лише аналізувати минуле, а й передбачати можливі сценарії розвитку. Це переводить організацію з «реактивного» режиму у «проактивний» [1].

Швидкість. Автоматичні алгоритми скорочують час між появою проблеми й ухваленням рішення, що особливо важливо в кризових умовах.

Якість рішень. Алгоритми машинного навчання здатні виявляти складні нелінійні закономірності, які не видно при класичному аналізі. Це зменшує ризик помилок та підвищує точність прогнозів.

Масштабованість. Використання AutoML і хмарних обчислень (Cloud Computing) робить передові технології доступними навіть для невеликих підприємств [2].

Разом із перевагами існують і певні труднощі:

Якість даних. Неповні або некоректні дані можуть призвести до хибних прогнозів і значних фінансових втрат.

Інтерпретованість моделей. Багато методів, зокрема глибинне навчання (Deep Learning), дають хороші результати, але є «чорними скриньками». Для керівників та регуляторів важливо розуміти логіку рішень.

Організаційні бар'єри. Недостатня культура роботи з даними або слабка взаємодія між IT-відділом і бізнес-підрозділами гальмують ефективне впровадження.

Етичні питання. Використання персональних даних створює ризики для приватності, а упередженість алгоритмів може призводити до несправедливих рішень [3].

ВИСНОВКИ. Системи бізнес-аналітики у поєднанні з машинним навчанням стають ключовим інструментом для підтримки управлінських рішень. Їх ефективність залежить не лише від технологій, а й від належної організації роботи з даними, інтерпретованості результатів та розвитку компетенцій персоналу.

Список використаних джерел:

1. Davenport T., Harris J. *Competing on Analytics: The New Science of Winning*. Harvard Business School Press, 2007.

2. Jiménez-Partearroyo M. et al. *Leveraging Business Intelligence Systems for Enhanced Decision Making*. Systems, 2024.

3. Soori M. et al. *AI-Based Decision Support Systems in Industry 4.0: A Review*. 2024.

УДК 330.42

Вигоднер І.В.

*старший викладач кафедри інформатики та комп'ютерних наук
Херсонський національний технічний університет*

Полозова С.Є.

*здобувач вищої освіти,
Херсонський національний технічний університет*

РОЗВ'ЯЗУВАННЯ ОПТИМІЗАЦІЙНИХ ЗАДАЧ ЗА ДОПОМОГОЮ ТАБЛИЧНОГО ПРОЦЕСОРУ EXCEL

Дисципліна “Економіко – математичні методи та моделі” дає можливість студентам економічних спеціальностей набути навички вирішення задач, які потребують знаходження оптимального розв'язку. При розв'язанні таких задач доцільно використовувати можливості сучасного програмного забезпечення, зокрема, табличного процесору EXCEL.

Приклад. Для виготовлення трьох виробів A , B і C використовується три види сировини. Витрати сировини, необхідні для виробництва виробів A , B і C , а також забезпечення сировиною виробів кожного виду, прибуток від реалізації виробів наведені в таблиці:

Таблиця 1

Вид сировини	Витрати сировини на одиницю виробу (в кг)			Загальна кількість сировини
	A	B	C	
I	18	15	12	360
II	6	4	8	192
III	5	3	3	180
Прибуток від реалізації одиниці виробу	9	10	10	

Скласти план виробництва продукції A , B і C , який забезпечив би максимальний прибуток від реалізації. Розв'язати задачу симплексним методом.

Розв'язання. Побудуємо математичну модель ЗЛП. Спочатку введемо змінні задачі.

Припустимо, що x_1 – кількість виробів A , x_2 – кількість виробів B , x_3 – кількість виробів C . Тоді математичну модель запишемо у вигляді:

$$Z = f(X) = 9x_1 + 10x_2 + 16x_3 \Rightarrow \max,$$

$$\begin{cases} 18x_1 + 15x_2 + 12x_3 \leq 360, \\ 6x_1 + 4x_2 + 8x_3 \leq 192, \\ 5x_1 + 3x_2 + 3x_3 \leq 180, \\ x_j \geq 0, \quad j = \overline{1,3}. \end{cases}$$

при обмеженнях

Складемо екранну форму для введення даних в EXCEL таблицю:

	A	B	C	D	E	F	G	H	I	J	K	L
1	Змінні											
2		x1	x2	x3								
3	Значення											
4	Нижня границя	0	0	0								
5												
6	Цільова функція											
7		9	10	16								
8												
9												
10	Система обмежень											
11	Обмеження 1	18	15	12	0 <=	360						
12	Обмеження 2	6	4	8	0 <=	192						
13	Обмеження 3	5	3	3	0 <=	180						

$$\begin{cases} Z = f(X) = 9x_1 + 10x_2 + 16x_3 \Rightarrow \max, \\ 18x_1 + 15x_2 + 12x_3 \leq 360, \\ 6x_1 + 4x_2 + 8x_3 \leq 192, \\ 5x_1 + 3x_2 + 3x_3 \leq 180, \\ x_j \geq 0, \quad j = \overline{1,3}. \end{cases}$$

Рис.1

Оскільки цільова функція та обмеження є лінійними виразами, то використаємо формулу **SUMPRODUCT**.

	A	B	C	D	E	F	G	H	I
1	Змінні								
2		x1	x2	x3					
3	Значення								
4	Нижня границя	0	0	0					
5									
6	Цільова функція				=SUMPRODUCT(B3:D3;B7:D7)				
7		9	10	16	SUMPRODUCT(масив1; [масив2]; [масив3]; [масив4]; ...)				
10	Система обмежень								
11	Обмеження 1	18	15	12	=SUMPRODUCT(B3:D3;B11:D11)				
12	Обмеження 2	6	4	8	=SUMPRODUCT(B3:D3;B12:D12)				
13	Обмеження 3	5	3	3	=SUMPRODUCT(B3:D3;B13:D13)				

Рис.2

Для розв'язання цього завдання в Excel слід скористатися надбудовою **Пошук розв'язання**. Обмеження в нерівностях та обмеження значень змінних виставляємо у вікні:

Параметри розв'язувача

Оптимізувати цільову функцію:

До: ☒ Максимум ☐ Мінімум ☐ Значення:

Змінюючі клітинки змінних:

Підлягає обмеженням:

\$B\$3 >= \$B\$4
 \$C\$3 >= \$C\$4
 \$D\$3 >= \$D\$4
 \$E\$11 <= \$G\$11
 \$E\$12 <= \$G\$12
 \$E\$13 <= \$G\$13

☒ Зробити необмежені змінні не від'ємними

Вибір метод розв'язання:

Метод розв'язання
 Для розв'язання гладких нелінійних задач виберіть розв'язувач нелінійних задач за методом зведеного градієнта. Для розв'язання лінійних завдань виберіть розв'язувач за симплекс-методом, для негладких завдань виберіть розв'язувач розв'язувач.

Додати
 Змінити
 Видалити
 Скинути
 Завантажити/зберегти

Параметри

Довідка Розв'язати Закрити

Рис.3

При необхідності можливо задати виведення на екран значень проміжних ітерацій. Тоді Для отримання наступної ітерації натискаємо команду **Продовжити**.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1		Змінні												
2		x1	x2	x3										
3	Значення	0	0	24										
4	Нижня границя	0	0	0										
5														
6		Цільова функція			384									
7		9	10	16										
8														
9														
10		Система обмежень												
11	Обмеження 1	18	15	12	288	<=	360							
12	Обмеження 2	6	4	8	192	<=	192							
13	Обмеження 3	5	3	3	72	<=	180							
14														
15														
16														

Показати пробне розв'язання

Пошук розв'язання призупинено. Поточні значення відображено на аркуші.

Продовжити Зупинити Зберегти сценарій...

Рис.4

Після натискання ОК отримаємо розв'язок, що є оптимальним:

	A	B	C	D	E	F	G
1	Змінні						
2		x1	x2	x3			
3	Значення	0	8	20			
4	Нижня границя	0	0	0			
5							
6	Цільова функція				400		
7		9	10	16			
8							
9							
10	Система обмежень						
11	Обмеження 1	18	15	12	360	<=	360
12	Обмеження 2	6	4	8	192	<=	192
13	Обмеження 3	5	3	3	84	<=	180

Рис.5

Для нашої задачі оптимальний розв'язок має вигляд: $x_1 = 0$, $x_2 = 8$, $x_3 = 20$, значення цільової функції 400.

Список використаних джерел:

1. Григорків В.С. Оптимізаційні методи та моделі : підручник / В.С. Григорків, М.В. Григорків, О.І. Ярошенко. – Чернівці : Чернівецький нац. ун-т, 2022. – 440 с.
2. Кветний Р.Н. Комп'ютерне моделювання систем та процесів. Методи обчислень. Ч 2 : Навчальний посібник/ Р.Н. Кветний. – Вінниця: ВНТУ, 2013. 235 с.

УДК 330.341.1:334.722:338.12

Власов І.В.

здобувач вищої освіти,

Вінницький національний аграрний університет

Томашук І.В.

PhD, доцент, доцент кафедри економіки та підприємницької діяльності

Вінницький національний аграрний університет

ІННОВАЦІЇ У РОЗВИТКУ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ ЯК ФАКТОР ЕКОНОМІЧНОГО ЗРОСТАННЯ

Інновації відіграють ключову роль у розвитку малого та середнього бізнесу як важливого фактора економічного зростання. Вони забезпечують підвищення продуктивності, оптимізацію витрат і впровадження нових продуктів та послуг, що зміцнює конкурентоспроможність підприємств на внутрішньому й зовнішньому ринках.

Інновації – це нововведення у вигляді ідей, продуктів, технологій, методів або процесів, які забезпечують якісні зміни, спрямовані на підвищення ефективності, конкурентоспроможності та стійкості розвитку підприємства чи суспільства загалом.

Для малого та середнього бізнесу інноваційність є особливо значущою, адже дозволяє швидко адаптуватися до змін ринкових умов, ефективно використовувати обмежені ресурси та відкривати нові ніші [1]. На макрорівні це сприяє створенню доданої вартості, зростанню зайнятості, активізації інвестиційних процесів і формуванню стійкої економічної динаміки. Таким чином, інновації виступають не лише інструментом розвитку МСП, а й каталізатором економічної модернізації та довгострокового зростання країни [2].

Вплив інновацій на розвиток малого та середнього бізнесу проявляється у створенні нових можливостей для зростання, підвищенні конкурентоспроможності та зміцненні позицій на ринку. Завдяки впровадженню інноваційних технологій, цифрових рішень, нових методів організації виробництва і збуту підприємства можуть ефективніше використовувати ресурси, знижувати витрати та підвищувати якість продукції й послуг [3]. Інновації відкривають доступ до нових ринків і сегментів, стимулюють розвиток партнерств і кооперації, сприяють інтеграції у глобальні ланцюги доданої вартості. Водночас вони посилюють гнучкість і здатність бізнесу швидко адаптуватися до економічних, технологічних та соціальних змін, що є особливо важливим в умовах нестабільності та високої конкуренції [4].

Табл. 1 узагальнює основні види інновацій, які застосовуються у малому та середньому аграрному бізнесі, зокрема технологічні, організаційні, маркетингові та соціальні. Вони охоплюють упровадження сучасних агротехнологій, цифровізацію процесів, нові форми кооперації та управління, розширення ринків збуту, а також підвищення екологічної та соціальної відповідальності. Сукупність таких інновацій забезпечує зростання ефективності виробництва, зміцнення конкурентоспроможності та сталий розвиток аграрного підприємництва.

Таблиця 1

Види інновацій у малому та середньому аграрному бізнесі

Вид інновацій	Приклади застосування в аграрній галузі	Очікуваний ефект
<i>Технологічні</i>	Використання точного землеробства (GPS-навігація, дрони), автоматизовані системи поливу, біотехнології	Підвищення врожайності, зниження витрат ресурсів, екологічність
<i>Продуктові</i>	Виробництво органічної продукції, нові сорти культур, фермерські еко-продукти	Розширення ринків збуту, задоволення попиту на якісні продукти
<i>Процесні (управлінські)</i>	Впровадження ERP-систем, цифрових платформ управління фермою, електронний документообіг	Оптимізація бізнес-процесів, підвищення прозорості та ефективності

Маркетингові	Використання e-commerce, просування через соцмережі, брендування фермерської продукції	Розширення каналів продажу, підвищення впізнаваності продукції
Організаційні	Кооперативні моделі господарювання, аграрні кластери, партнерські мережі	Зниження витрат, доступ до інновацій і ринків, підвищення стійкості
Соціальні	Розвиток агротуризму, створення соціальних підприємств у селі	Підвищення зайнятості та добробуту населення, розвиток громад
Екологічні («зелені»)	Впровадження відновлюваних джерел енергії (біогазові установки, сонячні панелі), утилізація відходів	Зменшення екологічного навантаження, економія енергоресурсів

Джерело: сформовано за результатами дослідження

Інновації у розвитку малого та середнього бізнесу виступають ключовим чинником економічного зростання, оскільки сприяють підвищенню продуктивності, конкурентоспроможності та гнучкості підприємств. Вони дозволяють ефективно використовувати ресурси, відкривати нові ринки, впроваджувати сучасні технології та адаптуватися до змін зовнішнього середовища. Завдяки цьому МСБ стає драйвером сталого розвитку економіки, формує нові робочі місця та підвищує якість життя населення.

Список використаних джерел:

1. Галаз Л. В., Лесик В. Й., Ковтун І. І., Битяк В. Ю., Козак А. М. Стратегії інноваційного зростання для малого та середнього бізнесу. *Інвестиції: практика та досвід*. 2024. № 22. С. 136-142. DOI: 10.32702/2306-6814.2024.22.136
2. Стрельбіцька Н. Є., Редько Т. В. Мале та середнє підприємництво як фактор соціально-економічного зростання ЄС. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*. 2016. Вип. 7. Ч. 3. С. 118-122. URL: http://www.visnyk-econom.uzhnu.uz.ua/archive/7_3_2016ua/32.pdf
3. Tomashuk I.V., Tomashuk I.O. Enterprise development strategy: innovation and internal flexibility. *Colloquium-journal*. 2021. № 3 (90). Vol. 4. P. 51-66. DOI: 10.24412/2520-2480-2021-390-50-64
4. Гончарук І.В., Томашук І.В. Вплив інноваційних процесів на підвищення конкурентоспроможності сільськогосподарських підприємств. *Економіка, фінанси, менеджмент: актуальні питання науки і практики*. 2023. № 1. (63). С. 30-47. DOI: 10.37128/2411-4413-2023-1-3

ПЕРЕВАГИ ІНФОРМАЦІЙНИХ СИСТЕМ В КОНТЕКСТІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА

Цифрова трансформація суспільства є одним із важливих процесів сучасності, що зумовлює переосмислення економічних, соціальних та культурних відносин у глобальному масштабі. Її основою є широке впровадження інформаційних систем та електронних ресурсів, що забезпечують збір, зберігання, обробку та передавання даних, створюють нові можливості для комунікації та взаємодії між людьми, інституціями та державами. Поступовий перехід від традиційних форм організації діяльності до цифрових моделей визначає нову якість суспільних процесів, де інформація стає стратегічним ресурсом, а вміння ефективно її використовувати – передумовою розвитку та конкурентоспроможності [4, с. 111].

Застосування інформаційних систем дедалі більше охоплює ключові сфери функціонування суспільства. У сфері державного управління вони стають основою для впровадження електронних послуг, функціонування цифрових реєстрів та електронного документообігу, що підвищує прозорість управлінських процесів, зменшує рівень бюрократії та забезпечує доступність адміністративних сервісів для громадян. У бізнесі поширення корпоративних інформаційних систем дозволяє автоматизувати виробничі процеси, оптимізувати управління ресурсами, здійснювати аналітику великих масивів даних та забезпечувати прийняття рішень на основі отриманої інформації. Освітня сфера також зазнала значних змін завдяки появі цифрових освітніх платформ, що створюють умови для дистанційного та змішаного навчання, формування електронних бібліотек і баз знань, реалізації персоналізованого навчання тощо. Важливим напрямом стало впровадження електронної медицини, що реалізується через дистанційні консультації, ведення електронних карт пацієнтів та ін.

Розширення сфери застосування інформаційних систем формує не лише економічні та управлінські переваги, а й соціокультурні наслідки. Використання цифрових технологій змінює стиль повсякденного життя громадян, створює нові можливості для професійної діяльності та освіти, сприяє формуванню культури відкритості й прозорості в суспільстві. Використання інформаційних систем у процесах цифрової трансформації створює підґрунтя для активного розвитку електронної демократії. Доступ громадян до онлайн ресурсів органів влади, можливість брати участь у публічних обговореннях чи електронних петиціях формують нові моделі взаємодії держави й суспільства, що підвищує рівень довіри до управлінських структур, сприяє прозорості ухвалення рішень та залученню громадян до процесу вироблення державної політики [3, с. 108].

Попри очевидні переваги інформаційних систем та онлайн сервісів не слід забувати і про потенційні ризики. Зокрема, йдеться про ризики, пов'язані з цифровою нерівністю, зростання рівня кіберзлочинності, необхідність захисту персональних даних, брак достатньо підготовлених фахівців в ІТ-сфері. Такі процеси потребують посиленої уваги до питань кібербезпеки, розвитку цифрової грамотності та забезпечення інклюзивності доступу до сучасних інформаційних рішень. Ефективність цифрової трансформації залежить не лише від технічного рівня впроваджених систем, але й від готовності суспільства адаптуватися до нових умов, виробляти навички безпечної та відповідальної поведінки в цифровому середовищі. Для України це має особливе значення, адже інтеграція у європейський цифровий простір вимагає не лише технічної модернізації, але й формування єдиних стандартів у сфері захисту даних та управління інформаційними ресурсами [1, с. 16].

Подальший розвиток інформаційних систем безпосередньо пов'язаний із впровадженням новітніх технологій, таких як штучний інтелект, хмарні обчислення, блокчейн та аналіз великих даних. Зазначені інновації відкривають нові можливості для вдосконалення бізнес-моделей, удосконалення державних сервісів та розвитку суспільства знань. В умовах глобалізації важливим питанням є міжнародна взаємодія у сфері цифрових технологій, адже ефективне використання інформаційних систем вимагає уніфікації стандартів, спільної роботи над забезпеченням безпеки та розширенням доступу до сучасних цифрових платформ. Для України, яка перебуває в процесі активної цифрової трансформації, стратегічним завданням є формування безпечної та стійкої цифрової інфраструктури, що відповідатиме європейським та міжнародним стандартам [2, с. 334]. Такий підхід передбачає не лише модернізацію технічних компонентів інформаційних систем, таких як сервери, мережеве обладнання та програмне забезпечення, а й розвиток нормативно-правової бази, яка регламентує безпечне зберігання та обробку даних, захист персональної інформації та дотримання принципів кібергігієни.

Отже, використання інформаційних систем у процесах цифрової трансформації суспільства виступає не лише технічним чинником, але й соціально-економічною умовою розвитку. Вони створюють фундамент для модернізації управління, підвищують конкурентоспроможність бізнесу, сприяють розвитку інноваційної освіти та забезпечують якісно новий рівень соціальних послуг. Разом із тим ефективність цього процесу можлива лише за умови врахування викликів, пов'язаних із безпекою, доступністю та підготовкою людських ресурсів. Цифрова трансформація суспільства має стати комплексним процесом, що поєднує технологічний прогрес із розвитком цифрової культури, правових і етичних норм використання інформації.

Список використаних джерел:

1. Бондаренко Т. Інтелектуальні інформаційні технології як складник цифрової трансформації освіти (аналітичний огляд). *Аналітичний вісник у сфері освіти й науки*. 2024. № 19. С. 3–23.

2. Серденко Т.В., Рейс Т.Г. Персоналізація навчання за допомогою інформаційних систем. *Вісник Херсонського національного технічного університету*. 2025. № 2.2(93). С. 333–338.

3. Тесля Ю.М., Заспа Г.О. Розробка концентричної інформаційної технології цифрової трансформації закладів вищої освіти. *Управління розвитком складних систем*. 2020. № 44. С. 105–115.

4. Шаров С. В. Сучасний стан розвитку інтелектуальних інформаційних систем. *Вісник Чернігівського національного педагогічного університету. Серія: Педагогічні науки*. 2015. № 130. С. 111–114.

УДК 336.7:338.28

Глушко Р. О.

*здобувач першого (бакалаврського) рівня вищої освіти
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна;
науковий керівник:*

Філатова Л. Д.

*к. ф-м. н., доцент
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна*

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА РОЗВИТОК ФІНАНСОВИХ ТЕХНОЛОГІЙ

Останнім часом використання цифрових технологій та можливість аналізувати великі масиви даних сприяє створенню нових банківських продуктів. Ринок банківських послуг стрімко поповнюється сучасними технологіями, а штучний інтелект (AI) стає одним із ключових елементів цифрової трансформації економіки. Його застосування надає банкам конкурентні переваги, адже дозволяє пропонувати інноваційні сервісні рішення, які легко інтегруються в єдину систему.

Технології з використанням AI дедалі помітніше впливають на наше повсякденне життя, і фінансовий сектор – один із найяскравіших прикладів такого впливу. Щоб залишатися «в грі», сучасні банки повинні йти в ногу з часом. Повна інтеграція таких технологій дозволить клієнтам проводити фінансові операції в онлайн та офлайн режимах без особливих труднощів, користуючись при цьому інтуїтивно зрозумілими сервісами. Штучний інтелект є інструментом, що забезпечує набагато зрозуміліший процес взаємодії людини з програмами. Інтелектуальні системи все частіше сприяють розвитку промисловості, охоплюючи дедалі більше сфер, в тому числі і фінансову.

Розвиток AI відбувається завдяки доступу до великих обсягів даних для навчання і, як результат, зростають можливості систем для складних обчислень. Наразі штучний інтелект є ключовим аспектом для банківської галузі, що

поступово розширює можливості передових технологій. Переваги AI для фінансового сектору мають такі аспекти:

- висока швидкість та якість обслуговування клієнтів;
- низькі витрати на вирішення проблем;
- висока якість обробки значних обсягів даних;
- мінімальна ймовірність експлуатаційних витрат і ризиків;

Завдяки таким технологіям, споживачі отримують індивідуальні рекомендації від служби підтримки у реальному часі, які допомагають ефективніше керувати власними фінансами.

Штучний інтелект найчастіше використовують для:

- автоматизації підтримки клієнтів;
- збір та аналіз даних для проведення досліджень ринку;
- систем, які розпізнають шахрайські транзакції;

Крім того, за допомогою AI різні фінансові організації створюють чат-боти, які можуть консультувати споживачів та відповідати на прості питання. Боти розробляють таким чином, щоб формулювати відповіді та рекомендації на основі переваг та інтересах клієнтів.

Спершу фінтех може здатися чимось складним та незрозумілим, однак у наш час це вже повсякденність. Інвестиції на фондовому ринку, оформлення кредиту онлайн, оплата комунальних послуг, переказ грошей за кордон – це приклади фінансових технологій, якими ми успішно користуємося щодня. Фінансові технології (або фінтех) – це також і цифрові інновації у фінансовому секторі. Стрімкий розвиток мобільних і інтернет-технологій забезпечили його ефективний розвиток.

Штучний інтелект у фінтех-рішеннях проявив себе не лише теоретично, а й практично. Організації узгоджують свій стратегію щодо впровадження AI у фінансову індустрію. Найпомітніший приклад такого впровадження AI – це сфера клієнтського досвіду, де чат-боти, такі як Erica від Bank of America, підняли планку рівня взаємодії з клієнтами в банківському середовищі на новий рівень. Ці системи на базі штучного інтелекту надають користувачам проактивні сповіщення, інформацію про баланс рахунку та підтримку з фінансових запитів, імітуючи розмови, подібні до людських, та зменшуючи потребу в людському втручанні з боку агентів служби підтримки клієнтів.

Штучний інтелект також значно просунувся в кредитному андеррайтингу – процесі оцінки ризику прийняття на страхування особи. Завдяки моделям машинного навчання, з'явилася можливість систем проводити кредитний скоринг – процес, який допомагає визначити клієнтів, здатних повернути кредит, а також виявляти потенційних шахраїв. Ці рішення дозволяють обробляти та аналізувати величезні обсяги даних для оцінки кредитоспроможності, при цьому збільшується швидкість та точність процесу схвалення позики. Впровадження ШІ у фінтех значною мірою змінює її. Технології на основі інтелектуальних систем дозволяють учасникам фінансового ринку досягати справжніх технологічних проривів, при цьому:

- підвищується рівень безпеки;
- фінансові послуги персоналізуються під кожного користувача;

- зростає ефективність, прибутковість та адаптивність бізнесів;

Не дивлячись на всю технологічність, інтеграція AI у фінтех не обходиться і без недоліків:

- велика ймовірність кібератак;
- інтелектуальні системи можуть приймати несправедливі або необ'єктивні рішення при кредитуванні клієнтів або наймі працівників;
- високі складнощі розгортання AI систем;
- дефіцит спеціалістів з розробки та управління штучним інтелектом;
- організаціям необхідна чітка стратегія та правильні партнери, яким можна довіряти;

ВИСНОВКИ. На сьогоднішній день, у фінансовому секторі відбувається жорстка конкуренція і впровадження штучного інтелекту може допомогти банкам масштабувати фінансові системи, тим самим залучаючи більше нових клієнтів і стаючи більш конкурентоспроможним. Нині ця технологія активно розвивається, інтегруючи все більше нових інструментів. Це актуально, оскільки кількість фінансових транзакцій зростає чи не щодня. Тому штучний інтелект стає пріоритетом для фінансового сектора майбутнього.

Список використаних джерел

1. Штучний інтелект у Фінтеху (Фінансова сфера). [Електронний ресурс] Режим доступу: <https://pnn.com.ua/ua/blog/detail/artificial-intelligence-in-fintech-finance-sphere>
2. Штучний інтелект у фінтех-сфері 2025: як штучний інтелект революціонізує розробку фінтех-додатків та програмного забезпечення. [Електронний ресурс] Режим доступу: <https://www.techverdi.com/uk/blog/ai-in-fintech-app-and-software-development/>
3. AI in Fintech: Use Cases and Benefits. [Електронний ресурс] Режим доступу: <https://aisera.com/blog/ai-in-fintech/#:~:text=AI%20in%20fintech%20is%20used,compliance%20monitoring%20and%20transaction%20analysis.>

**Гончарук Д.О.,
Заїченко Ю.П.,**

здобувачі вищої освіти

ННІ «Комп'ютерних наук та штучного інтелекту» ХНУ імені В.Н. Каразіна

Науковий керівник

Новіков А.О.

викладач, доктор філософії

ННІ «Комп'ютерних наук та штучного інтелекту» ХНУ імені В.Н. Каразіна

ОСВІТНІ ПЛАТФОРМИ ТА ЗАСТОСУНКИ НОВОГО ПОКОЛІННЯ

У сучасних умовах цифровізації освіти освітні платформи та застосунки нового покоління стають ключовим елементом формування інноваційного навчального середовища. Вони дозволяють подолати обмеження традиційних методів навчання, забезпечують гнучкість і доступність знань, а також підвищують мотивацію студентів за рахунок інтерактивності [1]. Серед прикладів можна назвати глобальні системи Coursera, EdX, Udemy, український Prometheus, мобільні додатки на кшталт Duolingo, а також спеціалізовані інструменти управління навчанням Moodle чи Canvas.

Окрему групу серед освітніх застосунків складають платформи для роботи з особистими знаннями та нотатками, які стають дедалі популярнішими в академічному середовищі [2]. Зокрема, Notion та Obsidian вважаються яскравими прикладами освітніх застосунків нового покоління. Notion поєднує функції блокнота, бази даних та менеджера проєктів, дозволяючи студентам і викладачам організовувати інформацію у вигляді сторінок, таблиць і інтерактивних панелей [3]. Дослідження показують, що використання Notion у навчальному процесі сприяє підвищенню продуктивності студентів, адже воно допомагає керувати розкладом, створювати списки завдань і впорядковувати конспекти більш ефективно [5]. Його гнучкість робить його ефективним для створення індивідуальних освітніх планів та спільної роботи над проєктами [3].

Obsidian, у свою чергу, базується на концепції зшивання знань (knowledge graph): кожна нотатка зберігається локально і може бути пов'язана з іншими через систему гіперпосилань [4]. Це формує у користувача власну «базу знань», що є особливо актуальною для дослідників, які працюють з великими обсягами інформації [2]. Практичне застосування Obsidian у вищій освіті демонструє, що студенти розробляють індивідуальні стратегії сортування та пов'язування інформації, що дозволяє підвищувати ефективність навчання і навіть створювати нові форми персоналізованих цифрових освітніх середовищ [6].

Такі застосунки виходять за межі класичного «онлайн-курсу» і створюють умови для персонального навчання (personal knowledge management) [2]. Вони дозволяють студентам інтегрувати лекційні матеріали, наукові статті, завдання та власні ідеї у єдину екосистему знань. Викладачі ж отримують можливість створювати спільні освітні простори для групової роботи, що поєднують елементи традиційних LMS із сучасними інструментами колаборації.

Застосування Notion та Obsidian у навчальному процесі демонструє тренд на поєднання формального та неформального навчання [5, 6]. Якщо Coursera чи Moodle орієнтовані на курси й модулі, то note-taking застосунки забезпечують середовище для постійного накопичення та осмислення знань, яке не обмежується часовими чи структурними рамками. Вони створюють основу для lifelong learning і дозволяють студентам формувати унікальні освітні траєкторії [1, 2].

Водночас широке впровадження освітніх платформ і застосунків нового покоління супроводжується низкою проблем. Серед них – нерівність цифрового доступу, складність інтеграції різних систем між собою, ризики комерціалізації освіти, а також необхідність формування у студентів нових навичок самоорганізації [1]. Проте перспективи розвитку очевидні: майбутнє освіти формується на перетині адаптивних платформ, мобільних додатків, систем управління знаннями та технологій віртуальної/доповненої реальності.

Таким чином, Notion і Obsidian поряд із глобальними освітніми платформами є прикладом переходу до нового рівня цифрової освіти, де головними цінностями стають персоналізація, інтерактивність та інтеграція знань. Їхня роль у майбутньому лише зростатиме, оскільки вони відповідають потребам як окремих студентів, так і цілих академічних спільнот [2, 5, 6].

Список використаних джерел:

1. Сіменс Г. Конективізм: теорія навчання для цифрової доби // International Journal of Instructional Technology and Distance Learning. – 2005. – Т. 2, № 1. – С. 3–10.
2. Ахренс С. Як робити розумні нотатки: проста техніка для розвитку письма, навчання і мислення. – North Charleston: CreateSpace, 2017. – 192 с.
3. Notion Labs Inc. Notion for Education. – URL: <https://www.notion.so/for-education>
4. Obsidian.md. Obsidian for Knowledge Management. – URL: <https://obsidian.md>
5. Troncoso D. J. 16 Alternatif Notion Terbaik di 2023 (Gratis & Berbayar). MarketSplash, 2023. – URL: <https://marketsplash.com/id/alternatif-notion/>
6. Ferreira J. J., Segura V., Souza J. G., Brasil J. H. G. How People Manage Knowledge in their “Second Brains” – A Case Study with Industry Researchers Using Obsidian. – 2025.

ЦИФРОВА ТРАНСФОРМАЦІЯ ОСВІТИ КРІЗЬ ПРИЗМУ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація: У статті розглядається трансформаційний потенціал штучного інтелекту (ШІ) в сучасній освітній системі. Аналізуються ключові переваги технології: персоналізація навчання, автоматизація рутинних завдань, підвищення інклюзивності та глобальної доступності знань. Особлива увага приділяється архітектурі освітніх систем на основі ШІ, практичним прикладам впровадження та поетапному процесу створення освітніх платформ. У висновку представлено збалансований погляд на виклики та ризики, пов'язані з інтеграцією ШІ, та визначено його вектор розвитку як інструменту-помічника для педагога.

Вступ: Ера інтелектуальної освіти

Штучний інтелект перестав бути футуристичною концепцією і перетворився на потужний інструмент модернізації однієї з найконсервативніших сфер — освіти. Як зазначається на міжнародних майданчиках, таких як конференція AIED (Artificial Intelligence in Education), ШІ є одним з найбільш перспективних напрямків. Його суть полягає в синтезі комп'ютерних наук, педагогіки та психології, що дозволяє створювати адаптивні, персоналізовані та надзвичайно ефективні освітні середовища. Незважаючи на величезний потенціал, інтеграція ШІ в педагогічну практику пов'язана з необхідністю вирішення складних методологічних та етичних проблем.

Ключові переваги ШІ в освіті

Впровадження технологій штучного інтелекту відкриває ряд унікальних можливостей для переосмислення традиційного навчального процесу.

— Глибока персоналізація. ШІ-системи здатні аналізувати індивідуальну динаміку навчання кожного студента: швидкість засвоєння матеріалу, бажані формати сприйняття інформації, типові помилки. На основі цих даних формуються персональні освітні траєкторії та навчальні плани, що максимально відповідають потребам і можливостям учня.

— Автоматизація та ефективність. Значна частина рутинного навантаження викладача — перевірка стандартизованих тестів, домашніх завдань, складання звітності — може бути передана ШІ. Це вивільняє цінний час педагога для творчої роботи, наставництва та розвитку у студентів навичок, таких як критичне мислення та креативність.

— Підвищення інклюзивності. ШІ-технології стирають бар'єри для учнів з обмеженими можливостями здоров'я. Системи автоматичного розпізнавання мови та генерації субтитрів роблять контент доступним для

людей з вадами слуху, а адаптивні інтерфейси допомагають людям з порушеннями зору. Навчання стає доступним для тих, хто за станом здоров'я не може відвідувати заняття очно.

- Глибока аналітика і зворотний зв'язок. За допомогою комп'ютерного зору і аналізу даних ШІ може відстежувати не тільки результати навчання, але і емоційний стан учнів під час заняття. Це дозволяє системі вчасно виявити труднощі в розумінні матеріалу та адаптувати подачу контенту для кращого засвоєння.

- Глобалізація та доступність. Машинний переклад (Google Translate) та багатомовні платформи руйнують мовні бар'єри, дозволяючи студентам з усього світу отримувати доступ до найкращих освітніх ресурсів.

Архітектура освітніх систем на основі ШІ (AIED)

Ефективна освітня система на базі ШІ базується на чотирьох ключових компонентах:

1. Модель знань: Містить структуровану інформацію про предметну область і забезпечує інтелектуальну основу для вирішення навчальних завдань.

2. Модель учня: Ядро персоналізації. Цей компонент безперервно відстежує та аналізує прогрес, знання та прогалини кожного учня, формуючи його цифровий профіль.

3. Педагогічна модель: «Мозок» системи, який приймає рішення про те, як, коли і який навчальний матеріал подати учневі, ґрунтуючись на даних з моделі учня.

4. Інтерфейс взаємодії: Забезпечує комунікацію між системою та користувачем. Сьогодні це не тільки веб-інтерфейси, але й голосові помічники, які роблять взаємодію інтуїтивною та природною.

Приклади успішного впровадження та майбутні тенденції

Світовий ринок пропонує безліч успішних кейсів інтеграції ШІ в освіту:

- Third Space Learning: Платформа аналізує стиль викладання в реальному часі, даючи педагогу рекомендації щодо оптимізації темпу і ясності пояснень.

- Carnegie Learning & CTI: Розробляють адаптивні платформи для всіх рівнів освіти. Сервіс Cram101 використовує ШІ для аналізу підручників і автоматичного створення конспектів, тестів і карток для запам'ятовування.

- Little Dragon: Створює рішення, що аналізують емоції та навчання учня через камеру, адаптуючи інтерфейс для підвищення комфорту.

- Голосові помічники в університетах: Наприклад, Арізонський державний університет використовує Amazon Alexa для орієнтації нових студентів і відповідей на поширені запитання, що скорочує витрати на друковані матеріали та персонал.

- Майбутні тренди вказують на зростання застосування: Доповненої (AR) та віртуальної (VR) реальності для створення імерсивних освітніх середовищ.

- ШІ-наставників — цифрових асистентів, які супроводжують учня 24/7.

- Гейміфікації для підвищення мотивації та залученості.

Ризики та виклики на шляху цифрової трансформації

Незважаючи на оптимізм, впровадження ШІ пов'язане з серйозними ризиками, які вимагають уважного регулювання:

- Загроза дегуманізації. Головний ризик — заміна живої, мотивуючої взаємодії «вчитель-учень» на знеособлений машинний інтерфейс. Це може негативно позначитися на розвитку соціальних навичок та емоційного інтелекту студентів.

- Проблеми конфіденційності. Для своєї роботи ШІ-системи вимагають колосальних обсягів персональних даних учнів, що створює ризики витоків та несанкціонованого використання інформації.

- Висока вартість. Розробка, впровадження та підтримка ШІ-рішень вимагають значних інвестицій, що може поглибити цифровий розрив між багатими та бідними освітніми закладами.

- Опір персоналу. Викладачі сприймають ШІ як загрозу своїм робочим місцям, що створює організаційні бар'єри для впровадження.

- Технічна вразливість. Системи стають критично важливою інфраструктурою. Їх відмова в результаті збоїв або кібератак може паралізувати навчальний процес і призвести до безповоротної втрати даних.

Висновок: ШІ як партнер, а не заміна

Штучний інтелект — не панацея, а потужний інструмент, покликаний не замінити педагога, а стати його надійним партнером. Він бере на себе рутину, аналіз даних і тиражовані завдання, дозволяючи вчителю сконцентруватися на тому, що машини поки не вміють: на вихованні, творчому натхненні та розвитку людського потенціалу. Повний ефект від його впровадження стане очевидним лише з часом. Однак уже зараз ясно, що майбутнє освіти лежить на шляху розумної, етичної та виваженої інтеграції технологій, де людина залишається в центрі освітнього всесвіту.

Список використаних джерел

1. Bustamante Bula, R., & Camacho Bonilla, A. (2024). Inteligencia artificial (IA) en las escuelas: Una revisión sistemática (2019-2023). *Enunciación*, 29(1), 62–82. <https://doi.org/10.14483/22486798.22039>
2. Ibarra Martínez, R. L., Caro Morales, J. L., & Pérez González, M. N. (2023). Inteligencia artificial en la educación. *Revista Digital de Tecnologías Informáticas y Sistemas*, 7(1), 100–106. <https://doi.org/10.61530/redtis.vol7.n1.2023.136.100-106>
3. Pokrivcakova, S. (2019). Preparing teachers for the application of AI-powered technologies in foreign language education. *Journal of Language and Cultural Education*, 7(3), 135–153. <https://doi.org/10.2478/jolace-2019-0025>
4. Stower, R., Calvo-Barajas, N., Castellano, G., & Kappas, A. (2021). A Meta-analysis on Children's Trust in Social Robots. *International Journal of Social Robotics*, 13(8), 1979–2001. <https://doi.org/10.1007/s12369-020-00736-8>

Гуржій К. А.
здобувач вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Науковий керівник
Ковальчук Д.М.
PhD, старший викладач кафедри інформаційних технологій
та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПРОГРАМНИХ ЗАСОБІВ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ ВЕБ-ЗАСТОСУНКІВ

Автоматизація процесів тестування веб-застосунків на сучасному етапі розвитку інформаційних технологій є однією з ключових складових забезпечення їх якості, надійності та безпеки. Веб-застосунки активно інтегруються у повсякденне життя суспільства, обслуговують критичні бізнес-процеси та стають основою для функціонування цілих галузей. У таких умовах постає потреба у створенні програмних засобів, що дозволяють мінімізувати людський фактор, пришвидшити процес перевірки коректності роботи системи та забезпечити повторюваність тестових сценаріїв. Саме автоматизоване тестування стає фундаментальним підходом у процесах забезпечення якості програмного забезпечення [1].

Дослідження у цій сфері показують, що використання лише ручного тестування має ряд суттєвих недоліків. По-перше, це висока трудомісткість процесу, особливо для великих проєктів, де кількість функціональних модулів та сценаріїв значно перевищує можливості тестувальників. По-друге, ручне тестування схильне до помилок через втому або неуважність людини. По-третє, у випадках, коли потрібно багаторазово повторювати однакові дії, ручна перевірка стає економічно невигідною. Натомість автоматизовані засоби дозволяють один раз створити набір тестових сценаріїв і надалі використовувати їх без значних витрат часу та ресурсів.

Розробка програмних засобів автоматизованого тестування веб-застосунків передбачає врахування низки вимог. Серед них важливими є кросбраузерність, можливість тестування у різних операційних системах та середовищах, підтримка інтеграції з системами керування версіями та системами безперервної інтеграції, а також зручність у створенні та модифікації тестових сценаріїв. Крім того, сучасні підходи орієнтовані на забезпечення масштабованості та можливість проведення навантажувальних тестів.

Існує значна кількість інструментів, які використовуються у практиці автоматизованого тестування веб-застосунків. До найбільш відомих належать Selenium, Cypress, Playwright, Puppeteer, TestCafe, JUnit, NUnit та інші. Вибір конкретного засобу залежить від особливостей проєкту, мови програмування, яку використовують розробники, та вимог до середовища виконання. Наприклад, Selenium завдяки своїй відкритій архітектурі та підтримці багатьох

мов програмування (Java, Python, C#, JavaScript) залишається найпоширенішим інструментом. Cypress та Playwright забезпечують швидке виконання тестів і тісну інтеграцію з сучасними фреймворками JavaScript, що робить їх популярними серед розробників фронтенду. TestCafe дозволяє легко організовувати тестування без необхідності встановлення додаткових драйверів [1-2].

Особливу увагу варто звернути на архітектуру програмних засобів автоматизації. Найбільш поширеним підходом є використання шаблону Page Object Model (POM), який дозволяє відокремити логіку тестів від опису елементів інтерфейсу. Це забезпечує високу гнучкість, зручність у підтримці та масштабованість тестових наборів. Інший підхід — Behavior Driven Development (BDD), який базується на використанні опису поведінки системи зрозумілою мовою (наприклад, Gherkin) і дозволяє налагодити комунікацію між тестувальниками, розробниками та бізнес-аналітиками. Поєднання цих підходів створює умови для ефективного управління тестами у складних програмних проектах.

Автоматизоване тестування веб-застосунків може охоплювати різні рівні перевірок. Найнижчим рівнем є модульне тестування, що перевіряє роботу окремих функцій чи класів. Далі йде інтеграційне тестування, яке досліджує взаємодію компонентів між собою. Наступним рівнем є системне тестування, що охоплює увесь застосунок цілком. Окремо слід виділити регресійне тестування, яке є особливо зручним для автоматизації, оскільки дозволяє швидко перевіряти, чи не вплинули нові зміни у коді на вже існуючий функціонал. Важливим є також навантажувальне тестування, яке допомагає оцінити стійкість та продуктивність системи під час значної кількості одночасних запитів.

Розробка власних програмних засобів для автоматизації тестування часто зумовлена необхідністю врахування специфічних вимог певного проекту, які не можуть бути реалізовані за допомогою готових рішень. При цьому можна виділити кілька ключових етапів створення такого інструменту:

- 1) аналіз вимог до тестування та визначення цілей автоматизації;
- 2) вибір мови програмування та архітектурного підходу;
- 3) реалізація модулів для взаємодії з браузером, введення даних та перевірки результатів;
- 4) інтеграція із системами контролю версій та безперервної інтеграції;
- 5) тестування самого інструменту та його вдосконалення.

На практиці ефективність автоматизованого тестування значною мірою залежить від грамотної стратегії впровадження. Занадто велика кількість автоматизованих сценаріїв може призвести до складності у підтримці, тоді як надмірна орієнтація на ручне тестування знижує ефективність розробки. Тому важливо визначати баланс між автоматизацією та ручними перевітками. Зазвичай автоматизуються ті тести, які виконуються часто, вимагають багаторазового повторення або є критично важливими для працездатності системи.

Серед сучасних тенденцій у цій сфері слід відзначити інтеграцію автоматизованого тестування із концепцією DevOps. Безперервна інтеграція (CI) та безперервне розгортання (CD) передбачають, що кожна зміна у коді автоматично запускає набір тестів, і лише у разі успішного їх проходження застосунок може бути розгорнутий на сервері. Це суттєво підвищує якість кінцевого продукту та скорочує час виходу нових версій. Важливою тенденцією є також застосування штучного інтелекту та машинного навчання у процесі тестування. Такі системи можуть автоматично генерувати нові сценарії, прогнозувати можливі помилки та оптимізувати процес перевірки.

Окремої уваги заслуговує проблема підтримки автоматизованих тестів у динамічних веб-застосунках. Сучасні інтерфейси, побудовані на основі фреймворків Angular, React або Vue.js, часто мають динамічну структуру, що ускладнює ідентифікацію елементів. Це вимагає від інструментів автоматизації гнучкості та здатності працювати зі змінами у DOM-структурі. Крім того, варто враховувати, що різні браузері можуть по-різному інтерпретувати одні й ті самі елементи, що ще більше підвищує складність завдання.

З огляду на економічні та організаційні аспекти, автоматизація тестування є вигідною у середньо- та довгостроковій перспективі. Хоча початкові витрати на впровадження інструментів, навчання персоналу та створення сценаріїв можуть бути високими, у подальшому це дозволяє суттєво скоротити час виходу продукту на ринок і зменшити ризик критичних помилок. Таким чином, автоматизоване тестування слід розглядати як інвестицію у якість та конкурентоспроможність продукту.

Проведене дослідження показує, що розробка програмних засобів автоматизованого тестування веб-застосунків є складним, але надзвичайно перспективним напрямом. У майбутньому очікується ще більша інтеграція таких засобів із системами штучного інтелекту, що дозволить автоматично виявляти дефекти та генерувати тестові сценарії на основі аналізу користувацької поведінки. Крім того, розвиток хмарних технологій створює умови для організації масштабованих систем тестування, де можна одночасно перевіряти застосунок у сотнях різних конфігурацій браузерів та операційних систем. Загалом автоматизоване тестування веб-застосунків виступає необхідною умовою створення якісних програмних продуктів. Воно дозволяє досягти високої точності перевірок, підвищити ефективність команд розробників, знизити витрати на підтримку та забезпечити стабільність функціонування застосунку у різних середовищах.

Список використаних джерел:

1. Якість програмного забезпечення та тестування: базовий курс: навч. посіб. / за ред. С. Я. Крепич, І. Я. Співак. – Тернопіль : ФОП Паляниця В. А., 2020. – 478 с.
2. Трофименко О. Г., Дика А. І. Тестування та забезпечення якості програмних систем : навч.-метод. посіб. [Електронне вид.] / Нац. ун-т «Одеська юридична академія». – Одеса : Фенікс, 2024. – 140 с. – URL: <https://hdl.handle.net/11300/27246>. – ISBN 978-617-8395-32-2.

Денисенко Г.В.,

здобувач освіти

*Харківський національний університет ім. В.Н.Каразіна,**ННІ «Каразінський банківський інститут»***Стяглик Н.І.,***к.п.н., доцент, завідувачка кафедри інформаційних технологій та**математичного моделювання**Харківський національний університет ім. В.Н.Каразіна,**ННІ «Каразінський банківський інститут»*

ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Штучний інтелект (ШІ) стає однією з ключових технологій ХХІ століття. Від автоматизації бізнес-процесів до створення автономних транспортних систем – ШІ трансформує сучасне суспільство. Актуальність цієї теми зумовлена зростаючим впливом технологій на повсякденне життя, економіку та наукові дослідження.

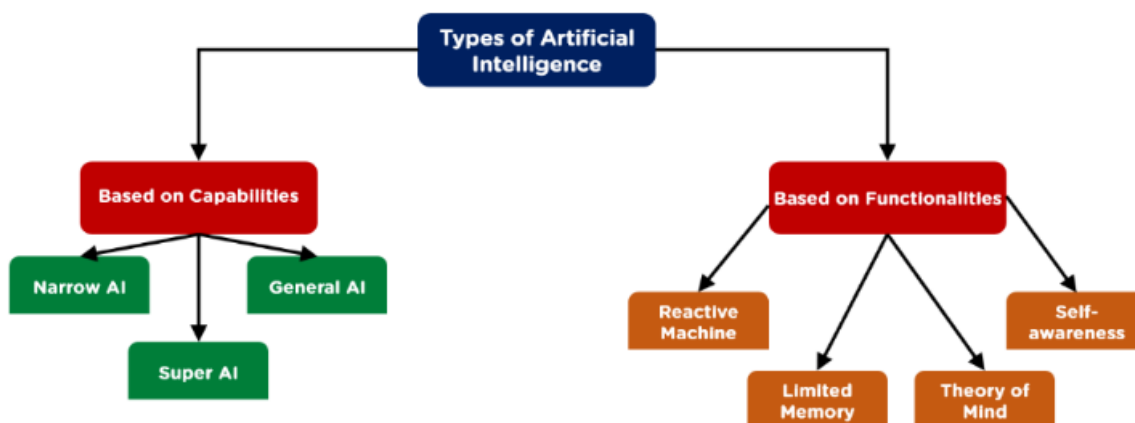


Рисунок 1. Види штучного інтелекту у сучасній класифікації

Теоретичні засади. Штучний інтелект – це галузь комп’ютерних наук, яка розробляє системи, здатні виконувати завдання, що зазвичай потребують людського інтелекту: розпізнавання образів, обробка природної мови, прогнозування, ухвалення рішень. Основні напрямки ШІ включають машинне навчання, нейронні мережі, глибинне навчання та обробку природної мови (NLP).

Чому питання використання штучного інтелекту є актуальним? Попит на фахівців зі ШІ зростає у всьому світі. Згідно з дослідженнями, до 2030 року ШІ здатен створити мільйони нових робочих місць, водночас автоматизуючи рутинні процеси. Технології ШІ застосовуються у медицині для діагностики, у фінансах для управління ризиками, в автомобільній промисловості для створення автономних транспортних систем, у маркетингу та кібербезпеці.

Таблиця 1.

Динаміка попиту на спеціалістів зі ШІ у світі

Рік	Попит на фахівців зі ШІ (тис.)	Примітки
2023	450	Світовий ринок праці
2025	600	Прогноз зростання
2030	1000	Очікуване впровадження ШІ у всіх сферах

Доцільність дослідження штучного інтелекту зумовлена його потенціалом кардинально трансформувати суспільство та забезпечити вирішення складних завдань, які є малоефективними або неможливими для людини без застосування сучасних технологій. Дослідження у цій сфері інтегрують програмування, математичні методи, статистичний аналіз та креативний підхід до розв'язання проблем, що робить штучний інтелект міждисциплінарним напрямом із високою науковою та практичною цінністю.

Технології штучного інтелекту активно інтегруються у різні галузі:

- у медицині – для підтримки діагностики, персоналізованої медицини та аналізу великих обсягів даних;
- у фінансах – для управління ризиками, автоматизації операцій та виявлення шахрайських транзакцій;
- в автомобільній промисловості – для створення автономних транспортних систем;
- у маркетингу – для персоналізованої реклами та аналізу поведінки споживачів;
- у сфері кібербезпеки – для прогнозування та запобігання кібератакам;
- в освіті – для адаптивних навчальних систем і віртуальних асистентів;
- виробництво – для автоматизації виробничих процесів та управління робототехнікою.

Таким чином, розвиток штучного інтелекту має стратегічне значення не лише для технологічного прогресу, а й для соціально-економічного розвитку суспільства. Вибір цього напрямку як професійної діяльності є перспективним завдяки високому попиту на фахівців, широким можливостям практичного застосування знань та залученню до створення інноваційних рішень. Штучний інтелект відкриває доступ до роботи у різних сферах та формує умови для активного впливу на глобальний технологічний розвиток.

Список використаних джерел

1. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach. Pearson.
2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
3. IBM. (2023). What is Artificial Intelligence (AI)? URL: <https://www.ibm.com/topics/artificial-intelligence>

ФІЛОСОФІЯ ОСВІТИ І НАУКИ В УМОВАХ ЦИФРОВІЗАЦІЇ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

На сучасному етапі розвитку суспільства цифровізація виступає ключовим чинником трансформацій, що охоплюють економіку, соціальні відносини та саму природу знання. В умовах глобальних змін і модернізації української освітньо-наукової сфери, інтегрованої у європейський та світовий контекст, ця проблема набуває особливої уваги. Саме освіта й наука, як фундаментальні основи суспільного поступу, опиняються у фокусі технологічних інновацій.

Отже, використання програмних засобів для освітнього процесу та наукових досліджень ставить перед філософією освіти і науки нові завдання: осмислення природи цифрових технологій, їхнього впливу на мислення, комунікацію та структуру знання.

На думку М. Кастельса, інформаційне суспільство формується навколо інформаційних мереж, які стають «новою морфологією соціального буття» [1]. Таким чином, цей підхід дозволяє розглядати освіту і науку як інститути, що не просто використовують інформаційні системи, а й трансформуються під їхнім впливом. Слід підкреслити, що виклики пов'язані не лише з технічною ефективністю цифрових рішень, а й з ціннісними аспектами їхнього застосування.

Відбувається переосмислення ролі викладача і науковця. Якщо традиційно викладач виступав носієм та ретранслятором знання, то в умовах цифрових платформ і систем штучного інтелекту він стає модератором освітнього середовища, навігатором у світі надлишкової інформації. Невипадково Ю. Габермас зазначав, що знання не може існувати поза комунікативною взаємодією, що визначає його значущість [2]. Тому завдання викладача сьогодні полягає не лише у передаванні знань, а й у формуванні критичного мислення, уміння працювати з даними та відповідально приймати рішення.

Цифровізація науки зумовлює нову онтологію наукового знання. Можна стверджувати, що великі масиви даних, інтелектуальні алгоритми та автоматизовані системи обробки інформації змінюють саму структуру наукового пошуку. У науковий обіг входить феномен так званої «філософії даних», коли не теорія передуює емпірії, а навпаки - емпіричний масив даних формує нові гіпотези. Варто зазначити, що це потребує критичного аналізу меж і можливостей такого підходу, адже дані не говорять самі за себе - вони завжди інтерпретуються у певному світоглядному та ціннісному контексті.

Особливої уваги набуває проблема етики. Справді, використання програмних засобів для прийняття рішень в освіті та науці створює ризики втрати автономії людини, знеособлення комунікації та підміни педагогічних і наукових смислів технологічними процедурами. Як підкреслював М. Гайдеггер, «сутність техніки не є чимось технічним» [3]. Тобто справжня загроза полягає не в самих інструментах, а в тому, що людина починає мислити і діяти за логікою техніки, втрачаючи гуманістичні орієнтири.

У цьому контексті філософія освіти і науки має виконати дві ключові функції: критично-рефлексивну (осмислення онтологічних і гносеологічних змін у структурі знання під впливом цифрових технологій) та ціннісно-нормативну (визначення етичних і культурних засад використання інформаційних систем у сфері освіти та науки).

Таким чином, цифровізація відкриває широкі можливості для розвитку освіти і науки, проте водночас висуває виклики, які неможливо розв'язати лише технічними засобами. Відтак, потрібна філософська рефлексія, яка здатна забезпечити баланс між інноваціями та гуманістичними цінностями. Майбутнє освіти й науки залежить від того, наскільки вдасться інтегрувати технологічний прогрес у контекст людського розвитку, свободи й відповідальності.

Список використаних джерел:

1. Кастельс М. Інформаційне суспільство та держава добробуту. Фінська модель [Текст]: пер. з англ. / М. Кастельс, П. Хіманен. К.: Ваклер, 2006. 230 с. ISBN 966-543-087-4
2. Хабермас Юрген. Комунікативна дія і дискурс. *Першоджерела комунікативної філософії*. К.: Либідь. 1996. С. 84–91.
3. Heidegger M. Die Frage nach der Technik // Vorträge und Aufsätze. Pfullingen: Neske, 1954. URL: <https://philpapers.org/rec/HEIVUA-5>

УДК 004.4

Захарова М.Д.

здобувач вищої освіти,

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

Науковий керівник

Стяглик Н.І.

к.п.н., доцент, завідувач кафедри інформаційних технологій та

математичного моделювання

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

SOFTWARE4LIFE: ВИРОБНИЦТВО, НАВЧАННЯ, АНАЛІТИКА

Сучасний етап розвитку інформаційного суспільства характеризується стрімким впровадженням програмних засобів у різні сфери діяльності людини. Виробництво, освіта, бізнес-аналітика, інтелектуальне опрацювання даних та

системи підтримки прийняття рішень дедалі більше залежать від ефективності використання програмних комплексів. Це пояснюється зростанням обсягів інформації, необхідністю швидкої обробки даних, а також потребою в автоматизації складних процесів. Метою даних тез є аналіз сучасних програмних засобів для вирішення прикладних задач у зазначених сферах, а також визначення їх ролі у цифровій трансформації суспільства.

Програмні засоби у виробництві

Програмні засоби, такі як MES (Manufacturing Execution Systems) та ERP (Enterprise Resource Planning), відіграють ключову роль у підвищенні ефективності та якості виробничих процесів. MES-системи забезпечують реальний моніторинг обладнання, автоматизацію збору даних та контроль виробництва. Наприклад, H&T Presspart впровадила Infor MES, що дозволило скоротити час простою і підвищити продуктивність.

ERP-системи інтегрують фінанси, постачання, виробництво та продажі, оптимізуючи планування ресурсів і управління запасами. DELMIAWorks поєднує функції MES і ERP, що дає підприємствам можливість отримувати дані у реальному часі, знижувати витрати та покращувати управлінські рішення.

Інтеграція MES та ERP дозволяє забезпечити безперервний потік інформації між цехом та адміністративними підрозділами, підвищуючи ефективність ресурсів, покращуючи планування та прогнозування. Ці програмні засоби дають змогу швидше приймати обґрунтовані рішення, зменшувати витрати та підвищувати якість продукції, що важливо для сучасних конкурентних ринків.

Програмні засоби в освіті

Спеціалізоване прикладне програмне забезпечення допомагає оптимізувати навчальний процес, підвищувати ефективність викладання та забезпечувати персоналізоване навчання. Такі програмні засоби застосовують у школах, університетах та дистанційних курсах. Основні типи включають системи управління навчанням для керування курсами та відстеження прогресу студентів, аналітичні освітні платформи для оцінки навчальних досягнень і інтерактивні програми та симулятори, що підвищують залученість учнів. Приклади: Moodle, Khan Academy, Coursera, Edmodo, Nearpod. Використання таких систем дозволяє скоротити час на адміністрування курсів, покращити навчальні результати та адаптувати освітній процес під потреби кожного учня.

Програмні засоби у бізнес-аналітиці

У сучасному бізнес-середовищі ефективне використання програмних засобів для аналізу даних є критичним для досягнення стратегічних переваг. Організації застосовують платформи бізнес-аналітики (Business Intelligence, BI), такі як Microsoft Power BI, Tableau, Qlik Sense, а також інструменти аналітики з елементами штучного інтелекту (ШІ), наприклад IBM Watson Analytics, Salesforce Einstein Analytics та Google Cloud AI Platform, для збору, візуалізації та прогнозування ключових показників ефективності (KPI).

Згідно з дослідженням MIT Sloan Management Review та Boston Consulting Group (2024), організації, які інтегрують ШІ у процес створення та вдосконалення KPI, демонструють значне покращення в кількох аспектах:

- Покращення співпраці: Організації, що використовують ШІ для створення нових KPI, відзначають 4-кратне збільшення співпраці між співробітниками.

- Прогнозування та ефективність: Такі організації в 3 рази ефективніше прогнозують майбутні результати та в 2 рази ефективніше досягають оперативної ефективності.

- Фінансові результати: Вони в 3 рази частіше досягають значних фінансових переваг порівняно з тими, хто не використовує ШІ для вдосконалення KPI.

Ці результати підкреслюють важливість інтеграції передових технологій у процеси бізнес-аналітики для досягнення конкурентних переваг.

Програмні засоби для інтелектуального оброблення даних

Інтелектуальне оброблення даних (Intelligent Data Processing, IDP) є ключовим елементом сучасних інформаційних систем, що дозволяє організаціям автоматизувати аналіз великих обсягів даних, покращувати прогнозування та прийняття рішень. Програмні засоби для інтелектуального оброблення даних включають платформи для машинного навчання, штучного інтелекту та обробки великих даних, такі як Python (з бібліотеками Pandas, Scikit-learn, TensorFlow), R, Apache Spark, KNIME, Alteryx, RapidMiner.

Згідно з дослідженням MIT Sloan Management Review та Boston Consulting Group (2024), організації, що впровадили інтелектуальні системи оброблення даних, показують такі результати:

- Покращення точності прогнозів: понад 70 % компаній, що використовують IDP, відзначили підвищення точності прогнозів бізнес-процесів.

- Прискорене прийняття рішень: 65 % компаній скоротили час ухвалення рішень на до 30 % завдяки автоматизації аналітики.

- Збільшення ефективності операцій: 60 % організацій повідомили про зниження витрат на аналітичні процеси та підвищення продуктивності персоналу.

Програмні засоби для інтелектуального оброблення даних використовуються в різних галузях: фінанси (для прогнозування ринку), виробництво (для передбачення поломок обладнання), охорона здоров'я (для аналізу медичних даних) та маркетинг (для аналізу поведінки клієнтів).

Програмні засоби для прийняття рішень

Програмні засоби для прийняття рішень (Decision Support Systems, DSS) допомагають організаціям приймати ефективні рішення, використовуючи аналітику даних, моделі прогнозування та експертні правила. Вони широко застосовуються у бізнесі, фінансах, виробництві, логістиці та управлінні ресурсами. Основні типи DSS включають модельно-орієнтовані системи, які оцінюють варіанти рішень за допомогою математичних та фінансових моделей; дані-орієнтовані системи, що аналізують великі обсяги даних та надають інтерактивні дашборди для виявлення тенденцій; знання-орієнтовані системи, що використовують експертні знання для рекомендацій та автоматизації рішень; а також групові DSS, які підтримують колективне прийняття рішень,

забезпечуючи спільний доступ до даних і інструментів для обговорення альтернатив.

Приклади програмних засобів DSS у бізнесі та фінансах:

- QlikView – аналітична платформа з інтерактивними дашбордами для бізнес-аналітики;
- SAP BusinessObjects – рішення для створення звітів, аналізу даних та прогнозування;
- Minitab – програма для статистичного аналізу та оптимізації процесів;
- Tableau – інструмент для візуалізації даних та інтерактивного аналізу;
- Oracle Crystal Ball – DSS для фінансового прогнозування та моделювання ризиків.

Програмні засоби DSS дозволяють підвищувати точність прогнозів, зменшувати витрати, оптимізувати виробничі та управлінські процеси, а також покращувати ефективність роботи компаній. Важливим аспектом є те, що ці системи застосовуються не лише в бізнесі, а й у сфері охорони здоров'я. Наприклад, системи клінічної підтримки рішень (CDSS) допомагають лікарям аналізувати електронні медичні записи та швидше приймати правильні діагностичні рішення. Стартап Hera-MI розробив Breast-SlimView, AI-програму для діагностики раку молочної залози, яка автоматично виділяє здорові ділянки тканин і дозволяє фахівцям концентруватися на складних випадках, що скорочує час діагностики та підвищує точність лікування.

Отже, програмні засоби є ключовим фактором розвитку виробництва, освіти, бізнесу та медицини. Вони забезпечують автоматизацію, аналітику й підтримку прийняття рішень, створюючи умови для підвищення конкурентоспроможності та ефективності організацій.

Список використаних джерел:

1.	DELMIAWorks.	URL:
	https://www.solidworks.com/story/delmiaworks/erp-success/	
2.	Infor.	URL:
	https://www.infor.com/customer-stories/driving-digital-transformation	
3.	Forbes.	URL:
	https://www.forbes.com/advisor/business/software/best-data-analytics-tools/	
4.	MIT Sloan Management Review.	URL:
	https://sloanreview.mit.edu/projects/the-future-of-strategic-measurement-enhancing-kpis-with-ai/	
5.	Boston Consulting Group.	URL:
	https://web-assets.bcg.com/c1/a7/af0e57dc4b47a31eb7409d981d3e/mitsmr-bcg-ai-report-november-2024.pdf	
6.	StartUs Insights.	URL:
	https://www.startus-insights.com/innovators-guide/decision-support-systems-startups	

Істомін А. О.
здобувач вищої освіти,
ННІ «Енергетичної, інформаційної та транспортної
інфраструктури» ХНУМГ ім. О.М. Бекетова
Науковий керівник
Пахомов Ю.В.
к.т.н., доцент, доцент кафедри комп'ютерних наук
та інформаційних технологій
ННІ «Енергетичної, інформаційної та транспортної
інфраструктури» ХНУМГ ім. О.М. Бекетова

ЦИФРОВІЗАЦІЯ БУДІВЕЛЬНИХ ПРОЦЕСІВ: РОЛЬ SAAS-РІШЕНЬ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ПРОЄКТАМИ

Сучасна будівельна галузь стикається з низкою викликів, пов'язаних із масштабованістю проєктів, складною координацією учасників та високими вимогами до термінів і якості. Традиційні методи управління дедалі частіше виявляються недостатніми для забезпечення прозорості процесів та ефективного використання ресурсів. У цьому контексті цифровізація стає ключовим чинником розвитку галузі, а SaaS-рішення (Software as a Service) відіграють провідну роль у підвищенні ефективності будівельних проєктів.

Цифровізація стала не просто модним трендом, а фактично життєвою необхідністю для компаній, які прагнуть залишатися конкурентоспроможними, постійно розвиватися та ефективно реагувати на зміни ринку. Особливо це стосується будівельної галузі, де швидкість прийняття рішень, точність планування та прозорість процесів відіграють ключову роль у досягненні успіху. В умовах сучасного ринку, який постійно трансформується під впливом нових технологій, підвищених вимог до якості та дедалі більшого акценту на екологічну відповідальність.

Серед сучасних підходів до управління будівельними проєктами особливе місце займають SaaS-рішення, які дозволяють об'єднувати управління завданнями, документацією, фінансами та комунікаціями в одній платформі. Такі сервіси значно спрощують взаємодію всіх учасників проєкту, дають можливість відстежувати виконання завдань у режимі реального часу, контролювати графіки робіт і ефективно розподіляти ресурси. Централізовані системи комунікацій допомагають уникати розривів у передачі інформації між командами, підрядниками та клієнтами, що часто трапляється при використанні традиційних методів управління. Всі повідомлення, документи та звіти зберігаються у хмарі, що забезпечує швидкий доступ до них у будь-який момент і гарантує збереження історії змін.

Одним із методів такого підходу є сервіс Procore, який широко використовується на міжнародному ринку та демонструє, як цифрові інструменти можуть підвищити ефективність управління будівельними проєктами.

Головним досягненням використання Procore є значна оптимізація фінансового обліку. Традиційні методи управління будівельними проектами часто пов'язані з великими витратами часу на ручне ведення документації, складання звітів і контроль бюджету. Procore дозволяє автоматизувати ці процеси, забезпечуючи точність та прозорість фінансових операцій. Крім того, сервіс допомагає зменшити ймовірність помилок і втрат, що часто трапляються при ручному введенні даних, та дозволяє оперативно реагувати на будь-які відхилення від запланованого бюджету.

Ще однією важливою перевагою сучасних SaaS-рішень, які використовуються для управління будівельними проектами, є їхня висока доступність та гнучкість. Такі платформи дозволяють працювати з будь-якого пристрою: – комп'ютера, планшета чи смартфона і з будь-якої точки світу, де є інтернет. Це особливо актуально для компаній, які реалізують великі проекти на кількох локаціях одночасно та потребують постійного моніторингу виконання робіт, контролю ресурсів та своєчасного реагування на будь-які відхилення. Завдяки цьому керівники та менеджери можуть отримувати актуальну інформацію в режимі реального часу, незалежно від того, де вони знаходяться, що суттєво підвищує оперативність прийняття рішень та дозволяє уникати непотрібних затримок у роботі.

Використання SaaS-рішень дозволяє компаніям значно економити ресурси, адже відпадає потреба у великих витратах на власні сервери, складну локальну інфраструктуру та постійне обслуговування технічних систем. Це не лише знижує фінансові витрати, а й робить процес управління більш ефективним і менш залежним від фізичної наявності обладнання. Дані, що зберігаються у хмарі, шифруються та регулярно резервуються, що гарантує їхню безпеку, захист від втрат і можливість швидко відновити інформацію у разі непередбачуваних ситуацій.

Основні переваги запропонованих методів представлені у таблиці 1.

Таблиця 1.

Порівняння традиційних методів управління та SaaS-рішень

Критерій	Традиційні методи управління	SaaS-рішення (Procore)
Доступність	Обмежена офісним ПК	Будь-який пристрій, онлайн
Комунікація	E-mail, телефон	Централізовані чати
Документообіг	Паперові документи, локальні файли	Хмарне зберігання, версії та історія змін
Фінансовий облік	Ручний або локальний софт	Інтеграція методів з бухгалтерією
Масштабування	Додаткове обладнання	Підписка або модулі
Безпека даних	Залежить від внутрішньої політики	Шифрування, резервне копіювання, багаторівнева автентифікація

Використання Procore також позитивно впливає на внутрішню організацію роботи компанії. Менеджери отримують змогу швидко реагувати на

будь-які зміни у графіках робіт, контролювати ефективність підрядників та вчасно виявляти проблемні ділянки. Співробітники компанії оцінюють зручність платформи через інтуїтивно зрозумілий інтерфейс та можливість централізованого доступу до всієї необхідної інформації. Крім того, використання SaaS-рішень підвищує прозорість усіх процесів, що позитивно впливає на взаємини з клієнтами та партнерами, оскільки всі дані можуть бути надані у зручному вигляді для сторонніх користувачів.

Таким чином, використання SaaS-рішень у будівельних проєктах забезпечує:

- централізований доступ до даних для всіх учасників процесу;
- підвищення прозорості комунікацій і контролю виконання завдань;
- зменшення ризиків, пов'язаних із дублюванням чи втратою даних;
- оптимізацію ресурсів і скорочення часу виконання робіт.

До найбільш поширених рішень належать Autodesk Construction Cloud, Procore, PlanRadar, які інтегрують управління документацією, плануванням і контролем будівельних процесів у єдиному середовищі.

SaaS-рішення виступають важливим інструментом цифровізації будівельної галузі, сприяючи підвищенню ефективності управління проєктами, зниженню витрат та підвищенню якості реалізації. Перспективним напрямом розвитку є інтеграція SaaS-платформ з технологіями BIM, IoT та штучного інтелекту, що дозволить створити інтелектуальні системи управління будівництвом та закласти основу для «розумних будмайданчиків».

Список використаних джерел

1. Procore Technologies. Procore Announces Fourth Quarter and Full Year 2023 Financial Results [Електронний ресурс]. – Режим доступу: <https://investors.procore.com/news/news-details/2024/Procore-Announces-Fourth-Quarter-and-Full-Year-2023-Financial-Results/default.aspx>
2. MarketsandMarkets. Building Information Modeling Market Size, Share & Trends [Електронний ресурс]. – Режим доступу: <https://www.marketsandmarkets.com/Market-Reports/building-information-modeling-market-95037387.html>
3. Business Research Insights. SaaS Project Management Market Size, Share [Електронний ресурс]. – Режим доступу: <https://www.businessresearchinsights.com/market-reports/saas-project-management-market-124009>

МІЖДИСЦИПЛІНАРНІ ЗВ'ЯЗКИ: ЯК ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІНТЕГРУЮТЬСЯ В НАВЧАЛЬНІ ДИСЦИПЛІНИ 1 КУРСУ

За останні декілька років в Україні стало поширеним онлайн навчання або змішане навчання. У цій роботі буде описана інтеграція інформаційних технологій в навчання та визначення плюсів і мінусів.

Зауважимо, що інтеграція ІТ в навчальний процес на більшості його етапах полягає в проведенні лекцій та практичних занять, ознайомленні з додатковими джерелами та підготовці матеріалів для занять (текстові документи, електронні книжки, презентації, відео, аудіо, симуляції тощо), а також оцінюванні робіт. Це сприяє вдосконаленню старих методів викладання та розвитку нових [1].

Зосередимо увагу на нашому прикладі міждисциплінарних зв'язків для освітньої програми “Банківська справа та фінансовий консалтинг”. Наведемо приклади взаємозв'язку дисциплін 1 семестру та тематичних завдань всередині курсу “Інформаційні технології” (Таблиця 1).

Таблиця 1.

Міждисциплінарні зв'язки дисциплін спеціальності D2 Фінанси, банківська справа, страхування та фондовий ринок

№	Дисципліна 1 семестру/ Приклад завдання	Завдання з дисципліни “Інформаційні технології”
1.	<i>Вступ до фаху</i>	Створення презентації про обрану спеціальність; Проходження онлайн-курсів з академічної доброчесності; Тестування на різноманітних освітніх платформах (Дія.Освіта, Гаразд); Відвідування віртуальної екскурсії “Гривня - наш символ” від Музею грошей НБУ
	Знайомство з програмами, які в майбутньому знадобляться для професії. Ознайомлення з правилами академічної доброчесності. Створення презентації про професію пов'язану зі спеціальністю. Відвідування конференції “Money & Banking: історія та майбутнє грошей” від НБУ.	
2	<i>Історія України: цивілізаційний вимір</i>	Персональна історія знайомства та використання інформаційних технологій
	Можливість ознайомлення з електронними версіями історичних джерел та статей. Підготовка доповідей та презентацій для семінарів.	Перегляд фільму “Перший код” у контексті історії обчислювальної техніки та ролі українських розробників. Складання списку українських і

		закордонних пісень та кліпів із комп'ютерною технікою.
3	<i>Іноземна мова за фахом</i>	Підготовка матеріалу для написання тез. Англomовний інтерфейс програм та застосунків (Zoom, Google Workspace), налаштування перекладу. Пошук та автоматизований переклад через Google Об'єкти. Професійна термінологія та варіанти перекладу.
4	<i>Банківська студія "Тайм-менеджмент та міжособистісні комунікації в бізнесі"</i>	Проходження тематичних онлайн-курсів на платформах Prometheus, Edera, пов'язаних зі спеціальністю. Створення командної презентації із цікавою інформацією про кожного студента Робота в команді над спільним завданням із розподілом ролей та командною звітністю, а також різними правами доступу.
5	<i>Мікроекономіка</i>	Побудова графіків, діаграм та аналіз даних при роботі з табличним редактором Microsoft Excel та Google Sheets
6	<i>Вища математика</i>	Інтегроване завдання з теми "Системи лінійних рівнянь та методи їх розв'язування" на відпрацювання навичок роботи з редактором формул

Джерело: сформовано за результатами дослідження авторами

Отже, інтеграція інформаційних технологій у дисципліни дає можливість покращити навчальний процес, знайти нові методи викладання, але супроводжується викликами сучасності. До позитивних сторін інтеграції можна віднести: упровадження більшої кількості інтерактивів у навчання; молодь частіше практикує ІТ навички (вдосконалює їх); мобільність. А ось серед негативних наслідків неоднорідність технічного забезпечення; відсутність навичок (не всі мають/не хочуть набувати відповідні навички); складно контролювати якість інформації; питання академічної доброчесності, зокрема проблема плагіату.

На жаль, повного вирішення цих проблем немає, але є декілька рекомендацій як можна спробувати покращити ситуацію:

- визначити та розказати студентам як працювати із незнайомими серверами [1]
- забезпечити базові ресурси (якщо навчання відбувається очно чи у змішаній формі) [2];
- інвестувати у професійний розвиток (для викладачів), та стимулювати студентів також покращувати навички [3];
- спонукати студентів до ознайомлення з правилами академічної доброчесності та їхнього дотримання [4].

Перспективними напрямками подальших досліджень є розширення переліку дисциплін в межах обраної освітньої програми за період навчання на першому (бакалаврському) рівні освіти, а також пошук нових ідей для завдань.

Список використаних джерел:

1. Giuffrida, I., & Hall, A. (2023). Technology integration in higher education and student privacy beyond learning environments-A comparison of the UK and US perspective. British Journal of Educational Technology, 54, 1587-1603. URL: <https://doi.org/10.1111/bjet.13375>
2. Msambwa M., Kangwa D., Cai L. Integration of information and communication technology in secondary education for better learning: A systematic literature review. URL: <https://doi.org/10.1016/j.ssaho.2024.101203>
3. Chesley A., Parupudi T., Holtan A., Farrington Sh., Eden C., Baniya S., Interdisciplinary Pedagogy, Integrated Curriculum, and Professional Development. URL: https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1014&context=aseeil-in-sectionconference&utm_source=chatgpt.com
4. Bittle K., El-Gayar O. Generative AI and Academic Integrity in Higher Education: A Systematic Review and Research Agenda. URL: https://www.mdpi.com/2078-2489/16/4/296?utm_source=chatgpt.com#

УДК 004.056.53

Ключніков О.С.

здобувач вищої освіти,

Харківський національний університет радіоелектроніки

Кобилін І.О.

к.т.н., асистент кафедри Інформатики,

Харківський національний університет радіоелектроніки

МЕТОДИ ВИКОРИСТАННЯ ТА ПРОТИДІЯ ШАХРАЙСЬКИМ ПРОГРАМАМ У КОМП'ЮТЕРНИХ ІГРАХ ТИПУ «ШУТЕР»

Сучасні підходи використання шахрайських програм в стрілецьких комп'ютерних іграх для здобування переваги над суперником включають перегляд крізь стіни (Wall Hack), автоприцілювання (AimBot) та універсальний радар (Radar Hack). Кожна з них має свій вплив на ігровий процес та порушення

чесності у рамках ігрового матчу. Наразі існує багато програм цих типів, кожна з яких має свої переваги та недоліки. Більшість з них є платними, що лише вказує на глобальну популяризацію використання даних програм.

Ця проблема є особливо актуальною для таких ігор, як Counter-Strike 2, PUBG: BATTLEGROUNDS, серія ігор BATTLEFIELD, де шахраї полегшують собі ігровий процес впливаючи на загальну ситуацію у ігрових матчах. Наприклад, гравці, що стикнулися у протистоянні не лише з суперником але й шахрайською програмою мають колосально низькі шанси на перемогу.

Основна перевага AimBot – легкість, що дозволяє лише за один клік викреслити фактор людини. Однак суттєвий недолік – механіка роботи, AimBot притягує приціл до певних пікселів, тому гравця, що використовує цю програму, легко визначити за прицілом, що смикається. AimBot має різні конфігурації спираючись на потреби гравця такі як:

1. Вхідні дані:

- позиція камери (гравця) $p = (p_x, p_y, p_z)$.
- позиція цілі в 3D (наприклад хітбокс) $t = (t_x, t_y, t_z)$.
- матриця вигляду V і матриця проєкції P (4×4). Розмір екрану $W \times H$.

2. Вектор напрямку (у світових координатах):

$$\Delta_x = t_x - p_x, \quad \Delta_y = t_y - p_y, \quad \Delta_z = t_z - p_z,$$

3. Перетворення в кути (yaw, pitch). Використовуємо звичну геометрію:

$$yaw = \text{atan2}(\Delta_y, \Delta_x) \quad pitch = \text{atan2}(\Delta_z, \sqrt{\Delta_x^2 + \Delta_y^2}).$$

4. 3D $\rightarrow$ 2D (псевдо-матрична проєкція).

- У гомогенних координатах:

$$t_h = [t_x, t_y, t_z, 1]^T, \quad c = PVt_h = [c_x, c_y, c_z, c_w]^T$$

- NDC (normalized device coordinates):

$$x_{ndc} = \frac{c_x}{c_w}, \quad y_{ndc} = \frac{c_y}{c_w}.$$

- Піксельні координати екрана:

$$x_{screen} = \frac{W}{2}(1 + x_{ndc}), \quad y_{screen} = \frac{H}{2}(1 - y_{ndc})$$

- Ці (x_{screen}, y_{screen}) — пікселі, куди приціл має спрямовуватись.

5. Інтерполяція / згладжування руху прицілу (щоб рух не був миттєвим):

- лінійний LERP:

$$\varphi_{new} = \varphi_{cur} + s \cdot (\varphi_{des} - \varphi_{cur}), \quad 0 \leq s \leq 1$$

- Експоненційне згладжування (краще кадрам)

$$\varphi_{new} = (1 - \alpha)\varphi_{cur} + \alpha\varphi_{des}, \quad 0 \leq \alpha \leq 1,$$

де φ означає будь-який з кутів – yaw/pitch.)

За допомогою цих формул також можна виконати симуляцію поведінки AimBot за допомогою синтетичного набору даних. Пропустимо траєкторії через кілька моделей прицілення:

- Ідеальний (миттєвий);
- LERP ($s = 0.08, 0.25, 0.6$);
- Експоненційне згладжування ($\alpha = 0.05, 0.2$);
- «Людський» (обмеження кутової швидкості + шум).

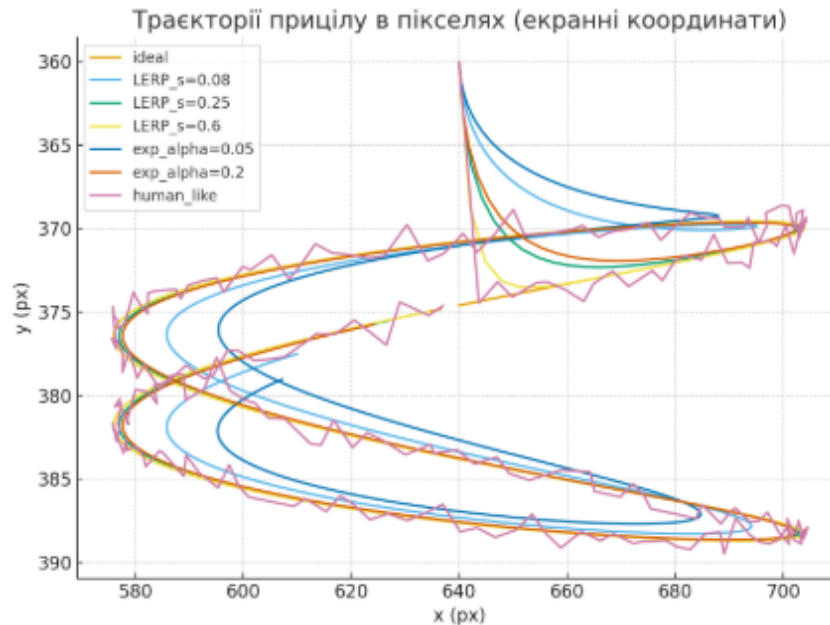


Рис.1 – Траєкторія наведення прицілу у піксельних координатах

Аналізуючи графік можна помітити, що модель з малим s (LERP $s = 0.08$) та малим α дає повільніше націлювання (велика затримка), але рух гладкий. Модель з великим s/α швидше наближається до мети, але може створювати більше різких змін. «Людська» модель має ширший розподіл кутових швидкостей і помітний випадковий компонент – це видно в гістограмі та в FFT (більш рівномірний спектр без виразних піків). FFT помилки yaw показує, що деякі моделі (особливо експоненційні/LERP із середніми параметрами) створюють помітні низькочастотні компоненти в помилці – це може бути індикатором «штучності» руху, якщо в реальності рухи гравця мають іншу спектральну структуру.

Для протистояння даним програмам розробники ігор використовують свій анти-шахрай софт. Деякі анти-шахрай продукти виконують перевірку на рівні ядра комп'ютера наприклад Vanguard та Faceit Anticheat. Анти-шахрай може визначати, чи рухається приціл природно, чи занадто «ідеально». Людський рух завжди має мікрошум – маленькі випадкові коливання. AimBot намагається вести приціл по оптимальній траєкторії, через що рух виглядає надто гладким таким що в кожен момент часу маємо положення прицілу (x_t, y_t) на екрані:

$$\vec{v}_t = x_{t+1} - x_t, y_{t+1} - y_t$$

Кутова швидкість прицілу (yaw/pitch):

$$w_t = \frac{\Delta\theta}{\Delta t}$$

Ентропія руху:

$$H = - \sum p(w) \log \log p(w)$$

У живої людини ентропія руху висока (хаотичність), у шахрая – низька (рухи одноманітні і «чисті»). Розробники анти-шахраїв експериментують з алгоритмами штучного інтелекту. Анти-шахрай збирає велику кількість даних: позиції, час реакції, точність пострілів, траєкторії миші. Потім система тренує модель, яка відділяє «людську поведінку» від «машинної». Математична суть:

$$f(X) \rightarrow \{0, 1\}$$

де X – вектор ознак: точність, швидкість наведення, ентропія руху, частота попадань і голову, зависання реакції, спектр рухів прицілу, а $f(X)$ – класифікатор (0 = чесна гра, 1 = шахрай).

Попередні дослідження здебільшого вказують на те, що анти-шахрай програми які мають доступ до ядра комп'ютера на даний момент є найефективнішими з усіх існуючих. Компанія EA під час розробки нової гри серії Battlefield представила новий анти-шахрай Javelin. Він має доступ до ядра комп'ютера, що дозволяє йому більш точно сканувати файлові системи. Під час пробного тесту гри анти-шахрай заблокував більше трьохсот тисяч користувачів за кілька днів. Отже, при дослідженні методів використання шахрайських програм слід розуміти кінцевий результат та необхідність їх використання. При протидії шахрайським програмам треба орієнтуватися на можливості системи, враховувати можливі конфлікти, розуміння ризиків та логіку роботи програми.

Список використаних джерел:

1. Форум гравців гри Battlefield
https://www.reddit.com/r/pcgaming/comments/1mf095m/battlefield_6_includes_a_kernellevel_anticheat/
2. Новини ігрової індустрії
<https://www.unian.net/games/battlefield-6-antichit-za-vremya-otkrytoy-bety-battlefield-6-v-igre-uzhe-zabanili-330-tysyach-chiterov-13094091.html>
3. How AI is changing the VAC system of CS2
<https://dataconomy.com/2024/07/29/how-ai-is-changing-the-vac-system-of-cs2/>

Коваленко К. А.
здобувач вищої освіти,
Державний податковий університет
Науковий керівник
Скасків Л. В.
к.ф.-м.н., доцент, доцент кафедри
вищої та прикладної математики
Державний податковий університет

МОДЕЛІ ТА ПРОГРАМНІ ІНСТРУМЕНТИ ЛІНІЙНОГО ТА НЕЛІНІЙНОГО ПРОГРАМУВАННЯ

Лінійне програмування, також відоме як лінійна оптимізація, є методом пошуку оптимального рішення, наприклад, для максимізації прибутку чи мінімізації витрат, у рамках математичної моделі, де обмеження описуються за допомогою лінійних рівнянь або нерівностей. Ця область є складовою математичного програмування, що спеціалізується на розв'язанні задач оптимізації.

Нелінійне програмування – це підхід, який полягає у максимізації або мінімізації певної цільової функції при врахуванні ряду обмежень. Його головна особливість полягає в тому, що цільова функція або деякі з обмежень мають нелінійний характер. Інакше кажучи, якщо цільова функція чи обмеження не дотримуються вимог лінійності (тобто не є рівняннями першого степеня), застосовують методи нелінійного програмування [6].

Модель лінійного програмування передбачає розв'язання задачі оптимізації з лінійною цільовою функцією і множиною допустимих рішень, визначених лінійними рівняннями або нерівностями.

Для вирішення таких задач використовуються різні методи, зокрема метод потенціалів, розроблений у 1940 році вченими Л. В. Канторовичем і М. К. Гавурінім для транспортних задач; симплекс-метод, запропонований Джорджем Данцігом у 1949 році як узагальнення методу потенціалів для загальної задачі лінійного програмування; та двоїстий симплекс-метод – модифікація симплекс-методу, яка дозволяє розв'язувати задачі двоїстого типу через використання їх початкових параметрів [7].

Цілочисельне програмування – це тип математичного програмування, де шукані змінні мають бути цілими числами. Мета полягає у віднайденні екстремуму функції в умовах параметричного простору, де всі або лише обрані змінні мають цілочисельний характер.

Найпростіший спосіб вирішення таких задач полягає в їхньому зведенні до задач лінійного програмування із подальшим аналізом знаходження цілочисельного рішення.

Булеве програмування є приватним випадком цілочисельного лінійного програмування, де змінні можуть набувати лише значення 0 або 1. Класичними

прикладом таких задач є призначення працівників завданням, пошук оптимальних маршрутів (задача комівояжера, задача листоноші) тощо.

Для вирішення таких задач застосовуються алгоритми, засновані на методах комбінаторики й теорії графів. У розв'язанні задач цілочисельного програмування найчастіше використовуються методи відтинання, зокрема метод Гоморі; а також комбінаторні прийоми, такі як метод гілок та меж [5].

Програмні інструменти лінійного програмування:

GeoGebra. За допомогою програми GeoGebra можна розв'язувати задачі лінійного програмування. Коли ти вставляєш рівняння та нерівності в GeoGebra, не потрібно переміщати члени так, щоб у залишався сам ліворуч від знака рівності [8].

MatLab. Ви можете використовувати MatLab для реалізації наступних поширених алгоритмів для розв'язання задач лінійного програмування:

- Внутрішня точка: Використовує первинно-дуальний алгоритм предиктора-коректора та особливо корисний для великомасштабних лінійних програм, які мають структуру або можуть бути визначені за допомогою розріджених матриць.

- Симплекс: Використовує систематичну процедуру для генерації та тестування кандидатів на вершинні розв'язки лінійної програми. Симплекс-алгоритм та пов'язаний з ним алгоритм подвійного симплексу є найбільш широко використовуваними алгоритмами для лінійної оптимізації [4].

LINDO. LINDO (Лінійний, Інтерактивний та Дискретний Оптимізатор) – це програмний пакет для лінійного програмування, цілочисельного програмування, нелінійного програмування, стохастичного програмування та глобальної оптимізації [3].

Програмні інструменти нелінійного програмування:

GEKKO. Це пакет Python для машинного навчання та оптимізації змішаних цілочисельних та диференціальних алгебраїчних рівнянь. Він поєднаний з великомасштабними розв'язувачами для лінійного, квадратичного, нелінійного та змішаного цілочисельного програмування (LP, QP, NLP, MILP, MINLP). Режими роботи включають параметричну регресію, узгодження даних, оптимізацію в реальному часі, динамічне моделювання та нелінійне прогнозування [2].

Excel Solver – метод GRG Nonlinear. У кращому випадку, метод розв'язання GRG сам по собі – як і практично всі “класичні” нелінійні алгоритми оптимізації – може знайти локально оптимальне рішення для досить добре масштабованої, неопуклої моделі. Часом розв'язувач зупиняється, не знайшовши локально оптимального рішення, коли він просувається дуже повільно (цільова функція дуже мало змінюється від одного пробного рішення до іншого) або з інших причин [1].

Бібліотека Galahad – це потокобезпечна бібліотека пакетів для розв'язання задач математичної оптимізації. Бібліотека охоплює такі галузі, як безумовна та обмежено-обмежена оптимізація, квадратичне програмування, нелінійне програмування, системи нелінійних рівнянь та нерівностей, а також нелінійні задачі найменших квадратів.

Список використаних джерел:

1. Excel Solver – GRG Nonlinear Solving Method Stopping Conditions. URL: <https://surl.li/ifcdvw>
2. GEKKO Optimization Suite. URL: <https://surl.lu/owqktv>
3. LINDO. URL: <https://surl.li/cnxaph>
4. What Is Linear Programming? URL: <https://surl.lu/auwxdi>
5. Модель лінійного програмування. URL: <https://surli.cc/xhfiad>
6. Нелінійне програмування – що це таке, визначення та поняття. URL: <https://surl.li/eyudbf>
7. Скасків Л. В. Теорія чисел та основні структури сучасної математики: навчальний посібник. – Ірпінь: Університет ДФС України, 2021. – 70 с.
8. Як розв'язувати задачі лінійного програмування в GeoGebra. URL: <https://surl.li/xavhxf>

УДК 004.738.5:658.5

Коваленко Ю. О.

здобувач вищої освіти,

Миколаївський національний аграрний університет

Науковий керівник:

Кучмійова Т. С.

к. е. н. доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій

Миколаївського національного аграрного університету

РОЛЬ ЦИФРОВИХ КОМУНІКАЦІЙНИХ ІНСТРУМЕНТІВ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ РОБОТИ КОМПАНІЙ

У сучасних умовах розвитку бізнесу ефективна комунікація стає одним із ключових факторів успіху компаній. Цифрові комунікаційні інструменти відкривають нові можливості для взаємодії всередині організації та з зовнішніми партнерами, дозволяючи оптимізувати процеси, підвищувати продуктивність працівників та швидше приймати управлінські рішення. Використання таких інструментів забезпечує гнучкість у роботі, сприяє кращому розподілу ресурсів та зміцнює конкурентні позиції компаній на ринку.

Метою є, дослідити роль цифрових комунікаційних інструментів у підвищенні ефективності роботи компаній та визначити, яким чином їх використання впливає на продуктивність, організаційну взаємодію та стратегічні результати підприємств.

Комунікації відіграють ключову роль у ефективній роботі підприємства, забезпечуючи своєчасний обмін необхідною інформацією між підрозділами та її передачу всім зацікавленим сторонам, включно зі співробітниками. Ефективна система комунікацій сприяє координації діяльності різних департаментів,

підвищує продуктивність праці та забезпечує швидке доведення продуктів і послуг до кінцевого споживача, що безпосередньо впливає на конкурентоспроможність компанії на ринку. Використання сучасних цифрових комунікаційних інструментів дозволяє оптимізувати внутрішні процеси, знизити ризик затримок у передачі інформації та забезпечити доступ до актуальних даних у режимі реального часу. Це дає можливість приймати більш обґрунтовані управлінські рішення, підвищує оперативність реагування на зміни зовнішнього середовища та сприяє реалізації стратегічних цілей підприємства [1].

Глобалізація сучасного світу розширює значення цифрових комунікацій, які виступають як стратегічний інструмент для бізнесу. Вони використовуються компаніями для просування продуктів та послуг, взаємодії з клієнтами та побудови бренду в умовах активної діджиталізації. Сучасні організації застосовують інтернет-маркетинг, соціальні мережі, контент-маркетинг та інші цифрові стратегії для досягнення конкурентних переваг. Формування ефективної системи цифрових комунікацій передбачає вибір оптимального набору інструментів, які на різних рівнях — макро, мезо та мікро — створюють умови для реалізації стратегічних цілей компанії та підтримки її пріоритетів розвитку. Аналіз практики українських підприємств у сферах страхування, логістики, ритейлу та швидкого харчування дозволяє виділити ключові тенденції розвитку цифрових комунікацій та оцінити їхній вплив на ефективність бізнес-процесів [2].

Підтримка залученості, мотивації та корпоративної культури в онлайн-середовищі є важливим аспектом дистанційного управління. Відсутність неформального спілкування та корпоративних заходів може послаблювати командний дух, тому компанії використовують цифрові платформи для його зміцнення. Поширені практики включають віртуальні «кавові паузи», внутрішні соціальні мережі та канали для обговорень, системи гейміфікації та відзнак, а також регулярний зворотний зв'язок через опитування та індивідуальні відео-зустрічі. Онлайн-вікторини, командні ігри та віддалені майстер-класи допомагають зменшити ізоляцію та створити позитивну атмосферу. Цифрові інструменти при цьому слугують засобом підтримки комунікації, а не самоціллю, допомагаючи керівникам ефективно взаємодіяти з командою [3].

Цифрові комунікаційні інструменти відіграють ключову роль у підвищенні ефективності роботи сучасних компаній. Вони забезпечують своєчасний обмін інформацією, координують діяльність підрозділів та сприяють швидкому прийняттю управлінських рішень. Використання цифрових платформ дозволяє оптимізувати внутрішні процеси, зменшити ризики інформаційних затримок та підвищити продуктивність працівників. Крім того, цифрові інструменти сприяють формуванню корпоративної культури, підтримці мотивації та згуртованості команд, особливо в умовах дистанційної роботи. Аналіз практики українських та міжнародних компаній показує, що ефективно впровадження цифрових комунікацій сприяє реалізації стратегічних цілей,

зміцненню конкурентних позицій на ринку та забезпеченню стабільного розвитку підприємств.

Список використаних джерел:

1. Бучнев М. М., Сучков І. О. Роль цифрових комунікацій у підвищенні ефективності управлінських процесів. Наукові вісті Дніпровського університету. 2024. №27. DOI: <https://doi.org/10.33216/2222-3428-2024-27-11> URL: <https://dspace.snu.edu.ua/handle/123456789/1983>
2. Осокін, М., & Осокін, А. Цифрові комунікації в системі управління бізнесом. Економіка та суспільство, 2024 (64). <https://doi.org/10.32782/2524-0072/2024-64-31>
3. Нестерук, В. Цифрові інструменти як засіб реалізації підходів до дистанційного та гібридного управління. Економіка та суспільство, 2025 (74). <https://doi.org/10.32782/2524-0072/2025-74-152>
4. Кучмілова Т. С., Сивоок Д. О. Нові парадигми менеджменту в умовах діджиталізації та активного цифрового розвитку. Моделювання соціально-економічного розвитку в системі забезпечення продовольчої безпеки : зб. тез II Всеукр. наук.-практ. конф. (м. Миколаїв, 08-09 трав. 2024 р.). Миколаїв : МНАУ, 2024. С. 126-127.

УДК 338.45:330.341.1

Коваль Н.А.

здобувач вищої освіти,

Вінницький національний аграрний університет

Томашук І.В.

PhD, доцент, доцент кафедри економіки та підприємницької діяльності

Вінницький національний аграрний університет

ІННОВАЦІЇ ЯК ЧИННИК ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ТА ЕФЕКТИВНОСТІ АГРАРНИХ ПІДПРИЄМСТВ

Важливість інновацій у аграрній сфері полягає в їхній здатності підвищувати продуктивність і ефективність виробництва, оптимізувати використання природних і матеріальних ресурсів та зменшувати негативний вплив на довкілля [1]. Впровадження новітніх технологій, цифрових рішень, сучасних агротехнологій і біотехнологій дозволяє аграрним підприємствам швидко адаптуватися до змін ринкових умов, забезпечувати високу якість продукції та вихід на нові ринки. Інновації також сприяють розвитку додаткових бізнес-напрямів, підвищенню конкурентоспроможності підприємств і залученню інвестицій, що у підсумку формує стійкий економічний розвиток сільських територій і продовольчу безпеку держави [2].

Особливості інновацій для підвищення конкурентоспроможності та ефективності аграрних підприємств полягають у їхній комплексності та різноплановості [3]. Вони охоплюють технологічні нововведення (сучасні агротехнології, автоматизація, цифровізація процесів), продуктово-продуктивні зміни (нові сорти культур, органічна продукція), управлінські та організаційні інновації (ефективні бізнес-моделі, кооперативи, кластери) і маркетингові підходи (брендинг, електронна комерція) [4]. Інновації забезпечують гнучкість підприємств, швидку адаптацію до змін ринкового середовища, оптимізацію витрат і підвищення якості продукції [5]. Водночас вони сприяють розширенню ринків збуту, підвищенню інвестиційної привабливості та зміцненню соціально-економічної стабільності сільських територій, що робить їх ключовим чинником довгострокового економічного зростання аграрного сектору [6].

Табл. 1 узагальнює основні характеристики інновацій у аграрній сфері, включаючи технологічні, продуктові, процесні, організаційні, маркетингові, екологічні та соціальні аспекти. Вони охоплюють впровадження сучасних агротехнологій, цифровізацію виробничих процесів, створення нових продуктів, оптимізацію управлінських та маркетингових практик, а також підвищення соціальної та екологічної відповідальності підприємств. Сукупність цих характеристик сприяє підвищенню продуктивності, конкурентоспроможності та сталого розвитку аграрного бізнесу.

Таблиця 1

Основні характеристики інновацій у аграрній сфері

Характеристика	Опис	Приклади у аграрному секторі
Технологічність	Використання новітніх технологій для підвищення продуктивності та оптимізації ресурсів	Дрони для моніторингу полів, автоматизовані системи поливу, точне землеробство
Продуктова інноваційність	Створення нових або покращених продуктів	Нові сорти культур, органічна та функціональна продукція
Процесна ефективність	Модернізація виробничих та управлінських процесів	ERP-системи для фермерських господарств, автоматизація обліку
Маркетингова новизна	Використання сучасних методів просування та збуту	Е-commerce, соціальні мережі, брендування продукції
Організаційна	Вдосконалення структур і моделей управління підприємством	Аграрні кластери, кооперативи, партнерські мережі
Екологічна («зелена») орієнтація	Застосування рішень для збереження довкілля та сталого використання ресурсів	Біогазові установки, сонячні панелі, переробка відходів
Соціальна значущість	Вплив на зайнятість, соціальну інфраструктуру та якість життя населення	Агроосвіта, агротуризм, створення робочих місць на селі

Пропонуємо розглянути ряд показників конкурентоспроможності аграрного підприємства на основі впровадження інновацій до яких належать [1, 7]:

— 1. Індекс інноваційної активності (I_i), який відображає ступінь впровадження інновацій у діяльність підприємства. результат у % – показує відносну інноваційну активність підприємства.

$$I_i = \frac{K_{\text{іннов}}}{K_{\text{заг}}} \times 100\%$$

де:

— $K_{\text{іннов}}$ – кількість впроваджених інновацій (технологічних, продуктових, організаційних);

— $K_{\text{заг}}$ – загальна кількість можливих або запланованих інновацій;

— 2. Показник підвищення продуктивності праці за рахунок інновацій (P_i) – це результат у %, який показує ефективність впливу інновацій на продуктивність.

$$P_i = \frac{V_{\text{після}} - V_{\text{до}}}{V_{\text{до}}} \times 100\%$$

де:

— $V_{\text{до}}$ – продуктивність праці до впровадження інновацій;

— $V_{\text{після}}$ – продуктивність праці після впровадження інновацій;

— 3. Індекс конкурентоспроможності продукції (K_p) дозволяє оцінити конкурентоспроможність продукції на ринку з урахуванням інновацій.

$$K_p = \frac{C_{\text{ринк}} - C_{\text{соб}}}{C_{\text{ринк}}} \times \frac{Y_{\text{пр}}}{100}$$

де:

— $C_{\text{ринк}}$ – середня ціна продукції на ринку;

— $C_{\text{соб}}$ – собівартість виробництва продукції;

— $Y_{\text{пр}}$ – індекс якості продукції (0–100);

— 4. Фінансовий ефект інновацій (Φ_i) показує прямий економічний ефект інновацій.

$$\Phi_i = \text{Дох}_{\text{іннов}} - \text{Дох}_{\text{градиц}}$$

де:

— $\text{Дох}_{\text{іннов}}$ – дохід підприємства після впровадження інновацій;

— $\text{Дох}_{\text{традиц}}$ – дохід підприємства без впровадження інновацій.

Інновації виступають ключовим чинником підвищення ефективності та конкурентоспроможності аграрних підприємств, оскільки впровадження сучасних технологій, автоматизації виробничих процесів та цифрових рішень дозволяє підвищувати продуктивність, зменшувати витрати та покращувати якість продукції. Активне застосування інновацій забезпечує адаптацію до змін ринкового середовища, сприяє розширенню ринків збуту та формує стійкі конкурентні переваги, водночас підтримуючи екологічну безпеку та сталий розвиток. Максимальний ефект досягається через інтегроване впровадження технологічних, організаційних та управлінських новацій у поєднанні з підготовкою кваліфікованого персоналу.

Список використаних джерел:

1. Іванишин О.Р., Шевчук С.В. Інновації, як чинник встановлення конкурентоспроможного АПК України. URL: https://www.lute.lviv.ua/uploads/media/LAC_SNT_Vydannya_Stattya_Ivanysyn-Sh evchyk-2.pdf
2. Томашук І.В., Мулик М.В. Інноваційна складова конкурентоспроможності національних економік на сучасному етапі глобального розвитку. *Вчені записки Таврійського національного університету ім. В.І. Вернадського. Серія: Економіка і управління*. 2019. Том 30 (69). №1. С. 78-83
3. Гончарук І.В., Томашук І.В. Формування стратегії економічного розвитку сільськогосподарського підприємства для підвищення його конкурентоспроможності. *Економіка, фінанси, менеджмент: актуальні питання науки і практики*. 2022. № 4 (62). С. 7-24. DOI: 10.37128/2411-4413-2022-4-1
4. Tomashuk I. Competitiveness of agricultural enterprises in market conditions and ways of its increase. *Green, Blue & Digital Economy Journal*. 2023. № 1. Vol. 4. P. 64-81. DOI: <https://doi.org/10.30525/2661-5169/2023-1-7>
5. Гончарук І.В., Томашук І.В. Вплив інноваційних процесів на підвищення конкурентоспроможності сільськогосподарських підприємств. *Економіка, фінанси, менеджмент: актуальні питання науки і практики*. 2023. № 1. (63). С. 30-47. DOI: 10.37128/2411-4413-2023-1-3
6. Томашук І.В., Томашук І.О. Сільське підприємництво в умовах війни: оцінка розвитку та конкурентних переваг. *Управління змінами та інновації*. 2025. №14. С. 59-68. DOI: <https://doi.org/10.32782/CMI/2025-14-9>
7. Томашук І.В. Модернізація аграрної галузі через сталу інтеграцію інноваційних рішень. *Держава та регіони. Серія «Економіка та підприємництво»*. 2025. Вип. № 2 (136). С. 36-45. DOI: <https://doi.org/10.32782/1814-1161/2025-2-6>

Коваль О.Т.

здобувач вищої освіти,

Карпатського національного університету ім. Василя Стефаника

Науковий керівник

Савка І.Я.

к.ф.м.н., ст. викл. кафедри інформаційних технологій

Карпатського національного університету ім. Василя Стефаника

ЗАЛЕЖНІСТЬ ЯКОСТІ ПЗ ДЛЯ ВИЯВЛЕННЯ ВТОРГНЕНЬ У МЕРЕЖІ ВІД МЕТОДІВ ВИБОРУ ОЗНАК У МОДЕЛЯХ ML

Сучасні системи виявлення вторгнень IDS (Intrusion Detection System) є критично важливим компонентом кібербезпеки, що покликані ідентифікувати атаки у мережевому трафіку та вчасно реагувати на інциденти. Однак, в цілому ефективність таких систем визначається не лише точністю класифікації трафіку, а й іншими характеристиками програмного забезпечення (ПЗ) – швидкістю, надійністю та здатністю до масштабування. Для всебічної оцінки якості такої системи можна орієнтуватися на міжнародний стандарт ISO/IEC 25010 [1], який формалізує модель якості ПЗ. Зокрема, у контексті IDS особливого значення набувають такі характеристики: функціональна придатність F_{func} – середнє між загальною точністю *Accuracy* та мірою *FI*, надійність F_{rel} – показник *Precision*, продуктивність F_{perf} – поєднує швидкість навчання моделі F_{train} та пропускну здатність прогнозування F_{infer} , масштабованість F_{scale} – показник, що збільшується при меншій кількості використаних ознак.

Метою проведеного дослідження було оцінити вплив різних методів вибору ознак (Feature Selection, FS) на якість IDS з використанням інтегрального показника Q , що враховує як функціональні, так і нефункціональні характеристики. Для розрахунку застосовувалася вагова формула

$$Q = 0.4 * F_{func} + 0.2 * F_{rel} + 0.2 * F_{perf} + 0.2 * F_{scale}.$$

Тут продуктивність F_{perf} визначається як зважене середнє між ефективністю часу навчання моделі ML та швидкістю її прогнозування з ваговим коефіцієнтом $\alpha \in [0, 1]$:

$$F_{perf} = \alpha * F_{train} + (1 - \alpha) * F_{infer},$$

де $F_{train} = \exp\left(-\beta * \frac{T_{eff}}{T_{train}^{base}}\right)$, $T_{eff} = T_{train} + \frac{T_{FS}}{K}$ – ефективний час навчання, β

– коефіцієнт згладжування часу навчання, T_{train}^{base} і T_{train} – час навчання без FS і після застосування FS, відповідно, T_{FS} – додатковий час на виконання процедури

FS, K – кількість навчальних ітерацій, протягом деякого періоду використання системи, $F_{infer} = 1 - \frac{T_{predict}}{T_{max}}$, T_{max} – найдовший час прогнозу серед усіх моделей, $T_{predict}$ визначає час прогнозу моделі для обраного FS методу.

Масштабованість F_{scale} розраховувалась за формулою:

$$F_{scale} = \max \left\{ 0, 1 - \frac{N}{N_{base}} \right\},$$

де N – кількість ознак після застосування FS, N_{base} – кількість ознак у початковому датасеті. Якщо кількість ознак не є зменшено або, можливо, збільшено у порівнянні з початковим набором, то масштабованість моделі вважається нульовою. Навпаки, зменшення ознак підвищує гнучкість і масштабованість моделі, що спрощує її використання та дозволяє ефективніше масштабувати на більші обсяги даних.

У дослідженні використано датасет CIC-IDS-2017 [2], який містить широкий спектр мережових атак [3]. Для моделювання застосовано алгоритми RandomForest та XGBoost, для скорочення кількості ознак застосовувалися методи Filter [4], Embedded [5], Wrapper [6], а також контрольний сценарій без вибору ознак (noFS).

Зведені результати дослідження наведено у таблиці 1.

Таблиця 1

Порівняння результатів тренування моделей та обрахунку інтегрального показника у випадку $\alpha = \beta = 0.5$, $K=36$

	Метод	Модель	N	F_{func}	F_{rel}	F_{perf}	F_{scale}	T_{FS}	T_{train}	Q
1	embedded	RF	52	0.99	0.99	0.30	0.35	161.1	56.30	0.730
2	embedded	XGBoost	52	0.99	0.99	0.60	0.35	161.1	5.20	0.791
3	filter	RF	32	0.99	0.99	0.52	0.60	80	28.97	0.824
4	filter	XGBoost	32	0.99	0.99	0.69	0.60	80	4.68	0.858
5	wrapper	RF	20	0.99	0.99	0.46	0.75	1590	24.42	0.842
6	wrapper	XGBoost	20	0.99	1.0	0.40	0.75	1590	3.03	0.829
7	noFS	RF	80	0.99	0.99	0.30	0.0	0.0	59.50	0.660
8	noFS	XGBoost	80	0.99	0.99	0.65	0.0	0.0	8.06	0.730

Аналіз результатів показав, що усі методи вибору ознак забезпечують високу функціональну точність моделей IDS (F_{func} та $F_{rel} \approx 0.99$), однак інтегральний показник якості Q суттєво відрізняється, в залежності від обчислювальних витрат та масштабованості. Найнижчі значення Q спостерігаються у сценарії без застосування FS (0.660 для RF та 0.730 для XGBoost). Метод filter продемонстрував найкращі результати ($Q = 0.824$ і 0.858 відповідно), що зумовлено оптимальним балансом між точністю, швидкістю навчання ($T_{train} \approx 29$ с та 4.7 с) і часом процедури FS ($T_{FS} = 80$ с).

Embedded-метод показав прийнятний компроміс між продуктивністю та часовими витратами. Wrapper-метод досяг високої якості ($Q = 0.842$ та 0.829 відповідно) завдяки найвищій масштабованості ($F_{scale} = 0.75$) та скороченню кількості ознак ($N = 20$), що позитивно вплинуло на швидкість тренування моделі.

Таким чином, результати дослідження підтверджують доцільність застосування комплексного підходу до оцінки IDS. Використання лише традиційних характеристик (Ассурасу, F1, тощо) дає обмежене уявлення про роботу системи: модель без FS демонструє високу точність, але водночас має нижчі показники з точки зору якості програмного забезпечення. Запропонований інтегральний показник Q дозволяє враховувати практичні вимоги до IDS у сфері кібербезпеки, де критично важливими є швидкість реакції та здатність до обробки великих обсягів даних.

Список використаних джерел

1. ДСТУ ISO/IEC 25010:2016. Інженерія систем і програмних засобів – Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE) – Моделі якості системи та програмних засобів.
2. Canadian Institute for Cybersecurity. (2018). Intrusion Detection Evaluation Dataset (CICIDS2017). University of New Brunswick. URL: <https://www.unb.ca/cic/datasets/ids-2017.html>.
3. Reis, B., Maia, E., Praça, I. (2020). Selection and Performance Analysis of CICIDS2017 Features Importance. In: Benzekri, A., Barbeau, M., Gong, G., Laborde, R., Garcia-Alfaro, J. (eds) Foundations and Practice of Security. FPS 2019. Lecture Notes in Computer Science(), vol 12056. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-45371-8_4.
4. Zouhri, Houssam & Idri, Ali & Ratnani, Ahmed. (2023). Evaluating the impact of filter-based feature selection in intrusion detection systems. International Journal of Information Security. 23. DOI: <https://doi.org/10.1007/s10207-023-00767-y>.
5. Yin, Y., Jang-Jaccard, J., Xu, W. et al. IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset. J Big Data 10, 15 (2023). DOI: <https://doi.org/10.1186/s40537-023-00694-8>.
6. Rahman, M. S., & Khan, J. A. (2015). Building a Robust Linear Model with Backward Elimination Procedure. Dhaka University Journal of Science, 62(2), 87–93. DOI: <https://doi.org/10.3329/dujs.v62i2.21971>.

*Ковальський А.А.
здобувач вищої освіти
Науковий керівник
Тулученко Г.Я.*

*д.т.н., професор, професор кафедри вищої математики
Національний технічний університет «Харківський політехнічний інститут»*

БІБЛІОТЕКА MANIM ЯК ІНСТРУМЕНТ ДЛЯ АНІМАЦІЇ ВЕКТОРНИХ ПОЛІВ У ОСВІТНЬОМУ ПРОЦЕСІ

На сучасному етапі цифрової трансформації вищої технічної освіти її ефективність значною мірою залежить від використання візуальних та інтерактивних програмних засобів, особливо при викладанні таких складних розділів вищої математики, як векторний аналіз. Традиційні статичні методи викладання часто не дозволяють студентам сформувати інтуїтивне просторове розуміння векторних полів, що знижує мотивацію та якість засвоєння матеріалу. Вирішення цієї проблеми лежить у площині програмного моделювання та динамічної візуалізації.

Бібліотека Manim (Mathematical Animation Engine), розроблена Grant Sanderson та розвинута спільнотою як open-source проєкт, є потужним інструментом, спеціально призначеним для створення високоякісних математичних анімацій [1-2]. Її інтеграція з мовою програмування Python – однією з найпопулярніших у сучасному ІТ-просторі – відкриває перспективи для інноваційного візуального супроводу дисциплін фізико-математичного циклу.

Метою даної роботи є обґрунтування методичних засад використання бібліотеки Manim для розробки інтерактивного візуального супроводу викладання векторного аналізу та оцінка його впливу на якість засвоєння складних математичних концепцій здобувачами освіти.

Наявні високоякісні ресурси, зокрема навчальні відеоматеріали каналу 3Blue1Brown, розроблені за допомогою бібліотеки Manim, демонструють величезний потенціал математичної анімації. Проте, зовнішній відеоконтент часто є стандартним і не може бути адаптований для розв'язання конкретних навчальних задач або інтегрований у систему перевірки знань. У цьому контексті, необхідність створення власних модульних застосунків зумовлена можливістю їхньої персоналізації під навчальну програму та їхнім використанням не лише як візуального супроводу, але і як інструменту для самостійної роботи та контролю. Зокрема, програмний підхід дозволяє реалізувати елементи гейміфікації та автоматичної перевірки правильності розв'язків.

Розробка навчальних застосунків для вивчення векторного аналізу набуває нового рівня завдяки комплексному використанню бібліотек Manim, Tkinter та PyQt. Бібліотека Manim забезпечує генерування високоякісних анімацій понять векторного аналізу. Інтеграція з Tkinter, простим і доступним інструментом для

швидкого створення графічних інтерфейсів, дозволяє розробляти інтерактивні застосунки, де студенти можуть задавати параметри анімацій (наприклад, координати векторних полів) та візуально досліджувати просторову конфігурацію поля завдяки вбудованим механізмам 3D-огляду в анімації.

Для більш складних і масштабованих рішень бібліотека PyQt пропонує розширені можливості дизайну інтерфейсів, включаючи підтримку мультимедійних елементів та інтеграцію з онлайн-платформами. Комплексне використання цих бібліотек дає змогу створювати модульні навчальні застосунки, які поєднують професійну візуалізацію, інтерактивний GUI та автоматизацію обчислень, відповідаючи сучасним тенденціям цифровізації освіти.

За допомогою команд бібліотеки Manim було розроблено набір інтерактивних навчальних застосунків для візуалізації ключових концепцій векторного аналізу, зокрема векторних полів та криволінійних інтегралів. Реалізовано програмні модулі з використанням класів VectorField та ArrowVectorField. Інтерфейс застосунків дає змогу студентам вводити компоненти векторних полів, отримувати автоматичну перевірку правильності розв'язків та генерувати анімацію як візуальний результат. Ці застосунки включають елементи гейміфікації, де успішне виконання завдання винагороджується динамічною візуалізацією, що підсилює мотивацію.

Спираючись на відомі результати досліджень ефективності візуального навчання, можна очікувати на підвищення успішності студентів на 20-30% при вивченні розділу «Векторний аналіз» [3-4].

Таким чином, використання бібліотеки Manim як програмного засобу для візуального супроводу векторного аналізу відповідає сучасним тенденціям цифровізації освіти. Запропонований підхід забезпечує підвищення якості викладання та засвоєння матеріалу завдяки модульності (інтеграція в Moodle, Google Classroom та Jupyter Notebook), персоналізації (гейміфікація та автоматична перевірка завдань) та індивідуалізації навчального процесу.

Список використаних джерел:

1. Eertmans, W. Manim Slides: A Python package for presenting Manim content anywhere // Journal of Open Source Education. 2023. Vol. 6, iss. 66. P. 206. doi: <https://doi.org/10.21105/jose.00206>
2. Manim Community Documentation. (2025). Available at: <https://docs.manim.community/en/stable/>
3. Mayer, R. E. (2009). Multimedia Learning (2nd ed.). Cambridge University Press.
4. Heeren, T., & Prins, R. (2020). Visualization in Mathematics Education: Tools and Techniques. Journal of Educational Technology, 47(3), 321–335. DOI: <https://doi.org/10.24297/jam.v21i.9136>

Колісниченко М.В.
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Науковий керівник
Кобилін О.А.
Завідувач кафедри інформатики, кандидат технічних наук, доцент
Харківський національний університет радіоелектроніки

ВИКОРИСТАННЯ РІВНІВ ДЕТАЛІЗАЦІЇ (LOD) У МЕРЕЖЕВИХ ІГРАХ ДЛЯ ЗНИЖЕННЯ НАВАНТАЖЕННЯ

Тема оптимізації комп'ютерних ігор є актуальною, адже сучасна ігрова індустрія демонструє сталу тенденцію до зростання складності 3D-графіки. Це спричиняє навантаження на апаратні ресурси, а особливо в мережесіткових іграх, де обробляється велика кількість об'єктів і гравців одночасно. Одним із перевірених та широко застосовуваних способів підвищення продуктивності є використання технології Level of Detail (LOD), яка динамічно змінює складність відтворення об'єкта залежно від його наближеності до камери, важливості в сцені або пріоритету для геймплею.

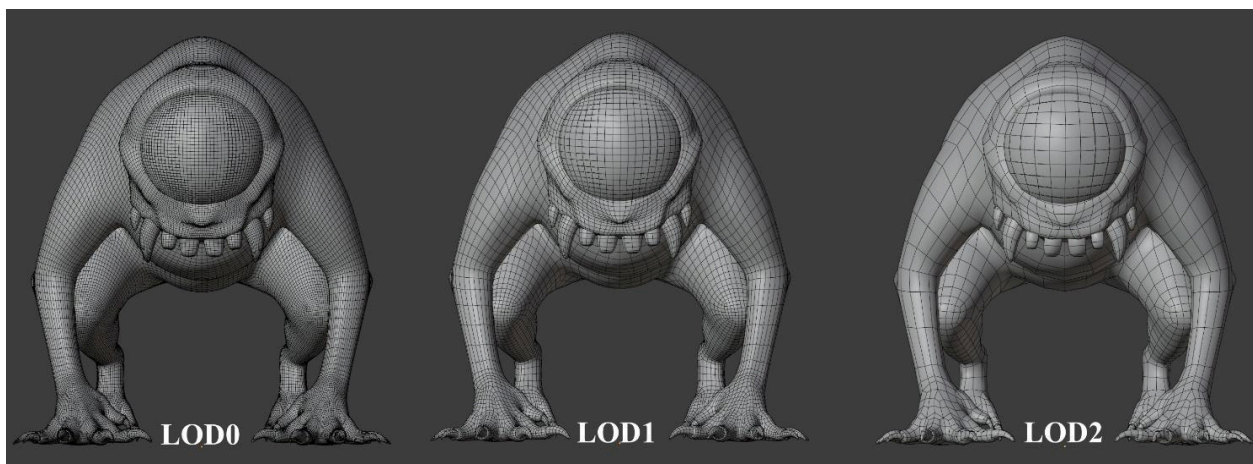


Рисунок 1 – Приклад реалізації LOD на 3D-персонажі

Основними методами реалізації LOD є:

- геометричний LOD – поступове зменшення кількості полігонів на 3D-моделях. Це дозволяє зменшити навантаження на графічний процесор, використовуючи спрощену геометрію для віддалених об'єктів;
- LOD для текстур – використання MIP-карт, які дозволяють підвантажувати текстури з різною роздільністю. Це дає змогу підвищити швидкість відтворення сцен;
- імпостери та білборди – заміна складних моделей на плоскі зображення на великій відстані. Такий підхід найчастіше використовується та є найефективнішим для віддалених елементів довкілля (дерева, гори, будівлі, тощо);

- комбіновані методи – поєднання кількох варіантів для досягнення найбільшої ефективності.

Існують адаптивні методи перемикання рівнів деталізації. Сучасні рушії можуть враховувати не лише геометричну відстань до камери, перемикаючи рівні, а також такі параметри як швидкість руху гравця, кут його огляду або важливість для поточної сцени. Наприклад, рухаючись на великій швидкості, гравець фізично не встигне помітити меншу деталізацію об'єкта. Такий підхід дозволяє значно зменшити навантаження на GPU, при цьому не знижуючи рівень візуального комфорту гравця.

У багатокористувацьких іграх ця технологія має свої особливості:

- необхідно узгоджувати оптимізацію з мережею, аби уникнути відмінностей у відображенні сцени;
- зберегти баланс між економією ресурсів і чесністю геймплею;
- можливість застосувати серверний LOD, що зменшить навантаження на клієнтські пристрої.

У популярних ігрових рушіях (Unreal Engine, Unity) є власні модулі для роботи з LOD. Але досконалість кінцевого результату залежатиме також від роботи дизайнерів та програмістів, які налаштовують пороги перемикання між рівнями LOD та контролюють візуальну правдоподібність.

Метод оптимізації за допомогою LOD широко застосовується у багатьох сучасних ігрових проєктах. Наприклад, у грі World of Warcraft активно використовуються білборди для відображення віддаленої рослинності та будівель, що дозволяє підтримувати стабільний рівень FPS. У проєкті The Witcher 3 розробники застосовують комбінований підхід, поєднуючи геометричний LOD, імпостерів та системи «динамічного обрізання» об'єктів, непомітних для камери. У Fortnite та PUBG особливу увагу приділяють балансуванню між продуктивністю та чесністю геймплею, наприклад, об'єкти, з якими може взаємодіяти гравець, завжди будуть мати більшу деталізацію, ніж об'єкти, з якими взаємодіяти не можна. Таким чином, розробники одночасно допомагають гравцю фокусуватися на важливих речах, при цьому економлячи ресурси на інших об'єктах.

Отже, технологія рівнів деталізації є одним із найважливіших інструментів оптимізації у сфері мережеских ігор. Застосування цієї технології дозволяє зменшити використання пам'яті, стабілізувати частоту кадрів і забезпечити плавний ігровий процес для усіх його учасників навіть у масштабних багатокористувацьких ігрових сесіях.

Список використаних джерел

1. Вільямс Д., Акеніне-Меллер Т., Гейнс Е. Рендеринг у реальному часі. 4-те вид. Бока-Ратон: CRC Press, 2018. 1269 с.
2. Фішер Д. Оптимізація ігор: підвищення FPS. Бірмінгем: Packt Publishing, 2017. 352 с.
3. Unity Technologies. Документація Unity: Рівні деталізації (LOD). Unity Docs, 2023. URL: <https://docs.unity3d.com/Manual/LevelOfDetail.html> (дата звернення: 14.09.2025)

4. Epic Games. Документація Unreal Engine: Система LOD. Unreal Docs, 2023. URL: <https://docs.unrealengine.com/5.0/en-US/level-of-detail-in-unreal-engine/> (дата звернення: 14.09.2025)
5. Се Л., Чжан Цз., Ван Ю. Оптимізація 3D-ресурсів для ігор із використанням штучного інтелекту. IEEE Transactions on Games. 2021. Т. 13, № 4. С. 26–38.

УДК 004.056.53

Корепанов І.С.
здобувач вищої освіти,
Бахмутський навчально-науковий професійно-педагогічний інститут
ХНУ ім. В.Н. Каразіна
Науковий керівник
Нефьодова І.В.
к. ф.-м. н., доцент, доцент кафедри електромеханічних та
комп'ютерних систем,
Бахмутський навчально-науковий професійно-педагогічний інститут
ХНУ ім. В.Н. Каразіна

PYTHON ТА JUPYTER NOTEBOOK ЯК ІНСТРУМЕНТИ ДЛЯ РОЗВИТКУ STEM-ОСВІТИ

Нові програмні засоби та інформаційні технології використовуються в цифровій трансформації сучасної освіти. Поєднання теоретичних знань з моделюванням реального світу стає все більш важливим у викладанні дисциплін STEM (наука, технологія, інженерія та математика). Поєднання інтерактивного середовища Jupyter Notebook з мовою програмування Python є одним з найкращих способів вирішення цієї проблеми. Завдяки поєднанню програмного коду, навчального тексту та візуалізації результатів їх використання дозволяє розробляти освітні ресурси нового покоління.

Python є однією з найпоширеніших мов програмування у світі. Її універсальність, низький поріг входу та простий синтаксис є причинами її популярності. Це означає, що студенти можуть швидко почати працювати з мовою, навіть якщо вони мають невеликий досвід програмування. Міжнародна спільнота також активно підтримує Python, надаючи користувачам доступ до великої кількості навчальних матеріалів, реальних прикладів та відкритих проєктів. За допомогою розвиненої екосистеми бібліотек (NumPy, Pandas, Matplotlib, SciPy, TensorFlow) можна виконувати численні завдання, від простих алгоритмів до аналізу даних та штучного інтелекту. Завдяки цьому Python є незамінним інструментом у сферах STEM. Jupyter Notebook, у свою чергу, створює інтерактивне середовище, де програмний код поєднується з поясненнями, формулами та візуалізаціями, що робить навчання більш наочним

і практикоорієнтованим. Разом вони сприяють глибшому засвоєнню знань, розвитку дослідницьких умінь та ефективній організації як аудиторної, так і дистанційної роботи.

Можливості для STEM-дисциплін.

- Математика: обчислення, розв'язування рівнянь, моделювання процесів і побудова графіків функцій.
- Фізика: візуалізація хвильових процесів, оцінка експериментальних даних і моделювання механічних коливань.
- Хімія та біологія: моделювання біохімічних реакцій, статистичний аналіз експериментальних даних.
- Інформатика та інженерія: вивчення алгоритмів і структур даних, аналіз великих даних та оптимізація.
- Соціальні науки та економіка: використання бібліотек Python для моделювання, прогнозування та аналізу даних.

Приклади використання у навчанні.

- Створення інтерактивних навчальних матеріалів.
- Автоматизовані лабораторні роботи з аналізом даних.
- Відкриті освітні курси на базі Jupyter (наприклад, у Coursera, EdX).

Використання Python та Jupyter Notebook у навчальному процесі відкриває широкі можливості для поєднання теоретичних знань із практичними навичками. Завдяки інтерактивному середовищу студенти можуть одночасно читати пояснення, виконувати код та одразу бачити результати, що сприяє кращому засвоєнню матеріалу. Важливою перевагою є наочність: числові обчислення, графіки чи симуляції відображаються у зрозумілому візуальному форматі, що значно підвищує мотивацію до навчання. Крім того, інтеграція Jupyter Notebook із сучасними інструментами співпраці, такими як GitHub чи Google Colab, робить можливим дистанційне та колективне навчання. Студенти можуть спільно працювати над завданнями, ділитися результатами й удосконалювати власні рішення, що формує не лише технічні, а й комунікативні навички, необхідні для сучасної освіти.

Попри значні переваги, використання Python та Jupyter Notebook у навчанні супроводжується певними викликами. Однією з головних проблем є потреба у відповідній технічній підготовці викладачів, адже для ефективного використання інструментів необхідні не лише базові знання програмування, а й розуміння можливостей бібліотек та методик інтеграції їх у навчальний процес. Додатковим обмеженням стає різний рівень підготовки студентів: для частини з них навіть простий синтаксис Python може бути складним на початковому етапі, що потребує поступового введення матеріалу. Важливим чинником є й технічні ресурси – складні обчислювальні задачі, наприклад у фізиці чи обробці великих масивів даних, можуть вимагати потужнішого обладнання або доступу до хмарних сервісів. Таким чином, успішна інтеграція Python та Jupyter Notebook в освітній процес потребує методичної підготовки, поступовості у викладанні та врахування технічних можливостей навчального середовища.

Jupyter Notebook і Python є корисними ресурсами для розвитку освіти в галузі STEM. Вони сприяють набуттю практичних навичок, розвитку

критичного мислення та впровадженню цифрових технологій в освітній процес. Вони ідеально підходять для навчальних цілей завдяки відкритому коду та доступності. Правильний баланс між перевагами й усвідомленням обмежень дає змогу максимально розкрити освітній потенціал цих технологій. Створення безкоштовних освітніх ресурсів, інтеграція цих інструментів із хмарними сервісами та їх активне застосування в змішаному та дистанційному навчанні є потенційними напрямками розвитку.

Список використаних джерел:

1. Using Jupyter Notebooks as digital assessment tools: An empirical examination of student teachers' attitudes and skills towards digital assessment. *Education and Information Technologies*, 2025.

URL: <https://link.springer.com/article/10.1007/s10639-025-13507-7>

2. Трейтяк Д. В. Python programming language as a tool in scientific and pedagogical activities. *Інформаційні технології і засоби навчання*, 2025.

URL: <https://lib.iitta.gov.ua/id/eprint/745924/>

3. Rais D., Rochmad R., Dwijayanti I., Wardono W., Pratiwi H. Elevating student engagement and academic performance: A quantitative analysis of Python programming integration in the Merdeka Belajar curriculum. *Journal on Mathematics Education*, 2024. URL: <https://arxiv.org/abs/2309.06158>

УДК 004.932.2

Косовський С.Б.

здобувач вищої освіти,

Харківський національний університет радіоелектроніки

Науковий керівник

Кобилін І.О.

к.т.н., асистент кафедри Інформатики,

Харківський національний університет радіоелектроніки

ВИКОРИСТАННЯ ІГРОВОГО РУШІЮ UNITY ДЛЯ СТВОРЕННЯ AR ТА VR ОСВІТНЬО-ІГРОВИХ ПРОГРАМ

У сучасних умовах цифровізації освіти дедалі більшої актуальності набуває використання технологій доповненої (Augmented Reality, AR) та віртуальної реальності (Virtual Reality, VR). Їхня інтеграція в освітній процес динамічні симуляції та забезпечувати високий рівень залученості студентів.

Віртуальну реальність можна описати наступним чином (1):

У VR користувач повністю занурюється у віртуальне середовище, це можна описати так(1):

$$V(x, y, z) \subset \mathbb{R}^3 \quad P_{VR} = f_{VR}(V, C) \quad (1)$$

де: C — положення та орієнтація камери,
 f_{VR} — функція рендерингу віртуального середовища на екрані або шоломі.

V — це координати об'єктів у віртуальному просторі.

Суть VR: користувач бачить тільки V (віртуальний світ), R (реальний світ) не враховується.

У AR же ми накладаємо віртуальні об'єкти на реальний світ, це можна описати так(2):

$$R(x, y, z) \subset \mathbb{R}^3 \quad P_{AR} = f_{AR}(R, V, C) \quad (2)$$

де: R — реальний світ (кадр з камери),
 V — віртуальні об'єкти,
 C — положення та орієнтація камери,
 f_{AR} — функція накладання (композиції) віртуального на реальний світ.

Особливе значення має використання ігрових рушіїв, що дозволяють поєднати інтерактивність і педагогічні принципи. Одним із найпоширеніших інструментів цього типу є Unity.

Unity є кросплатформним рушієм, що підтримує розробку застосунків для мобільних пристроїв, комп'ютерів та VR/AR гарнітур. Його перевага полягає у наявності універсальної архітектури, яка поєднує редактор сцен, засоби роботи з фізикою, системами частинок, анімацією та аудіо. Для AR та VR Unity пропонує інтеграцію з платформами ARCore (Google), ARKit (Apple), а також підтримку гарнітур Oculus, HTC Vive, Microsoft HoloLens та інших.

AR та VR застосовуються в освіті для створення умов, що моделюють практичні ситуації або забезпечують нові форми подання знань. AR дає змогу «накладати» віртуальні об'єкти на фізичне середовище, що особливо корисно в природничих науках, архітектурі та медицині. VR, у свою чергу, забезпечує повне занурення у навчальний простір, наприклад лабораторій, де студенти можуть безпечно експериментувати з обладнанням.

Unity як інструмент для реалізації таких сценаріїв має кілька ключових теоретичних характеристик:

- Модульність: освітні сцени будуються з окремих об'єктів, що мають компоненти для візуалізації, фізики та взаємодії;
- Кросплатформність: одна й та сама освітньо-ігрова програма може бути запущена на смартфоні, у браузері чи VR-шоломі;
- Система подій: забезпечує інтерактивність, що є основою ігрових підходів до навчання;
- Робота з 3D-моделями та мультимедіа: дозволяє інтегрувати складні освітні ресурси, включаючи анімацію й реалістичну графіку.

Педагогічний ефект AR/VR заснований на поєднанні візуалізації та активної взаємодії. Теорія когнітивного навантаження (Cognitive Load Theory) стверджує, що візуалізація складних понять у інтерактивному середовищі

знижує рівень абстракції та спрощує розуміння. Конструктивістський підхід у навчанні підкреслює важливість діяльної компоненти – студенти краще засвоюють знання, коли самостійно взаємодіють із навчальним середовищем. AR/VR-застосунки на Unity дають змогу поєднувати обидва підходи, роблячи процес навчання більш гнучким і продуктивним. Далі наведений графік з дослідження про використання AR та VR в освіті.

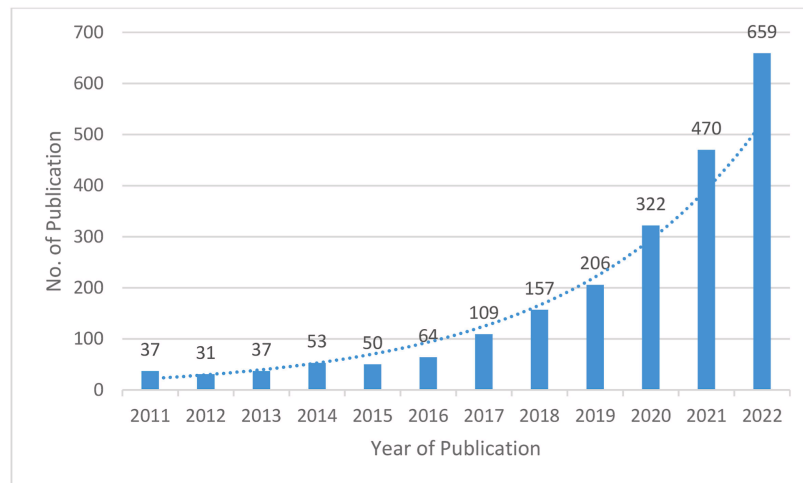


Рисунок 1 – Розподіл документів за роками використання віртуальної та доповненої реальності в освіті з 2011 по 2022 роки [4].

Практика застосування AR та VR у навчанні показує, що вони особливо ефективні у медичній освіті (віртуальні операційні зали), інженерії (симуляція робочих процесів), історії (віртуальні тури), архітектурі та дизайні (візуалізація проектів). Використання Unity як рушія для створення таких програм має теоретичне обґрунтування у вигляді універсальності, масштабованості та підтримки найсучасніших апаратних платформ. Далі у вигляді діаграми представлені різні галузі науки, що охоплюють VR та AR.

Дослідження останніх років підтверджують системне зростання інтересу до використання AR та VR в освітніх середовищах. Espinoza Castro та співавт. (2025) проаналізували рівні занурення у VR та їхній вплив на якість навчання, що підтверджує доцільність створення різних освітніх сценаріїв з урахуванням глибини інтерактивності.

Таким чином, Unity виступає не лише інструментом для розробки ігор, але й потужним освітнім середовищем, яке дає змогу впроваджувати нові педагогічні моделі. Теоретичний аналіз показує, що завдяки модульності, кросплатформеності та інтеграції з технологіями AR/VR Unity забезпечує фундамент для створення освітньо-ігрових програм нового покоління. Це відкриває перспективи для подальших досліджень у напрямку оптимізації інтерактивних навчальних середовищ і розробки методологій, що поєднують педагогічну ефективність і технологічну інноваційність.

Список використаних джерел:

1. Billinghamurst, M., Clark, A., & Lee, G. (2015). A Survey of Augmented Reality. *Foundations and Trends in Human-Computer Interaction*, 8(2-3), 73–272. <https://doi.org/10.1561/11000000049>
2. Radianti, J., Majchrzak, T. A., Fromm, J., & Wohlgenannt, I. (2020). A Systematic Review of Immersive Virtual Reality Applications for Higher Education: Design Elements, Lessons Learned, and Research Agenda. *Computers & Education*, 147, 103778. <https://doi.org/10.1016/j.compedu.2019.103778>
3. Unity Technologies. (2024). Unity Manual. <https://docs.unity3d.com/>
4. Al-Ansi, A. M. (2023). Analyzing augmented reality (AR) and virtual reality (VR) development in education: A comprehensive review. *Journal of Educational Technology & Society*. <https://doi.org/10.1016/j.ssaho.2023.100532>
5. Espinoza Castro, K. E., Gaona Pineda, J. S., Apolo Buenaño, D. E., & Plaza Chalco, J. L. (2025). *Levels of Virtual Reality Immersion and their Use in Education: A Systematic Literature Review*. *International Journal of Learning, Teaching and Educational Research*, 24(4), 354–369. <https://doi.org/10.26803/ijlter.24.4.17>

УДК 004.41

Кулалаєв Н. А.

здобувач вищої освіти,

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

Науковий керівник

Ковальчук Д.М.

PhD, старший викладач кафедри інформаційних технологій

та математичного моделювання

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ДОСЛІДЖЕННЯ ВПЛИВУ ГНУЧКИХ МЕТОДОЛОГІЙ НА ЕФЕКТИВНІСТЬ ПРОЦЕСУ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У сучасних умовах швидкого розвитку інформаційних технологій ефективність процесу розробки програмного забезпечення стає одним із ключових факторів успіху компаній на ринку. Програмні продукти мають відповідати високим вимогам користувачів, швидко адаптуватися до змін бізнес-середовища, підтримувати масштабованість та стабільність роботи. Традиційні підходи до розробки, зокрема каскадна модель, поступово втрачають свою актуальність у зв'язку з низькою гнучкістю та складністю адаптації до нових вимог. На зміну їм прийшли гнучкі методології (Agile), які орієнтовані на швидке реагування на зміни, тісну співпрацю з замовниками та забезпечення цінності продукту на кожному етапі життєвого циклу [1]. У даній роботі розглянемо вплив гнучких методологій на ефективність процесу розробки

програмного забезпечення, окреслимо їхні переваги, недоліки та перспективи подальшого використання.

Гнучкі методології є результатом пошуку альтернативи жорстким і формалізованим підходам, які не завжди відповідали динаміці сучасних проєктів. У 2001 році було опубліковано «Маніфест Agile», що став своєрідною відправною точкою для широкого розповсюдження цих методологій. Основними принципами Agile є орієнтація на людей і взаємодію, створення працюючого програмного продукту, співпраця із замовником та готовність реагувати на зміни. На практиці ці принципи реалізуються у таких підходах, як Scrum, Kanban, Extreme Programming (XP), Lean Software Development тощо [1-2].

Одним із найважливіших впливів гнучких методологій на ефективність є підвищення швидкості створення програмного забезпечення. Завдяки ітеративному підходу розробники можуть випускати проміжні версії продукту (інкременти), які відразу ж тестуються і отримують оцінку від замовника. Це дозволяє швидко виявляти недоліки та вносити зміни без значних витрат часу й ресурсів. У традиційних моделях розробки виявлення помилок на пізніх етапах часто призводило до затримок і значного перевищення бюджету [1, 3].

Ще одним важливим аспектом є покращення комунікації всередині команди та із зовнішніми стейкхолдерами. У рамках Agile організовуються регулярні зустрічі (daily meetings, sprint reviews, retrospectives), які забезпечують постійний обмін інформацією та контроль за ходом проєкту. Це підвищує прозорість процесу, сприяє зростанню довіри між розробниками й замовником та дозволяє знизити ризики непорозумінь. У результаті створюється програмне забезпечення, яке максимально відповідає потребам користувачів.

Гнучкі методології також позитивно впливають на мотивацію команди. У традиційних моделях часто домінувала сувора ієрархія, де розробники виконували лише конкретні завдання без можливості впливати на процес ухвалення рішень. У Agile передбачена саморганізація команд: учасники спільно визначають пріоритети, планують завдання і відповідають за кінцевий результат. Це підвищує рівень відповідальності, стимулює творчий підхід та розвиток професійних навичок [3-4].

Водночас не можна стверджувати, що гнучкі методології є універсальним вирішенням усіх проблем у розробці. Їх ефективність залежить від особливостей проєкту, розміру команди та культури організації. Наприклад, у великих компаніях, де необхідна сувора регламентація процесів і документації, впровадження Agile може супроводжуватися труднощами. Крім того, висока гнучкість іноді призводить до ризику постійних змін у вимогах, що може затягнути процес розробки та збільшити витрати.

Ще одним викликом є потреба у високій кваліфікації членів команди. Agile вимагає не лише технічних навичок, а й умінь ефективно комунікувати, працювати у динамічному середовищі та приймати швидкі рішення. Якщо команда не готова до таких умов, ефективність може знижуватися. Таким чином, для досягнення успіху необхідне поступове впровадження гнучких практик, навчання персоналу та створення відповідної корпоративної культури.

Важливою перевагою Agile є орієнтація на задоволення кінцевого користувача. Програмний продукт створюється не за абстрактними технічними вимогами, а на основі реальних потреб і зворотного зв'язку від клієнтів. Це дозволяє підвищити конкурентоспроможність продукту, скоротити час виходу на ринок (time-to-market) та збільшити прибутковість компанії. Для бізнесу це означає швидше реагування на зміни ринкової кон'юнктури та більш ефективне використання ресурсів [2, 4].

У сучасних дослідженнях відзначається, що Agile сприяє зменшенню кількості дефектів у програмному забезпеченні завдяки регулярному тестуванню та інтеграції. Практика безперервної інтеграції (Continuous Integration) та безперервної доставки (Continuous Delivery), яка часто використовується разом із гнучкими методологіями, дозволяє своєчасно виявляти проблеми та забезпечувати стабільність продукту. Це особливо важливо для великих і складних систем, де помилки можуть призвести до значних фінансових втрат.

Отже, аналіз впливу гнучких методологій на ефективність процесу розробки програмного забезпечення свідчить, що вони дійсно змінюють підхід до управління проєктами, орієнтуючи команди на гнучкість, швидкість і результативність. Agile забезпечує зменшення ризиків, підвищує якість продукту, покращує комунікацію та мотивацію команди, а також сприяє кращому задоволенню потреб замовника. Водночас ефективність застосування цих методологій залежить від низки факторів: розміру організації, специфіки проєкту, рівня підготовки фахівців та корпоративної культури.

У перспективі гнучкі методології, ймовірно, і надалі будуть удосконалюватися та інтегруватися з іншими підходами, такими як DevOps, що дозволить ще більше підвищити ефективність процесів розробки. Зростаюча складність програмних систем і вимоги до швидкої адаптації вимагають саме таких підходів, які поєднують технічні інновації з ефективною організацією роботи команд. Тому Agile можна розглядати як один із найважливіших інструментів сучасної індустрії програмного забезпечення, що формує нові стандарти розробки та управління проєктами.

Список використаних джерел:

1. Фендьо О. Управління ІТ-проєктами з використанням гнучких методологій Agile, Scrum, Kanban // Дистанційна освіта в Україні: інноваційні, нормативно-правові, педагогічні аспекти. – 2023. – Т. 1, № 2. – С. 419–425.
2. Дегтярьова Л. М., Гроза П. М., Сомов С. В. Технології розробки програмного забезпечення: навчальний посібник для студентів спеціальності «Комп'ютерна інженерія». Полтавський національний технічний університет, 2017. – 218 с.
3. Леонова Т. Особливості впровадження agile-методології в управлінні на підприємствах морського транспорту України // Розвиток методів управління та господарювання на транспорті. – 2025. – № 2(91). – С. 153–164. <https://doi.org/10.31375/2226-1915-2025-2-153-164>.

4. Шапошнікова О.П., Кірвас В.В. Застосування методології Agile в практиці проектного навчання при підготовці ІТ спеціалістів. Системи обробки інформації. 2020. № 4(163). С. 94-100. <https://doi.org/10.30748/soi.2020.163.10>.

УДК 004.65

Липченко І. В.

*здобувач вищої освіти другого рівня,
Сумський національний аграрний університет*

ВИСОКОДОСТУПНА АРХІТЕКТУРА МІКРОСЕРВІСІВ У KUBERNETES

У нинішніх умовах цифрової трансформації бізнесу та освіти вимоги до стійкості систем та їхньої доступності різко зросли. Будь-яка помилка у роботі сервісу здатна спричинити фінансові збитки, зниження довіри споживачів і порушення ключових бізнес-процесів. Тому розробка архітектур, які гарантовано підтримуватимуть безперервну роботу навіть при відміні окремих компонентів, стає надзвичайно важливою.

Kubernetes, як платформа для оркестрації контейнерів, надає потужний арсенал засобів для створення високодоступних мікросервісних рішень. Завдяки механізмам реплікації, автоматичного відновлення та географічного резервування можна конструювати системи, що відповідають сучасним стандартам надійності.

У світовій науковій та технічній літературі активно вивчаються підходи до розробки fault-tolerant архітектур у Kubernetes. У працях К. Hightower, В. Burns, J. Beda викладено основи застосування Kubernetes для забезпечення масштабованості та надійності. Приклади від провідних хмарних провайдерів (AWS, Google Cloud, Microsoft Azure) демонструють стратегії використання кластерів у кількох AZ, систем резервного копіювання та планів аварійного відновлення (Disaster Recovery). Проте в українській науковій літературі питання створення катастрофостійких рішень у Kubernetes ще недостатньо розгорнуті, що підкреслює актуальність нашого дослідження.

Високодоступна архітектура мікросервісів у Kubernetes спирається на поєднання декількох основних підходів:

Копіювання сервісів. Для безстанних (stateless) додатків використовують об'єкти Deployment, що створюють кілька однакових копій сервісу. Такий підхід забезпечує автоматичне перенаправлення навантаження на інші поди при відмові одного з них.

У випадку сервісів зі станом (stateful) доцільно застосовувати StatefulSet, який гарантує постійні ідентифікатори і зберігання даних у персистентних томах. Клонування баз даних, кешів або брокерів повідомлень (наприклад, PostgreSQL, Redis, Kafka) дозволяє запобігти втраті даних і зберегти цілісність системи.

Стратегії відновлення після збоїв. Kubernetes включає в себе механізми самовідновлення (self-healing). Коли под завершує роботу з помилкою або вузол перестає бути доступним, система сама перезапускає контейнер або переносить навантаження на інший вузол.

Крім того, Kubernetes підтримує різні підходи до оновлення додатків: Rolling Update (поетапне оновлення без простою) та Blue-Green Deployment (одночасне функціонування старої та нової версій для плавного переходу). Це дозволяє знизити ризики під час розгортання нових релізів.

Забезпечення катастрофостійкості. Для підвищення надійності інфраструктури критично важливо застосовувати кластери в декількох зонах доступності (multi-AZ). Тобто вузли Kubernetes розташовуються у різних дата-центрах або регіонах. При відмові одного дата-центру інші продовжують обслуговувати користувачів.

Для ключових систем впроваджуються стратегії Disaster Recovery (DR), що передбачають регулярне резервне копіювання (backup), використання інструментів типу Velero для відновлення кластерів і розробку сценаріїв відмовостійкості.

Моніторинг і превентивний контроль. Інтеграція з Prometheus та Grafana дає можливість збирати метрики доступності, навантаження та використання ресурсів, що забезпечує швидке виявлення аномалій і оперативне реагування на можливі збої.

Налаштування алертів і SLA (Service Level Agreement) допомагає точно контролювати відповідність роботи сервісу встановленим показникам.

Автоматизація та IaC (Infrastructure as Code). Для ефективного керування інфраструктурою використовують Helm Charts та Terraform, що уніфікують процес розгортання і мінімізують людський фактор. Автоматизація спрощує швидке відновлення кластера у випадку масштабних збоїв.

Досягнення високої доступності мікросервісів у Kubernetes вимагає всебічного підходу, який поєднує реплікацію сервісів, механізми самовідновлення, географічне резервування та автоматизацію управління інфраструктурою. Використання зазначених принципів дозволяє знизити вплив відмов, забезпечити безперервність бізнес-процесів і підвищити довіру користувачів до ІТ-систем.

Список використаних джерел:

1. Amazon Web Services. Amazon Elastic Kubernetes Service (EKS) URL: <https://docs.aws.amazon.com/eks>
2. Hightower K., Burns B., Beda J. Kubernetes: Up and Running. – 3rd ed. – Sebastopol, CA : O'Reilly Media, 2021. – 350 p.
3. Kubernetes Documentation URL: <https://kubernetes.io>
4. Velero. Disaster recovery for Kubernetes URL: <https://velero.io>

ІНДУСТРІАЛЬНІ ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ: АКТУАЛЬНІ ТРЕНДИ ТА ПЕРЕХІД ДО AUTOML У МАСШТАБАХ 2025 – 2030 РОКІВ

Штучний інтелект остаточно перестав бути явищем, притаманним лише науковій фантастиці. Сьогодні він трансформує світову економіку та повсякденне життя, стаючи ключовим фактором інноваційного розвитку. Одним із провідних напрямів ШІ є машинне навчання (Machine Learning, ML), яке забезпечує автономне навчання комп'ютерних систем та здатність обробляти великі обсяги даних без чітко прописаних алгоритмів.

Упродовж останніх років сфера ML демонструє динамічний розвиток. За даними Statista, у 2024 році глобальний ринок рішень машинного навчання оцінювався в \$204,3 млрд, а до 2030 року його обсяг прогнозовано зросте більш ніж удвічі – до \$528 млрд із середньорічним темпом розвитку близько 17 %. Це свідчить про масштабні трансформації, що охоплюють широкий спектр індустрій [1,2].

Технології машинного навчання сьогодні охоплюють практично всі сфери, де необхідна аналітика великих обсягів даних і прогнозування. Найбільші інвестиції спрямовані у виробництво (18,88 %), фінансовий сектор (15,42 %) та охорону здоров'я (12,23 %). Важливу роль відіграють транспортні перевезення (10,63 %), системи безпеки (10,10 %), бізнес та юридичні послуги (9,86 %). Також зростає застосування ML у сфері енергетики (5,58 %), медіа та розваг (5,19 %), роздрібно́ї торгівлі (4,67 %). Частка інших напрямів складає 5,83 %, а використання у напівпровідниковій індустрії – 1,61 % (рис.1).

Приклади сучасних застосувань ML охоплюють гіперперсоналізований маркетинг і рекомендаційні системи, автоматизацію бізнес-процесів в ERP-середовищах, комп'ютерний зір та предиктивне обслуговування обладнання, діагностику медичних знімків, а також фрод-моніторинг у фінансовій сфері.

Машинне навчання відкрило для медицини можливості, які ще десятиліття тому вважалися фантастичними. Сьогодні моделі ML застосовуються для аналізу рентгенівських та МРТ-знімків, діагностики, обробки клінічних даних та підтримки прийняття рішень. Відомим прикладом є проєкт *Microsoft InnerEye*, що використовує алгоритми комп'ютерного зору для виявлення пухлин на 3D-знімках. Додатково ML сприяє прориву у генетиці та

фармакології: у 2023 році дослідники МІТ вперше за 60 років відкрили нові антибіотики завдяки алгоритмам машинного навчання [4].

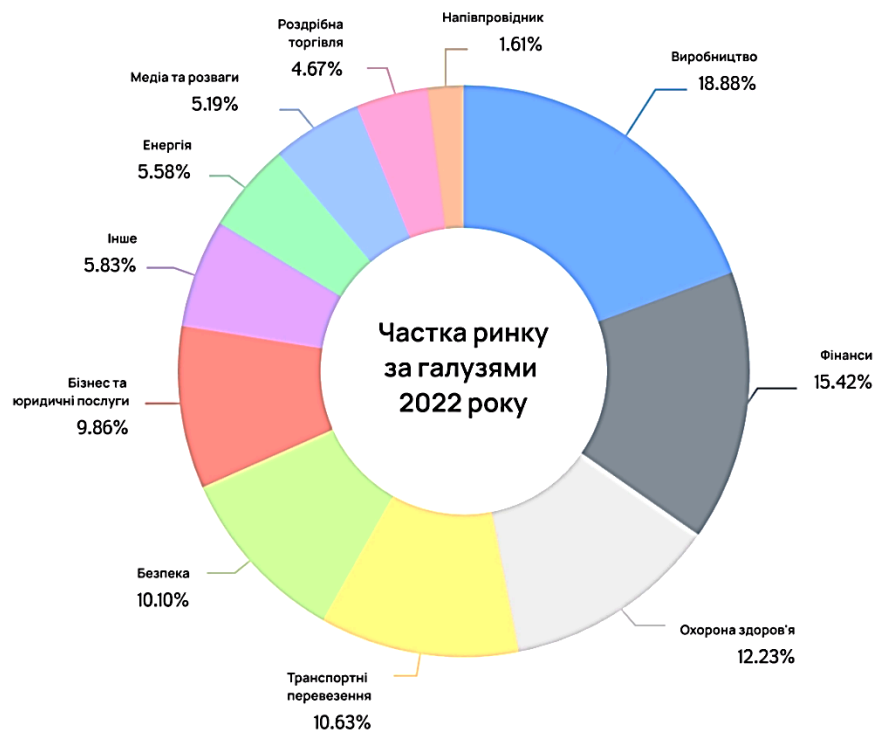


Рис. 1. Частка ринку застосувань ML за галузями у 2022 році
Джерело: побудовано автором за даними [5]

У фінансовій сфері ML є ключовою складовою FinTech. Алгоритми застосовуються для кредитного скорингу, управління ризиками, фрод-моніторингу та автоматизації операцій. Прогнози свідчать, що до 2030 року штучний інтелект та ML дозволять світовому банківському сектору заощаджувати близько \$1 трлн щорічно. Показовим прикладом є використання системи кібербезпеки *Falcon* у банку *Greenhill*, що скоротило кількість хибних тривог на 75 % і забезпечило щорічну економію понад \$300 тис [3].

У роздрібній торгівлі машинне навчання забезпечує точне прогнозування попиту, персоналізований маркетинг, оптимізацію ланцюгів постачання та роботизацію процесів. Провідні корпорації (*Amazon*, *Walmart*, *Alibaba*) довели ефективність таких рішень: за даними *Precedence Research*, ринок III-рішень у ритейлі у 2024 році складав \$11,8 млрд і до 2032 року зросте до \$45,7 млрд [5].

У виробництві ML застосовується для автоматизованого контролю якості та предиктивного обслуговування обладнання. Так, компанія *Siemens* оснащує газові турбіни сотнями сенсорів, дані з яких обробляються алгоритмами машинного навчання для оптимізації робочих режимів. Це підвищує безпеку й ефективність виробничих процесів.

Транспорт і логістика використовують ML для оптимізації маршрутів, підвищення ефективності перевезень і моніторингу безпеки. Поштовий оператор *UPS* впровадив інструменти прогнозової аналітики, що дозволило скоротити обсяг робочих годин на 10 % завдяки адаптації до зміни попиту у 2023 році.

В енергетиці алгоритми ML сприяють розвитку «розумних» мереж, прогнозуванню попиту та розвитку відновлюваних джерел. Ініціатива *SunShot* у США довела ефективність використання ML у прогнозуванні сонячної активності, що підвищило точність прогнозів на 30 % та сприяло зниженню вартості сонячної енергії на 75 % [5].

Отже, машинне навчання стає не лише технологічним інструментом, а й рушійною силою глобальних змін. Його подальший розвиток визначатиметься зростанням попиту на AutoML-рішення, поширенням глибокого навчання та інтеграцією з інтелектуальними системами реального часу. Це підкреслює необхідність подальших досліджень як у технологічному, так і в соціально-економічному вимірах.

Список використаних джерел:

1. Russell S., Norvig P. *Artificial Intelligence: A Modern Approach*. – 4th ed. – Pearson, 2021. – 1136 p.
2. Topol E. *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*. – Basic Books, 2019. – 400 p.
3. Rajpurkar P., Chen E., Banerjee O., Topol E. AI in health and medicine. // *Nature Medicine*, 2022. – Vol. 28. – P. 31–38. doi: <https://doi.org/10.1038/s41591-021-01614-0>
4. MIT News. Machine learning identifies new antibiotics. – 2020. – URL: <https://news.mit.edu/2020/machine-learning-antibiotic-discovery-0220>
5. Wezom. Майбутнє машинного навчання: індустрії та тренди. – URL: <https://wezom.com.ua/ua/blog/maybutnje-mashinnogo-navchannya-industriyi-ta-tren-di>

Макарова Г.В.,

*доцент кафедри інформаційних технологій та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна*

Артемчук А.В.

здобувач вищої освіти

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

РОЗРОБКА ТА ДОСЛІДЖЕННЯ TELEGRAM-БОТА ДЛЯ ОРГАНІЗАЦІЇ СПОРТИВНИХ ЗАХОДІВ

У сучасному середовищі організація спортивних заходів стикається з рядом викликів: неоднорідні канали комунікації, складність централізованої реєстрації учасників, проблеми зі сповіщеннями та координацією. Багато клубів та соціальних груп використовують месенджери, зокрема Telegram, для обміну інформацією — однак без спеціалізованого інструменту багато процесів залишаються ручними і неефективними. Це обґрунтовує актуальність теми «Розробка та дослідження Telegram-бота для організації спортивних заходів».

Мета цієї розробки полягає в створенні Telegram-бота, який забезпечить автоматизацію ключових процесів у підготовці та проведенні спортивних заходів, а також дослідження його ефективності з точки зору зручності використання організаторами та учасниками.

Проводячи аналіз існуючих аналогів і систем, які використовують Telegram-ботів для організації заходів або управління групами, ми зрозуміли, що складові реалізації повинні дозволяти виконувати наступні дії:

- створювати ігри з точним часом,
- керувати списком учасників,
- автоматично рахувати кількість учасників,
- формувати команди.

Розглядаючи існуючі проєкти на GitHub, ми побачили, що вони дозволяють обмежувати кількість учасників, підтримувати резервних учасників і вести статистику, надихають на вибір функціоналу.

Тому для розробляемого нами бота ми розглядаємо:

- визначення вимог до подібних ботів і найкращі практики;
- проектування системи, що включатиме модель даних (база даних учасників, заходів), архітектуру бота (команди, взаємодії, інтерфейс користувача), а також визначення технологій (наприклад, Python + бібліотеки такі як aiogram чи python-telegram-bot,);
- реалізація бота: функції реєстрації учасників, формування заходів, автоматичне повідомлення (нагадування), управління списками (основний, резервний), можливість редагувати чи відмінити події;
- тестування та апробація на реальному спортивному заході чи серії заходів, збирання відгуків від користувачів-організаторів і учасників;

— оцінка ефективності, за кількісними критеріями (час реєстрації, кількість учасників, кількість помилок, відсоток підтверджень участі), і якісними (задоволення користувачів, зручність, простота використання).

Очікується, що результатом роботи стане Telegram-бот, що значно спростить організацію спортивних заходів: зменшення часу на адміністративні завдання, зниження кількості помилок у реєстрації чи нагадуваннях, покращення комунікації між організаторами та учасниками. Крім того, буде виділено рекомендації щодо подальшого розвитку (наприклад, розширення функціоналу, інтеграція з календарями чи геолокацією).

Список використаних джерел

1. Як створити бота в Телеграмі <https://hostiq.ua/blog/ukr/chatbot-telegram/>
2. Як створити чат-бот у Telegram https://sendpulse.ua/knowledge-base/chatbot/telegram/create-telegram-chatbot?utm_source=chatgpt.com
3. Вебхуки та методи Long Polling для розміщення бота Telegram https://cit.lntu.edu.ua/index.php/cit/article/view/397?utm_source=chatgpt.com

УДК 004.5

Макарова Г.В.,

*доцент кафедри інформаційних технологій та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна*

Орешко Д.В.

*здобувач вищої освіти
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна*

ІНТЕЛЕКТУАЛЬНИЙ МОБІЛЬНИЙ ЗАСТОСУНОК ДЛЯ АДАПТИВНИХ ТРЕНУВАНЬ

У сучасному світі значна частина повсякденного життя людей проходить у малорухливому режимі: робота за комп'ютером, використання мобільних пристроїв та транспорт для пересування зменшують рівень фізичної активності. Наслідками гіподинамії є погіршення фізичної витривалості, порушення обміну речовин, зростання ризику ожиріння та серцево-судинних захворювань. У цих умовах особливого значення набуває регулярна фізична активність, яка дозволяє підтримувати здоров'я та високу працездатність.

Проте неконтрольовані тренування без урахування індивідуальних особливостей організму можуть призводити до перевтоми, травм або відсутності очікуваного результату.

Сучасний розвиток цифрових технологій відкриває нові можливості для вирішення цієї проблеми. Використання мобільних застосунків у поєднанні з носимими пристроями (смарт-годинники, фітнес-браслети) дозволяє здійснювати постійний моніторинг фізіологічних показників користувача у

реальному часі. Отримані дані можуть бути проаналізовані алгоритмами штучного інтелекту та аналітики даних, що робить можливим створення персоналізованих тренувальних програм із динамічною корекцією навантаження.

Запропонований мобільний застосунок має на меті поєднати можливості збору даних, їхньої інтелектуальної обробки та практичного застосування для організації ефективних тренувань. Його функціональні можливості передбачають:

- збір даних про користувача (вага, зріст, вік, рівень фізичної підготовки, досвід тренувань, пульс, тривалість та якість сну, харчування);
- аналіз фізичних можливостей із використанням алгоритмів машинного навчання та прогнозування оптимальних навантажень;
- формування індивідуального плану занять, що включає кількість повторень, підходів, тривалість відпочинку, інтенсивність вправ;
- адаптацію тренувань у реальному часі залежно від пульсу, швидкості чи ваги під час виконання вправ, що дозволяє уникати перевантаження;
- розрахунок оптимальної гідратації – визначення необхідної кількості води для підтримки водного балансу під час інтенсивних занять;
- аналіз після тренування: формування статистики, прогноз покращення результатів, рекомендації щодо наступних занять.

Для технічної реалізації передбачається застосування технологій Big Data для обробки великих масивів інформації, алгоритмів машинного навчання та прогнозної аналітики для визначення оптимальних параметрів навантаження, а також інтеграція з API носимих пристроїв для збору фізіологічних показників у режимі реального часу.

Використання такого застосунку забезпечить низку переваг:

- індивідуальний підхід до формування тренувальних програм;
- зменшення ризику перевантаження та травм;
- ефективний контроль прогресу та постійний моніторинг стану організму;
- підвищення мотивації користувачів завдяки зручному доступу до персоналізованих рекомендацій;
- популяризацію здорового способу життя серед широких верств населення.

Таким чином, запропонований мобільний застосунок поєднує сучасні технології обробки даних та практичні потреби користувачів, створюючи ефективний інструмент для адаптивних тренувань. Його впровадження дозволить оптимізувати процес фізичної активності, зробити його безпечнішим та результативнішим, а також сприятиме збереженню здоров'я та підвищенню якості життя в умовах цифрової епохи.

Список використаних джерел

1. World Health Organization. Physical activity. — <https://www.who.int/news-room/fact-sheets/detail/physical-activity>

2. Lee I.-M., Shiroma E.J., Lobelo F., et al. Effect of physical inactivity on major non-communicable diseases worldwide: an analysis of burden of disease and life expectancy. *The Lancet*. 2012; 380(9838): 219–229.

3. Bunn J.A., Navalta J.W., Fountaine C.J., Reece J.D. Current State of Commercial Wearable Technology in Physical Activity Monitoring 2015–2017. *Int J Exerc Sci*. 2018; 11(7): 503–515.

4. Piwek L., Ellis D.A., Andrews S., Joinson A. The Rise of Consumer Health Wearables: Promises and Barriers. *PLoS Med*. 2016; 13(2): e1001953.

УДК 004.5

Макарова Г.В.,

*доцент кафедри інформаційних технологій та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна*

Пархоменко О.А.,

*здобувач вищої освіти
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна*

ВИКОРИСТАННЯ СУЧАСНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ У СФЕРІ ОСВІТИ І НАУКИ

Сучасна освіта та наука переживають етап стрімкої цифровізації, що безпосередньо пов'язано з розвитком інформаційно-комунікаційних технологій, штучного інтелекту, аналітичних платформ та хмарних сервісів. Перехід великої частини навчального та наукового процесу у цифрову площину дозволяє не лише значно підвищити ефективність обробки даних та обміну інформацією, але й сприяє глобалізації знань, дистанційному доступу до освітніх ресурсів і персоналізації навчання. Однією з ключових проблем сучасної освіти є адаптація навчального процесу до швидкозмінних технологічних реалій та забезпечення високої якості освітніх результатів у умовах великого обсягу інформації.

Цифрові технології відкривають нові можливості для організації навчання та наукових досліджень. Онлайн-платформи та системи дистанційного навчання, такі як Moodle, Canvas чи Google Classroom, забезпечують інтерактивну взаємодію між викладачами та студентами, дають змогу проводити лекції, тестування та колаборативні проєкти без прив'язки до фізичного простору. При цьому методи Learning Analytics та Data Mining дозволяють збирати та аналізувати інформацію про прогрес студентів, ефективність навчальних програм та особливості наукових досліджень, що дає змогу оптимізувати процеси та приймати обґрунтовані управлінські рішення.

Використання сучасних цифрових технологій у науковій діяльності дозволяє прискорювати обробку великих масивів даних, аналіз

експериментальних результатів, моделювання складних систем та візуалізацію інформації.

Переваги впровадження цифрових технологій у освіту та науку очевидні. По-перше, вони забезпечують швидкий та зручний доступ до знань і наукових ресурсів, відкриваючи можливості дистанційного навчання та міжнародної колаборації. По-друге, автоматизація рутинних процесів і аналіз великих масивів даних дозволяє знизити навантаження на викладачів і дослідників, звільняючи час для творчої та методологічної роботи. По-третє, цифрові інструменти підтримують індивідуалізацію навчання, враховують рівень підготовки студента та його темп засвоєння матеріалу, що підвищує мотивацію та ефективність навчального процесу.

Водночас використання цифрових технологій супроводжується певними викликами. До них належать потреба у високому рівні цифрової компетентності користувачів, ризики пов'язані з конфіденційністю та безпекою персональних даних, а також залежність від стабільного інтернет-з'єднання та цифрової інфраструктури. Особлива увага повинна приділятися контролю якості автоматизованих систем, оскільки некоректне або неповне оброблення даних може призводити до помилкових висновків і неправильного планування освітніх і наукових процесів.

У контексті практичного застосування цифрових технологій у сфері науки, нами розробляється спеціальний модуль для розміщення навчальних матеріалами. Модуль дозволяє централізовано зберігати та організовувати різні типи матеріалів: документи, презентації, відео та інтерактивні ресурси, а також забезпечує зручний доступ до них для людей котрі хочуть отримати доступ до матеріалу та відповідно розробники самих матеріалів.

Основний функціонал модуля включає:

1. Завантаження та організація матеріалів — користувачі можуть додавати нові ресурси, групувати їх за темами та рівнями складності.
2. Пошук і фільтрація — реалізовано можливість швидкого пошуку матеріалів за ключовими словами, предметами або категоріями, а також застосування фільтрів для зручного доступу до потрібних ресурсів.
3. Персоналізація доступу — система дозволяє призначати рівні доступу для користувачів, що забезпечує безпечну роботу з контентом та контроль за його використанням.
4. Візуалізація та попередній перегляд — користувачі можуть попередньо ознайомлюватися з матеріали без завантаження, отримуючи швидкий доступ до необхідної інформації та заощаджуючи особистий час під час пошуку потрібної інформації.
5. Аналітика використання — збір даних про перегляди, завантаження та активність користувачів дозволяє оцінювати ефективність матеріалів та оптимізувати пошук для користувачів.

Розробка такого модуля демонструє практичне впровадження сучасних цифрових технологій у освітню сферу, підвищує ефективність обміну унікальною інформацією, відповідаючи сучасним потребам цифрової трансформації освіти.

Підсумовуючи, можна констатувати, що сучасні цифрові технології формують нові стандарти у сфері освіти та науки, сприяють підвищенню ефективності навчання і наукових досліджень, забезпечують доступність знань у глобальному масштабі та створюють умови для індивідуалізованого і творчого підходу до навчання та наукової роботи. Для повноцінного використання цих можливостей необхідна стратегія інтеграції цифрових інструментів, підготовка персоналу та постійне оновлення технологічної інфраструктури, що дозволить забезпечити стійкий розвиток освіти і науки в умовах цифрової трансформації.

Список використаних джерел

1. "The NMC Horizon Report: 2023 Higher Education Edition" (Johnson et al., 2023). URL: <https://eric.ed.gov/?id=ED559358&>
2. "Language Models are Few-Shot Learners" (Brown et al., 2020). URL: <https://arxiv.org/abs/2005.14165>
3. "Learning Analytics Dashboards: Emerging Themes in Design and Implementation". URL: <https://link.springer.com/article/10.1007/s10639-023-12401-4>

УДК 338.124:332.1(477)

Маніта А.С.

здобувач вищої освіти,

Вінницький національний аграрний університет

Томашук І.В.

PhD, доцент, доцент кафедри економіки та підприємницької діяльності

Вінницький національний аграрний університет

ВПЛИВ ІННОВАЦІЙ НА ІНВЕСТИЦІЙНУ ПРИВАБЛИВІСТЬ РЕГІОНІВ УКРАЇНИ

Роль інновацій у розвитку регіонів України є стратегічною і багатогранною. Впровадження новітніх технологій, сучасних управлінських практик та інноваційних моделей ведення бізнесу сприяє підвищенню продуктивності виробництва, покращенню якості послуг і товарів, а також оптимізації використання ресурсів [1]. Інновації стимулюють економічне зростання регіонів, залучення інвестицій та розвиток малих і середніх підприємств, створюючи нові робочі місця та сприяючи покращенню соціально-економічного становища населення. Крім того, інноваційний розвиток регіонів формує конкурентні переваги на національному та міжнародному рівні, зміцнює їхню інвестиційну привабливість і забезпечує умови для сталого та екологічно безпечного розвитку.

Інновації є одним із ключових факторів формування інвестиційної привабливості регіонів, оскільки вони підвищують ефективність виробництва, сприяють впровадженню сучасних технологій та створюють додаткові

можливості для розвитку бізнесу. Регіони, які активно стимулюють інноваційну діяльність, залучають більше інвестицій, оскільки інвестори віддають перевагу територіям із передбачуваним розвитком, високою продуктивністю та сучасною інфраструктурою [3]. Інноваційний розвиток включає впровадження цифрових рішень, розвиток стартапів, інтелектуальних підприємств та екологічно безпечних технологій, що підвищує конкурентоспроможність регіону на національному та міжнародному рівні [4]. Крім економічних ефектів, інновації стимулюють соціальний розвиток територій, підвищують зайнятість та рівень життя населення, створюючи сприятливий інвестиційний клімат. Дійсно, інноваційна активність стає стратегічним чинником, що визначає успішність регіонів у залученні інвестицій та забезпеченні сталого економічного розвитку [5].

Табл. 1 показує, що властивості інновацій у розвитку регіонів мають комплексний характер і охоплюють як економічні, так і соціальні та екологічні аспекти. Вони сприяють підвищенню продуктивності та ефективності регіональних підприємств, формуванню конкурентних переваг, залученню інвестицій і розвитку високотехнологічних секторів економіки. Одночасно інновації забезпечують адаптивність до змін ринкового середовища, інтеграцію технологічних та управлінських рішень, покращення соціальних стандартів і екологічної безпеки, що робить їх стратегічним чинником сталого розвитку регіонів.

Таблиця 1

Властивості інновацій у розвитку регіонів

Властивість інновацій	Опис впливу на розвиток регіонів
Продуктивність	Підвищують ефективність виробництва та економічну віддачу підприємств і регіону в цілому.
Конкурентоспроможність	Формують конкурентні переваги регіону на національному та міжнародному рівні.
Адаптивність	Дозволяють швидко реагувати на зміни ринкового середовища та економічні виклики.
Інвестиційна привабливість	Стимулюють залучення інвестицій завдяки передбачуваному розвитку та сучасній інфраструктурі.
Сталий розвиток	Сприяють екологічній безпеці та соціально-економічному розвитку регіону.
Трансформаційність	Викликають структурні зміни в економіці та управлінні регіональним розвитком.
Інтегративність	Поєднують технологічні, організаційні та управлінські інновації для комплексного розвитку.

Джерело: [3]

Табл. 2 демонструє різноманітність видів інвестицій, які відрізняються за формою, метою та рівнем участі інвестора у процесі. Прямі інвестиції забезпечують контроль та активну участь у підприємницькій діяльності, портфельні – дозволяють вкладати кошти у фінансові інструменти без управлінського впливу, а державні та приватні інвестиції стимулюють розвиток економіки і бізнесу регіону. Інноваційні та венчурні інвестиції спрямовані на

впровадження нових технологій і високоризикових перспективних проєктів, тоді як іноземні інвестиції сприяють притоку зовнішнього капіталу та інтеграції регіональної економіки у світові ринки. Таким чином, різні види інвестицій взаємодоповнюють один одного, формуючи комплексну основу для економічного та інноваційного розвитку регіонів.

Таблиця 2

Види інвестицій

Вид інвестицій	Основна характеристика	Приклади
Прямі інвестиції	Вкладання коштів безпосередньо у виробництво або підприємство з метою контролю та участі в управлінні	Купівля акцій компанії, створення нового заводу
Портфельні інвестиції	Вкладання коштів у фінансові інструменти без участі в управлінні	Акції, облігації, інвестиційні фонди
Державні інвестиції	Вкладання коштів державою для розвитку економіки та соціальної сфери	Будівництво інфраструктури, субсидії, гранти
Приватні інвестиції	Кошти приватних осіб або компаній для отримання прибутку	Інвестування у стартапи, бізнес-проекти
Інноваційні інвестиції	Вкладання коштів у науково-технічні розробки та нові технології	R&D, впровадження цифрових рішень, нові технології виробництва
Іноземні інвестиції	Капітал, залучений з-за кордону	Прямі інвестиції іноземних компаній, кредитування міжнародними організаціями
Венчурні інвестиції	Вкладання коштів у ризикові, але перспективні проєкти	Стартапи, високотехнологічні проєкти на ранніх стадіях

Джерело: [2, 6]

Табл. 3 показує основні напрями покращення впливу інновацій на інвестиційну привабливість регіонів України, зокрема розвиток інноваційної інфраструктури, фінансову підтримку проєктів, стимулювання приватних та іноземних інвестицій, підвищення кваліфікації кадрів та цифровізацію управління. Реалізація цих заходів сприяє зростанню інноваційної активності, залученню інвесторів та сталому економічному розвитку регіонів.

Таблиця 3

Пропозиції для покращення впливу інновацій на інвестиційну привабливість регіонів України

Напрямок покращення	Конкретні пропозиції	Очікуваний ефект
Розвиток інноваційної інфраструктури	Створення технопарків, інкубаторів стартапів, центрів трансферу технологій	Підвищення рівня інноваційної активності, залучення інвесторів
Фінансова підтримка інновацій	Надання грантів, субсидій, пільгових кредитів для	Збільшення кількості інноваційних проєктів, зростання інвестиційної привабливості

	впровадження нових технологій	
Стимулювання приватних та іноземних інвестицій	Податкові пільги, державне партнерство, спрощення регуляторних процедур	Залучення додаткового капіталу та високотехнологічних підприємств
Підвищення кваліфікації кадрів	Програми навчання та перепідготовки, співпраця з університетами та дослідницькими центрами	Створення компетентного персоналу для реалізації інноваційних проектів
Сприяння розвитку стартапів та інноваційних компаній	Менторські програми, конкурси стартапів, підтримка венчурних фондів	Зростання кількості інноваційних продуктів і послуг, підвищення привабливості регіону для інвесторів
Цифровізація управління та інфраструктури	Впровадження цифрових платформ для бізнесу та управління регіоном	Покращення прозорості, ефективності та привабливості регіону для інвесторів

Джерело: [6]

Інновації підвищують інвестиційну привабливість регіонів України, стимулюючи економічне зростання, розвиток високотехнологічних секторів та залучення інвесторів.

Список використаних джерел:

1. Олійник В., Топчієв О. Інвестиційно-інноваційна діяльність в регіонах України та показники її активності й інтенсивності. URL: <http://rp.onmu.org.ua/bitstream/handle/123456789/2230/1.Олійник%20В.%20Іннов.ц.-інвестиційна%20д-сть.pdf?sequence=1&isAllowed=y>
2. Скринник Н. В. Фактори впливу на інвестиційний клімат регіону. *Вісник Хмельницького національного університету*. 2010. № 5. Т. 4. С. 237-242. URL: https://journals.khnu.km.ua/vestnik/pdf/ekon/2010_5_4/237-242.pdf
3. Інноваційні підходи до регіонального розвитку в Україні: аналіт. доп. / С. О. Біла, Я. А. Жаліло, О. В. Шевченко, В. І. Жук [та ін.]; за ред. С. О. Білої. К. : НІСД. 2011. 80 с.
4. Tomashuk I. Features of formation and use of innovative potential of rural territories of Ukraine. *Slovak international scientific journal*. 2020. № 46. Vol. 2. P. 27-42
5. Tomashuk I.V., Tomashuk I.O. Enterprise development strategy: innovation and internal flexibility. *Colloquium-journal*. 2021. № 3 (90). Vol. 4. P. 51-66. DOI: 10.24412/2520-2480-2021-390-50-64
6. Кузьміна О. В., Ярошенко К. В. Інвестиційна привабливість України: оцінка та перспективні напрямки активізації. *Економіка та суспільство*. 2023. Вип. 49. DOI: <https://doi.org/10.32782/2524-0072/2023-49-38>

Матвеев Є. Е.
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Науковий керівник
Кобилін І.О.
к.т.н., асистент кафедри Інформатики,
Харківський національний університет радіоелектроніки

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ FACE ID ДЛЯ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Сучасне інформаційне середовище характеризується високою динамікою, фрагментарністю та алгоритмічною персоналізацією, що ускладнює побудову стабільних моделей доступу, орієнтованих виключно на хронологічний вік користувача, а технології автентифікації користувачів за допомогою біометричних методів стрімко розвиваються та знаходять застосування у фінансових, медичних і освітніх системах.

Водночас, з наукової точки зору, продуктивне розмежування має ґрунтуватися не лише на біологічному віці, а й на когнітивних, емоційних та соціальних характеристиках. Це передбачає перехід від статичних вікових категорій до динамічних профілів користувача, які формуються на основі поведінкових даних, історії взаємодії з контентом, рівня медіаграмотності та здатності до критичного мислення.

Також важливу роль грають наступні маркери: а саме контентна типологія, поведінкові маркери та динамічні профілі, бо в моменті роботи соціальної інженерії класичні елементи розмежування доступу до контенту більше не можуть ефективно опрацьовувати вхідні параметри і видавати коректний результат.

Тому у цьому контексті штучний інтелект починає більш високо оцінювати ризики і працювати у вигляді ключового інструмента семантичного аналізу, прогнозування ризиків та адаптації інформаційного середовища до індивідуальних потреб. А однією із найбільш найрозповсюджених і технологічно нейтральних і поширених технологій є використання 3D-сканування обличчя із подальшою перевіркою документів, що в свою чергу забезпечує високий рівень зручності та захисту даних у порівнянні з традиційними паролями, SMS-кодами, та перевіркою на вікові знання тієї чи іншої групи користувачів для зручності у таблиці 1 наведено таке порівняння:

Таблиця 1.

Порівняння методів автентифікації користувачів

Рівень	Механізм контролю	Технологічна складність	Етична чутливість	Точність і адаптивність	Контекст застосування
0	Базовий батьківський контроль	Низька	Нейтральна	Низька, статична	Домашнє середовище, початкова медіаосвіта
1	Вікові обмеження на платформах	Середня	Помірна	Середня, шаблонна	Масові сервіси, базова сегментація
2	AI-фільтрація контенту	Висока	Висока	Висока, адаптивна	Освітні платформи, соціальні мережі
3	Динамічні профілі користувача	Дуже висока	Висока	Дуже висока, персоналізована	Інтелектуальні освітні системи, гейміфіковані середовища
4	Біометрична верифікація віку	Дуже висока	Дуже чутлива	Висока, але з ризиком помилок	Банківські сервіси, медичні платформи, VR
5	Перевірка документів для доступу 3D-сканування	Екстремально висока	Максимальна	Максимальна, фізично підтверджена	Високоризикові середовища: кібербезпека, військові симулятори, deep-fake захист

Поєднання 3D-сканування обличчя у вигляді використання технології Face ID, та додаткова звірка документа дозволяє досягти балансу між безпекою та зручністю використання, водночас знижуючи ризик несанкціонованого доступу. То ж в ситуаціях розмежування контенту за віковими ознаками необхідно мати багатовимірну систему, що поєднає алгоритмічну адаптацію, етичну рефлексію та освітню інтервенцію.

Лише така комплексна модель здатна забезпечити не лише захист, а й розвиток користувача в умовах інформаційного перенасичення, а технічно досконалим модулем стає як раз використання архітектури модуля Face ID, що передбачає кілька основних етапів: зйомку обличчя користувача з перевіркою «живості», сканування офіційного документа, вилучення з нього даних (ім'я, прізвище, дата народження) за допомогою OCR/MRZ, а також подальше порівняння фото обличчя та текстових даних із інформацією, зазначеною при реєстрації. Узагальнений процес який дозволяє використання подано на схемі:

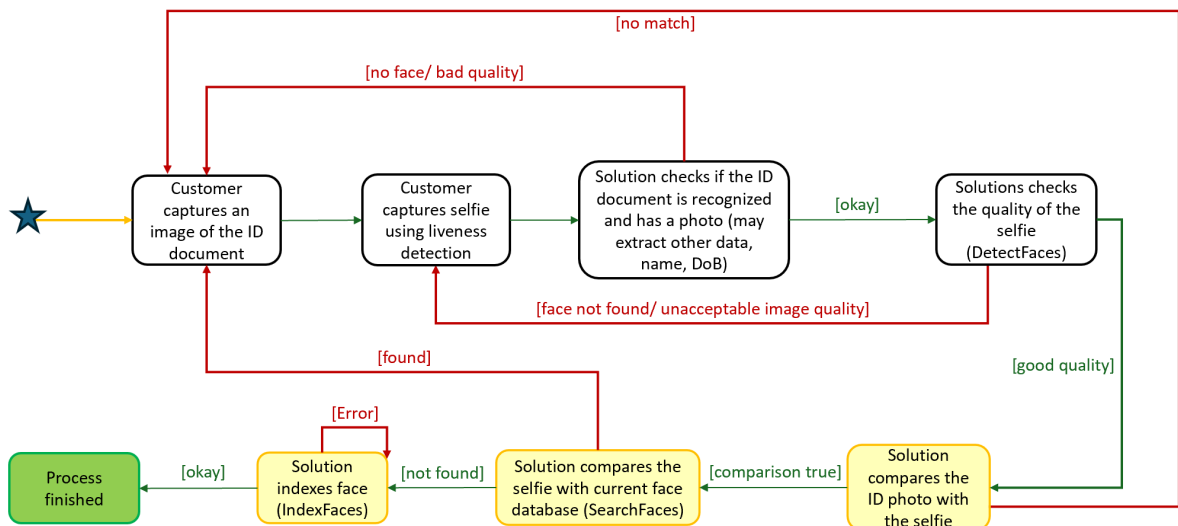


Рисунок 1 - Схема верифікації користувача за допомогою Face ID та документа

Тому впровадження Face ID у поєднанні з перевіркою документів поєднує у собі сучасні алгоритми комп'ютерного зору та вимоги до інформаційної безпеки. Подальший розвиток таких систем спрямований на вдосконалення методів перевірки «живості» та розширення інтеграції з іншими біометричними методами.

Такий підхід не лише відповідає принципам мінімізації даних, закладеним у GDPR, а й знижує ризики компрометації ідентичності. Таким чином, сучасні системи автентифікації мають еволюціонувати у напрямку контекстно-адаптивної, етично виваженої та технічно обґрунтованої архітектури, де безпека не суперечить приватності, а технології - не замінюють правову відповідальність.

Список використаних джерел:

1. arXiv. "DocFace: Matching ID Document Photos to Selfies." URL: <https://arxiv.org/abs/1805.02283>
2. Amazon Web Services, Inc. "ID + Selfie – Improving digital identity verification using AWS." URL: <https://aws.amazon.com/blogs/machine-learning/id-selfie-improving-digital-identity-verification-using-aws/>
3. Amazon Web Services, Inc. "Identity Verification with Amazon Rekognition." URL: <https://aws.amazon.com/rekognition/identity-verification/> (Whitepaper: <https://d1.awsstatic.com/rekognition/identity-verification-whitepaper-2024.pdf>)

Мостова Г.Г.

здобувач вищої освіти,

Маріупольський державний університет, м. Київ

Науковий керівник

Верительник С.М.

доктор філософії з публічного управління та адміністрування,

доцент, доцент кафедри публічного управління та адміністрування

Маріупольський державний університет, м. Київ

ВПРОВАДЖЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ТА УДОСКОНАЛЕННЯ СИСТЕМ КОНТРОЛЮ І МОНІТОРИНГУ У СФЕРІ ВИКОНАННЯ СУДОВИХ РІШЕНЬ

Цифровізація процесів у сфері виконання судових рішень є одним із провідних напрямів підвищення результативності публічного адміністрування та забезпечення прозорості роботи виконавчої служби. Використання сучасних інформаційних технологій дає змогу прискорити виконання рішень, знизити рівень бюрократичних процедур та підвищити довіру суспільства до державних інституцій.

Наразі діяльність виконавчої служби України характеризується низкою проблем:

- Недостатня інтеграція електронних систем. Виконавці користуються локальними базами даних і реєстрами, що ускладнює обмін інформацією між установами.

- Низький рівень автоматизації процесів. Значна частина операцій здійснюється вручну, що спричиняє затримки та помилки у документації.

- Обмежений доступ громадян до інформації. Стягувачі та боржники часто не мають можливості в режимі онлайн відстежувати перебіг провадження, що знижує відкритість процесу [1].

Для підвищення ефективності виконавчих проваджень доцільним є впровадження таких цифрових інструментів:

1. Єдина електронна платформа виконавчої служби.

- Консолідація всієї інформації про справи, боржників і стягувачів у єдиній системі.

- Забезпечення швидкого доступу до даних для виконавців та контролюючих органів.

2. Онлайн-кабінети для стягувачів та боржників.

- Можливість самостійно відстежувати статус провадження та отримувати повідомлення про зміни.

- Зменшення потреби у особистих зверненнях і телефонних консультаціях.

3. Автоматизація внутрішніх процесів.

- Використання програмних рішень для формування документів, ведення обліку справ та збору статистики.

- Запровадження систем електронного планування і контролю строків виконання рішень [2;3].

4. Аналітичні інструменти та моніторинг результативності.

- Використання цифрових панелей для контролю показників ефективності роботи виконавців.

- Прогнозування ризиків затримок і визначення проблемних ділянок у роботі служби.

Інтеграція цифрових технологій у сферу примусового виконання судових рішень дозволить:

- скоротити строки виконання;
- зменшити адміністративне навантаження на виконавців;
- підвищити рівень відкритості та доступності інформації;
- посилити контроль за діяльністю виконавчої служби;
- знизити корупційні ризики та зміцнити довіру до системи правосуддя [4].

Ефективність роботи виконавчої служби значною мірою визначається якістю контролю, моніторингу та підзвітності органів примусового виконання. Відсутність дієвих механізмів контролю й оцінки діяльності виконавців створює умови для затримок, неточностей та корупційних проявів, що негативно позначається на рівні довіри громадян.

Основні проблеми у сфері контролю та підзвітності [5]:

- недостатній розвиток внутрішнього контролю (відсутність систематичних перевірок та аудитів діяльності виконавців);
- низька прозорість роботи служби;
- слабкий моніторинг результативності;
- обмежена підзвітність перед суспільством і державними інституціями.

Пріоритетні напрями посилення контролю та підзвітності [6]:

1. Регулярний внутрішній аудит.

- Проведення систематичних перевірок дотримання процедур та якості виконання рішень.

- Залучення незалежних експертів для оцінювання результатів діяльності.

2. Прозорість та відкритість інформації.

- Створення онлайн-реєстрів справ із відкритим доступом для учасників провадження та громадськості.

- Опублікування статистичних даних і результатів перевірок.

3. Моніторинг ефективності.

- Запровадження ключових показників ефективності (KPI) для оцінки роботи виконавців і структурних підрозділів.

- Використання аналітичних інструментів для виявлення проблемних проваджень і управління ризиками [6].

4. Підзвітність перед суспільством та державними інституціями.

- Запровадження системи регулярних публічних звітів про результати діяльності виконавчої служби.

— Використання механізмів збору відгуків від громадян і стягувачів щодо рівня якості наданих послуг.

Розширення системи контролю, моніторингу та підзвітності дає можливість:

- підвищити результативність виконання судових рішень;
- зменшити кількість затримок і порушень процедур;
- забезпечити прозорість та зміцнити довіру громадян до системи;
- своєчасно виявляти проблемні аспекти та приймати ефективні управлінські рішення;
- сформувати культуру відповідального та підзвітного функціонування органів примусового виконання [7].

Отже, посилення контролю й підзвітності виступає ключовим елементом реформи системи виконання судових рішень та є важливим чинником підвищення якості публічного адміністрування.

Список використаних джерел:

1. Згама А.О. Щодо цифрової трансформації правосуддя та перспектив для сфери господарювання. Електронне наукове видання «Аналітично-порівняльне правознавство». С.320.-325. URL: <https://app-journal.in.ua/wp-content/uploads/2024/12/54.pdf>
2. Літвінова О. Цифровізація судових процесів та використання інструментів штучного інтелекту для правників. URL: <https://advokatpost.com/tsyfrovizatsiia-sudovykh-protsesiv-ta-vykorystannia-instrumentiv-shtuchnoho-intelektu-dlia-pravnykiv-radnyk-holovy-dsa-oksana-litvinova/>
3. Окремі питання ефективності виконання судових рішень. URL: <https://www.pravojustice.eu/ua/post/okremi-pitannya-efektivnosti-vikonannya-sudovi-h-rishen>
4. Цифровізація виконання судових рішень в Україні: теорія та практика. FEMIDA. 2025. URL: <https://femida.ua/news/czyfrovizacziya-vykonannya-sudovyh-rishen-v-ukrayini-teoriya-ta-praktyka/>
5. Цифровізація судової сфери: працюємо над оновленою концепцією е-Суду. URL: <https://www.kmu.gov.ua/news/tsyfrovizatsiia-sudovoi-sfery-pratsiuemo-nad-onovlenoiu-kontseptsiiu-e-sudu>
6. Цувіна Т.А. Онлайн суди та онлайн вирішення спорів у контексті міжнародного стандарту доступності правосуддя: міжнародний досвід. Проблеми законності. 2020. Вип. 149. С. 62–79.
7. Theoretical and Methodological Foundations for the Use of Digital Technologies in Ukraine through the Implementation of EU Experience: collective monograph / edited by A.V. Cherep, I.M. Dashko, Yu.O. Ohrenych, O.H. Cherep. Zaporizhzhia: publisher of FOP Mokshanov V.V., 2024. 246 p. URL: <https://dspace.znu.edu.ua/xmlui/handle/12345/24080>

*Ніжегородцев В.О.
к.пед.н., доцент, доцент кафедри комп'ютерних
та інформаційних технологій і систем
Державний податковий університет*

АНАЛІЗ ЦИФРОВИХ ТЕХНІЧНИХ РІШЕНЬ З МОНІТОРИНГУ СИСТЕМ КОМУНАЛЬНИХ ВИТРАТ

Традиційні підходи до обліку та контролю комунальних витрат стають наразі архаїчними та неефективними. Ручний збір даних, відсутність оперативної інформації та обмежені можливості для аналізу призводять до значних втрат, неточностей у нарахуваннях і, як наслідок, до зростання недовіри між споживачами та постачальниками послуг.

Аналіз технічних рішень з моніторингу систем комунальних витрат продемонстрував, що сучасні технології пропонують комплексний підхід до вирішення багаторічних проблем у сфері житлово-комунального господарства: від високоточних Smart-лічильників та ефективних мереж передачі даних до потужних аналітичних платформ та зручних користувацьких інтерфейсів.

Для якісного моніторингу комунальних послуг необхідне створення надійної цифрової інфраструктури, що базується на трьох ключових компонентах: сенсорах збору даних, мережевих технологіях передачі інформації та серверних системах для її обробки.

Впровадження систем моніторингу допомагає вчасно виявляти проблеми та адекватно на них відреагувати, не допускати дестабілізацію бізнес-процесів та діяльності підприємства в цілому, визначити внесок кожного працівника, об'єктивно оцінити результати роботи [2, с. 110].

Завдяки використанню IoT-пристроїв, хмарних платформ, протоколів безпечної передачі та засобів аналітики, суспільство отримує потужний інструмент для економії ресурсів, прогнозування навантажень і боротьби з несанкціонованими витратами.

Системою обліку і контролю споживача часто асоціюють систему, яка повинна працювати з параметрами кількості спожитих послуг та характеристиками, дані з сенсорів про кількість і якість послуг, що використані, можуть заноситися в пам'ять контролера сенсорів, з якої вони можуть тільки зчитуватися в комп'ютер споживача і по телефонному каналу зв'язку в комп'ютер виробника. Зниження вартості досягається також шляхом створення багатоканальної системи з одним вимірювально-обчислювальним ядром [1, с. 76-77].

До складу сучасного дистанційного моніторингу витрат входить і система обробки даних. Після збору дані передаються на центральний сервер, де для обробки та аналізу даних де може використовуватися спеціалізоване програмне забезпечення для управління величезними обсягами даних лічильників.

Завдяки розвитку інформаційних технологій, на українському ринку сформувався широкий спектр програмних рішень та вебсервісів для

моніторингу, що застосовуються як у державному, так і приватному секторах.

У нашому дослідженні відбулася спроба побудувати систему моніторингу комунальних платежів за допомогою смарт-камер та Wi-Fi. Для введення даних планувалося розробити у веб-додаток (систему), в якій би була можливість очищення та валідації цифрових даних, які автоматично передаються (наприклад, через API або пряме збереження в базу даних) у відповідні комірки веб-додатка.

Проведення моніторингу комунальних показників у дослідженні планувалося здійснювалося через веб-додаток, який відображав отримані дані, будував графіки споживання та надавав адміністратору повний моніторинг комунальних платежів. За допомогою мови HTML була сформована основна сторінка структура вебсистеми, в якій передбачалося розміщення текстових написів початкових та кінцевих показників лічильників та реалізовувався відео-моніторинг онлайн камер з лічильників. Технологія CSS використовувалася для за дизайнерського відображення елементів на сторінці, наприклад, розміри шрифтів, відступи між блоками, колір, тощо. Python забезпечив інтерактивну поведінку інтерфейсу, зокрема реакцію на дії користувача: підрахунки різниць показників, роботу з базою даних та побудові діаграм статистичних даних.

Прийом даних у дослідженні реалізовувався на отриманні відео-потоків, зображень або структурованих даних від камер. Обробка даних для відео або зображення, виконувалося серверною обробкою (застосовувалася OCR для розпізнавання цифр на лічильниках, аналіз рух, детектування об'єктів).

У результаті нашого дослідження виявилось що базовий моніторинг надає сирі дані та графіки, але справжня цінність полягає в здатності перетворювати ці дані на корисні інсайти та проактивні рекомендації. Tesseract OCR став потужним і широко використовуваним рушієм для оптичного розпізнавання символів, особливо після того, як Google взяв його під своє крило та значно вдосконалив, додавши підтримку нейронних мереж. Він чудово справився з багатьма завданнями, зокрема з розпізнаванням друкованого тексту та, зокрема, цифр. Однак, незважаючи на його можливості, Tesseract мав певні недоліки та обмеження, особливо коли йшлося про високу точність розпізнавання цифр у реальних сценаріях. Розуміння цих недоліків стало ключовим для ефективного використання Tesseract та вибору правильного інструменту для конкретного завдання.

Сучасні програми, засновані програмному коді штучного інтелекту на разі продовжують розвиватися, і їх потенціал полягає у генеруванні нових ідей, пропонуванні несподіваних корисних алгоритмів, тощо. Для функціонування інформаційних систем наразі повинні бути реалізовані уніфіковані правила створення і ведення баз даних, реалізації автоматизованих систем обліку і контролю енергоресурсів, аналізу, що значно дозволить проводити виявлення і припинення злочинства енергоресурсів.

Список використаних джерел:

1. Багацький В. О. Система обліку та контролю комунальних послуг з точки зору споживача/ В. О. Багацький, Н. М. Красноруцька, Л. Л. Тишковська, О. В. Багацький // Вісн. Вінниц. політехн. ін-ту. – 2005. – № 6. – С. 73-78.
2. Малтиз В.В. Автоматизація обліку та моніторингу показників ефективності використання персоналу на підприємствах. Актуальні проблеми економіки № 2 (272), 2024. С. 105-110. URL: https://eco-science.net/wp-content/uploads/2024/02/2.24._topic_Viktoriia-V.-Maltyz-105-110.pdf. (дата звернення: 20.07.2025 р.).

УДК 377.8:004.738.5

Ніколайчук С. Ю.

здобувач вищої освіти,

НРЗВО «Кам'янець-Подільський державний інститут»

Науковий керівник

Насмінчук І. А.

*к.філол.н., доцент, доцент кафедри цифрових,
освітніх та соціо-економічних технологій*

НРЗВО «Кам'янець-Подільський державний інститут»

ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ ДЛЯ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ У ЗАКЛАДАХ ПРОФЕСІЙНОЇ ОСВІТИ

У сучасному світі цифровізація освіти стає невід'ємною частиною реформування системи професійної освіти. Хмарні сервіси, будучи інноваційним інструментом, сприяють оптимізації освітнього процесу, забезпечують доступність ресурсів, співпрацю та гнучкість. У закордонних закладах освіти хмарні сервіси вже активно застосовуються для різних цілей – від аналізу даних про успішність здобувачів до підтримки навчальних і позакласних активностей. В Україні ж використання хмарних технологій набуло особливого поширення в останні роки, позначені пандемією COVID-19, що стала каталізатором переходу до дистанційних та змішаних форматів навчання. Додатковим фактором, який актуалізував потребу в хмарних рішеннях, стала повномасштабна війна: в умовах воєнних загроз і вимушеної релокації закладів освіти саме хмарні сервіси забезпечують безперервність освітнього процесу, доступність матеріалів та комунікацію між викладачами і здобувачами освіти.

Хмарні технології в освіті – це використання хмарних обчислювальних ресурсів і сервісів для підтримки та вдосконалення процесу навчання й управління освітніми процесами. Вони передбачають збереження та обробку даних у хмарному середовищі, доступному з будь-якого місця за допомогою Інтернету [1]. Завдяки цьому забезпечуються як вільний доступ до електронних ресурсів (підручників, відеоуроків, тестів тощо), так і можливість організації спільної роботи здобувачів і викладачів у режимі реального часу, а також

ефективне управління навчальною документацією та освітнім процесом. Важливим аспектом є захист і безпека даних, їх збереження та запобігання втратам чи несанкціонованому доступу.

У працях сучасних науковців наголошується, що використання хмарних технологій сприяє реалізації компетентнісного підходу в освіті. Це пов'язано з тим, що сервіси дозволяють формувати навички у напрямі здобуття знань, але й уміння працювати в команді, розвивати критичне мислення, адаптивність і здатність до самонавчання [2; 3].

У професійній освіті хмарні сервіси сприяють вдосконаленню компетентностей, пов'язаних із цифровими навичками, які є ключовими для сучасного ринку праці. Дослідження показують, що впровадження хмарних технологій підвищує продуктивність навчання за рахунок персоналізації та інтерактивності. Наприклад, вони дозволяють створювати віртуальні лабораторії для практичних занять у технічних спеціальностях, де традиційне обладнання є дорогим або недоступним.

Хмарні сервіси надають низку переваг для організації освітнього процесу. По-перше, вони забезпечують гнучкість та доступність: здобувачі освіти можуть отримувати доступ до матеріалів з будь-якого пристрою та місця, що особливо актуально для професійної освіти з її акцентом на практичні навички. По-друге, сприяють співпраці, наприклад платформи Google Workspace for Education дозволяють спільно редагувати документи, проводити онлайн-зустрічі та обмінюватися ресурсами в реальному часі. По-третє, завдяки використанню хмарних сервісів заклади професійної освіти досягають економічної ефективності, оскільки можуть відмовитися від витрат на придбання й обслуговування серверів та баз даних, орендуючи необхідні ресурси у провайдерів. Крім того, хмарні технології підтримують масштабування, дозволяючи обробляти великі обсяги даних для аналізу успішності та адаптації програм. У vocational education це трансформує процес навчання, роблячи його більш доступним та інклюзивним, наприклад, через хмарні LMS (learning management systems) [4].

Особливу увагу варто звернути на потенціал хмарних сервісів для забезпечення інклюзивності освіти. Такі платформи дозволяють адаптувати навчальні матеріали для здобувачів із особливими освітніми потребами, наприклад, шляхом використання текстових редакторів із функціями озвучування, адаптивних шрифтів чи мультимедійних ресурсів. Однак впровадження інклюзивного навчання через хмарні сервіси пов'язане з певними викликами. Розробка спеціалізованих матеріалів, які враховують різноманітні потреби здобувачів, вимагає додаткових ресурсів і підготовки викладачів. Недостатній рівень технічної інфраструктури в деяких закладах освіти може створювати бар'єри для безперебійного доступу до хмарних сервісів, що обмежує інклюзивність. Також необхідна систематична підготовка педагогів до використання інструментів, які сприяють інклюзивному навчанню, таких як адаптивні LMS чи спеціалізовані додатки.

Серед популярних хмарних сервісів для освіти виділяють Google Workspace for Education, Microsoft Office 365 Education та Amazon Web Services

(AWS). Google Workspace надає інструменти для створення навчальних ситуацій, де здобувачі освіти можуть освоювати навички через інтерактивні завдання. Microsoft пропонує інтеграцію з Teams для відеоконференцій та спільного навчання.

Попри очевидні переваги, існують і проблемні аспекти. По-перше, це інфраструктурні обмеження: низька якість інтернет-з'єднання чи застаріла техніка у деяких закладах освіти. По-друге, питання безпеки даних, адже зберігання особистої інформації у хмарі вимагає дотримання високих стандартів захисту. Крім того, варто враховувати потребу у підготовці викладачів. Не всі педагоги володіють достатніми цифровими навичками, а також готовністю змінювати традиційні підходи до навчання. Як зазначають науковці, лише систематичне підвищення цифрової грамотності педагогів дозволить повноцінно інтегрувати хмарні технології у професійну підготовку [5].

Отже, хмарні сервіси є важливим інструментом трансформації професійної освіти. Вони сприяють доступності, співпраці, гнучкості освітнього процесу й оптимізації витрат. Разом з тим їх ефективне використання потребує належного технічного забезпечення, цифрової компетентності викладачів і продуманих стратегій упровадження, зокрема для забезпечення інклюзивності. Подальші дослідження варто спрямувати на аналіз моделей змішаного навчання із застосуванням хмарних сервісів, оцінку їх економічної ефективності та вивчення впливу на розвиток цифрових компетентностей майбутніх фахівців, а також розробку стратегій для подолання викликів інклюзивного навчання, включаючи створення універсальних навчальних матеріалів і підвищення доступності технічної інфраструктури.

Список використаних джерел:

1. Бабак О. А., Ісак Л. М. Хмарні технології в освіті. URL: <https://doi.org/10.36074/grail-of-science.12.05.2023.079>
2. Кононюк А. Е., Фундаментальна теорія хмарних технологій. *Загальнонаукові підходи формування систем хмарних технологій*. 2018. № 2. С. 52–88.
3. Смірнова Т. В., Поліщук Л. І., Смірнов О. А., Буравченко К. О., Макевнін А. О. Дослідження хмарних технологій як сервісів. *Кібербезпека: освіта, наука, техніка*. 2020. № 3(7). С. 43–62.
4. Kononova N., Berbyuk Lindström N., Panchuk A. Teaching and learning amid war crisis: Perceptions of Ukrainian academic staff and students on online education. *IBIMA Business Review*, 2024. URL: <https://doi.org/10.5171/2024.465847>
5. Kovalchuk V., Maslich S., Movchan L. Digitalization of vocational education under crisis conditions. *Educational Technology Quarterly*. 2023. Iss. 1. P. 1–14. URL: <https://doi.org/10.55056/etq.49>

ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ВПРОВАДЖЕННЯ ІННОВАЦІЙ НА ПІДПРИЄМСТВАХ АГРАРНОГО СЕКТОРУ

Впровадження інновацій на підприємствах аграрного сектору є ключовим чинником підвищення їх конкурентоспроможності та забезпечення сталого розвитку. Інноваційні технології дозволяють підвищити продуктивність праці, оптимізувати використання ресурсів, знизити витрати виробництва та підвищити якість сільськогосподарської продукції [1]. Вони сприяють екологізації виробництва, впровадженню енергоощадних і ресурсоефективних рішень, що відповідають сучасним викликам продовольчої та екологічної безпеки. Окрім того, інновації стимулюють залучення інвестицій, розвиток інфраструктури та інтеграцію українського аграрного бізнесу у світові ринки. Саме завдяки інноваціям аграрні підприємства отримують можливість гнучко реагувати на зміни ринкової кон'юнктури та забезпечувати стабільне економічне зростання.

Економічна ефективність впровадження інновацій на підприємствах аграрного сектору полягає у досягненні оптимального співвідношення витрат і результатів від використання нових технологій, методів управління та організаційних рішень [2]. Інновації дозволяють підвищити врожайність і продуктивність, знизити собівартість продукції, оптимізувати використання матеріальних і трудових ресурсів, мінімізувати втрати та забезпечити стабільну якість продукції [3]. Водночас їх застосування відкриває доступ до нових ринків, стимулює залучення інвестицій і розширює експортні можливості аграрних підприємств [4]. Економічна ефективність інновацій визначається не лише фінансовими показниками (рентабельність, прибуток, окупність витрат), але й довгостроковими вигодами – підвищенням конкурентоспроможності, екологічною стійкістю та соціальною відповідальністю агробізнесу [5].

Пропонуємо розглянути систему показників для кількісної оцінки економічної ефективності впровадження інновацій у аграрному секторі, а саме [3, 4]:

1. Рентабельність інноваційного проєкту (R):

$$R = \frac{\Pi}{B} \times 100\%$$

де:

Π – прибуток від впровадження інновацій,

B – витрати на впровадження інновацій.

2. Ефективність інвестицій у інновації (ROI – Return on Investment):

$$ROI = \frac{D-B}{B} \times 100\%$$

де:

Д – додатковий дохід (виручка) від інновацій,

В – витрати на інновації.

3. Чистий дисконтований дохід (NPV – Net Present Value):

$$NPV = \sum_{t=1}^n \frac{CF_t}{(1+r)^t} - IC$$

де:

CF_t – чистий грошовий потік у році t,

r – ставка дисконту,

IC – інвестиційні витрати,

N – період розрахунку.

4. Індекс прибутковості інновацій (PI – Profitability Index):

$$PI = \frac{\sum_{t=1}^n \frac{CF_t}{(1+r)^t}}{IC}$$

Якщо PI > 1 – інноваційний проект економічно ефективний.

5. Термін окупності інновацій (PP – Payback Period):

$$PP = \frac{IC}{CF_{\text{сер}}}$$

де:

IC – інвестиційні витрати,

CF_{сер} – середній щорічний чистий грошовий потік.

6. Приріст продуктивності праці (ΔP):

$$\Delta P = \frac{P_1 - P_0}{P_0} \times 100\%$$

де:

P₁ – продуктивність праці після впровадження інновацій,

P₀ – базовий рівень продуктивності.

7. Зниження собівартості продукції (ΔC):

$$\Delta C = \frac{C_0 - C_1}{C_0} \times 100\%$$

де:

C₀ – собівартість продукції до інновацій,

C₁ – після впровадження інновацій.

Використання цих показників дозволяє комплексно оцінити економічну результативність інноваційних процесів на аграрних підприємствах, враховуючи як фінансові, так і виробничі ефекти.

Економічна ефективність впровадження інновацій на підприємствах аграрного сектору полягає у зростанні продуктивності, зниженні витрат, підвищенні рентабельності та конкурентоспроможності продукції, що забезпечує стабільний розвиток і посилює позиції агробізнесу на внутрішньому та світових ринках.

Список використаних джерел:

1. Мамчур В. А., Студінська Г. Я. Інноваційний розвиток аграрної сфери в умовах реалізації національної системи стійкості. *Економіка та суспільство*. 2023. Вип. 56. DOI: <https://doi.org/10.32782/2524-0072/2023-56-144>
2. Вернюк Н. О., Дяченко М. І. Регулювання інноваційного розвитку аграрного сектору України. *Ефективна економіка*. 2021. №4. DOI: 10.32702/2307-2105-2021.4.96
3. Заїка С., Грідін О., Заїка О. Інновації в сталому розвитку аграрного виробництва: тенденції, проблеми, перспективи. *Економіка та суспільство*. 2023. Вип. 52. DOI: <https://doi.org/10.32782/2524-0072/2023-52-69>
4. Tomashuk I.V., Tomashuk Ir.O. Enterprise development strategy: innovation and internal flexibility. *Colloquium-journal*. 2021. № 3 (90) Vol. 4. P. 51-66. DOI: 10.24412/2520-2480-2021-390-50-64
5. Гончарук І.В., Томашук І.В. Вплив інноваційних процесів на підвищення конкурентоспроможності сільськогосподарських підприємств. *Економіка, фінанси, менеджмент: актуальні питання науки і практики*. 2023. № 1. (63). С. 30-47. DOI: 10.37128/2411-4413-2023-1-3

УДК 004.65

Павленко Р. О.

здобувач вищої освіти другого рівня,
Сумський національний аграрний університет

ПРОБЛЕМИ РОЗРОБКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ПІДТРИМКИ ПРОЦЕСУ РОЗПІЗНАВАННЯ ХІМРЕАКТИВІВ

На сьогоднішній день компанії, які працюють із хімічними реактивами, зіштовхуються із задачами забезпечення безпечного зберігання, ведення обліку та оперативного доступу до інформації про засоби. Ручний облік, який традиційно застосовується, несе високий ризик помилок, що може спричинити порушення норм безпеки та порушення виробничих процесів. Впровадження автоматизованого розпізнавання хімічних реактивів підвищує точність і швидкість роботи з даними, зменшує вплив людського фактора та удосконалює контроль над залишками на складі.

Проблема автоматизації складських процесів ідентифікації хімічних матеріалів перебуває у центрі уваги міжнародних досліджень. Застосування штрих-коду, QR-коду, RFID-міток і технології OCR вважається ефективним способом поєднання фізичного середовища з ІТ-системами. Проте в українських компаніях рівень впровадження цих технологій залишається низьким, зокрема через складність розробки та інтеграції баз даних, а також через суворі вимоги до інформаційної безпеки.

Дані для дослідження були зібрані під час проходження виробничої практики науково-промислового підприємстві "Квалітет". Були виявлені

основні об'єкти системи: реактив, партія, постачальник, склад, умови зберігання, відвантаження, контроль якості, користувач і маркування. Складена ER-модель описує логічні взаємозв'язки між цими елементами, забезпечуючи комплексний облік інформації.

Схема взаємозв'язків задач інформаційної системи з підтримки процесу розпізнавання хімреактивів (рис. 1), включає такі функціональні блоки:

- ХІМРЕАК1 – занесення даних про хімреактиви;
- ХІМРЕАК2 – облік партій реактивів;
- ХІМРЕАК3 – контроль руху реактивів;
- ХІМРЕАК4 – маркування та ідентифікація (штрих-код, QR, OCR);
- ХІМРЕАК5 – контроль залишків і термінів придатності;
- ХІМРЕАК6 – формування звітності;
- ХІМРЕАК7 – ведення довідника постачальників і клієнтів;
- ХІМРЕАК8 – керування доступом користувачів;
- ХІМРЕАК9 – формування запитів користувачів.

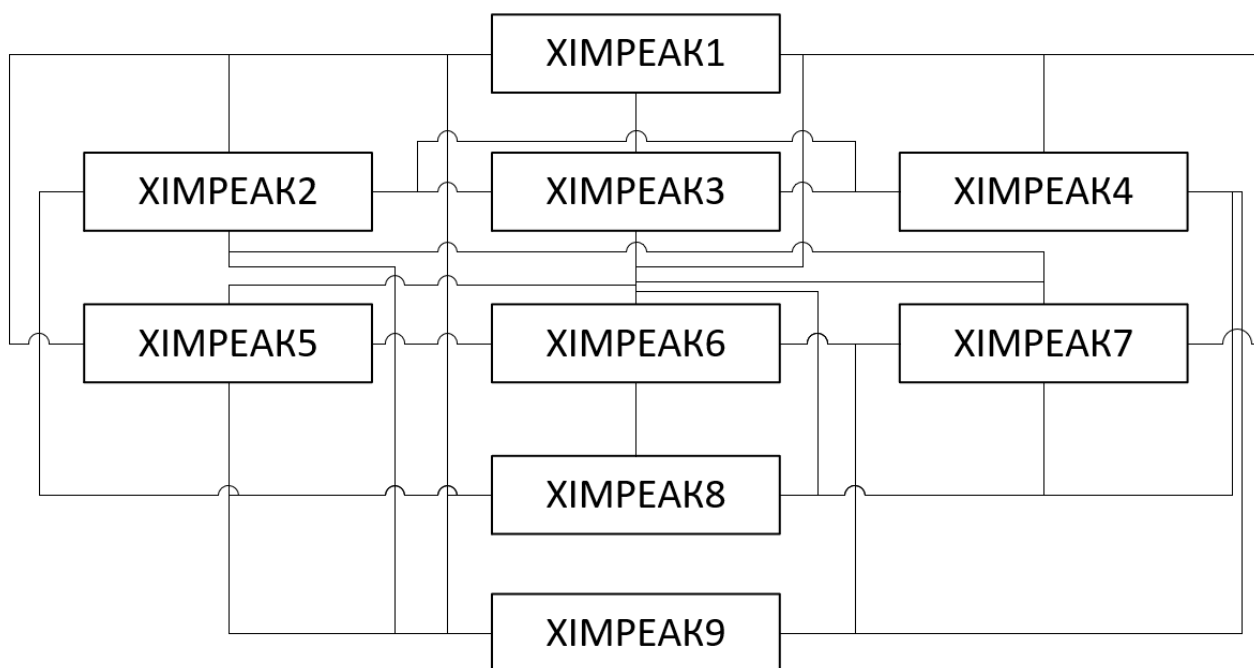


Рисунок 1 – Схема взаємозв'язків задач інформаційної системи з підтримки процесу розпізнавання хімреактивів

Такий підхід формує уніфіковану структуру автоматизованої системи, у якій усі підмодулі взаємодіють і гарантують цілісність даних. Ключовими труднощами на етапі розробки залишаються інтеграція технологій автоматичного розпізнавання, створення надійної бази даних та захист інформації від несанкціонованого доступу.

Отже, створення інформаційної системи, яка підтримує процес розпізнавання хімічних реактивів, відповідає актуальним потребам компаній, що працюють з небезпечними матеріалами. Діаграма взаємозв'язків завдань системи демонструє комплексність питання: від реєстрації реактивів і партій до підготовки звітності та контролю доступу. Основні виклики пов'язані з

інтеграцією автоматизованих ідентифікаційних технологій, розробкою масштабованої бази даних із забезпеченням інформаційної безпеки. Подальші дослідження повинні бути спрямовані на розробку прототипу системи та його випробування у практичних умовах.

Список використаних джерел:

1. GitHub – tesseract-ocr/tesseract: Tesseract Open Source OCR Engine (main repository). *GitHub*. URL: <https://github.com/tesseract-ocr/tesseract>.
2. ResearchGate / ERD examples: "Diagram for chemical inventory ERD and database schema". URL: <https://surl.li/beobvi>.
3. Zhao B., Tu C. Research and Development of Inventory Management and Human Resource Management in ERP. *Wireless Communications and Mobile Computing*. 2021. Vol. 2021. P. 1–12. URL: <https://doi.org/10.1155/2021/3132062>

УДК 005.53:004.89

Петріщев Д. А.

здобувач фахової передвищої освіти,

ВСП Харківський комп'ютерно-технологічний коледж НТУ ХПІ

Науковий керівник

Сомова А.А.

викладач циклової комісії комп'ютерних та інформаційних дисциплін,

ВСП Харківський комп'ютерно-технологічний коледж НТУ ХПІ

БРЕЙНСТОРМ З LLM У БІЗНЕС-АНАЛІЗІ: КОРИСТЬ, РИЗИКИ ТА ПРАКТИЧНІ КЕЙСИ

Брейнстормінг у бізнес-аналізі використовується для генерації ідей, пошуку рішень та формування вимог. Це інструмент, що дозволяє швидко зібрати широкий спектр думок і бачень, залучити команду до обговорення проблеми та створити основу для подальшого аналізу.

Однак класичний брейнсторм має свої недоліки:

- домінування найактивніших учасників;
- повторюваність ідей;
- обмежений час для генерації;
- хаос у віддалених командах.

Тут на допомогу приходять великі мовні моделі (LLM), які можуть стати «нейтральним учасником» брейнсторму.

Завдяки правильно сформульованим промптам бізнес-аналітик може:

- згенерувати широкий спектр ідей, включно з нестандартними;
- випробувати різні техніки (наприклад, SCAMPER чи 5 Whys) без модератора;
- швидко створити альтернативи та структурувати відповіді;

– уникнути бар'єру «мені соромно сказати цю ідею».

Під час дослідження були випробувані різноманітні структури промптів у різних llm. Приклади промптів та отриманих результатів для ідеї «створення мобільного додатку для вивчення мов».

Gemini 2.5 Flash «Розроби інноваційну навчальну методологію для вивчення іспанської мови з нуля, яка поєднує інтервальне повторення (spaced repetition) та ситуативні діалоги. Опиши, як буде відбуватися тестування та відстеження прогресу користувачів на різних рівнях (A1-B2).»

Приклади ідей: інтерактивні діалоги, вправи у реальних сценаріях, прогресивна шкала рівнів, звіти у вигляді графіків.

Grok «Запропонуй унікальну концепцію мобільного додатку для вивчення мов, який поєднує ігрові елементи та штучний інтелект. Опиши основні функції, цільову аудиторію та як додаток може виділитися серед конкурентів, таких як Duolingo чи Babbel.»

Приклади ідей: AI-співрозмовник, пригодницька гра з квестами, PvP-батли на швидкість перекладу, щоденні виклики.

DeepSeek «Опиши концепцію мовного додатку, заснованого на методі інтервальних повторень (spaced repetition) та аудіюванні (listen-first approach). Як має виглядати основне меню та процес навчання?»

Приклади ідей: просте меню (слухати, повторювати, тест), подкасти від носіїв, вправи на «заповни пропуск», миттєвий фідбек з вимови.

Результати показали, що LLM генерують структуровані ідеї різного рівня деталізації, пропонують інноваційні функції та допомагають оцінювати ризики й можливості.

Важливо: у випадку брейнсторму вигадані відповіді мовних моделей (так звані “галюцинації”) не шкодять, а навпаки, створюють асоціативний ряд для нових ідей, допомагають бізнес-аналітику мислити ширше.

Нерозголошеність даних у ситуації з брейнстормінгом якоїсь ідеї також не є блокуючою у контексті статті, тому що llm віддається лише базова ідея для старту.

Випробування на різних моделях (Gemini, Grok, DeepSeek) демонструють різницю у стилі та фокусі відповідей, але всі вони знижують проблеми класичного брейнстормінгу.

Використання LLM у бізнес-аналізі може суттєво доповнити класичний брейнсторм, особливо у великих або розподілених командах. Моделі допомагають швидко отримати масив ідей, структурувати їх та уникнути упередженості учасників.

Проте бізнес-аналітик завжди має виступати «фільтром» — перевіряти реалістичність, релевантність і бізнес-цінність ідей.

Таким чином, LLM — це не заміна команді, а потужний асистент, який підсилює процес генерації вимог.

Список використаних джерел:

1. SendPulse. «Брейнсторм: що це і як проводити». URL: <https://sendpulse.ua/blog/brainstorm>
2. Vitalflux. Different Types of Brainstorming Techniques for Great Ideas. URL: <https://vitalflux.com/different-types-brainstorming-techniques-great-ideas/>

УДК 316.7:339.138

Пилипенко А. О.,

здобувачка вищої освіти

Науковий керівник

Линенко А. В.,

доцент кафедри управління персоналом і маркетингу,

кандидат економічних наук, доцент,

Запорізький національний університет

ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ДОСЛІДЖЕННІ МІЖНАРОДНИХ РИНКІВ

Міжнародна конкуренція зростає, а вихід компаній на нові ринки вимагає глибокого розуміння національних особливостей. Тому успіх маркетингової діяльності залежить від якості зібраної інформації про поведінку споживачів, культурні та соціальні відмінності, специфіку конкурентного середовища. Опитування, інтерв'ю, аналіз статистичних даних є традиційними методами збору інформації, що залишаються актуальними, проте мають низку обмежень. Вони вимагають значних фінансових і часових ресурсів, не завжди дають змогу швидко реагувати на ринкові зміни, тому часто відображають застарілі дані. У зв'язку з цим все більшої популярності набувають сучасні цифрові інструменти маркетингових досліджень, серед яких особливе місце займають соціальні мережі.

Маркетинг у соціальних мережах охоплює використання платформ соціальних мереж для зв'язку з цільовою аудиторією для створення та розвитку бренду, збільшення відвідуваності сайту та підвищення продажів. Загалом користувачі у світі в середньому витрачають на Інтернет 6 годин 40 хвилин. Із них 2 години 23 хвилин – на соціальні медіа, майже півтори години – на музичні стримінгові сервіси, 49 хвилин – на прослуховування подкастів [1].

Серед найбільш популярних онлайн-ресурсів користувачі насамперед зазначають чати та месенджери, соціальні мережі, пошукові системи, а також платформи електронної комерції (shopping, auctions, classified). Далі за рівнем поширеності йдуть сервіси геолокації. Потім уже електронна пошта, яку назвали 49,5% опитаних як один із найбільш уживаних сервісів. Майже така ж частка респондентів (48,1%) зазначили музичні ресурси. Новинні сайти включили до переліку найчастіше використовуваних 40,3% користувачів.

Частка переходів із пошукових систем у 2024 році

Пошукові системи	Частка, відсотки	Річна зміна, відсотки
Google	91,62	-1,0
Bing	3,37	+11,2
Yahoo!	1,12	+2,8
Baidu	0,96	-21,3
DuckDuckGo	0,51	-12,1
Naver	0,21	+10,5
Cốc Cốc	0,16	-14,1
Sogou	0,07	-33,3
Інші	0,33	+0,3

Джерело: розроблено авторами на основі [2]

Важливою складовою дослідження є статистика про використання соціальних мереж у процесі пошуку інформації про бренди. Згідно з отриманими даними, понад 83% користувачів звертаються до різних платформ для ознайомлення з брендами. Водночас найбільш популярними серед них залишаються Instagram (62,7%) та Facebook (54%). Однак ефективність такого пошуку суттєво відрізняється, якщо розглядати його з позиції переходів на офіційні сайти компаній.

Лідером за обсягами реферального трафіку з соціальних медіа є Facebook, який формує понад 64% таких переходів. Другу позицію займає Instagram з часткою близько 10%. Водночас обидві ці платформи демонструють тенденцію до зниження показників. Натомість LinkedIn продемонстрував стрімке зростання – на рівні 83%, хоча його частка у 0,5% поки що залишається незначною. Важливим є помітне збільшення реферального трафіку з Pinterest, який зріс на 51%, що свідчить про потенціал цієї платформи у просуванні візуального та нішевого контенту.

Окрему увагу привертає те, за ким саме користувачі віддають перевагу стежити у соціальних мережах. Більшість респондентів (понад 47%) зазначили, що підписані на сторінки друзів, членів родини та знайомих. Досить високий рівень популярності мають актори, знаменитості, а також акаунти з гумористичним і розважальним контентом. У той же час журналісти та новинні медіа займають останні позиції в рейтингу, адже лише 15% опитаних включили їх до переліку цікавих для себе джерел [1].

Соціальні платформи мають власну географію та специфіку поширення, тому наприклад в Китаї ключова мережа WeChat, вона об'єднує не лише функції комунікації, але й послуги онлайн-торгівлі. У Північній Америці ключовими мережами залишаються Instagram і TikTok, які формують молодіжні тренди. В країнах Європи більш поширеним інструментом для бізнесу є Facebook, а в професійному середовищі провідну позицію займає LinkedIn. Ці відмінності вже самі по собі є цінним джерелом інформації для компаній, адже дають можливість визначати пріоритетні канали комунікації та оцінювати

культурні особливості конкретних ринків.

Таблиця 2

Веб-трафік із соціальних мереж у січні 2024 року

Соціальні мережі	Частка веб-трафіку, відсотки	Зміна за рік, відсотки
Facebook	64,79	-4,3
Instagram	10,03	-5,1
Pinterest	9,97	+51,3
X (Twitter)	7,75	-25,1
YouTube	5,88	+7,1
Reddit	0,70	-9,1
LinkedIn	0,55	+83,3
Tumblr	0,22	-15,4
Інші	0,04	-42,9

Джерело: розроблено авторами на основі [2]

Найбільш поширеним напрямом використання соціальних мереж у дослідженні міжнародних ринків є технологія social listening – відстеження та аналіз відгуків, коментарів, емоційних реакції користувачів. Такий підхід дає компаніям змогу отримати зворотній зв'язок у режимі реального часу, доволі швидко реагувати на негативні відгуки та побудувати більш ефективну стратегію просування. На практиці міжнародні бренди часто застосовують інструменти автоматичного аналізу [3], щоб зрозуміти, як сприймаються їхні товари в різних країнах. Це допомагає адаптувати рекламні компанії з урахуванням культурного контексту, а також коригувати асортимент залежно від локальних уподобань [4].

Також важливим напрямом є контент-аналіз, дослідження популярних хештегів, трендів і форматів публікацій дає змогу оцінювати культурні тренди та з'ясовувати, які цінності й ідеї близькі для місцевої аудиторії. У європейських країнах все більшого значення набуває тема сталого розвитку, екології та етичного споживання, тоді як в країнах Азії часто на перший план виходять інновації, технології та престиж брендів. Тож аналіз контенту в соціальних мережах дає можливість визначити, які цінності варто враховувати під час виходу на міжнародний ринок.

Важливу роль також відіграє і кількісна аналітика, сучасні інструменти такі як Socialinsider чи Brandwatch надають компаніям змогу оцінювати охоплення аудиторії, рівень взаємодії з контентом, темпи зростання підписників, порівнювати ефективність різних кампаній. Соціальні мережі дають можливість не лише аналізувати поведінку споживачів, але й досліджувати конкурентне середовище, виявляючи сильні й слабкі сторони різних стратегій. Використання big data відкриває перспективи прогнозування попиту, а можливість експериментів у реальному часі (зокрема А/В-тестування) допомагає швидко адаптувати маркетингові рішення й зменшувати ризики виходу на нові ринки. Попри виклики, пов'язані з достовірністю даних, етичними аспектами та захистом персональної інформації, переваги соціальних

мереж – швидкість, масштабність і гнучкість – значно переважають їхні обмеження.

Дослідження Marzanna Witek-Hajduk та Piotr Zaborek показує, що використання соціальних мереж у міжнародному маркетингу позитивно впливає на ефективність бренду й фінансові результати компаній. Найбільший успіх досягають ті бізнеси, що орієнтуються на потреби споживачів і адаптують контент під культурні особливості локальних ринків. Гнучке управління соціальними мережами та їх застосування для збору даних і комунікації стають важливим чинником конкурентних переваг на глобальному ринку [5].

Соціальні мережи сьогодні виступають не лише як канал комунікації між брендами та споживачами, але й потужним аналітичним інструментом. Вони дають можливість збирати дані в режимі реального часу, оцінювати поведінку споживачів, досліджувати конкурентів і враховувати культурні особливості різних ринків. Використання соціальних медіа у дослідженні міжнародних ринків підвищує точність прогнозування, знижує витрати на дослідження та сприяє більш успішному виходу компаній на глобальний рівень. З розвитком технологій штучного інтелекту та аналітики big data роль соціальних мереж у маркетингових дослідженнях лише зростатиме, формуючи нові підходи до розуміння міжнародних ринків і поведінки споживачів.

Список використаних джерел:

1. Популярність соцмереж і можливості для брендів. URL: <https://mediamaker.me/yak-lyudstvo-vzayemodiye-z-czyfrovymy-tehnologiyamy-zvit-digital-2024-8566> (дата звернення: 22.09.2025).
2. Як людство взаємодіє з цифровими технологіями. URL: <https://mediamaker.me/yak-lyudstvo-vzayemodiye-z-czyfrovymy-tehnologiyamy-zvit-digital-2024-8566> (дата звернення: 22.09.2025).
3. Аналіз тональності тексту. URL: <https://salo.li/763E09A> (дата звернення: 23.09.2025).
4. Що таке соціальне прослуховування та переваги його використання. URL: <https://www.post-up.com.ua/chto-takoe-soczialnoe-proslushivanie-social-listening> (дата звернення: 23.09.2025).
5. Witek-Hajduk M. K., Zaborek P. Social media use in international marketing: impact on brand and firm performance. *International journal of management and economics*. 2022. URL: <https://doi.org/10.2478/ijme-2022-0011> (date of access: 23.09.2025).

Підлужний П.А.
здобувач вищої освіти,
Харківський національний університет міського господарства імені
О.М. Бекетова
Науковий керівник
Булаєнко М.В.
к.т.н., доцент, доцент кафедри комп'ютерних наук та інформаційних
технологій
Харківський національний університет міського господарства імені
О.М. Бекетова

ВИКЛИКИ ПРИ ІНТЕГРАЦІЇ LLM У БІЗНЕС ПРОЦЕСИ

Сучасні інформаційні системи характеризується стрімким зростанням обсягів даних та складності бізнес-процесів, зокрема в сфері документообігу та написання текстових повідомлень чи іншої текстової інформації. Традиційні системи автоматизації, досягли своїх меж у завданнях, що потребують: аналізу неструктурованого тексту, створення змістовного контенту, шаблонної генерації тексту. Поява генеративних текстових моделей – Large Language Model (LLM), які здатні генерувати текст, надає нові можливості у розробці систем, які можуть використовувати штучний інтелект у бізнес-процесах. [1]

Но ефективне використання цих технологій супроводжується низкою викликів, серед яких ключовими є забезпечення безпечної інтеграції, контролю якості результатів та захисту персональних даних користувача та бізнесу.

У результаті проведеного аналізу порівняння людини та LLM у задачі створення типових документів або текстів, ми можемо виділити основні переваги і недоліки використання LLM при написанні текстів.

Переваги людини – більш глибоке знання і розуміння теми. Людина несе повну відповідальність за результати своєї роботи, що забезпечує юридичну прозорість та відповідальність. Гнучкість та адаптивність людини у нестандартних випадках підвищує надійність бізнес-процесу.

Недоліки людини – повільніше і дорожче при потребі у масовому створенні текстів. Масштабування команди для виконання великих обсягів завдань є складним і затратним процесом. Якість роботи може суттєво відрізнятися між різними виконавцями. Варіативність якості між авторами, ризик помилок і упереджень. Крім того, співробітник потребує навчання та контролю якості його роботи.

Переваги LLM – здатні майже миттєво генерувати величезні обсяги тексту, що значно економить час та ресурси на виконанні рутинних завдань. Дотримання формату й стилю при налаштуванні запитів та шаблонів. Головна перевага моделей, це можливість автоматизації у робочих процесах.

Недоліки LLM – ризик “галюцинацій”, це правдоподібні але фактично хибні відповіді. Використання сторонніх хмарних сервісів створює ризики для конфіденційності даних та супроводжується юридичною невизначеністю щодо

відповідальності за згенерований контент. Локальне розгортання моделей вимагає значних інвестицій в інфраструктуру та експертизи для їх тонкого налаштування. Моделі це чорна скринька, іноді діагностика та усунення несподіваних проблем можуть бути надзвичайно складними. [2]

Є багато різних підходів для інтеграції LLM у інформаційні системи, які мають власні недоліки та переваги. Ключовим архітектурним рішенням у цьому, це вибір між розгортанням моделі на власній інфраструктурі та використанням сторонніх хмарних сервісів. [3]

Хмарна – забезпечує високу продуктивність та доступність найновіших моделей, але створює залежність від зовнішнього постачальника, витрати на API-запити та потенційні проблеми з доступом до зовнішніх серверів. Але легка для реалізації.

Локальна – дає повний контроль над даними та конфіденційність, але вимагає значних обчислювальних ресурсів для створення та використання. Складніша в реалізації, але надійна і потенційно більш якісна та ефективніша, в залежності від потреб бізнесу та предметної області.

Сучасні рішення дозволяють створювати системи які можуть легко переключатися між різними моделями, наприклад ви можете мати власну слабку але ефективну спеціалізовану модель на своїх серверах для коротких шаблонних запитів, а у разі складних використовувати зовнішню потужну модель. Також для розробки власних моделей необхідна власна команда розробників, тоді як для підключення і налаштування зовнішньої моделі достатньо базових знань з використання API та пром프트-інжинірингу.

Підсумовуючи вищесказане – розробка інтелектуальної системи автоматизації бізнес-процесів із використанням генеративних моделей, це реалістичний і перспективний напрямок, але його успіх залежить від зваженого вибору архітектури, систем якості та комплексного підходу до безпеки.

Отже, при розробки майбутньої інформаційної системи з використанням генеративних моделей для бізнес-процесів, необхідно мати на увазі багато факторів бізнесу, його потреби, предметну область, інфраструктуру та вимоги до безпеки.

Список використаних джерел:

1. Brown T., Mann B., Ryder N., et al. Language Models are Few-Shot Learners : preprint. – 2020. – 25 p.
2. Calopereanu M. F., Șuică M., Calopereanu A. N. Considerations regarding compliance with the Regulation (EU) 2016/679 (GDPR) in Human Resources Departments. Proceedings of the International Conference on Business Excellence. 2019. T. 13, № 1. С. 548-559. URL: <https://doi.org/10.2478/picbe-2019-0048> (дата звернення: 26.09.2025).
3. Офіційна документація OpenAI API. URL: <https://platform.openai.com/docs> (дата звернення: 26.09.2025).
4. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. Київ : УкрНДНЦ, 2016. – 16 с.

Плотніков Д.А.
здобувач вищої освіти,
Харківський національний університет міського господарства
імені О.М. Бекетова
Науковий керівник
Сізова Н.Д.
докт.фіз.-мат.наук., професор, професор кафедри комп'ютерних наук та
інформаційних технологій
Харківський національний університет міського господарства
імені О.М. Бекетова

РОЗРОБКА ТА ВПРОВАДЖЕННЯ WEB APP ДЛЯ ІНТЕГРАЦІЇ БІЗНЕС-ПРОЦЕСІВ ЗАЛУЧЕННЯ ГОТІВКОВИХ ТА БЕЗГОТІВКОВИХ ТРАНЗАКЦІЙ

У сучасних умовах розвитку цифрової економіки ефективна інтеграція готівкових та безготівкових транзакцій є ключовим фактором успішного функціонування підприємств у сферах торгівлі, фінансових послуг та сервісного бізнесу. Традиційні системи управління бізнес-процесами часто не забезпечують повноцінну підтримку багатоканальних платежів, що ускладнює роботу з клієнтами та підвищує ризики фінансових помилок [1].

Розробка вебзастосунку (WebApp) для інтеграції бізнес-процесів оплати дозволяє автоматизувати облік операцій, забезпечити прозорість руху коштів та підвищити рівень безпеки фінансових транзакцій.

Зростання обсягів безготівкових платежів і одночасне збереження ролі готівкових операцій потребують створення універсальних систем інтеграції.

Для малого та середнього бізнесу необхідні рішення, що поєднують у собі простоту використання, масштабованість та мінімальні витрати на впровадження.

В умовах цифрової трансформації WebApp на основі сучасних вебтехнологій виступає оптимальним інструментом інтеграції.

Все це підкреслює актуальність теми дослідження.

Мета полягає у створенні прототипу вебзастосунку для інтеграції бізнес-процесів залучення готівкових та безготівкових транзакцій із можливістю подальшого розширення функціоналу.

Основними завданнями визначено.

1. Аналіз існуючих систем і сервісів інтеграції платежів.
2. Визначення архітектури WebApp та вибір оптимальних технологій розробки.
3. Реалізація функціоналу інтеграції готівкових та безготівкових операцій.
4. Забезпечення інформаційної безпеки та відповідності стандартам (PCI DSS, GDPR).

5. Тестування та оцінка ефективності застосунку в умовах реальних бізнес-процесів.

Теоретичні основи у роботі наступні.

Інтеграція бізнес-процесів у сфері платежів охоплює:

- Фінансові бізнес-процеси: приймання, облік, контроль готівкових та електронних операцій.
- Інформаційні бізнес-процеси: передача даних між касовими апаратами, банківськими системами та внутрішніми CRM/ERP.
- Аналітичні бізнес-процеси: формування звітності, прогнозування грошових потоків, виявлення підозрілих транзакцій.

Важливим аспектом є створення єдиної інтеграційної платформи, яка дозволяє уникнути фрагментації даних.

Практична реалізація спрямована на такі питання.

Для реалізації WebApp було обрано технологічний стек:

- Back-end: Node.js + Express для обробки транзакцій та інтеграції з платіжними API.
- Front-end: React для побудови інтерактивного інтерфейсу користувача.
- База даних: MySQL для зберігання операцій та користувацьких даних.
- Інтеграція з API: підключення до банківських шлюзів, платіжних систем (Visa/Mastercard, LiqPay, Stripe), а також внутрішніх касових модулів.

Для реалізації системи WebApp розроблено:

1. Модуль управління готівковими операціями (облік, контроль, верифікація).
2. Модуль безготівкових транзакцій (інтеграція з банківськими та електронними системами).
3. Модуль аналітики (звіти, графіки, прогнозування).
4. Модуль безпеки (шифрування даних, багатофакторна автентифікація).

Очікувані результати передбачають :

- Зменшення часу обробки транзакцій на 30–40% у порівнянні з традиційними системами.
- Підвищення прозорості фінансових потоків за рахунок централізованого обліку.
- Зниження ризиків шахрайських операцій завдяки інтеграції механізмів верифікації.
- Масштабованість рішення для підприємств різного рівня.

Висновки

Система WebApp є ефективним інструментом інтеграції готівкових та безготівкових бізнес-процесів. Його впровадження дозволить:

- автоматизувати фінансові операції;
- підвищити безпеку та надійність;
- адаптуватися до сучасних вимог цифрової економіки.

Подальші дослідження можуть бути спрямовані на використання методів штучного інтелекту для автоматичної класифікації транзакцій, прогнозування фінансових потоків та виявлення аномалій у бізнес-процесах.

Список використаних джерел:

1 McKinsey. The balancing act: Omnichannel excellence in retail banking https://www.mckinsey.com/~media/McKinsey/Industries/Financial%20Services/Our%20Insights/The%20balancing%20act%20Omnichannel%20excellence%20in%20retail%20banking/The-balancing-act-Omnichannel-excellence-in-retail-banking-vF.pdf?utm_source=chatgpt.com

УДК 378:004

Половян Н.С.

*К.е.н., доцент, доцент кафедри організації вищої освіти, управління
охороною здоров'я та гігієни
Донецький національний медичний університет*

ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОГО ПРОФЕСІЙНОГО РОЗВИТКУ ПРАЦІВНИКІВ СФЕРИ ОХОРОНИ ЗДОРОВ'Я

Сучасна медична освіта в Україні перебуває на етапі активної трансформації, коли традиційні методи підготовки фахівців уже не здатні повною мірою відповідати вимогам стрімкого науково-технічного прогресу та викликам глобалізованого світу. Особливо актуальною є проблема впровадження інформаційних технологій (ІТ) у процес додипломної підготовки лікарів і безперервного професійного розвитку (БПР) практикуючих фахівців. Адже здатність швидко реагувати на інновації, оперативно адаптуватися до нових лікувально-діагностичних протоколів та забезпечувати високий рівень послуг пацієнтам стає одним із ключових показників ефективності роботи всієї системи охорони здоров'я.

Упровадження інформаційних технологій у систему безперервного професійного розвитку (БПР) працівників сфери охорони здоров'я вимагає розробки та реалізації продуманих механізмів, які охоплюють технічні, організаційні, методичні та мотиваційні аспекти. Нижче наведено розширений перелік конкретних кроків і рішень, що дають змогу якісно впроваджувати ІТ-інструменти у процесі підвищення кваліфікації медичних працівників та формувати цілісне цифрове середовище для навчання, оцінювання й керування освітніми заходами.

Передусім важливо створити інтегрований веб-портал, у межах якого можна організувати повний цикл навчального процесу: від ознайомлення з доступними програмами чи курсами до формування аналітичних звітів про

успішність слухачів. Така платформа повинна мати зручний інтерфейс і бути оптимізованою для різних пристроїв. Відразу після авторизації користувач отримує доступ до індивідуального кабінету, де може переглядати список актуальних заходів БПР, записуватися на них, реєструватися, оплачувати і отримувати розгорнуту інформацію про розклад та вимоги до учасників. При цьому електронна система може містити автоматизований облік навчальних годин, що спрощує процедуру звітності перед державними органами чи професійними асоціаціями. У разі успішного завершення кожного конкретного курсу слухачеві генерується електронний сертифікат із унікальним ідентифікатором і QR-кодом, який дає змогу швидко перевірити достовірність документа.



Рисунок 1. Механізм функціонування Єдиної електронної платформи (порталу) для реєстрації та управління заходами БПР

Ефективна система БПР повинна містити синхронні та асинхронні формати взаємодії, оскільки в медичній сфері слухачі часто обмежені в часі через роботу в клініках та лікарнях. Для синхронної взаємодії корисно впроваджувати доступ до онлайн-занять у реальному часі (вебінари, майстер-класи, клінічні розбори). Наприклад, заплановані заходи можна інтегрувати з Google Calendar або Outlook, аби слухачі отримували автоматизовані нагадування на електронну пошту й мали швидкий перехід до віртуальної аудиторії (через Google Meet, Zoom або Microsoft Teams). Під час таких онлайн-зустрічей викладач має змогу демонструвати презентації, проводити інтерактивні опитування, обговорювати клінічні кейси, а також

записувати всю сесію, щоб надалі слухачі могли повторно переглянути матеріал.

Водночас асинхронний формат навчання дає змогу працювати з контентом у зручний час та у своєму власному темпі. Для цього зазвичай застосовують платформи на кшталт Moodle чи Google Classroom. Там викладачі розміщують відеолекції, методичні рекомендації, перелік літератури, статті з профільних журналів, інтерактивні презентації тощо. Завдання можуть бути як тестові, так і творчі. Бали, виставлені за кожне виконане завдання, автоматично синхронізуються з електронним журналом, а слухачі отримують сповіщення про нові матеріали чи дедлайни. Таким чином, поєднання синхронного та асинхронного підходів створює гнучку модель, яка враховує особливості графіка медичних працівників і дозволяє їм ефективніше планувати власний час для підвищення кваліфікації.

Щоб забезпечити прозорість процесу БПР і вчасно реагувати на труднощі, необхідно створити потужні інструменти збору й обробки даних. Автоматичний моніторинг відвідуваності, аналіз прогресу та підрахунок часу перебування на платформі дозволяють визначити ступінь залученості слухачів. Окрім цього, викладачам надається можливість детально аналізувати результати проміжних тестів, спостерігати за динамікою успішності й, за необхідності, коригувати освітню програму.

Системне навчання кадрів та мотивація всіх учасників. Ключову роль у впровадженні ІТ-технологій для БПР відіграють люди, які забезпечують навчальний процес і беруть у ньому участь. Щоб викладачі та слухачі ефективно користувалися електронними сервісами, їм потрібна певна підготовка. Першочерговим завданням є організація тренінгів для викладацького складу: теми можуть охоплювати методики створення інтерактивного контенту, способи проведення дистанційних занять, оцінювання завдань, роботу із системою тестування, а також рекомендації щодо ведення онлайн-дискусій і перевірки робіт на плагіат.

Слухачам теж доцільно пропонувати короткі онлайн-курси з цифрової грамотності, покрокові відеоінструкції та консультації. На початкових етапах запровадження платформи особливо корисні тематичні вебінари, де детально показують процес реєстрації, завантаження файлів, виконання тестів, спілкування в чатах тощо. Крім того, важливо розробити систему мотиваційних механізмів – наприклад, відзначення найактивніших викладачів, присвоєння їм статусу «цифрових менторів» із додатковими можливостями. Слухачам можна пропонувати знижки чи пріоритетний доступ до певних програм, якщо вони успішно виконали проміжні тести або продемонстрували високий рівень залученості в цифрове навчальне середовище.

Таким чином, усі перелічені механізми – від автоматизованої реєстрації й управління заходами до використання симуляторів та інструментів аналітики – можуть бути логічно об'єднані в межах єдиної комплексної платформи, яка слугуватиме «цифровим ядром» системи безперервного професійного розвитку.

Список використаних джерел:

1. Баличева Н. Інформаційні технології в освіті. Актуальні питання у сучасній науці. 2024. № 4(22). URL: [https://doi.org/10.52058/2786-6300-2024-4\(22\)-838-847](https://doi.org/10.52058/2786-6300-2024-4(22)-838-847)
2. Мінцер О. П., Жуковський О. М., Грачова Т. І. Формування шляхів створення глобальних, регіональних та персональних освітніх просторів для бпр лікарів та провізорів. Medical informatics and engineering. 2023. № 4. С. 4–8. URL: <https://doi.org/10.11603/mie.1996-1960.2022.4.13409>

УДК 378:004

Половян О.О.

здобувач вищої освіти,

Вінницький національний медичний університет ім. М.І. Пирогова

Лобас В.М.

д.держ.упр., професор завідувач кафедри організації вищої освіти,

управління охороною здоров'я та гігієни

Донецький національний медичний університет

ЦИФРОВІЗАЦІЯ СИСТЕМИ БЕЗПЕРЕРВНОГО ПРОФЕСІЙНОГО РОЗВИТКУ В УКРАЇНІ

Важливим фактором розвитку сучасної системи БПР в Україні є її цифровізація. В умовах цифрової трансформації медицини використання інформаційних технологій набуває особливого значення, стаючи не просто додатковим елементом, а ключовим інструментом розвитку системи БПР. Доступність електронних освітніх ресурсів та платформ дистанційного навчання створює додаткові можливості для швидкого оновлення знань медичних працівників без відриву від основної роботи. Інтеграція сучасних технологій дозволяє забезпечити зручний доступ до навчальних матеріалів, підвищує рівень доступності освітніх заходів та сприяє підвищенню їхньої ефективності.

Одним із ключових напрямів розвитку сучасної системи БПР в Україні є широке впровадження інформаційних технологій (ІТ), які суттєво розширюють можливості для професійного зростання медичних фахівців. Інформаційні технології стали невід'ємною частиною навчального процесу завдяки своїм перевагам, зокрема доступності, економічності та зручності використання.

Використання ІТ-технологій реалізується через низку освітніх платформ, вебсервісів та електронних ресурсів. Серед найбільш популярних і поширених в Україні платформ для дистанційного професійного навчання медичних працівників є платформи Medvoice, Ассемедін та Medplatforma. Ці ресурси надають можливість проходження сертифікованих курсів, онлайн-тренінгів, вебінарів і майстер-класів, що дозволяє здобувати необхідні знання у зручний

для слухачів час, без відриву від основної роботи. Порівняльна таблиця платформ для дистанційного професійного навчання медичних працівників приведена у таблиці 1.

Особливу роль у забезпеченні функціонування сучасної системи БПР відіграють провайдери освітніх послуг вони зобов'язані забезпечити високу якість освітніх послуг, надавати методичний супровід, здійснювати підготовку навчальних матеріалів і контролювати рівень їх відповідності сучасним вимогам медичної науки та практики. Крім цього, вони повинні звітувати перед адміністратором системи БПР щодо результатів своєї освітньої діяльності. Такий контроль дозволяє гарантувати відповідність освітніх заходів міжнародним стандартам якості.

Таблиця 1

Порівняльна таблиця платформ для дистанційного професійного навчання медичних працівників

Платформа	Основні функції	Переваги	Недоліки
Medvoice	Забезпечує онлайн-курси, вебінари, інтерактивні тренінги та дистанційне навчання. Платформа орієнтована на надання широкого спектру освітніх матеріалів для медичних працівників.	• Велика база курсів та навчальних модулів. • Зручний інтерфейс та доступність ресурсів. • Адаптована до потреб користувачів.	• Можливі технічні проблеми в регіонах із слабким інтернетом. • Не завжди актуальний контент для спеціальних груп.
Acce medin	Пропонує сертифіковані тренінги та практичні заняття, часто з акцентом на симуляції та практичне відпрацювання навичок.	• Сильний акцент на практичних аспектах. • Висока якість контенту та інтерактивність занять. • Підвищення практичних навичок.	• Обмежена кількість курсів порівняно з іншими платформами. • Менше онлайн-ресурсів для теоретичного навчання.
Medpl atform a	Функціонує як система обліку балів БПР: реєстрація заходів, моніторинг результатів та планування подальшого професійного розвитку.	• Централізований контроль за освітньою діяльністю. • Зручний інструмент для моніторингу та планування балів. • Прозорість процесу.	• Може бути складною у використанні для користувачів з низьким рівнем комп'ютерної грамотності. • Обмежена інтерактивність.

Завдяки залученню провайдерів створюється конкурентне середовище, що позитивно впливає на якість і різноманітність пропонованих освітніх послуг. Серед провідних провайдерів на українському ринку БПР варто назвати

університети та медичні академії, науково-дослідні інститути, приватні освітні платформи, професійні медичні асоціації та громадські організації.

Ефективність системи БПР підтверджується позитивними змінами в якості медичних послуг. За даними дослідження, проведеного Центром тестування МОЗ України, у лікарів, які регулярно брали участь у заходах БПР, зменшилася кількість помилок при діагностуванні та лікуванні пацієнтів. Зокрема, кількість професійних помилок у лікарів, що набрали необхідну кількість балів БПР, знизилася на 30% порівняно з їх колегами, що не брали активної участі у заходах професійного розвитку [2].

Незважаючи на позитивні результати, впровадження системи БПР в Україні супроводжується низкою проблемних питань і труднощів. Однією з ключових проблем залишається нерівномірність доступу до якісних освітніх заходів. У медичних працівників у великих містах є значно ширший вибір освітніх можливостей порівняно з працівниками сільських та віддалених регіонів. Причиною цього є недостатня інфраструктура, низький рівень технічного забезпечення медичних закладів у віддалених регіонах та недостатній рівень комп'ютерної грамотності серед частини медичних працівників.

Іншою важливою проблемою є нерівномірність якості освітніх послуг, які надаються різними провайдерами БПР. Хоча діяльність провайдерів підлягає контролю, їхні програми можуть значно відрізнятись за рівнем змісту та актуальністю матеріалів. Це зумовлює потребу у впровадженні додаткових механізмів моніторингу якості освітніх програм та сертифікації провайдерів.

Зважаючи на існуючі проблеми та виклики, система безперервного професійного розвитку в Україні потребує подальшого вдосконалення. Основним напрямом подальшого розвитку є поглиблення цифровізації освіти. Подальше розширення доступу до електронних навчальних платформ, створення єдиного загальнонаціонального цифрового порталу для БПР, та запровадження інтерактивних форм навчання можуть значно покращити доступність та ефективність освітніх заходів. [1, с. 36].

Особливу увагу необхідно приділити розширенню можливостей дистанційного навчання та запровадженню єдиних стандартів якості освітнього контенту. Доцільним є також створення окремих освітніх програм для медичних працівників сільських регіонів, що передбачатиме спеціалізовані курси підвищення рівня комп'ютерної грамотності та цифрових компетенцій.

Отже, попри наявні труднощі, система безперервного професійного розвитку медичних працівників в Україні має значний потенціал для подальшого розвитку. Впровадження сучасних інформаційних технологій та ефективних механізмів мотивації дозволить забезпечити високий рівень професійних компетенцій українських медиків та відповідність національної системи охорони здоров'я сучасним світовим стандартам.

Список використаних джерел:

1. Абдін А. В., Лисяк Л. В. Удосконалення методичних засад оцінки ефективності фінансування охорони здоров'я. *Investytsiyi: praktyka ta dosvid*. 2024. № 22. С. 29–37. URL: <https://doi.org/10.32702/2306-6814.2024.22.29>
2. Мінцер О. П., Жуковський О. М., Грачова Т. І. Формування шляхів створення глобальних, регіональних та персональних освітніх просторів для бпр лікарів та провізорів. *Medical informatics and engineering*. 2023. № 4. С. 4–8. URL: <https://doi.org/10.11603/mie.1996-1960.2022.4.13409>

УДК 528.9

Проненко С.С.

здобувач вищої освіти,

Миколаївський національний аграрний університет

Науковий керівник

Борян Л.О.

старший викладач

кафедри економічної кібернетики, комп'ютерних наук

та інформаційних технологій,

Миколаївський національний аграрний університет

ІНФОРМАЦІЙНІ СИСТЕМИ В ГЕОДЕЗІЇ ТА ЗЕМЛЕУСТРОЇ

Рациональне і безпечне управління земельними ресурсами в сучасних умовах неможливе без використання інформаційних систем, що об'єднують просторові дані різних джерел і надають інструменти для аналізу, візуалізації та документування. Публічна кадастрова карта та відповідні електронні сервіси державних органів становлять основу для доступу до інформації, однак для практичної роботи інженера-землевпорядника необхідна більш глибока інтеграція: ГІС як платформа для роботи, автоматизовані модулі кадастру для реєстрації назв і прав, а також модулі обробки даних з БПЛА, супутників і тахеометричних комплексів. В Україні працюють державні платформи й сервіси, що надають публічні та професійні інструменти для роботи з кадастром, і їх інтеграція з ГІС забезпечує масштабованість і сумісність даних.

Значущість використання БПЛА у кадастрових і землевпорядних роботах полягає у можливості швидко та недорого отримати високоякісні ортофотознімки і цифрові моделі території для ділянок різних масштабів. Дані, отримані з дронів, дозволяють здійснювати детальну інвентаризацію рослинності, моніторити зміни у землекористуванні та виявляти несанкціоновані втручання. Запропонований робочий процес включає планування польоту, збір зображень із належним перекриттям, геоприв'язку через контрольні точки або GNSS-RTK, фотограмметричну обробку для створення ортофотоплану й тривимірної моделі, а потім імпорт результатів у ГІС для подальшого аналізу і додавання до кадастру. Практика з використання

безпілотників для локального картографування підтверджується міжнародними дослідженнями й прикладами, які демонструють ефективність цих методів для створення якісних карт для місцевих громад і державних органів.

Для досягнення високої точності просторових вимірювань, які важливі при визначенні меж ділянок і складанні кадастрових планів, широко використовують GNSS-приймачі у режимі RTK (Real-Time Kinematic) або застосовують методи постобробки, такі як PPP/PPK. Сучасні системи RTK здатні забезпечити точність у межах кількох сантиметрів у реальному часі за умови правильної організації базової станції або підключення до мережі опорних пунктів; це дозволяє істотно зменшити час польових робіт і підвищити точність вихідних координат для подальшої обробки у ГІС. Водночас рівень точності й стабільності визначаються типом приймача, кількістю супутникових систем (GPS, GLONASS, Galileo, BeiDou), умовами огляду неба та використовуваними методами корекції.

ГІС-платформи, включаючи комерційні та відкриті проекти, відіграють важливу роль у землевпорядкуванні, виконуючи кілька основних завдань: вони дозволяють об'єднувати багатошарові геодані (кадастрові шари, аерофото, супутникові знімки, цифрові моделі рельєфу), використовувати інструменти просторової аналітики для визначення придатності земельних ділянок, автоматично перевіряти цілісність просторових даних і створювати тематичні карти для прийняття управлінських рішень. Інтеграція з нормативно-правовими реєстрами та сервісами сприяє автоматичному оновленню додаткової інформації, що знижує ризик помилок у оформлюваних документах. Сучасна практика часто включає поєднання роботи з QGIS для підготовки і перевірки даних із використанням ArcGIS або інших корпоративних ГІС-рішень для інтеграції у державні робочі процеси.

Об'єднання різноманітних даних, таких як польові тахеометричні зйомки, точкові дані GNSS, ортофотоплани, отримані з БПЛА, та супутникові знімки, у єдиній ГІС-системі надає можливість здійснювати багатовимірний моніторинг якості. Це включає порівняння меж ділянок, контроль відповідності реального використання землі з офіційними даними, а також просторовий аналіз потенційних ризиків ерозії, підтоплень і забудови. Автоматизація таких процесів дозволяє швидше готувати документи, підвищує прозорість роботи й швидко реагувати на порушення. Водночас необхідно враховувати особливості системи координат, формати даних і метаданих при обміні інформацією між системами, щоб уникнути втрати точності та появи неточностей при об'єднанні різних шарів.

Майбутній розвиток галузі пов'язаний із розгортанням мережі опорних GNSS-станцій та впровадженням універсальних стандартів обміну даними, таких як LADM/ISO 19152 для кадастрової документації. Очікується активне застосування супутникового моніторингу для систематичного контролю великих територій і створення сучасних хмарних платформ GIS для швидкого доступу та спільної роботи фахівців. Реальні переваги таких підходів включають покращення точності кадастрових даних, скорочення термінів виконання робіт, зниження витрат і підвищення громадської довіри до рішень у

сфері земельних відносин. Втім, для досягнення цих цілей необхідно поєднання технічних нововведень, регуляторної підтримки і підготовки кадрів: навчання спеціалістів, адаптація нормативних актів до сучасних методів збору даних та забезпечення доступу до високоякісних геопросторових сервісів.

Список використаних джерел:

1. Офіційний сайт Державної служби України з питань геодезії, картографії та кадастру – інформація про Публічну кадастрову карту та е-послуги. URL: https://land.gov.ua/?utm_source=chatgpt.com
2. Janos D. et al., Evaluation of low-cost RTK GNSS receiver – приклади точності RTK та практичні значення для геодезії (джерело про сантиметрову точність приладів). URL: https://www.sciencedirect.com/science/article/pii/S0263224122008570?utm_source=chatgpt.com

УДК 004.8

Проценко Н.М.

*к.е.н, доцент, доцент кафедри інформаційних технологій,
кібернетики та захисту інформації
Державний біотехнологічний університет*

ІНТЕЛЕКТУАЛЬНА ОБРОБКА ДАНИХ ТА ХМАРНІ ТЕХНОЛОГІЇ: СТРАТЕГІЇ ВПРОВАДЖЕННЯ НА ПІДПРИЄМСТВІ

Продуктивність та успіх будь-якої організації залежать від ефективного управління даними та документами. Протягом багатьох років обробка документів змінилася від ручної обробки до цифрового зберігання файлів. Зміни, що відбуваються в цьому напрямку, є дуже важливими для бізнесу. Використання новітніх інформаційних технологій відкриває чимало можливостей для підвищення ефективності та економії коштів. Компанії, впроваджуючи інтелектуальну обробку даних (IDP), можуть зменшити кількість помилок, пов'язаних з ручним обробленням, пришвидшити прийняття рішень та зосередитися на стратегічних ініціативах. Однак, глобальне генерування даних продовжує прискорюватися, і обробка даних в хмарних обчисленнях стає наріжним каменем цифрової трансформації.

Еволюція можливостей хмарних технологій засвідчила зміну парадигми від традиційних систем пакетної обробки, які могли обробляти лише до 20000 транзакцій за секунду, до складних архітектур потокової обробки, які тепер обробляють понад 1 мільйона подій за секунду в розподілених середовищах [1, С. 323]. Ці можливості стають дедалі важливішими: за даними німецького статистичного порталу Statista у 2024 році глобальний обсяг створених, зібраних, скопійованих та спожитих даних становив 149 зеттабайтів. Очікується, що до кінця 2025 року цей показник досягне 181 зеттабайта (для

порівняння, зеттабайт еквівалентний зберігання 250 мільярдів DVD-дисків). Недавні аналітичні дослідження показують, що приблизно 90 % світових даних було згенеровано протягом останніх двох років, і, за даними IDC, обсяг даних, що зберігаються в усьому світі, подвоюється приблизно кожні чотири роки. Щодня генерується приблизно 402,74 мільйона терабайтів даних, що охоплює новостворену, захоплену, скопійовану та спожиту інформацію [2]. Це зростання зумовлене збільшенням використання пристроїв Інтернету речей, обробкою даних у режимі реального часу та хмарним сховищем і відображає всеосяжну цифровізацію глобальної діяльності: від споживчих додатків до промислових операцій, включаючи попит на аналітику в режимі реального часу, автоматизацію та ефективні рішення для зберігання даних, і підкреслює необхідність передових рішень для зберігання та надійних систем управління даними в цьому безпрецедентному за масштабами інформаційному середовищі.

Мільярди взаємопов'язаних датчиків, пристроїв та машин безперервно виробляють величезні обсяги структурованих і неструктурованих даних, що сприяє формуванню того, що зараз називають великими даними. Обсяг, швидкість та різноманітність даних, які виробляються, перевищують можливості традиційних систем обробки даних. Такий стан подій вимагає більш надійних та гнучких обчислювальних інфраструктур.

Питання інтеграції інтелектуальної обробки даних з хмарними обчисленнями для аналізу великих даних широко обговорюються в дослідницьких спільнотах. На ранніх етапах досліджень в цьому напрямку вчені наголошували на необхідності рішень проміжного програмного забезпечення, які могли б сприяти безперебійній передачі даних між периферійними пристроями та централізованими центрами обробки даних. У новіших роботах досліджуються хмароорієнтовані фреймворки, що підтримують аналітику великих даних, використовуючи такі технології, як Hadoop, Spark та Apache Storm. Ці платформи пропонують розподілені можливості обробки, які добре підходять для обробки великомасштабних наборів даних, що генеруються системами IDP.

У сучасному світі IDP використовує штучний інтелект та машинне навчання для чіткого зчитування деталей у документах. Це рішення дозволяє обробляти різні формати даних – структуровані, напівструктуровані чи неструктуровані, гарантуючи, що дані сумісні з цільовими системами та готові до аналізу, та зменшуючи потребу в ручному втручанні. Багато власників бізнесу називають цей інструмент справжнім переломним моментом. Статистичні показники від Statista вказують, що 77 % організацій у всьому світі використовують великі дані для стимулювання інновацій, тоді як близько 50 % покладаються на дані для підвищення своєї конкурентоспроможності, що підкреслює критичну роль цієї технології в сучасних бізнес-операціях [3].

Інтелектуальна обробка даних використовує штучний інтелект та автоматизацію для вилучення, інтерпретації та обробки даних з документів та інших джерел, тоді як хмарні технології забезпечують масштабовану інфраструктуру на вимогу для підтримки цих процесів. Це поєднання дозволяє компаніям автоматизувати завдання, підвищувати ефективність та отримувати

аналітику з величезних обсягів даних. Галузеві аналітичні звіти свідчать, що компанії, які впроваджують ці рішення для обробки даних, повідомляють про скорочення операційних витрат на 42 %, покращення показників задоволеності клієнтів на 31 %, збільшення швидкості реагування на ринок на 28 %, скорочення часу простою системи на 67 % та покращення використання ресурсів на 45 % у своїй хмарній інфраструктурі.

Особливу увагу привертають гібридні моделі, які розподіляють завдання обробки між периферійним та хмарним рівнями (83 % організацій з усього світу застосовують гібридні підходи) [4]. Завдяки використанню граничних вузлів для попередньої фільтрації даних та виявлення аномалій, резервуючи хмарну інфраструктуру, досягається довгострокове зберігання та поглиблення аналізу. Алгоритми машинного та глибокого навчання також використовуються разом із хмарними платформами для покращення можливостей прогнозування та розпізнавання образів. Такі програми, як розумне сільське господарство, промисловий Інтернет речей та інтелектуальні транспортні системи, отримали значні переваги від цих інновацій.

Дуже важливими є питання своєчасного надання ресурсів та еластичність. Оскільки хмарні обчислення дозволяють надавати ресурси на вимогу, підприємства можуть масштабуватися у відповідь на коливання робочого навантаження. Ця гнучкість необхідна для управління різним ступенем вимог до обробки даних у реальному часі. Організації можуть розширювати свою інфраструктуру відповідно до фактичного попиту, уникаючи надмірного виділення ресурсів та мінімізуючи непотрібні витрати протягом періодів низької активності.

Проте, незважаючи на усі позитивні моменти, важливо розуміти труднощі та фактори, що пов'язані з практичним впровадженням IDP у хмарі. Проблеми управління даними, безпеки та конфіденційності залишаються значними та потребують постійного розгляду та інноваційних рішень. Для захисту конфіденційних даних зацікавлені сторони повинні надати головний пріоритет надійним системам кібербезпеки та відповідності. Компанії, що надають хмарні послуги, роблять значні інвестиції з метою дотримання правил, стандартів та інструкції щодо IT-безпеки [5]. Це критично важливо для галузей, що працюють з конфіденційними даними, забезпечуючи відповідність процесів аналізу даних нормативним вимогам.

Інтелектуальна обробка даних та хмарні обчислення разом пропонують проривну синергію, яка має величезні перспективи для бізнесу в різних секторах. Окрім забезпечення ефективної обробки та аналізу великих обсягів інформації, поєднання цих передових технологій пропонує масштабованість, гнучкість та економічну ефективність, яких ніколи раніше не було. Додавання тонкощів сучасного бізнес-середовища завдяки поєднанню аналітики великих даних та хмарних обчислень стає каталізатором інновацій, що починають нову еру продуктивності, ефективності та конкурентоспроможності у швидко розвиваючій сфері сучасного бізнесу.

Список використаних джерел

1. Технології сучасних кібер-фізичних систем: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2020. 327 с.
2. Bartley K. Big data statistics: How much data is there in the world? [Електронний ресурс]. Доступно URL: <https://rivery.io/blog/big-data-statistics-how-much-data-is-there-in-the-world/>.
3. Top 9 Data and Analytics Trends to Watch in 2025. [Електронний ресурс]. Доступно URL: <https://intellias.com/data-analytics-trends/>.
4. Mounica Achanta, «The Impact of Real-Time Data Processing on Business Decision – making.» International Journal of Scientific Research, vol. 13, no. 7, July. 2024. [Електронний ресурс]. Доступно URL: <https://www.ijsr.net/archive/v13i7/SR24708033511.pdf>.
5. A. Johannsen, D. Kant, and R. Creutzburg, Measuring IT security, compliance and data governance within small and medium-sized IT enterprises, Electronic Imaging, 2020, 2020(3), pp. 252-1-252-11. [Електронний ресурс]. Доступно URL: <https://library.imaging.org/ei/articles/32/3/art00005>.

УДК 004.056.53

Проценко П.Р.

здобувач вищої освіти,

Харківський національний університет радіоелектроніки

Науковий керівник

Тітова О.В.

к.т.н., доцент кафедри інформатики, доцент

Харківський національний університет радіоелектроніки

АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ДЛЯ ОПТИМІЗАЦІЇ УПРАВЛІННЯ БІЗНЕС-ПРОЦЕСАМИ БАГАТОПРОФІЛЬНИХ ПІДПРИЄМСТВ

У сучасних умовах ведення бізнесу компанії стикаються з високим рівнем конкуренції, швидкою зміною ринкових тенденцій та постійним ускладненням регуляторних вимог. Це призводить до того, що управління підприємством за допомогою лише традиційних методів — паперових документів чи простих облікових програм — стає неефективним і навіть ризикованим. Саме тому виникла потреба у комплексних інформаційних системах, які б могли не лише вести бухгалтерський облік, а й інтегрувати всі ключові бізнес-процеси підприємства.

В Україні таку нішу зайняли програмні продукти Business Automation Software (BAS).

Одним із найбільш комплексних продуктів лінійки є BAS ERP, що орієнтований на середні та великі підприємства з багатопрофільною структурою. Це рішення охоплює практично всі сфери діяльності підприємства — від виробництва й логістики до управління фінансами та персоналом. Його

ключовою перевагою є повна інтеграція бізнес-процесів у єдиній системі, що забезпечує прозорість управління та можливість контролю на всіх рівнях. Крім того, BAS ERP підтримує гнучке налаштування під специфіку діяльності компанії, дозволяє формувати розширену аналітику та здійснювати бюджетування. Разом із тим, варто враховувати, що впровадження цієї системи є довготривалим і ресурсомістким процесом: від шести місяців до півтора року, залежно від масштабу компанії та складності інтеграцій. Також суттєвим бар'єром для невеликих організацій виступає висока вартість ліцензій, налаштування і супроводу, що робить BAS ERP менш привабливим для малого бізнесу[1].

Для компаній середнього масштабу часто обирають BAS Комплексне управління підприємством (BAS КУП). Це рішення позиціонується як більш доступна альтернатива BAS ERP, яке водночас дозволяє охопити ключові напрями діяльності: фінанси, закупівлі, продажі, складський облік і виробничі процеси. Його основною перевагою є баланс між функціональністю та вартістю: система впроваджується швидше, ніж ERP, і потребує менших витрат на обслуговування. Разом із тим, BAS КУП має певні обмеження. Наприклад, його модулі аналітики та виробництва менш глибокі, ніж у BAS ERP, а також існують обмежені можливості для масштабування в умовах великого підприємства. Таким чином, це рішення можна розглядати як перехідний етап для тих компаній, які з часом планують перейти на повноцінну ERP-систему[2].

Важливим сегментом у продуктивній лінійці виступає BAS Управління торгівлею (BAS УТ). Система орієнтована насамперед на торговельні підприємства — як оптові, так і роздрібні. Вона надає можливість ефективно управляти закупівлями, продажами та складськими залишками, а також має базові CRM-функції для роботи з клієнтами. Її сильними сторонами є підтримка різних схем ціноутворення, управління знижками та акційними програмами, а також інтеграція з касовим обладнанням та онлайн-торгівлею. Однак, у BAS УТ відсутні можливості управління виробництвом, а фінансові модулі представлені у спрощеній формі. Це створює необхідність інтеграції з бухгалтерськими рішеннями для повноцінного ведення обліку. Для великих торгових мереж таке рішення може потребувати значних доопрацювань, аби відповідати їхнім вимогам.

Таким чином, кожне з цих рішень має свою сферу оптимального застосування: BAS ERP орієнтоване на великі корпорації, BAS КУП — на середній бізнес, тоді як BAS УТ є найкращим вибором для торговельних підприємств. Це підтверджує, що ефективність використання BAS-продуктів залежить не лише від функціональності системи, але й від її відповідності потребам конкретної організації.

Слід зазначити, що BAS-продукти потребують не тільки врахування масштабів та цілей організації, а й певних заходів щодо їх оптимізації під існуючі задачі. Для цього проводиться аналіз поточної роботи СУБД, діагностика продуктивності системи в різних конфігураціях та умовах навантаження. Робота з СУБД передбачає оптимізацію запитів, застосування індексів для прискорення вибірки даних, контроль блокувань та транзакцій, а

також коректну організацію структури бази даних. Важливим аспектом є розподіл навантаження між серверами, налаштування кешування та моніторинг ресурсів (CPU, RAM, дискових операцій), що дозволяє знизити час відгуку системи та уникати «вузьких місць».

Список використаних джерел:

1. Kostiuk, V. V. (2020). ERP systems as a tool for improving enterprise management efficiency. *Business Inform*, (6), 112–118.
2. Ihnatenko, M. (2021). Implementation of information systems for business process management of enterprises: current state and prospects. *Economy and Society*, (31), 45–52.

УДК 37.07:004.67

Рава А.В.

здобувач вищої освіти,

Центральноукраїнський державний університет імені Володимира Винниченка,

м. Кропивницький, Україна

Лупан І.В.

к. п. н., доцент, доцент кафедри інформаційних та цифрових технологій

Центральноукраїнський державний університет імені Володимира Винниченка,

м. Кропивницький, Україна

РОЗРОБКА ДИЗАЙНУ ДАШБОРДУ ДЛЯ ВІЗУАЛІЗАЦІЇ ВІДКРИТИХ ДАНИХ ЄДЕБО

Сучасна освіта дедалі більше спирається на цифрові рішення, які забезпечують швидкий доступ до даних, їх аналіз і презентацію у зручному вигляді. Одним із найбільш ефективних інструментів для цього є інформаційні панелі (дашборди), за допомогою яких можна здійснювати комплексний аналіз ключових показників освітнього процесу та представляти результати у наочній формі [1; 2; 3].

Завдання нашого дослідження полягало у розробці дашборду на основі відкритих даних, розміщених на сайті *Єдиної державної електронної бази з питань освіти* (ЄДЕБО), зокрема даних про кількість осіб, зарахованих на навчання, у період з 2022 по 2024 р.р. [4].

На першому етапі розробки за допомогою засобу Google Looker Studio було створено тестовий дашборд для відстеження динаміки вступних кампаній та визначення популярних спеціальностей. Проте він мав істотні недоліки (Рис. 1): недостатньо гармонійне візуальне оформлення, обмеження списку спеціальностей та ЗВО тощо.

2. Розширення списку спеціальностей і ЗВО.

Попередня версія дашборду показувала лише топ-10 спеціальностей, що обмежувало можливість аналізу менш популярних напрямів. Також обмеженим був і перелік ЗВО.

У вдосконаленій версії:

- додано динамічні фільтри (drop-down та multi-select), які дозволяють користувачам обирати як одну, так і кілька спеціальностей чи університетів (рис. 3);
- реалізовано таблицю з повним переліком спеціальностей і ЗВО з пагінацією та сортуванням, що дає змогу швидко переходити між сторінками та знаходити потрібні дані (рис. 3);
- забезпечено поєднання режимів «топ-N» і «повний список», що дає змогу гнучко варіювати масштаб аналізу.

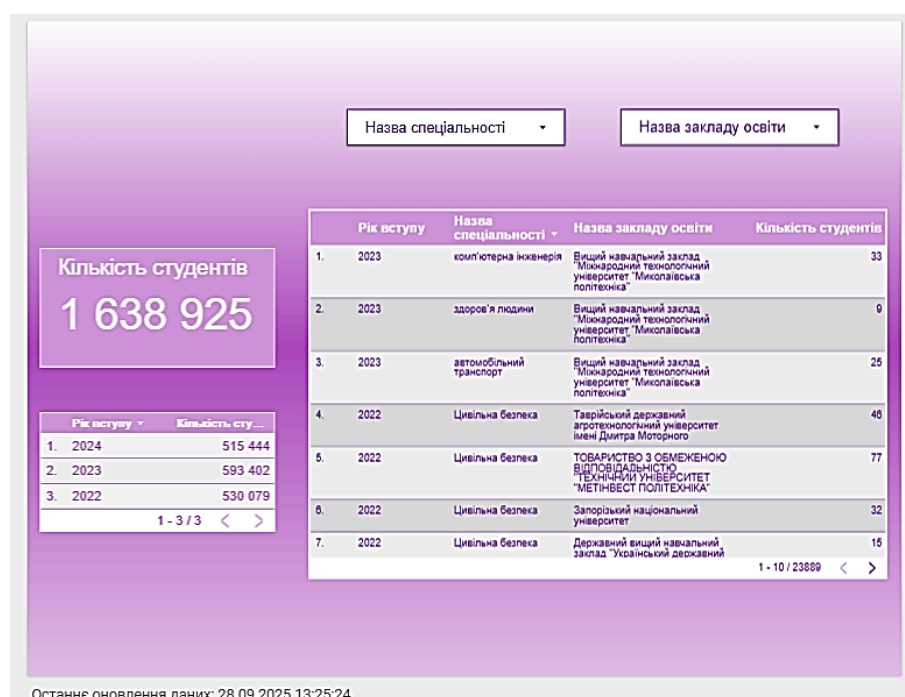


Рис. 3

Після внесення змін дашборд отримав низку переваг:

- сучасний і візуально привабливий дизайн, що сприяє кращому сприйняттю інформації;
- зручну навігацію завдяки логічному розташуванню блоків та підписів;
- можливість аналізувати як найпопулярніші, так і менш поширені спеціальності та університети.

Отже, єдина кольорова палітра, структурованість і впровадження динамічних фільтрів значно розширили аналітичні можливості панелі. Однак для здійснення більш глибокого аналізу опублікованих освітніх даних бажано продовжити роботу над розробкою дашборду та долучити дані за більш тривалий період і врахувати такі дані, як освітній рівень, основа вступу, регіон.

Список використаних джерел:

1. Окунькова О.О. Візуалізація даних. Від простого до складного // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки, 2022. – №3. – С.61–66.
2. Lavanya A., Sindhuja S., Gaurav L., Ali W. A Comprehensive Review of Data Visualization Tools: Features, Strengths, and Weaknesses. International Journal of Computer Engineering in Research Trends. Vol.10 (1), 2023. – С.10-20.
3. Yigitbasioglu O.M., Velcu O. A review of dashboards in performance management: Implications for design and research. International Journal of Accounting Information Systems. 2012. – Vol.13 (1). – С.41-59.
4. Реєстр суб'єктів освітньої діяльності: Кількість осіб, зарахованих на навчання. URL: <https://registry.edbo.gov.ua/opendata/entrant/> (дата звернення: 25.07.2025)

УДК 004.056.53

Савченко С.В.

здобувач вищої освіти,

Миколаївський національний аграрний університет

Науковий керівник

Борян Л. О.

старший викладач кафедри економічної кібернетики, комп'ютерних наук та

інформаційних технологій,

Миколаївський національний аграрний університет

ВИКОРИСТАННЯ CHATGPT ТА ШТУЧНОГО ІНТЕЛЕКТУ У НАВЧАННІ: МОЖЛИВОСТІ, ПЕРЕВАГИ ТА РИЗИКИ

Раціональне використання сучасних цифрових технологій у сфері освіти є одним із головних факторів підвищення її якості та конкурентоспроможності. Освітня сфера постійно перебуває в стані змін, і нові інструменти дають змогу удосконалювати як зміст, так і методи викладання. Сьогодні університети та школи дедалі частіше інтегрують у навчальний процес інноваційні рішення, адже саме вони дозволяють оптимізувати роботу викладачів, зробити навчання більш гнучким, різноманітним і доступним для широкого кола студентів. Стрімкий розвиток штучного інтелекту (ШІ) створив абсолютно нові можливості для освітнього середовища, відкривши доступ до ресурсів, які дозволяють швидко отримувати знання, моделювати складні процеси, проводити експерименти у віртуальному середовищі та організовувати навчання у новому, зручнішому форматі. Одним із найпопулярніших і найбільш обговорюваних інструментів сьогодення є ChatGPT, що вже знайшов застосування не лише у сфері освіти, а й у повсякденному житті, допомагаючи людям вирішувати завдання різного рівня складності.

Штучний інтелект відкриває широкі перспективи у сфері навчання і стає своєрідним помічником як для викладачів, так і для студентів. ChatGPT здатний швидко генерувати пояснення до складних тем, пропонувати варіанти розв'язання задач, допомагати у вивченні іноземних мов завдяки перекладам, тренуванню діалогів і навіть моделюванню реальних комунікативних ситуацій. Такий підхід дозволяє студентам не просто механічно засвоювати матеріал, а й формувати цілісне розуміння теми. Наприклад, у процесі підготовки до семінарів або іспитів студенти можуть попросити модель скласти перелік основних понять, пояснити теорію простими словами чи дати визначення ключових термінів. Це особливо цінно у дисциплінах із великою кількістю формул і абстрактних понять, як-от геодезія, фізика або вища математика. Для майбутніх геодезистів ChatGPT може пояснити алгоритм обчислення координат або згенерувати тестові завдання для самоперевірки. Крім того, ШІ здатен автоматично створювати конспекти, плани занять, презентації чи інші навчальні матеріали, що значно економить час і сили студентів. Це дозволяє спрямувати увагу не лише на заучування, а й на аналіз, критичне мислення та практичні навички.

Особливе значення у використанні ChatGPT має персоналізоване навчання. На відміну від традиційних підходів, де для всіх студентів пропонується єдина програма і матеріали, штучний інтелект здатен пристосовувати інформацію до потреб кожного учня. Модель може пояснити тему максимально простими словами для новачка або надати більш складні приклади, детальні пояснення та навіть посилання на наукові джерела для тих, хто прагне заглибитись у тему. Це робить навчання індивідуалізованим і враховує різний рівень підготовки студентів. Такий підхід створює нові можливості: один студент може зосередитися на базових завданнях, тоді як інший одразу переходить до більш складних викликів. Наприклад, під час вивчення іноземної мови один студент може просити перекладати прості речення й тренувати базову лексику, тоді як інший практикує написання есе чи ділових листів. Це дозволяє кожному просуватися у власному темпі й отримувати саме ті знання, які потрібні для досягнення конкретних цілей.

Окремо варто відзначити можливості ChatGPT у створенні інтерактивних навчальних матеріалів. Завдяки йому студенти та викладачі можуть розробляти рольові діалоги, навчальні ігри, інтерактивні квести чи сценарії для практичних занять. Такий підхід робить навчання більш живим, захопливим і практично орієнтованим. Наприклад, під час вивчення іноземних мов студенти можуть «спілкуватися» з моделлю у вигляді віртуального співрозмовника, відпрацьовуючи вимову, граматику та лексику у реалістичних діалогах. Для економістів ChatGPT може створювати бізнес-ситуації з ринковими коливаннями, де потрібно ухвалювати рішення. Для інженерних спеціальностей модель може запропонувати різноманітні задачі, поступово ускладнюючи їх, що дозволяє студентам переходити від простих прикладів до реальних виробничих ситуацій.

Не менш важливим напрямом розвитку є інтеграція ChatGPT у адаптивні освітні платформи. Сучасні онлайн-сервіси, як-от Duolingo чи Coursera, вже

активно застосовують технології штучного інтелекту для створення індивідуальних траєкторій навчання. Такі системи аналізують результати студентів, враховують їхні помилки, темп навчання та пропонують завдання відповідного рівня складності. У результаті кожен студент отримує персоналізований освітній маршрут. Подібний підхід можна застосовувати і в українських університетах: наприклад, у вигляді платформ для самоперевірки знань, де завдання поступово ускладнюються залежно від досягнень студента. Це дозволяє не лише закріпити матеріал, а й підтримати інтерес до навчання, адже студенти бачать власний прогрес у реальному часі.

Використання ChatGPT у навчанні має цілу низку очевидних переваг. По-перше, це висока доступність та швидкість отримання інформації: студент може поставити запитання і вже за кілька секунд отримати відповідь. Це надзвичайно актуально в умовах обмеженого часу, особливо під час підготовки до іспитів чи захисту робіт. По-друге, інструмент дозволяє значно економити час, автоматизуючи рутинні процеси, такі як підбір літератури, складання планів або створення коротких конспектів. По-третє, ChatGPT підтримує розвиток самостійності й критичного мислення, адже студент отримує не готовий кінцевий результат, а основу, з якої він може почати власне дослідження. Важливо також, що штучний інтелект сприяє інклюзивності: завдяки голосовим інтерфейсам та текстовим підказкам він допомагає студентам з особливими потребами. Це означає, що навіть ті, хто стикається з труднощами у традиційному навчанні, отримують шанс на рівний доступ до знань.

Разом з тим широке використання ChatGPT має і свої ризики. Однією з основних проблем є недостовірність або застарілість даних, адже модель не завжди гарантує абсолютну точність. Крім того, існує загроза академічній доброчесності: студенти можуть використовувати ШІ для автоматичного написання робіт, не докладаючи власних зусиль. Це, своєю чергою, знижує рівень їхньої самостійності та здатність до аналітичного мислення. Ще одним викликом є ризик залежності від технологій, коли навчання фактично зводиться до використання лише цифрових інструментів. Також важливим аспектом є безпека персональних даних, адже будь-які онлайн-сервіси пов'язані з можливістю витоку інформації. Усі ці фактори потребують уважного контролю з боку викладачів та усвідомленого ставлення самих студентів.

Отже, ChatGPT та інші системи штучного інтелекту є потужним засобом трансформації освітнього процесу. Вони створюють умови для швидкого доступу до знань, розвитку персоналізованого навчання та побудови інтерактивних освітніх середовищ. Завдяки інтеграції в освітні платформи ШІ сприяє формуванню більш гнучких моделей навчання, де кожен студент може обрати власну траєкторію. Водночас для уникнення негативних наслідків важливо формувати культуру відповідального використання ШІ, що забезпечить баланс між технологічними можливостями та розвитком мислення, творчості й критичного аналізу студентів.

Список використаних джерел:

1. Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., ... & Wamba, S. F. (2023). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 71, 102642.
2. Kasneci, E., Sessler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., ... & Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. *Learning and Individual Differences*, 103, 102274.
3. Риженко О. С., Левченко Н. В. Використання штучного інтелекту в освітньому процесі: переваги та виклики. *Інформаційні технології і засоби навчання*, 2023, Т. 96, № 4. С. 24–39.

УДК 004.891

Сазонов В.О.

здобувач вищої освіти,
ХНУМГ імені О.М.Бекетова
Науковий керівник
Новожилова М.В.

Доктор фізико-математичних наук, професор, завідувач кафедри
комп'ютерних наук та інформаційних технологій
ХНУМГ імені О.М.Бекетова

РЕКОМЕНДАЦІЙНІ ПІДСИСТЕМИ ПЕРЕГЛЯДУ СЕРІАЛІВ ЯК СКЛADOBA СУЧАСНИХ ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Сучасний цифровий простір характеризується стрімким зростанням кількості аудіовізуального контенту, що пропонується користувачам через різні онлайн-платформи. Значне розширення асортименту серіалів ускладнює вибір і часто призводить до інформаційного перевантаження. Користувач витрачає все більше часу на пошук відповідного матеріалу, що знижує ефективність споживання контенту та негативно впливає на загальне враження від сервісу. Тому виникає потреба у створенні систем, здатних інтелектуально аналізувати дані про глядацькі вподобання, формувати персоналізовані рекомендації та автоматизувати процес вибору [1].

В основі рекомендаційних рішень лежать методи машинного навчання, що дозволяють будувати математичні моделі взаємодії користувача з контентом і прогнозувати його інтереси на основі попередньої активності. Традиційні підходи, які базуються на простому рейтинговому оцінюванні чи загальних трендах, дедалі частіше виявляються недостатніми, адже вони не враховують індивідуальних особливостей глядача та не забезпечують високого рівня

персоналізації. Застосування методів обробки великих даних у поєднанні з алгоритмами класифікації та кластеризації дозволяє створити гнучкі системи, здатні постійно вдосконалювати якість рекомендацій за рахунок накопичення нового досвіду [2].

Рекомендаційна підсистема для перегляду серіалів повинна враховувати не лише явні сигнали, як-от оцінки чи лайки, а й приховані патерни поведінки, включаючи час перегляду, кількість завершених епізодів, повторні перегляди та взаємозв'язки між жанрами. Аналіз цих даних дає можливість виділити ключові фактори, які впливають на інтерес користувача. Наприклад, глядач, який переглянув кілька серіалів з однією сюжетною тематикою або в подібному стилістичному виконанні, із високою ймовірністю зацікавиться новим контентом тієї ж категорії. Таким чином, підсистема здатна виявляти приховані закономірності, які неможливо визначити без застосування складних алгоритмів.

Одним із ключових аспектів є використання методів колаборативної фільтрації, які дозволяють знаходити подібності між користувачами за схожістю їхніх уподобань. Якщо певна група глядачів проявляє схильність до однакових серіалів, то система може рекомендувати новий контент усім представникам цієї групи. Паралельно застосовуються алгоритми контентного аналізу, що зосереджуються на властивостях самих серіалів, таких як жанр, акторський склад, режисерський підхід чи наративні особливості. Поєднання цих підходів забезпечує більш точні та різнобічні результати, оскільки враховується як індивідуальна поведінка користувача, так і структурні характеристики контенту.

У цьому контексті особливого значення набуває метод Аpriori, який широко застосовується для виявлення асоціативних правил у великих наборах даних. Його принцип базується на пошуку часто повторюваних комбінацій об'єктів і формуванні закономірностей, що описують їхню спільну появу. Для підсистеми рекомендацій перегляду серіалів цей підхід може бути використаний з метою виявлення неочевидних зв'язків між різними назвами та жанрами [3]. Якщо значна кількість користувачів після завершення перегляду певного драматичного серіалу переходить до науково-фантастичних сюжетів, то система, спираючись на результати алгоритму Аpriori, здатна сформулювати правило, що поєднує ці категорії. Це дозволяє рекомендувати подібні переходи іншим глядачам і збагачує досвід взаємодії користувачів із платформою. Такий підхід сприяє підвищенню точності персоналізованих рекомендацій та формує більш різноманітний набір пропозицій.

Важливу роль у створенні підсистеми відіграє робота з великими обсягами даних. Оскільки платформи для перегляду серіалів оперують мільйонами записів, що постійно оновлюються, необхідно застосовувати методи розподіленої обробки та оптимізовані алгоритми. Системи машинного навчання повинні бути здатними масштабуватися, аби підтримувати зростаючий обсяг користувацької активності та забезпечувати безперервність процесу формування рекомендацій. Використання хмарних технологій у поєднанні з інструментами обробки потокових даних дозволяє скоротити затримку між

моментом отримання інформації та її аналізом, що забезпечує своєчасність рекомендацій.

Окремим викликом є необхідність забезпечення інтерпретованості моделей. Незважаючи на високу точність прогнозів, користувачі часто прагнуть розуміти, чому саме їм було запропоновано той чи інший серіал. Тому сучасні підсистеми повинні надавати пояснення рекомендацій, наприклад, через підсвічування спільних характеристик з попередньо переглянутим контентом. Це підвищує довіру до системи й мотивує до подальшої взаємодії.

Не менш важливим є питання етичності й захисту персональних даних. Оскільки рекомендаційні механізми ґрунтуються на зборі та аналізі великої кількості інформації про поведінку користувачів, виникають ризики, пов'язані з порушенням приватності. Тому розробка таких систем потребує впровадження методів анонімізації, диференційної приватності та надійних протоколів шифрування. Забезпечення безпеки даних сприяє формуванню позитивного ставлення до сервісу та підвищує рівень довіри аудиторії.

Ефективність рекомендаційної підсистеми визначається не лише точністю прогнозів, а й здатністю адаптуватися до змін у поведінці користувачів. Інтереси глядачів можуть змінюватися під впливом сезонних трендів, появи нових жанрів чи соціальних факторів. Алгоритми машинного навчання повинні бути чутливими до цих змін і забезпечувати динамічне оновлення моделей. Одним із перспективних напрямів розвитку є застосування глибоких нейронних мереж, здатних моделювати складні багатовимірні залежності між характеристиками контенту й поведінкою користувачів. Це відкриває можливість не лише прогнозувати ймовірність перегляду, а й створювати багаторівневий профіль користувача, що охоплює його емоційні та когнітивні вподобання.

Крім того, актуальним стає завдання подолання ефекту "інформаційної бульбашки", коли користувач постійно отримує рекомендації лише в межах уже знайомих йому жанрів і сюжетних ліній. Такий підхід знижує різноманітність контенту та обмежує культурний горизонт глядача. Для вирішення цієї проблеми пропонуються моделі, які поєднують персоналізовані рекомендації з елементами випадкового вибору, що дозволяє відкривати нові напрямки і поступово розширювати коло інтересів.

Отже, створення рекомендаційної підсистеми перегляду серіалів на основі методів машинного навчання є комплексним завданням, яке охоплює обробку великих даних, застосування гібридних алгоритмів, забезпечення прозорості рішень та захисту приватності. Така підсистема здатна не лише підвищити якість взаємодії користувача з платформою, а й сприяти більш раціональному використанню часу, формуючи індивідуалізоване середовище для споживання цифрового контенту.

Користувачі повинні бути обізнані про важливість політики паролів і нести відповідальність за її дотримання.

Список використаних джерел:

1. Метанов, А. В. Моделі машинного навчання для формування рекомендацій: магістерська робота. Київ: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2023. 85 с. doi: <https://doi.org/10.33216/1998-7927-2023-278-2-96-105>
2. Матвієнко, А. І. Формалізовані методи та алгоритми для створення рекомендаційних систем. Сучасні інформаційні технології та системи. 2023. № 4. С. 27–34. doi: <http://dx.doi.org/10.15421/432411>
3. Алгоритм Apriori. Вікіпедія. Дата звернення: 10.09.2025. URL: https://uk.wikipedia.org/wiki/Алгоритм_Apriori/

УДК 37.018.43:004.94

Салтиков Б. Г.,

здобувач вищої освіти

НРЗВО «Кам'янець-Подільський державний інститут»

Науковий керівник

Сидорук Л.М.,

доктор філософії в галузі педагогіки,

викладач кафедри цифрових, освітніх та соціо-економічних технологій

НРЗВО «Кам'янець-Подільський державний інститут»

VR/AR ТЕХНОЛОГІЇ: НОВА ЕРА ПРОФЕСІЙНОГО НАВЧАННЯ

Сучасна система професійної освіти перебуває у стані трансформації, що зумовлена як розвитком цифрових технологій, так і зростанням вимог до якості підготовки майбутніх фахівців. Традиційні методи навчання часто виявляються недостатньо ефективними для формування практичних умінь. У цьому контексті інноваційні технології віртуальної (VR) та доповненої (AR) реальності стають важливим інструментом, що відкриває нові можливості для організації освітнього процесу. Їх використання дозволяє наближати навчання до реальних умов професійної діяльності, забезпечуючи високу інтерактивність і безпечність засвоєння знань. VR/AR також дозволяють адаптувати навчальні програми під індивідуальні потреби здобувачів освіти, що значно покращує ефективність освітнього процесу. Наприклад, за допомогою VR можна створювати персоналізовані сценарії для кожного студента залежно від рівня його підготовки [3, с. 134].

За даними численних досліджень, технології VR/AR створюють сприятливі умови для активного залучення здобувачів освіти у процес навчання, завдяки тому, що одночасно залучають різні органи чуття. Ці технології дозволяють моделювати складні й абстрактні явища у формі доступної візуалізації. Наприклад, вивчення анатомії за допомогою 3D-моделей чи засвоєння фізичних законів через віртуальні симуляції забезпечує глибше

розуміння матеріалу порівняно з традиційними підходами [4, с. 550-551]. Порівняння можливостей VR та AR у навчанні наведено в таблиці 1.

Таблиця 1

Порівняння можливостей VR та AR у навчанні

Характеристика	VR	AR
Рівень занурення	Повне занурення у штучно створене середовище	Поєднання реального середовища з цифровими елементами
Основна мета	Імітація професійної діяльності	Візуалізація та доповнення реальних об'єктів навчання
Приклади застосування	Віртуальні лабораторії, симулятори, тренажери	Інтерактивні підручники, 3D-моделі, інструкції

Використання VR/AR у професійній освіті має комплексний позитивний вплив. По-перше, дослідження в галузі когнітивної психології свідчать про те, що занурення у віртуальне середовище активізує різні канали сприйняття інформації, що сприяє формуванню міцніших нейронних зв'язків та кращому запам'ятовуванню матеріалу. Ефект присутності, який створюють VR-технології, стимулює емоційну залученість студента, що є ключовим фактором ефективного навчання [1, с. 74-76].

По-друге, VR/AR-технології створюють умови для безпечного відпрацювання складних або небезпечних дій. Це особливо актуально для спеціальностей, де помилка може мати серйозні наслідки: авіація, хімічне виробництво, медицина. Такі симуляції дозволяють студентам робити помилки і виправляти їх без ризику, що підвищує якість підготовки.

По-третє, інтеграція VR/AR у освітній процес сприяє економії ресурсів. Віртуальні лабораторії або тренажери дають змогу зменшити витрати на обладнання та матеріали, які у реальних умовах швидко зношуються або потребують значних фінансових витрат. Це робить освіту більш доступною, особливо для закладів, що не мають можливості забезпечити здобувачів освіти повним комплектом матеріально-технічних ресурсів.

Попри значний потенціал, у процесі впровадження VR/AR у професійну освіту виникають певні труднощі, зокрема висока вартість обладнання та програмного забезпечення. Якісні VR-шоломи, контролери руху та спеціалізовані симуляційні програми залишаються дорогими для більшості закладів освіти. Також не менш актуальною проблемою є потреба у спеціальній підготовці викладачів, щоб вони вміли ефективно використовувати і інтегровувати VR/AR у освітній процес. Додатково існує ризик розумового перевантаження студентів. Надмірне використання VR/AR може ускладнювати сприйняття навчального матеріалу через перенасиченість інформацією та велику кількість візуальних і аудіоефектів.

Більшість досліджень демонструють позитивний ефект VR/AR на освітній процес завдяки підвищенню рівня залученості студентів, створенню інтерактивних середовищ та моделюванню реальних робочих ситуацій [2, с. 3-5].

Медична освіта є однією з найбільш показових сфер застосування VR/AR. Майбутні медики мають змогу відпрацьовувати хірургічні втручання у віртуальному середовищі, вивчати анатомію за допомогою AR-додатків, що відтворюють тривимірні моделі людського тіла.

У будівельній галузі VR використовується для створення моделей будівельних майданчиків, де майбутні інженери та робітники тренуються у плануванні та виконанні робіт з урахуванням техніки безпеки.

В авіаційній сфері застосовуються віртуальні тренажери польотів, що дозволяють імітувати роботу у складних погодних умовах чи аварійних ситуаціях. Це значно знижує витрати на підготовку пілотів і водночас забезпечує високу якість навчання.

У машинобудуванні AR-додатки використовуються для візуалізації складних агрегатів. Студенти можуть взаємодіяти з тривимірними моделями двигунів або механізмів, що сприяє кращому розумінню принципів їх роботи.

Отже, використання VR/AR технологій у професійній освіті відкриває широкі можливості для модернізації освітнього процесу. Вони дозволяють поєднувати теоретичні знання з практичними навичками, роблять навчання більш наближеним до умов реальної професійної діяльності. VR/AR сприяють формуванню професійної компетентності, підвищують мотивацію студентів та забезпечують безпечне відпрацювання складних виробничих ситуацій.

У перспективі VR/AR можуть стати невід'ємною складовою професійної освіти, особливо у галузях, де важливим є відпрацювання практичних дій у максимально наближених до реальності умовах.

Список використаних джерел:

1. Гуменний О. Технології віртуальної реальності та штучного інтелекту в освіті. інноваційна професійна освіта. 2022. Т. 1, № 2. С. 73–77. URL: <https://www.conference.ivet.edu.ua/index.php/1/article/view/9> (дата звернення: 16.09.2025).
2. Akçayır M., Akçayır G. Advantages and challenges associated with augmented reality for education: A systematic review of the literature. Educational Research Review. 2017. Т. 20. С. 1-11. URL: <https://doi.org/10.1016/j.edurev.2016.11.002> (дата звернення: 10.08.2025).
3. Jorge Bacca, Silvia Baldiris, Ramon Fabregat, Sabine Graf, and Kinshuk. "Augmented Reality Trends in Education: A Systematic Review of Research and Applications." Journal of Educational Technology & Society 17, no. 4 (2014): 133-149. URL: <http://www.jstor.org/stable/jeductechsoci.17.4.133> (дата звернення: 16.09.2025).
4. The effectiveness of virtual and augmented reality in health sciences and medical anatomy / C. Moro та ін. Anatomical Sciences Education. 2017. Т. 10, № 6. С. 549–559. URL: <https://doi.org/10.1002/ase.1696> (дата звернення: 20.09.2025).

Семикрас Д.О.
здобувач вищої освіти,
*Харківський національний університет міського господарства
імені О.М. Бекетова*
Науковий керівник
Сізова Н.Д.
докт.фіз.-мат.наук., професор, професор кафедри комп'ютерних наук та
інформаційних технологій
*Харківський національний університет міського господарства
імені О.М. Бекетова*

АНАЛІЗ ДАНИХ ТА МОДЕЛЮВАННЯ ІНСТРУМЕНТІВ ЗБОРУ ІНФОРМАЦІЇ У СИСТЕМАХ ГУМАНІТАРНОГО РЕАГУВАННЯ

Сучасний світ характеризується стрімким зростанням гуманітарних криз, викликаних війнами, техногенними аваріями, природними катастрофами, економічними потрясіннями та глобальними явищами, такими як пандемії чи кліматичні зміни. Наслідками цих процесів є масштабні людські втрати, руйнування інфраструктури та порушення доступу до базових послуг (житло, охорона здоров'я, освіта, водопостачання). У такій ситуації гуманітарні організації відіграють ключову роль, адже саме вони забезпечують надання допомоги постраждалим громадам, координацію партнерських ініціатив та прозорість у використанні ресурсів.

Щоб ефективно здійснювати цю діяльність, організаціям необхідні сучасні інформаційні інструменти, здатні не лише фіксувати дані про бенефіціарів та обсяги допомоги, але й дозволяти проводити аналіз, формувати звіти та контролювати розподіл ресурсів. Одним із рішень, що активно використовується у міжнародній практиці, є ActivityInfo – веборієнтована система управління гуманітарною інформацією, яка поєднує мобільний збір даних, інтегровану аналітику та механізми контролю доступу [1].

Актуальним питанням є створення структурованої бази даних у системі ActivityInfo для організації обліку та моніторингу гуманітарної допомоги.

Для цього розглядаються такі завдання:

- аналіз підходів до збору й обробки даних у сфері гуманітарного реагування;

- проектування логічної структури бази даних, що охоплює ключові процеси (реєстрацію бенефіціарів, ведення каталогів допомоги, облік локацій, реєстрацію фактів видачі ресурсів);

- впровадження зв'язків між таблицями для підвищення цілісності даних;

- створення механізму унікальної ідентифікації бенефіціарів та запобігання дублюванню;

- формування підґрунтя для подальшого аналізу динаміки розподілу допомоги та підготовки звітності для донорів.

У межах роботи розроблено базу даних, що складається з чотирьох взаємопов'язаних таблиць:

“Локації” – довідникова форма з інформацією про адміністративно-територіальні одиниці, яка використовується як reference-таблиця, забезпечуючи географічну прив'язку даних.

“Каталог допомоги” – таблиця, що містить категорії (продовольча, медична, непродовольча), типи допомоги та детальний опис наборів, завдяки чому забезпечується уніфікація обліку.

“Реєстрація бенефіціарів” – форма, яка включає автоматичне кодування отримувачів, їхній статус, соціально-демографічні характеристики та зворотне посилення (reverse reference) на історію отримання допомоги;

“Видача допомоги” – форма, де фіксуються факти передачі ресурсів із зазначенням дати, місця, обсягу й типу набору.[2]

Запропонована структура дозволяє будувати гнучку систему звітності, відстежувати потреби у розрізі регіонів, контролювати відповідність наданої допомоги заявленим потребам та аналізувати динаміку підтримки.

Розроблена база даних може застосовуватись гуманітарними організаціями для:

- централізованого ведення обліку наданої допомоги;
- оперативного моніторингу діяльності;
- формування звітності для керівництва та донорів;
- оптимізації планування і координації гуманітарних програм.

Таким чином, система забезпечує підвищення прозорості, виключення дублювань у даних та ефективніший розподіл ресурсів.

Створена інформаційна модель на базі ActivityInfo демонструє високу ефективність у задачах моніторингу та управління гуманітарною допомогою. Її перевагами є простота реалізації, можливість масштабування та інтеграції з іншими інструментами. Подальший розвиток може передбачати розширення аналітичного функціоналу та впровадження візуалізації даних для більш глибокого аналізу. [3]

Список використаних джерел:

1. Activity Info. URL: <https://www.activityinfo.org/>
2. ActivityInfo Data Model. URL: <https://www.activityinfo.org/support/docs/database/understanding-activityinfo-s-data-model.html>
3. ActivityInfo for M&E – One platform for the complete data lifecycle. URL: <https://www.activityinfo.org/support/webinars/2024-08-22-demo-activityinfo-for-the-complete-data-lifecycle.html>

ПРОБЛЕМИ РОЗРОБКИ ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ ДЛЯ РЕЄСТРАЦІЇ ДАНИХ ВІДХОДІВ ВІД РУЙНУВАНЬ

Теперішній військовий конфлікт в Україні спричиняє широкомасштабні пошкодження інфраструктурних об'єктів та житлових будинків, внаслідок чого виникає велика кількість будівельних і змішаних відходів. Ці матеріали створюють екологічну загрозу, ускладнюють відновлення зруйнованих територій та вимагають швидкого обліку й контролю. Відсутність уніфікованої системи збору, зберігання та аналізу інформації про такі відходи перешкоджає ефективному плануванню та координації відновлювальних дій.

Дослідження у сфері ІТ-технічних рішень для екології переважно орієнтовані на управління промисловими та побутовими відходами. Створено ряд державних реєстрів і баз, які дозволяють моніторити окремі потоки відходів. Однак специфіка відходів, що утворюються внаслідок руйнувань, вивчена недостатньо. Наукові та практичні розробки не забезпечують інтеграцію різних джерел (акти обстеження, геопросторові дані, фотозвіти, адміністративна документація) і не пропонують комплексну модель автоматизованої звітності.

Розробникам підсистеми інформації ставиться завдання створити інтегроване рішення, яке дозволить:

- уніфіковано збирати дані про відходи, що виникають від руйнувань, незалежно від їхнього походження;
- зберігати інформацію в єдиній, чітко структурованій базі;
- автоматизувати формування звітності для різних рівнів управління – від місцевих громад до центральних органів;
- впровадити інструменти аналізу, прогнозування та візуалізації даних, зокрема за допомогою геоінформаційних технологій;
- забезпечити захист і контроль доступу, оскільки дані можуть містити службову або конфіденційну інформацію.

Функціональна структура звітності щодо відходів від руйнувань, що зображена на рисунку 1, може бути представлена послідовними модулями:

1. Модуль збору даних – передбачає введення інформації з актів обстеження, супутникових і аерофотозйомок, даних місцевих органів.
2. Модуль попередньої обробки – відповідає за перевірку достовірності, усунення дублюючих записів, уніфікацію форматів.
3. База даних підсистеми – містить ключові сутності («Об'єкт руйнування», «Тип відходів», «Місце виникнення», «Обсяг», «Стан переробки»), пов'язані між собою ER-моделлю.
4. Модуль формування звітності – забезпечує підготовку аналітичних зведень, періодичної звітності та інтерактивних карт.

5. Модуль захисту даних – реалізує автентифікацію користувачів, розмежування прав доступу та резервне копіювання.

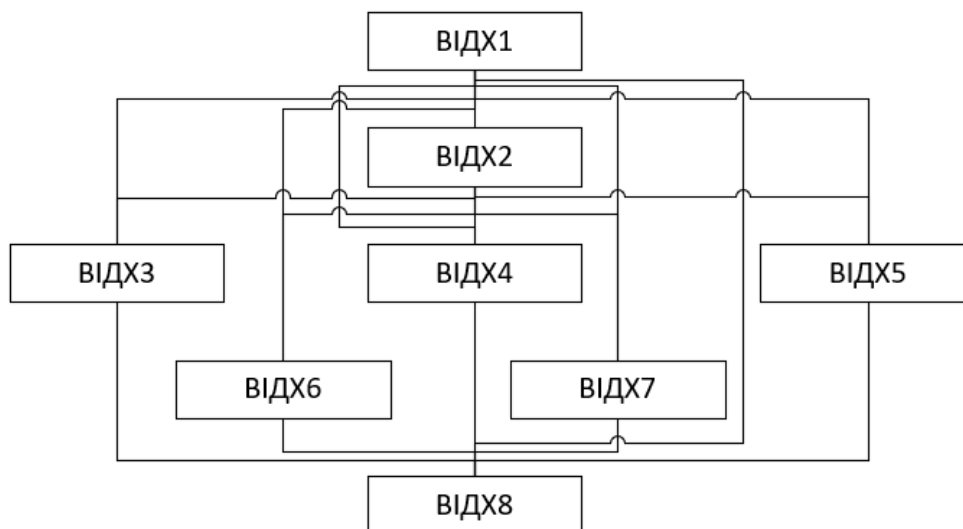


Рисунок 1 – Функціональна структура звітності відходів від руйнувань

Завдання системи охоплюють:

- створення єдиного формату внесення даних про відходи;
- забезпечення прозорості та відстежуваності руху відходів від моменту їх утворення до фінальної утилізації або переробки;
- оптимізацію процесів планування логістики та утилізації;
- інтеграцію з національними екологічними реєстрами і GIS-системами;
- формування актуальної аналітичної інформації для прийняття управлінських рішень.

Розробка інформаційної підсистеми для реєстрації даних про відходи, що виникають внаслідок руйнувань, – це складне, проте вкрай необхідне завдання. Воно вимагає об'єднання методик проектування баз даних, інструментів геоінформаційного аналізу та сучасних засобів кіберзахисту. Запровадження такої системи дозволить підвищити ефективність екологічної політики, оптимізувати відновлювальні процеси і сприятиме безпечному використанню ресурсів у поствоєнний період.

Список використаних джерел:

1. Закон України «Про управління відходами» від 20.06.2022 № 2320-IX. URL: <https://zakon.rada.gov.ua/laws/show/2320-20#Text>
2. Розпорядження Кабінету Міністрів України «Про схвалення Національної стратегії управління відходами в Україні до 2030 року» від 08.11.2017 № 820-р. URL: <https://zakon.rada.gov.ua/laws/show/820-2017-%D1%80#Text>
3. Департамент захисту довкілля та природних ресурсів Сумської обласної державної адміністрації. Звітні та аналітичні матеріали практики (2025). URL: <https://eco.sm.gov.ua/>

Смірнов О.С.
здобувач вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Тимошенко Юлія,
Dr.sc.ing., Baltic International Academy, doc.

ДОСЛІДЖЕННЯ МЕТОДІВ І АЛГОРИТМІВ ОПТИМАЛЬНОГО КОДУВАННЯ ТА СТИСНЕННЯ ДАНИХ У КОМП'ЮТЕРНИХ СИСТЕМАХ

У сучасному цифровому світі величезні обсяги даних постійно генеруються, передаються та зберігаються в комп'ютерних системах. Інформаційні технології все більше інтегруються у всі сфери діяльності людини: від побуту та освіти до промисловості й наукових досліджень. Це зумовлює необхідність ефективного використання ресурсів – пам'яті, пропускну здатності каналів зв'язку та обчислювальних потужностей. Одним із ключових інструментів для досягнення цієї мети є методи та алгоритми кодування й стиснення даних. Вони дозволяють зменшити обсяг інформації без втрати або з частковою втратою її змісту, що напряму впливає на продуктивність та економічність комп'ютерних систем [1].

Стиснення даних можна поділити на два основні підходи: без втрат (lossless) та з втратами (lossy). Методи без втрат забезпечують повне відновлення вихідної інформації після декодування. Вони критично важливі для текстових документів, програмного коду, фінансових та медичних даних, де навіть мінімальна втрата інформації неприпустима. До таких алгоритмів належать кодування Гаффмана, арифметичне кодування, алгоритми Lempel–Ziv (LZ77, LZ78, LZW), які використовуються у форматах ZIP, PNG, GIF. Методи з втратами допускають видалення частини даних, які мають незначний вплив на сприйняття користувачем. Вони застосовуються переважно у мультимедіа – аудіо, відео, зображеннях, де людина не здатна помітити незначні спотворення. Прикладами є JPEG, MP3, MPEG, H.264, де активно використовуються перетворення Фур'є та дискретне косинусне перетворення (DCT) [1, 2].

Одним із найпоширеніших алгоритмів оптимального кодування є кодування Гаффмана. Його суть полягає у використанні змінної довжини кодових слів залежно від частоти появи символів. Символи, які зустрічаються частіше, отримують коротші коди, а рідкісні – довші. Це забезпечує мінімальну середню довжину кодового слова та ефективне використання бітів. Хоча алгоритм Гаффмана простий у реалізації, він залишається одним із базових методів оптимального кодування й широко застосовується в архівації файлів.

Арифметичне кодування є більш складним і математично витонченим підходом. Воно представляє весь потік символів як підінтервал $[0,1)$, де кожен символ звужує діапазон залежно від своєї ймовірності. У результаті вихідний текст кодується у вигляді одного дробового числа. Цей метод здатен досягати

коефіцієнтів стиснення, близьких до теоретичної межі, визначеної ентропією Шеннона. Проте його реалізація вимагає значних обчислювальних ресурсів і складних арифметичних операцій з високою точністю [2].

Алгоритми Lempel–Ziv використовують інший принцип – пошук і заміну повторюваних підрядків у даних. Вони створюють словник (таблицю фраз), де зберігаються вже зустрінуті послідовності символів. Кожен новий повтор замінюється посиланням на словниковий запис, що суттєво скорочує обсяг. Алгоритми сімейства LZ стали основою багатьох форматів архівації, таких як ZIP, RAR, а також протоколів стиснення даних у мережах. Їхня перевага полягає у відносній простоті та високій швидкості роботи [2, 3].

Особливе місце у стисненні даних займають методи, що базуються на трансформації сигналів. Дискретне косинусне перетворення використовується у JPEG для стиснення зображень. Воно дозволяє перейти від просторового подання до частотного, де значна частина коефіцієнтів є близькою до нуля і може бути відкинута. Аналогічно у відеокодеках застосовується дискретне вейвлет-перетворення (DWT), яке забезпечує ще кращу ефективність, зберігаючи високу якість при низькому бітрейті [3].

Варто відзначити і методи ентропійного кодування, які розглядаються як оптимальні з точки зору теорії інформації. Ентропія характеризує середню кількість інформації на символ. Алгоритми стиснення прагнуть наблизитися до цієї межі, використовуючи статистичні властивості даних. Тому попередній аналіз інформації (наприклад, побудова статистики частот або моделей імовірностей) є важливим етапом будь-якого сучасного кодека.

У комп'ютерних системах, де важливими є швидкодія та масштабованість, часто використовується комбінація методів. Наприклад, у форматі JPEG поєднано дискретне косинусне перетворення, квантування та кодування Гаффмана. У сучасних відеокодеках, таких як H.265/HEVC, застосовується складний набір алгоритмів: блочне прогнозування, трансформації, адаптивне квантування, ентропійне кодування CABAC. Це дозволяє суттєво скоротити обсяг даних без значної втрати якості.

Окремої уваги заслуговує стиснення у режимі реального часу, що є актуальним для потокового відео та хмарних сервісів. Тут алгоритми повинні не лише забезпечувати високий коефіцієнт стиснення, а й працювати з мінімальними затримками. Тому сучасні системи активно застосовують апаратне прискорення за допомогою графічних процесорів та спеціалізованих мікросхем.

Стиснення даних також має велике значення для зберігання у великих сховищах (Big Data). Використання оптимальних алгоритмів дозволяє зменшити витрати на інфраструктуру, підвищити швидкість доступу до даних і знизити енергоспоживання. У поєднанні з технологіями розподіленої обробки (наприклад, Hadoop, Spark) це відкриває нові можливості для роботи з петабайтами інформації.

Однак варто враховувати і обмеження. Стиснення завжди пов'язане з додатковими обчисленнями, що може збільшити час обробки та навантаження на процесор. У випадку алгоритмів з втратами існує ризик погіршення якості,

особливо при багаторазовому перекодуванні. Тому вибір методу завжди має бути компромісом між швидкістю, якістю та коефіцієнтом стиснення залежно від конкретних завдань.

Підсумовуючи, можна зазначити, що дослідження методів і алгоритмів оптимального кодування та стиснення даних є однією з найважливіших галузей інформатики. Від ефективності цих алгоритмів залежить продуктивність комп'ютерних систем, вартість зберігання та передавання інформації, а також комфорт кінцевих користувачів. Подальший розвиток у цій сфері пов'язаний із застосуванням інтелектуальних підходів – машинного навчання та нейронних мереж, які дозволяють адаптивно вибирати параметри стиснення залежно від контенту. Це відкриває перспективи створення нових поколінь кодеків, що наблизяться до теоретичної межі Шеннона та забезпечуватимуть ще більш ефективне використання ресурсів у комп'ютерних системах майбутнього.

Список використаних джерел:

1. Майданюк В. П., Романюк О. Н., Тужанський С. Є. Основи теорії інформації та кодування : навч. посібник / Вінницький нац. техн. ун-т. – 2023.
2. Святослав Мичка, Наталія Голян. Методи стиснення бінарних даних без втрат для підвищення продуктивності програмних систем // Information Technology: Computer Science, Software Engineering and Cyber Security. – 2025. DOI: <https://doi.org/10.32782/IT/2025-1-22>
3. Мартинюк Т. Б., Войналович О. Ю. Класифікаційна модель методів цифрового кодування // Оптико-електронні інформаційно-енергетичні технології. – 2024. – № 1-47. – С. 42-49. DOI: <https://doi.org/10.31649/1681-7893-2024-47-1-42-49>

УДК 004.422

Стяглик Н.І.,
*завідувач кафедри інформаційних технологій та
математичного моделювання
Харківський національний університет імені В.Н.Каразіна,
Žilinskis Vjačeslavs,
Dr.sc.ing., inv. doc.
Baltic International Academy*

АЛГОРИТМІЧНІ АСПЕКТИ ВИКОРИСТАННЯ ДЕРЕВ ТА ГРАФІВ У ЗАДАЧАХ БІЗНЕС-АНАЛІТИКИ

Сучасний бізнес функціонує в умовах надзвичайно великих обсягів даних (Big Data), які потребують швидкого аналізу та обробки. Традиційні методи вже не завжди забезпечують ефективність у пошуку зв'язків та закономірностей. Використання дерев та графів як математичних моделей дозволяє представити

інформацію у зручному вигляді та застосовувати ефективні алгоритми для аналізу даних.

Основна складність полягає у масштабуванні: алгоритми, які працюють для невеликих наборів даних, часто втрачають ефективність у випадку мільйонів вершин чи ребер. Це створює виклики для бізнес-аналітики, де швидкість прийняття рішення критично важлива.

Мета дослідження: дослідити алгоритмічні аспекти використання дерев та графів у бізнес-аналітиці, визначити ефективність різних підходів і проаналізувати можливості їх застосування у реальних бізнес-задачах. З цим пов'язані завдання аналізу основних алгоритмів роботи з деревами та графами, оцінки їх придатності до різних бізнес-сценаріїв, визначення перспективних напрямів розвитку.

Розглянемо теоретичні основи дерев та графів. Дерево – це зв'язаний ациклічний граф, який часто використовується для представлення ієрархічних структур. Граф – узагальнена структура, що складається з множини вершин та ребер, які описують зв'язки між об'єктами.

Наведемо основні властивості. До ключових характеристик належать: ступінь вершини, довжина шляху, цикли, діаметри графів, глибина дерев. Ці параметри впливають на складність алгоритмів.

Якщо говорити про класифікацію алгоритмів, то можна виділити алгоритми пошуку (DFS, BFS), алгоритми оптимізації (мінімальні шляхи, остовні дерева), алгоритми кластеризації (виділення спільнот у графах) та алгоритми візуалізації (графові розкладки для відображення структур).

Схарактеризуємо роль обраних структур даних у бізнес-аналітиці. Дерева дозволяють будувати системи прийняття рішень, а графи допомагають у виявленні залежностей у соціальних мережах, логістичних системах чи фінансових потоках.

Алгоритмічні аспекти використання дерев

1. Алгоритми обходу дерев.

DFS (глибинний пошук) і BFS (пошук у ширину) дозволяють аналізувати структуру дерева та здійснювати пошук необхідних елементів. Preorder, inorder та postorder обходи є основою для роботи з бінарними деревами.

2. Алгоритми балансування.

AVL-дерева, червоно-чорні дерева та B-дерева використовуються для підтримки рівноваги структури, що дозволяє зберігати швидкий доступ до даних. Це критично для баз даних і пошукових систем.

3. Дерева рішень.

Decision Trees застосовуються у машинному навчанні та бізнес-аналітиці для класифікації даних і прогнозування. Вони дозволяють будувати зрозумілі для людини моделі прийняття рішень.

Отже, приклади використання дерев є: сегментація клієнтів за характеристиками; прогнозування фінансових показників; оптимізація баз даних (індексація); побудова сценаріїв розвитку ризиків.

Алгоритмічні аспекти аналізу графів

1. Алгоритми пошуку шляхів:

- алгоритм Дейкстри знаходить найкоротший шлях у графах із невід’ємними вагами;
- алгоритм Беллмана-Форда працює з графами, де можливі від’ємні ваги;
- алгоритм Флойда-Воршелла дозволяє обчислювати найкоротші шляхи між усіма парами вершин.

2. Мінімальні остовні дерева. Алгоритми Пріма та Крускала будують мінімальні мережі зв’язків. Це корисно у задачах оптимізації витрат у логістиці чи мережах постачання.

3. Алгоритми кластеризації. Метод Girvan–Newman виділяє спільноти у соціальних графах, а метод Louvain забезпечує ефективність на великих наборах даних.

4. Методи виявлення центральних вершин. PageRank та показники центральності допомагають визначити ключові вузли у графах, наприклад впливових клієнтів у мережі чи вузли, важливі для логістики.

Прикладами використання служать: аналіз соціальних мереж для маркетингу; оптимізація транспортних маршрутів; виявлення шахрайських транзакцій; моделювання бізнес-процесів.

Проте вибір алгоритму має здійснюватись з урахуванням порівняльного аналізу ефективності алгоритмів. В якості критеріїв оцінки можуть бути обрані часова складність, просторові витрати пам’яті, можливість масштабування.

Якщо казати про порівняння класичних та сучасних підходів, то класичні алгоритми ефективні на малих даних, однак сучасні підходи (розподілені обчислення, GPU-прискорення) дозволяють працювати з Big Data.

Для задач реального часу потрібні швидкі евристики, тоді як для стратегічного планування можна застосовувати більш складні, але точні алгоритми. Це свідчить про залежність від бізнес-контексту. Візуалізація продуктивності дозволяє показати, які алгоритми краще підходять для конкретних сценаріїв.

Та не можна оминати увагою виклики та перспективи використання. По-перше, проблема обробки графових структур пов’язана із масштабуванням, постає проблема обробки графів із мільйонами вершин. В даному випадку потрібні спеціалізовані алгоритми з високою обчислювальною ефективністю. По-друге, виникає потреба паралельних та розподілених алгоритмів, в чому можуть допомогти сучасні інструменти та спеціалізовані платформи для обробки графів у великих системах (Hadoop, Spark, GraphX).

Перспективним стає й поєднання зі штучним інтелектом. Графові нейронні мережі (GNN) дозволяють автоматично знаходити закономірності у складних структурах даних. Комбінування decision trees з ансамблевими методами (Random Forest, Gradient Boosting) дає ще кращі прогнози.

Основними тенденціями наразі є розвиток алгоритмів у напрямі потокових даних, реального часу та інтерактивної візуалізації.

Отже, дерева і графи – універсальні структури, які мають ключове значення для бізнес-аналітики. Практичне значення цих структур полягає в тому, що алгоритми на основі дерев і графів допомагають підвищити

ефективність аналізу клієнтів, оптимізації процесів, управління ризиками. А от поєднання класичних алгоритмів із сучасними методами машинного навчання та Big Data відкриває нові можливості для бізнесу.

Список використаних джерел.

1. Бізнес-аналітика та моделювання : навчальний посібник / В. В. Лаговський, В. М. Краєвський. – Ірпінь : Університет ДФС України, 2020. – 442 с. – (Серія «На допомогу студенту УДФСУ»; т. 58)
2. Ситник В. Ф. Дерева рішень у системах дейтамайнінгу / В. Ф. Ситник, Н. В. Ситник // Формування ринкової економіки : зб. наук. пр. / Київ. нац. екон. ун-т ім. В. Гетьмана ; редкол.: О. О. Беляєв (відп. ред.) [та ін.]. – Київ : КНЕУ, 2006. – Вип.16. – С. 442–454.
3. Vercellis C. Business Intelligence: Data Mining and Optimization for Decision Making / C. Vercellis. – Wiley Publishing, Inc., 2009
4. What Are the Different Types of Graph Algorithms & When to Use Them? URL: <https://neo4j.com/blog/graph-data-science/graph-algorithms/>

УДК 004.093

Суровикін Ю.В.

здобувач вищої освіти,

Харківський національний університет радіоелектроніки

Науковий керівник

Маишталір С.В.

д.т.н., професор, професор кафедри інформатики,

Харківський національний університет радіоелектроніки

МЕТОД ПРОГНОЗУВАННЯ ПОПУЛЯРНОСТІ АРТИСТІВ НА ОСНОВІ КОМБІНОВАНИХ СТАТИСТИЧНИХ МЕТРИК ТА ФАКТОРІВ КОЛАБОРАЦІЙ

Сучасна музична індустрія характеризується високою конкуренцією, де увага слухачів стає найціннішим ресурсом. Популярність артиста змінюється динамічно під впливом як внутрішніх факторів так і зовнішніх. Серед таких факторів: активність, стиль, частота релізів, співпраця з іншими виконавцями, просування на різних платформах. Для музикантів, продюсерів і стрімінгових сервісів важливо мати інструменти, які дозволяють не лише аналізувати поточний стан, але й прогнозувати зміни у майбутньому [1].

Задача прогнозування популярності артистів є складною через багатофакторний характер. Прослуховування залежать від якості релізів, відповідності ринку, впливу соціальних мереж та від колаборацій [2], що здатні швидко розширювати аудиторію. Тому виникає необхідність у методі, який би поєднував часові статистичні характеристики з аналітикою колективної творчості.

У цьому дослідженні запропоновано метод прогнозування, що базується на трьох ключових складових: виявленні кореляції між колабораціями та зростанням аудиторії, врахуванні ваги партнерів у спільних проектах і оцінці стабільності популярності через варіаційний аналіз. Такий підхід дозволяє створити більш комплексну картину розвитку артиста, ніж класичні методи, які зазвичай враховують лише часові тренди.

Першим етапом є визначення залежності між кількістю колаборацій та приростом прослуховувань. Для цього використовується коефіцієнт кореляції [3]:

$$r = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}},$$

де:

x_i – кількість колаборацій у періоді;

y_i – приріст прослуховувань;

$\bar{y}, \bar{x}$ – середні значення відповідних змінних.

Дане співвідношення дає можливість виявити силу та напрямок взаємозв'язку: чим ближче r до 1, тим більший позитивний ефект мають колаборації.

Оскільки не всі спільні проєкти однаково впливають на популярність, наступним кроком є введення зваженого середнього. Воно дозволяє враховувати різницю у значущості артистів, з якими відбувалася співпраця [3]:

$$P = \frac{\sum_{i=1}^k \omega_i y_i}{\sum_{i=1}^k \omega_i},$$

де:

y_i – кількість прослуховувань після i -ї колаборації;

ω_i – ваговий коефіцієнт, що відповідає популярності запрошеного артиста.

Таким чином, співпраця з відомим артистом отримує більший вплив на прогноз, ніж колаборація з менш відомим.

Щоб оцінити стабільність слухацької бази виконавця, застосовується коефіцієнт варіації:

$$V = \frac{\sigma}{\mu},$$

де:

σ – стандартне відхилення кількості прослуховувань;

μ – середнє значення кількості прослуховувань.

Низьке значення коефіцієнта варіації вказує на постійну та віддану аудиторію, тоді як високі значення демонструють коливання, які можуть бути наслідком різких змін у стилі чи нестабільної активності.

Поєднання вищенаведених метрик дозволяє отримати комплексний показник, що враховує одночасно тенденції зростання популярності, силу впливу колаборацій та стабільність слухацької бази. Це створює підґрунтя для більш точного прогнозування змін у кількості прослуховувань і може застосовуватись як музичними платформами, так і продюсерами для планування маркетингових стратегій.

Список використаних джерел:

1. Kang, I., Mandulak, M., & Szymanski, B. K. (2022). Analyzing and predicting success of professional musicians. *Scientific Reports*, 12(1), 21838.
2. Deshmane, A., & Martínez-de-Albéniz, V. (2023). Come together, right now? An empirical study of collaborations in the music industry. *Management Science*, 69(12), 7217-7235.
3. Lee, J., & Lee, J. S. (2018). Music popularity: Metrics, characteristics, and audio-based prediction. *IEEE Transactions on Multimedia*, 20(11), 3173-3182.

УДК 658.5:004.89:658.8

Тарасюк М.В.

*д.е.н., професор, професор кафедри менеджменту, маркетингу та підприємництва
Національний університет «Києво-Могилянська академія»*

PROCESS MINING ЯК ІНСТРУМЕНТ ОПТИМІЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ У МАРКЕТИНГОВІЙ ДІЯЛЬНОСТІ

Сучасний розвиток цифрових технологій суттєво змінює підходи до управління маркетинговою діяльністю. Зростання обсягів даних, багатоканальна взаємодія з клієнтами та висока динамічність ринкового середовища роблять традиційні методи планування та контролю менш ефективними. У таких умовах виникає нагальна потреба у впровадженні інноваційних інструментів, здатних забезпечити глибоку аналітику бізнес-процесів, своєчасне виявлення неефективностей та швидку адаптацію до змін.

Проблема полягає у складності моніторингу та оптимізації маркетингових бізнес-процесів у реальному часі. Різноманітні джерела даних — CRM-системи, рекламні платформи, соціальні мережі, веб-аналітика — призводять до інформаційної фрагментації, що ускладнює формування цілісної картини клієнтського шляху. Традиційні методи аналітики здебільшого є ретроспективними та не дозволяють своєчасно реагувати на відхилення або

виявляти приховані закономірності, що створює ризики втрати конкурентних переваг і зниження ефективності маркетингових кампаній.

Традиційні підходи до реінжинірингу бізнес-процесів, зокрема експертні оцінки, методи нечіткої логіки та структурного аналізу, дозволяють формувати покращені моделі процесів та визначати напрями оптимізації [1]. Водночас вони мають суттєві обмеження: зосередженість на статичному представленні процесів ускладнює аналіз їх перебігу в динаміці, відсутність моніторингу у реальному часі не дає змоги виявляти «вузькі місця» та аналізувати причини їх виникнення, а також ускладнює моделювання альтернативних сценаріїв поведінки процесів для адаптації до змін середовища.

У цьому контексті особливого значення набуває технологія Process Mining, яка доповнює класичні методи новими можливостями. Вона дозволяє об'єктивно аналізувати фактичний перебіг бізнес-процесів на основі цифрових слідів у журналах подій інформаційних систем, створюючи реалістичну модель процесів. Process Mining забезпечує виявлення проблемних ділянок, аналіз причин виникнення «вузьких місць», а також моделювання сценаріїв поведінки процесів. Таким чином, її застосування стає ключовим для підвищення прозорості, гнучкості та ефективності управління маркетинговою діяльністю, забезпечуючи компаніям можливість оперативно адаптуватися до змін ринку та підвищувати клієнтоорієнтованість.

Особливого значення у цьому контексті набуває технологія Process Mining, яка доповнює класичні методи новими можливостями. Вона дозволяє об'єктивно аналізувати фактичний перебіг бізнес-процесів на основі цифрових слідів у журналах подій інформаційних систем, створюючи реалістичну модель процесів. Process Mining забезпечує виявлення проблемних ділянок, аналіз причин виникнення «вузьких місць», а також моделювання сценаріїв поведінки процесів. Таким чином, її застосування стає ключовим для підвищення прозорості, гнучкості та ефективності управління маркетинговою діяльністю, забезпечуючи компаніям можливість оперативно адаптуватися до змін ринку та підвищувати клієнтоорієнтованість.

Наукові дослідження показують, що ефективне управління у сучасних умовах можливе лише за умови цифровізації. Цифрові технології виступають як інноваційний інструмент подолання кризових явищ, підвищення стійкості та конкурентоспроможності підприємств. Важливими технологічними рішеннями є Big Data, штучний інтелект, машинне навчання, IoT та хмарні сервіси, які дозволяють забезпечити проактивність, гнучкість, автоматизацію та оперативність прийняття управлінських рішень [2]. Цифрові інструменти дають змогу не лише моніторити та оптимізувати бізнес-процеси в режимі реального часу, але й прогнозувати потенційні ризики, оцінювати сценарії розвитку процесів та адаптувати організаційні стратегії під нові виклики ринку. У цьому контексті цифровізація та використання технологій Process Mining стають стратегічно важливими для забезпечення ефективності управлінських процесів, антикризової стійкості та довгострокового розвитку компаній.

Доцільним є метод синтезу Process Mining та Enterprise Dynamics, який дозволяє створювати альтернативні варіанти покращених моделей

бізнес-процесів. Такий підхід поєднує аналіз фактичного перебігу процесів на основі цифрових слідів у журналах подій із можливостями імітаційного моделювання, що забезпечує комплексне дослідження бізнес-процесів у динаміці. Застосування цього методу дає змогу здійснювати детальне моделювання, візуалізацію та моніторинг процесів у різних предметних областях, враховуючи взаємозв'язки, потоки ресурсів та потенційні «вузькі місця».

Для маркетингової діяльності запропонований підхід має особливу цінність. Він дозволяє екстраполювати методологію Process Mining на тестування сценаріїв клієнтської взаємодії та оцінку ефективності маркетингових стратегій. Завдяки цьому маркетологи отримують можливість моделювати альтернативні шляхи поведінки клієнтів, оцінювати наслідки різних тактичних рішень та прогнозувати результати кампаній до їх фактичного запуску. Візуалізація та аналітика на основі цифрових даних сприяють виявленню критичних точок у клієнтському шляху, підвищенню ефективності маркетингових процесів та оптимізації ресурсів компанії. Таким чином, синтез Process Mining і Enterprise Dynamics створює нові можливості для підвищення прозорості, адаптивності та стратегічної гнучкості маркетингової діяльності у сучасному цифровому середовищі.

Проведений аналіз показав, що сучасний розвиток цифрових технологій суттєво змінює підходи до управління маркетинговою діяльністю та вимагає застосування інноваційних інструментів для ефективного моніторингу та оптимізації бізнес-процесів. Традиційні методи реінжинірингу бізнес-процесів, включно з експертними оцінками, методами нечіткої логіки та структурного аналізу, дозволяють формувати покращені моделі та визначати напрями оптимізації, проте вони мають суттєві обмеження: орієнтація на статичне подання процесів ускладнює аналіз динаміки, відсутність моніторингу у реальному часі обмежує можливість виявлення «вузьких місць» та причин їх виникнення, а також ускладнює прогнозування альтернативних сценаріїв.

У цьому контексті технологія Process Mining виступає ключовим інструментом, який доповнює класичні підходи новими можливостями. Вона забезпечує об'єктивний аналіз фактичного перебігу бізнес-процесів на основі цифрових слідів у журналах подій інформаційних систем, що дозволяє виявляти проблемні ділянки, аналізувати причини зниження ефективності та моделювати сценарії поведінки процесів. Застосування Process Mining сприяє підвищенню прозорості, гнучкості та оперативності управлінських рішень, що є критично важливим для адаптації маркетингової діяльності до динамічного ринкового середовища.

Дослідження підтверджує, що ефективне управління у сучасних умовах можливе лише за умови цифровізації. Використання технологій Big Data, штучного інтелекту, машинного навчання, IoT та хмарних сервісів дозволяє забезпечити проактивність, автоматизацію та оперативність прийняття рішень, прогнозувати ризики та оцінювати сценарії розвитку процесів.

Доцільним є застосування методу синтезу Process Mining та Enterprise Dynamics, який поєднує аналіз фактичного перебігу процесів на основі

цифрових слідів із можливостями імітаційного моделювання. Це забезпечує комплексне дослідження бізнес-процесів у динаміці, включно з візуалізацією потоків ресурсів, виявленням «вузьких місць» та оцінкою ефективності альтернативних сценаріїв.

Для маркетингової діяльності запропонований підхід дозволяє моделювати клієнтські шляхи, тестувати сценарії взаємодії та оцінювати наслідки різних стратегічних і тактичних рішень до їх фактичного впровадження. Це сприяє підвищенню ефективності маркетингових кампаній, оптимізації ресурсів компанії та забезпечує стратегічну гнучкість і адаптивність.

На основі проведеного дослідження пропонується впроваджувати синтез Process Mining та імітаційного моделювання як стандартний інструмент оптимізації маркетингових бізнес-процесів у компаніях, орієнтованих на цифрову трансформацію та підвищення клієнтоорієнтованості, а також здійснювати регулярний моніторинг та аналіз даних для оперативного виявлення та усунення «вузьких місць» у процесах.

Список використаних джерел:

1. Левикін І. В. Метод синтезу технології Process Mining і засобів імітаційного моделювання / І. В. Левикін // Технологія і техніка друкарства. – 2016. – № 3(53). DOI: 10.20535/2077-7264.3(53).2016.73113.
2. П'янкова О., Рула О. Вплив цифрових трансформацій на ефективність антикризового управління в міжнародних компаніях / О. П'янкова, О. Рула // Економіка та суспільство. – 2025. – № 72. DOI: 10.32782/2524-0072/2025-72-155.

УДК 004.8

Терещенко А.С.

*здобувач першого (бакалаврського) рівня
факультету фінансів та цифрових технологій*

Ніжегородцев В.О.

*к.пед.н., доцент, доцент кафедри комп'ютерних
та інформаційних технологій і систем
Державний податковий університет*

ЕТИЧНІ АСПЕКТИ ТА РИЗИКИ ШТУЧНОГО ІНТЕЛЕКТУ: ВИКЛИКИ СУЧАСНОГО ЦИФРОВОГО СУСПІЛЬСТВА

Сучасні технології штучного інтелекту на сьогодні перетворилися з футуристичної концепції на реальність, яка глибоко проникла в усі сфери людського життя. Наразі діяльність нейромереж застосовується від персональних помічників у персональних смартфонах до складних систем прийняття рішень у медицині, фінансах, дизайні, тощо.

Однак стрімкий розвиток технологій штучного інтелекту і породжує

фундаментальні питання про їхній вплив на суспільство, економіку та саму природу людських відносин. Центральною етичною проблемою сучасного ІІІ є питання справедливості та упередженості алгоритмів. Машинне навчання, залежить від якості та репрезентативності тренувальних даних. Коли ці дані відображають історичні або соціальні упередження, алгоритми неминуче відтворюють та навіть посилюють існуючі нерівності в суспільстві.

Зокрема, на платформі для машинного навчання AI Azure ML Studio – завдяки зміщується фокус з адміністрування та розгортання моделі на безпосередню взаємодію з платформою та її налаштуваннями, що не тільки скорочує час на впровадження рішень, але й підвищує рівень безпеки та захисту інформації [3].

Особливо яскраво це проявляється в системах кримінальної юстиції, де алгоритми прогнозування ризику рецидиву можуть демонструвати расову упередженість, або у фінансовому секторі, де автоматизовані системи оцінки кредитоспроможності можуть дискримінувати певні соціальні групи. Такі рішення мають далекосяжні наслідки, адже вони не лише впливають на конкретних індивідів, але й формують соціальні структури та можливості для цілих спільнот.

Проблема ускладнюється і тим, що упередженість часто є прихованою та неочевидною навіть для розробників. Вона може проявлятися через історичні дані, які відображають минулі дискримінаційні практики, через неповну репрезентацію певних груп у тренувальних вибірках, або через складні кореляції між різними змінними, які можуть непрямо вказувати на захищені характеристики.

Сучасні ІІІ-системи вимагають величезних обсягів персональних даних для ефективного функціонування. Це створює безпрецедентні виклики для захисту приватності, оскільки кордони між публічною та приватною інформацією стають все більш розмитими. Персональні дані перетворилися на нове джерело цифрової економіки, що породжує складні питання про власність, контроль та використання інформації.

Інтеграція ІІІ в повсякденне життя має також і глибокий психологічний вплив на людей, змінюючи способи їхньої взаємодії з інформацією та один з одним. Алгоритми рекомендацій формують те, що бачать користувачі, створюючи персоналізовані інформаційні екосистеми та ізоляцію від альтернативних точок зору.

Феномен «інформаційних бульбашок» може сприяти поляризації суспільства та ускладнювати демократичний діалог, адже споживачам ІІІ стає важче приймати протилежні точки зору. Така інформізоляція підсилює незнання стосовно певних речей, процесів, подій та поглядів. Вона може стати причиною розколу суспільства, навіть, укріпленню екстремістських поглядів [1].

Крім того, постійна взаємодія з ІІІ може змінювати когнітивні процеси та соціальні навички. Дослідження показують, що надмірна залежність від автоматизованих систем може призводити до атрофії певних розумових здібностей та зниження здатності до самостійного прийняття рішень.

Етичні аспекти та ризики штучного інтелекту являють собою один із найбільших викликів сучасної цивілізації. Ці технології мають потенціал, що здатен кардинально покращити життя людей, але їхнє неконтрольоване використання може призвести до посилення нерівності, ерозії приватності та інших серйозних соціальних проблем.

Ключовим вирішенням проблеми може стати створення міжнародних механізмів співпраці та координації у сфері етики ШІ, оскільки глобальний характер технологій вимагає глобальних рішень. Водночас важливо зберігати простір для культурного різноманіття та різних підходів до питань приватності, справедливості та свободи.

Успішна інтеграція ШІ в суспільство вимагає активної участі всіх зацікавлених сторін – від технологічних компаній та урядів до громадянського суспільства та окремих користувачів. Лише через відкритий діалог, міжнародну співпрацю та постійну увагу до етичних питань ми зможемо забезпечити, що ШІ слугуватиме загальному благу людства, а не лише вузьким інтересам окремих груп. Наразі особливо актуальним питанням залишається проблема закладення етичних основ для розвитку в ці технології для забезпечення безпечного та сталого майбутнього всього людства.

Список використаних джерел:

1. Море А. У чому небезпека «інформаційної бульбашки» та як комфортно із неї вийти? URL: <https://hromadske.radio/podcasts/myslennia-bazova-funktsiia/1065085>.
2. SMART business. Розповідаємо про перший європейський закон, що контролює використання AI-технологій, а також про ризики нерегульованого використання штучного інтелекту для бізнесу. URL: <https://ce.smart-it.com/blog-post/the-good-the-bad-and-the-regulated-ai>.

УДК 004.65

*Терещенко С.С.
здобувач вищої освіти другого рівня,
Сумський національний аграрний університет*

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ СУПРОВОДЖЕННЯ ДІЯЛЬНОСТІ СУМСЬКОЇ БІЗНЕС-ШКОЛИ

Вступ. Бізнес-освіта в умовах цифрової трансформації потребує впровадження нових підходів до організації управлінських та навчальних процесів. Бізнес-школа Сумського національного аграрного університету є сучасним освітнім осередком, що реалізує інноваційні програми підготовки для студентів, підприємців, ветеранів та інших соціальних груп. Масштабність

діяльності, велика кількість освітніх курсів і слухачів створюють потребу в автоматизації процесів, які раніше здійснювалися вручну.

Викладення основного матеріалу. Супровід діяльності бізнес-школи охоплює низку завдань: прийом заяв на навчання, перевірку пакету документів, формування навчальних груп, планування занять, облік результатів слухачів, підготовку сертифікатів, а також створення звітності для адміністрації. Виконання цих функцій без інформаційної підтримки пов'язане зі значними витратами часу та ймовірністю помилок. Аналіз ринку програмних продуктів показав, що не існує загальновідомих рішень та програмних засобів, які б забезпечували повну автоматизацію виконання вказаних завдань. В таких умовах засобом вирішення процесів супроводження діяльності бізнес-школи є інформаційна система, функціонування якої забезпечує формування інформації, необхідної для прийняття обґрунтованих рішень.

Розробка та впровадження інформаційної системи базується на використанні реляційної бази даних, що забезпечує структуроване збереження відомостей про слухачів, викладачів, навчальні програми й розклад занять. Ключовим завданням є створення інтерфейсу, зрозумілого як адміністрації, так і користувачам. У такій системі адміністратор отримує можливість швидко реєструвати нових слухачів, контролювати повноту їхніх документів, формувати тематичні плани й вести електронні журнали результатів навчання. Викладач має доступ до інформації про групи, закріплені за ним. На рис.1 наведена діаграма варіантів використання, що відображає користувачів та спільні межі функціональності пропонованої інформаційної системи.

Для реалізації бази даних було обрано систему керування реляційними базами даних MySQL [1-3]. Система забезпечує ефективне збереження інформації, швидкий пошук, сортування та отримання потрібних відомостей. Керування доступом здійснюється сервером MySQL, який підтримує одночасну роботу багатьох користувачів, гарантує високу швидкодію та захищає дані від несанкціонованого доступу. MySQL функціонує як багатопотоковий сервер із підтримкою багатокористувацького режиму та використовує стандартну мову структурованих запитів SQL.

Для створення користувацького інтерфейсу, тобто клієнтської частини, застосовуються сучасні веб-технології: HTML, CSS, JavaScript та PHP [4]. Додатково адміністрування бази даних може здійснюватися за допомогою phpMyAdmin [5] – веб-інструменту з відкритим кодом, який надає зручний графічний інтерфейс для роботи з MySQL. За його допомогою можна виконувати SQL-запити, переглядати структуру й вміст таблиць, а також управляти базами даних без необхідності введення команд вручну. Це робить адміністрування доступним навіть для користувачів, які мають мінімальні знання в MySQL.



Рисунок 1. Діаграма варіантів використання

Висновок. Автоматизація процесів супроводження діяльності Сумської бізнес-школи дозволяє оптимізувати адміністративні процедури, зменшити навантаження на персонал, забезпечити швидкий доступ до інформації. Впровадження єдиної інформаційної системи сприяє створенню сучасного освітнього середовища, яке відповідає вимогам цифрової економіки та глобальним освітнім стандартам.

Список використаних джерел:

1. Welling L., Thomson L. PHP and MySQL Web Development. – Addison-Wesley, 2021. – 928 с.
2. MySQL Documentation. – Oracle Corporation, 2023. – [Електронний ресурс]. – Режим доступу: <https://dev.mysql.com/doc/>
3. W3Schools. MySQL Tutorial. – 2023. – [Електронний ресурс]. – Режим доступу: <https://www.w3schools.com/mysql/>
4. Mozilla Developer Network (MDN). HTML, CSS, JavaScript Documentation. – 2023. – [Електронний ресурс]. – Режим доступу: <https://developer.mozilla.org/>
5. phpMyAdmin. Documentation. – 2023. – [Електронний ресурс]. – Режим доступу: <https://www.phpmyadmin.net/docs/>

РОЛЬ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ДАНИХ У ПРОЦЕСІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УПРАВЛІННЯ БІЗНЕСОМ

У сучасному світі бізнес переживає фундаментальні зміни під впливом цифрової трансформації. Якщо раніше інформаційні технології виконували допоміжну функцію, забезпечуючи автоматизацію окремих процесів, то сьогодні вони визначають логіку управління компанією загалом. Використання хмарних сервісів, великих даних, штучного інтелекту, систем електронної комерції та цифрових платформ дозволяє бізнесу оптимізувати виробничі процеси, скорочувати витрати, покращувати взаємодію з клієнтами та створювати нові бізнес-моделі. Однак поряд із перевагами виникають і значні ризики, пов'язані з кіберзагрозами, що можуть зруйнувати не лише конкретний бізнес-проект, а й репутацію компанії, її ринкову вартість та довіру інвесторів [1]. У цьому контексті кібербезпека та захист даних набувають статусу стратегічних чинників, без яких цифрова трансформація управління бізнесом не може бути успішною.

Цифровізація управління бізнесом передбачає перехід до моделі, де ключовим ресурсом стають дані. Вони слугують основою для аналітики, прогнозування попиту, управління персоналом, розробки нових продуктів та стратегічного планування. Але водночас дані є найуразливішим активом компанії. Витоки персональної інформації клієнтів, фінансових звітів чи комерційної таємниці можуть призвести до судових позовів, штрафів і втрати довіри партнерів. Саме тому захист даних слід розглядати не лише як технічне завдання ІТ-відділу, а як інтегровану частину управлінської стратегії. Бізнес, що ігнорує ці виклики, ризикує втратити конкурентоспроможність, адже у світі, де дані визначають успіх, їхня безпека дорівнює життєздатності компанії.

Одним із головних викликів для бізнесу є складність глобального ринку кіберзагроз. Атаки на компанії дедалі частіше здійснюються організованими угрупованнями, які діють транснаціонально, використовуючи найновіші технології, включаючи штучний інтелект. При цьому об'єктами стають не лише великі корпорації, але й середній та малий бізнес, що часто має слабший рівень захисту. Це свідчить про те, що інвестиції у кібербезпеку не можуть обмежуватися лише окремими елементами, наприклад, антивірусними програмами. Потрібна комплексна система, яка включає моніторинг загроз, управління ризиками, розробку політик безпеки та навчання персоналу. Лише за такої умови цифрова трансформація управління бізнесом може здійснюватися без руйнівних наслідків [2].

Важливим аспектом є регуляторний тиск. У різних країнах ухвалено закони, які зобов'язують компанії дотримуватися високих стандартів захисту персональних даних. Європейський регламент GDPR, закони США та подібні

ініціативи в Азії змінюють умови ведення бізнесу на глобальному рівні. Для компаній, що прагнуть працювати на міжнародному ринку, дотримання цих стандартів є обов'язковою умовою. Порушення законодавства може призвести до мільйонних штрафів і обмеження доступу до ринку. Тому кібербезпека стає не лише фактором внутрішньої стійкості бізнесу, а й інструментом його інтеграції у світову економіку. Фактично, захист даних перетворюється на конкурентну перевагу, яка дозволяє компанії залучати нових клієнтів і партнерів.

Особливе значення у процесі цифрової трансформації управління бізнесом має довіра клієнтів. Сучасний споживач дедалі обережніше ставиться до обробки власних персональних даних. Кожна історія про витік інформації чи шахрайство в мережі негативно впливає на готовність користуватися новими сервісами. Якщо компанія не може гарантувати безпеку даних, вона втрачає клієнтів, навіть якщо пропонує привабливі продукти чи ціни. Водночас підприємства, що відкрито комунікують про заходи кіберзахисту та демонструють відповідальність у сфері безпеки, здобувають конкурентну перевагу. Це означає, що інвестиції у кібербезпеку стають не лише захисним інструментом, але й маркетинговим активом, який формує позитивний імідж бренду [3].

Цифрова трансформація управління бізнесом нерозривно пов'язана з автоматизацією та інтеграцією процесів. Використання систем управління ресурсами підприємства, CRM-платформ та інтернету речей створює єдині цифрові екосистеми, де кожен елемент взаємодіє з іншими. Проте уразливість одного компонента може поставити під загрозу всю систему. Це ще раз підкреслює стратегічне значення кібербезпеки, адже від її рівня залежить стабільність роботи всієї компанії. Тому у сучасному управлінні безпека стає невід'ємною частиною стратегічного планування, а її інтеграція у бізнес-процеси визначає здатність підприємства до сталого розвитку.

Не можна ігнорувати й людський чинник. Дослідження свідчать, що значна частина кіберінцидентів пов'язана з помилками або недбалістю співробітників. Використання слабких паролів, ігнорування оновлень програмного забезпечення чи необережне відкриття підозрілих листів може призвести до серйозних наслідків. Тому навчання персоналу та формування культури кібергігієни є не менш важливим, ніж впровадження технічних рішень. Успішна цифрова трансформація бізнесу потребує інвестицій у людський капітал, що дозволяє підвищити рівень відповідальності та готовності до дій у разі загроз [4].

Важливим є і стратегічний вимір кібербезпеки. Для багатьох компаній вона стає умовою залучення інвестицій. Інвестори все частіше оцінюють не лише фінансові показники, але й рівень захищеності бізнес-моделі від кіберризиків. Це пояснюється тим, що один серйозний інцидент здатний знищити роками напрацьовану вартість компанії. Тому прозора політика у сфері кібербезпеки та підтвердження відповідності міжнародним стандартам збільшує шанси компанії отримати доступ до капіталу і стратегічних партнерств.

У підсумку можна стверджувати, що роль кібербезпеки та захисту даних у процесі цифрової трансформації управління бізнесом є фундаментальною. Вони визначають стабільність цифрових процесів, довіру клієнтів, привабливість для інвесторів та здатність компанії інтегруватися у глобальну економіку. Кібербезпека перестає бути лише технічним завданням і стає стратегічним ресурсом, який формує конкурентоспроможність бізнесу у XXI столітті. Лише ті компанії, які усвідомлюють цю роль і розглядають інвестиції у захист даних як основу своєї стратегії, зможуть успішно пройти шлях цифрової трансформації та забезпечити довгостроковий розвиток.

Список використаних джерел:

1. Семчук Ж., Іваш А., Хоростіль О., Вовк Ю., Хміль Ю., Підгірняк О., Зубрицький В. Роль цифрових технологій у трансформації бізнес-моделей сучасних підприємств. *Академічні візії*. 2024. Випуск 28. DOI: <https://doi.org/10.5281/zenodo.11356659>
2. Шостак Л.В., Федонюк А. А., Помазун О. О. Кібербезпека в системі формування бізнес-моделі підприємства в умовах цифрової економіки. *Економіка та суспільство*. 2024. №64. DOI: <https://doi.org/10.32782/2524-0072/2024-64-37>
3. Чотири елементи сильної стратегії кібербезпеки. URL: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/four-elements-of-a-strong-cybersecurity-strategy>
4. Захист бізнесу: як убезпечити підприємство від кіберзлочинів? URL: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/business-security-how-to-protect-your-company-from-cybercrime>

УДК 004.85:616-07

**Ткаченко О. С.,
Цоколенко А. С.**
здобувачі вищої освіти,
Черкаський державний технологічний університет
Науковий керівник
Федоров Є. Є.
Професор кафедри інформаційної безпеки
та комп'ютерної інженерії
Черкаський державний технологічний університет

РОЗРОБКА АСИСТЕНТА ДЛЯ ДІАГНОСТИКИ ЗАХВОРЮВАНЬ

Актуальність теми зумовлена стрімким зростанням обсягів медичних даних та потребою в розробці точних і надійних інструментів для автоматизованої діагностики захворювань. Застосування статистичних методів

та алгоритмів машинного навчання дозволяє не лише пришвидшити процес діагностики, а й виявляти складні, нелінійні залежності в даних, що є недоступним для традиційних підходів.

Метою даної роботи є порівняльний аналіз та оцінка ефективності сучасних класифікаційних моделей для створення асистента, здатного надавати попередню оцінку стану пацієнта.

Задача діагностики захворювань формалізується як задача статистичної класифікації, де медичні показники пацієнта виступають у ролі вектора ознак, а діагноз – цільовою змінною (класом). У роботі досліджуються та порівнюються чотири ключові моделі:

1. Логістична регресія. Розглядається як базовий лінійний метод, що належить до узагальнених лінійних моделей (GLM). Її перевагою є високий рівень інтерпретованості, оскільки коефіцієнти моделі дозволяють оцінити вплив кожної ознаки на ймовірність наявності захворювання.

2. Метод k-найближчих сусідів (k-NN). Це непараметричний метод, що класифікує об'єкт на основі класів його найближчих сусідів у просторі ознак. Ефективність моделі значною мірою залежить від вибору метрики відстані (наприклад, евклідової) та гіперпараметра

3. Random Forest. Ансамблевий алгоритм, що усереднює прогнози великої кількості незалежних дерев рішень. Завдяки використанню технік бутстрепа та випадкового вибору підмножини ознак, цей метод є стійким до перенавчання та дозволяє оцінювати

4. Нейронні мережі. Цей підхід дозволяє моделювати складні нелінійні залежності між предикторами. Нейронні мережі потенційно здатні досягати найвищої точності завдяки своїй гнучкості та здатності виявляти приховані патерни у великих масивах даних.

Основою для побудови асистента є вирішення задачі бінарної або багатокласової класифікації. Процес включає наступні етапи:

1. Попередня обробка даних. Медичні дані пацієнтів, представлені у вигляді векторів ознак, підлягають процедурам нормалізації та стандартизації.

2. Вибір та обґрунтування моделей. Для аналізу обрано чотири статистичні моделі

3. Статистична оцінка якості моделей. Для порівняння прогностичної здатності моделей використовується метод перехресної валідації (cross-validation). Якість оцінюється за допомогою комплексу метрик.

Результати дослідження дозволять надати обґрунтовані рекомендації щодо вибору оптимального статистичного алгоритму для побудови асистента медичної діагностики, враховуючи баланс між точністю прогнозу, інтерпретованістю моделі та обчислювальною складністю.

Список використаних джерел:

1. Довідник по Machine Learning. URL: <https://itwiki.dev/data-science/ml-reference>

Уткін Євгеній,
студент групи ІНФМ-24-2
Харківський національний університет радіоелектроніки,
uevhenii.utkin@nure.ua
Тітова О.В.,
к.т.н., доцент, доцент кафедри інформатики
Харківський національний університет радіоелектроніки,
olena.titova@nure.ua

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ RAG ЯК ОДНА ІЗ СТРАТЕГІЙ ПОКРАЩЕННЯ РОБОТИ LLM СИСТЕМ

Сучасні великі мовні моделі (Large Language Models, LLM) здобули широке застосування у різноманітних сферах, включаючи автоматизацію текстових процесів, машинний переклад, генерацію контенту та побудову чат-ботів. LLM, такі як GPT, BERT та їх модифікації, демонструють високу ефективність у задачах розпізнавання природної мови завдяки здатності працювати з великими обсягами даних та навчатися на багатомільярдних параметрах. Проте, незважаючи на значні успіхи, існують обмеження цих систем, пов'язані з точністю, контекстуальною релевантністю відповідей та обмеженнями у роботі з специфічною або динамічною інформацією.

Одним із ключових напрямів удосконалення LLM є інтеграція технологій пошуку та доступу до зовнішніх баз знань, що дозволяє системі підвищити точність відповідей і враховувати актуальні дані. Технологія RAG (Retrieval-Augmented Generation) є одним із таких підходів. RAG поєднує два етапи: етап пошуку релевантної інформації (retrieval) та етап генерації тексту (generation). Перший етап передбачає використання векторних представлень запитів та документів для знаходження найбільш релевантних джерел у великих корпусах даних. Другий етап – генерація відповіді на основі знайдених джерел із залученням LLM, що дозволяє підвищити точність та достовірність результатів.

Суттєвим аспектом є методи представлення текстових даних у вигляді векторів (embedding), які забезпечують ефективний пошук релевантних документів. Використання різних алгоритмів для побудови векторних репрезентацій – таких як BERT embeddings, Sentence Transformers чи OpenAI embeddings – впливає на якість результатів системи RAG. Вибір конкретного методу залежить від характеру текстових даних, розмірів бази знань та необхідної точності генерації [1-2].

Крім того, у предметній області досліджуються аспекти оптимізації продуктивності LLM систем у поєднанні з RAG. Це включає питання швидкості обробки запитів, масштабованості системи при збільшенні обсягу даних, а також ефективності навчання моделей. Однією з актуальних проблем є баланс

між швидкістю відповіді та якістю генерації: більш детальний пошук релевантних документів може покращити точність, але збільшити час обробки запиту.

Також варто відзначити сучасні підходи до покращення роботи LLM з RAG у практичних додатках. Наприклад, інтеграція систем RAG у корпоративні бази знань дозволяє забезпечити користувачів актуальною інформацією з внутрішніх джерел. У наукових дослідженнях RAG використовується для автоматичного пошуку літератури та синтезу оглядів по заданій темі. У комерційних продуктах, таких як чат-боти підтримки клієнтів, застосування RAG забезпечує відповіді на специфічні запити, знижуючи кількість некоректних або узагальнених відповідей.

Важливо зазначити, що успіх інтеграції RAG у LLM залежить від кількох факторів:

- якість та структура бази знань: релевантність і повнота інформації у документальному корпусі;
- вибір методу пошуку: ефективність алгоритмів векторного пошуку та обробки запитів;
- параметри генерації: оптимізація архітектури LLM для роботи з додатковими джерелами інформації;
- механізми оновлення знань: здатність системи швидко адаптуватися до нових даних та змін у базі знань;

Отже, аналіз предметної області показує, що інтеграція технології RAG із LLM системами дозволяє значно підвищити їх ефективність у задачах генерації тексту та пошуку релевантної інформації. Це відкриває перспективи для подальших досліджень у сфері оптимізації архітектури LLM, удосконалення методів пошуку інформації та адаптації систем під специфічні задачі користувача. Виявлені закономірності та підходи до покращення роботи LLM через RAG лягатимуть в основу подальших експериментальних досліджень та розробки прототипів систем підвищеної продуктивності [3-4].

Список використаних джерел:

1. Lewis, M., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., ... & Riedel, S. (2020) Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks.
2. Karpukhin, V., Oguz, B., Min, S., Lewis, P., Wu, L., Edunov, S., ... & Yih, W.-t. (2020) Dense Passage Retrieval for Open-Domain Question Answering.
3. Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2019) BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding.
4. Тітов С.В., Тітова О.В., Чорна О.С. Опис нескоротних наборів ознак в приблизних множинах з використанням систем числення // Збірник наукових праць Харківського національного університету Повітряних Сил. № 1 (71) 2022, с. 106–110.

Хомсі Как С.М.

здобувач вищої освіти,

Харківський національний університет радіоелектроніки

Науковий керівник

Кобилін О. А.

Завідувач кафедри інформатики, кандидат технічних наук, доцент

Харківський національний університет радіоелектроніки

МЕТОДИ ДІАГНОСТИКИ СТАНУ СОНЯЧНИХ ПАНЕЛЕЙ ЗА ДОПОМОГОЮ КОМП'ЮТЕРНОГО ЗОРУ

Сонячна енергетика є одним із найперспективніших напрямів відновлюваної енергетики, частка якої в світовому енергобалансі постійно зростає. За даними Міжнародного агентства відновлюваної енергетики (IRENA), глобальна потужність відновлюваних джерел енергії зросла на рекордних 15,1% у 2024 році, досягнувши 4,448 ГВт [1]. Проте ефективність роботи сонячних панелей значною мірою залежить від їх технічного стану та своєчасного виявлення дефектів.

Забруднення поверхні панелей є однією з найпоширеніших проблем. Дослідження показують, що накопичення пилу може призводити до зниження ефективності панелей від 10% в помірних умовах до понад 40% в посушливих регіонах [2]. У найгірших випадках, у запилених або забруднених умовах накопичення твердих частинок може призводити до зниження ефективності до 60% без регулярного очищення [3]. Це перешкоджає ефективному поглинанню сонячного випромінювання та значно зменшує вироблення енергії.

Традиційні методи діагностики сонячних панелей, такі як візуальний огляд, термографічний контроль та електричні вимірювання, мають ряд обмежень: високу вартість, значні витрати часу, необхідність кваліфікованого персоналу та складність автоматизації процесу. Візуальний огляд потребує фізичної присутності інспекторів на об'єкті, що створює додаткові логістичні витрати та обмеження по часу. Термографічні методи вимагають спеціалізованого обладнання та сприятливих погодних умов, оскільки хмарність або дощ можуть значно вплинути на точність вимірювань. Електричні тести часто потребують відключення панелей від мережі, що призводить до втрати виробництва електроенергії під час діагностики. Ручні інспекції стикаються з такими обмеженнями [3]: безпековими ризиками (падіння, електричні удари), значними витратами часу для великих установок, суб'єктивністю оцінки різними інспекторами, обмеженнями через погодні умови та складністю доступу до віддалених панелей.

На основі аналізу практичного досвіду експлуатації виділяють ключові типи дефектів [3], такі як забруднення та накопичення пилу (навіть 1-мікронний шар може спричинити 25,5% зниження ефективності [4]), вологопроникнення з корозією контактів, пошкодження від штормів та граду, дефекти контактів із

утворенням гарячих точок, механічні пошкодження від тварин, неправильне підключення та дефектні байпасні діоди.

Ринок дронів інспекцій в енергетиці зростає з 118,8 млн доларів (2020) до 476,5 млн (2028), CAGR 18,9% [3]. Дрони з комп'ютерним зором забезпечують високоякісне захоплення даних камерами та тепловізорами, автоматизоване виявлення аномалій через алгоритми CV, точну класифікацію дефектів за допомогою глибокого навчання, прогнозувальне обслуговування на основі аналізу патернів.

Розвиток сучасних методів комп'ютерного зору відкриває нові можливості для автоматизованої діагностики. Конволюційні нейронні мережі (CNN) показують високу ефективність при класифікації дефектів, досягаючи точності понад 95% на тестових наборах даних. Методи семантичної сегментації дозволяють не лише виявляти наявність дефекту, а й точно локалізувати його межі на зображенні панелі.

Алгоритми предобробки зображень включають корекцію освітлення, нормалізацію контрасту та фільтрацію шумів, що критично важливо для забезпечення стабільності роботи системи в різних погодних умовах. Застосування методів аугментації даних дозволяє підвищити стійкість моделей до варіацій в умовах знімання.

Автоматизовані системи діагностики забезпечують [2,3,4] попередження втрат ефективності до 60% через забруднення, підвищення безпеки інспекційних робіт, зниження експлуатаційних витрат через прогнозувальне обслуговування, швидку окупність інвестицій у сонячну енергетику.

Застосування комп'ютерного зору та машинного навчання для виявлення дефектів сонячних панелей є актуальним напрямом з високим практичним потенціалом. Стрімкий розвиток дронів технологій та їх економічна ефективність підтверджують перспективність автоматизованих рішень для підвищення надійності та ефективності сонячної енергетики.

Список використаних джерел

1. World Economic Forum. Renewable energy capacity surged around the world in 2024. URL: <https://www.weforum.org/stories/2025/04/renewable-energy-transition-wind-solar-power-2024/> (дата звернення: 16.09.2025).
2. Gholami, A., et al. A holistic review of the effects of dust buildup on solar photovoltaic panel efficiency. ScienceDirect, 2024. URL: <https://www.sciencedirect.com/science/article/pii/S2772940024000353> (дата звернення: 17.09.2025).
3. ImageVision.AI. Insights from Above: Advancements in Solar Panel Inspection with Vision AI Drones. URL: <https://imagevision.ai/blog/insights-from-above-advancements-in-solar-panel-inspection-with-vision-ai-drones/> (дата звернення: 18.09.2025).
4. MIT News. How to clean solar panels without water. Massachusetts Institute of Technology, 2022. URL:

УДК: 004.738. 5

*Хом'як А.В.
здобувач вищої освіти
другого (магістерського) рівня,
Державний податковий університет
Науковий керівник
Погорєловська І. Д.
к.е.н., доцент, доцент кафедри
комп'ютерних та інформаційних технологій і систем
Державний податковий університет*

ТЕХНОЛОГІЯ BLOCKCHAIN ТА ЇЇ ЗАСТОСУВАННЯ

У сучасному світі, де цифровізація проникає практично в усі сфери життя, виникає нагальна потреба у нових підходах до збереження, обробки та захисту інформації. Однією з найбільш перспективних інновацій останніх десятиліть є технологія blockchain, яка ґрунтується на принципах децентралізації, прозорості та незмінності даних. Ця технологія створює фундамент для розвитку нових інформаційних систем, які здатні забезпечити високий рівень безпеки та довіри між учасниками процесів, навіть за умови їхньої географічної віддаленості чи відсутності особистого контакту [1].

Blockchain можна визначити як розподілений реєстр, у якому інформація зберігається у вигляді послідовно з'єднаних блоків. Кожен блок має криптографічний зв'язок із попереднім, що робить зміну даних практично неможливою без відома всіх учасників системи. На відміну від традиційних централізованих баз даних, блокчейн виключає можливість маніпуляцій однією стороною та гарантує прозорість усіх транзакцій. Це робить технологію надзвичайно актуальною у тих сферах, де довіра та захист інформації є ключовими факторами [2].

Сучасні технології блокчейну охоплюють публічні мережі (Bitcoin, Ethereum), приватні та консорціумні рішення для бізнесу, смарт-контракти, які автоматизують угоди, та DeFi-платформи, що замінюють посередників у фінансах. Важливими напрямками є NFT для підтвердження унікальної цифрової власності, DAO для децентралізованого управління, рішення другого рівня (Layer 2) для масштабування й здешевлення транзакцій, токенизація реальних активів, кросчейн-платформи (Polkadot, Cosmos) для взаємодії між мережами, а також Blockchain-as-a-Service (BaaS), що дає змогу компаніям швидко впроваджувати технологію без створення власної інфраструктури (рис.1).

Найбільш відомим прикладом використання блокчейну стали криптовалюти. Bitcoin, Ethereum та інші цифрові валюти стали символом нової

економічної епохи, в якій гроші існують у вигляді коду, а операції відбуваються без посередників. Проте значення цієї технології виходить далеко за межі фінансових транзакцій.

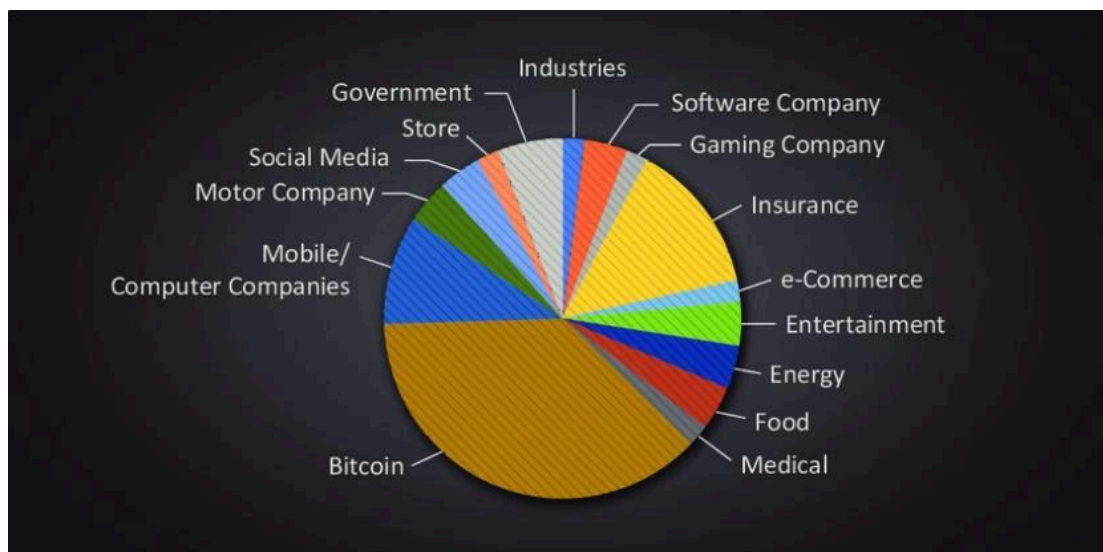


Рис. 1. Використання блокчейну в різних сферах <https://surl.li/nyaxjd>

Сьогодні активно розвивається сфера децентралізованих фінансів (DeFi), яка дозволяє користувачам здійснювати обмін, інвестування та кредитування без участі банків. Це не лише знижує вартість операцій, але й робить фінансову систему більш прозорою та доступною [3].

Не менш значущим є застосування блокчейну у сфері логістики та управління ланцюгами постачання. Завдяки цій технології можна відстежувати походження товарів, контролювати їхній рух від виробника до кінцевого споживача та уникати підробок. Наприклад, міжнародні корпорації вже впроваджують блокчейн-рішення для моніторингу вантажів у реальному часі, що дозволяє мінімізувати витрати на документообіг та забезпечити прозорість усіх операцій [4].

Важливим напрямом використання є цифрова ідентифікація. Blockchain надає можливість створювати унікальні захищені цифрові профілі, які можна застосовувати для отримання державних послуг, відкриття банківських рахунків або доступу до медичної інформації. Одним із найяскравіших прикладів є досвід Естонії, яка використовує блокчейн у системі електронного урядування. Це дозволяє громадянам здійснювати більшість адміністративних процедур онлайн із повною впевненістю у захисті своїх персональних даних [5].

Особливий інтерес становить використання блокчейну у сфері електронного голосування. Демократичні процеси завжди потребували максимальної прозорості та захисту від фальсифікацій. Технологія блокчейну дозволяє створювати системи, у яких кожен голос буде зафіксований та підтверджений, а можливість його зміни чи видалення буде виключена. Пілотні проекти у Швейцарії та США продемонстрували потенціал таких рішень для зміцнення довіри суспільства до виборчого процесу [6].

Ще однією важливою галуззю є охорона здоров'я. Тут блокчейн допомагає вирішувати проблему захисту медичних даних, забезпечуючи конфіденційність і контрольований доступ до історії хвороб. Лікарні та страхові компанії можуть швидко обмінюватися даними, не ризикуючи безпекою пацієнтів. Це значно спрощує взаємодію у медичній сфері та підвищує ефективність роботи.

У сфері енергетики блокчейн дає змогу створювати нові моделі торгівлі електроенергією. В окремих країнах уже впроваджуються проекти, у межах яких власники сонячних панелей продають надлишкову енергію іншим споживачам через блокчейн-платформи. Це сприяє розвитку «зеленої» енергетики та формуванню децентралізованих енергетичних систем [7].

Усі ці приклади демонструють, чому блокчейн вважають однією з найважливіших сучасних технологій. Його головна перевага полягає в поєднанні безпеки, прозорості та децентралізації. Завдяки цьому технологія здатна мінімізувати корупційні ризики, знизити витрати на посередників, забезпечити довіру між сторонами та створити системи, стійкі до кібератак. Саме тому вибір на користь блокчейну є найкращим для тих сфер, де надійність даних і безпека процесів мають вирішальне значення.

Таким чином, блокчейн поступово перетворюється на універсальний інструмент, що охоплює фінанси, логістику, охорону здоров'я, енергетику та політичні процеси. Його впровадження дозволяє не лише оптимізувати бізнес-процеси, але й підвищити довіру в інформаційному середовищі, що є особливо актуальним у сучасних умовах розвитку кібербезпеки.

Список використаних джерел

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. URL: <https://bitcoin.org/bitcoin.pdf>
2. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. Blockchain technology: Beyond bitcoin. Applied Innovation Review. 2016. URL: <https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf>
3. Schär, F. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis Review, 2021. URL: <https://www.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets>
4. IBM Newsroom. Blockchain in Supply Chain. URL: <https://www.ibm.com/solutions/blockchain-supply-chain>
5. E-Estonia Official Website. Blockchain in Estonian e-Governance. URL: <https://e-estonia.com/>
6. Zug, Switzerland e-voting pilot projects. Swissinfo. URL: <https://www.swissinfo.ch/eng/swiss-politics/most-swiss-abroad-wont-be-able-to-vote-online-in-2027/89522794>
7. Power Ledger. Blockchain in Energy Trading. URL: <https://powerledger.io/media/the-future-of-decentralised-energy-powerledgers-research-in-blockchain-and-p2p-trading/>

Чалій К.Р.

*здобувачка вищої освіти,
Факультет фінансів та цифрових технологій,
Державний податковий університет
Науковий керівник*

Омельчук А.А.

*к.т.н., доцент кафедри комп'ютерних та інформаційних технологій і
систем, Факультет фінансів та цифрових технологій,
Державний податковий університет*

ВІРТУАЛЬНА ЛАБОРАТОРІЯ НА ОСНОВІ ГЕНЕРАТИВНОГО ШІ

Аналіз ринку показує, що існуючі платформи, такі як Labster та PhET Interactive Simulations, функціонують за моделлю бібліотек із готовими, попередньо запрограмованими сценаріями. Labster є зразковим інструментом завдяки глибокій інтеграції в навчальні програми (LMS) та B2B-моделі, тоді як PhET є лідером серед інструментів у відкритому доступі.

Запропонований у роботі вебзастосунок QuantumLear не є безпосереднім їх конкурентом, але натомість створює нову категорію [1]. Його стратегічне позиціонування визначається наступними факторами:

- Платформа є не просто віртуальною лабораторією, а «генеративним науковим верстатом», що дозволяє користувачам проводити значну кількість експериментів, а не просто використовувати шаблони [2].

- QuantumLear підвищує доступність наукового моделювання, надаючи можливості обчислювальних інструментів (аналогічних NetLogo або Wolfram|Alpha) аудиторії без навичок програмування.

- стратегія полягає у створенні інструменту, який архітектура конкурентів не може підтримати. Це дозволяє орієнтуватися не лише на студентів, а й на дослідників, яким потрібне швидке прототипування моделей [3].

В основі QuantumLear лежить архітектура, що діє як компілятор природної мови. Запит користувача обробляється моделлю Gemini Pro. Критично важлива технологія «Function Calling» використовується для видобування неструктурованого тексту та перетворення його на чіткі, машиночитані параметри симуляції (наприклад, маси об'єктів, початкові швидкості, часові рамки). Структуровані параметри передаються до Gemini з новим завданням: «Згенеруй скрипт на Python для цієї симуляції». Модель створює виконуваний код, використовуючи стандартні наукові бібліотеки (NumPy, SciPy, ChemPy, AgentPy).

Згенерований код виконується в ізольованому серверному середовищі (пісочниці, наприклад, Docker-контейнер) для забезпечення безпеки та стабільності (Рис. 1).

Числові результати симуляції передаються на фронтенд і візуалізуються за допомогою інтерактивних бібліотек: Plotly.js для 2D-графіків та Three.js для імерсивних 3D-сцен (наприклад, зіткнення галактик).

Цей підхід є модульним, що дозволяє додавати підтримку нових наукових дисциплін шляхом створення нових «галузових пакетів» без зміни ядра системи.

Для побудови довіри та запобігання дезінформації і галюцинаціям ШІ, проєкт включає кілька рівнів захисту та підвищення цінності результатів:

– Після завершення симуляції асистент «Ньютон» (елемент QuantumLeap) не просто показує дані. Він аналізує результати, виявляє ключові тенденції та автоматично генерує звіт у науковому форматі (вступ, методологія, результати, аналіз, висновки). Це може слугувати функціональним педагогічним інструментом для навчання студентів науковому письму [4].

– Архітектура RAG (Retrieval-Augmented Generation) є ключовою стратегією боротьби з неточністю. Перш ніж генерувати будь-яке пояснення, система виконує пошук у власній базі знань (підручники від OpenStax, статті з arXiv). Отримана фактична інформація вставляється в запит до ШІ, змушуючи його обґрунтовувати свої висновки на перевірених джерелах. Це перетворює ШІ з «чорної скриньки» на верифікованого асистента.

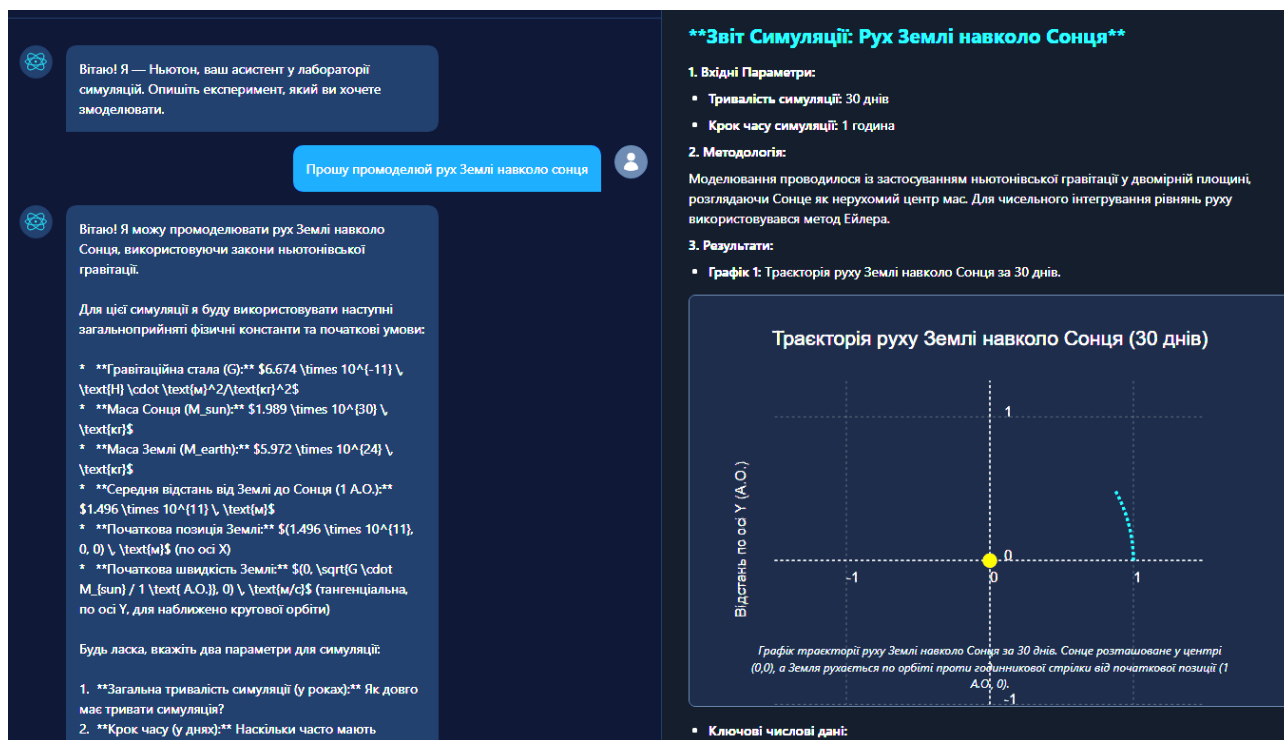


Рис.1 – Робоче вікно вебзастосунку QuantumLeap

Інтерфейс застосунку проєктується для побудови довіри через прозорість:

– Замість простого текстового поля, користувач взаємодіє з системою через діалог. Після введення запиту ШІ показує видобуті параметри у структурованій формі («Я зрозумів, що маса об'єкта A = X. Це правильно?») і дає користувачеві можливість їх відредагувати перед запуском. Цей підхід «людина в циклі» надає користувачеві додатковий контроль.

– Для перетворення платформи на справжній науковий інструмент пропонується реалізувати симуляції Монте-Карло (багаторазові запуски з

варіаціями). Результати будуть представлені не як одна лінія на графіку, а як довірчий інтервал або ймовірнісне хмара точок, що візуалізує варіативність та надійність моделі.

Можливі ризики та стратегії їх пом'якшення:

– Потенційна генерація некоректного коду, яка вимагає багаторівневої валідації (статичний аналіз коду, автоматичне модульне тестування та порівняння результатів із заздалегідь обчисленими еталонами для стандартних задач).

– Високі операційні витрати на API та обчислення потребують вибіркового використання багаторівневих моделей (дешевші моделі для простих завдань), кешування згенерованого коду для повторних запитів та оптимізація моделей.

– Низька продуктивність у вузькоспеціалізованих наукових галузях, яке передбачатиме Застосування параметро-ефективних методів доналаштування (PEFT), таких як LoRA, на наборах даних з конкретної дисципліни.

Перспективи подальшого розвитку:

1. Почати з однієї, візуально вражаючої та популярної галузі – астрофізики (наприклад, симуляція зіткнення галактик). Це дозволить довести працездатність концепції та стане ефективним маркетинговим інструментом.

2. Послідовно розширювати платформу на інші галузі (біологія, хімія, економіка) та розробити інтеграції з ключовими системами управління навчанням (LMS), такими як Canvas та Moodle.

3. Справжня перевага буде не в самій технології ШІ, а в екосистемі (бібліотеці шаблонів, створених користувачами, наборі рецензованих перевірених моделей для викладачів та унікальних даних про тенденції в науці та освіті).

Поліпшення вебзастосунку полягає у розширенні можливостей для прийому мультимодальних вхідних даних (наприклад, аналіз зображення або CSV-файлу) та еволюції асистента «Ньютон» у повноцінного автономного ШІ-агента, здатного самостійно планувати та виконувати серії експериментів для досягнення дослідницької мети.

Список використаних джерел:

1. Горбовий, А. Ю., Лаговський, В. В., & Омельчук, А. А. (2023). Штучний інтелект у текстильній промисловості. Прикладні питання математичного моделювання, 3(2.2), 123–132. <https://doi.org/10.32782/KNTU2618-0340/2020.3.2-2.11>
2. Google AI Studio. URL: <https://aistudio.google.com/>
3. Hladchenko, O., Ratushnyak, T., Omelchuk, A., Nizhehorodtsev, V., Vyshemirska, Y., & Bespartochna, O. (2023). Peculiarities of the formation of information culture of future specialists of digital design (education and professional program “digital design technology”). Theory and Practice of Social Systems Management, (4), 85–103. <https://doi.org/10.20998/2078-7782.2023.4.08>
4. Римар, Б., Гобир, Л., & Ваврик, Т. (2025). ШТУЧНИЙ ІНТЕЛЕКТ В ОСВІТІ: МОЖЛИВОСТІ ТА ВИКЛИКИ. *Herald of Khmelnytskyi National*

УДК 004.7

Чистохін О.Ю.

здобувач вищої освіти,

ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ДОСЛІДЖЕННЯ ВПЛИВУ ГНУЧКИХ МЕТОДОЛОГІЙ НА ЕФЕКТИВНІСТЬ ПРОЦЕСУ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Інтернет речей (Internet of Things, IoT) сьогодні розглядається як одна з ключових технологій цифрової трансформації. Завдяки об'єднанню фізичних пристроїв, датчиків, контролерів та програмного забезпечення у єдину інфраструктуру, IoT відкриває широкі можливості для автоматизації, аналітики даних та підвищення ефективності виробничих і побутових процесів. Водночас розширення масштабів використання IoT супроводжується зростанням вимог до його відмовостійкості та надійності. Збої в роботі сенсорних мереж, шлюзів або хмарних платформ можуть спричинити суттєві економічні втрати, зниження рівня безпеки або навіть загрози для життя людей, особливо у критично важливих сферах, як-от охорона здоров'я, транспорт чи енергетика. Саме тому дослідження методів забезпечення безперервності функціонування та надійності IoT є одним з основних напрямів сучасної науки і практики [1].

Відмовостійкість у контексті IoT означає здатність системи продовжувати виконувати основні функції навіть у разі часткового виходу з ладу окремих її компонентів. На відміну від традиційних інформаційних систем, IoT має децентралізовану архітектуру, де численні пристрої можуть працювати в різних умовах, мати різні обчислювальні ресурси і рівень енергозабезпечення. Це ускладнює завдання розробників, оскільки класичні методи забезпечення відмовостійкості (наприклад, дублювання серверів) не завжди можуть бути прямо застосовані [2-3].

Одним із базових методів підвищення відмовостійкості є надлишковість. Йдеться про дублювання каналів зв'язку, сенсорів або вузлів мережі, що дозволяє у випадку виходу з ладу одного елемента автоматично переключитися на резервний. Для критично важливих систем застосовують багаторівневу надлишковість – на рівні датчиків, шлюзів та хмарних обчислювальних ресурсів. Однак цей метод потребує значних фінансових витрат та підвищує складність управління [2].

Інший напрям забезпечення надійності пов'язаний із використанням розподілених протоколів маршрутизації та балансування навантаження. У сенсорних мережах IoT часто застосовують алгоритми, що дозволяють динамічно визначати найоптимальніші шляхи передачі даних залежно від

поточного стану вузлів та мережевих каналів. Прикладом можуть бути протоколи RPL (Routing Protocol for Low-Power and Lossy Networks) або спеціалізовані варіанти адаптивних алгоритмів, які враховують енергоспоживання датчиків. Таким чином, забезпечується не лише підвищення надійності, але й ефективне використання обмежених ресурсів [3].

Важливою складовою є також моделі прогнозування відмов. Завдяки методам машинного навчання та аналізу великих даних можливо заздалегідь виявляти тенденції до деградації вузлів чи мережі. Наприклад, аналіз частоти втрати пакетів або змін у рівні сигналу дозволяє виявити проблеми ще до їх критичного прояву. Це забезпечує можливість проактивного обслуговування, що особливо важливо для промислових IoT-систем.

Для підвищення надійності все частіше застосовують технології віртуалізації та хмарних обчислень. Хмарні сервіси дають змогу масштабувати ресурси у разі зростання навантаження, а також швидко відновлювати роботу системи після відмов. Використання контейнеризації (Docker, Kubernetes) дозволяє автоматизувати розподіл завдань між віртуальними вузлами та підтримувати безперервність роботи сервісів. Це особливо ефективно у великих розподілених IoT-мережах [1, 3].

Окрему увагу варто приділити захисту від кібератак, адже надійність IoT визначається не лише технічними відмовами, а й стійкістю до зовнішніх загроз. Атаки типу «відмова в обслуговуванні» (DoS, DDoS) можуть паралізувати роботу системи навіть без фізичних поломок. Для протидії застосовують багаторівневі механізми шифрування, аутентифікації та виявлення аномалій у трафіку. Важливим є також використання блокчейн-технологій для забезпечення цілісності даних та надійності транзакцій між пристроями.

Дослідження показують, що комбінований підхід є найбільш ефективним. Поєднання надлишковості, інтелектуальних алгоритмів маршрутизації, прогновної аналітики та хмарних сервісів дозволяє створити стійку і гнучку інфраструктуру IoT. Проте при проектуванні таких систем необхідно враховувати специфіку галузі застосування: для розумних будинків акцент робиться на енергоефективності, для промислових систем – на реальному часі та стійкості до відмов, для медицини – на надійності та безпеці даних.

Таким чином, забезпечення відмовостійкості та надійності IoT є комплексним завданням, яке включає інженерні, програмні та організаційні заходи. Сучасні методи дозволяють суттєво знизити ризики збоїв, проте зростання масштабів та різноманітності IoT-впроваджень потребує подальших наукових досліджень та розробки нових алгоритмів, здатних адаптуватися до динамічного середовища.

Список використаних джерел:

1. Жураковський Б. Ю., Зенів І. О. Технології інтернету речей : навчальний посібник / Б. Ю. Жураковський, І. О. Зенів. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 271 с.
2. Agrawal A., Toshniwal D. Fault Tolerance in IoT: Techniques and Comparative Study // Asian Journal for Convergence in Technology. – 2021. – Vol. 7,

3. Ілляшенко О. О., Колісник М. А., Стрелкіна А. Е., Коцюба І. В., Харченко В. С. Conception and application of dependable internet of things based systems. Radio Electronics, Computer Science, Control. 2020. № 4. С. 139–150. DOI: <https://doi.org/10.15588/1607-3274-2020-4-14>

УДК 004:[33+37]-004.922

Чорненко С.В.

курсант 2-го курсу,

ННІ№4 Харківський національний університет внутрішніх справ

Науковий керівник

Світличний В.А.

доцент кафедри протидії кіберзлочинності, к.т.н., доцент

ННІ№4 Харківський національний університет внутрішніх справ

РОЗВИТОК ІНТЕЛЕКТУАЛЬНИХ ПРОГРАМНИХ СИСТЕМ ДЛЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ВИРОБНИЧИХ, ОСВІТНІХ ТА БІЗНЕС-ПРОЦЕСІВ

У сучасному світі цифрова трансформація стала ключовим фактором розвитку суспільства, економіки та освіти, особливо під час війни. Програмні системи, побудовані на основі інтелектуальних технологій, відіграють важливу роль у підвищенні ефективності процесів, прийнятті управлінських рішень і створенні нових можливостей для розвитку підприємств та організацій. Сьогодні особливої актуальності набуває дослідження перспектив та шляхів розвитку інтелектуальних програмних систем, здатних забезпечувати комплексну підтримку виробничих, освітніх і бізнес-процесів – рис.1. [2]

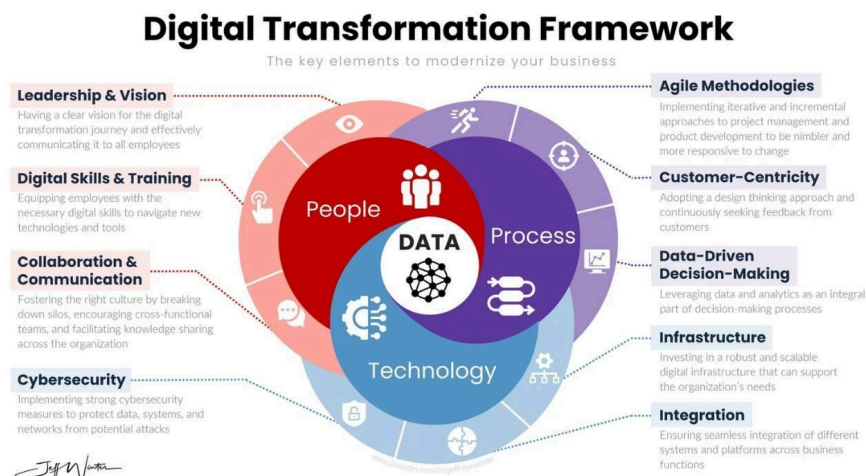


Рисунок 1 – Розвиток програмних систем для цифрової трансформації
*дані сформовано [5]

У виробничій сфері впровадження інтелектуальних програмних систем дозволяє автоматизувати процеси планування, моніторингу та управління ресурсами. Системи прогнозової аналітики на основі машинного навчання здатні передбачати потреби в матеріалах, оптимізувати логістику та знижувати витрати. Використання цифрових двійників (digital twins) дає змогу моделювати виробничі процеси в реальному часі, що сприяє зменшенню кількості помилок і підвищенню продуктивності. Таким чином, цифрова трансформація виробництва ґрунтується на використанні програмних засобів, які поєднують традиційну автоматизацію з алгоритмами штучного інтелекту.[1]

Освіта є ще одним напрямом, де інтелектуальні програмні системи сприяють суттєвим змінам. Адаптивні освітні платформи забезпечують індивідуалізацію навчання, враховуючи потреби, рівень підготовки та темп засвоєння матеріалу кожним студентом. Використання технологій аналізу освітніх даних (Learning Analytics) дозволяє своєчасно виявляти прогалини у знаннях і пропонувати персоналізовані рекомендації. Віртуальні лабораторії та симулятори створюють умови для практичного навчання без значних матеріальних витрат. Таким чином, інтелектуальні програмні засоби сприяють розвитку освіти нового типу – інтерактивної, персоналізованої та доступної.[4]

У сфері бізнесу інтелектуальні програмні системи стали основою для прийняття стратегічних і тактичних рішень. Сучасні платформи бізнес-аналітики дозволяють інтегрувати та аналізувати великі масиви даних у режимі реального часу. Це забезпечує компанії можливість оперативно реагувати на зміни ринку, оптимізувати маркетингові кампанії, прогнозувати попит і формувати нові бізнес-моделі. Алгоритми штучного інтелекту допомагають не лише автоматизувати рутинні завдання, але й пропонувати нові управлінські сценарії, що знижує рівень ризику та підвищує конкурентоспроможність.[3]

Важливо підкреслити, що розвиток інтелектуальних програмних систем не обмежується окремими сферами діяльності. Сучасні технології спрямовані на створення інтегрованих цифрових екосистем, де виробництво, освіта та бізнес-аналітика взаємодіють у єдиному інформаційному просторі. Такий підхід сприяє формуванню нової цифрової економіки, де дані стають основним стратегічним ресурсом, а програмні рішення – головним інструментом їх ефективного використання.[4]

Отже, інтелектуальні програмні системи відіграють визначальну роль у цифровій трансформації сучасного суспільства. Виробництво отримує інструменти для оптимізації процесів і зниження витрат, освіта – нові можливості для персоналізованого навчання, а бізнес – ефективні механізми аналітики та прийняття рішень. Подальший розвиток таких систем пов'язаний з інтеграцією штучного інтелекту, великих даних та хмарних обчислень, що створює умови для формування єдиної цифрової екосистеми майбутнього.

Список використаних джерел:

1. OECD. Digital Transformation: Shaping Policies, Improving Lives. – OECD Publishing, Paris, 2019.

2. Gartner. Top Strategic Technology Trends for 2024: AI and Beyond. – Gartner Research, 2024.

3. Стець О.В., Осіпчук К.О. Вплив цифровізації на ефективність бізнес-аналітики підприємства. Цифрова економіка та економічна безпека. 2024. Випуск 4(13). С. 187–190. URL: <http://dees.iei.od.ua/index.php/journal/article/view/436/418>

4. Конрад Тетяна; Волкогон Вікторія. Цифрова трансформація освіти і науки України в контексті стратегічного галузевого партнерства з країнами ЄС та інтеграції до ЄПВО (огляд). Наукоємні технології, № 63, 2024. URL: <https://doi.org/10.18372/2310-5461.63.18946>

5. Jeff Winter. Digital Transformation Framework – People , Process, Technology, & Data. URL: <https://www.jeffwinterinsights.com/insights/digital-transformation-framework-ppt>

УДК 004.4:005.8:005.52

Шаров С.В.

*к.пед.н., доцент, завідувач кафедри комп'ютерних наук
Таврійський державний агротехнологічний університет
імені Дмитра Моторного*

СИСТЕМИ УПРАВЛІННЯ ІТ-ПРОЄКТАМИ ЯК СУЧАСНИЙ ПІДХІД ДО АВТОМАТИЗАЦІЇ УПРАВЛІНСЬКИХ РІШЕНЬ

Сучасний розвиток цифрових технологій актуалізує потребу у застосуванні нових підходів до організації управлінських і виробничих процесів. Особливої актуальності набуває використання програмних продуктів (локальних та онлайн), що забезпечують автоматизацію та оптимізацію прикладних задач у різних сферах діяльності людини. Водночас, розробка різноманітного програмного забезпечення та його впровадження в управлінські процеси також вимагає дієвого проектного менеджменту. Це дозволяє не лише підвищувати продуктивність команди, але й адаптуватися до викликів зовнішнього середовища.

Управління проектами, що пов'язані з розробкою та впровадженням програмних засобів, вимагає координації ресурсів, часу та комунікацій між учасниками [2, с. 1927]. Проблематика ІТ-проектів ускладнюється постійним розвитком технологій та відповідними змінами вимог, що висуваються до програмних продуктів. Водночас, традиційні методи управління часто виявляються недостатніми для реалізації таких проектів. Зазначені тенденції зумовлюють необхідність аналізу сучасних програмних інструментів та методологій управління ІТ-проектами.

На сьогодні існують відповідні методології управління проектами, що дозволяють гнучко адаптуватися до мінливих закономірностей в ІТ-сфері, підвищувати ефективність роботи команд, забезпечувати прозорість усіх

бізнес-процесів. Серед найбільш поширених підходів до управління ІТ-проєктами виокремлюють моделі Waterfall, Agile, Scrum, Lean та Kanban, кожна з яких має власні переваги, обмеження та сфери застосування. Зокрема, каскадна модель Waterfall використовується для проєктів із чітко визначеними етапами та вимогами, тоді як Agile і Scrum [5, с. 170] орієнтовані на ітеративний розвиток, швидке реагування на зміни та активну комунікацію в команді. Lean та Kanban спрямовані на усунення зайвих витрат часу й ресурсів, забезпечуючи максимальну ефективність ІТ-менеджменту.

Крім методологій, управління ІТ-проєктами тісно пов'язане із застосуванням спеціалізованих цифрових інструментів що значно розширюють можливості менеджменту. Такі платформи дозволяють здійснювати моніторинг виконання завдань у режимі реального часу, автоматизувати рутинні операції, оптимізувати розподіл ресурсів, а також забезпечують високу якість комунікації між учасниками проєкту. Крім того, у більшості з них наявний інтегрований функціонал для аналітики, прогнозування ризиків та підтримки прийняття рішень. Завдяки цим можливостям системи управління ІТ-проєктами можна розглядати у якості невід'ємної складової ефективного функціонування сучасних ІТ-команд. Коротко розглянемо можливості найбільш відомих систем управління ІТ-проєктами.

Microsoft Project є однією з найбільш поширених систем управління ІТ-проєктами, що поєднує зручний користувацький інтерфейс, відносну простоту у використанні та орієнтацію на користувачів без спеціальної фахової підготовки. Програмний продукт підтримує покрокову розробку ІТ-проєкту, надає інтелектуальні підказки, а також забезпечує гнучкі можливості для створення звітності на основі великої кількості вбудованих шаблонів. Серед функціональних можливостей даного програмного продукту можна виділити інтеграцію з іншими інструментами Microsoft, наявність інструментів для побудови графіків, засобів відстеження ходу реалізації завдань, прогнозування можливих затримок та оцінки термінів виконання проєкту. До обмежень Microsoft Project слід віднести недостатньо розвинену підтримку управління фінансовими, матеріальними та іншими типами ресурсів [1, с. 75], орієнтацію на невеликі ІТ-проєкти. Microsoft Project розповсюджується на платній основі; також доступна ознайомча 30-денна версія.

Open Plan Professional є потужною системою управління ІТ-проєктами, розробленою американською компанією Deltek, Inc. Програмний продукт має розширені можливості у сфері ресурсного та бюджетного планування, що дозволяє йому ефективно формувати моделі проєктів, здійснювати контроль за витратами, аналізувати ризики та одночасно управляти кількома проєктами [3, с. 29]. Завдяки своїй функціональності Open Plan Professional використовується в організаціях, де є потреба у високому рівні деталізації планування та управління. Завдяки можливості управління різними типами ресурсів, здійснення детального вартісного аналізу, наявності гнучких засобів формування звітів із різним рівнем деталізації Open Plan Professional можна вважати універсальним інструментом для проєктного менеджменту.

Серед безкоштовних та умовно безкоштовних онлайн сервісів, що підтримують управління ІТ-проєктами за методологією Agile, слід виокремити KanbanTool, Wrike [4, с. 6] та інші сервіси. Досить популярний сервіс KanbanTool рекомендується використовувати для швидкої організації робочого процесу в малих командах або для індивідуального користування. Він дозволяє створювати цифрові Kanban-дошки з картками, доріжками, мітками та кольоровим маркуванням, за рахунок чого забезпечується висока наочність та ефективний контроль за виконанням завдань. Базова версія даного онлайн інструменту є безкоштовною для двох користувачів і двох дошок. Платні тарифи розширюють функціонал даного онлайн сервісу, зокрема можливість аналітики продуктивності та інтеграцію з іншими корпоративними інструментами.

Більш потужна хмарна платформа Wrike підтримує як класичні, так і гнучкі методології управління. Вона дозволяє створювати завдання та підзадачі, будувати діаграми Ганта, налаштовувати інформаційні панелі, формувати звіти, відстежувати навантаження працівників, здійснювати інтеграцію з популярними сервісами (Google Drive, Microsoft Teams тощо). Безкоштовна версія обмежена командами до 5 користувачів. За умови використання платних тарифів для користувачів відкривається доступ до розширених можливостей, зокрема управління ресурсами, автоматизації робочих процесів і розширеної аналітики.

Доволі популярним онлайн сервісом для управління ІТ-проєктами є система Trello, розроблена компанією Atlassian. Цей інструмент підтримує гнучку методологію Kanban та відрізняється серед інших програмних продуктів можливістю візуалізувати увесь обсяг роботи на одній дошці, що значно спрощує організацію та контроль виконання завдань. Основними перевагами Trello є зручність використання, інтуїтивно зрозумілий інтерфейс та наочне представлення задач у вигляді колонок (списків), що відображають різні етапи проєкту. Для користувачів доступна обмежена безкоштовна версія, яка підходить для індивідуального використання або малих груп. Для професійного застосування пропонуються платні підписки з розширеним функціоналом, що включає аналітику продуктивності, автоматизацію робочих процесів, розширені можливості безпеки та адміністрування.

Отже, системи управління ІТ-проєктами є важливим інструментом для автоматизації управлінських рішень, що допомагають вирішувати прикладні задачі у виробництві, освіті, бізнес-аналітиці тощо. Їх застосування забезпечує автоматизацію процесів, оптимізацію ресурсів, зниження ризиків та підвищення якості результатів. Проведений аналіз підтвердив, що сучасні системи, такі як Microsoft Project, Open Plan, Trello та Agile-інструменти, мають потенціал для комплексного впровадження та здатні підтримувати реалізацію інноваційних проєктів у різних сферах діяльності.

Список використаних джерел:

1. Качан Г. М. Особливості курсу «Управління ІТ-проєктами» в закладах вищої освіти. *Науковий часопис Українського державного*

університету імені Михайла Драгоманова. Серія 2. Комп'ютерно-орієнтовані системи навчання. 2020. № 22(29). С. 73–80.

2. Паращук С. Д., Васильковська Ж. В., Василенко І. М., Щербина О. В. Основи управління ІТ-проектами: принципи, методи та інструменти. *Наука і техніка сьогодні*. 2025. № 5(46). С. 1925–1933.

3. Ткаченко О., Ткаченко К. Огляд сучасних систем управління ІТ-проектами. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2019. № 1(2). С. 27–40.

4. Храпкін О., Кіндрат О., Чопей Р. Управління проектами в ІТ-галузі: методики, інструменти та керування ризиками. *Економіка та суспільство*. 2023. № 55. С. 1–9.

5. Шашкова Н. І., Фадєєва І. Г., Казакова Т. С. Управління проектами в ІТ сфері: застосування гнучких методологій. *Наукові записки Львівського університету бізнесу та права*. 2021. № 28. С. 166–172.

УДК 004.78:331

Шепелев А.В.,

здобувач освіти

Харківський національний університет ім. В.Н.Каразіна,

ННІ «Каразінський банківський інститут»

науковий керівник:

Стяглик Н.І.,

*к.п.н., доцент, завідувачка кафедри інформаційних технологій та
математичного моделювання*

Харківський національний університет ім. В.Н.Каразіна,

ННІ «Каразінський банківський інститут»

ЦИФРОВІ ІНСТРУМЕНТИ УПРАВЛІННЯ ЧАСОМ І ПРОДУКТИВНІСТЮ

Сучасний світ характеризується високою динамікою розвитку та значним інформаційним навантаженням, що ускладнює ефективне використання робочого часу. В умовах багатозадачності та постійних відволікань користувачі часто стикаються з проблемами планування діяльності та об'єктивної оцінки власної продуктивності. Тому актуальним є впровадження цифрових інструментів, які сприяють усвідомленій організації робочого процесу, аналітиці виконаних завдань та виявленню індивідуальних чинників, що впливають на ефективність. Використання таких інструментів дозволяє не лише підвищити результативність, а й вчасно ідентифікувати причини перевантаження або низької продуктивності. Метою цієї роботи є обґрунтування та розробка концепції програмного застосунку, який інтегрує можливості планування задач, управління часом і персональної аналітики продуктивності.

Почнемо з огляду існуючих рішень. На сучасному ринку існує безліч інструментів для тайм-менеджменту та моніторингу продуктивності, таких як Toggl, Clockify, RescueTime, Notion та інші. Більшість з них орієнтується на методології Agile, що включають роботу зі спринтами та регулярне планування завдань; постійне відстеження прогресу через канбан-дошки або таск-трекери; акцент на командній взаємодії та швидкому реагуванні на зміни. Проте, багато існуючих рішень не забезпечують достатньо персоналізовану аналітику, часто обмежені базовими показниками часу та продуктивності, і не завжди підходять для індивідуальних користувачів, які прагнуть глибшого аналізу свого робочого процесу.

Спробуємо обґрунтувати потребу саме цифрового рішення управління проектами з урахуванням часу та продуктивності команди. Ефективне управління часом вимагає інтеграції перевірених методик та сучасних підходів. Поєднання принципів тайм-менеджменту (Pomodoro, Eisenhower Matrix, GTD (Getting Things Done)), інструментів персональної аналітики (облік часу за категоріями, відстеження продуктивності, аналіз історії роботи) та data-driven підходу (збір і обробка даних для виявлення закономірностей і оптимізації діяльності) створює підґрунтя для формування цифрового рішення. Така система забезпечує користувачу не лише можливість ефективного планування задач, але й надає індивідуалізовану аналітику, що сприяє усвідомленому управлінню робочим процесом. Завдяки цьому користувач отримує інструмент, який поєднує планування, контроль та аналіз продуктивності, забезпечуючи прийняття обґрунтованих рішень для підвищення ефективності роботи.

З метою вирішення поставленої проблеми спробуємо окреслити концепцію програмного застосунку. Розроблюваний застосунок може бути реалізований як мобільний додаток, веб-платформа, десктопне рішення або бути крос-платформним. Основна ідея полягає у створенні інструменту, який дозволяє користувачу:

- планувати завдання та визначати пріоритети;
- відстежувати час, витрачений на виконання різних активностей;
- аналізувати власну продуктивність та отримувати рекомендації щодо покращення ефективності.

Застосунок не має бути прив'язаний до конкретної архітектури або технології, що забезпечить його гнучкість і можливість подальшої модифікації.

З огляду на потреби цільової аудиторії, у такому застосунку має бути реалізовано:

- інструменти для планування та структурування робочого часу;
- методи збору та обробки даних про виконання задач;
- персоналізовану аналітику продуктивності та візуалізацію результатів;
- можливості інтеграції з іншими сервісами для підвищення зручності використання.

Таким чином, користувач отримає інструмент, що забезпечує не лише ефективне планування робочого часу, а й формування усвідомленого підходу до власних професійних звичок та їх подальшу оптимізацію.

Спрогнозуємо очікуваний ефект. Впровадження такого застосунку дозволить:

- підвищити продуктивність на індивідуальному та командному рівнях;
- зменшити кількість непродуктивних переривань;
- сформувати більш усвідомлені робочі звички;
- надати користувачу інструмент для самоконтролю і розвитку професійних навичок.

Запропоновану систему можна реалізувати в різних форматах та адаптувати під потреби конкретних користувачів. По-перше, вона здатна ефективно функціонувати як у режимі індивідуального використання, так і в корпоративному середовищі. По-друге, перспективним напрямом є розширення функціоналу: впровадження нових аналітичних модулів, інтеграція з технологіями штучного інтелекту для прогнозування робочого навантаження та автоматичного формування рекомендацій. По-третє, система має високий потенціал до модифікації й подальшого вдосконалення відповідно до розвитку цифрових технологій та змін у професійних практиках користувачів.

Підсумуємо вищезазначене. Концепція програмного застосунку для аналітики робочого часу поєднує інструменти планування задач, управління часом і персональної аналітики продуктивності. Такий підхід відповідає сучасним вимогам до ефективної організації праці та має перспективи розвитку як в індивідуальному, так і корпоративному сегменті. Основна цінність системи полягає у гнучкості, персоналізації та можливості подальшої еволюції, що робить її релевантним рішенням у контексті цифрової трансформації робочих процесів.

Список використаних джерел

1. Agile Alliance. What is Agile? [Електронний ресурс] Режим доступу: <https://agilealliance.org/agile101/12-principles-behind-the-agile-manifesto/>
2. Agile Glossary [Електронний ресурс] Режим доступу: <https://agilealliance.org/agile101/agile-glossary/>
3. Toggl Track Software [Електронний ресурс] Режим доступу: <https://toggl.com/track>
4. Cirillo F. The Pomodoro Technique. – Francesco Cirillo, 2006.
5. Clockify. Time Tracker & Timesheet App [Електронний ресурс] Режим доступу: <https://clockify.me/timekeeping>
6. Allen D. Getting Things Done: The Art of Stress-Free Productivity. – New York : Viking, 2001.

Шишман Т.О.

здобувач вищої освіти,

Маріупольський державний університет, м. Київ

Науковий керівник

Верительник С.М.

доктор філософії з публічного управління та адміністрування,

доцент, доцент кафедри публічного управління та адміністрування

Маріупольський державний університет, м. Київ

ВПРОВАДЖЕННЯ СУЧАСНИХ ІННОВАЦІЙНИХ І ЦИФРОВИХ МЕХАНІЗМІВ БЮДЖЕТНОГО УПРАВЛІННЯ

В умовах сучасних викликів, зокрема дії воєнного стану, цифрові технології виступають важливим інструментом підвищення результативності бюджетного управління в міських громадах. Використання інноваційних підходів сприяє оптимізації бюджетних процесів, забезпечує відкритість та оперативність ухвалення управлінських рішень.

У таблиці 1 подано перелік основних цифрових інноваційних інструментів, які доцільно впровадити в міській громаді для вдосконалення системи бюджетного управління [1;2]. Для кожного інструмента наведено стислий опис функціональних можливостей, очікувані переваги та потенційний вплив на бюджетний процес. Серед них – автоматизація процесів бюджетування, підвищення прозорості через використання порталів відкритих даних, застосування аналітики на основі штучного інтелекту, спрощення податкового адміністрування за допомогою мобільних застосунків, проведення електронних тендерних процедур для закупівель, а також удосконалення системи внутрішнього аудиту.

Автоматизовані системи бюджетного управління (наприклад, платформа «Електронний бюджет» або спеціалізовані ERP-рішення) дозволяють інтегрувати всі етапи бюджетного процесу – від планування до контролю виконання. Такі системи забезпечують централізоване зберігання даних, оперативний доступ до інформації та можливість гнучкого коригування бюджету відповідно до змін, зокрема в умовах воєнного стану.

Портали відкритих даних, наприклад публічні сайти, дають мешканцям громади можливість онлайн переглядати бюджетні показники, звіти про виконання бюджету та інформацію про витрати на соціальні, інфраструктурні та безпекові програми. Це підвищує прозорість управління і сприяє зміцненню довіри між громадою та владою.

Аналітичні платформи з використанням штучного інтелекту та машинного навчання дозволяють обробляти великі обсяги бюджетних даних, прогнозувати ризики й тенденції та моделювати наслідки різних управлінських рішень. Наприклад, такі системи можуть автоматично визначати статті бюджету з найбільшим потенціалом для економії або попереджати про можливі дефіцити [3;4].

Таблиця 1.

Інноваційні цифрові інструменти для управління бюджетом громади

Інструмент	Опис функцій	Очікувані переваги	Потенційний вплив на бюджет
Платформа електронного бюджетування	Автоматизація бюджетного планування, моніторингу, звітності	Швидкий доступ до даних, гнучке коригування бюджету	Підвищення ефективності та прозорості
Портал відкритих даних	Публічний доступ до бюджетної інформації	Прозорість, залучення громади до контролю	Зниження ризиків корупції
Аналітичні системи з ШІ	Прогнозування, виявлення ризиків, аналіз даних	Точніший бюджет, мінімізація дефіцитів	Поліпшення планування
Мобільні додатки для платників	Спрощення сплати податків, нагадування	Збільшення доходів, покращення адміністрування	Зростання надходжень
Електронні тендерні системи	Проведення відкритих закупівель	Зниження вартості, підвищення конкуренції	Економія бюджетних коштів
Системи внутрішнього аудиту	Моніторинг операцій, виявлення аномалій	Зниження ризиків зловживань	Забезпечення цільового використання коштів

Мобільні додатки для платників податків спрощують процес сплати місцевих податків і зборів, забезпечують миттєвий доступ до інформації про податкові зобов'язання, надають електронні квитанції та нагадування. Це підвищує дисципліну платників і сприяє зростанню доходів бюджету, зменшуючи адміністративні бар'єри.

Використання електронних тендерних систем (наприклад, «ProZorro») стимулює конкуренцію серед постачальників, сприяє зниженню вартості закупівель і підвищує якість робіт та послуг, що фінансуються з бюджету громади.

Цифрові інструменти для внутрішнього аудиту та контролю дозволяють автоматично моніторити операції, аналізувати відповідність видатків затвердженому бюджету, виявляти аномалії та потенційні зловживання. Це мінімізує ризики нецільового використання коштів [5;6].

Впровадження таких технологій потребує інвестицій у розвиток ІТ-інфраструктури, підготовку персоналу та забезпечення кібербезпеки. Проте досвід українських громад, що вже застосовують подібні системи, демонструє покращення фінансової дисципліни, зростання доходів і підвищення ефективності використання бюджетних ресурсів.

Отже, цифровізація та впровадження інноваційних інструментів є ключовими чинниками модернізації бюджетного управління в Ірпінській міській громаді. Вони забезпечують оперативне реагування на виклики воєнного часу та формують міцну основу для післявоєнного розвитку.

Список використаних джерел:

1. Місцеві бюджети під час війни: що варто знати? URL: <https://law-in-war.org/misczevi-byudzhety-pid-chas-vijny-shho-varto-znaty/>
2. Місцеві бюджети під час війни: як виконуються та якого законодавства потребують. URL: <https://hromady.org/misczevi-byudzhety-pid-chas-vijni/>
3. Модерні фінанси: глобальні виклики і сучасні тренди. Монографія / за ред. д.е.н., проф. А.І. Крисоватого. Тернопіль: Економічна думка, 2024. 1011 с.
4. Стойка А.В., Верительник С.М., Мацука В.М. Діджиталізація управління проєктами і вплив на світову економіку та інвестиції. Збірник наукових праць «Вчені записки». 2025. № 39(2). С. 45-58. URL: [https://vz.kneu.ua/archive/2025/39\(2\).04](https://vz.kneu.ua/archive/2025/39(2).04)
5. Matsuka V., Horbashevskaya M. Digital technologies in economic management: European trends of development and implementation [2.5]. Європейський досвід використання цифрових технологій в економіці=European experience in the use of digital technologies in the economy: кол. монографія / за ред. А. В. Череп, І. М. Дашко, Ю. О. Огренич та ін. Рига, Латвія: Baltija Publishing, 2025. С. 186–210. URL: <http://repository.mu.edu.ua/jspui/handle/123456789/9278>
6. Matsuka V., Horbashevskaya M. International business strategies of digital transformation of the economy [3.2]. Теоретико-методичні засади використання цифрових технологій в Україні шляхом впровадження досвіду ЄС: кол. монографія / за ред. А.В. Череп, І.М. Дашко, Ю.О. Огренич, О.Г. Череп. Запоріжжя: Вид. ФОП Мокшанов В.В., 2024. С. 132-155. URL: <http://repository.mu.edu.ua/jspui/handle/123456789/8408>

Юженко О.О.

здобувач вищої освіти, ННІ «КБІ» ХНУ імені В.Н. Каразіна

Єрмакова Н.А.

ст.викл. кафедри інформаційних технологій та математичного моделювання

ННІ «КБІ» ХНУ імені В.Н. Каразіна

Mihails Kopeikins,

Mg. art, BIA Design School koordinatoris mākslas jomā, doc., LDS member, Riga,

Latvia

РОЗРОБКА МОБІЛЬНОГО ЗАСТОСУНКУ ECODAILY ДЛЯ ФОРМУВАННЯ ЕКОЛОГІЧНОЇ СВІДОМОСТІ ЗАСОБАМИ ГЕЙМІФІКАЦІЇ

У сучасному світі проблеми екології та сталого розвитку набувають дедалі більшої гостроти. Глобальні зміни клімату, забруднення довкілля та вичерпання природних ресурсів вимагають негайних дій не лише на рівні держав та корпорацій, але й від кожного окремого індивіда. Разом з тим, однією з ключових перешкод на шляху до масового впровадження екологічних звичок є низький рівень мотивації та відсутність чіткого розуміння впливу щоденних дій на довкілля.

Актуальність даної роботи полягає у використанні потенціалу сучасних мобільних технологій та психологічних механізмів гейміфікації для вирішення цієї проблеми. Мобільні застосунки стали невід'ємною частиною життя мільярдів людей, що робить їх ідеальною платформою для поширення знань та формування корисних звичок. Гейміфікація, тобто застосування ігрових елементів у неігровому контексті, доведено підвищує залученість та мотивацію користувачів [1]. Поєднання цих двох підходів дозволяє створити ефективний інструмент для популяризації екологічного способу життя.

Метою роботи є опис розробки та функціональних можливостей мобільного застосунку EcoDaily, призначеного для підвищення екологічної свідомості та заохочення користувачів до щоденних екологічно дружніх дій через систему винагород та відстеження прогресу.

Застосунок EcoDaily розроблено як інтерактивну платформу, що перетворює рутинні екологічні дії на захопливий процес. В основі його концепції лежить принцип позитивного підкріплення: користувач виконує завдання, отримує за це винагороду та бачить свій внесок у збереження довкілля.

Ключовими функціональними компонентами застосунку є:

1. Система щоденних дій. Користувачеві пропонується перелік простих завдань, згрупованих за категоріями: «Енергія», «Вода», «Транспорт», «Відходи», «Їжа» (рис. 1). Прикладами таких дій є:

- Вимкнення електроприладів з розеток (+15 балів).
- Прийняття 5-хвилинного душу (+20 балів).

- Використання громадського транспорту або велосипеда (+25 балів).
- Сортування сміття (+15 балів).
- Вживання їжі рослинного походження (+25 балів).

2. Освітній компонент. Кожна дія супроводжується інформаційною картою, що пояснює її екологічний вплив. Наприклад, при виборі дії «Використовувати громадський транспорт» користувач дізнається, що це допомагає скоротити викиди CO₂ на 4,800 фунтів на рік. Також надаються практичні поради щодо виконання дії («Як це зробити»). Цей підхід не лише мотивує, але й підвищує рівень обізнаності користувачів.

3. Система гейміфікації та відстеження прогресу. За виконання дій користувач отримує бали, які накопичуються на його рахунку. Прогрес візуалізується за допомогою щоденної шкали виконання та статистики, яка включає:

- Загальну кількість балів.
- Кількість днів активності поспіль (Day Streak).
- Середню кількість балів на день.
- Кількість виконаних дій.

Для довгострокової мотивації впроваджено систему рівнів («Еко-початківець», «Зелений воїн») та досягнень («Перший крок», «Тижневий воїн», «Еко-ентузіаст»). Такий підхід створює відчуття змагання та особистого зростання, що є ключовим елементом успішної гейміфікації [2] (рис.1).

4. На сторінці профілю користувач може бачити розбивку зароблених балів за категоріями. Це дозволяє аналізувати, в яких сферах його екологічний внесок є найбільшим, і на які аспекти варто звернути додаткову увагу (рис.1).

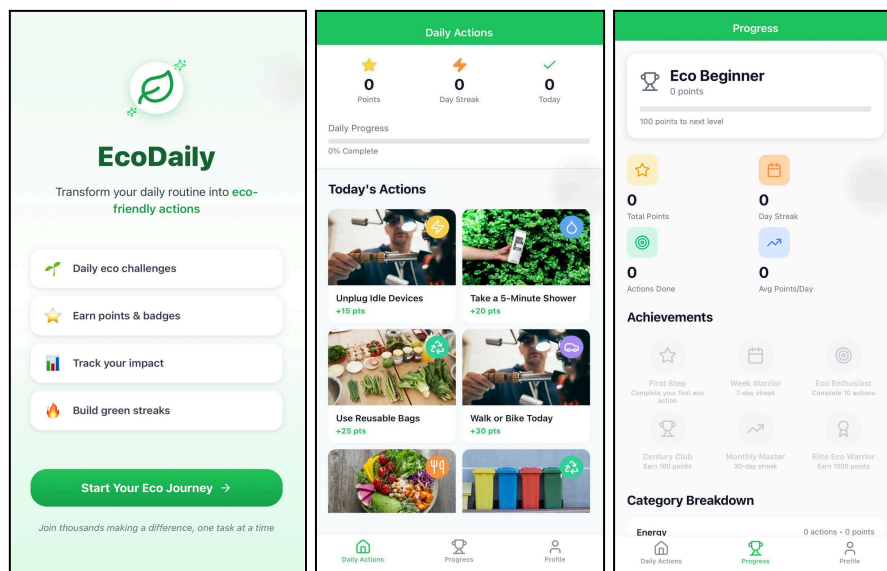


Рисунок 1 - інтерфейс застосунку EcoDaily

Застосунок розроблено з урахуванням сучасних вимог до користувацького досвіду (UX/UI). Інтерфейс є інтуїтивно зрозумілим, мінімалістичним та орієнтованим на швидку взаємодію. Яскрава візуалізація та анімації підсилюють позитивний досвід від користування застосунком.

Концепцію та прототип застосунку EcoDaily було розроблено в межах міжнародної літньої школи «International Summer School Sustainability Thinking and Entrepreneurship». Проект успішно пройшов апробацію серед цільової аудиторії (студенти 17–21 років), отримавши цінний зворотний зв'язок та підтвердивши високу зацікавленість молоді в інтерактивних інструментах для формування екологічних звичок. Завдяки інноваційності та ефективному використанню гейміфікації, проект посів перше місце у фінальному конкурсі стартап-ідей, отримавши високу оцінку експертного журі. Це свідчить про соціальну значущість EcoDaily та його високий потенціал для масштабування на глобальному ринку.

Отже, мобільний застосунок EcoDaily є прикладом успішного поєднання інформаційних технологій, освітнього контенту та ігрових механік для вирішення актуальної соціальної задачі. Він не просто інформує про важливість екологічних дій, а й створює мотиваційне середовище, де кожен крок користувача є частиною більшого процесу збереження планети. Перетворення абстрактних екологічних цілей на конкретні, вимірювані та винагороджувані завдання дозволяє ефективно формувати довгострокові корисні звички.

Перспективи розвитку проекту включають:

- Впровадження соціального функціоналу: можливість додавати друзів, створювати команди, змагатися у рейтингах та ділитися досягненнями в соціальних мережах.
- Розширення бази даних екологічних дій та освітніх матеріалів.
- Інтеграція з календарем та системою сповіщень для нагадування про заплановані дії.
- Партнерство з екологічними організаціями та брендами для надання реальних винагород (знижок на еко-товари) за досягнення у застосунку.

Таким чином, подальший розвиток EcoDaily може перетворити його на комплексну екосистему для людей, що прагнуть жити у гармонії з природою.

Список використаних джерел:

1. Deterding S., Dixon D., Khaled R., Nacke L. From Game Design Elements to Gamefulness: Defining "Gamification". Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments. 2011. P. 9–15. URL: https://www.researchgate.net/publication/230854710_From_Game_Design_Elements_to_Gamefulness_Defining_Gamification (дата звернення: 28.09.2025)
2. Hamari J., Koivisto J., Sarsa H. Does Gamification Work? – A Literature Review of Empirical Studies on Gamification. 2014 47th Hawaii International Conference on System Sciences. 2014. P. 3025–3034. URL: https://www.researchgate.net/publication/256743509_Does_Gamification_Work_-_A_Literature_Review_of_Empirical_Studies_on_Gamification (дата звернення: 28.09.2025)
3. Lo F. Y., Yao Y. C. Promoting Pro-Environmental Behavior: The Role of Gamified Mobile Applications. International Journal of Environmental Research and Public Health. 2021. Vol. 18, № 21. P. 11569. URL:

https://www.researchgate.net/publication/367147565_Gamification_as_a_Learning_Tool_for_Pro-Environmental_Behavior_A_Systematic_Review (дата звернення: 28.09.2025)

ЗМІСТ

РОЗДІЛ 1.

ЗАГРОЗИ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩУ, КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ.....	5
Hart D.O., Pavlina T.V. ANALYSIS OF SOCIAL ENGINEERING ATTACKS IN THE MODERN INFORMATION SPACE AND METHODS OF PREVENTING THEM.....	6
Kviatkivska A. P., Geseleva N.V. INNOVATION AND BUSINESS: MODERN TRENDS.....	8
Nikolaichuk A.I., Kobylin I.O. SYNTACTIC COMPLEXITY AS A FACTOR IN PREDICTION ACCURACY FOR SENTENCE SIMILARITY TASKS IN UKRAINIAN.....	10
Osmanov S.S.O. INFORMATION SECURITY ISSUES.....	13
Аджимян К.О. БЕЗПЕКА ПІД'ЄДНАННЯ ДО КОРПОРАТИВНОЇ МЕРЕЖІ.....	17
Алькова А.М. ЦИФРОВА ФОРЕНЗИКА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У СЕРЕДОВИЩІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.....	19
Андрущенко С.А., Геселева Н.В. МЕТОДИ АНОНІМІЗАЦІЇ ТА ПСЕВДОНІМІЗАЦІЇ У BIG DATA ДЛЯ ЗАХИСТУ ПРИВАТНОСТІ.....	22
Антошук С.А., Стародубцев І.В., Лучик В.Є. ПОРІВНЯННЯ МІЖНАРОДНИХ СТАНДАРТІВ ISO/IEC 27001 ТА NIST У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....	25
Бабчук І.С., Бабчук Л.Р. ЗАГРОЗИ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩУ ХІМІЧНОЇ НАУКИ З БОКУ ЧАТУ GPT.....	28
Бедринський В.П., Будник І.М. ІНВЕСТИЦІЇ В КІБЕРЗАХИСТ ЯК ОСНОВА ЕКОНОМІЧНОЇ КОНКУРЕНТОСПРОМОЖНОСТІ.....	31
Борисова К.Є., Мойко О.О., Макаліш Б.Д. ВИКОРИСТАННЯ ДРОНІВ ЯК ОБ'ЄКТА ТА СУБ'ЄКТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....	34
Ботик М.І., Шкодін І.В. КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ ЧИННИК У ТРАНСФОРМАЦІЇ РІТЕЙЛ-МОДЕЛЕЙ ПІД ВПЛИВОМ ЕЛЕКТРОННОЇ КОМЕРЦІЇ.....	37

Величко С. Ю., Геселева Н.В.	
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК.....	39
Вінічук М.В., Лавриш Софія	
СТАТИСТИЧНІ МЕТОДИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХОДІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ НА ПІДПРИЄМСТВА ІТ-СФЕРИ.....	41
Витковець І.О.	
РОЛЬ І ВАЖЛИВІСТЬ КІБЕРБЕЗПЕКИ.....	44
Гладій А.Л.	
ЗАХИСТ БАНКІВСЬКИХ КАРТОК ВІД КІБЕРЗАГРОЗ.....	47
Гудзь О.Є.	
БЕЗПЕКА ІНФОРМАЦІЙНИХ РЕСУРСІВ У ФІНАНСОВИХ УСТАНОВАХ.	50
Дракон Д.С.	
СУЧАСНІ ПІДХОДИ ДО ЗАХИСТУ ПРОГРАМНИХ ПРОДУКТІВ: ВІД ПОЛІТИК БЕЗПЕКИ ДО ІНСТРУМЕНТІВ АВТОМАТИЗАЦІЇ.....	53
Жилін І.С.	
СУЧАСНІ СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ.....	56
Заріцький О. В.	
КІБЕРСТІЙКІСТЬ БАНКІВСЬКОГО СЕКТОРУ УКРАЇНИ: АНАЛІЗ ФРЕЙМВОРКІВ ТА ПІДХОДІВ.....	58
Ішу В.В., Степанов А.А., Горбань Ю.В.	
CERT: ЇХ ДІЯЛЬНІСТЬ В УКРАЇНІ ТА ІНШИХ КРАЇНАХ.....	63
Кам'янський Я.Б., Лучик В. Є.	
ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ.....	66
Карапетян О.М., Карапетян А.Е.	
АКТУАЛЬНІ ЗАГРОЗИ ТРАНСФОРМАЦІЯМ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА.....	68
Карапетян О.М., Коженювський Ю.В., Рудий Р.В.	
ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ В УМОВАХ ГЛОБАЛЬНИХ ВИКЛИКІВ: ЗАГРОЗИ, КІБЕРБЕЗПЕКА ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ...	71
Кравченко В.В.	
ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СИСТЕМИ ЗАХИЩЕНОГО ЗБЕРІГАННЯ Й ПЕРЕДАВАННЯ ІНФОРМАЦІЇ.....	73
Куліуш Д. О., Мойко О.О., Борисова К. Є.	
ВПЛИВ OSINT-ДАНИХ НА ЕФЕКТИВНІСТЬ ФІШИНГОВИХ АТАК.....	76

Кушніков В. В.	
СПЕЦИФІКА ДОТРИМАННЯ ІНФОРМАЦІЙНОЇ ЕТИКИ В МЕЖАХ ДЕРЖАВНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....	79
Легойда Ю.В.	
ОЦІНКА СТІЙКОСТІ ІОТ-СИСТЕМИ УПРАВЛІННЯ НАСОСОМ ДО DOS-АТАК.....	81
Лєвкіна А.Р., Янчук С.М.	
ЗАХИСТ ІНФОРМАЦІЇ. МЕТОДИ ШИФРУВАННЯ.....	84
Логунов О.С.	
АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ У ВІРТУАЛЬНИХ ТА ДОПОВНЕНИХ СЕРЕДОВИЩАХ (VR/AR).....	86
Лук'яненко С.В.	
НАПРЯМИ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ СИСТЕМИ УПРАВЛІННЯ SMART- БУДИНКОМ.....	88
Лучик В.Є., Маловажна А.Р., Руденко М.А.	
ФЕЙКОВІ НОВИНИ ТА ДЕЗІНФОРМАЦІЯ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ.....	90
Ляшенко А.С., Куліуш Д.О., Мойко О.О.	
КІБЕРБУЛІНГ: МЕХАНІЗМИ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ ПОЛІЦІЇ..	93
Макеєв В. В., Пархоменко О. Ю.	
ЗАХИСТ І ЗБІР ДАНИХ КОРИСТУВАЧІВ У ЦИФРОВІЙ ЕКОНОМІЦІ ЯК ПРОБЛЕМА ПОШУКУ БАЛАНСУ.....	95
Мірошниченко М.Ю.	
ШЛЯХИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ.....	98
Нагірна О.В.	
ІНФОРМАЦІЙНА БЕЗПЕКА ТА ПРОФЕСІЙНИЙ РОЗВИТОК: ВИКЛИКИ Й УПРАВЛІННЯ В СУЧАСНОМУ ОФІСІ.....	101
Наконечна Н.В.	
СТРАХУВАННЯ КІБЕРРИЗИКІВ В УКРАЇНІ.....	104
Новікова Д.Г.	
СТІЙКІСТЬ СУЧАСНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ У КОНТЕКСТІ НОВИХ ЗАГРОЗ.....	107
Новосад А.В., Шинкаренко В.В.	
ВИКОРИСТАННЯ ЕЛЕМЕНТІВ АРТ-ТЕРАПІЇ В УМОВАХ ОСВІТНЬОГО ПРОЦЕСУ ЗДО: ТЕОРЕТИЧНІ ЗАСАДИ, МЕТОДИЧНІ ТА ПРАКТИЧНІ ПІДХОДИ ДЛЯ МАЙБУТНІХ ВИХОВАТЕЛІВ.....	109
Павлюк Р.О.	
КІБЕРГІГІЕНА КОРИСТУВАЧІВ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....	112

Пархоменко О. Ю., Ємельянов С. І.	
ВПЛИВ ДИСБАЛАНСУ КЛАСІВ НА ЕФЕКТИВНІСТЬ МЕТРИК ОЦІНКИ В ЗАДАЧАХ ДЕТЕКЦІЇ ШАХРАЙСТВА З КРЕДИТНИМИ КАРТКАМИ.	114
Пархоменко О. Ю., Морозова Г. С.	
КОНЦЕПЦІЯ ВИЯВЛЕННЯ ЧАСОВИХ АНОМАЛІЙ У ЛОГАХ RFID-СИСТЕМ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ.....	117
Подвальний А. О., Ішу В. В., Мойко О. О.	
АНАЛІЗ ФУНКЦІОНАЛЬНОСТІ НАЙБІЛЬШ ПОПУЛЯРНИХ МЕНЕДЖЕРІВ ПАРОЛЕЙ ДЛЯ ОСОБИСТОГО КОРИСТУВАННЯ.....	120
Поліщук А.В.	
АКТИВНІ МЕТОДИ МОНІТОРИНГУ ДОСТУПНОСТІ МЕРЕЖЕВИХ РЕСУРСІВ У СИСТЕМАХ КІБЕРЗАХИСТУ.....	123
Полякова Є.Р.	
ЦИФРОВІ ДОКАЗИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ: ВИКЛИКИ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ УКРАЇНСЬКОГО ЗАКОНОДАВСТВА В УМОВАХ РОЗВИТКУ КРИПТОВАЛЮТ.....	125
Редзюк Є.В.	
ІНФОРМАЦІЯ ЯК ЕКОНОМІЧНИЙ РЕСУРС У ГЛОБАЛЬНОМУ СВІТІ: ЗАГРОЗИ І ПЕРСПЕКТИВИ РОЗВИТКУ.....	127
Романюк В.І.	
ЗАПРОВАДЖЕННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ В УПРАВЛІННІ БЕЗПЕКОВОЮ СФЕРОЮ.....	130
Руденко Б.В.	
МОДЕЛЬ ZERO TRUST ДЛЯ ІНФОРМАЦІЙНИХ СИСТЕМ У СУЧАСНИХ УМОВАХ КІБЕРЗАГРОЗ.....	133
Самойленко А.Р.	
КІБЕРБЕЗПЕКА В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ У ГІБРИДНИХ КОНФЛІКТАХ ТА ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ.....	136
Світличний В.А., Ковтун І.А.	
СУЧАСНА БОРОТЬБА КІБЕРПОЛІЦІЇ З РОСІЙСЬКОЮ ПРОПАГАНДОЮ..	138
Семенюта В.І.	
МОЖЛИВОСТІ І ЗАГРОЗИ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ.....	141
Спіцина А.О.	
ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА.....	144
Тищенко С. І., Богатєнкова О. Є.	
СТАТИСТИЧНИЙ АНАЛІЗ ВІДМІННОСТЕЙ РОЗПОДІЛІВ ОЗНАК І ЧАСОВИХ ПАТЕРНІВ ШАХРАЙСЬКИХ ТРАНЗАКЦІЙ.....	146

Топалова С.О., Торяник Ж.І., Шевченко В.І.

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ: ЗАГРОЗИ ДЛЯ
ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ТА ОСВІТНІ ЗАСОБИ ПРОТИДІЇ. 149

Тюрєнкова К.В.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: ПРОБЛЕМИ ТА
ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ В УКРАЇНІ..... 154

Ульянченко О.В.

РОЛЬ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ (ШІ)
У СФЕРІ КІБЕРБЕЗПЕКИ..... 156

Філатов О.П.

ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРЗАХИСТ: ГЛОБАЛЬНІ ВИКЛИКИ І
УКРАЇНСЬКИЙ ДОСВІД..... 159

Філатова Л. Д., Фаткулін В. В.

СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА ЛЮДСЬКИЙ ФАКТОР..... 161

Черєдничєнко Б.І.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ДАНИХ: ВІД ПАРОЛІВ ДО
БЕЗПАРОЛЬНИХ ТЕХНОЛОГІЙ..... 163

Шабалтас В.Я., Чеканова Н.М.

МЕТОДИ ОПТИМІЗАЦІЇ В ЗАДАЧАХ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ
ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У СУЧАСНОМУ ІНФОРМАЦІЙНОМУ
СЕРЕДОВИЩІ..... 165

Шутова А.В.

МЕТОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ХМАРНИХ СЕРВІСАХ.
..... 167

Щувайло Д.О.

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ КІБЕРЗАХИСТУ ТА ЯК
ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ..... 169

Яхно Н.Є.

ПРАКТИЧНІ АСПЕКТИ КРИПТОГРАФІЧНОГО ЗАХИСТУ
ПЕРСОНАЛЬНИХ ДАНИХ У ВЕБ-СЕРВІСАХ..... 170

РОЗДІЛ 2.

**ТЕХНІЧНІ СКЛАДОВІ ПРОЄКТУВАННЯ, РОЗРОБКИ,
ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ І
МЕРЕЖ..... 174**

Kravchenko O.O.

METHODS OF FINITE PREDICATE ALGEBRA FOR FORMALIZING
SEMANTIC STRUCTURES OF TEXTS..... 175

Nikolaichuk A.I., Kobylın I.O.

SENSITIVITY OF TRANSFORMER MODELS TO SYNTACTIC
COMPLEXITY LEVELS IN UKRAINIAN SENTENCE SIMILARITY..... 177

Oliinyk Yehor, Korpan Veronika, Zavora Yana	
INFORMATION SYSTEMS AND NETWORKS: TECHNICAL SUPPORT....	180
Skorin Yuriy	
THE PROCESS OF ASSESSING THE CORRUPTION ORIENTATION OF REGULATORY LEGAL ACTS AND ITS MODELING.....	182
Skorin Yuriy, SUN Xiaohai	
AGILE PROJECT MANAGEMENT METHODS.....	185
Skorin Yuriy, Zhao Lina	
AGILE PROJECT MANAGEMENT METHODS BASED ON THE SCRUM METHOD.....	188
Skorin Yuriy, Zhu Zhongbiao	
IMPLEMENTATION OF THE VORONYI DIAGRAM METHOD.....	191
Timokhin Mikhail	
THE ROLE OF ARTIFICIAL INTELLIGENCE IN BUSINESS DECISION MAKING.....	194
Toriansky Zh., Topalova S., Shevchenko V., Kraievyy N.	
THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES AT THE STAGES OF FORMING THE BANK'S MARKETING STRATEGY.....	196
Афанасьев А.С.	
АНАЛІЗ ВПЛИВУ ЯКОСТІ ВЕКТОРИЗАЦІЇ НА ТОЧНІСТЬ КЛАСИФІКАЦІЇ ТЕКСТІВ.....	199
Бур'ян С. С., Погореловська І. Д.	
TELEGRAM-БОТ ЯК ІНСТРУМЕНТ СПРОЩЕННЯ КОМУНІКАЦІЇ ЗІ СЛУЖБОЮ ПІДТРИМКИ.....	201
Гема О.Г.	
КЛАСИФІКАЦІЯ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ ХЕШУВАННЯ.....	204
Зіма В. О.	
ОЦІНКА ЯКОСТІ І ВАЛІДАЦІЯ КРАУДСОРС-РЕПОРТІВ ПРО ПРОБЛЕМИ ДОСТУПНОСТІ МІСЬКОЇ ІНФРАСТРУКТУРИ.....	208
Іванічева С.В., Гладка М.І., Мартишко Є.С.	
ХМАРНІ ТЕХНОЛОГІЇ: ЧОМУ МИ ЗБЕРІГАЄМО ФАЙЛИ В GOOGLE DRIVE ЧИ ICLOUD.....	211
Камишан П.С.	
КОМБІНОВАНИЙ ПІДХІД КОМП'ЮТЕРНОГО ЗОРУ ТА ОПТИЧНОГО РОЗПІЗНАВАННЯ ТЕКСТУ ДЛЯ ПІДВИЩЕННЯ ТОЧНОСТІ ІДЕНТИФІКАЦІЇ ЗОБРАЖЕНЬ.....	214
Ковальчук В.О., Кобилін І.О.	
ЗАСТОСУВАННЯ ML.NET У СЕМАНТИЧНОМУ АНАЛІЗІ МОВЛЕННЄВИХ КОМАНД ДЛЯ ГОЛОСОВИХ АСИСТЕНТІВ.....	217

Максімов І.М., Бондаренко Я.Ю., Бутова Д.О. ДОСЛІДЖЕННЯ ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ОБРОБКИ ПРИРОДНОЇ МОВИ.....	220
Мітла М. О. РОЛЬ ЛІНІЙНОГО ПРОГРАМУВАННЯ У ФОРМУВАННІ МЕТОДІВ ДОСЛІДЖЕННЯ ОПЕРАЦІЙ.....	223
Скорін Юрій РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНОЇ СИСТЕМИ НА БАЗІ ВІРТУАЛЬНИХ КОМП'ЮТЕРНИХ ТРЕНАЖЕРІВ.....	225
Скорін Юрій, Васильєв Ігнат ОПТИМІЗАЦІЯ ПРОЦЕСІВ ПРОЄКТНОГО МЕНЕДЖМЕНТУ.....	228
Скорін Юрій, Кондратьєв Олександр РОЗРОБЛЕННЯ СИСТЕМИ АВТОМАТИЗОВАНОГО АНАЛІЗУ ВІДГУКІВ КОРИСТУВАЧІВ НА ОСНОВІ МЕТОДІВ ПРИРОДНОЇ МОВНОЇ ОБРОБКИ	231
Скорін Юрій, Лактіонов Артем ГІБРИДНІ МЕТОДИ ШИФРУВАННЯ У БЛОКЧЕЙН-МЕРЕЖАХ.....	234
Скорін Юрій, Лук'янчук Софія ШТУЧНИЙ ІНТЕЛЕКТ В СИСТЕМАХ УПРАВЛІННЯ ФІНАНСОВИМИ РИЗИКАМИ.....	238
Скорін Юрій, Петренко Богдан ПРИРОДНА МОВНА ОБРОБКА ДЛЯ АНАЛІЗУ ВІДГУКІВ КОРИСТУВАЧІВ.....	241
Скорін Юрій, Симонович Станислав СИСТЕМА КЕРУВАННЯ ЗМІСТОМ WORDPRESS.....	244
Скорін Юрій, Хусаїнов Микита ПРОГНОЗУВАННЯ ПОПИТУ НА ТУРИСТИЧНІ ПОСЛУГИ ТУРИСТИЧНОГО АГЕНТСТВА.....	247
Філатова Л. Д., Артур Узвеков, Свинаренко А. А. РОЛЬ DBaaS У БІЗНЕС-АНАЛІТИЦІ ТА УПРАВЛІННІ КОРПОРАТИВНИМИ ДАНИМИ.....	251
Шатович Я. В., Геселева Н. В. СУЧАСНІ ПІДХОДИ ДО ОРГАНІЗАЦІЇ БАЗ ДАНИХ: ПОРІВНЯННЯ РЕЛЯЦІЙНИХ ТА НЕРЕЛЯЦІЙНИХ МОДЕЛЕЙ.....	256
Шевченко О.О. ІНСТРУМЕНТИ ВІЗУАЛІЗАЦІЇ ДАНИХ ЯК ЗАСІБ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ.....	258

РОЗДІЛ 3.

ПРОГРАМНІ ЗАСОБИ ДЛЯ ВИРІШЕННЯ ПРИКЛАДНИХ ЗАДАЧ ВИРОБНИЦТВА, ОСВІТИ, БІЗНЕС-АНАЛІТИКИ, ІНТЕЛЕКТУАЛЬНОГО ОБРОБЛЕННЯ ДАНИХ, ПРИЙНЯТТЯ РІШЕНЬ... 261

Bachmaniuk D.O., Dr. Schreibweis M.

AUTOMATED ABC ANALYSIS IN PYTHON: A PRACTICAL
IMPLEMENTATION WITH OPPORTUNITIES FOR LINEAR
PROGRAMMING INTEGRATION..... 262

Bondar Sofiia

SILENT VIDEOS IN ENGLISH LANGUAGE TEACHING: TASKS FOR
YOUNG LEARNERS' SPEAKING AND STORYTELLING.....266

Kapatsyn Alona

PODCASTS IN ENGLISH LANGUGUAGE TEACHING: NEW
OPPORTUNITIES FOR LISTENING, PRONUNICATION AND CLASSROOM
TASKS.....269

Krasovska Anastasiia

AI IN EDUCATION: BENEFITS, LIMITATIONS, AND CORE FUNCTIONS.....
..... 271

Kushnierov Andriy

AUTHENTIC MEDIA IN TEACHING ENGLISH: VIDEO AND PODCAST. 273

Lubko D.V., Motornyi Dmytro

THE USE OF MODERN INTERACTIVE INFORMATION SYSTEMS IN
TEACHING THE DISCIPLINE "COMPUTERS AND COMPUTER
TECHNOLOGIES" FOR 1ST YEAR UNIVERSITY STUDENTS..... 275

Lysenko D. O.

METRICS FOR EVALUATING MACHINE TRANSLATION BASED ON
VECTOR -BASED REPRESENTATIONS..... 278

Mazepa A.S.

DYNAMIC DECISION SUPPORT SYSTEM WITH MULTI-AGENT
ORCHESTRATION FOR RISK MANAGEMENT IN SOFTWARE PROJECTS...
..... 281

Oliinyk M.V.

USING ARTIFICIAL INTELLIGENCE AND BIG DATA ANALYTICS TO
PREDICT CONFLICTS.....283

Onyshchenko Iryna

BALANCING TRADITIONAL EXAMS AND ALTERNATIVE ASSESSMENT
IN ONLINE EDUCATION..... 286

Postol Yulia	
TIKTOK AS A LANGUAGE LEARNING TOOL: PRONUNCIATION AND COMMUNICATION PRACTICE.....	289
Repchonok S.A.	
PROMISING NETWORK TECHNOLOGIES IN THE DEVELOPMENT OF INFORMATION INFRASTRUCTURE.....	291
Skorin Yuriy	
APPLYING ARTIFICIAL INTELLIGENCE TECHNIQUES TO CREATE TYPICAL WEB APPLICATIONS.....	293
Skorin Yuriy	
APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS FOR ENTERPRISE OPERATIONAL RISK MANAGEMENT.....	296
Skorin Yuriy	
FORECASTING THE ECONOMIC ACTIVITY OF A TRADING ENTERPRISE USING WEB TECHNOLOGIES.....	298
Skorin Yuriy	
INTRODUCTION OF FORECASTING METHODS DURING THE EXECUTION OF LONG-TERM TRADE OPERATIONS OF THE ENTERPRISE.....	301
Skorin Yuriy	
METHOD OF RATING ASSESSMENTS OF TOOLS FOR CREATING WEB APPLICATIONS.....	303
Suprun Anna	
A COMBINED METHOD FOR LEVERAGING LARGE LANGUAGE MODELS IN THE ANALYSIS AND GENERATION OF CREATIVE TEXTS.....	306
Temnikov G.E.	
DESIGNING APPLICATIONS FOR PROCESSING AND ANALYZING LARGE AMOUNTS OF DATA (BIG DATA) IN DISTRIBUTED SYSTEMS.	309
Verhun Sofia	
INTEGRATING SONGS, MEMES, AND VIRAL VIDEOS INTO ENGLISH TEACHING.....	312
Kolesnychenko K. M.	
SOFTWARE TOOLS FOR ENHANCING EFFICIENCY IN COMPUTER SCIENCE.....	315
Астаф'єва К.Ю.	
ВИКЛИКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ В УКРАЇНСЬКОМУ БІЗНЕСІ ТА МОЖЛИВІ РІШЕННЯ.....	318

Білоцерківська В.А.	
МЕТОДИ ЗБОРУ ТА ПОПЕРЕДНЬОЇ ОБРОБКИ ДАНИХ ВАКАНСІЙ ДЛЯ ПОДАЛЬШОГО МАШИННОГО АНАЛІЗУ	320
Бобейко К.С., Кобилін О.А.	
ІНТЕЛЕКТУАЛЬНІ ПРОГРАМНІ ЗАСОБИ ДЛЯ ЕНЕРГОЗБЕРЕЖЕННЯ В ЖИТЛОВОМУ СЕКТОРІ.....	322
Богдан Н.І.	
ПОРІВНЯЛЬНИЙ АНАЛІЗ АРХІТЕКТУРНИХ РІШЕНЬ ДЛЯ ІНТЕГРАЦІЇ ДОВГОТРИВАЛОЇ ПАМ'ЯТІ У ДІАЛОВОЇ СИСТЕМІ.....	325
Бойко М.К.	
МЕТОД БАГАТОВИМІРНОГО АНАЛІЗУ ЕФЕКТИВНОСТІ РЕКЛАМНИХ КАМПАНІЙ З АДАПТИВНИМ МОНІТОРИНГОМ.....	327
Бондаренко А. Є.	
АНАЛІЗ МІЖНАРОДНИХ РИНКІВ ДЛЯ ОПТИМІЗАЦІЇ ПОСТАЧАВАННЯ.....	329
Будник В.І.	
ПЕРСПЕКТИВИ ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ В ОБЛІКУ ЦИФРОВИХ АКТИВІВ.....	332
Веприцький А.В.	
СИСТЕМИ БІЗНЕС-АНАЛІТИКИ ТА МАШИННЕ НАВЧАННЯ: СУЧАСНІ РІШЕННЯ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ.....	335
Вигоднер І.В., Полозова С.Є.	
РОЗВ'ЯЗУВАННЯ ОПТИМІЗАЦІЙНИХ ЗАДАЧ ЗА ДОПОМОГОЮ ТАБЛИЧНОГО ПРОЦЕСОРУ EXCEL.....	337
Власов І.В., Томашук І.В.	
ІННОВАЦІЇ У РОЗВИТКУ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ ЯК ФАКТОР ЕКОНОМІЧНОГО ЗРОСТАННЯ.....	340
Галчанська В.В.	
ПЕРЕВАГИ ІНФОРМАЦІЙНИХ СИСТЕМ В КОНТЕКСТІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА.....	343
Глушко Р. О.	
ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА РОЗВИТОК ФІНАНСОВИХ ТЕХНОЛОГІЙ.....	345
Гончарук Д.О., Заїченко Ю.П.	
ОСВІТНІ ПЛАТФОРМИ ТА ЗАСТОСУНКИ НОВОГО ПОКОЛІННЯ.....	348
Григоров Г.А.	
ЦИФРОВА ТРАНСФОРМАЦІЯ ОСВІТИ КРІЗЬ ПРИЗМУ ШТУЧНОГО ІНТЕЛЕКТУ	350

Гуржій К. А.	
ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПРОГРАМНИХ ЗАСОБІВ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ ВЕБ-ЗАСТОСУНКІВ.....	353
Денисенко Г.В., Стяглик Н.І.	
ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ.....	356
Ємельяненко Г.Д.	
ФІЛОСОФІЯ ОСВІТИ І НАУКИ В УМОВАХ ЦИФРОВІЗАЦІЇ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ.....	358
Захарова М.Д.	
SOFTWARE4LIFE: ВИРОБНИЦТВО, НАВЧАННЯ, АНАЛІТИКА.....	359
Істомін А. О.	
ЦИФРОВІЗАЦІЯ БУДІВЕЛЬНИХ ПРОЦЕСІВ: РОЛЬ SAAS-РІШЕНЬ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ПРОЄКТАМИ.....	363
Кірічек К.Т., Єрмакова Н.А.	
МІЖДИСЦИПЛІНАРНІ ЗВ'ЯЗКИ: ЯК ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІНТЕГРУЮТЬСЯ В НАВЧАЛЬНІ ДИСЦИПЛІНИ І КУРСУ.....	366
Ключніков О.С., Кобилін І.О.	
МЕТОДИ ВИКОРИСТАННЯ ТА ПРОТИДІЯ ШАХРАЙСЬКИМ ПРОГРАМАМ У КОМП'ЮТЕРНИХ ІГРАХ ТИПУ «ШУТЕР».....	368
Коваленко К. А.	
МОДЕЛІ ТА ПРОГРАМНІ ІНСТРУМЕНТИ ЛІНІЙНОГО ТА НЕЛІНІЙНОГО ПРОГРАМУВАННЯ.....	372
Коваленко Ю. О.	
РОЛЬ ЦИФРОВИХ КОМУНІКАЦІЙНИХ ІНСТРУМЕНТІВ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ РОБОТИ КОМПАНІЙ.....	374
Коваль Н.А., Томашук І.В.	
ІННОВАЦІЇ ЯК ЧИННИК ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ТА ЕФЕКТИВНОСТІ АГРАРНИХ ПІДПРИЄМСТВ.....	376
Коваль О.Т.	
ЗАЛЕЖНІСТЬ ЯКОСТІ ПЗ ДЛЯ ВИЯВЛЕННЯ ВТОРГНЕНЬ У МЕРЕЖІ ВІД МЕТОДІВ ВИБОРУ ОЗНАК У МОДЕЛЯХ ML.....	380
Ковальський А.А.	
БІБЛІОТЕКА МАНІМ ЯК ІНСТРУМЕНТ ДЛЯ АНІМАЦІЇ ВЕКТОРНИХ ПОЛІВ У ОСВІТНЬОМУ ПРОЦЕСІ.....	383
Колісниченко М.В.	
ВИКОРИСТАННЯ РІВНІВ ДЕТАЛІЗАЦІЇ (LOD) У МЕРЕЖЕВИХ ІГРАХ ДЛЯ ЗНИЖЕННЯ НАВАНТАЖЕННЯ.....	385

Корепанов І.С. PYTHON ТА JUPYTER NOTEBOOK ЯК ІНСТРУМЕНТИ ДЛЯ РОЗВИТКУ STEM-ОСВІТИ.....	387
Косовський С.Б. ВИКОРИСТАННЯ ІГРОВОГО РУШІЮ UNITY ДЛЯ СТВОРЕННЯ AR ТА VR ОСВІТНЬО-ІГРОВИХ ПРОГРАМ.....	389
Кулалаєв Н. А. ДОСЛІДЖЕННЯ ВПЛИВУ ГНУЧКИХ МЕТОДОЛОГІЙ НА ЕФЕКТИВНІСТЬ ПРОЦЕСУ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	392
Лапченко І. В. ВИСОКОДОСТУПНА АРХІТЕКТУРА МІКРОСЕРВІСІВ У KUBERNETES...	395
Лебідь О.В. ІНДУСТРІАЛЬНІ ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ: АКТУАЛЬНІ ТРЕНДИ ТА ПЕРЕХІД ДО AUTOML У МАСШТАБАХ 2025 – 2030 РОКІВ.....	397
Макарова Г.В., Артемчук А.В. РОЗРОБКА ТА ДОСЛІДЖЕННЯ TELEGRAM-БОТА ДЛЯ ОРГАНІЗАЦІЇ СПОРТИВНИХ ЗАХОДІВ.....	400
Макарова Г.В., Орешко Д.В. ІНТЕЛЕКТУАЛЬНИЙ МОБІЛЬНИЙ ЗАСТОСУНОК ДЛЯ АДАПТИВНИХ ТРЕНУВАНЬ.....	401
Макарова Г.В., Пархоменко О.А. ВИКОРИСТАННЯ СУЧАСНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ У СФЕРІ ОСВІТИ І НАУКИ.....	403
Маніта А.С., Томашук І.В. ВПЛИВ ІННОВАЦІЙ НА ІНВЕСТИЦІЙНУ ПРИВАБЛИВІСТЬ РЕГІОНІВ УКРАЇНИ.....	405
Матвеев Є. Е. ВИКОРИСТАННЯ ТЕХНОЛОГІЇ FACE ID ДЛЯ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ.....	409
Мостова Г.Г. ВПРОВАДЖЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ТА УДОСКОНАЛЕННЯ СИСТЕМ КОНТРОЛЮ І МОНІТОРИНГУ У СФЕРІ ВИКОНАННЯ СУДОВИХ РІШЕНЬ.....	412
Ніжегородцев В.О. АНАЛІЗ ЦИФРОВИХ ТЕХНІЧНИХ РІШЕНЬ З МОНІТОРИНГУ СИСТЕМ КОМУНАЛЬНИХ ВИТРАТ.....	415

Ніколайчук С. Ю.	
ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ ДЛЯ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ У ЗАКЛАДАХ ПРОФЕСІЙНОЇ ОСВІТИ.....	417
Олійник Є.С., Томашук І.В.	
ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ВПРОВАДЖЕННЯ ІННОВАЦІЙ НА ПІДПРИЄМСТВАХ АГРАРНОГО СЕКТОРУ.....	420
Павленко Р. О.	
ПРОБЛЕМИ РОЗРОБКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ПІДТРИМКИ ПРОЦЕСУ РОЗПІЗНАВАННЯ ХІМРЕАКТИВІВ.....	422
Петріщев Д. А.	
БРЕЙНСТОРМ З LLM У БІЗНЕС-АНАЛІЗІ: КОРИСТЬ, РИЗИКИ ТА ПРАКТИЧНІ КЕЙСИ.....	424
Пилипенко А. О.	
ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ДОСЛІДЖЕННІ МІЖНАРОДНИХ РИНКІВ.....	426
Підлужний П.А.	
ВИКЛИКИ ПРИ ІНТЕГРАЦІЇ LLM У БІЗНЕС ПРОЦЕСИ.....	430
Плотніков Д.А.	
РОЗРОБКА ТА ВПРОВАДЖЕННЯ WEB APP ДЛЯ ІНТЕГРАЦІЇ БІЗНЕС-ПРОЦЕСІВ ЗАЛУЧЕННЯ ГОТІВКОВИХ ТА БЕЗГОТІВКОВИХ ТРАНЗАКЦІЙ.....	432
Половян Н.С.	
ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОГО ПРОФЕСІЙНОГО РОЗВИТКУ ПРАЦІВНИКІВ СФЕРИ ОХОРОНИ ЗДОРОВ'Я.....	434
Половян О.О., Лобас В.М.	
ЦИФРОВІЗАЦІЯ СИСТЕМИ БЕЗПЕРЕРВНОГО ПРОФЕСІЙНОГО РОЗВИТКУ В УКРАЇНІ.....	437
Проненко С.С.	
ІНФОРМАЦІЙНІ СИСТЕМИ В ГЕОДЕЗІЇ ТА ЗЕМЛЕУСТРОЇ.....	440
Проценко Н.М.	
ІНТЕЛЕКТУАЛЬНА ОБРОБКА ДАНИХ ТА ХМАРНІ ТЕХНОЛОГІЇ: СТРАТЕГІЇ ВПРОВАДЖЕННЯ НА ПІДПРИЄМСТВІ.....	442
Проценко П.Р.	
АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ДЛЯ ОПТИМІЗАЦІЇ УПРАВЛІННЯ БІЗНЕС-ПРОЦЕСАМИ БАГАТОПРОФІЛЬНИХ ПІДПРИЄМСТВ.....	445
Рава А.В., Лупан І.В.	
РОЗРОБКА ДИЗАЙНУ ДАШБОРДУ ДЛЯ ВІЗУАЛІЗАЦІЇ ВІДКРИТИХ ДАНИХ ЄДЕБО.....	447

Савченко С.В.	
ВИКОРИСТАННЯ СНАТГРТ ТА ШТУЧНОГО ІНТЕЛЕКТУ У НАВЧАННІ: МОЖЛИВОСТІ, ПЕРЕВАГИ ТА РИЗИКИ.....	450
Сазонов В.О.	
РЕКОМЕНДАЦІЙНІ ПІДСИСТЕМИ ПЕРЕГЛЯДУ СЕРІАЛІВ ЯК СКЛАДОВА СУЧАСНИХ ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНИХ СИСТЕМ.....	453
Салтиков Б. Г.	
VR/AR ТЕХНОЛОГІЇ: НОВА ЕРА ПРОФЕСІЙНОГО НАВЧАННЯ.....	456
Семикрас Д.О.	
АНАЛІЗ ДАНИХ ТА МОДЕЛЮВАННЯ ІНСТРУМЕНТІВ ЗБОРУ ІНФОРМАЦІЇ У СИСТЕМАХ ГУМАНІТАРНОГО РЕАГУВАННЯ.....	459
Сіденко А. С.	
ПРОБЛЕМИ РОЗРОБКИ ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ ДЛЯ РЕЄСТРАЦІЇ ДАНИХ ВІДХОДІВ ВІД РУЙНУВАНЬ.....	461
Смірнов О.С., Тимошенко Юлія	
ДОСЛІДЖЕННЯ МЕТОДІВ І АЛГОРИТМІВ ОПТИМАЛЬНОГО КОДУВАННЯ ТА СТИСНЕННЯ ДАНИХ У КОМП'ЮТЕРНИХ СИСТЕМАХ.....	463
Стяглик Н.І., Žilinskis Vjačeslavs	
АЛГОРИТМІЧНІ АСПЕКТИ ВИКОРИСТАННЯ ДЕРЕВ ТА ГРАФІВ У ЗАДАЧАХ БІЗНЕС-АНАЛІТИКИ.....	465
Суровикін Ю.В.	
МЕТОД ПРОГНОЗУВАННЯ ПОПУЛЯРНОСТІ АРТИСТІВ НА ОСНОВІ КОМБІНОВАНИХ СТАТИСТИЧНИХ МЕТРИК ТА ФАКТОРІВ КОЛАБОРАЦІЙ.....	468
Тарасюк М.В.	
PROCESS MINING ЯК ІНСТРУМЕНТ ОПТИМІЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ У МАРКЕТИНГОВІЙ ДІЯЛЬНОСТІ.....	470
Терещенко А.С., Ніжегородцев В.О.	
ЕТИЧНІ АСПЕКТИ ТА РИЗИКИ ШТУЧНОГО ІНТЕЛЕКТУ: ВИКЛИКИ СУЧАСНОГО ЦИФРОВОГО СУСПІЛЬСТВА.....	473
Терещенко С.С.	
АВТОМАТИЗАЦІЯ ПРОЦЕСІВ СУПРОВОДЖЕННЯ ДІЯЛЬНОСТІ СУМСЬКОЇ БІЗНЕС-ШКОЛИ.....	475
Тигач Г.Г.	
РОЛЬ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ДАНИХ У ПРОЦЕСІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УПРАВЛІННЯ БІЗНЕСОМ.....	478
Ткаченко О. С., Цоколенко А. С.	
РОЗРОБКА АСИСТЕНТА ДЛЯ ДІАГНОСТИКИ ЗАХВОРЮВАНЬ.....	480

Уткін Євгеній	
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ RAG ЯК ОДНА ІЗ СТРАТЕГІЙ ПОКРАЩЕННЯ РОБОТИ LLM СИСТЕМ.....	482
Хомсі Как С.М.	
МЕТОДИ ДІАГНОСТИКИ СТАНУ СОНЯЧНИХ ПАНЕЛЕЙ ЗА ДОПОМОГОЮ КОМП'ЮТЕРНОГО ЗОРУ.....	484
Хом'як А.В.	
ТЕХНОЛОГІЯ BLOCKCHAIN ТА ЇЇ ЗАСТОСУВАННЯ.....	486
Чалій К.Р.	
ВІРТУАЛЬНА ЛАБОРАТОРІЯ НА ОСНОВІ ГЕНЕРАТИВНОГО ШІ.....	489
Чистохін О.Ю.	
ДОСЛІДЖЕННЯ ВПЛИВУ ГНУЧКИХ МЕТОДОЛОГІЙ НА ЕФЕКТИВНІСТЬ ПРОЦЕСУ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	492
Чорненька С.В.	
РОЗВИТОК ІНТЕЛЕКТУАЛЬНИХ ПРОГРАМНИХ СИСТЕМ ДЛЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ВИРОБНИЧИХ, ОСВІТНІХ ТА БІЗНЕС-ПРОЦЕСІВ.....	494
Шаров С.В.	
СИСТЕМИ УПРАВЛІННЯ ІТ-ПРОЄКТАМИ ЯК СУЧАСНИЙ ПІДХІД ДО АВТОМАТИЗАЦІЇ УПРАВЛІНСЬКИХ РІШЕНЬ.....	496
Шепелев А.В.	
ЦИФРОВІ ІНСТРУМЕНТИ УПРАВЛІННЯ ЧАСОМ І ПРОДУКТИВНІСТЮ..	499
Шишман Т.О.	
ВПРОВАДЖЕННЯ СУЧАСНИХ ІННОВАЦІЙНИХ І ЦИФРОВИХ МЕХАНІЗМІВ БЮДЖЕТНОГО УПРАВЛІННЯ.....	502
Юженко О.О., Єрмакова Н.А., Mihails Kopeikins	
РОЗРОБКА МОБІЛЬНОГО ЗАСТОСУНКУ ECODAILY ДЛЯ ФОРМУВАННЯ ЕКОЛОГІЧНОЇ СВІДОМОСТІ ЗАСОБАМИ ГЕЙМІФІКАЦІЇ.....	505

Електронне наукове видання
комбінованого використання
Можна використовувати в локальному та мережному режимах

ІТ-ПРОСТІР СЬОГОДЕННЯ: ТЕНДЕНЦІЇ, ІННОВАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Збірник тез доповідей
II Міжнародної науково-практичної студентської конференції

(15 жовтня 2025 року, м. Харків, Україна)

Матеріали подаються в авторській редакції

Формат 60×84/8. Гарнітура Таймс.
Обл.-вид. арк 26,73 Умовн. друк. арк. 21,38

Системні вимоги:
Процесор Pentium-класа; ОС Windows 7/10;
дисковод CD-ROM; Acrobat Reader 10.
Об'єм даних 16,8 Мб. Замовлення № 561/25.

Харківський національний університет імені В. Н. Каразіна,
м. Харків, 61022, майдан Свободи, 4.
Свідоцтво суб'єкта видавничої справи ДК No 3367 від 13.01.2009 р.