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

Проєкт збірника конференції

ІТ-ПРОСТІР СЬОГОДЕННЯ: ТЕНДЕНЦІЇ, ІННОВАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Збірник тез доповідей
Всеукраїнської науково-практичної студентської конференції

(16 жовтня 2024 року, м. Харків, Україна)

Електронний ресурс

Харків – 2024

УДК 338.46:004](063)
І-70

Реєстраційне посвідчення УкрІНТЕІ МОН України
(№ 551 від 07 грудня 2023 р.)

Затверджено до розміщення в мережі Інтернет рішенням Вченої ради
Харківського національного університету імені В. Н. Каразіна
(протокол №___ від _____ 2024 р.)

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

І-70 ІТ-простір сьогодення: тенденції, інновації та перспективи розвитку: збірник тез доповідей Всеукраїнської науково-практичної студентської конференції (16 жовтня 2024 року, м. Харків, Україна) [Електронний ресурс]. – Харків : ХНУ імені В. Н. Каразіна, 2024. – 1 ел. опт. диск (CD-ROM). – Систем. вимоги: Процесор Pentium-класса ; ОС Windows 7/10 ; дисковод CD-ROM; Acrobat Reader 10. – 236 с.

ISBN _____

У збірнику представлені тези доповідей учасників Всеукраїнської 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.

УДК 338.46:004](063)

URI: _____

© Харківський національний
університет імені В. Н. Каразіна, 2024

ISBN _____

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 All-Ukrainian Scientific and Practical
Student Conference

(October 16, 2024, Kharkiv, Ukraine)

Electronic resource

Kharkiv – 2024

UDC 338.46:004](063)

I-70

Registration certificate of UkrINTEI of the Ministry of Education and Science of Ukraine
(No. 551 dated December 07, 2023)

Approved for publication on the Internet by the decision of the Academic Council of V. N. Karazin Kharkiv National University
(Minutes № ___ dated _____ 2024)

Editorial board address:
4 Svobody Square, Kharkiv, 61022, Ukraine

I-70 IT space of today: trends, innovations and development prospects: a collection of abstracts of the All-Ukrainian Scientific and Practical Student Conference (October 16, 2024, Kharkiv, Ukraine) [Electronic resource]: V. N. Karazin Kharkiv National University, 2024. 1 electronic disk (CD-ROM). – System requirements: Pentium-class processor; OC Windows 7/10; CD-ROM drive; Acrobat Reader 10. 236 p.

ISBN _____

The collection presents abstracts of the participants of the All-Ukrainian 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.

UDC 338.46:004](063)

URL: _____

ISBN _____

РОЗДІЛ 1.

ЗАГРОЗИ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩУ, КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

UDC 004.056

Drakon D.S.
ERI "Karazin Banking Institute"
V.N Karazin Kharkiv National University
Scientific advisor:
Stiahlyk N.I.
Ph.D., Head of the Department of Information Technology and Mathematical Modeling
Karazin Banking Institute, V.N. Karazin Kharkiv National University

PROTECTION OF CRITICAL INFRASTRUCTURE FROM CYBERATTACKS: MODERN CHALLENGES AND SOLUTIONS

Protection of critical infrastructure (CI) amid growing cyber threats is one of the most significant challenges of our time. CI encompasses key sectors such as energy, transport, finance, water supply, communications, and healthcare, all of which are crucial for a nation's stability. Cyber threats can lead to severe social, economic, and political consequences. This issue is particularly relevant for Ukraine, which has been under constant cyberattacks aimed at destabilizing its critical infrastructure since 2014.

The 2015 cyberattack on Ukraine’s power grid was the first large-scale example of such actions. However, in 2022–2024, the threat significantly escalated as cyberattacks became systematic and coordinated with physical assaults during the full-scale Russian invasion, causing serious damage to the country’s energy, financial, and telecommunications sectors. In these circumstances, cyber threats have become an integral part of hybrid warfare.

One of the key challenges in protecting critical infrastructure is the difficulty in identifying attackers and their methods. Modern cyberattacks are often carried out through complex, multi-phase strategies, such as advanced persistent threat (APT) attacks, which exploit zero-day vulnerabilities and malware that can remain undetected for extended periods. This allows attackers not only to penetrate systems but also to gather information or prepare for large-scale destructive attacks.

The constant modernization of attack methods by organized cyber groups, often state-sponsored, poses additional challenges. Ukraine faces systematic attacks from cyber structures funded and directed by foreign governments. Attacks on energy systems, banking structures, and telecommunications during the 2022 military actions demonstrated that cyberattacks are coordinated with physical strikes, further exacerbating threats to the country’s security.

Another significant issue is the inadequate preparedness of many critical infrastructure facilities to effectively counter cyberattacks. Many enterprises in Ukraine lack the resources to implement modern cybersecurity technologies and suffer from a shortage of qualified cybersecurity specialists, increasing the risk of successful attacks.

To enhance the protection of critical infrastructure, strategic solutions must be implemented. Legislative modernization and regulatory updates are key. Ukraine has passed important laws, including the 2017 “Law on the Basic Principles of Cybersecurity of Ukraine,” which regulates interaction between government bodies, the private sector, and international partners. However, the legislation needs constant updates to keep pace with the rapid development of new threats. Mandatory cybersecurity standards must be introduced for private companies managing critical infrastructure, along with ensuring state-level oversight of their compliance.

International cooperation and knowledge exchange are vital. Ukraine actively collaborates with NATO, the EU, and the United States to strengthen its cybersecurity. Participation in cyber drills, such as "Cyber Coalition," enhances preparedness for cyberattacks and allows Ukraine to adapt international best practices to its own reality. Integration into global platforms for sharing information on cyberattacks and vulnerabilities, such as CERT and MISP, promotes faster responses to new threats and better coordination of defense efforts globally.

The adoption of modern protection technologies is also critical. Advanced technologies play a key role in cybersecurity for critical infrastructure. Effective strategies include deploying early warning systems for cyberattacks that rely on network traffic analysis using artificial intelligence and machine learning. Network segmentation, isolated segments with controlled access, multi-factor authentication, hardware encryption, and Zero Trust models significantly enhance security.

Training personnel and improving cyber literacy are essential components of effective defense. The shortage of cybersecurity professionals is a global problem, and Ukraine is no exception. The solution lies in improving education in higher institutions and providing ongoing training for specialists already working in the field. Regular drills and cyberattack simulations improve the readiness of professionals to handle real threats. Establishing a cyber reserve could help mobilize additional resources during large-scale attacks. Raising cyber literacy among the leadership of enterprises responsible for critical infrastructure is also crucial, as management decisions play a key role in implementing protective measures.

In addition, it is essential to focus on raising public awareness and cyber hygiene at all levels of society. The increasing reliance on digital infrastructure means that even individuals and small organizations can become entry points for larger cyberattacks, particularly through social engineering, phishing schemes, or compromised devices. Promoting awareness of basic cybersecurity practices, such as password management, recognizing phishing attempts, and safeguarding sensitive data, can significantly reduce the success rate of attacks. This requires joint efforts from both the government and private sectors to educate citizens and ensure that cybersecurity is a shared responsibility across society.

Coordination between the public and private sectors is essential for effective protection. Mechanisms for the rapid exchange of information about threats and responses to incidents need to be established. While Ukraine has several platforms for this, their efficiency can be improved by streamlining coordination procedures and reducing bureaucratic barriers for the private sector. Developing partnerships between

the state and private companies in cybersecurity research and development will foster innovative solutions that address the specific challenges of Ukraine's cyber landscape.

Ukraine has become a testing ground for cutting-edge cyberattacks on critical infrastructure, spurring the development of innovative cybersecurity solutions. Alongside state efforts, volunteer initiatives, cooperation with private companies, and international partners play a crucial role in strengthening defense. During the war, particularly after the 2022 Russian invasion, volunteer cyber initiatives have become a critical element of Ukraine’s defense in the digital space. A prime example is Ukraine’s IT Army, which mobilized thousands of volunteers to launch cyberattacks on enemy resources and defend Ukrainian systems. Supported by government structures, the IT Army coordinates efforts to counter cyber threats and conducts operations to collect information and disrupt enemy networks.

Since the 2015 power grid attack, energy companies have implemented serious measures to boost cybersecurity. Network traffic monitoring systems and tools for detecting anomalous activity have been introduced. Some companies are working with international leaders such as IBM and Cisco to develop specialized solutions.

Ukraine actively cooperates with international partners to strengthen critical infrastructure protection. In 2022, the EU and the U.S. provided significant assistance in cybersecurity, including equipment, training, and resources. Cooperation programs with NATO have enabled Ukrainian specialists to participate in training aimed at defending critical facilities against complex multi-phase attacks.

Private Ukrainian companies also play an important role in bolstering cybersecurity. IT companies develop innovative solutions for network monitoring and protection, while banks implement multi-factor authentication systems and data encryption. Cooperation between the state and private sectors in sharing threat information allows for better coordination of efforts to swiftly respond to incidents.

The protection of critical infrastructure is a key element of Ukraine's national security amid modern cyberattacks and hybrid warfare. The main priorities should include improving legislation, adopting cutting-edge cybersecurity technologies, and enhancing international cooperation. The successful experience of Ukraine’s IT Army and international assistance demonstrates the importance of collective efforts in countering threats. Systematic steps are needed to protect critical facilities effectively, including developing cybersecurity personnel and raising awareness. Only a comprehensive approach combining technological, organizational, and human resources can ensure the resilience of Ukraine's critical infrastructure in the modern cyber landscape.

References:

1. Reznik O.V., Sopko V.V., Chebanenko O.I. Problems of Ensuring Cybersecurity of Ukraine's Critical Infrastructure // Weapons and Military Equipment Systems. – 2020. – No. 1. – P. 72-79. – Available at: https://doi.org/10.30748/soivt.2020.58.09

2. ITU Recommendations on Critical Infrastructure Cybersecurity: Analytical Report. – Geneva: International Telecommunication Union, 2021. – 50 p. – Available at: https://www.itu.int
3. Lynn W.J. Defending a New Domain: The Pentagon's Cyberstrategy // Foreign Affairs. – 2010. – Vol. 89, No. 5. – P. 97-108.
4. NATO and Ukraine: Current State of Cooperation in the Field of Cybersecurity // Official website of the Ministry of Defense of Ukraine. – Available at: https://www.mil.gov.ua

UDC 004.8:004.056.5

Kobylianska O.
student of higher education,
ERI "Institute of Computer Science and Artificial Intelligence"

ENCHANCING NEURAL NETWORK SECURITY: DEFENSE AGAINST ADVERSARIAL ATTACKS IN APPLIED AI SYSTEMS

Artificial intelligence (AI) is rapidly being integrated into various industries, such as manufacturing, education, business analytics, and decision-making systems. By automating processes and analyzing large amounts of data, AI opens new opportunities for the development of these sectors. AI enables increased efficiency in production processes, improved resource management, and enhanced decision-making quality based on accurate predictions. In education, AI helps create adaptive learning platforms that take into account the individual needs of each student, making the learning process more personalized and interactive. In business analytics, artificial intelligence allows for deeper market analysis, understanding consumer needs, and developing effective growth strategies. In decision-making systems, AI facilitates complex multifactor analyses, helping organizations respond more quickly to market changes or internal conditions [1].

However, despite these advantages, a serious challenge arises-ensuring the security of neural networks, which are the foundation of many modern AI systems. Neural networks can be vulnerable to various types of cyberattacks, posing a threat to their reliability and security. One of the most dangerous types of such attacks is adversarial attacks [2]. These involve making slight modifications to the input data, which can significantly reduce the model's accuracy and, as a result, lead to incorrect decisions. These changes may be imperceptible to humans but drastically alter the AI's performance. This poses significant risks, especially for industries that rely on the correct functioning of AI, such as healthcare, transportation, finance, and government services. In cases where decisions based on compromised models are wrong, the consequences can be catastrophic: from misdiagnoses in medicine to incorrect financial operations or accidents in transportation systems.

The goal of research was to analyze existing types of adversarial attacks on neural networks and develop methods for their protection. Adversarial attacks present a serious threat as they allow attackers to manipulate the model's operation without needing access to its outputs or internal parameters. First, let's examine the main attack methods. Data-level attacks are some of the most common. Attackers may use various techniques, such as the Fast Gradient Sign Method (FGSM) or Projected Gradient Descent (PGD), which allow for minimal changes to the input data, such as images or text, which, after modification, are interpreted completely differently by the model. These attacks can be carried out in the form of "black-box, white-box, or gray-box" attacks, depending on how familiar the attacker is with the model's internal structure. In a "black-box" attack, the attacker has limited information about the model, while in a "white-box" attack, they have detailed information about the model's architecture and parameters, greatly increasing the effectiveness of the attacks. "Gray-box" attacks lie between the two, combining features of both [3].

In addition to data-level attacks, there are also model-level attacks, where attackers manipulate the neural network itself during the training or deployment phases. These attacks may involve embedding "backdoors" that open the possibility for further manipulation or influencing the data selection process, which degrades the model's performance. For example, models can be designed to output a predetermined result when given a specific set of input data, while showing no errors under normal conditions. These backdoors may remain undetected for extended periods, allowing attackers to use them at a critical moment. This type of attack is particularly dangerous for systems with a high degree of automation, where human oversight is minimal.

Protecting neural networks from such attacks is a critically important task. One of the most effective methods is adversarial training [4]. This approach involves incorporating adversarial examples into the model's training process, making it more resistant to malicious influences. During adversarial training, the model learns to recognize not only typical data but also specially modified examples, which increases its ability to resist attacks. However, this approach is not universal and requires constant updating and improvement of defense methods in response to new types of attacks.

Another key component of protection is monitoring the model's performance. Monitoring systems can detect anomalous input data and alert about potential attacks, reducing the risks of manipulation in real-time. Monitoring ensures timely response to suspicious activities and helps identify discrepancies between predicted and actual model performance. Another important measure is strengthening the model's robustness. This can be achieved by using filtering structures that help reduce the impact of adversarial noise-small perturbations in the input data that can throw the model off course. Such filters can reduce noise levels at the input stage or strengthen critical components of the model, making it less vulnerable to attacks.

Additionally, strategies for eliminating adversarial perturbations are used, involving the application of filtering and other algorithms to mitigate or completely remove such disturbances. This allows the model to "clean" the input data from any

potentially dangerous changes and maintain stable performance even under targeted interference.

The conducted research confirmed that adversarial attacks can significantly affect the accuracy of neural networks. However, the developed defense methods, such as adversarial training, have proven effective in increasing the robustness of models against such attacks. This significantly reduces the risks of incorrect decisions, which is especially important for industries where the reliability and safety of AI technologies are critical. The importance of protecting models becomes even more apparent in fields such as healthcare, where erroneous decisions can cost lives, or in finance, where inaccurate predictions can lead to substantial losses.

The proposed defense methods can be applied in various fields, including healthcare, banking, transportation, and education. In these industries, AI is a crucial tool for automating processes and ensuring more accurate predictions. Automation and intelligent data processing reduce the impact of the human factor, ensuring more stable and reliable outcomes.

Further research in this area will contribute to the improvement of methods for protecting neural networks, which, in turn, will minimize the risks associated with cyberattacks. Specifically, the constant enhancement of adversarial training approaches, the introduction of new algorithms to detect and block attacks, and the integration of protective technologies into a wider range of systems will allow AI technologies to continue evolving without compromising their security. Another important direction is the development of standards and regulations that will ensure oversight over the development and implementation of AI systems with stricter requirements for protection against attacks.

Thus, AI security in today's world is a multifaceted task requiring both deep technical knowledge and strategic planning. Ensuring the reliability and resilience of neural networks is a key factor that will allow the full potential of AI to be utilized in various fields of life while minimizing the risks and threats associated with cyberattacks. Through ongoing research and improvement of defense methods, artificial intelligence has every chance to remain a safe and reliable technology in the future, contributing to further societal and economic development.

References:

1. Incredible Advantages of AI | Notable 23 Benefits of AI. Режим доступу: https://www.simplilearn.com/advantages-and-disadvantages-of-artificial-intelligence-article

2. What Is Adversarial Machine Learning? Attack Methods in 2024. Режим доступу: https://viso.ai/deep-learning/adversarial-machine-learning/

3. N. Carlini and H. Farid, “Evading Deepfake – Image detectors with white- and black-box attacks,” in Proc. IEEE Conf. Comput. Vis.Pattern Recognit. (CVPR’20), Seattle, WA, USA, Липень 14-19, 2020, ст. 2804–2813.

4. Adversarial Training: What you didn’t know yet. Режим доступу: https://datascientest.com/en/adversarial-training-what-you-didnt-know-yet

UDC 004.056

Naumik-Gladka Kateryna
Doctor of Economics, Professor, Department of Marketing
Simon Kuznets Kharkov National University of Economics
Kaliuzhna Olha
higher education student, group: 6.03.073.020.23.2
Simon Kuznets Kharkov National University of Economics

PHISHING: PSYCHOLOGICAL MECHANISMS AND PROTECTION AGAINST DECEPTION

Phishing represents a form of cyberattack in which the attacker exploits social engineering tactics to perpetrate identity theft. Typically, phishing involves sending fraudulent emails that mimic trusted entities, such as online banks, auction platforms, or payment services. These emails direct users to counterfeit websites that closely resemble legitimate login pages, with the ultimate goal of collecting sensitive information, including usernames, passwords, credit card details, and monetary assets. Aleroud and Zhou have demonstrated that phishing succeeds largely due to its reliance on psychological manipulation through social engineering tactics [1, p.1]. Phishing has become one of the most prevalent cyber threats, continually evolving in sophistication, necessitating user vigilance in all forms of digital communication.

Those most susceptible to phishing attacks are individuals with low cyber hygiene, those who fail to scrutinize suspicious emails or messages, and those inclined to act under the pressure of urgent communications. Research by Pureti has established a significant correlation between age and vulnerability to phishing ($r = 0.35$, $p < 0.01$), with younger individuals aged 18-30 displaying greater susceptibility than older age groups. However, no significant gender differences were noted in phishing victimization [3, pp. 7-8]. The increased vulnerability of younger users may be attributed to overconfidence in their technological expertise, leading to inadequate attention to potential threats. Maintaining a high level of cyber hygiene is crucial for all age groups.

Phishing infiltrates devices through deceptive emails or messages containing malicious links or attachments. Once clicked, these links redirect users to fraudulent websites where personal information is requested. Alternatively, opening malicious attachments can install harmful software that collects data or grants unauthorized access to the device. According to Boskin and Chornyi, phishing messages often appear to originate from reputable organizations, such as PayPal or government agencies, but are counterfeit. These emails typically request users to update or verify their personal information, and direct them to fraudulent websites designed to closely mimic legitimate ones, where users are prompted to enter sensitive data. If attackers obtain this information, it may result in theft of personal data or funds [4, p.184]. These findings underscore the importance of verifying the legitimacy of any request for personal information.

The psychological mechanisms behind phishing's success include trust in technology and the perception of the internet as a secure environment. Many users unconsciously regard information received via email or message as reliable, which is exploited by attackers. Phishing schemes frequently employ urgency, such as messages indicating that an account will be blocked unless immediate action is taken, inducing panic and prompting impulsive behavior without verifying the authenticity of the message. Social engineering plays a central role in these attacks, with scammers often using emotional appeals and posing as trusted representatives or acquaintances to manipulate victims. This fosters a sense of trust, making individuals more likely to disclose sensitive information. Jari highlights that under such emotional pressure, human behavior is driven more by subconscious processes, which lack logical or analytical rigor-an aspect that phishers exploit [2, p.5].

Inexperience in online security further increases vulnerability, as individuals may lack confidence in their ability to identify phishing threats, leading to poor decision-making. Additionally, social pressure in online networks can contribute to phishing risks, with users often disregarding warning signs in an effort to conform to group behavior.

Protection Against Phishing**:** Phishing remains a serious threat, making education and awareness essential defensive measures. Understanding the various types of phishing attacks and recognizing the methods employed by scammers can enhance vigilance. When receiving messages requesting personal information, users should always verify the legitimacy of the source by directly contacting the organization through official channels, rather than clicking on suspicious links. Phishing attacks frequently create a false sense of urgency, encouraging impulsive actions; therefore, it is important to remain calm and cautious in such situations.

Two-factor authentication (2FA) can greatly improve account security. Yevseiev and Korol emphasize that this additional layer of security makes it more difficult for attackers to access personal data [5]. Regular password updates, the use of complex passwords, and avoiding the same password for multiple accounts are also effective strategies to minimize unauthorized access. Most banking systems now incorporate 2FA, using one-time passwords (OTP) delivered via email or SMS, or tokens from providers such as RSA Security, VASCO Data Security, and ActivIdentity. Although 2FA significantly enhances security, it should be noted that no method provides absolute protection.

In addition, monitoring financial and online accounts for suspicious activity is a critical step in protecting against phishing. Immediate action should be taken if any unusual activity is detected. By staying vigilant and adopting proactive protective measures, individuals can better safeguard themselves from phishing attacks.

Conclusion: Phishing poses a significant risk to all internet users. Understanding the psychological mechanisms that make individuals vulnerable to phishing can help mitigate these risks. Through education, awareness, and the adoption of proactive protective measures, individuals can reduce the likelihood of falling victim to phishing and protect their personal information from cybercriminals.

References:

1. Aleroud, Ahmed, and Lina Zhou. "Phishing environments, techniques, and countermeasures: A survey." Computers & Security 68 (2017): 160-196. URL: https://scholar.google.ru/schhp?hl=ru
2. Jari, Mousa. "An overview of phishing victimization: Human factors, training and the role of emotions." arXiv preprint arXiv:2209.11197 (2022). URL:https://www.csitcp.org/paper/12/1213csit19.pdf
3. Pureti, Nagaraju. "Phishing Scams: How to Recognize and Avoid Becoming a Victim." International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence 15.1 (2024): 51-73.
URL: https://scholar.google.ru/schhp?hl=ru
4. Boskin, O.O., and P.K. Chornyi. "ANALYSIS OF PROTECTION AGAINST PHISHING." "Modern Youth in the World of Information Technologies": Proceedings(2021):182.
URL:https://ksau.kherson.ua/files/konferencii/20210514/Збірка%20конференції%20CMCIT-2021.pdf#page=184
5. Yevseiev, Serhii Petrovych, and O.H. Korol. "Research on the Threats of Two-Factor Authentication Methods." Bulletin of the Lviv Polytechnic National University. Computer Systems and Networks 806 (2014): 62-71. URL: https://scholar.google.ru/schhp?hl=ru

UDC 004.056

Naumik-Gladka Kateryna
Doctor of Economics, Professor, Department of Marketing
Simon Kuznets Kharkiv National University of Economics
Tkachenko Ariana
higher education student, group:6.03.073.020.23.2
Simon Kuznets Kharkiv National University of Economics

DIGITAL TECHNOLOGIES, NEUROPLASTICITY, AND COGNITIVE SKILLS: DEVELOPMENT AND INFLUENCE

In the modern era, digital technologies play a pivotal role in human life, becoming an inseparable component of various domains-from professional and educational spheres to communication and entertainment. As technology continues to evolve, it is crucial to consider its impact on the human brain and nervous system.

Neuroplasticity refers to the brain's remarkable ability to adapt and reorganize itself in response to new experiences. This adaptability is not only crucial for physical changes, such as sensory compensation (e.g., heightened hearing in individuals with vision loss), but also for cognitive recovery following neurological injuries like strokes. This concept is well-articulated by Halyna Kovalchuk in her work *"What is neuroplasticity and how it helps to heal: 6 ways to support brain health and achieve*

resilience", where she highlights neuroplasticity's role in healing and resilience. The brain's plasticity allows for the continuous reshaping of functional neural networks in response to modern cognitive tasks and the new forms of communication fostered by digital technologies. This adaptability enhances our ability to process information in digital environments, showcasing the trainability of cognitive-perceptual abilities, as noted by Marios A. Pappas and Athanasios Drigas in their research on computerized learning for neuroplasticity and cognitive improvement [2, p.2].

With the increasing integration of technology into daily life, our interaction with the world has shifted towards digital platforms. As A.M. Monastirska argues in her work on *"The Impact of Digital Technologies on the Production and Consumption of Cultural Content: Clip Thinking"*, human interaction is increasingly confined to the screens of gadgets [3, p.125]. This shift not only alters social interactions but also shapes new cognitive habits, including those related to attention, memory, and information processing.

While digital technologies offer unprecedented access to information and enhance multitasking capabilities, excessive reliance on them can have adverse effects on mental and physical health. Long-term use of gadgets can lead to cognitive overload, decreased concentration, and sleep disturbances. The constant influx of notifications fragments attention, and reliance on external information sources contributes to "digital amnesia". Moreover, the blue light emitted by screens disrupts circadian rhythms, impairing sleep and cognitive function. Furthermore, the ready availability of solutions diminishes the need for creative thinking, reducing opportunities for problem-solving.

Despite these challenges, digital technologies also hold immense potential for enhancing cognitive functions. Interactive educational platforms stimulate learning, while cognitive training can foster memory retention and logical reasoning. To maximize the benefits of digital technology, it is important to follow certain principles: regular breaks during screen use, limited exposure to reduce information overload, and engagement in physical activities to support cognitive health. Meditation and mindfulness exercises, in particular, demonstrate the positive effects of neuroplasticity on attentional networks, as discussed by Pappas and Drigas [2, p.2].

Conclusion: Digital technologies exert a profound influence on neuroplasticity and cognitive skill development. While they offer opportunities for enhanced learning and mental flexibility, unregulated use can lead to cognitive deficits, such as reduced attention and memory problems. To mitigate these risks, a balanced approach is essential—incorporating breaks, managing screen time, and engaging in activities that promote both mental and physical well-being. By adopting a mindful approach to technology use, individuals can not only preserve cognitive health but also enhance neuroplasticity, contributing to a healthier and more productive life.

References:

1. Що таке нейропластичність та як вона допомагає зцілюватися: 6 способів підтримати здоров'я мозку й досягти стійкості; автор: Галина Ковальчук; Січень 2023р.

https://nus.org.ua/articles/shho-take-nejroplastychnist-ta-yak-vona-dopomagaye-ztsilyuvatysya-6-sposobiv-pidtrymaty-zdorov-ya-mozku-j-dosyagty-stijkosti/

2. Computerized Training for Neuroplasticity and Cognitive Improvement; author: Marios A. Pappas, Athanasios Drigas; p.2 https://www.researchgate.net/profile/Athanasios-Drigas/publication/335487670_Computerized_Training_for_Neuroplasticity_and_Cognitive_Improvement/links/5d68e14f92851c154cc5beba/Computerized-Training-for-Neuroplasticity-and-Cognitive-Improvement.pdf

3. Вплив цифрових технологій на виробництво та споживання культурного контенту. кліпове мислення; автор: Монастирська Анастасія Ярославівна ; с.125 https://moodle.znu.edu.ua/pluginfile.php/568053/mod_resource/content/1/almanach.pdf#page=125

4. 8 змін в людині, що сформувалися під впливом технологій https://cikavosti.com/8-zmin-v-lyudini-shho-sformuvalisya-pid-vplivom-tehnologiy/

UDC 004.056.5

Peliukh O. I.
student of higher education,
ERI "Institute of Public Administration"
of V. N. Karazin Kharkiv National University

CLASSIFICATION AND STRATEGIC APPROACHES TO CYBER THREAT PROTECTION

With the development of digital technologies, information and communication systems (ICS) have become the foundation for many areas of societal activity. However, cyber threats aimed at destabilizing the functioning of ICS, compromising data security, and stealing information are also increasing. These threats continuously evolve, becoming increasingly sophisticated and dangerous. In response to these challenges, new cybersecurity strategies are being developed to reduce risk levels and minimize potential losses. This study will examine the classification of cyber threats and effective protection methods.

Cybersecurity threats can be classified according to several criteria, among which the key ones are the principles of the cybersecurity triad: confidentiality, integrity, and availability of data. Confidentiality involves protecting information from unauthorized access, integrity ensures that data remains unchanged, while availability guarantees that information can be accessed by authorized users when needed [1]. These principles define the primary objectives of cybersecurity.

Threats can be classified as internal and external. Internal threats arise from the actions or negligence of employees who have access to ICS. They can be intentional or unintentional but can cause serious security breaches in both cases [2]. External

threats come from outside the organization, often from cybercriminals, hackers, or competitors trying to access confidential information or disrupt system operations [3].

Additionally, threats are classified by the level of harm caused: general threats (which impact the entire system) and private threats (affecting the operation of specific components). By their nature, threats can be natural (such as natural disasters or technical equipment failures) or artificial (actions of malicious individuals) [4].

One of the biggest problems for organizations is internal threats, which are often underestimated. They can arise due to the human factor, where employees inadvertently violate security policies, or through the actions of insiders who misuse their access to the systems [5]. Insiders can be part of the company or act in collusion with other individuals or organizations to steal information or destabilize system operations.

According to research [6], most internal threats stem from unintentional actions, such as using weak passwords, negligence in handling confidential information, or a lack of knowledge of security protocols. Insufficient employee education in this area is one of the reasons for such incidents.

However, intentional threats also pose significant danger. Insiders may act in their own interest or for the benefit of third parties, including competitors or criminal groups. They may intentionally share confidential information, alter or delete data, or even incapacitate key components of the ICS [7].

External threats are becoming increasingly complex due to the rapid evolution of technologies and the growing number of cybercriminals. Among the main attack methods are phishing, DDoS attacks, SQL injection, brute force attacks, and man-in-the-middle attacks.

Phishing attacks are among the most common types of threats. Malicious actors use fake emails or websites to trick users into providing their personal data or account credentials. As many users lack sufficient awareness of security, such attacks are effective and pose a significant threat to organizations of any level.

DDoS attacks (denial of service attacks) aim to overload servers or systems with a massive number of requests, leading to temporary unavailability. Such attacks can be particularly destructive for businesses, as any delay in access to online resources or services can result in substantial financial losses, especially for large corporations.

SQL injections are used to steal or alter information in databases (DB) through vulnerabilities in software. Hackers can inject malicious commands into DB queries, allowing them to access or even modify confidential information.

Man-in-the-middle attacks involve intercepting communications between two parties. This method can be used to steal data during transmission over unsecured channels, such as public Wi-Fi networks. Such an attack can remain unnoticed by both parties and lead to serious security breaches.

Malware, including spyware and ransomware, also poses a significant threat to ICS. Spyware enables malicious actors to monitor user activity and transmit confidential information to third-party servers. Ransomware blocks access to systems or files, demanding a ransom for restoring access. This can cause significant harm to

businesses, as organizations are forced to spend substantial sums on data recovery or payments to criminals.

Effective protection of ICS requires the application of various approaches and methods, which can be classified according to several criteria [1]. The main criteria for classification are the level of impact on the object of protection and the level of implementation of protection methods and means.

Information protection methods can be divided into physical, software, cryptographic, and legal means. Physical methods involve controlling physical access to equipment, such as locks, video surveillance, and restricting access to premises. Software tools include antivirus software, firewalls, intrusion detection and prevention systems, and other technologies to prevent cyberattacks.

Cryptographic methods ensure the encryption of data to protect the confidentiality and integrity of information transmitted through ICS. Cryptographic algorithms are used to create secure data transmission channels and protect information from unauthorized access.

Legal methods include legislative acts and regulatory documents that govern security policies and define legal measures for protecting information, as well as responsibilities for violations of cybersecurity laws.

Technical protection methods encompass a wide range of technological solutions, including user authentication and authorization systems, data encryption, network firewalls, and intrusion detection systems. They provide protection at the network level and at the level of application programs and data.

Organizational methods involve creating and implementing an information security policy that regulates access to ICS resources, monitoring compliance with security policies, and training personnel. Security policies should cover all aspects of the organization's work, from managing access to secure systems to monitoring the use of personal devices.

Thus, in modern conditions, ensuring cybersecurity requires a comprehensive approach that includes not only technical protection measures but also organizational measures and employee training. It is crucial to implement modern access control systems, authentication, data encryption, and to utilize monitoring and threat detection systems. At the same time, considerable attention must be paid to internal threats, especially the human factor. Careful staff selection, regular training, and the implementation of clear security policies can significantly reduce the risk of cyber threats. Information security demands constant adaptation to new threats and the enhancement of protective mechanisms.

References:

1. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020.

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.

3. What is an Insider Threat? Definition Types & Examples. OpenText. Режим доступу: https://www.opentext.com/what-is/insider-threat.

4. A guide to External Security Threats in 2024. Dashlane. Режим доступу: https://www.dashlane.com/blog/guide-to-external-security-threats.
5. RiskOptics. Most Common Types of Network Security Attacks. Режим доступу: https://reciprocity.com/blog/most-common-types-of-network-security-attacks/.
6. What is a Cryptographic Attack? Your Comprehensive Guide. Packetlabs. Режим доступу: https://www.packetlabs.net/posts/what-is-a-cryptographic-attack/.
7. Основи інформаційної безпеки: навч. посібник / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020.

УДК 004.056.55, 004.051

Аверков О.Ю.
здобувач вищої освіти,
ННІ «Комп'ютерних наук та штучного інтелекту» ХНУ імені В.Н. Каразіна
Науковий керівник
Лисицька І.В.
д.т.н., професор,
професор кафедри безпеки інформаційних систем і технологій
ННІ «Комп'ютерних наук та штучного інтелекту» ХНУ імені В.Н. Каразіна

РЕЗУЛЬТАТИ ТЕСТУВАННЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ ПЕРШОГО ЕТАПУ РОБОТИ ПРОТОКОЛУ ZK-STARK «АРИФМЕТИЗАЦІЯ»

Існує перспективне рішення заощадження ресурсів мережі Блокчейн за рахунок використання для процедури автентифікації сучасного постквантово-стійкого протоколу ZK-STARK [1,4,5]. Тестування на ефективність програмної реалізації першого етапу роботи протоколу ZK-STARK та надання рекомендацій щодо його найбільш ефективного впровадження визначає актуальність даної роботи. На основі постановки задачі та визначення вхідних даних будуть подані результати тестування програмної реалізації «Арифметизації» (мова програмування С++):

Нехай за умовою задачі нам дано:

Поле Z_{13} = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12} і воно складається з $\left|Z_{13}\right| = 13$ чисел зі складанням і множенням за модулем 13 (вхідні дані в програму). Це поле має мультиплікативну підгрупу G, таку, що $|G|$ =6 (вхідні дані в програму) і породжувальний елемент групи g = 4 (вхідні дані в програму). Існування такої підгрупи гарантоване, оскільки 6 ділить розмір цієї групи (який дорівнює 12) без залишку [3].

Припустімо, що розглянуте твердження про необхідність перевірки обчислювальної цілісності транзакції звучить так: «Перевіряючий має послідовність із 6 чисел, усі з яких це числа Фібоначчі».

Цю послідовність чисел Фібоначчі необхідно перевірити, прочитавши істотно менше 6 чисел [3]. Ця задача має такий розв'язок:

Послідовність чисел Фібоначчі формально визначається так (це вхідні дані в програму): $a_0 = 1; a_1 = 1; a_{n+2} = (a_{n+1} + a_n) \bmod 13$.

Можливо створити слід виконання, записавши поспіль усі 6 чисел Фібоначчі: 1, 1, 2, 3, 5, 8. Поліноміальні обмеження можуть мати вигляд [2, 3]:

$$\{A_0 - 1 = 0 \text{ та } A_1 - 1 = 0, \quad \forall\, 0 \le i < 4\colon A_{i+2} - A_{i+1} - A_i = 0, \; A_5 - 8 = 0.$$

Тепер приведемо поліноміальні обмеження до поліноміального вигляду: Рекурентне співвідношення Фібоначчі втілює набір обмежень на весь слід виконання, і його можна альтернативно інтерпретувати так [3]:

$$\forall\, 0 \le i < 4\colon f\left(g^{i+2}\right) - f\left(g^{i+1}\right) - f\left(g^{i}\right) = 0\,,$$

Тепер Верифікатор може створити поліном композицію за формулою [3]:

$$q(x) = \frac{f\left(g^{i+2}\right) - f\left(g^{i+1}\right) - f\left(g^{i}\right)}{\prod_{i=0}^{3}(x - g^{i})}\,,$$

Обчислення цього виразу для особливого випадку, коли ступені g утворюють підгрупу, може бути виконано так [4]:

$$x^{|G|} - 1 = \prod_{g \in G}(x - g),$$

Ця рівність є правильною, оскільки обидві сторони є многочленами ступеня |G|, корені яких у точності є елементами G [3]. А фактичний знаменник розглянутого композиційного полінома Фібоначчі можна отримати, переписавши його у вигляді [3]:

$$\frac{f\left(g^{i+2}\right) - f\left(g^{i+1}\right) - f\left(g^{i}\right)}{\prod_{i=0}^{3}(x - g^{i})} = \frac{\left(w - g^{4}\right) * \left(w - g^{5}\right) * [f\left(g^{2} * w\right) - f\left(g^{1} * w\right) - f(w)]}{w^{6} - 1}\,,$$

де $w \in \left\{1, g^{1}, g^{2}, g^{3}, g^{4}, g^{5}\right\}$.

Ця послідовність обчислень Арифметизації запрограмована на C^{++} та використана для тестування першого етапу роботи протоколу ZK-STARK.

Тестування трьох реалізацій Арифметизації (на основі методу Гауса (Г), зворотних матриць (ЗМ) та швидкого зворотного перетворення Фур'є (ШЗПФ) для процедури інтерполяції) показало, що найефективнішим є метод ШЗПФ для інтерполяції. Його найбільшу ефективність серед трьох методів можна

зобразити за допомогою графіку (рис.1).

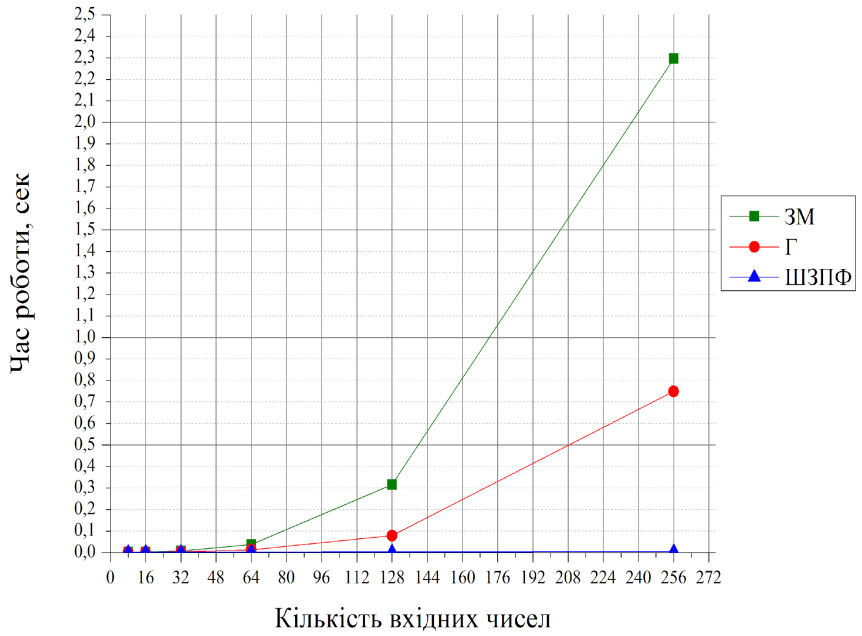


Рис.1 Залежність часу роботи Арифметизації на основі методів ЗМ, Г, ШЗПФ від кількості вхідних чисел Фібоначчі

На графіку вісь Oy означає середній за 1000 вимірювань час роботи програми, вісь Ox означає кількість вхідних в програму чисел Фібоначчі, зеленим кольором позначено час роботи варіанту Арифметизації, який використовує метод ЗМ для проведення процедури інтерполяції, червоним кольором позначено час роботи варіанту Арифметизації, який використовує метод Г для проведення процедури інтерполяції та синім кольором позначено час роботи варіанту Арифметизації, який використовує метод ШЗПФ для проведення процедури інтерполяції. При цьому, розрахунки у варіантах Арифметизації, які використовують метод Г та ЗМ для інтерполяції проходять у полі GF (257), а розрахунки у варіанту Арифметизації, який використовує метод ШЗПФ проходять у полі Златовласки, тобто у GF ($2^{64} - 2^{32} + 1$). Тобто розрахунки за допомогою ШЗПФ для 256 вхідних чисел Фібоначчі (256 невідомих та 256 рівнянь) проходять, як мінімум в 176 разів швидше при умові, що величини невідомих чисел в полі Златовласки більші в $\frac{2^{64}-2^{32}+1}{257}$ разів ніж в полі GF (257). До того ж, тестування показало, що максимальна кількість чисел Фібоначчі, яку можна подати на вхід при використанні ШЗПФ для інтерполяції, становить 2^{24} чисел, тобто за допомогою методу ШЗПФ можливо вирішувати СЛАР (проводити процедуру пошуку коефіцієнтів інтерполяційного полінома) розміром 2^{24} невідомих та 2^{24} рівнянь за середній за 100 вимірювань час 177, 45 секунди.

Використання саме методу ШЗПФ у першому етапі роботи «Арифметизація» протоколу ZK-STARK може прискорити роботу етапу у $\frac{n^3}{n*log_2 n}$ разів.

Список використаних джерел:

1. STARK Math: The Journey Begins / StarkWare // Medium. URL: https://medium.com/starkware/stark-math-the-journey-begins-51bd2b063c71
2. Arithmetization I / StarkWare // Medium. URL: https://medium.com/starkware/arithmetization-i-15c046390862
3. Arithmetization II / StarkWare // Medium. URL: https://medium.com/starkware/arithmetization-ii-403c3b3f4355
4. Кравченко П., Скрябін Б., Дубініна О. Блокчейн і децентралізовані системи: навчальний посібник [для студентів вищих навчальних закладів, які навчаються за напрямами підготовки «Безпека інформаційних і комунікаційних систем»]. Х.: ХНУ імені В. Н. Каразіна, 2013. – 632 с.
5. Lorne Lantz and Daniel Cawrey. Mastering Blockchain // Errata. URL: http://oreilly.com/catalog/errata.csp?isbn=9781492054702

УДК 004.56.5+004.89

Андренко К. В.,
здобувач бакалаврського рівня вищої освіти
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна;
Стяглик Н. І.,
к.п.н., доцент, завідувач кафедри інформаційних технологій
та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ: МОЖЛИВОСТІ ТА ЗАГРОЗИ

У сучасному світі інформаційні технології стали важливою складовою суспільства. Вони впливають на всі аспекти діяльності людини, включаючи бізнес, освіту, охорону здоров’я та державне управління. Саме з поширенням таких технологій зростає ризик кіберзагроз, які можуть завдати серйозної шкоди як окремим особам, так і організаціям. Кіберзлочинці постійно вдосконалюють свої методи, використовуючи новітні інструменти для здійснення атак, що вимагає від фахівців кібербезпеки постійної адаптації та пошуку нових рішень. В цих умовах особливої значущості набуває штучний інтелект. Завдяки своїм можливостям обробляти великі обсяги даних, виявляти аномалії та автоматизувати реакцію на загрози, він стає потужним інструментом у боротьбі з кіберзлочинністю. Системи на основі ШІ навчаючись на актуальних оновлюваних даних, можуть прогнозувати можливі атаки та забезпечувати своєчасне реагування на загрози. Проте, штучний інтелект несе в

собі й ризики, бо може використовуватися і злочинцями для створення більш складних і небезпечних атак.

Дослідження ролі штучного інтелекту є надзвичайно актуальним, адже необхідно не лише розуміти можливості ШІ, але й виявляти та нейтралізовувати загрози, пов'язані із його використанням. Важливо знайти баланс між перевагами та ризиками, які виникають у процесі інтеграції штучного інтелекту в стратегії кібербезпеки.

Обсяги даних у інформаційному середовищі, які генеруються щодня, є колосальними, тому звичайні методи обробки інформації часто не в змозі впоратися з таким масштабом. На допомогу приходять алгоритми машинного навчання, що можуть швидко обробити величезні масиви даних, виявляючи аномалії, пов'язані з наявністю кіберзагроз. Це дозволяє фахівцям знизити ризик серйозних інцидентів.

Позитивною можливістю є й автоматизація реагування на загрози. Виявляючи аномалію або загрозу, система на основі ШІ може автоматично запустити протидії, такі як блокування підозрілих IP-адрес, ізоляція заражених систем або відновлення даних з резервних копій. Це значно скорочує час реакції на інциденти, зменшуючи шкоду, яку можуть завдати кіберзлочинці.

ШІ демонструє свою ефективність в прогнозуванні атак. Алгоритми, аналізуючи дані про атаки, можуть виявляти шаблони та тенденції, що дозволяє передбачити потенційні загрози в майбутньому. Наприклад, якщо система виявляє, що певні типи атак частіше відбуваються в конкретні дати або в певних умовах, вона може підготуватися до них заздалегідь, забезпечуючи більш надійний захист.

Штучний інтелект може ідентифікувати шаблони поведінки користувачів і виявляти відхилення від норми. Це важливо як для виявлення внутрішніх загроз (наприклад, шахрайства з боку співробітників), так і для захисту від зовнішніх атак. Системи, що використовують ШІ, можуть адаптуватися до змін у поведінці користувачів, що дозволяє своєчасно виявляти підозрілі дії.

Не менш важливим є використання ШІ для підвищення безпеки мереж і систем. Інтелектуальні алгоритми можуть моніторити мережевий трафік в реальному часі, виявляючи аномалії та потенційні атаки, такі як DdoS-атаки. Це дає змогу своєчасно вжити заходів для захисту критично важливих ресурсів.

Зупинимось окремо на загрозах використання ШІ. Однією з основних небезпек є те, що кіберзлочинці можуть застосовувати ШІ для вдосконалення своїх атак. Наприклад, зловмисники можуть використовувати алгоритми машинного навчання для автоматизації процесів виявлення вразливостей у системах, а також для створення шкідливого програмного забезпечення, яке адаптується до захисних механізмів. Тому, навіть найсучасніші системи безпеки можуть виявитися неефективними. Другою значною загрозою є фальшиві дані та дезінформація. Використання ШІ для генерації контенту, такого як фальшиві новини, може підривати довіру до інформаційних джерел. Наприклад, створення правдоподібних новин та постів в соціальних мережах дезорієнтує користувачів і може призводити до паніки або дезінформації у великих

масштабах. Це ставить перед суспільством нові виклики у боротьбі з дезінформацією та маніпуляціями.

Крім того, алгоритми ШІ, можуть бути піддані "атакам на дані", коли зловмисники маніпулюють даними, що використовуються для навчання моделей. Це може призвести до необачних рішень, та втрати довіри до системи безпеки. Окрім цього, викликають тривогу етичні та правові аспекти використання ШІ в кібербезпеці. Впровадження автоматизованих систем може призводити до порушення приватності, тому що такі системи часто вимагають доступу до чутливої інформації. Необхідність захисту персональних даних підвищує вимоги до регулювання використання ШІ, але також може стати предметом конфлікту між безпекою та правами особистості.

Системи штучного інтелекту часто вимагають доступу до великих обсягів даних, включаючи особисту інформацію користувачів. Це підвищує ризик порушення приватності, адже дані можуть бути використані не лише для покращення безпеки, але й для неналежного збору та аналізу інформації про людей. Важливо, щоб організації, які використовують ШІ, дотримувалися принципів прозорості та підзвітності, чітко інформуючи користувачів про те, як їхні дані будуть використовуватися. Алгоритми машинного навчання можуть відтворювати та навіть посилювати наявні упередження в даних, що може призводити до дискримінаційних рішень. Наприклад, автоматизовані системи безпеки можуть ненавмисно виявляти більшу увагу до певних груп населення, що викликає серйозні етичні питання щодо справедливості та рівності у доступі до захисту.

Інтеграція ШІ в кібербезпеку потребує адаптації чинних правових норм та стандартів, включаючи розробку законодавства, яке б регулювало використання ШІ, захист персональних даних, а також визначення відповідальності за наслідки, що можуть виникнути внаслідок використання таких інструментів. Наприклад, хто нестиме відповідальність у разі, якщо система ШІ помилково заблокує легітимного користувача? Крім того, необхідно враховувати міжнародні аспекти, оскільки кіберзагрози часто не мають кордонів. Співпраця між країнами в розробці правових норм та етичних стандартів стає важливою умовою для ефективної боротьби з кіберзлочинністю.

Етичні та правові аспекти використання штучного інтелекту в кібербезпеці є складними і багатогранними. Вони вимагають зваженого підходу, що поєднує інновації з дотриманням прав людини та етичних норм. Тільки таким чином можна забезпечити ефективний та справедливий захист інформаційних систем у сучасному цифровому середовищі.

Узагальнюючи, роль штучного інтелекту в кібербезпеці є надзвичайно важливою і складною. З одного боку, ШІ надає потужні інструменти для виявлення, аналізу та реагування на кіберзагрози, що суттєво підвищує рівень захисту інформаційних систем. Водночас із цими можливостями виникають і серйозні виклики: зловмисники можуть використовувати ШІ для вдосконалення своїх атак, що ставить перед фахівцями нові завдання. Крім того, етичні та правові аспекти, такі як питання приватності, упередженості в алгоритмах та

регулювання використання ШІ, потребують уважного розгляду та розробки відповідних стандартів. Тому, щоб знайти баланс між інноваціями та безпекою, можливостями та ризиками, потрібні колективні зусилля з боку державних структур, бізнесу та суспільства в цілому, а також постійна адаптація стратегій захисту до нових викликів. Лише таким чином можна забезпечити надійний та оптимальний захист інформаційного середовища в умовах швидко змінюваного цифрового світу.

Список використаних джерел:

1. Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y. (2016). "Information Security in Big Data: Privacy and Data Mining." *IEEE Access*. [Електронний ресурс] Режим доступу: https://ieeexplore.ieee.org/document/7445143
2. Штучний інтелект і права людини. [Електронний ресурс] Режим доступу: https://thedigital.gov.ua/news/shtuchniy-intelekt-i-prava-lyudini-prezentuvali-rekomendatsii-z-vidpovidalnogo-vikoristannya-shi
3. Переваги та недоліки штучного інтелекту. [Електронний ресурс] Режим доступу: https://ardenis.com.ua/blog/shtuchnyj-intelekt-shi-perevagy-ta-nedoliky-chastyna-1/

УДК 004.056.53

Анісіч Д.В.
здобувач вищої освіти,
*кафедра MCiT, «*Навчально-науковий інститут інформаційних технологій*»*
ХНЕУ імені С. Кузнеця
Науковий керівник
Грабовський Є.М.
к.е.н., доцент, доцент кафедри мультимедійних систем і технологій
*кафедра MCiT, «*Навчально-науковий інститут інформаційних технологій*»*
ХНЕУ імені С. Кузнеця

ВПЛИВ ІНТЕРНЕТУ НА РОЗВИТОК ФЕНДОМ-СПІЛЬНОТ

Безперечна перевага, яку Інтернет приніс людям, – це швидкий обмін інформацією: за лічені секунди можна знайти в мережі необхідну книгу, зв'язатися з другом, що знаходиться на іншому кінці світу, відшукати відповідь на питання, що цікавить. Складно навіть уявити, наскільки такі можливості змінили уявлення про знання, інформацію, бізнес, відносини. Причому можна не лише подивитися фільм, але й відразу обговорити його з іншими користувачами; не тільки прочитати статтю, але й поцікавитися у фахівців, наскільки вона компетентна.

За допомогою цифрових технологій люди створили нову соціальну онлайн-форму на основі Інтернету. Колишня групова структура, заснована на крові та клані, поступово руйнується та створюються спільноти в Інтернеті. Сьогодні шанувальники прагнуть знаходити один одного та створювати групи через Інтернет.

Завдяки появі соціальних мереж фанати також знайшли ефективний спосіб створити відділення для своїх кіл. Вони використовують спеціальні лінгвістичні символи, щоб визначити межі групи своїх уболівальників. Ці лінгвістичні символи не лише створюють спільний простір значення для шанувальників, але й роблять тих, хто не належить до групи, «іншими» [1-3]. Ці дискурсивні системи стають правилами за замовчуванням у спільноті фанатів, сприяючи більшому відчуттю єдності та приналежності серед уболівальників.

Соціальна ідентичність – це усвідомлення того, що індивід є членом певної соціальної групи, і що усвідомлення приналежності до певної групи приносить їй унікальні емоції та цінності. Фан-спільноти мають не надто стабільну структуру. Уболівальники можуть об’єднуватися в різні фан-групи, і ніхто не має абсолютної лояльності. Усі шанувальники насолоджуються тимчасовою ідентичністю в Інтернеті. Таким чином, відносини між окремим фанатом і фендом-спільнотою змінюються.

Інтернет надає фанатам віртуальну ідентичність, дозволяючи їм вільніше приєднуватися та залишати. Так само, як є фанат, який може бути фанатом Гаррі Поттера, він також може бути фанатом корейської жіночої групи Blackpink, і вони можуть приєднатися та залишити з відносною легкістю.

Інтернет допоміг користувачам Інтернету створити кращі механізми для ефективної співпраці. Потужність офлайн-груп не зрівняється з потужністю сьогоднішніх скупчень фанатів. Завдяки оновленню та вдосконаленню медіа фанатів на платформах соціальних мереж частіше об’єднуватимуть спільні емоції та почуття [4]. Їхнє зібрання, як правило, створює емоційний консенсус, і колективна ідентичність, яка приходить разом із групою, може швидко підігріти цей емоційний консенсус. Однак існує також небезпека того, що в цій емоційній атмосфері вболівальники також можуть використовувати кластеризацію фанатських кіл для досягнення дискурсивної гегемонії. Шанувальники люблять створювати ілюзію, що кумир дуже популярний, постійно публікуючи багато про нього, нападаючи та приховуючи будь-які коментарі й факти, які ображають їх кумира. Віртуальна висока популярність впливає на справедливість акторсько-співацької індустрії та навіть створює фальшиву популярність деяких неякісних артистів, що погано впливає на здорове зростання підлітків.

Окреслимо основні характеристики впливу Інтернету на фендом-спільноти:

1. спеціальні лінгвістичні символи;
2. соціальна ідентичність;
3. віртуальна ідентичність;
4. колективна ідентичність;
5. кластеризація фанатських кіл;

6. кумиризація будь-яких дій фендом-об’єкту.

Отже, Інтернет має глибокий вплив на створення, взаємовідносини фендом-спільнот. Він може як об’єднувати абсолютно різних людей будь-якого віку, статі, національності, так і зіштовхувати різні фанатські кола, в результаті перетинання, зазіхання один фендомів над іншими.

Список використаних джерел:

1. Starkova, O., Bondarenko, D., Hrabovskyi, Y. Providing software support for economic analysis. Technology Audit and Production Reserves, 2023, № 5 (2 (73)), 34–39.

2. Khoroshevska I., Khoroshevskyi O., Hrabovskyi Y., Lukyanova V., Zhytlova I. Development of a multimedia training course for user self-development. Eastern-European Journal of Enterprise Technologies, 2024, № 2(2 (128), P. 48–63

3. Ushakova, I., Hrabovskyi, Ye. Methodology for developing an information site with Workflow support for publishing articles. Development management. 2022. № 20(3). P. 20–28. DOI: 10.57111/devt.20(3).2022.20-28

4. Hrabovskyi, Y., Bondarenko, D., Ushakova, I. Usage of adaptive design technologies for the designing of a web application for analysis of the efficiency of solar panels. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки, 2024, Т. 35 (74), № 1, С. 118 – 126.

УДК 004.056.53

Ахмедзянов А.Р., Вакар В.С.
здобувачи фахової передвищої освіти
Харківський комп’ютерний фаховий коледж
Керівник
Ахмедзянова О.А.
викладач вищої категорії
Харківський комп’ютерний фаховий коледж

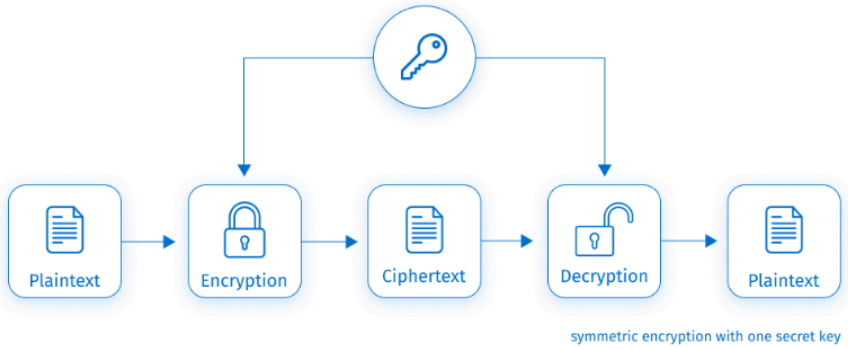
ІНСТРУМЕНТИ БЕЗПЕКИ В СКБД MYSQL

У світі, коли обмін інформацією в мережі стає невід’ємною частиною сучасного життя, одним з найважливіших завдань стає захист даних від несанкціонованого доступу. Кількість кіберзагроз постійно зростає, безпека конфіденційної інформації від несанкціонованого доступу й кібератак стає критично важливим завданням для безперервної роботи, збереження репутації та фінансової стабільності будь-якої компанії або організації.

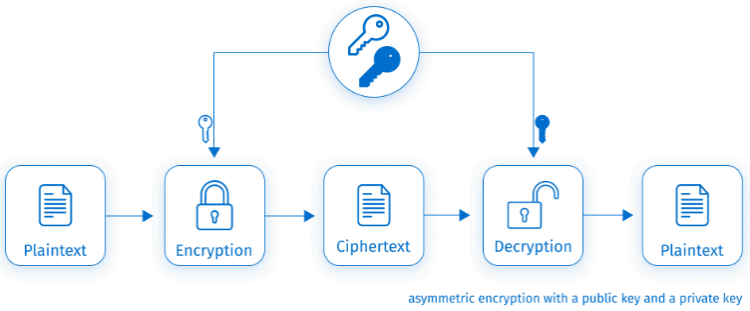
Одним зі способів захисту конфіденційної інформації є шифрування даних. Процес шифрування стає можливим завдяки криптографічним ключам в поєднанні з різними математичними алгоритмами.

Існує кілька видів шифрування, які використовуються для різних цілей та сценаріїв безпеки. Розглянемо деякі з них, що є найпопулярнішими:

– Симетричне шифрування – використовує один криптографічний ключ для шифрування і дешифрування даних. Використання одного ключа для обох операцій робить процес шифрування простим. Популярними алгоритмами симетричного шифрування є DES (Data Encryption Standard), AES (Advanced Encryption Standard) та IDEA (International Data Encryption Algorithm).



– Асиметричне шифрування – 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». Приватний ключ має бути захищеним і ніколи не надаватися (відкриті ключі можуть бути надані спільно або навіть опубліковані). Найвідомішим протоколом асиметричного шифрування є RSA (Rivest-Shamir-Adleman).



– Хешування – процес перетворення даних у вигляді випадкової послідовності фіксованої довжини (хеш-коду), який неможливо розшифрувати. Даний метод широко використовується для збереження паролів та перевірки цілісності даних. Популярні хеш-функції включають MD5, SHA-1 та SHA-256.

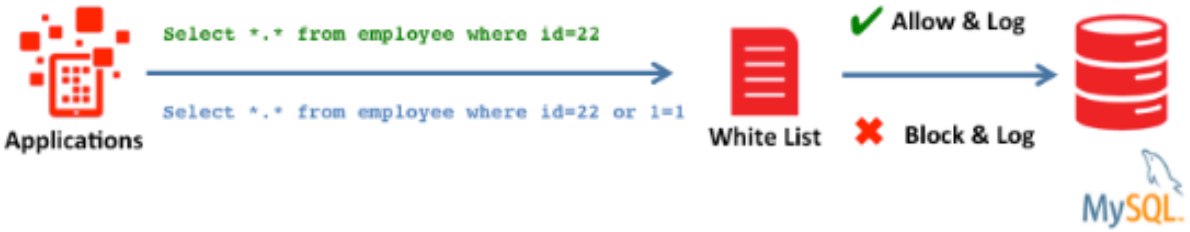
Говорячи про шифрування MySQL, ми маємо справу з двома сценаріями: шифрування даних, що зберігаються в базах даних MySQL, і шифрування підключень до серверів MySQL. Кожен сценарій передбачає певні методи та засоби.

Data-at-rest encryption – використовується для даних, що зберігаються в базах даних MySQL, оскільки він підтримується механізмом зберігання MySQL за замовчуванням InnoDB. Він застосовується до загальних табличних просторів, табличних просторів файлів на таблицю, системних табличних просторів MySQL, а також журналів повторення та скасування.

Advanced Encryption Standard (AES) – це стандартний алгоритм шифрування для MySQL, який використовується для захисту даних. Він

використовує той самий ключ (пароль) для операцій шифрування та дешифрування. Довжина ключа за замовчуванням становить 128 біт. Це може бути 192 або 256 біт.

Використовуючи стандартні алгоритми AES дані шифруються автоматично в режимі реального часу перед записом у сховище й розшифровуються під час читання зі сховища. Як результат, хакери та зловмисники не можуть прочитати конфіденційні дані безпосередньо з файлів бази даних.



Найпоширенішими варіантами використання хешування є сценарії автентифікації. Цифрові підписи та сертифікати SSL базуються на хешах. Рекомендованою функцією є SHA2(), найбезпечніший варіант.

Функція RANDOM_BYTES повертає двійковий рядок випадкових байтів, згенерованих бібліотекою SSL. Довжина цього двійкового рядка може бути від 1 до 1024. Найпоширенішим сценарієм використання RANDOM_BYTES() на практиці є генерування паролів.

Data-in-transit encryption захищає дані під час їх передачі з бази даних MySQL до програми. Дані шифруються в джерелі та передаються в зашифрованому вигляді по мережі для розшифровки в пункті призначення. MySQL використовує протокол безпеки транспортного рівня (TLS) з OpenSSL для шифрування даних під час передачі.

В MySQL для надійного шифрування даних передбачено можливість використання наступних функцій:

- ENCODE(string, key) і DECODE(string, key);
- AES_ENCRYPT(string, key) – шифрування AES;
- AES_DECRYPT(string, key) – розшифровка AES;
- COMPRESS() – повернення результату у бінарному виді;
- DES_ENCRYPT(string, key) – шифрування DES;
- DES_DECRYPT(string, key) – дешифровка DES;
- ENCODE() – шифрування рядка паролем;
- DECODE() – розшифровка тексту, обробленого функцією ENCODE();

– ENCRYPT() – шифрування за допомогою Unix-системного виклику crypt();

– MD5() – хешування даних алгоритмом MD-5;

– SHA1() або SHA() – хешування даних алгоритмом SHA-1 (160-біт).

Таким чином, шифрування MySQL є одним із критично важливих аспектів захисту баз даних MySQL, а саме:

– парольний захист;

– захист полів і записів таблиць БД;

– встановлення прав доступу до об'єктів БД;

– шифрування даних і програм.

Використовуючи IDE для розробки та керування MySQL у спеціальному диспетчері безпеки можна налаштувати параметри безпеки відповідно вимогам організації та кінцевих користувачів.

Список використаних джерел:

1. Інструменти безпеки в системі керування базами даних (СКБД) MySQL Enterprise Edition. URL: https://erc.ua/news-reviews/24517/instrumenti-bezpeki-v-sistemi-keruvannia-bazami-danikh-skbd-mysql-enterprise-edition

2. Деякі можливості адміністрування в MySQL. URL: https://okt.kmf.uz.ua/dw/doku.php?id=mysql:my-11

3. Encrypting Your MySQL: A How-to Guide. URL: https://www.devart.com/dbforge/mysql/studio/mysql-encryption.html

4. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються? URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/

УДК 004.35:004.67

Волік В.В.,
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

ТЕОРЕТИЧНІ ЗАСАДИ ДОКАЗОВОГО СПОСТЕРЕЖЕННЯ

У багатьох сферах, таких як медичні клінічні дослідження, фармацевтика, екологія та економіка, доказове спостереження стало необхідною та невід'ємною складовою, яка забезпечила дотримання міжнародних стандартів та зменшила ризик помилок та зловживань. А з появою нових технологій, таких як штучний інтелект, великі дані, інтернет речей, доказове спостереження стало значно точнішим та більш масштабним. Що, в свою чергу, відкрило нові можливості для аналізу та інтерпретації даних.

Спробуємо схарактеризувати сучасний стан доказового спостереження, яке активно використовується як в Україні, так і в Європі для забезпечення безпеки у різних галузях - від громадського порядку до охорони здоров'я та транспорту. Прикладом доказового спостереження є використання відеокамер, дронів, датчиків для контролю дорожнього руху, моніторингу здоров'я пацієнтів тощо.

Сучасні системи доказового спостереження використовують бездротові мережі (Wi-Fi, Bluetooth), хмарні технології, криптографічні методи для захисту даних та алгоритми штучного інтелекту для аналізу великих обсягів даних.

Проте, збільшення обсягів зібраних даних і зростання кіберзагроз роблять кібербезпеку однією з ключових проблем. Крім того, виникають і певні етичні питання щодо конфіденційності. Особливо це актуально у випадках, коли системи доказового спостереження використовуються для моніторингу публічних місць, що може порушувати права на приватність.

Одним із головних викликів є зростання обсягів даних, які збираються сучасними системами. З кожним роком кількість підключених до мережі пристроїв зростає, що створює серйозні проблеми для зберігання, обробки та аналізу даних. Зокрема, це стосується систем із використанням IoT (Інтернет речей), де пристрої безперервно збирають інформацію в режимі реального часу. Це вимагає не тільки великої обчислювальної потужності, але й ефективних алгоритмів обробки та аналізу. Через те, що збільшення кількості підключених до інтернету пристроїв збільшує ризик кібератак, мережі, що обробляють дані з сенсорів і пристроїв, стають вразливими до втручання, перехоплення або підробки даних. Тому збереження конфіденційності і захист інформації є критично важливими завданнями для забезпечення надійності систем

доказового спостереження. Наголосимо на важливості дотримання норм і стандартів захисту даних, що забезпечує правовий захист користувачів від порушення конфіденційності.

Датчики є основними елементами систем доказового спостереження, оскільки вони збирають дані з навколишнього середовища для подальшої обробки й аналізу. Розглянемо різні типи датчиків, їх принципи роботи та застосування в різних сферах.

Біосенсори: використовуються для моніторингу стану здоров'я пацієнтів або контролю за хімічним складом навколишнього середовища. Їх застосовують у медичній діагностиці, харчовій промисловості та екологічному моніторингу.

Наноматеріали: датчики на основі наноматеріалів забезпечують високу чутливість і точність при вимірюванні таких параметрів, як температура, тиск або гази. Ці датчики активно використовуються у наукових дослідженнях і промисловості.

Оптоелектронні датчики: використовують світло для вимірювання різних параметрів. Їх застосовують у системах інфраструктурного моніторингу.

Бездротові датчики: передають дані за допомогою радіозв'язку (Wi-Fi, Bluetooth, LoRa), що дозволяє використовувати їх для віддаленого моніторингу в розумних містах, промисловості та у сфері безпеки.

Датчики мікроелектромеханічних систем: використовуються в смартфонах, автомобілях та медичних пристроях для вимірювання прискорення, тиску або магнітних полів.

Гнучкі та носимі датчики: використовуються для моніторингу біометричних показників людини.

Розмаїття датчиків провокує й формування тенденцій розвитку сенсорних технологій. Так, зменшення розміру датчиків дозволяє використовувати їх у більш широкому спектрі пристроїв. Сучасні датчики надають більш точну і надійну інформацію, що є критично важливим для систем безпеки та управління процесами, а значить покращується якість даних. Датчики з низьким енергоспоживанням забезпечують тривалу роботу без частих змін елементів живлення. Все частіше датчики інтегруються з відеоспостереженням та іншими системами для створення комплексних рішень безпеки.

Ми бачимо значний прогрес у розвитку систем доказового спостереження, що підкреслює їх значущість для забезпечення безпеки в сучасному суспільстві.

Важливою складовою систем доказового спостереження є програмні платформи, оскільки вони дозволяють аналізувати зібрані дані, виявляти загрози та приймати інформовані рішення. Таким чином, програмні рішення відіграють важливу роль у забезпеченні безпеки в сучасних системах доказового спостереження, дозволяючи аналізувати великі обсяги даних і оперативно реагувати на загрози.

Список використаних джерел

1. Sensor-based intelligent tool online monitoring technology: Applications and progress / J. Huang et al. Measurement Science and Technology. 2024.

2. Application of Raspberry Pi microcontroller for management and monitoring of IoT Systems / R. Minailenko et al. Central Ukrainian Scientific Bulletin Technical Sciences. 2023. Vol. 2, no. 7 (38). P. 12–18.

3. Review on Blockchain for IoT Security and Data Integrity / M. Shaima et al. Security, Privacy and Trust Management : 12th International Conference. 2024. P. 115–126.

УДК 004.056.53

Гарбуз Є.О.
здобувач фахової передвищої освіти,
Харківський фаховий комп'ютерний коледж
Науковий керівник
Батирева Т.І.
викладач,спеціаліст вищої категорії
Харківський фаховий комп'ютерний коледж

СУЧАСНІ МЕТОДИ ШИФРУВАННЯ ТА БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ В ХМАРНИХ СЕРВІСАХ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ КОРИСТУВАЧІВ

У сучасному світі використання хмарних технологій стає дедалі популярнішим, оскільки організації прагнуть оптимізувати свої бізнес-процеси, знижуючи витрати на інфраструктуру та забезпечуючи доступ до даних з будь-якого місця. Однак, з цим зростанням виникають серйозні виклики щодо захисту персональних даних користувачів. Хмарні середовища часто містять величезні обсяги персональної інформації, що робить їх цілями для кіберзлочинців.

Основними проблемами у сфері конфіденційності даних є:

- кіберзагрози (хмара піддається різним типам атак, наприклад, фішинг, зловмисне програмне забезпечення, що може призвести до витоку даних);
- недостатня прозорість (багато провайдерів хмарних послуг не надають чіткої інформації про те, як обробляються і захищаються дані користувачів. Це може викликати занепокоєння у клієнтів щодо безпеки їхньої інформації);
- регуляторні вимоги (країни мають різні закони та регуляції щодо захисту даних, що ускладнює діяльність міжнародних компаній, які працюють у хмарних середовищах);
- проблеми шифрування (реалізація шифрування може бути складною, і не всі організації впроваджують ефективні стратегії шифрування);
- людський фактор (часто помилки користувачів або недбалість співробітників можуть призвести до витоків даних, тому навчання персоналу та усвідомлення важливості захисту інформації є критично важливими).

Обговорення цих проблем та пошук ефективних рішень стають дедалі важливішими для забезпечення безпеки персональних даних у хмарних середовищах. Шифрування, як механізм захисту даних, розвивається у наступних напрямках:

- Симетричне шифрування.
- Асиметричне шифрування.
- Гібридне шифрування.
- Шифрування на рівні файлової системи та бази даних.

1. Симетричне шифрування

Симетричне шифрування передбачає використання одного ключа для шифрування та дешифрування даних. Цей механізм часто швидший за інші методи шифрування, але вимагає, щоб обидві сторони мали доступ до одного ключа, що є менш безпечним.

2. Асиметричне шифрування

Асиметричне шифрування, також відоме як шифрування з відкритим ключем, використовує два ключі: один для шифрування даних, а інший – для їх дешифрування. Цей механізм повільніший за симетричне шифрування, але забезпечує більший захист, оскільки закритий ключ залишається секретним.

3. Гібридне шифрування

Гібридне шифрування поєднує переваги симетричного та асиметричного шифрування. У цьому методі для шифрування даних використовується симетричний ключ, який, в свою чергу, шифрується асиметричним шифруванням. Це забезпечує високу швидкість шифрування при збереженні безпеки, оскільки сам симетричний ключ передається захищено за допомогою відкритого ключа.

4. Шифрування на рівні файлової системи

Шифрування на рівні файлової системи використовується для автоматичного захисту всіх файлів, які завантажуються на сервери хмарних середовищ. Це означає, що дані шифруються на сервері перед їх зберіганням, і доступ до них можливий лише за наявності відповідного ключа. Ключі для шифрування можуть зберігатися як у хмарному сервісі, так і у користувача.

У разі компрометації фізичних серверів дані залишаються недоступними без відповідного ключа, що робить шифрування на рівні файлової системи важливим компонентом безпеки даних у хмарі.

5. Шифрування бази даних

Шифрування бази даних є важливим для захисту конфіденційних даних, таких як особисті дані користувачів, фінансова інформація та інші записи. Шифрування може бути реалізоване як на рівні окремих полів, так і на рівні всієї бази даних. Як і в попередньому випадку, ключі для шифрування бази даних можуть зберігатися: і в хмарному сервісі, і у користувача.

Таким чином, шифрування бази даних допомагає зменшити ризик витоку даних і відповідає вимогам конфіденційності, що вимагає захисту особистих даних. За умови правильного управління ключами, навіть у випадку компрометації системи, дані залишаться недоступними для зловмисників.

Другим напрямком у забезпеченні конфіденційності і захисту даних у хмарних сервісах є багатофакторна автентифікація.

Багатофакторна автентифікація (MFA) – це метод автентифікації (ідентифікації), який вимагає від користувача надання двох або більше доказів особистості, щоб отримати доступ до даних або увійти у свій обліковий запис.

В концепції MFA існують 3 основні фактори автентифікації, серед яких:

- Фактор знання. Це може бути пароль, пін-код або відповідь на секретне питання. Фактор є найбільш поширеним та доступним, але його безпека може бути порушена, якщо пароль стає відомим зловмисникам.
- Фактор власності. Це може бути фізичний токен, такий як USB-ключ або мобільний телефон, на якому встановлено спеціальний захищений додаток. Фактор зазвичай надійніший, оскільки зловмисник мусить мати доступ до фізичного пристрою, щоб отримати доступ.
- Фактор приналежності. Це може бути біометричний фактор, такий як відбиток пальця, розпізнавання обличчя або голосу. Фактор зазвичай надійніший, оскільки біометричні дані не можуть бути викрадені або відтворені.

Кожен з цих факторів має свої переваги та недоліки. Використання більше, ніж одного фактору автентифікації забезпечує вищий рівень безпеки, оскільки зловмиснику потрібно пройти крізь кілька факторів, щоб отримати доступ до ресурсу.

Залежно від конкретної реалізації MFA, можуть використовуватися різні комбінації факторів автентифікації. Наприклад, процедура може вимагати від користувача ввести пароль та одноразовий код, який згенерується спеціальним додатком на мобільному телефоні. Або ж MFA може використовувати біометричний фактор, такий як відбиток пальця, та фізичний токен, який містить захищений ключ доступу.

Отже, зважаючи на високі ризики витоків даних та кібератак у сучасному світі, використання методів захисту на кшталт симетричних/асиметричних шифрувань та багатофакторної автентифікації (MFA) стає все більш необхідним для бізнесу. Вони підвищують рівень безпеки даних, знижуючи ризик витоку інформації та захищаючи дані від шахрайства.

Список використаних джерел:

1. Дослідження та програмна реалізація системи забезпечення конфіденційності даних хмарних сервісів. Жупило М., 2023 URL: https://bit.ly/3ZE5ZQF
2. Розробка системи криптографічного захисту інформації у хмарному сховищі. Левашов М.О. 2022. URL: https://ami.lnu.edu.ua/wp-content/uploads/2024/02/Levashov.pdf
3. Метод шифрування даних в хмарних сервісах. Мельник П. 2023 URL: http://bit.ly/3XQySGS

УДК 004.056.5

Грайворонський О.М.
здобувач вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Науковий керівник
Кобилін А.М.
к.т.н., доцент, доцент кафедри інформаційних технологій
та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ЗАГРОЗИ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩУ, КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Розглянемо загрози інформаційному середовищу.

Кіберзлочинність: Кіберзлочини включають крадіжку даних, фінансові махінації, несанкціонований доступ до систем та інші шкідливі дії. Наприклад, злочинці можуть використовувати фішингові атаки для збору конфіденційних даних користувачів.

Шкідливе програмне забезпечення: Віруси, трояни, шпигунські програми та програми-вимагачі загрожують пристроям, викрадаючи або пошкоджуючи дані, порушуючи роботу систем.

DDoS-атаки: Масові атаки на сервери, мета яких - паралізувати роботу вебсайтів або онлайн-сервісів шляхом перевантаження їх запитами.

Соціальна інженерія: Маніпуляції з людьми для отримання конфіденційної інформації. Атакуючі часто використовують психологічні прийоми для обману жертв, змушуючи їх передати важливі дані.

Атаки на критичну інфраструктуру: Енергетика, фінансові системи, транспорт та інші критичні сектори піддаються ризику кібератак, що можуть спричинити масштабні економічні та соціальні наслідки.

Дамо визначення поняттю “кібербезпека”. Кібербезпека – це комплекс процесів, практичних порад і технологічних рішень, які допомагають захистити важливі системи й дані від несанкціонованого доступу.

Конфіденційність: Захист даних від несанкціонованого доступу. Це досягається за допомогою шифрування, контролю доступу та двофакторної автентифікації.

Цілісність: Забезпечення того, щоб дані не змінювалися або не пошкоджувалися під час передачі або зберігання. Це досягається за допомогою хешування та використання цифрових підписів.

Доступність: Забезпечення доступу до інформаційних систем і даних для уповноважених користувачів у потрібний час.

Аутентифікація та автентифікація: Процеси підтвердження особи користувача або пристрою перед наданням доступу до ресурсів.

Виявлення та усунення джерел загроз у комплексі захисту інформації

Дії шахраїв та хакерів, націлених на отримання конфіденційних даних. Кіберзлочинці постійно вдосконалюють свої методи атак та намагаються проникнути в інфосистему підприємства.

Можливі збої у роботі системи. Технічні збої та відмови в роботі інформаційної інфраструктури можуть призвести до витоку або пошкодження даних.

Неправомірна зміна відомостей для одержання несправедливої вигоди. Внутрішні співробітники компанії можуть зловжити своїми привілеями та змінити дані на свою користь або на шкоду підприємству.

Крадіжка інформації з використанням спеціальних систем. Існують різні методи крадіжки відомостей з підприємства, включаючи використання програмного забезпечення для збирання та передачі конфіденційних даних.

Загрози можуть походити як від конкурентів, які бажають отримати конкурентну перевагу, так і від самих співробітників підприємства, які можуть вирішити скористатися своїм доступом до інформації та передати її третім особам.

Розберемо методи захисту інформації

Усі матеріали повинні зберігатися в одному місці: Забезпечити контроль за її обробкою та обмежити доступ співробітників до секретних матеріалів. Комплексний підхід до захисту даних допоможе запобігти інфовитіканню через необережність або навмисні дії.

Система виявлення та запобігання вторгненням *(IDS/IPS)*: Системи, що виявляють підозрілу активність у мережі та можуть автоматично блокувати можливі атаки.

Шифрування даних: Один із найефективніших способів захисту конфіденційної інформації. Шифрування забезпечує захист даних навіть у разі їх викрадення.

Регулярне оновлення програмного забезпечення: Уразливості в старих версіях ПЗ можуть стати "воротами" для кіберзлочинців. Постійне оновлення систем допомагає зменшити ризики.

Отже, кібербезпека набуває критичного значення для сучасного інформаційного суспільства. Однак, досягнення ефективного захисту можливе лише за умови усвідомлення існуючих загроз, регулярного оновлення технологій захисту та дотримання принципів безпеки на всіх рівнях - від індивідуального до державного. Важливою складовою цього процесу є навчання користувачів основам кібергігієни, адже людський фактор залишається однією з найвразливіших ланок у захисті інформації. Крім того, підприємства та державні установи мають впроваджувати сучасні технології, такі як штучний інтелект та блокчейн, для підвищення рівня безпеки своїх даних. Потрібно також забезпечити постійний моніторинг і аналіз можливих загроз, аби реагувати на них в режимі реального часу.

Список використаних джерел:

1. Що таке кібербезпека? https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity/
2. Класифікація загроз безпеці даних у комп'ютерних системах https://tausoft.com.ua/klasyfikacziya-zagroz-bezpeczi-ta-poshkodzhennya-danyh-u-kompyuternyh-systemah/
3. Методи захисту інформації для підприємства https://resit.com.ua/zachist-informacii-na-pidpriemstvi/

УДК 004.056.53

Ечкенко К.В.
здобувач вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Науковий керівник
Ковальчук Д.М.
старший викладач кафедри інформаційних технологій
та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ ТРАДИЦІЙНИХ СИМЕТРИЧНИХ КРИПТОСИСТЕМ ДЛЯ БАНКІВСЬКИХ ДОДАТКІВ

З часу своєї появи банки незмінно притягували до себе злочинців. В останні десятиліття, з появою систем електронного банкінгу, питання безпеки фінансових технологій та банківського сектору, не втратило своєї актуальності. У наші дні значна частка всіх злочинів пов’язана з використанням автоматизованих систем обробки інформації банку. Отже, при створенні банківського програмного забезпечення велику увагу слід приділяти забезпеченню безпеки банківських додатків.

В банківському програмному забезпеченні зберігається й обробляється конфіденційна інформація. Наприклад, така як: персональні дані клієнтів (імена, адреси, номери телефонів, номери рахунків); інформація про фінансові операції (транзакції, кредити, платежі); інформація про внутрішні процеси банку, яка може використовуватися для шахрайських дій.

Тому, дослідження застосування традиційних симетричних криптосистем для банківських додатків є важливим аспектом забезпечення безпеки фінансових операцій. Симетричні криптосистеми використовуються для шифрування даних, переданих між клієнтами та банківськими системами, щоб захистити конфіденційну інформацію від несанкціонованого доступу. Вони забезпечують швидке та ефективне шифрування, але мають певні обмеження,

що вимагає їх комплексного використання з іншими криптографічними методами.

Симетричне шифрування використовує один ключ для шифрування та дешифрування інформації. Це робить процес шифрування швидким та ефективним, що важливо для банківських операцій в реальному часі.

Основні симетричні криптосистеми, що застосовуються у фінансових додатках:

- AES (Advanced Encryption Standard) – один з найбільш надійних та широко використовуваних алгоритмів, що підтримує ключі довжиною 128, 192 і 256 біт.
- DES (Data Encryption Standard) та його вдосконалена версія 3DES.

Виділимо основні переваги використання симетричних криптосистем у банківських додатках:

- висока швидкість шифрування: симетричні алгоритми набагато швидші в порівнянні з асиметричними методами (RSA, ECC), що робить їх ідеальними для великих обсягів транзакцій, які відбуваються в реальному часі.
- низька обчислювальна складність: симетричне шифрування вимагає менше обчислювальних ресурсів, що дозволяє використовувати його навіть на пристроях з обмеженими ресурсами, таких як мобільні телефони.
- надійний захист: алгоритми AES та 3DES добре захищені від багатьох відомих криптографічних атак, якщо вони правильно реалізовані.

Серед обмежень симетричних криптосистем можна виділити:

- проблема управління ключами: основним недоліком симетричних систем є необхідність безпечного обміну ключами між сторонами. Якщо ключ скомпрометований, зловмисник може розшифрувати всю інформацію, захищену цим ключем.
- проблема масштабування: зі збільшенням кількості користувачів кількість унікальних ключів, необхідних для захисту взаємодій між кожною парою сторін, різко зростає. Це створює значні складнощі для управління ключами у великих системах.

На практиці, у реальних банківських додатках симетричні криптосистеми зазвичай використовуються в комбінації з асиметричними алгоритмами. Асиметричні системи, такі як RSA або ECC, використовуються для безпечної передачі симетричних ключів, після чого симетричне шифрування застосовується для основної частини даних.

Такий підхід дозволяє ефективно вирішити проблему безпечного розповсюдження ключів та одночасно забезпечує високу швидкість обробки даних.

Отже, симетричні криптосистеми, такі як AES, є важливим інструментом для захисту даних у банківських додатках завдяки їх швидкості та ефективності. Однак через проблеми управління ключами їх необхідно використовувати у поєднанні з іншими методами, такими як асиметричне шифрування. Гібридні криптосистеми забезпечують оптимальне поєднання безпеки і продуктивності, що є критично важливим для сучасних банківських додатків.

Список використаних джерел:

1. Тарнавський Ю. А. Технології захисту інформації : підручник для студентів спеціальності 122 «Комп’ютерні науки». – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.
2. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навчальний посібник. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 192 с.
3. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.

УДК 004.056.53

Єрьомін Д.А.
здобувач фахової передвищої освіти
Харківський радіотехнічний фаховий коледж
Науковий керівник:
Радченко О.П.
викладач
Харківський радіотехнічний фаховий коледж

СУЧАСНІ ЗАСОБИ КІБЕРБЕЗПЕКИ ДЛЯ КРИПТОГАМАНЦІВ

Зі зростанням популярності крипто валютних активів, таких як Bitcoin та Ethereum, спостерігається постійне збільшення кількості кібератак на власників крипто гаманців. На відміну від традиційних фінансових установ, транзакції в крипто валютах децентралізовані та майже не підлягають поверненню. Це робить крипто валютні активи привабливою ціллю для зловмисників, а захист крипто гаманців – найважливішим аспектом безпеки в цифровому світі. Крипто гаманці зберігають приватні ключі, які надають доступ до коштів користувачів, і їх втрата може призвести до повної втрати активів. Тому питання кібербезпеки для крипто валютних гаманців є вкрай актуальним і потребує впровадження нових, більш ефективних методів захисту.

Методи атак на крипто валютні гаманці.

Існує багато різних способів атак на крипто валютні гаманці, деякі з яких стають дедалі витонченішими з розвитком технологій:

Фішинг. Зловмисники створюють підроблені веб-сайти і розсилають електронні листи, які зовні виглядають як офіційні повідомлення від сервісів крипто валютних гаманців. Метою таких атак є отримання доступу до приватних ключів та іншої важливої інформації користувачів.

Шкідливе ПЗ (Malware). Це одна з найпоширеніших загроз. Трояни та віруси можуть бути завантажені на комп'ютер або смартфон жертви з метою крадіжки даних криптогаманців. Вони можуть перехоплювати введені користувачем дані або навіть змінювати адреси криптогаманців під час транзакцій.

Соціальна інженерія. Цей метод передбачає обман користувачів з метою отримання конфіденційної інформації. Шахраї можуть видавати себе за представників служби підтримки, друзів або навіть відомих осіб у крипто спільноті.

Атаки на слабкі паролі. Криптогаманці можуть бути зламані через підбір слабких паролів. Використання однакових паролів на різних платформах також піддає користувачів додатковому ризику.

Експлойти смарт-контрактів. У разі використання гаманців, що взаємодіють з децентралізованими додатками (dApps), вразливості в смарт-контрактах можуть бути використані для крадіжки коштів або зміни транзакцій.

Сучасні засоби захисту крипто гаманців.

Для протидії цим загрозам розроблено різні рішення, які активно впроваджуються як у програмних, так і в апаратних гаманцях:

Апаратні гаманці. Одним із найбезпечніших способів зберігання криптовалют є використання апаратних гаманців (hardware wallets), таких як Ledger та Trezor. Ці пристрої зберігають приватні ключі в офлайн-режимі, що робить їх захищеними від більшості онлайн-атак, включно з фішингом та шкідливим ПЗ.

Мультипідписи (multisig). Ця технологія дозволяє для проведення транзакцій використовувати кілька ключів, які можуть бути розподілені між різними пристроями або користувачами. У результаті, якщо один ключ буде скомпрометований, зловмисник не зможе отримати доступ до коштів без інших ключів.

Аутентифікація з використанням блокчейна. Розробка децентралізованих систем аутентифікації з використанням смарт-контрактів може запропонувати вищий рівень безпеки порівняно з традиційними методами входу та пароля. Такі системи можуть усунути фактор довіри до одного центрального сервісу, зменшуючи ризик злому.

Протоколи конфіденційності (zk-SNARKs). Технології нульового розголошення інформації (Zero-Knowledge Proofs) можуть захистити транзакції, не розкриваючи жодних даних про користувача або суму транзакції. Такі протоколи, як zk-SNARKs, вже використовуються в деяких крипто валютах, таких як Zcash.

Машинне навчання та штучний інтелект. Системи, що використовують AI та машинне навчання, можуть відстежувати підозрілу активність, аналізувати поведінку користувачів та запобігати атакам на основі виявлених патернів. Наприклад, різкі зміни у геолокації або часу використання гаманця можуть стати підставою для блокування підозрілих операцій.

Концепція захисту крипто гаманців: впровадження гібридних методів.

Для забезпечення максимальної безпеки крипто валютних гаманців можна запропонувати гібридний підхід, що включає поєднання кількох методів захисту:

Апаратна безпека. Важливим компонентом повинно стати використання апаратних гаманців або безпечних елементних рішень, які зберігають приватні ключі в захищеному середовищі.

Мультифакторна аутентифікація (MFA). Включення кількох рівнів аутентифікації, таких як паролі, біометрія та підтвердження через вторинні пристрої, може значно знизити ризик несанкціонованого доступу.

Мультипідписи. Розподіл доступу між кількома ключами та користувачами робить крадіжку коштів складнішою задачею для зловмисників.

Регулярні оновлення ПЗ. Платформи, що надають послуги зберігання та управління крипто валютою, повинні регулярно оновлювати свої системи, усуваючи можливі вразливості.

Поведінковий аналіз із використанням AI. Системи, що відстежують аномальні дії на гаманці, можуть автоматично блокувати підозрілі транзакції та сповіщати користувача.

Освітні кампанії. Більшість зломів відбувається через людський фактор, тому важливо навчати користувачів основам безпеки, включаючи використання складних паролів та уникання фішингових сайтів.

Висновок: в умовах зростання популярності криптовалют захист крипто гаманців стає пріоритетним завданням для користувачів та розробників. Традиційні методи кібербезпеки вже не можуть забезпечити повний захист від нових видів атак. Сучасні рішення, такі як апаратні гаманці, мультипідписи та AI-технології, пропонують нові можливості для підвищення безпеки, але повинні поєднуватися з грамотним поведінкою користувачів та регулярним оновленням програмного забезпечення. Інтеграція гібридних методів захисту може стати основою для створення більш безпечної екосистеми для зберігання та управління крипто валютами.

Список використаних джерел:

1. Як захиститися від викрадення криптовалюти: поради юриста. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/yak-zahistitisya-vid-vikradennya-kriptovalyuti-poradi-yurista.html.
2. Crypto crime report 2023. URL: https://blog.chainalysis.com/reports/crypto-crime-report-2023
3. How-to-secure-your-cryptocurrency. URL: https://www.zdnet.com/article/how-to-secure-your-cryptocurrency

УДК 658.8

Кириченко А.В.
к.е.н., доцент, доцент кафедри організації підприємництва та біржової діяльності
Національний університет біоресурсів і природокористування України

СТРАТЕГІЇ ЗАХИСТУ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА В ЕЛЕКТРОННІЙ КОМЕРЦІЇ

Стратегії захисту інформаційного середовища в електронній комерції є критично важливими для забезпечення надійності бізнесу, захисту даних клієнтів і мінімізації ризиків кібератак. У сучасних умовах розвитку електронної комерції ці стратегії повинні бути комплексними, охоплювати технологічні, організаційні та правові аспекти захисту.

Електронна комерція є висококонкурентним середовищем із постійними змінами технологій. Вона змінила підприємництво, принесла більш конкурентоспроможні ціни завдяки ширшій пропозиції, різноманітності продуктів, збільшенню маркетингових стратегій і зробила споживачів товарів та послуг більш вимогливими [1]. Але, враховуючи всі сильні сторони роботи в онлайн форматі, підприємствам необхідно враховувати, що існують загрози інформаційному середовищу, врахування яких дозволить вести бізнес безпечно та ефективно.

Серед основних стратегій захисту інформаційного середовища в електронній комерції можна виділити: багаторівневий підхід до кібербезпеки, шифрування даних, використання багатофакторної аутентифікації, підтримка відповідності регуляторним стандартам, моніторинг та аналіз поведінки користувачів, регулярне оновлення програмного забезпечення, регулярне резервне копіювання даних, навчання співробітників і підвищення обізнаності, партнерство з фахівцями з кібербезпеки, захист платіжних операцій.

Багаторівневий підхід до кібербезпеки включає кілька рівнів захисту, щоб максимально мінімізувати ризики: міжмережеві екрани (забезпечують фільтрацію вхідного і вихідного трафіку, перешкоджаючи доступу зловмисників до мережі), системи виявлення і запобігання вторгнень (виявляють та блокують підозрілу активність у мережі), антивірусне програмне забезпечення (захищає кінцеві пристрої від шкідливого програмного забезпечення).

Шифрування даних забезпечує захист конфіденційних даних під час їх зберігання та передачі.

Впровадження багатофакторної аутентифікації дозволяє зменшити ризик компрометації акаунтів користувачів і співробітників. Окрім паролю, користувачі мають підтверджувати свою особу за допомогою додаткового фактора, наприклад, одноразового пароля або біометричних даних.

Для захисту інформації необхідно відповідати міжнародним та місцевим стандартам і регуляціям.

Використання сучасних інструментів моніторингу та аналізу поведінки споживачів дозволяє виявляти аномальну активність.

Своєчасне оновлення програмного забезпечення є важливим елементом стратегії безпеки, оскільки старі версії можуть містити вразливості. Це стосується: операційних систем, вебсерверів та баз даних, вебсайтів і платформ електронної комерції, систем безпеки, зокрема антивірусного програмного забезпечення і міжмережевих екранів.

Резервні копії захищають компанію від втрати даних через кібератаки. Резервне копіювання має відбуватися автоматично та регулярно зберігатися у захищеному середовищі, відокремленому від основних систем.

Багато атак використовують людський фактор, тому важливо навчати персонал щодо: розпізнавання фішингових атак і соціальної інженерії, дотримання політик безпеки при роботі з даними, використання надійних паролів і багатофакторної аутентифікації.

Співпраця з зовнішніми компаніями та фахівцями з кібербезпеки може допомогти в: проведенні регулярних тестів на проникнення, оцінці поточного рівня безпеки та рекомендаціях щодо покращення, реалізації систем моніторингу загроз та кіберзахисту.

Безпека платіжних систем є важливою для збереження довіри клієнтів: використання токенізації та шифрування для захисту фінансових транзакцій, впровадження 3D Secure та інших технологій для автентифікації користувачів під час онлайн-платежів [2; 3].

Стратегії захисту інформаційного середовища в електронній комерції повинні бути комплексними та включати різні рівні захисту – від технічних рішень до навчання співробітників. Важливо постійно адаптувати та вдосконалювати ці стратегії, оскільки загрози кібербезпеці змінюються і стають дедалі складнішими.

Список використаних джерел:

1. Ilchuk M., Kyrychenko A., Vodnitskyi M. Development of e-Commerce in Ukraine in the War and Post-War Conditions. *Science and Innovation*, 2023. №*19*(3), 3-14. URL: https://doi.org/10.15407/scine19.03.003

2. *Булах О. В.* Розвиток кібербезпеки в електронній комерції в умовах глобалізації. *Наукові записки Львівського університету бізнесу та права.* 2023. № 37, С. 298-306. URL: https://nzlubp.org.ua/index.php/journal/article/view/814/741

3. Кириченко А. В. Розвиток кібербезпеки у сфері електронної комерції. Кібербезпека та інноваційність фінансових інструментів на біржовому ринку: круглий стіл (Київ, 30 листопада 2023 р.). Київ: ВНЗ «Київський університет ринкових відносин». С. 29-31.

УДК 005:[378.147.091.3:004.056]

Логвиненко М.С
здобувач вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Єрмакова Н.А.
старший викладач кафедри інформаційних
технологій та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ ТА КІБЕРБЕЗПЕКА МАЙБУТНЬОГО МЕНЕДЖЕРА

Сучасна людина постійно взаємодіє з інформаційним середовищем, яке складається з інтернету, телебачення, електронних книг і комп'ютерних ігор. Інформація стає все більш важливою в її житті, пронизує всі аспекти діяльності та формує інформаційний спосіб існування. Інформаційне середовище – це світ інформації навколо людини і світ її інформаційної діяльності. Це сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням, споживанням інформації.

Введення карантину через пандемію COVID-19 та оголошення в Україні військового стану у зв’язку із повномасштабним вторгненням РФ стали причиною переходу професійної освіти та професійної діяльності українців до переважного використання дистанційної та змішаної форм організації цих процесів.

Таблиця 1.

Вимоги до інформаційного середовища

Людські ресурси - ІКТ-грамотність - Психологічна готовність - Наявність фахівців	Соціальні вимоги - Етичний аспект - Культурологічний аспект - Нормативно-правовий аспект
Академічні вимоги - Методичне наповнення -Відповідність навчальним програмам	Технічні вимоги - Комп’ютерна техніка - Об’єднання в мережу - Wi-Fi-технології
Програмні вимоги - Взаємодія - Питання безпеки	

Отже, професійна освіта та діяльність стали системою підготовки майбутніх фахівців, які працюють з інформаційними потоками в цифровому середовищі та вміють ефективно використовувати їх для якісного виконання нових професійних ролей і обов'язків. Вони здатні до безперервного особистісного, культурного, соціального та професійного розвитку протягом усього життя через формальну, неформальну та інформальну освіту.

На сьогоднішній день однією з найбільш популярних і затребуваних на ринку праці галузей діяльності є сфера управління. Саме тому професія менеджера (фахівця з управління) надзвичайно актуальна та має місце в різних напрямах діяльності компанії.

У сфері менеджменту працюють люди, які спілкуються, перебуваючи в різних часових поясах, і отримують доступ до важливої інформації звідусіль. Варто зазначити, що фахівці у сфері менеджменту можуть бути як найслабшою ланкою, так і першою лінією захисту. Відомо, що кіберзлочинці розробляють складні методи, щоб отримувати доступ до ресурсів, викрадати дані, саботувати роботу компаній або вимагати гроші. Ефективна програма з кібербезпеки включає фахівців, процеси й технологічні рішення, які разом зменшують ризик перерв у роботі компаній, фінансових втрат і підриву репутації внаслідок атак.

Саме тому компаніям варто інвестувати в їх навчання та впроваджувати ефективні системи захисту даних. Запорукою ефективного захисту даних та безпеки інфраструктури організації є дотримання трьох принципів інформаційної безпеки: конфіденційність, цілісність і доступність.

Отже, в сучасних умовах цифровізації та глобального використання інформаційних технологій захист інформаційного середовища стає однією з ключових задач у професійній діяльності менеджера. Оскільки менеджери мають справу з великим обсягом конфіденційної та стратегічної інформації, їх обов'язком є не лише управління процесами, а й забезпечення захисту даних.

Список використаних джерел:

1. Інформаційне середовище. [Електронний ресурс]. – Режим доступу: http://surl.li/hdqzhi
2. Навіщо вам кібергігієна? [Електронний ресурс]. – Режим доступу: https://osvita.diia.gov.ua/guides/naviso-vam-kibergigiena
3. Шевчук С. С. Інформаційне середовище як елемент цифрової дидактики професійної освіти. електронний ресурс [Електронний ресурс] / С. С. Шевчук. – 2023. – Режим доступу до ресурсу: https://lib.iitta.gov.ua/id/eprint/735783/1/%D0%A1%D1%82%D0%B0%D1%82%D1%82%D1%8F%20%D0%A8%D0%B5%D0%B2%D1%87%D1%83%D0%BA%20%D0%9C%D1%96%D0%B6%D1%80%D0%B5%D0%B3%20%D0%9D%D0%9F%D0%A1%2023.03.23.pdf
4. Що таке інформаційна безпека (InfoSec)?[Електронний ресурс]. – Режим доступу: http://surl.li/teqwve
5. Що таке кібербезпека?[Електронний ресурс]. – Режим доступу: http://surl.li/olealg

УДК 004.056.5

Микитенко В.І.
здобувач вищої освіти,
Науковий керівник
Черненко О.О.
кандидат фізико-математичних наук, доцент кафедри комп'ютерних наук та інформаційних технологій,
Полтавський університет економіки і торгівлі

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ІНСТРУМЕНТ КІБЕРАТАК: ВИКЛИКИ ТА ПРОТИДІЯ

На сьогодні соціальна інженерія залишається одним із найбільш небезпечних методів кібератак, тому що зазвичай саме люди являються найбільш вразливою ланкою системи безпеки. В умовах розвитку цифрових технологій та збільшення обсягів цифрової інформації, атаки на користувачів стають все частішим явищем. Зважаючи на важливість захисту конфіденційної інформації, тема вивчення методів соціальної інженерії та методів захисту від неї є надзвичайно актуальною як для компаній та організацій, так і для окремих користувачів.

Однією з основних вразливостей користувачів є недостатня обізнаність. Багато людей мало знайомі з поняттям "Соціальна інженерія". Також важливо знати про техніки та методи зловмисників. Більшість користувачів не вміє розрізняти фальшиві електронні листи або дзвінки. Найчастіше саме це дозволяє зловмисникам відносно легко заволодіти інформацією.

Ще однією вразливістю є довірливість. Люди схильні довіряти офіційним та авторитетним джерелам, не перевіряючи їхню оригінальність. Зловмисники, знаючи це, можуть видавати себе за працівників банків, правоохоронних органів або інших організацій, з якими жертва могла мати справу. Наприклад, шахраї можуть представлятися працівниками банку, і заявляти, що рахунок жертви в небезпеці. У стані стресу людина може випадково поділитися конфіденційною інформацією, не перевіривши достовірність запиту.

Третій важливий фактор вразливості – людський фактор. Помилки, спричинені поспіхом або неуважністю, є поширеними. Наприклад, необережні дії можуть призвести до необдуманих рішень, таких як натискання на підозрілі посилання або надання особистих даних. Саме на цю слабкість зазвичай орієнтуються зловмисники.

Методи соціальної інженерії можуть бути різними, проте найбільш поширеним є фішинг. Зловмисники надсилають підробні електронні листи або повідомлення, що імітують справжні організації. Метою таких повідомлень є змусити жертву розкрити конфіденційну інформацію, зокрема, паролі чи логіни. Часто такі листи містять посилання на сайти, які схожі на оригінальні, але є підробками.

Ще один популярний метод – претекстинг. Це метод, який передбачає створення приводу або ситуації для обману жертви з метою отримання приватної інформації. Наприклад, у 2016 році така атака була здійснена на бельгійський банк “Crelan Bank”. Зловмисники переконали працівника банку в тому, що він спілкується з керівництвом і змусили здійснити транзакції на суму близько 75 мільйонів євро на рахунки кіберзлочинців.

Для захисту від новітніх методів кібератак потрібно проводити низку заходів. Найбільш дієвим методом є навчання та підвищення обізнаності. Компанії, які піклуються про безпеку своїх даних і співробітників, повинні регулярно проводити тренінги. Під час таких тренінгів співробітникам варто пояснювати існуючі методи соціальної інженерії та способи їх розпізнавання. Практичні приклади повинні стати обов'язковою частиною таких програм. Додатковим рівнем захисту може бути багатофакторна автентифікація (MFA), яка значно ускладнює доступ до облікових записів навіть у випадку, коли зловмисник має логін і пароль.

Компанії також повинні розробляти чіткі процедури безпеки, що регламентують порядок доступу до конфіденційної інформації та обов'язкові дії працівників у випадку спроби несанкціонованого доступу. Регулярний моніторинг та аналіз мережевого трафіку допоможе своєчасно виявляти потенційні загрози або спроби несанкціонованого доступу. Наприклад, спроби входу в обліковий запис з незвичного місця можуть бути ознакою небезпеки, яку варто перевіряти.

Крім того, періодичні симуляції атак дозволять перевірити обізнаність працівників та готовність протистояти загрозам соціальної інженерії. Такі тести допоможуть виявити слабкі місця в системі безпеки та підвищити загальну безпеку організації.

Також можливо впровадити штучний інтелект для захисту від подібних атак. Можливості штучного інтелекту досить широкі і якщо його правильно навчити, він може стати одним із найкращих видів захисту від кібератак. Наприклад, його можна використовувати для аналізу вмісту, метаданих та структури електронних листів. Також штучний інтелект може допомогти розпізнати ознаки фішингових телефонних дзвінків. Аналізуючи голосові дані в реальному часі, він може виявити підозрілі патерни в діях або мовленні зловмисників.

Соціальна інженерія залишається одним із найбільш ефективних методів кібератак. Для захисту від такого виду атак необхідно не лише впроваджувати технологічні рішення, а й підвищувати власну обізнаність в цій сфері. Наприклад, бельгійський “Crelan Bank” після вдалої кібератаки провів розслідування та виявив, що це стало можливим через недбалість у перевірці автентичності запитів. Після цього випадку банк значно посилив заходи безпеки, впровадивши чіткий регламент перевірки фінансових запитів, навчання для працівників та багаторівневу автентифікацію. Статистика показує, що кібератаки здійснені з використанням методів соціальної інженерії

продовжують зростати. Згідно з дослідженням Verizon,у 2023 році такі становлять близько 74% всіх інцидентів, що пов’язані з витоком інформації.

Отже, впровадження багатофакторної автентифікації, використання штучного інтелекту, регулярний моніторинг мережі та підвищення обізнаності користувачів є ключовими аспектами, які дозволять мінімізувати ризики витоку інформації. Тільки комплексний підхід до захисту дозволить ефективно протистояти загрозам.

Список використаних джерел:

1.Соціальна інженерія: в аспекті забезпечення кібербезпеки. URL: https://bdut.co.ua/pro-nas/socialna-inzheneriya/

2. Бойко О. М. Розробка методології захисту інформації від атак соціальної інженерії : дипломна робота магістра за спеціальністю „125 — кібербезпека“ / О. М. Бойко. — Тернопіль : ТНТУ, 2020. — 63 с. URL: http://elartu.tntu.edu.ua/handle/lib/33576

3. Technology Services Group. The 3 most expensive phishing attacks in recent history. URL: https://www.tsg.com/insights/the-3-most-expensive-phishing-attacks-in-recent-history/

4. The HIPPA Journal. Verizon 2023 DBIR: Social engineering attacks increase; Ransomware plateaus. URL: https://www.hipaajournal.com/verizon-2023-data-breach-investigations-report/

УДК 65.012.8

Нарушкевич О.М.
здобувач вищої освіти
Національна академія Служби безпеки України

ТЕОРЕТИЧНІ ЗАСАДИ ОРГАНІЗАЦІЇ РОБОТИ РЕЖИМНО-СЕКРЕТНОГО ОРГАНУ

У сучасному світі, де інформація відіграє вагоме значення у забезпеченні національної безпеки та конкурентоспроможності держави, питання захисту секретних відомостей набуває особливої актуальності. Режимно-секретні органи (РСО) виступають невіддільними елементами в системі захисту державної таємниці, забезпечуючи комплексний підхід до організації та здійснення заходів щодо охорони секретної інформації. У контексті національної безпеки та захисту інтересів держави ключову роль відіграє концепція державної таємниці. Поняття охоплює широкий спектр інформації, яка має критичне значення для забезпечення суверенітету, територіальної цілісності та економічного розвитку країни. Розуміння сутності державної

таємниці є фундаментальним для ефективного функціонування державних інституцій, правоохоронних органів та спеціальних служб.

Державна таємниця являє собою особливий вид інформації з обмеженим доступом, розголошення якої може завдати шкоди національній безпеці та інтересам держави.

У доктринальній сфері існують різні підходи до розуміння державної таємниці. Наприклад, І. І. Трембач визначає державну таємницю як вид таємної (секретної) інформації, що має обмежений доступ у певних сферах відносин. Посягання на таку інформацію може спричинити шкоду національній безпеці держави [1, с. 230]. Цей підхід акцентує увагу на обмеженому доступі до інформації та потенційній шкоді, яку може завдати розголошення.

Державна таємниця вважається правовим інститутом, що дозволяє державі проводити незалежну політику, обстоювати власні інтереси і впливати на поведінку інших держав та перебіг міжнародних подій у бажаному для себе напрямі [2, с. 356]. Таке визначення підкреслює стратегічне значення державної таємниці для забезпечення суверенітету та національної безпеки.

Інші автори визначають державну таємницю як інформацію або певні відомості, несанкціонований доступ до яких може завдати шкоди інтересам держави [3, с. 14]. Наведене визначення акцентує на потенційній шкоді, яка виникає від розголошення інформації, що потребує захисту.

Законодавче визначення державної таємниці в Україні закріплено у статті 1 Закону України «Про державну таємницю» [4]. Згідно з даним нормативно-правовим актом, державна таємниця представляє собою особливий вид таємної інформації, що охоплює відомості у сферах оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку. Важливою характеристикою такої інформації є те, що її розголошення може завдати шкоди національній безпеці України. Крім того, така інформація має бути визнана державною таємницею у встановленому законом порядку та підлягає охороні з боку держави.

Ст. 2 Закону України «Про державну таємницю» зазначає, що регулювання відносин у сфері охорони державної таємниці здійснюється на основі Конституції України, законів України, зокрема Закону «Про інформацію» [5] та Закону «Про доступ до публічної інформації» [6], а також міжнародних договорів, які набули чинності на основі згоди Верховної Ради України та інших нормативно-правових актів.

Сутність державної таємниці полягає у забезпеченні інформаційної безпеки держави шляхом обмеження доступу до найбільш важливих відомостей, розголошення яких може завдати шкоди національним інтересам. Державна таємниця виступає інструментом захисту стратегічно важливої інформації у різних сферах державного управління та національної безпеки.

Аналіз концепції державної таємниці виявляє низку ключових аспектів, які потребують ретельного розгляду. В. М. Шлапаченко звертає увагу на некоректність формулювання «може завдати» у визначенні поняття державної таємниці. Науковець аргументує свою позицію тим, що така фраза допускає й

альтернативний сценарій – «може не завдати». Відтак, пропонується заміна на формулювання «завдає або створює загрозу завдання шкоди». Така пропозиція видається обґрунтованою, оскільки сам факт посягання на відомості, що становлять державну таємницю, вже передбачає завдання шкоди державним інтересам [7, с.43].

Закон України «Про державну таємницю» дозволяє виділити наступні характерні ознаки державної таємниці:

1. Надзвичайно важлива інформація.

2. Розголошення інформації потенційно шкодить державним інтересам.

3. Законодавче закріплення переліку інформації, яка може бути віднесена до державної таємниці.

4. Охорона інформації засобами адміністративної та кримінальної відповідальності.

5. Створення спеціального режиму таємності для охорони інформації [4].

Автор О. Шамсутдінов пропонує більш розширений перелік ознак державної таємниці, а саме:

1. Обмеженість доступу до державної таємниці як виду таємної інформації, що передбачає засекречування відомостей.

2. Значущість та важливість відомостей для інтересів держави у певний часовий проміжок, що обумовлює потенційну суттєву шкоду національній безпеці України у разі розголошення (матеріальний критерій).

3. Чітке визначення сфер існування державної таємниці: оборона, економіка, наука і техніка, зовнішні відносини, державна безпека й охорона правопорядку.

4. Законодавче визначення переліку відомостей, що становлять державну таємницю, у спеціальному правовому акті - Зводі (формальний критерій).

5. Державна охорона секретної інформації шляхом встановлення єдиного порядку забезпечення охорони на основі чинного законодавства [8, с.22-23].

В. І. Олійник, розглядаючи державну таємницю як кримінально-правове явище, виділяє такі ознаки:

1. Нормативне закріплення відомостей у певних сферах життя держави (оборона, економіка, наука й техніка, зовнішні відносини, державна безпека та охорона правопорядку).

2. Наявність відповідного грифу секретності та регламентованого порядку засекречування і розсекречування.

3. Обмеження доступу до відомостей лише особами, які мають відповідний допуск та зобов’язані зберігати таємницю.

4. Забезпечення недоторканності відомостей державним захистом та встановленою юридичною відповідальністю.

5. Потенційна шкода національним інтересам у разі незаконного отримання і поширення відомостей [9, с. 145].

Важливо відзначити, що всі дослідники підкреслюють значущість інформації, яка становить державну таємницю, для національних інтересів та безпеки держави. Також спільним є акцент на необхідності законодавчого

регулювання та встановлення спеціального режиму охорони такої інформації. У воєнний час в Україні захист державної таємниці набуває особливого значення. Впроваджується комплекс заходів для збереження конфіденційності важливої інформації та гарантування національної безпеки. Проводиться аналіз даних щодо їх значущості для безпеки держави, і найважливіша інформація отримує статус державної таємниці. Законодавча база України встановлює чіткі рамки та правила діяльності режимно-секретних органів, визначаючи їхні повноваження, обов'язки та відповідальність.

Основоположним документом, який регламентує діяльність режимно-секретних органів, є Закон України «Про державну таємницю» [4]. Відповідно до закону, режимно-секретні органи є невід'ємною частиною системи захисту державної таємниці та виконують функції контролю за дотриманням режиму секретності в установах, підприємствах та організаціях.

Важливим аспектом нормативно-правового регулювання є Постанова Кабінету Міністрів України "Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування на підприємствах, установах і організаціях. ДСК" [10]. Документ детально описує процедури створення та функціонування режимно-секретних органів, визначає їхню структуру, повноваження керівників та співробітників, а також встановлює вимоги до організації робочого процесу та документообігу.

Особливу увагу слід приділити нормативним актам, які регулюють порядок допуску та доступу до державної таємниці. Зокрема, Указ Президента України "Про Порядок здійснення криптографічного захисту інформації в Україні" [11] встановлює вимоги до захисту секретної інформації під час її обробки та передачі засобами зв'язку. Дотримання положень даного указу є обов'язковим для всіх режимно-секретних органів та сприяє забезпеченню належного рівня безпеки інформації з обмеженим доступом.

Нормативно-правова база також передбачає механізми контролю за діяльністю режимно-секретних органів. Закон України «Про Службу безпеки України» надає повноваження Службі безпеки України здійснювати контроль за станом охорони державної таємниці в усіх органах державної влади, підприємствах, установах та організаціях [12].

Відповідно до чинного законодавства, режимно-секретні органи створюються в державних органах, органах місцевого самоврядування, підприємствах, установах і організаціях, які провадять діяльність, пов'язану з державною таємницею. Правовий статус РСО визначається Положенням про режимно-секретний орган, яке затверджується керівником відповідного органу або установи за погодженням із Службою безпеки України.

Важливим аспектом нормативно-правового регулювання діяльності РСО є визначення критеріїв віднесення інформації до державної таємниці. Звід відомостей, що становлять державну таємницю, затверджується наказом Служби безпеки України та періодично переглядається з метою актуалізації переліку відомостей, які підлягають засекречуванню.

Законодавство також встановлює вимоги до працівників РСО, зокрема щодо їх професійної підготовки, морально-ділових якостей та відсутності обмежень на роботу з секретною інформацією. Процедура призначення на посади в РСО передбачає обов'язкове погодження кандидатур із Службою безпеки України.

Особливістю нормативно-правового регулювання діяльності РСО є наявність значної кількості відомчих нормативних актів, які деталізують загальні положення законодавства та враховують специфіку діяльності конкретних органів та установ. Координація діяльності РСО різних відомств здійснюється Службою безпеки України, яка також проводить перевірки стану охорони державної таємниці та дотримання режиму секретності.

Режим секретності є невід'ємною складовою системи захисту державної таємниці та інших видів інформації з обмеженим доступом. Його забезпечення вимагає комплексного підходу та врахування численних факторів, які впливають на ефективність захисту конфіденційної інформації.

Основні завдання у цій сфері спрямовані на попередження несанкціонованого доступу до даних, що можуть загрожувати національній безпеці або інтересам компанії. Специфіка роботи в режимно-секретних умовах потребує особливих методів і підходів, які враховують сучасні загрози та ризики.

Особлива увага приділяється людському фактору, адже співробітники, які мають доступ до секретних даних, можуть стати потенційною загрозою безпеці організації. Тому, важливим аспектом забезпечення режиму секретності є проведення ретельного відбору та підготовки персоналу. Співробітники проходять спеціальні навчальні курси, що включають ознайомлення з правилами обігу конфіденційної інформації, а також регулярні перевірки на наявність компрометуючих зв'язків або дій.

Іншим ключовим елементом є контроль за документами та інформаційними потоками. Ведення реєстрів секретних документів, встановлення чітких правил їх знищення або передачі іншим особам є обов'язковими умовами для ефективного функціонування режимно-секретного органу. Забезпечення прозорості й точності у цих процесах мінімізує ризики витоку інформації.

Забезпечення режиму секретності є комплексним процесом, що вимагає ретельного підходу до захисту конфіденційної інформації. Основними аспектами цього процесу є фізичний захист приміщень, контроль за документообігом, а також підготовка і відбір персоналу. Успішне забезпечення режиму секретності можливе лише за умов дотримання ключових принципів організації роботи режимно-секретного органу, таких як централізоване управління, комплексність, відповідальність, конфіденційність і безперервність. Безпека організації, що працює з конфіденційною інформацією, напряму залежить від здатності її керівництва інтегрувати в діяльність режимно-секретного органу сучасні методи захисту, відповідно до постійно змінюваних викликів та ризиків. У підсумку, реалізація надійного режиму

секретності є запорукою успішної діяльності організації та збереження її стратегічних інтересів.

Список використаних джерел:

1. Трембач, І.І. Поняття державної таємниці як об'єкта кримінально-правової охорони. *Актуальні проблеми вітчизняної юриспруденції*. 2017. Спецвипуск. Частина 1. С. 227-230.

2.Антонов, К.В. Проблеми правової охорони інституту державної таємниці у кримінальному провадженні. *Юрид. наук. електрон. журн*. 2020. №2. С. 355-358. URL: http://www.lsej.org.ua/2_2020/94.pdf.

3.Супруненко, А.М., Башта І. І., Лисеюк А. М., Свіріна К. С. Організація охорони державної таємниці в Україні: : навч. посіб. Ун-т ДФС.-Ірпінь: УДФСУ, 2020. 370с

4. Про державну таємницю : Закон України від 21 січня 1994 року № 3855-XII. Законодавство України URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення 02.09.2024).

5. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. Законодавство України URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 02.09.2024).

6. Про доступ до публічної інформації : Закон України від 13 січня 2011 року № 2939-VI. Законодавство України URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення 02.09.2024).

7. Шлапаченко, В. М. Шляхи удосконалення нормативно-правового визначення державної таємниці. Inf*ormation Security of the Persons, Society and State.* 2013. №3. С.41-14.

8. Шамсутдінов, О. Відповідальність за розголошення державної таємниці за новим кримінальним законодавством України. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник*. 2001. Вип.2. С. 21-25.

9. Олійник, В. І. Визначення родової належності поняття «державна таємниця. *Право і суспільство*. 2015. №5(2). С. 143-148.

10. Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування на підприємствах, установах і організаціях. ДСК: Постанова від 18 грудня 2013 р № 939.

11. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22 травня 1998 р. № 505/98. URL: https://zakon.rada.gov.ua/laws/show/505/98#Text

12. Про Службу безпеки України: Закон України від 25 березня 1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

УДК 004.056.53

Оченашко М. О.
здобувач ступеня доктора філософії,
Харківський національний університет радіоелектроніки
Науковий керівник
Гороховатський В.О.
д.т.н., професор, професор кафедри інформатики,
Харківський національний університет радіоелектроніки

ВПЛИВ GDPR НА ЗАХИСТ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ У ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩУ

Персональні дані користувачів використовуються більшістю сервісів, від соціальних мереж до охорони здоров'я та фінансових послуг. Ці дані, у більшості випадків, необхідні для надання різноманітних послуг. Оскільки компанії продовжують накопичувати величезні обсяги даних, вони стикаються зі зростаючим тиском щодо їх захисту не тільки для збереження своєї репутації, але й для дотримання суворих правових норм, таких як Загальний регламент про захист даних (GDPR).

GDPR, запроваджений у 2018 році, встановив суворіші вимоги щодо захисту даних, конфіденційності та безпеки. Згідно з регламентом, компанії зобов'язані впроваджувати відповідні технічні та організаційні заходи для забезпечення безпеки персональних даних, включаючи методи шифрування, токенізації, та псевдонімізації [1, 2].

Одним із ключових методів забезпечення відповідності GDPR та зменшення ризику витоку даних є токенізація. Замінюючи конфіденційні дані унікальним ідентифікатором або «токеном», компанії можуть ефективно захистити особисту інформацію, зберігаючи при цьому можливість використовувати її в операційних цілях. Токенізація змінює спосіб роботи з даними, мінімізуючи ймовірність витоку в разі кібератаки або злому.

Загрози для корпоративного інформаційного середовища. Інформаційне середовище, що складається з цифрових систем, які зберігають, обробляють і передають дані, стикається зі зростаючим набором загроз з розвитком технологій. Вразливості «нульового дня» становлять значні ризики, оскільки вони включають невідомі недоліки безпеки, якими користуються зловмисники до того, як з'являються патчі. Інсайдерські загрози ще більше ускладнюють безпеку, оскільки співробітники або підрядники можуть ненавмисно або навмисно скомпрометувати конфіденційну інформацію. Ці різноманітні загрози вимагають багаторівневого підходу до безпеки і забезпечення захисту даних користувачів.

Токенізація даних. Токенізація – це ефективний метод підвищення безпеки даних та забезпечення дотримання GDPR. Вона передбачає заміну конфіденційних даних, таких як персональні дані (PII), неконфіденційним еквівалентом, який називається токеном. Цей токен не має ніякої цінності або

значення поза конкретною системою, де він створюється і управляється, що робить його марним для зловмисників, якщо його перехоплять. На відміну від деяких видів шифрування, які допускають розшифрування за допомогою правильного ключа, токенізація повністю видаляє конфіденційні дані з системи компанії, зменшуючи ризики витоку.

Оскільки токени не вважаються персональними даними відповідно до GDPR, організації можуть токенізувати конфіденційні дані, продовжуючи використовувати токени для внутрішніх операцій, таких як аналітика, обслуговування клієнтів або обробка транзакцій, не порушуючи GDPR. Конфіденційна інформація зберігається окремо і безпечно, що мінімізує ризики, пов'язані з витоком даних або зловживанням ними [3].

Навіть якщо зловмисник отримає доступ до баз даних компанії, токени, які він знайде, не матимуть сенсу без доступу до відповідних даних, що зберігаються у сховищі токенів. Таке утримання конфіденційної інформації значно знижує ризик порушень GDPR, оскільки витік токенів не прирівнюється до витоку персональних даних [5]. Оскільки токени легко від'єднуються від конфіденційних даних, які вони представляють, організації можуть видалити персональні дані користувача за запитом без необхідності пошуку в декількох системах, що спрощує дотримання цього аспекту GDPR. Таким чином, токенізація мінімізує ризики витоку конфіденційних даних, зменшує обсяг регуляторного нагляду та спрощує управління персональними даними [4].

Приклад 1. Токенізація даних у фінансових організаціях. У секторі фінансових послуг захист конфіденційних платіжних даних є головним пріоритетом через високий ризик шахрайства та крадіжки персональних даних. Банки та фінтех-компанії щодня обробляють величезні обсяги персональної та фінансової інформації, включаючи номери кредитних карток, дані рахунків та історії транзакцій.

Токенізація стала ключовим рішенням для захисту платіжних даних у цій галузі. Замінюючи конфіденційні дані, такі як інформація про власника картки, випадково згенерованими токенами, банки та фінтех-компанії можуть обробляти платежі, не піддаючи оригінальні дані впливу хакерів. Наприклад, під час транзакції номер кредитної картки перетворюється на токен і зберігається в захищеному сховищі, а в процесі оплати використовується лише токен. Це гарантує, що навіть якщо систему буде зламано, викрадені дані не матимуть жодної цінності [1].

Приклад 2. Токенізація даних пацієнтів у сфері охорони здоров'я. Медичні організації керують дуже чутливими даними, включаючи медичні записи, діагнози та історії лікування, що робить їх головними мішенями для кібератак і витоків даних. Замінюючи конфіденційну медичну інформацію унікальними токенами, медичні працівники можуть безпечно зберігати та передавати записи, не розкриваючи реальні дані. Наприклад, під час зберігання записів пацієнтів або обміну ними між медичними установами, токенізовані дані гарантують, що будь-яка перехоплена інформація буде марною для несанкціонованих осіб.

Для токенізації часто використовують різні методи, такі як кодування, хешування, та оцінка інформативності, щоб підвищити безпеку та корисність даних. Хешування додає додатковий рівень захисту, генеруючи незворотні рядки фіксованої довжини з токенізованих даних. Оцінка інформативності гарантує, що токенізовані набори даних зберігають свою аналітичну цінність, залишаючись при цьому сумісними з правилами конфіденційності. [6-9]

Висновок. Загальний регламент про захист даних (GDPR) встановив новий глобальний стандарт конфіденційності даних, змушуючи організації впроваджувати більш ефективні практики безпеки для захисту даних користувачів. Токенізація, зокрема, пропонує високоефективний метод підвищення безпеки та досягнення відповідності вимогам. Замінюючи конфіденційні дані токенами, які не мають сенсу поза захищеною системою, компанії можуть значно знизити ризик витоку даних і мінімізувати ризик витоку особистої інформації.

Впровадження токенізації не тільки забезпечує відповідність суворим вимогам GDPR, таким як псевдонімізація та мінімізація даних, але й надає організаціям практичне рішення для безпечного управління даними в різних галузях. У сфері фінансових послуг, охорони здоров'я чи електронної комерції токенізація допомагає зменшити ризики кіберзагроз, дозволяючи компаніям продовжувати працювати ефективно та безпечно.

Список використаних джерел:

1. Data Sharing Under the General Data Protection Regulation / A. Vlahou et al. Hypertension. 2021. Vol. 77, no. 4. P. 1029–1035. URL: https://doi.org/10.1161/hypertensionaha.120.16340 (дата звернення: 22.09.2024).

2. General Data Protection Regulation (GDPR) Compliance Guidelines. GDPR.eu. URL: https://gdpr.eu/ (дата звернення: 22.09.2024).

3. IBM Minimizing application privacy risk. URL: https://developer.ibm.com/articles/s-gdpr3/ (дата звернення: 22.09.2024).

4. Knutsson M. Compliance with the General Data Protection Regulation: an exploratory case study on business systems' adaptation : thesis. 2017. URL: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-209772 (дата звернення: 23.09.2024).

5. Welch R. GDPR and Tokenizing Data (Part 3 in a Series) | TDWI. TDWI. URL: https://tdwi.org/articles/2018/06/06/biz-all-gdpr-and-tokenizing-data-3.aspx (дата звернення: 22.09.2024).

6. Gorokhovatsky, V. (2014), Structural Analysis and Intellectual Data Processing in Computer Vision, SMIT, Kharkiv, 316 p.

7. Gorokhovatskyi V. Vlasenko N. (2021), The image description reduction in the set of descriptors on informativeness metric criteria base. Advanced Information Systems, 5 (4), 10–16. doi: https://doi.org/10.20998/2522-9052.2021.4.02

8. Гороховатський В.О., Гадецька С.В., Стяглик Н.І. Вивчення статистичних властивостей моделі блочного подання для множини дескрипторів

ключових точок зображень. Радіоелектроніка, інформатика, управління. – 2019. – №2 . – С. 100–107.

9. Y. I. Daradkeh, V. Gorokhovatskyi, I. Tvoroshenko, and M. Zeghid. Improving the effectiveness of image classification structural methods by compressing the description according to the information content criterion. Computers, Materials & Continua 80.2 (2024): 3085-3106.

УДК 339.9; 339.97

Редзюк Є.В.
к.е.н., доцент, старший науковий співробітник
сектору міжнародних фінансових досліджень
ДУ «Інститут економіки та прогнозування НАН України», м.Київ

ІНФОРМАЦІЯ ТА ІНФОРМАЦІЙНИЙ ВПЛИВ В СУЧАСНИХ ГЕОПОЛІТИЧНИХ І ГЕОЕКОНОМІЧНИХ ВІДНОСИНАХ

Період 2000-2024 рр. – це епоха світового розвитку може бути охарактеризована як момент біфуркації, як етап переходу від індустріального суспільства до постіндустріального, інформаційного, медійного та орієнтованого на системне оновлення і використання знань. При цьому глобалізація, гармонійність міжнародних економічних відносин та демократичні процеси в світі знаходяться під тиском сучасних проблем, особливо, що стосується в отриманні неупередженої і правдивої інформації, яка під тиском олігархії, охлократії, неефективності державних інституцій суттєво деформується і спотворюється. В цьому аспекті дослідження процесів глобального політичного й економічного розвитку у взаємодії зі створенням інформації та впливом інформації на сучасне суспільство є актуальним та необхідним для більш безпечного і системного розвитку людства.

Визначення геополітики як науки про світову політику, що становить систему знань про контроль над географічним простором обумовлює замислитись про роль інформації та інформаційного забезпечення в цьому процесі. Тому, на наш погляд, необхідно розуміти, що сучасна геополітика – це дієвий зовнішньополітичний інститут держави в розумінні структур, механізмів, інструментів, за допомогою яких різні правлячі еліти певної країни намагаються розділити “зони впливу”, “зони безпеки”, “зони національних інтересів” тощо й у такий спосіб досягти влади та можливості контролю над процесами, що відбуваються на міжкраїнному, регіональному і на світовому рівнях. В той же час у класичному розумінні геополітика як наука – це державна доктрина (вчення, система теоретично обґрунтованих поглядів на суттєво

важливі ідеологічні, ціннісні, державницькі, суспільно-політичні, соціально-економічні та інші максими), котра ґрунтується на врахуванні конкретно-історичних форм впливу територіально-просторових умов країни на формування її статусу та політики в локальних, регіональних, континентальних та глобальних аспектах. І не завжди інтереси правлячих еліт певної країни співпадають з важливими ідеологічними, ціннісними, державницькими поглядами. Особливо це проявляється останнім часом в таких демократичних країнах світу, як США, Великобританія, країни ЄС. На відміну від них, автократичні і диктаторські країни (росія, Китай, Іран, КНДР) мають чітку ідеологію та систему (шкалу) цінностей, яких беззаперечно дотримуються завдяки відповідній пропаганді й державній системі управління інформаційними ресурсами. Таким чином з позиції геополітики завдяки інформаційним ресурсам, відсутності впливу олігархії, охлократії, чіткості у баченні певних проблем, автократичні і диктаторські країни завдяки інформаційному і фінансовому ресурсу в сучасному світі покращують розподіл і перерозподіл сфер впливу (центрів сили) різних держав і міждержавних об’єднань у багатовимірному геопросторі. Так, видно, що інформаційно-медійний вплив росії на країни ЄС і країни пострадянського простору має значний вплив на політичні процеси. Завдяки цьому впливу в країнах ЄС популяризуються крайні праві і крайні ліві рухи, що направлені на розкол, розбрат і дивергенцію в ЄС; на пострадянському просторі консервуються зручні режими для росії. Іранський вплив на Близькому Сході також спочатку пов’язаний з цілеспрямованою пропагандою, інформаційним налаштуванням на свої цінності, а вже потім відбуваються інші фінансово-мілітарні заходи, що приводять до низки конфліктів, воєн, терактів. Китай суттєво інтегрований в міжнародні економічні відносини, значна частка його експорту припадає на країни ЄС, США й інші країни демократичного світу, а тому він проводить більш м’яку інформаційну політику на зовні в порівнянні з внутрішніми інформаційними наративами і вказівками від центрального апарату комуністичної партії. Китай на противагу західним ЗМІ намагається в інформаційному просторі підтримувати і «розуміти» бачення автократичних і диктаторських партнерів у власних ЗМІ. Все це в комплексі останнім часом призвело до зниження рівня економічної співпраці між країнами світу, деглобалізації, регіоналізації з націленістю на співпрацю з країною зі схожими цінностями, а також посиленням протекціонізму [1;2].

В умовах, коли заангажовані традиційні ЗМІ (а в деяких країнах з нестійкими демократичними інституціями – олігархічні ЗМІ) включаються в політичні процеси; а крім того, до них долучаються певні успішні крупні бізнесмени, такі як Білл Гейтс, Марк Цукерберг та Ілон Маск, що належать не лише до найбагатших людей в історії людства. Вони також надзвичайно потужні в інформаційно-медійному аспекті – соціально, культурно та політично. Хоча це частково є відображенням соціального статусу, який сучасне суспільство надає багатству загалом, але такий статус може значно вплинути на реальні процеси і реальні проблеми. Ці конкретні мільярдери вважаються

геніями підприємництва, які демонструють унікальний рівень креативності, сміливості, далекоглядності та досвіду в широкому діапазоні тем. Потрібно врахувати й той факт, що багато з них контролюють основні засоби комунікації, а саме, ключові платформи соціальних мереж, що значно посилює їх вплив на соціальне середовище, як в країні, так і за її межами, чого не було ще в новітній історії. Якщо така людина помиляється, то мало хто і що може вплинути на неї. Їх зарозумілість, нестриманість, нерозсудливість й зухвалість в кращому випадку викривляють дійсність, а інколи їх хибне бачення можуть бути дуже руйнівними та соціально огидними. Для суспільства є сенс використовувати знання та мудрість тих, хто має досвід у певній темі, але контрпродуктивно підвищувати статус тих, хто вже має великий статус (і дуже старанно працює над його підвищенням) [3].

Крупні бізнесмени, олігархи і їх олігархічні ЗМІ, некомпетентні політики з маніпулятивними поглядами – руйнують демократичні інституції та суспільні цінності, а тому мають нести відповідальність, якщо зловживають величезним статусом, який їм надає багатство чи відповідна влада в умовах зростання нерівності. Це особливо вірно, коли вони використовують свій статус для просування власних економічних інтересів за рахунок інтересів інших або для поляризації і без того розділеного суспільства за допомогою провокаційної риторики чи поведінки, що шукає статусу.

Підсумовуючи, відзначимо, що незаангажована інформація та інституційно налаштований на потреби суспільства інформаційний ресурс є надважливим суспільним надбанням, який необхідно захищати й допускати до його формування тільки порядних, компетентних і високоосвічених фахівців. Разом з цим професійні стратегічно орієнтовані політичні еліти можуть вибудувати стійкі й незалежні ЗМІ до маніпуляцій й деструктивних впливів олігархічних кланів. Крім того, можливість маніпуляцій і впливів від автократичних й диктаторських країн має суттєво обмежуватись відповідним законодавством і оперативними безпековими заходами [4;5;6].

Список використаних джерел:

1. Бзежинський З. Велика шахівниця. Київ: Фабула. 2019. 288 с.
2. Stiglitz J. Globalization and Its Discontents. London : Penguin Books, 2002. 288 p.
3. Acemoglu D. Escaping the New Gilded Age. Project Syndicate. 2024. September 27. URL: https://www.project-syndicate.org/onpoint/wealth-inequality-billionaires-undue-influence-bad-for-society-by-daron-acemoglu-2024-09?utm_source=Project+Syndicate+Newsletter&utm_campaign=.....c20
4. Редзюк Є.В. Деолігархізація України – місія можлива? газета «Дзеркало тижня». Рубрика: Макрорівень. 09.06.2021 р. URL: https://zn.ua/ukr/macrolevel/deoliharkhizatsija-ukrajini-misija-mozhliva.html

5. Редзюк Є.В. Фінансово-економічні механізми та інструменти впливу на світогосподарські процеси. Наукові праці НДФІ. – 2021. – №4. – с. 34-47

6. Redziuk Y.V. 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

УДК 004.056.55

Ружицький К.В., Студенко А.В., Ігнатов О.Г.
здобувачі вищої освіти,
ННІ «Комп'ютерних наук та інформаційних технологій » НТУ «ХПІ»
Науковий керівник
Корольов Р.В.
к.т.н., доцент, доцент кафедри кібербезпеки
ННІ «Комп'ютерних наук та інформаційних технологій » НТУ «ХПІ»

РОЗРОБКА НЕЛІНІЙНОГО ФІЛЬТР-ГЕНЕРАТОРА НА ОСНОВІ ЛЕГКОВАГОВОГО ШИФРУ ASCON

На даний момент у світі розвиваються та все більше розповсюджуються "розумні" пристрої, будь то елементи інтернету речей (IoT) або RFID-технологій, яким в свою чергу необхідно обмінюватися інформацією з навколишньою середою. Виникає потреба у їх шифруванні для захисту від зловмисників, але тут постає проблема – зазвичай такі пристрої мають дуже високі обмеження на доступні ресурси: використання пам'яті, енергоспоживання та швидкість обробки інформації. І це лише основні пункти, залежно від поставленої цілі можуть додаватися й інші вимоги:

- Розмір пакетів даних;
- Тип з'єднання;
- Режимом роботи;
- Інші вимоги.

Тому необхідно йти на компроміс, баланс між безпекою, ефективністю та ціною, де досягнення усіх цілей є вкрай важкою задачею. Наприклад, можна реалізувати алгоритм який буде мати високу безпеку та ефективність, але при цьому виросте ціна його реалізації яка обумовлена збільшенням необхідної площі на кристалі пристрою. Або навпаки, зробити пристрій максимально дешевим з відносно невисоким рівнем безпеки та ефективності.

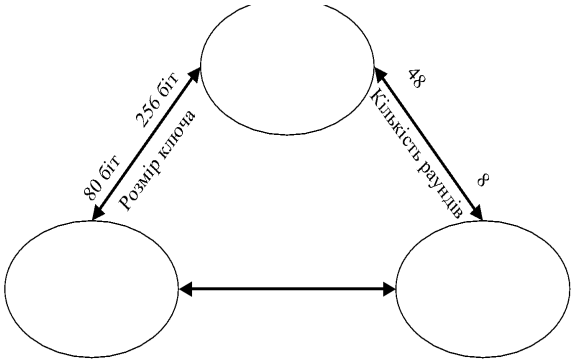


Рисунок 1 – Компроміс у криптографії

Метою даної роботи є формування псевдовипадкових послідовностей (ПВП) максимального періоду на базі регістрів зсуву з нелінійним зворотним зв'язком, де в якості функції ускладнення буде використаний легковаговий криптоалгоритм Ascon.

Як відомо, регістри зсуву з лінійним зворотним зв’язком (РЗЛЗЗ) прості у реалізації, швидкі, мають добрі статистичні властивості, але не вони не є криптостійкими і можуть бути використані лише як частина у будові системи. Існує декілька можливих варіантів, використання яких дозволило б подолати дану перешкоду, ми зупинилися на нелінійному методі. Який, в свою чергу, ділиться на:

- Нелінійний комбінуючий генератор – паралельно використовується декілька регістрів зсуву, після чого їх результат комбінується у функції;
- Нелінійний фільтр-генератор – використовуючи регістр генерує у нелінійній функції послідовність.

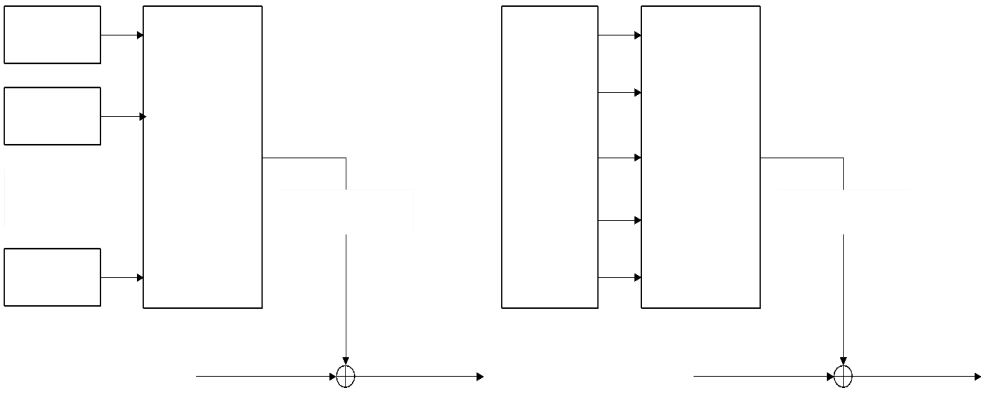


Рисунок 2 – Нелінійні генератори

Як можна зрозуміти, в таких генераторах ключовим елементом є функція *F* яка генерує потік послідовності. Вона може бути дуже простою, наприклад використовуючи операцію XOR, але звісно такий генератор буде легко піддаватися криптоаналізу.

В подальшому, аналізуючи можливості генераторів, у якості ускладнюючої функції *F* буде використано криптоалгоритм Ascon. Сімейство

Ascon – з 2023 року обране національним інститутом стандартів та технологій (NIST) як стандарт для приладів з обмеженими апаратними ресурсами.

Даний вибір обумовлений декількома факторами:

- Експеримент з легковаговим шифром, що станеться поєднавши його з нелінійним генератором та як які результати будуть отримані у кінці;
- По проведенню конкурсу від NIST у якому обирався новий стандарт у сфері, Ascon став його фіналістом і тим самим підтвердив свою ефективність та безпеку (згідно описаного вище компромісу);
- Дана комбінація, теоретично може дати легкий поточний шифр у якого буде сильна вихідна послідовність.

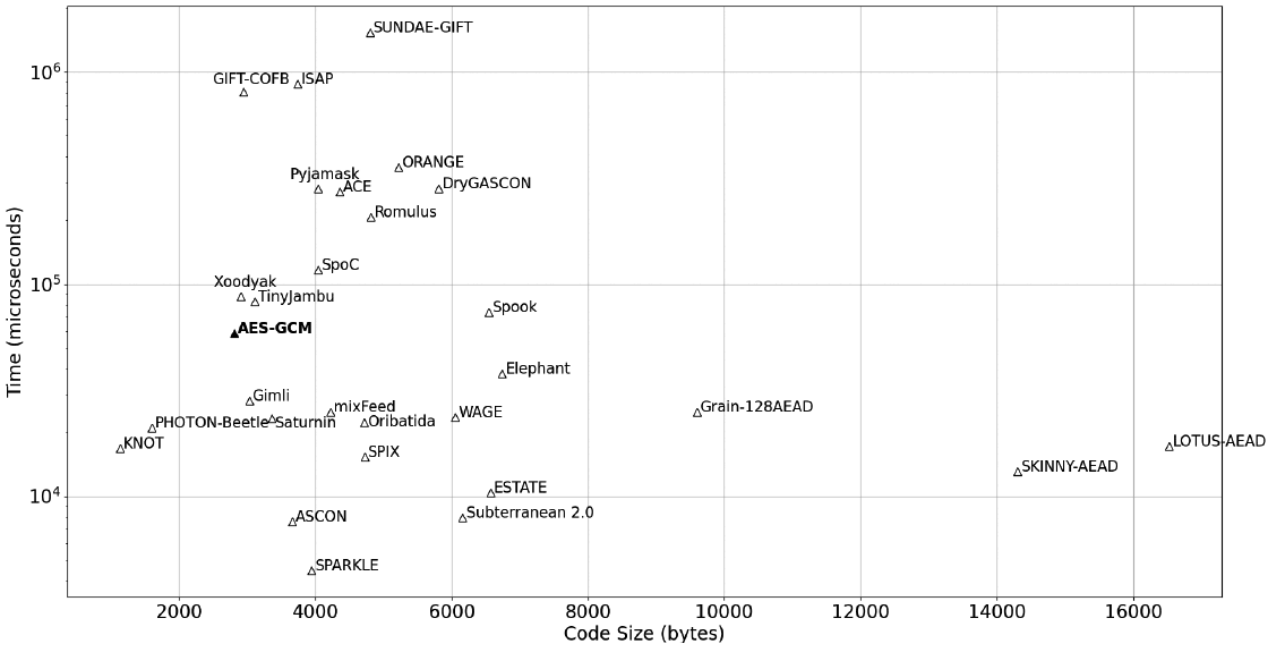


Рисунок 3 – Ефективність легковагових алгоритмів згідно NIST (Швидкість та розмір коду алгоритму)

В результаті даного дослідження буде отримано симетричний поточний шифр, та планується що він буде поєднувати в собі швидкість шифрування / дешифрування, ефективність у програмній та апаратній реалізації і високу криптостійкість. Дослідження вносить свою частку у аналіз генераторів псевдовипадкових послідовностей, легковагових криптоалгоритмів, поточних шифрів.

Список використаних джерел:

1. Теорія, застосування та оцінка якості генераторів псевдовипадкових послідовностей / [Іванов М. А. та Чугунков І. В.]. – М.:КУДИЦ-ОБРАЗ, 2003. – 240с.

2. Б. Шнайер Прикладна криптографія. Протоколи, алгоритми та вихідні тексти мовою Сі / Брюс Шнайер – Пер. з англ.: Видавництво Маяк, Одеса 2002. – 816с.

3. Поточні шифри: Результати зарубіжної відкритої криптографії / Анонім. –1997. – 400с.
4. NIST NISTIR 8369, named Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process, July 2021.
5. Блог Хабр – Легковагова криптографія. URL: https://habr.com/ru/companies/mvideo/articles/594369/

УДК 330.341

Фаткулін В.В.
здобувач вищої освіти, другий (магістерський) рівень 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

КІБЕРБЕЗПЕКА: ТЕХНОЛОГІЇ ТА ТРЕНДИ, ЩО ФОРМУЮТЬ СУЧАСНИЙ СТАН БЕЗПЕКИ

Кібербезпека - це сфера, що постійно розвивається, тому кіберзлочинці постійно адаптують свої навички та цілі відповідно до систем захисту. З розвитком технологій змінюються вектори атак кіберзлочинців та їхні засоби використання вразливостей.

Кібербезпека має вирішальне значення для захисту персональних і конфіденційних даних бізнесу та клієнтів. Жодна мережа не захищена від вторгнень, а витік даних і наслідки кіберзлочинів можуть дорого коштувати цим організаціям. Як зазначає PurpleSec, з 2021 року щорічні витрати на кібербезпеку зросли на 22,7%, а середня вартість витоку даних лише для малого бізнесу становить від 120 000 до 1,24 мільйона доларів США. [1]

Організації повинні покладатися на професіоналів з кібербезпеки, щоб підтримувати належний рівень захисту даних, за які вони несуть відповідальність. Ці фахівці повинні бути в курсі найновіших ресурсів, обізнаність про вектори загроз і останні тенденції в галузі кібербезпеки може допомогти їм підготуватися до кібератак на їхню організацію.

Топ-4 тренди кібербезпеки, про які потрібно знати. Незважаючи на зусилля, спрямовані на те, щоб привернути увагу підприємств до тенденцій кібербезпеки атаки на кібербезпеку продовжують поширюватися, особливо в останні роки в різних галузях промисловості. Кіберзлочинці досягають своїх цілей за допомогою складних методів, використовуючи переваги швидкої цифрової трансформації, яку переживає бізнес.

Як зазначає Івана Войнович, 70% малих підприємств не готові до нових загроз, а 88% досвідчених неетичних хакерів можуть проникнути в організації протягом 12 годин (2022 рік). Загальний збиток від кіберзлочинів у 2022 році

сягнув 6 трильйонів доларів США. [2]

Важливість безпеки в хмарних сервісах. Підприємства поступово переходять до мультихмарного або гібридного підходу, щоб оптимізувати витрати і зберегти важливі дані в межах компанії. Проте, це збільшує загрози кібербезпеки, оскільки хакери отримують більше можливостей для атак, зокрема через IoT і збереження медичних даних в хмарі. Основними викликами залишаються людські помилки і неправильні конфігурації. Підприємства повинні впроваджувати новітні технології, такі як багатофакторна автентифікація та штучний інтелект, щоб мінімізувати ризики атак і захистити свої хмарні рішення.

Загрози сучасних постійних атак (APT) є добре спланованими і дозволяють зловмисникам довго залишатися непоміченими в мережах, викрадаючи конфіденційну інформацію. Ці атаки можуть порушувати бізнес-операції та отримувати несанкціонований доступ до систем. APT військового класу особливо небезпечні для національних інфраструктур і урядових установ. Часто використовуються методи, такі як фішинг і соціальна інженерія. Щоб протистояти APT, підприємствам варто інвестувати в брандмауери, API-шлюзи та регулярно оновлювати свою інфраструктуру для захисту критичних систем.

Деякі APT є повномасштабними, а APT військового класу орієнтовані на національні інфраструктури та урядові установи. В аналітичному звіті про поточну кібервійну, з якою стикається Україна, «веб-вразливості та методи персистенції» були визначені як основні інциденти кібербезпеки у 2022 році через постійні атаки різних груп APT, спрямовані на «(перешкоджання) шпигунству та викраденню даних». [3]

Загрози безпеки в контексті метамережі швидко розвивається і до 2027 року може досягти ринкової вартості в 237 мільярдів доларів[4]. Користувацькі облікові записи в метапросторі стануть вразливими до підробок і крадіжок даних, особливо з огляду на зростаюче використання доповненої (AR) і віртуальної реальності (VR). Зловмисники можуть викрадати аватари та персональні дані, а також використовувати штучний інтелект для шахрайства. Технології на кшталт NLP, блокчейну і генеративного ШІ додають нових викликів для безпеки. Встановлення стандартів і використання машинного навчання може допомогти у боротьбі з цими загрозами.

Впровадження пост-квантової криптографії (PQC) необхідно для захисту інформаційної інфраструктури від загроз квантових комп'ютерів. Сучасні криптографічні алгоритми, такі як RSA та еліптична крива, можуть стати вразливими, коли квантові комп'ютери досягнуть достатньої потужності. Хоча такі комп'ютери ще не масові, розвиток технологій, зокрема процесори IBM на 433 і 1121 кубітів[5], наближає цю реальність. Організації на кшталт NIST [6] розробляють стандарти PQC, і планують публікації нових стандартів для стійкої криптографії. Деякі галузі, такі як телекомунікації, вже почали співпрацювати з експертами для оцінки впливу на телекомунікаційну галузь і необхідності «впровадження PQC для захисту мереж, пристроїв і систем» [7].

Як висновок кібербезпека має на меті забезпечити безпеку та конфіденційність даних і надає підприємствам гнучкість для обміну та передачі даних в Інтернеті, щоб зробити їхній бізнес більш прибутковим. Пропагуючи культуру кібер-обізнаності та впроваджуючи найкращі практики захисту особистої та ділової інформації, підприємства можуть випереджати час і проактивно захищати себе від нових кібер-загроз.

Обсяги та інтенсивність кібератак зростають, тому необхідно продовжувати оцінювати та вдосконалювати заходи безпеки, щоб зменшити будь-які ризики, які можуть завдати шкоди. Необхідно мотивувати фахівців до створення та проведення регулярних тренінгів з кібербезпеки та інформувати населення про нові ризики, пов'язані з впровадженням нових платформ і технологій нового покоління. Зрештою, готовність до кібербатаки не може бути досягнута за одну ніч.

Список використаних джерел

1. PurpleSec (2023). Cyber Security Statistics – The Ultimate List Of Stats, Data, & Trends For 2023. Взято з purplesec: https://purplesec.us/resources/cyber-security-statistics/#Cybercrime
2. Vojinovic, I. (2022, December 23).:More Than 70 Cybercrime Statistics – A $6 Trillion Problem.:Взято з DataProt: *https://dataprot.net/statistics/cybercrime-statistics/*
3. State Service of Special Communications and Information Protection of Ukraine, (2023, March 8). Russia's Cyber Tactics: Lessons Learned in 2022. Взято з: *https://cip.gov.ua/services/cm/api/attachment/download?id=53466*
4. Research and Markets (2023, January 25). Global Metaverse Market Report 2023: Market Value to Grow by Over $175 Billion from 2022 to 2027. Взято з: *https://www.globenewswire.com/en/news-release/2023/01/25/2594933/28124/en/Global-Metaverse-Market-Report-2023-Market-Value-to-Grow-by-Over-175-Billion-from-2022-to-2027.html*
5. IBM (2023). The IBM Quantum Development Roadmap. Взято з: *https://www.ibm.com/quantum/roadmap*
6. NIST, 2022. Post-Quantum Cryptography. Взято з: *https://csrc.nist.gov/projects/post-quantum-cryptography*
7. GSMA, 2023. Post Quantum Telco Network Impact Assessment Whitepaper. Взято з: *https://www.gsma.com/newsroom/wp-content/uploads//PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf*

УДК 004.056.53

Франчук В.Є.
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Науковий керівник
Петренко О.Є.
к.т.н., доцент, доцент кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки

КІБЕРБЕЗПЕКА ПІД ЧАС ВІЙНИ: ЯК ЗАХИСТИТИ ІНФОРМАЦІЮ НА ПОЛІ БОЮ

Сучасні військові конфлікти дедалі частіше супроводжуються кіберзагрозами, які можуть суттєво впливати на хід бойових дій. Кібербезпека стала невід'ємною частиною стратегічного управління військовими операціями, адже інформаційна перевага може вирішити результат війни. Актуальність цієї теми зростає у світлі останніх конфліктів, де кібератаки використовуються як ефективний інструмент війни. Метою даної роботи є оцінка важливості кібербезпеки для військових операцій та розробка стратегій захисту інформації на полі бою.

У сучасних війнах інформація стає такою ж цінною, як і бойова техніка. Зростання використання технологій, таких як дрони, супутникові системи та мережеві комунікації, відкриває нові можливості, але й створює нові ризики. Кібератаки можуть призвести до компрометації стратегічних даних, збоїв у системах управління та втрати контролю над військовими ресурсами. Приклади таких атак вже були зафіксовані у численних конфліктах, що підтверджує їхню небезпеку.

Важливість інформаційної переваги: успішні військові операції значною мірою залежать від здатності командування отримувати, обробляти та використовувати інформацію. Кіберзагрози можуть суттєво знизити цю можливість. Наприклад, атака на системи зв'язку може завадити виконанню завдань. У зв'язку з цим, забезпечення інформаційної безпеки є критично важливою для підтримки оперативної готовності та стратегічного планування.

Для ефективного захисту інформації на полі бою військові структури повинні розробити та реалізувати комплексні стратегії кібербезпеки. До основних аспектів таких стратегій відносяться:

1. Аналіз ризиків, який полягає в оцінці потенційних загроз і вразливостей систем, що використовуються під час операцій.

2. Впровадження технологій, таких як шифрування даних, захищені канали зв'язку, системи моніторингу та виявлення загроз.

3. Навчання персоналу, тобто регулярне навчання військовослужбовців щодо кіберзагроз, їх виявлення та реакції на них.

4. Співпраця з партнерами, це взаємодія з міжнародними організаціями та союзниками для обміну інформацією про кіберзагрози та найкращі практики.

5. Розробка планів реагування – створення чітких процедур для швидкого реагування на кіберінциденти та мінімізації їхніх наслідків.

Особливу увагу можна приділити до мереж Байєса – це потужний інструмент для моделювання й аналізу ймовірнісних зв'язків між змінними, що може бути особливо корисним у сфері кібербезпеки, зокрема у військових операціях. Ось кілька способів, як ці концепції можуть бути пов'язані.

Мережі Байеса можуть допомогти в оцінці ризиків, пов'язаних із кібератаками. Вони дозволяють створювати моделі, що описують ймовірність виникнення різних загроз на основі попередніх інцидентів. Це може включати:

- ідентифікацію ймовірності певних типів атак (наприклад, фішинг, DDoS);
- аналіз вразливостей систем, що використовуються у військових операціях.

Завдяки можливостям мереж Байеса, можна моделювати наслідки кібератак для різних військових операцій. Наприклад, можна прогнозувати, як певна атака вплине на здатність виконати завдання або на бойові втрати. Це дозволяє військовим планувальникам оцінити альтернативні стратегії.

Мережі Байеса можуть бути використані для виявлення аномалій у трафіку даних. Зібрані дані можуть бути проаналізовані для виявлення патернів, що свідчать про потенційні атаки. Наприклад, якщо система виявляє відхилення від звичного трафіку, це може сигналізувати про наявність кібератаки. У військових операціях важливо приймати обґрунтовані рішення в умовах невизначеності. Мережі Байеса допомагають моделювати різні сценарії розвитку подій, що дозволяє командуванню оцінити ймовірність успіху або невдачі різних рішень. Це може включати вибір стратегії кіберзахисту або реагування на кібератаку.

Отже, інтеграція мереж Байеса у стратегії кібербезпеки військових може суттєво підвищити ефективність захисту інформації. Вони дозволяють більш точно оцінювати ризики, прогнозувати наслідки та приймати обґрунтовані рішення в умовах невизначеності, що є критично важливим у сучасних бойових умовах. Кібербезпека у часи війни є важливим елементом, що впливає на ефективність військових операцій. У сучасному світі, де інформаційні технології грають вирішальну роль у військовій справі, зусилля з захисту інформації стають критично важливими. Реалізація стратегій кібербезпеки не лише підвищує обороноздатність, але й забезпечує збереження інформаційної переваги на полі бою. У зв'язку з цим, розвиток кіберзахисту має стати пріоритетом для військових структур, що прагнуть до успіху у сучасних конфліктах.

Список використаних джерел:

1. Richard A. Clarke, Robert K. Knake. "Cyber War: The Next Threat to National Security and What to Do About It" / HarperCollins Publishers – 2012.
2. Платформа навчальних курсів EdX. URL: https://www.edx.org/

3. "Bayesian Networks: A Practical Guide to Applications" (Olivier Pourret, Patrick Naim, Bruce Marcot / Wiley – 2008.
УДК 004.72:657.37

Шабалтас В.Я.
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

ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ КЛІЄНТІВ БАНКУ

З поширенням популярності цифрових банківських послуг та збільшенням фінансових транзакцій, кіберзагрози стали невід'ємним викликом для банківської структури. Витоки даних, фішинг, кібератаки є реальними загрозами для збереження конфіденційності інформації про клієнтів. Загальні методи захисту, такі як шифрування або багатофакторна автентифікація, хоча і є дуже важливими, але часто вони недостатні для запобігання новітнім викликам та загрозам.

Технологія блокчейн дозволяє створити захищений процес обміну даними між фінансовими установами, тим самим надаючи високий рівень довіри, мінімізуючи ризики, пов'язані з багатьма факторами. Верифікація користувачів через блокчейн сприяє надійності ідентифікації клієнтів, захищаючи їх від підробки даних.

Блокчейн, як децентралізована технологія зберігання даних, має декілька важливих властивостей, які роблять його ідеальним для захисту інформації клієнтів банку:

1. *Децентралізація*: відсутність центрального вузла для зберігання даних, що підвищує стійкість системи до кібератак
2. *Оригінальність*: після запису інформації в блокчейн її неможливо змінити, що унеможливлює будь-яку підробку даних клієнтів.

Кожен клієнт має власний криптографічний захищений блок, у якому зберігається інформація про деталі банківських операцій. Ключі для доступу до даних розподіляються між різними вузлами мережі, що в рази ускладнює несанкціонований доступ до даних користувачів.

Модель блокчейну для захисту персональних даних клієнтів банку буде виглядати наступним чином (рис. 1):

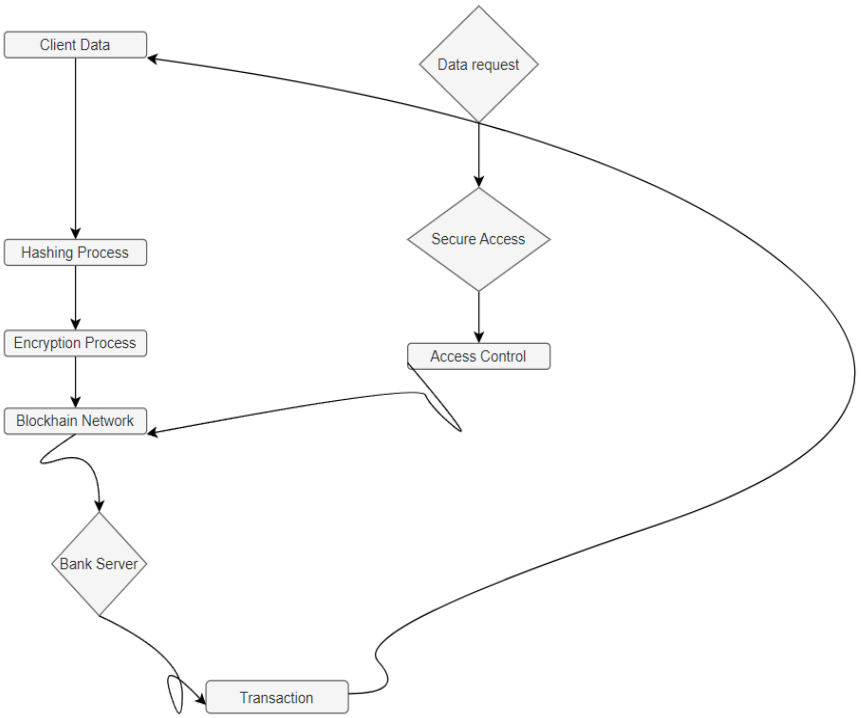


Рисунок 1 – Модель блокчейну для захисту персональних даних клієнтів банку

Власне блокчейн-технологія має потенціал бути однією з найбільш надійних систем захисту конфіденційних даних у банківській сфері завдяки децентралізації і оригінальності своїх записів. Юридичні та технічні аспекти потребують подальших досліджень для забезпечення постійної стабільності системи до будь-яких викликів, які можуть нести загрозу.

Список використаних джерел:

1. CrosbyM. Blockchain Technology/ Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman. // Berkeley Education, Sutardja Center for Entrepreneurship & Technology Technical

2. Binance Academy. URL: http://surl.li/ownuiu

3. H-X. URL: http://surl.li/bphilt

УДК 004.056.53

Штонда О.А.
здобувач фахової передвищої освіти
Харківський радіотехнічний фаховий коледж
Науковий керівник:
Радченко О.П.
викладач
Харківський радіотехнічний фаховий коледж

ЗАСОБИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ БАНКУ

Тема кіберзахисту в Україні у 2024 році є вкрай важливою через зростаючі кіберзагрози, які загрожують як державним установам, так і приватному сектору, особливо фінансовим організаціям. В умовах війни і посилених гібридних атак, захист критичної інфраструктури та банківських систем стає ключовим елементом національної безпеки. Інвестування в кібербезпеку та впровадження сучасних технологій є необхідними для збереження стабільності фінансової системи та економіки країни.

Основними тенденціями банківської цифровізації в Україні наразі є: оптимізація віддаленої роботи працівників банку, збільшення кількості операцій, що відбуваються онлайн, спрощення доступу до банківських послуг, програми тотальної персоніфікації, розробка власного програмного забезпечення, такого як, наприклад, розробка мобільного додатку, за допомогою якого клієнту банку можуть швидко надавати доступ до його рахунків та можливих операцій із ними.

Саме через такий швидкий розвиток цифрового банкінгу з’являється потреба банків у створенні систем захисту від зловмисників.

Безпека інформаційних технологій полягає у захисті від хакерів, шкідливого програмного забезпечення, фішингу, та інших можливих загроз. Безпека інформаційних технологій банку полягає у забезпеченні безпеки банківських процесів, насамперед забезпечення безперервності роботи банків та відділень.

Забезпечення безпеки банків регулюється за допомогою міжнародних та державних стандартів, правових положень. Найпопулярнішим стандартом є ISO/IEC 21001 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги». Цей стандарт використовується зацікавленими сторонами для оцінки можливості організацій відповідати власним вимогам щодо інформаційної безпеки. Тому банки зацікавлені у розробці якісного та безпечного програмного забезпечення.

Діями для покращення кіберзахисту інформаційних технологій банку є:

1. Використання технологій шифрування даних, таких як SSL/TLS-протоколи, які шифрують дані, які передаються між клієнтом та банком.
2. Використання алгоритмів кодування даних, таких як

AES-шифрування, який є найнадійнішим у світі.

3. Використання двофакторної аутентифікації, яка, у випадку, якщо клієнт банку втратив доступ до пристрою, який пов’язаний із банком, не дає зловмисникам доступ до рахунку клієнта.

Національний банк України має велику кількість норм та постанов, які регулюють роботу відділів кібербезпеки НБУ, в особливості «Постанова про затвердження Положення про організацію кіберзахисту в банківській системі України». Ця постанова дає змогу CRIST-NBU (Computer Security Incident Response Team of the National Bank of Ukraine) контактувати із кібервідділами банків України та збирати інформацію для подальшого моніторингу та реагування на кіберінциденти у банківській сфері України.

Місія цього підрозділу полягає у впровадженні найкращих європейських та світових практик, а також міжнародних і національних стандартів у сфері кіберзахисту та інформаційної безпеки. Вона спрямована на розвиток та вдосконалення систем і засобів для забезпечення кібербезпеки, а також на налагодження комунікації, координації та співпраці між учасниками системи кіберзахисту із обов’язковою організацією обміну інформацією про кіберзагрози, атаки та інциденти. Підрозділ також відповідає за функціонування Команди реагування на кіберінциденти в банківському секторі України (CSIRT-NBU).

Ключовими завданнями підрозділу є:

- моніторинг, виявлення та реагування на кіберінциденти у фінансовій сфері, збір і аналіз відповідних даних;
- дослідження сучасних кіберзагроз, аналіз шкідливого програмного забезпечення, створення індикаторів загроз та розробка рекомендацій для їхнього запобігання;
- оперативне інформування учасників кіберзахисту про спроби кібератак та поширення інформації про індикатори загроз;
- консультування фінансового сектору щодо організації кіберзахисту, реагування на кіберінциденти та подолання їх наслідків;
- підготовка рекомендацій щодо забезпечення інформаційної та кібербезпеки;
- співпраця та обмін інформацією з міжнародними організаціями та зовнішніми джерелами у питаннях протидії кіберзагрозам.

Здебільшого зловмисники використовують такі засоби для створення загрози банку:

1 Фішинг та соц. інженерія. За допомогою цього методу зловмисники можуть отримати персональні дані для проникнення до банківського рахунку жертви, або для того, щоб отримати доступ до працівника банку, який має більші права, чим звичайний користувач банку.

2 Зловмисне програмне забезпечення. Це можуть бути віруси, які можуть шифрувати дані та вимагати викуп за них.

3 DDoS-атаки. Такі атаки можуть перенавантажувати систему та виводити її з ладу, чим призводять до подальших витрат.

4 Атаки зсередини. Співробітники або підрядники, що мають доступ до критичних даних, можуть ненавмисно або навмисно сприяти кібератакам, передаючи конфіденційну інформацію або зловживаючи своїм доступом.

5 Скімінг. Це спосіб викрадення банківських даних за допомогою встановлення пристроїв на банкоматах або терміналах для оплати.

Отже, фінансовий сектор є однією з найбільш привабливих цілей для кіберзлочинців через високу концентрацію фінансових та персональних даних, методи проникнення у банківські системи постійно покращуються, тому сфера кіберзахисту цього сектору є надзвичайно важливою та вимагає постійної роботи та покращення різного виду спеціалістами.

Список використаних джерел:

1. «Команда НБУ стала частиною міжнародної спільноти з протидії кіберзагрозам» – https://bank.gov.ua/ua/news/all/komanda-nbu-stala-chastinoyu-mijnarodnoyi-spilnoti-z-protidiyi-kiberzagrozam.

2. «Національний банк України та Міністерство фінансів США продовжують обмін досвідом у сфері кібербезпеки» – https://bank.gov.ua/ua/news/all/natsionalniy-bank-ukrayini-ta-ministerstvo-finansiv-ssha-prodovjat-obmin-dosvidom-u-sferi-kiberbezpeki

3. Гончаренко, І. (2023). КІБЕРЗАГРОЗИ ФІНАНСОВОГО СЕКТОРА В УМОВАХ ВІЙНИ. Економіка та суспільство, (50). https://doi.org/10.32782/2524-0072/2023-50-82

4. Кіберзахист банківської системи України в умовах цифрових трансформацій. Наукові праці Таврійського державного агротехнологічного університету імені Дмитра Моторного (економічні науки). 2023. Вип. 1, № 47. С. 151–163. https://doi.org/10.31388/2519-884x-2023-47-151-163.

РОЗДІЛ 2.

ТЕХНІЧНІ СКЛАДОВІ ПРОЄКТУВАННЯ, РОЗРОБКИ, ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ І МЕРЕЖ

UDC 004.451

Pozharov Artem
student of higher education,
NNI "Karazinsky Banking Institute" KhNU named after V.N. Karazin
Chekanova Nataliia
Ph.D., Associate Professor, Associate Professor of the Department
of Information Technologies and mathematical modeling
NNI "Karazinsky Banking Institute" KhNU named after V.N. Karazin

RESEARCH OF DESKTOP OPERATING SYSTEMS IN THE CONTEXT OF SYSTEM ADMINISTRATION WITH A FOCUS ON SECURITY

The topic of selecting desktop operating systems in system administration is highly relevant in modern conditions, where increasing digitalization demands stable and secure corporate infrastructures. The choice of an operating system (OS) for workstations significantly impacts security, performance, compatibility with corporate software, and the ease of administration and scalability of the infrastructure.

Modern organizations utilize various desktop operating systems, including:

- Windows: A widely used OS [1] known for its compatibility with corporate applications and a multi-layered approach to protection using technologies like BitLocker and Windows Defender Application Control.
- macOS: Recognized for its security features such as System Integrity Protection (SIP), which safeguards system files and settings from unauthorized changes.
- Ubuntu: A popular UNIX-like OS [1] offering open-source solutions and tools like AppArmor and SELinux to protect against accidental user actions.
- Chrome OS: Oriented towards cloud computing with a built-in security architecture [2] that includes process and cross-environmental isolation [4][5] and user access restrictions.

Each of these operating systems presents different approaches to providing security and functionality in a corporate environment. They offer unique features for integrating with corporate software such as Microsoft 365, Intune, Adobe Creative Cloud, and Active Directory. Performance assessments using benchmarks like Geekbench help determine which OS is best suited for different corporate environments.

Therefore, the selection of an operating system should be made considering the specific needs and requirements of the organization, including protection against incorrect user actions [3], integration capabilities with local and cloud infrastructures, performance, and future development trends.

System administrators should be aware of the importance of choosing the appropriate OS and be responsible for ensuring it aligns with the organization's goals and security policies.

References

1. Statcounter Global Stats. "Operating Systems: Market Share Worldwide." URL: https://gs.statcounter.com. Data as of September 2024.
2. "The Most Secure OS Out of the Box." URL: https://services.google.com/fh/files/misc/chromeos-the-most-secure-os-out-of-the-box.pdf.
3. SunTimes. "Barmin's Patch Can Damage UEFI." URL: https://suntimes.com.ua/didzhytal/patch-barmina-mozhe-poshkoditi-uefi.html.
4. "Linux on Chrome OS." URL: https://chromeos.dev/en/linux.
5. "Android Apps on Chrome OS." URL: https://chromeos.dev/en/android.

УДК 004.02

Волков В.С.
здобувач вищої освіти,
Науковий керівник
Олексійчук Ю.Ф.
к. ф.-м. н., доцент кафедри комп'ютерних наук та інформаційних технологій
Полтавський університет економіки і торгівлі

ECMA-262 ТА JAVASCRIPT: ЯК ВІДКРИТІ СТАНДАРТИ ФОРМУЮТЬ СУЧАСНУ РОЗРОБКУ

Багато розробників не замислюються над тим, що технології, з якими вони працюють щодня, є реалізаціями відкритих специфікацій. Ці стандарти створюються міжнародними організаціями у співпраці з індивідуальними розробниками та великими компаніями, а потім публікуються у відкритому доступі для використання в різних цілях. Тому, розуміння принципів цих стандартів не лише покращує володіння технологіями на яких вони побудовані, але й відкриває перед розробником безліч можливостей.

JavaScript, одна з найпопулярніших мов програмування, є реалізацією специфікації ECMA-262. Цей стандарт детально описує синтаксис мови, управління пам'яттю, обробку помилок та взаємодію з різними середовищами виконання. Завдяки цій специфікації всі реалізації JavaScript, незалежно від платформи, зберігають сумісність і передбачуваність роботи. Це особливо важливо в умовах сучасної веб-розробки, де одна програма може працювати на безлічі пристроїв і браузерів, що вимагає єдиного стандарту для гарантії однакової поведінки коду.

Прикладом успішної реалізації ECMA-262 є рушій V8, розроблений компанією Google для браузера Chrome. V8 не тільки забезпечує високопродуктивну обробку JavaScript, але й постійно вдосконалюється для підтримки нових версій стандарту. Завдяки суворому дотриманню специфікацій, V8 гарантує, що код, написаний розробниками, працюватиме

однаково незалежно від середовища виконання, будь то браузер чи сервер. Крім того, цей рушій дозволяє оптимізувати виконання JavaScript-коду, підвищуючи продуктивність веб-додатків і забезпечуючи швидкий відгук інтерфейсів користувача.

Відкритість специфікацій і рушіїв на зразок V8 відкриває перед розробниками великі можливості для створення інноваційних продуктів. Наприклад, платформа Node.js, побудована на основі V8, стала революційним інструментом для серверної розробки. Вона дозволила використовувати JavaScript не тільки в браузерах, але й на стороні сервера, що значно розширило сферу його застосування. Це яскраво демонструє, як відкриті стандарти та технології сприяють появі нових рішень, прискорюючи розвиток екосистеми JavaScript та відкриваючи нові горизонти для розробників.

Можливості специфікацій значно виходять за межі класичної веб-розробки. JavaScript застосовується у вбудованих системах, інтернеті речей (IoT), а також для створення "розумного дому". Стандартизація на основі ECMA-262 забезпечує гнучкість мови, дозволяючи інтегрувати її у різноманітні технологічні рішення. Це включає програмування пристроїв, керування сенсорами та автоматизацію різних процесів. Така універсальність JavaScript не лише спрощує розробку, але й сприяє швидкому впровадженню інновацій, роблячи його ключовим інструментом для створення сучасних технологій, які змінюють наше повсякденне життя.

Отже, стандартизація JavaScript на основі ECMA-262 є важливим елементом розвитку сучасних технологій. Відкриті специфікації не лише забезпечують сумісність і передбачуваність роботи програм у різних середовищах, але й створюють основу для інновацій. Завдяки таким технологіям, як рушій V8 та платформа Node.js, JavaScript вийшов далеко за межі браузерів, відкривши можливості для серверної розробки, вбудованих систем та IoT. Універсальність і відкритість цієї мови роблять її ключовим інструментом для майбутніх технологічних досягнень, сприяючи розвитку як окремих програмістів, так і всієї галузі загалом.

Список використаних джерел:

1. Специфікація ECMA-262. URL: https://ecma-international.org/
2. Документація JavaScript. URL: developer.mozilla.org/
3. Документація V8. URL: https://v8.dev/
4. Документація Node.js. URL: https://nodejs.org/

УДК 005.81:004

Глушко Р.О.
Здобувач вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Науковий керівник
Кобилін А.М.
к.т.н., доцент, доцент кафедри інформаційних технологій
та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ТЕХНІЧНІ СКЛАДОВІ ПРОЄКТУВАННЯ, РОЗРОБКИ, ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ІТ-РІШЕНЬ

ІТ-індустрія, що колись була нішевим явищем, сьогодні пронизує всі сфери нашого життя. Від виникнення перших електронно-обчислювальних машин до сучасних хмарних платформ і штучного інтелекту, шлях розвитку програмної інженерії був довгим і тернистим. Сьогодні ми стоїмо на порозі нової ери, де технології розвиваються з небувалою швидкістю. Розробка проєктів стає дедалі складнішим і багатоаспектним завданням. Проєктний менеджер відіграє ключову роль у цьому процесі, координуючи роботу команди, слідуючи цілям і завданням проєкту, і забезпечуючи зв’язок між усіма учасниками. Для успішного управління розробкою проєкту важливо чітко розуміти всі етапи, з якими доведеться зіткнутися. Тому пропоную спочатку розглянути види проєктів, а потім окремі складові цих проєктів, а саме: проєктування, розробка, впровадження, використання.

За складністю проекти поділяються на монопроекти, малі проекти та мегапроекти.

Монопроект – це окремий проект певного виду і масштабу

Мультипроект – це комплексний проект, який складається з декількох монопроектів, що вимагає багатопроєктного управління.

Мегапроект – це комплексний проект розвитку регіони секторів економіки тощо, який складається з декількох монопроектів та мультипроектів, об'єднаних однією метою.

За якістю проекти поділяються на звичайної якості та бездефектні. На відміну від звичайних до бездефектних проєктів висуваються особливі вимоги щодо якості. їх вартість може бути значною. За тривалістю проекти поділяються на короткострокові (до 3 років), середньострокові (від 3 до 5 років) та довгострокові (більше 5 років).

Розглянемо технічні складові проєктування. Дамо визначення «проєктування в ІТ» – це процес створення технічної архітектури програмного забезпечення або інформаційної системи. Він містить в собі різні технічні складові, які допомагають ІТ-спеціалістам впроваджувати проєкти відповідно до вимог. Основні складові:

- Аналіз вимог: Збір вимог від замовника або користувачів. Це можуть бути функціональні та нефункціональні вимоги, такі як безпека, швидкодія, надійність тощо.
- Технічні вимоги: Опис інструментів, технологій, платформ та інфраструктури, які будуть використовуватися в проєкті.
- Архітектура системи: Розробка високорівневої схеми роботи системи (клієнт-сервер, мікросервіси, моноліт тощо).
- Моделювання: Використання UML або інших діаграм для візуалізації системи та її компонентів (схеми даних, потоки користувачів тощо).

Розглянемо технічні складові розробки. Дамо визначення «технічні складові розробки» – це фундаментальні елементи, які визначають структуру, функціональність та ефективність будь-якого програмного продукту.Основні складові:

- Програмування: Написання коду на обраних мовах програмування (Python, Java, C#, C++, PHP, Pascal, JavaScript).
- Контроль версій: Використання систем контролю версій (наприклад, Git) для збереження та відстеження змін у коді.
- Інтеграція: Об'єднання різних модулів або сервісів у єдину систему, забезпечуючи їхню взаємодію.
- Тестування: Використання автоматизованих та ручних методів тестування для перевірки якості коду. Можуть використовуватися юніт-тести, інтеграційні та системні тести.

Розглянемо технічні складові впровадження. Дамо визначення «технічні складові впровадження» – це сукупність елементів, процесів та інструментів, які необхідні для успішної реалізації IT-проекту. Вони охоплюють весь цикл розвитку програмного забезпечення, від початкової концепції до запуску та подальшої підтримки. Основні складові:

- Деплоймент: Перенесення системи на реальні сервери або хмарні платформи. Можливе використання CI/CD (безперервна інтеграція та розгортання) для автоматизації цього процесу.
- Налаштування інфраструктури: Налаштування серверів, баз даних, мереж та інших компонентів інфраструктури для стабільної роботи системи.
- Міграція даних: Якщо нова система замінює стару, потрібно перенести дані з попередньої системи, забезпечивши їх цілісність та безпеку.

Розглянемо технічні складові використання. Дамо визначення «технічні складові використання» – це сукупність апаратного та програмного забезпечення, мереж, даних та інших технологій, які взаємодіють між собою, щоб забезпечити функціонування інформаційних систем. Основні складові:

- Моніторинг: Постійний моніторинг системи за допомогою таких інструментів, як Prometheus, Grafana або ELK Stack, для контролю її продуктивності та виявлення проблем.
- Обслуговування та підтримка: Включає технічну підтримку користувачів, виправлення помилок, оновлення програмного забезпечення.

- Масштабування: В разі зростання навантаження на систему можуть застосовуватися методи горизонтального або вертикального масштабування.

Отже, проєктування передбачає визначення архітектури та вибір технологій, які забезпечують масштабованість та ефективність рішень. Розробка включає написання та тестування коду, дотримання стандартів програмування, а також інтеграцію різних компонентів системи. Впровадження охоплює налаштування середовищ, автоматизацію процесів розгортання та підготовку користувачів до експлуатації системи. На етапі використання здійснюється моніторинг продуктивності, оновлення та підтримка програмного забезпечення для забезпечення його безперебійної роботи та адаптації до змін у вимогах. Таким чином, кожен етап вимагає тісної інтеграції технічних аспектів для досягнення успішного результату.

Список використаних джерел:

1. Павло Устінов// Розробка IT-проєкту: етапи та роль проєктного менеджера.URL:https://iampm.club/ua/rozrobka-it-projektu-etapi-ta-rol-projektnogo-menedzhera/

2.Західноукраїнський національний університет// Управління IT-проєктами.
URL:http://dspace.wunu.edu.ua/retrieve/19638/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%97.pdf

УДК 336.7

Дракон Д. С.
здобувач вищої освіти
ННІ «Каразінський банківський інститут» ХНУ ім. В.Н. Каразіна
Науковий керівник:
Філатова Л. Д.
доцент кафедри інформаційних технологій та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ ім. В.Н. Каразіна

ТЕХНОЛОГІЧНІ ІННОВАЦІЇ У ФІНТЕХ СЕКТОРІ УКРАЇНИ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ ПІСЛЯ ПЕРЕМОГИ

Технологічні інновації у фінтех секторі України відіграють ключову роль у відбудові економіки та розвитку фінансової системи в умовах війни та після її завершення. Фінансові технології ще до початку повномасштабного вторгнення Росії демонстрували значний потенціал для трансформації економіки України. Проте війна значно вплинула на фінансову галузь, створивши як нові виклики,

так і можливості для фінтех сектору. У світлі цих змін, необхідно проаналізувати сучасні тенденції та перспективи розвитку фінтех галузі після перемоги.

До початку війни Україна вже мала добре розвинену екосистему фінансових технологій. Такі компанії, як ПриватБанк, monobank, були прикладом інноваційного підходу до цифрових фінансових послуг, надаючи клієнтам мобільні додатки для безконтактних платежів, управління рахунками та кредитами. Розвиток технологій безпеки та персоналізації дозволив банкам і фінтех компаніям вдосконалювати свої послуги, забезпечуючи зручність і швидкість обслуговування.

Війна змінила багато аспектів роботи фінтех сектору. Одним з основних викликів стало забезпечення безперебійної роботи фінансових систем у складних умовах, зокрема в регіонах, які постраждали від бойових дій. Цифрові платіжні системи, такі як Приват24 та інші онлайн-платформи, стали критично важливими для підтримки економічної активності, коли традиційна банківська інфраструктура була недоступною. Попит на криптовалюти значно зріс, оскільки вони використовувалися як альтернативний спосіб зберігання та переміщення коштів, особливо у випадках міжнародних розрахунків.

У таких умовах технології блокчейну стали важливим інструментом для забезпечення безпеки та прозорості транзакцій. Використання криптовалют у фінансових операціях зросло, оскільки вони дозволяли уникати традиційних банківських ризиків, пов'язаних з кібератаками або фізичною недоступністю банківських відділень. Блокчейн також забезпечує стійкість систем до зовнішніх загроз і підвищує довіру до фінансових інститутів у нестабільних умовах.

Штучний інтелект і технології обробки великих даних сприяли вдосконаленню процесів управління ризиками, автоматизації обслуговування клієнтів і персоналізації фінансових послуг. Інтернет речей (IoT) та хмарні обчислення також дозволили фінтех компаніям забезпечувати безперебійне функціонування в умовах обмеженого фізичного доступу до банківських офісів.

Однак, крім технологічних досягнень, війна виявила низку проблем, з якими зіткнувся фінтех сектор. Недосконалість законодавчої бази щодо криптовалют та цифрових активів створює перешкоди для легалізації та подальшого розвитку цих інструментів. Водночас зростання кількості кібератак на фінансові установи під час війни підкреслює важливість кібербезпеки та необхідність захисту персональних даних. В умовах воєнного стану забезпечення доступу до фінансових послуг для населення стало проблемою, особливо у віддалених регіонах та зонах активних бойових дій.

Крім технологічних інновацій, важливим фактором розвитку фінтех сектору після перемоги стане співпраця між державою, приватним сектором та міжнародними фінансовими організаціями. Для прискорення економічного відновлення та залучення інвестицій необхідно створити сприятливі умови для інновацій, включаючи підтримку стартапів, полегшення доступу до

фінансування для малого і середнього бізнесу, а також розвиток освітніх програм у галузі фінансових технологій. Інвестування у людський капітал та технологічну інфраструктуру стане критично важливим для забезпечення довгострокового успіху.

Також необхідно акцентувати увагу на соціальній відповідальності фінансових інститутів. У період післявоєнного відновлення соціальні інновації у фінтех мають сприяти вирішенню проблем, пов'язаних із економічною нерівністю, доступом до базових фінансових послуг та кредитів для відновлення бізнесу в постраждалих регіонах. Фінансові технології можуть слугувати інструментом для підвищення економічної інклюзії, що особливо важливо для відновлення стабільного розвитку країни.

Нарешті, довгострокова перспектива розвитку фінтех сектору в Україні пов'язана з подальшою інтеграцією у глобальний ринок фінансових послуг. Завдяки стратегічному партнерству з міжнародними фінансовими установами та впровадженню передових технологій, Україна має всі шанси стати регіональним хабом інноваційних фінансових технологій. Це відкриє нові можливості не лише для національної економіки, але й для зміцнення позицій України на світовому ринку технологій та інновацій.

Незважаючи на виклики, фінтех сектор має значний потенціал для відбудови та розвитку після перемоги. Економічне відновлення України неможливе без стабільної фінансової системи, в якій фінтех технології відіграватимуть важливу роль. Інноваційні рішення у сфері фінансових послуг допоможуть швидко інтегрувати країну в міжнародні фінансові ринки, залучити іноземні інвестиції та створити нові можливості для підприємців і споживачів.

Важливу роль у відбудові гратиме фінансова інклюзія, зокрема надання доступу до фінансових послуг тим верствам населення, які зазнали найбільших втрат через війну. Фінтех технології можуть забезпечити зручний і швидкий доступ до кредитних ресурсів, банківських послуг та інвестиційних можливостей. Співпраця з міжнародними фінансовими організаціями та інтеграція у глобальні ринки надасть додаткові можливості для розвитку інноваційних фінансових рішень.

Перспективи післявоєнного розвитку фінтех сектору також включають подальше вдосконалення законодавчої бази, яка відповідатиме європейським стандартам та сприятиме розвитку криптовалют, блокчейн-технологій та інших цифрових активів. Також особливу увагу потрібно приділити розвитку кібербезпеки для захисту фінансових транзакцій та персональних даних споживачів.

Загалом, фінтех сектор України в умовах війни продемонстрував свою стійкість та здатність до швидкої адаптації в складних умовах. Після перемоги розвиток технологій у цій сфері стане одним із ключових елементів економічного відновлення країни та її інтеграції у світову фінансову систему. Однак для досягнення успіху необхідна тісна співпраця держави, бізнесу та

наукової спільноти, спрямована на подолання викликів та реалізацію перспектив розвитку фінтех сектору в нових умовах.

Список використаних джерел:

1. Мартін Ч. Інновації в фінансовому секторі: блокчейн, криптовалюти та цифрові активи / Ч. Мартін. – Харків: «Фактор», 2022. – 290 с.

2. Forbes Ukraine. Фінансові технології під час війни: як Україна адаптує фінансову систему [Електронний ресурс] // Forbes Ukraine. – Режим доступу: https://forbes.ua – Дата звернення: 20.09.2024.

3. Довгань А. М. Розвиток фінтех сектору в Україні: перспективи та виклики / А. М. Довгань // Науковий журнал економічних досліджень. – 2022. – №5. – С. 40–50.

УДК 004.4

Житушкіна В.А.,
здобувачка бакалаврського рівня вищої освіти
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна;
Стяглик Н. І.,
к.п.н., доцент, завідувач кафедри інформаційних технологій
та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ТЕНДЕНЦІЇ У ГАЛУЗІ РОЗРОБКИ МОБІЛЬНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

В сучасному житті велику частину життя людина приділяє телефону та функціоналу, який він пропонує.

З кожним роком кількість користувачів мобільних телефонів збільшується. Новий звіт Digital 2024 July Global Statshot Report від DataReportal демонструє, що 70% людей користується мобільними телефонами, що надає нові можливості, зокрема для бізнесу, тому дослідження тенденцій та слідування трендам в цій галузі може надати перевагу над конкурентами.

Із впевненістю можна зазначити, що використання новітніх технологій у розробці мобільного програмного забезпечення надає можливості для покращення продуктивності, кібербезпеки та користувацького досвіду, що сприяє зростанню зацікавленості серед споживачів.

На сьогодні є два основних вектори розвитку тенденцій: покращення користувацького досвіду та удосконалення технічної складової мобільних додатків.

Основними тенденціями, які відносяться до першого вектору, можна вважати:

- Мінімалістичний дизайн. Цей тренд передбачає побудову неперенасиченого інтерфейсу, що робить додаток інтуїтивно зрозумілим та легшим у використанні
- Голосові інтерфейси. Керування за допомогою голосу вже активно використовується в мобільних асистентах, навігації та управлінні розумним будинком.
- Чат-боти. Їх використання прискорює обробку процесів пов'язаних з обслуговуванням клієнтів, що допомагає економити час користувача та операторів.

До другої категорії відносять:

- 5G технології. Інтеграція цих технологій підвищить швидкість роботи додатків, які використовують інтернет та покращить якість стримінгових сервісів.
- Розробка під носимі девайси. З зростанням популярності гаджетів на кшталт смарт-годинників, збільшується попит на адаптацію додатків під них.
- Кібербезпека. Зі збільшенням конфіденційної інформації, яка використовується у додатках, зростає потреба в захисті інформації, бо потенційні користувачі можуть відмовитися від використання додатку на користь більш захищеного.
- Хмарні технології. Хмарні технології на основі хмарних обчислень надають дешевий обчислювальний ресурс для IT сфери, у тому числі для мобільних технологій.

Отже, тенденції, пов'язані із розвитком сумісних технологій, покращенням користувацького досвіду та приверненням потенційних споживачів, стимулюють компанії до інноваційних рішень та адаптації до змін на ринку. Це також спонукає бізнес до впровадження більш гнучких та персоналізованих підходів, щоб задовольнити зростаючі очікування користувачів та підвищити конкурентоспроможність.

Список використаних джерел:

1. DataReportal – Global Digital Insights. URL: DataReportal – Global Digital Insights.
2. Аналіз трендів та ринкових тенденцій URL: Аналіз трендів та ринкових тенденцій (xvitaliy.com)

УДК 004.9:364.62"364"

Ісаєв Р.Р.
здобувач вищої освіти,
ННІ ЕІТІ ХНУМГ імені О.М. Бекетова
Науковий керівник
Пахомов Ю.В.
к.т.н., доцент, доцент кафедри комп'ютерних наук
та інформаційних технологій
ННІ ЕІТІ ХНУМГ імені О.М. Бекетова

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ПСИХОЛОГІЧНИХ ПОСЛУГ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

Сучасні події, зокрема війна в Україні, спричинили значне погіршення психічного здоров'я населення. Мільйони людей стикаються зі стресом, тривожністю, депресією та іншими психічними проблемами, що вимагають професійної допомоги. Однак через військовий стан доступ до традиційних офлайн-консультацій суттєво обмежений, що зумовлює необхідність використання інформаційних технологій для надання психологічних послуг онлайн.

Серед доступних онлайн-сервісів для пошуку та бронювання психологічних консультацій в Україні виділяються платформи, такі як Rozmova, Mindly, EgoBalance та Treatfield. Ці системи надають можливість пацієнтам легко знайти фахівців за різними критеріями, зокрема спеціалізацією, рейтингом та мовою консультації. Окрім цього, користувачі можуть вибирати формат консультацій (онлайн або офлайн) і самостійно бронювати час через інтуїтивні інтерфейси.

На рисунку 1 видно, як зріс попит на ці послуги в умовах евакуації, обмеженого пересування і психологічних наслідків військових дій. Платформи для надання психологічних консультацій також адаптують свої сервіси для надання допомоги українським військовим та переселенцям, пропонуючи спеціалізовані послуги з урахуванням кризових ситуацій. В умовах війни онлайн-консультації стають основним способом отримання психологічної допомоги для людей, які втратили можливість доступу до офлайн-консультацій через переміщення або зруйновану інфраструктуру.

Одним із головних технічних викликів під час війни є нестабільність інфраструктури: часті відключення електроенергії, перебої з інтернетом та кібератаки. Для підтримки безперервної роботи онлайн-платформ важливо забезпечити їхню стійкість до таких перебоїв, використовуючи резервні сервери, механізми автоматичного відновлення даних та хмарні технології. Також важливо дотримуватися найвищих стандартів безпеки, шифрування даних і двофакторної автентифікації для запобігання витоку інформації під час консультацій.

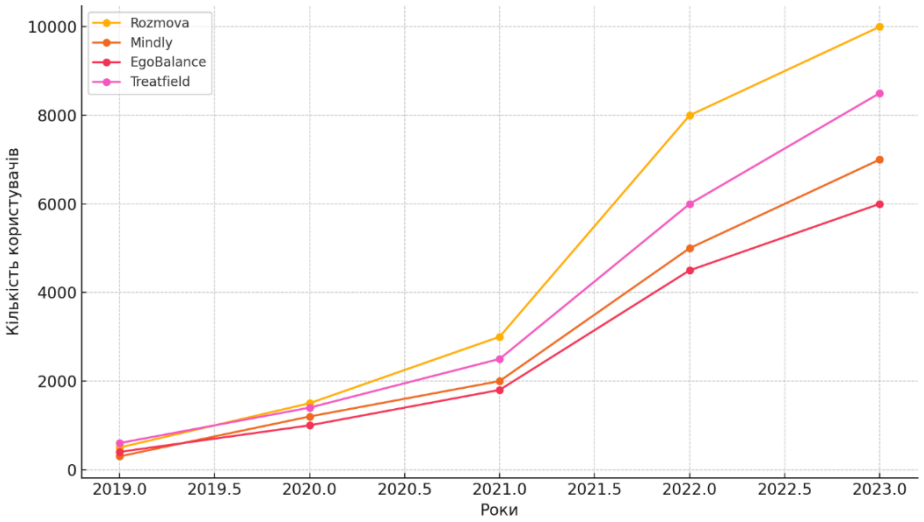


Рисунок 1. Приріст користувачів онлайн-платформ для психологічних консультацій у період 2019-2023 рр.

Військові дії ставлять додаткові виклики щодо конфіденційності психологічних консультацій. Консультантам та розробникам платформ необхідно забезпечувати надійний захист даних користувачів, особливо коли мова йде про травматичний досвід або військову інформацію. Також важливо враховувати етичні аспекти роботи в умовах війни, коли пацієнти можуть перебувати в особливо вразливому психологічному стані.

Таким чином, щоб покращити ефективність інформаційних систем у сфері психологічних послуг під час війни, рекомендується впроваджувати інструменти для швидкого доступу до консультацій у будь-який час, підвищувати безпеку та стабільність платформ, а також розширювати спектр кризових послуг для специфічних груп населення (військові, переселенці, постраждалі від війни). Розробники інформаційних систем повинні продовжувати розвивати інтеграцію з сучасними технологіями (ШІ, машинне навчання) для покращення процесу підбору фахівців та автоматизації деяких аспектів консультаційного процесу.

Список використаних джерел:

1. ООН та міжнародні організації: вплив війни в Україні на психічне здоров'я. https://www.un.org/uk

2. Американська психологічна асоціація: дослідження щодо зростання онлайн-консультацій (2023). https://www.apa.org

3. Міжнародна асоціація телемедицини та електронного здоров'я: дослідження онлайн-платформ для психологічної допомоги (2022). https://www.isfteh.org

4. Платформи Rozmova, Mindly, EgoBalance, Treatfield: аналіз функціоналу та переваг. https://rozmova.com.ua, https://mindly.com.ua, https://egobalance.com.ua, https://treatfield.com.

5. Українське законодавство про захист персональних даних: юридичні аспекти під час воєнних дій. https://zakon.rada.gov.ua/laws/show/2297-17

УДК 004.932.2:004.93'1

Макаров Д.С.
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Кобилін О.А.
Кандидат технічних наук, доцент
Харківський національний університет радіоелектроніки

МЕТОДИ СЕМАНТИЧНОГО АНАЛІЗУ ДЛЯ ВІДЕОСПОСТЕРЕЖЕННЯ

У сучасному світі, відеоспостереження стає невід'ємною частиною як у публічних, так і в приватних сферах життя. Безпека, моніторинг та контроль над публічними просторами – це завдання, які вимагають ефективних і сучасних рішень.

З огляду на великий обсяг інформації, що генерується відеокамерами, традиційні методи обробки відео не завжди здатні забезпечити належний рівень ефективності та точності. Тому впровадження семантичного аналізу в системи відеоспостереження набуло великого значення. Семантичний аналіз дозволяє автоматично виявляти та інтерпретувати об'єкти і події у відеопотоці, що дає можливість здійснювати більш детальне та точне моніторинг. У цій роботі розглядаються основні методи семантичного аналізу, які використовуються у відеоспостереженні.

Основні методи семантичного аналізу:

Deep Learning стало однією з ключових технологій у семантичному аналізі для відеоспостереження. Однією з найпоширеніших архітектур, що застосовується для цієї задачі, є згорткові нейронні мережі (Convolutional Neural Networks, CNN). Вони здатні автоматично виділяти ознаки з відео та класифікувати об'єкти в кадрі. Особливе місце займають рекурентні нейронні мережі (Recurrent Neural Networks, RNN) і Long Short-Term Memory (LSTM) моделі, які можуть аналізувати послідовності кадрів для виявлення змін у часі та розпізнавання складних дій.

Також, застосовуються трансформери (Transformers), що дозволяють обробляти відеопотоки з високою точністю завдяки механізмам самопідсилення. Ці моделі використовуються для розпізнавання об'єктів і подій у режимі реального часу.

Методи кластеризації та класифікації:

Семантичний аналіз за допомогою методів кластеризації полягає в групуванні подібних об'єктів або подій, що виникають у відео. Наприклад, методи кластеризації, такі як k-means або DBSCAN, можуть використовуватись для виявлення аномалій або нестандартних подій, що потребують уваги. Класифікаційні алгоритми, такі як Random Forest, Support Vector Machines (SVM), та інші, застосовуються для розпізнавання типів об'єктів, людей або їхніх дій у кадрі.

Методи опрацювання природної мови:

Для побудови ефективних відеоаналітичних систем, що здатні виконувати семантичний аналіз, важливо також інтегрувати методи опрацювання природної мови (Natural Language Processing, NLP). Наприклад, технології автоматичного підписування відео або побудови текстових описів подій на основі аналізу відео дозволяють системам надавати текстові звіти чи описи. Вони застосовуються для автоматичного генерування семантичної інформації, яку можна використовувати в системах безпеки.

Алгоритми трекінгу та сегментації:

Трекінг об'єктів у відеопотоці є важливим елементом семантичного аналізу. Сучасні методи трекінгу, такі як Kalman filter, Particle filter та алгоритми на основі CNN, дозволяють точно відстежувати рухомі об'єкти в різних кадрах відео. Це забезпечує безперервність аналізу й допомагає виявляти тривалі дії або відстежувати пересування осіб у складних середовищах.

Методи сегментації відео, як-от semantic segmentation та instance segmentation, дозволяють розділяти відеопотік на окремі регіони, що відповідають об'єктам чи подіям. Ці методи використовуються для точної інтерпретації відео та покращення результатів аналізу.

Використання семантичного аналізу у відеоспостереженні:

У системах відеоспостереження методи семантичного аналізу дозволяють автоматично визначати події, які потребують уваги, наприклад, розпізнавання облич або поведінки людей. Ці системи можуть бути налаштовані на виявлення аномалій, наприклад, якщо людина залишається на одному місці довше, ніж зазвичай, або входить у заборонену зону.

Завдяки семантичному аналізу можна також забезпечити більш детальне вивчення відеоданих з історичних записів, що є особливо корисним для правоохоронних органів або інших служб безпеки.

Семантичний аналіз дозволяє підвищити рівень автоматизації систем відеоспостереження, знижуючи навантаження на операторів і прискорюючи час реакції на потенційні загрози.

Крім того, завдяки інтеграції методів штучного інтелекту, системи відеоспостереження здатні навчатися нових шаблонів поведінки або дій.

Висновки:

Семантичний аналіз у відеоспостереженні має велике значення для підвищення ефективності моніторингу та забезпечення безпеки. Використання методів глибокого навчання, кластеризації, класифікації, опрацювання природної мови, трекінгу та сегментації дозволяє створювати більш точні та надійні системи відеоаналітики. Інтеграція таких систем у реальні процеси допоможе зменшити кількість помилкових тривог, збільшити швидкість реагування на події та покращити загальну ефективність моніторингу. З огляду на стрімкий розвиток технологій, подальший прогрес у цій галузі забезпечить ще більш ефективні рішення для безпеки та моніторингу.

Список використаних джерел:

1. Мельник П. В., Шестопалов С. В. Методи семантичного аналізу в системах відеоспостереження // Вісник Київського національного університету технологій та дизайну. 2018. №2. С. 45-51.
2. Горовий С. В. Застосування нейронних мереж для аналізу відеоданих у системах безпеки // Наукові праці Національного університету "Одеська політехніка". 2020. №7. С. 105-112.
3. Кравченко О. В. Використання методів машинного навчання для автоматизації відеоспостереження // Інформаційні системи та мережі. 2019. №4. С. 32-39.
4. Буряк О. М., Поліщук А. С. Технології глибокого навчання в аналізі відео: сучасний стан та перспективи // Вісник Харківського національного університету радіоелектроніки. 2021. №9. С. 90-98.

УДК 004.056.53

Ніколайчук А.І.
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Кобилін І.О.
к.т.н., асистент кафедри Інформатики,
Харківський національний університет радіоелектроніки

МЕТОДИ ПРОДУКТИВНОСТІ МОДЕЛЕЙ РОЗДІЛЕНОГО ФЕДЕРАТИВНОГО НАВЧАННЯ

Сучасні підходи для вирішення проблем конфіденційності в розподіленому навчанні включають розділене навчання (Split Learning, SplitNN, SL), федеративне навчання (Federated Learning, FL) та синхронний стохастичний градієнтний спуск (Stochastic Gradient Descent, SGD). Кожен з них має свої переваги та недоліки, застосовує різні інструменти підвищення рівня захищеності даних в процесі навчання, намагається вирішити недоліки інших методів. Наразі існує не так багато досліджень щодо адаптивності цих методів до мереж з обмеженими обчислювальними можливостями, більшість лише вказують на проблеми застосування методів на пристроях Інтернету речей (IoT), але не аналізують причини й не пропонують можливі шляхи вирішення.

Ця проблема є особливо актуальною для таких галузей, як охорона здоров’я та фінанси, де обмежені ресурси ускладнюють повноцінне навчання моделей машинного навчання. Наприклад, у середовищі Інтернету медичних речей (IoMT) для своєчасного виявлення аномалій або в фінансових системах для боротьби з шахрайством в режимі реального часу необхідно постійно оновлювати глобальні моделі на основі безперервних потоків даних.

FL дозволяє клієнтам спільно навчати власні моделі локально, без обміну персональними даними, а сервер лише агрегує ці моделі для створення глобальної. Основна перевага FL – паралелізм, що дозволяє ефективно навчати багато клієнтів одночасно. Однак суттєвим недоліком є те, що клієнти IoT з обмеженими ресурсами часто не мають достатньої обчислювальної потужності, чи пам'яті для локального зберігання повної моделі. Конфіденційність даних також залишається під загрозою, оскільки клієнти та сервер мають доступ до повних локальних і глобальних моделей, що дозволяє відтворити основні дані.

Для усунення недоліків FL було запроваджено SL [4]. Даний метод зменшує обчислювальне навантаження за рахунок розділення моделі – лише початкові шари моделі навчаються на стороні клієнта, а решта – на сервері, що робить SL більш придатним для пристроїв з обмеженими ресурсами. Крім того, цей метод пропонує підвищену конфіденційність, обмежуючи доступ сервера до клієнтської частини моделі, і навпаки. Однак лише один клієнт може взаємодіяти з сервером в будь-який момент часу, що призводить до простою інших клієнтів і створює труднощі при масштабуванні. Така послідовність підвищує навантаження та збільшує тривалість навчання, що знижує загальну ефективність процесу.

Для подолання обмежень як FL, так і SL, була запропонована нова архітектура – розділено-федеративне навчання (SplitFed Learning, SFL) [3]. SFL притаманна перевага паралелізму FL, що значно скорочує час навчання та вирішує проблему простою ресурсів, роблячи цей підхід більш масштабованим. Розділяючи модель на клієнтську та серверну частини, SFL також зменшує обчислювальне навантаження на клієнтів з обмеженими ресурсами, що робить його ідеальним для IoT середовищ. Крім того, SFL покращує конфіденційність даних завдяки впровадженню диференційної приватності. Емпіричні дослідження показують, що SFL досягає такої ж точності моделі та ефективності комунікації, як і SL, але при цьому працює швидше завдяки паралелізму FL.

Попередні дослідження здебільшого були зосереджені на конфіденційності та масштабованості методів розподіленого навчання, тож вплив параметрів пристроїв на ефективність навчання залишається недостатньо вивченим. Наприклад, робота [1] показує, що FL вимагає значних ресурсів від клієнтів, а SL збільшує комунікаційне навантаження, що залежить від кількості параметрів у зрізаному шарі (cut або split layer), де модель розділена між клієнтом і сервером. Тому досліджуючи вплив характеристик пристроїв (обчислювальної потужності, пам'яті, споживання енергії) та умов мережі (пропускної здатності, затримки) можна визначити, які параметри необхідно оптимізувати для підвищення продуктивності методів розподіленого навчання. Наприклад, запропонована схема адаптивного розділеного навчання (Adaptive Split Learning, ASL) [2] демонструє, що динамічне налаштування зрізаного шару з урахуванням різних можливостей пристроїв і мінливості мережі може значно зменшити затримку при навчанні та споживання енергії. Алгоритм OPEN, що використовується в ASL, показує, що пристрої з більшою

обчислювальною потужністю можуть обробляти більшу частину моделі, мінімізуючи навантаження при комунікації клієнта з сервером, зменшуючи споживання енергії на 22,1%, а також скорочуючи затримку при навчанні на 53,7%.

Розглянемо два ключові фактори, що впливають на ефективність навчання: загальну затримку та споживання енергії. Загальна затримка при навчанні – це час, необхідний клієнту для завершення одного раунду навчання, враховуючи як обчислювальні, так і комунікаційні затримки. Для кожного клієнта m на навчальному раунді n затримка при навчанні становить (1):

$$D\left(s_{m,n}, c_{m,n}\right) = d_{m,n}^{D,C} + d_{m,n}^{B,C} + d_{m,n}^{B,D} + d_{m,n}^{D,S} + d_{m,n}^{B,G} + d_{m,n}^{D,D}, \quad (1)$$

де $d_{m,n}^{D,C}$ – затримка обчислень на стороні клієнта, що є часом, необхідним для обробки локальної частини моделі клієнтом;

$d_{m,n}^{B,C}$ – затримка обчислень на стороні сервера;

$d_{m,n}^{B,D}, d_{m,n}^{D,S}, d_{m,n}^{B,G}, d_{m,n}^{D,D}$ – затримки при передачі даних, включаючи надсилання проміжних результатів (smashed data) та отримання градієнтів.

Детальний аналіз складових затримки представлений у [2], де враховуються такі фактори, як кількість операцій з рухомою комою (FLOPs), частота обробки пристрою, пропускна здатність мережі й швидкість передачі даних. Оптимізація загальної затримки є критично важливою для підвищення швидкості та масштабованості SFL, особливо в середовищах, де можливості пристроїв і мережеві умови можуть суттєво відрізнятися.

Загальне споживання енергії клієнтом m під час навчального раунду n охоплює як енергію, витрачену на передачу даних, так і енергію, необхідну для обчислень та становить (2):

$$E\left(s_{m,n}, c_{m,n}\right) = E_{m,n}^{D,T} + E_{m,n}^{D,C} + E_{m,n}^{B}, \quad (2)$$

де $E_{m,n}^{D,T}$ – енергія для передачі даних, що витрачається на надсилання та отримання даних між клієнтом і сервером;

$E_{m,n}^{D,C}$ – енергія для обчислень, що витрачається на обробку моделі на стороні клієнта;

$E_{m,n}^{B}$ – енергія для сервера, що використовується для обробки даних та управління зв’язком з клієнтськими пристроями.

Детальний аналіз цих компонентів, який враховує споживання енергії за цикл роботи процесора та вплив специфічних параметрів пристрою, таких, як частота обробки і потужність передачі, представлений у [2]. Мінімізація енергії

для обчислень і передачі даних є критично важливою для продовження терміну служби пристроїв в обмежених мережах та забезпечення ефективного навчання.

Отже, при дослідженні методів розподіленого навчання важливо враховувати характеристики пристроїв та можливості мережі, які безпосередньо впливають на ключові параметри, такі, як затримка при навчанні та енергоспоживання. На основі їхнього аналізу слід впроваджувати оптимізаційні методи, наприклад, динамічне призначення зрізаного шару, що дозволяє адаптувати модель до різних умов середовища використання. Такий підхід підвищить загальну ефективність навчання, забезпечить кращу масштабованість та зменшить витрати ресурсів у середовищах з обмеженими можливостями.

Список використаних джерел:

1. Gao, Y., Kim, M., Abuadbba, S., Kim, Y., Thapa, C., Kim, K., Camtepe, S. A., Kim, H. and Nepal, S. (2020). End-to-End Evaluation of Federated Learning and Split Learning for Internet of Things. The 39th International Symposium on Reliable Distributed Systems (SRDS). arXiv. https://doi.org/10.48550/arXiv.2003.13376
2. Li, Z., Wu, W., Wu, S., & Wang, W. (2024). Adaptive Split Learning over Energy-Constrained Wireless Edge Networks. arXiv. https://doi.org/10.48550/arXiv.2403.05158
3. Thapa, C., Mahawaga Arachchige, P. C., Camtepe, S. and Sun, L. (2022). SplitFed: When Federated Learning Meets Split Learning. Proceedings of the AAAI Conference on Artificial Intelligence, 36(8), 8485-8493. https://doi.org/10.1609/aaai.v36i8.20825
4. Vepakomma, P., Gupta, O., Swedish, T., & Raskar, R. (2018). Split learning for health: Distributed deep learning without sharing raw patient data. arXiv. https://doi.org/10.48550/arXiv.1812.00564

УДК 004.738

Ревенков В.В.
здобувач вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Наукові керівники
Ковальчук Д.М.
к.т.н., старший викладач
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Самородов Б.В.
д.е.н., к.т.н., професор
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ДОСЛІДЖЕННЯ НАДІЙНОСТІ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ У СИСТЕМІ «РОЗУМНИЙ БУДИНОК»

У сучасному світі більшість щоденних завдань стали простішими або автоматизованими, і ця тенденція продовжує зростати з кожним роком. Електроніка та технології дистанційного управління стали невід'ємною частиною повсякденного життя. Системи автоматизації, такі як «розумний будинок», набули популярності завдяки прагненню людей до комфорту та зручності. Крім того, вони забезпечують додатковий рівень безпеки, будь то протипожежні системи чи сигналізації з віддаленим сповіщенням.

Найчастіше, система «Розумного будинку» складається з таких частин:

- пристрої – безпосередньо всі електронні побутові речі, контроль над якими необхідно автоматизувати;
- датчики – пристрої збору інформації розумного дому;
- мікроконтролери – апаратні системи, що об'єднують датчики в групи, розрізняють також центральний процесор управління – мікроконтролер, що посилає від сервера інформацію в кінцеві вузли;
- сервер – комп'ютер, який створює інтерфейс між користувачем та системою розумного дому. Саме він відповідає за надійність, функціональність;
- канали передачі даних – логічні та фізичні канали, по яким передаються дані з урахуванням потреб (безпека, швидкість тощо);
- хмара – зовнішня служба, що виконує роль бази даних для статистики та іншої службової інформації;
- мобільні пристрої – пристрої, за допомогою яких користувач через сервер керує системою розумного дому.

Для передачі даних в системах «Розумного будинку» найчастіше використовуються такі бездротові технології як: Wi-Fi, Bluetooth, Zigbee, Z-Wave. Оскільки їхня надійність стає критичним чинником для коректної роботи всіх компонентів «Розумного будинку», то актуальною є тема дослідження надійності бездротових технологій у системі «Розумний будинок».

Розглянемо основні принципи функціонування бездротових технологій у системі «Розумний будинок». Бездротові технології дозволяють підключати

різноманітні пристрої, такі як датчики, камери, освітлювальні прилади та інші компоненти системи автоматизації без необхідності прокладання кабелів. Це робить процес установки більш зручним і гнучким. Основні технології, що використовуються в «розумних будинках», включають:

- Wi-Fi: використовується для передачі великих обсягів даних і для підключення до інтернету. Переваги – висока швидкість передачі даних, однак має обмежену дальність і підвищене енергоспоживання;
- Bluetooth: підходить для короткочасних з'єднань між пристроями на короткій відстані. Характеризується низьким енергоспоживанням, але не підтримує велику кількість одночасно підключених пристроїв;
- Zigbee і Z-Wave: ці протоколи споживають низький рівень електроенергії і підходять для управління пристроями у системі розумного будинку. Вони мають більшу надійність, оскільки працюють на частотах, менш схильних до перешкод.

До основних переваг бездротових технологій у системі «Розумного будинку» можемо віднести:

- гнучкість установки: бездротові пристрої можна розміщувати в будь-якому місці, не обмежуючи користувача потребою в прокладанні кабелів;
- масштабованість: легкість додавання нових пристроїв до системи дозволяє збільшувати кількість функцій та компонентів «Розумного будинку» без суттєвих змін в інфраструктурі;
- мобільність: бездротові технології дозволяють керувати пристроями за допомогою смартфона або інших мобільних пристроїв, що робить управління зручним і доступним з будь-якої точки світу.

Одним з ключових показників бездротових технологій є їх здатність забезпечувати стабільний зв'язок навіть у складних умовах. Наприклад, інтерференція від інших пристроїв або перешкоди від стін можуть впливати на якість сигналу.

Для забезпечення надійності рекомендується використовувати спеціалізовані протоколи з побудовою mesh-мереж (наприклад, Zigbee або Z-Wave), які можуть забезпечити зв'язок між пристроями навіть у разі втрати прямого сигналу.

Отже, надійність бездротових технологій є одним з основних чинників успішної роботи систем «Розумного будинку». Вивчення їхньої стабільності, стійкості до інтерференції, безпеки та енергоефективності дозволить не лише вдосконалити поточні системи, але й забезпечити основу для подальшого розвитку технологій, що сприяють підвищенню рівня комфорту та безпеки в повсякденному житті.

Список використаних джерел:

1. Розумний дім [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B7%D1%83%D0%BC%D0%BD%D0%B8%D0%B9_%D0%B4%D1%96%D0%BC.
2. Wi-Fi [Електронний ресурс] – Режим доступу: https://

uk.wikipedia.org/wiki/Wi-Fi
3. ZigBee [Електронний ресурс] – Режим доступу: https:// uk.wikipedia.org/wiki/ZigBee
4. Bluetooth [Електронний ресурс] – Режим доступу: https:// uk.wikipedia.org/wiki/Bluetooth

УДК 004.056.53

Санько К.Д.
здобувач фахової передвищої освіти,
Харківський комп'ютерний фаховий коледж
Науковий керівник
Наугольна Л.М.
викладач, спеціаліст вищої категорії
Харківський комп'ютерний фаховий коледж

ЗНАЧЕННЯ ВІДКРИТОГО ВИХІДНОГО КОДУ ДЛЯ СУЧАСНИХ ІТ-ПРОЄКТІВ

Зараз поширеною є тенденція розробки відкритого програмного забезпечення. Це означає, що кожен бажаючий може побачити вихідний код, на якому був розроблений цей продукт, ознайомитися з ним та логікою його створення. В цій сфері існує як безліч невеликих, так і масштабних всесвітньо відомих проєктів. Популярним прикладом є операційна система Linux з активною спільнотою, яка кожен раз покращує її функції. А з українських програмних забезпечень таким є державний проєкт Дія, який було опубліковано на GitHub [1]. В перші ж дні після відкриття коду інші розробники почали досліджувати його та пропонувати свої варіанти для вирішення знайдених недоліків та проблем.

Причин, чому розробники відкривають код свого проєкту, може бути декілька. Для звичайних програмістів це насамперед новий досвід і навички, отримані завдяки власній практиці та під час залучення до інших проєктів, або коментарям зацікавлених в його програмі людей. А для студентів коледжів та університетів подібна діяльність допоможе в заповненні портфоліо для демонстрації майбутнім роботодавцям. Для відомих компаній це може стати гарним способом показати прозорість своїх дій, підвищити довіру до себе та продемонструвати якість свого продукту, тому що інші розробники самотужки зможуть проаналізувати його, а у разі знаходження вразливостей – повідомити про них або запропонувати шляхи їх усунення та способи мінімізації подальших наслідків.

Перед тим, як відкривати код свого програмного забезпечення, розробники повинні проаналізувати всі ризики та визначити, чи варто це робити. На рішення впливають такі аспекти:

1. Право та законодавство. В Україні захист авторських прав на програмне забезпечення регулюється відповідно до статті 20 Закону України «Про авторське право і суміжні права» [2]. Він поширюється на текстовий код за тієї умови, що він буде оригінальним. Для надання дозволу на використання або розповсюдження вмісту програми недостатньо відкрити її вихідний код. Щоб розпорядитися правами, власнику необхідно укласти авторський договір. Для врегулювання умов на дії сторонніх осіб над відкритим програмним забезпеченням використовуються спеціальні ліцензійні договори. З них найпопулярнішими є MIT і Apache 2.0 [3]. Ліцензія MIT вважається однією з найпростіших. Вона звільняє автора від юридичної відповідальності та не дає обмежень на використання, модифікацію або поширення програмного забезпечення, якщо разом з копіями або зміненими версіями буде міститися повідомлення про авторські права і ліцензію. Apache 2.0 містить додаткові вимоги щодо розповсюдження, дозволяє використовувати інші ліцензійні умови для змінених частин і надає патентні права. Варто зазначити, що важливо відповідально підійти до вибору ліцензійних умов до програмного забезпечення і обрати ті, які найкраще підходитимуть під конкретну ситуацію і не конфліктуватимуть із законодавством, тому що після цього вони визначатимуть обмеження до можливостей використання поточного проєкту.

2. Мораль та етика. Окрім людей, що підтримують ідеї відкритого програмного забезпечення та дотримуються загальноприйнятих етичних норм, є й ті, хто нечесно використовує це для власної користі. Для компаній загрозу створюють їх конкуренти і зловмисники, коли ті спеціально шукають недоліки або слабкі місця в коді для пошкодження репутації цієї компанії або ж набагато легшого втручання в безпеку і стабільну роботу продукту. При цьому перевагою стане зацікавлена в покращенні програми спільнота, учасники якої навпаки будуть знаходити проблеми та повідомляти про них. Однак для розробників ще однією негативною стороною є те, що не всі, хто використовує їх програми, будуть ознайомлюватися з ліцензійними умовами використання, порушуючи встановлені дозволи [4]. Наприклад, в деяких ситуаціях не передбачено застосування коду відкритого програмного забезпечення в комерційних проєктах або його розповсюдження можливе лише з виконанням певних умов, але цього не завжди дотримуються, створюючи неприємності для обох сторін.

3. Ресурси компанії. Проблемною може стати ситуація, коли розробники відкривають до цього закритий код – тут постає питання з конфіденційною інформацією, власними бібліотеками та рішеннями, які приймалися під дією зовнішніх чинників у вигляді обмеженості в часі або вимог зацікавлених сторін. Усунення цих недоліків займає час, витрачаючи ресурси компанії. Окрім цього для команди стресовою є критика інших незнайомих фахівців. Подібна проблема стає на заваді їхньої продуктивності та власній впевненості на робочому місці. Важливим є етап вчасного обговорення даної ситуації з працівниками, щоб запобігти негативним наслідкам. Після впровадження відкритого коду додатковим обов’язком є аналіз коментарів від зацікавлених людей і вчасне обговорення, проведення оновлень. Розробникам бажано

показувати підтримуваність їхнього програмного забезпечення, впроваджувати в роботу доречні пропозиції і заохочувати цим до участі в розвитку проєкту.

Отже, якщо після розгляду всіх аспектів, автор вирішить відкрити код свого проєкту, то позитивний вплив відзначатиметься тим, що на цей код спрямують погляд досвідчені в ІТ галузі фахівці. Вони будуть дивитися в середину програмного забезпечення, тестувати його, а найголовніше – пропонувати свої рішення, технології і підходи до вирішення проблем, звітувати про помилки та вразливості, виявлені під час аналізу коду. Це слугує поштовхом для співпраці в спільноті, що дозволяє додавати нові цікаві функції, інтегрувати новітні технології в уже існуючі проєкти, вдосконалювати їх та сприяти розвитку ІТ індустрії в цілому. Це забезпечує пришвидшений розвиток та досягнення інноваційності в створених програмних продуктах.

Список використаних джерел:

1. GitHub Дії. URL: https://github.com/diia-open-source
2. Закон України «Про авторське право і суміжні права». URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text
3. The most popular licenses for each language in 2023. URL: https://opensource.org/blog/the-most-popular-licenses-for-each-language-2023
4. 2024 OSSRA report: Open source license compliance remains problematic. URL: https://www.synopsys.com/blogs/software-security/ossra-license-compliance-risks.html

РОЗДІЛ 3.

ПРОГРАМНІ ЗАСОБИ ДЛЯ ВИРІШЕННЯ ПРИКЛАДНИХ ЗАДАЧ ВИРОБНИЦТВА, ОСВІТИ, БІЗНЕС-АНАЛІТИКИ, ІНТЕЛЕКТУАЛЬНОГО ОБРОБЛЕННЯ ДАНИХ, ПРИЙНЯТТЯ РІШЕНЬ

UDC 004.02

Bodenchuk-Pastukhov Y. V.
higher education applicant,
Kharkiv National University of Radio Electronics
Academic advisor
Kobylin I. O.
PHD, assistant department informatics
Kharkiv National University of Radio Electronics

APPLICATION OF MULTI-HEAD ATTENTION MECHANISM IN SOFTWARE TOOLS FOR MACHINE TRANSLATION WITHIN INTELLIGENT DATA PROCESSING

In 2017, Google researchers introduced a new neural network architecture called the Transformer. The core of the neural network is multi-head attention, which relies heavily on the self-attention mechanism. Self-attention is an algorithm that calculates a matrix representing the relationships between words in a sequence. This matrix can be described by the following formula:

$$Attention(Q,\ V,\ K) = softmax(\frac{QK^T}{\sqrt{d_k}})V$$

Where Q is the query matrix, K is the key matrix, V is the value matrix, d_k is the dimensionality of the model's embeddings [1].

Each row in the output matrix captures not only the meaning of a word (as represented by its embedding) but also its position within the sentence (via positional encodings) and its interaction with other words in the sequence.

The matrices Q, K, and V typically have dimensions $n \times d_k$, where n is the sequence length, and d_k is the dimension of the model's embeddings. The resulting matrix will have dimensions $n \times d_k$.

In the attention formula, we use the softmax function to normalize the rows of the resulting matrix, ensuring that each row sums to 1. The softmax function also transforms large negative values (e.g. -∞) into 0, effectively ignoring them. The softmax function is defined as:

$$softmax\left(z_i\right) = \frac{e^{z_i}}{\sum_{j=1}^{n} e^{z_j}}$$

Where z_i – element of a vector [1].

And this is where multi-head attention comes in. As we've already discovered, self-attention helps us build a matrix of words relationships to understand the context of the text. However, one self-attention is not as effective as multi-head attention because, in the latter, we have multiple heads. Each head calculates the relationships

between words and then concatenates the result into a single matrix. The advantage of using multiple heads is that each head can focus on different parts of the input sequence. This allows the model to capture various aspects of the relationships between words, such as syntactic and semantic dependencies, which improves the overall performance of the attention mechanism. It can be described as:

$$MultiHead(Q,\ K, V) = Concat(head_1 \dots head_h)W^o$$

Where *head* is the result of the self-attention formula, *h* is the number of heads, W^o is the matrix of weights of the final linear projection after the concatenation of all heads [1].

Each head can be described as:

$$head_i = Attention(QW_i^Q,\ KW_i^K,\ VW_i^V)$$

Where W^Q_i, W^K_i, W^V_i is the matrices of weights for each *i*-th head [2].

As we've already discovered the matrices Q, K, and V have dimensions $n \times d_k$. The weights matrices map the inputs to different subspaces of dimension d_k/h where h is number of heads.

Overall, it can be said that the self-attention mechanism played a crucial role in the creation of the Transformer architecture through the use of the multi-head attention mechanism. This architecture solved many of the problems associated with recurrent neural networks (RNNs) and long short-term memory (LSTM) networks, such as slow word processing and the inability to parallelize computations efficiently.

Additionally, the Transformer architecture addresses the issue of capturing long-range dependencies in sequences, a challenge faced by RNNs and LSTMs due to their sequential nature. Unlike RNNs, where each word must be processed in order, the self-attention mechanism allows the Transformer to consider all words in a sequence simultaneously, making it far more efficient at modeling long-distance relationships between words [3].

Moreover, the ability to parallelize computations across entire sequences enables significantly faster training times compared to LSTM and RNN models, where sequential processing creates bottlenecks. This parallelization is one of the key reasons why Transformers have become the architecture of choice for large-scale language models.

References:

1. a-PyTorch-Tutorial-to-Transformers. URL: https://github.com/sgrvinod/a-PyTorch-Tutorial-to-Transformers

2. Setlak, G., Bodyanskiy, Y., Pliss, I., Vynokurova, O., Peleshko, D., & Kobylin, I. (2018). Adaptive fuzzy clustering of multivariate short time series with unevenly distributed observations based on matrix neuro-fuzzy self-organizing network. In Advances in Fuzzy Logic and Technology 2017: Proceedings of:

EUSFLAT-2017–The 10th Conference of the European Society for Fuzzy Logic and Technology, September 11-15, 2017, Warsaw, Poland IWIFSGN'2017–The Sixteenth International Workshop on Intuitionistic Fuzzy Sets and Generalized Nets, September 13-15, 2017, Warsaw, Poland, Volume 3 10 (pp. 308-315). Springer International Publishing.

3. Transformers for Neural Machine Translation. URL: https://medium.com/@ultimateabhi/transformers-for-neural-machine-translation-9144bd27dfcc

УДК 004.932.2

Kharchenko A. I.
Higher education student
Kharkiv National University of Radioelectronics
Scientific Supervisor
Kobylin I. O.
Ph.D. in Technical Sciences
Kharkiv National University of Radioelectronics

PERFORMANCE ANALYSIS OF SUPPORT VECTOR MACHINE FOR VEHICLE CLASSIFICATION

There are a lot of cases in manufacturing, institutions, and public spaces where information systems must be provided with computer vision, especially for objects like vehicles. Therefore, it's crucial to consider how the Support Vector Machine (SVM) performs classification [1-4].

The SVM is the algorithm for the classification of not just linearly separable data but also nonlinearly separable data. The problem of linearly nonseparable data is solved by SVM using the transformation of input feature space.

The SVM maps the nonlinearly separable input data into higher-dimensional space. The data become linearly separable in this space, and SVM finds a linear hyperplane for data separation. The formula (1) of the hyperplane is following:

$$\widehat{f(x)} = \sum_{i=1}^{N} \widehat{\alpha_i}\, y_i K(x, x_i) + \widehat{\beta_0}, \qquad (1)$$

where $\widehat{\alpha_i}$ are the Lagrange multipliers, y_i are the class labels, $K(x, x_i)$ is the kernel function and $\widehat{\beta_0}$ is the bias term.

For the hyperplane construction, the quadratic polynomial kernel was chosen, and its formula (2) is shown:

$$K(x, x_i) = (\gamma {x_i}^T x + b)^2, \qquad (2)$$

where γ and b are free parameters, x is the input data point, x_i are support vectors.

The input data consists of images, where their dimension is $225 \times 225 \times 3$ and it means that the model is working with the 151875 features. There are six classes: Ambulance, Bicycle, Bus, Jeep, Motorcycle, and Van**.** After input data normalisation, the 25 principal components were constructed.

To find what the dimension of the input data was mapped during the SVM model training, the binomial coefficient (3) is used:

$$C(n+k,k) = \binom{n+k}{k} = \frac{(27)!}{(27-2)!\,2!} = 351, \quad (3)$$

where k is the degree of polynomial, and n is the number of original dimensions

So, the SVM model mapped initial data into 351-dimensional space. The SVM didn't find the data points' new coordinates but calculated just the inner product of the data points' higher-dimensional space.

After input images were preprocessed and the SVM model was trained, the classification report was drawn and presented in Table 1.

Table 1 – Classification report for the Support Vector Machine model

Class	Precision	Recall	F1-Score	Support
Ambulance	0.55	0.54	0.54	141
Bicycle	0.57	0.55	0.56	155
Bus	0.54	0.55	0.54	148
Jeep	0.65	0.33	0.44	52
Motorcycle	0.59	0.69	0.64	245
Van	0.52	0.46	0.49	144
Accuracy	N/A	N/A	0.56	885
Macro Average	0.57	0.52	0.53	885
Weighted Average	0.56	0.56	0.56	885

The SVM model's accuracy is 0.56. The Motorcycle class is the best classified, where the F1-Score is equal to 0.64. The model classifies jeeps with the lowest accuracy, which is 0.44.

The confusion matrix was built to visualise the performance of the SVM model. It's shown in Figure 1.

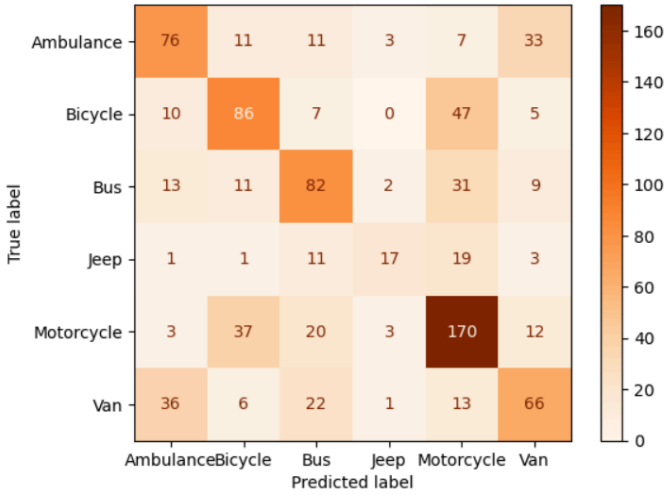


Figure 1 – Confusion matrix for the Support Vector Machine model

Figure 1 shows that the SVM model confused the 36 van images with ambulances and 22 images with busses.

It's important to note that there is confusion between the Bicycle and Motorcycle classes, where 31 instances of the Bus class were labelled as Motorcycle. Regarding the Jeep class, the SVM model failed to classify images, where 11 jeeps are predicted as Bus, and 19 jeeps are labelled as Motorcycle.

While the SVM model's current accuracy for image classification is 56 %, the model performance can be improved. A large dataset of images for each class may enhance the SVM model's predictions.

However, modern realities are such that the SVM algorithm doesn't guarantee an accuracy of approximately 100 % but provides an accuracy range between 50-80 %.

References:

1. Burges, C. (1998), "A Tutorial on Support Vector Machines for Pattern Recognition", Data Mining and Knowledge Discovery, No. 2(2), pp. 121-167. doi: https://link.springer.com/article/10.1023/A:1009715923555

2. Hastie, T., Tibshirani, R. and Friedman, J.H. (2009), "The Elements of Statistical Learning: Data Mining, Inference, and Prediction", 2nd ed., Springer, New York, 745 p. doi: https://doi.org/10.1111/j.1751-5823.2009.00095_18.x

3. Wu, X. and Kumar, V. (2009), "The Top Ten Algorithms in Data Mining", Chapman and Hall, New York, 230 p. doi: https://doi.org/10.1201/9781420089653

4. Bodyanskiy, Ye.,Vynokurova, O., Szymański, Zd., Kobylin, I., and Kobylin, O. (2016), "Adaptive Robust Models for Identification of Nonstationary Systems in Data Stream Mining Tasks", IEEE First International Conference on Data Stream Mining & Processing, Lviv, Ukraine, August 23-27, 2016, pp 263-268. doi: https://doi.org/10.1109/DSMP.2016.7583556

UDC 004.056.53

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

FUZZY MODELS FOR FAULT DETECTION IN ONLINE TIME SERIES MONITORING OF CRITICAL EQUIPMENT

In modern production systems, it is vital to uphold optimal efficiency and reduce downtime to prevent unforeseen equipment failures that can result in major disruptions. Conventional maintenance strategies, such as corrective and preventive techniques, frequently fail to foresee or stop failures prior to their interference with operations. Identifying errors in real time from time series data is complex due to the unpredictable nature of faults and subtle abnormalities, making reliable, automated fault detection systems essential for improving the reliability and efficiency of production systems.

There are two important methods to optimize maintenance management: predictive and proactive, which are complemented by corrective and preventive approaches [1]. The predictive maintenance process provides a report on the operational status of the equipment. This process consists of four main steps:

- identification of occurring fault modes;
- determination of the fault location;
- assessment of fault expansion;
- assessment of the remaining life of the equipment under consideration.

To detect early equipment failures, Automatic Diagnostic Systems (ADS) incorporate the combination of continuous monitoring and supervisory systems, which continuously collect operational data, gradually requiring less user intervention [2,4].

The following steps allow to transform a conventional monitoring and supervision system into an intelligent one. Using oscilloscopes, specialists perform phase analysis to check the balance between phases and harmonic analysis to observe the intensity of harmonics present in the signal. However, a major disadvantage of using oscilloscopes for monitoring is the significant increase in file size. To address this issue, redundant adaptive decompositions based on the Matching Pursuits (MP) technique are employed. This sparse approximation algorithm determines the best projections of multidimensional data onto the span of an overcomplete (redundant) dictionary D [3]. An approximate representation of a signal f from a Hilbert space H is given as a weighted sum of a finite number of functions called atoms taken from D. An approximation with N atoms (1) is represented as:

$$f(t) \approx \hat{f}_N(t) := \sum_{n=1}^{N} a_n g_{\gamma_n}(t), \quad (1)$$

where g_{γ_n} is the γ_n column of the matrix D, and a_n is the scalar weighting factor (amplitude) for the atom g_{γ_n}.

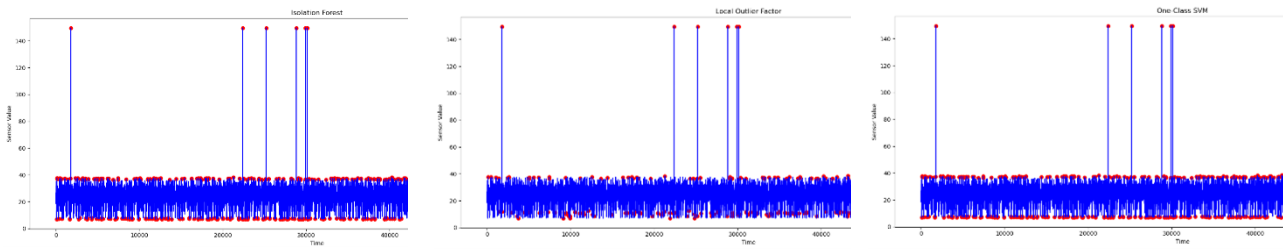
The algorithm minimizes absolute error by iteratively selecting atoms with the largest inner product with the signal, subtracting their approximations from the signal. This process continues until the signal is satisfactorily decomposed, i.e., the norm of the residual is small. The residual after finding γ_N and a_N (2) is represented as:

$$R_{N+1} = f - \hat{f}_N. \quad (2)$$

If R_n rapidly approaches 0, then only a few atoms are needed to satisfactorily approximate f. Such a sparse approximation is desirable for signal coding and compression.

Three methods for detecting anomalies were analyzed to improve fault detection of production systems. The Isolation Forest (IF) method is based on randomly isolating data points; the fewer isolation 'trees' required to isolate a point, the more likely it is to be an anomaly. The Local Outlier Factor (LOF) estimates the local density of the data, where anomalous points have a significantly lower density. The One-Class SVM (OCSVM) uses the support vector method to detect the boundary that separates normal data from anomalies.

To analyze these methods, a dataset provided by Schneider Electric was used [5]. It contains time series measurements from PT100 temperature sensors, known for their reliability and accuracy in harsh environments. The results are presented in Fig. 1 with blue lines indicating normal values and red dots marking detected anomalies.



a) b) c)

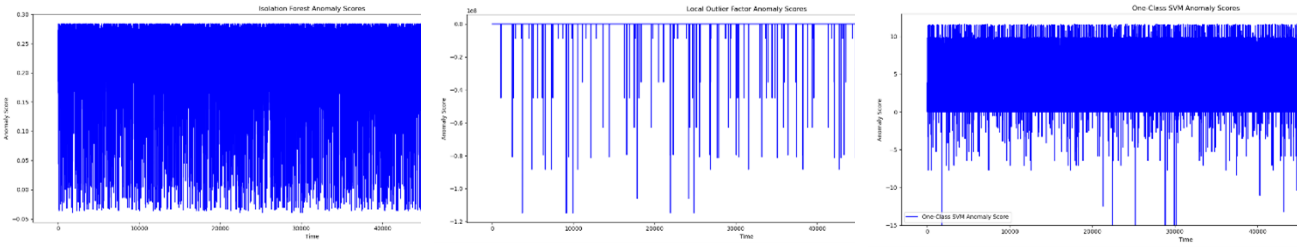
Figure 1 – Detecting anomalies using a) IF, b) LOF, c) OCSVM

Source: developed by the authors based on the data [5].

Fig. 1 (a) shows that the IF method detected anomalies that occur sporadically in the time series; they are evenly distributed, with noticeable peaks. LOF in Fig. 1 (b) detected anomalies only at more specific points, as this method considers the local density of data points and detects cases that cannot be identified by general

methods. The OCSVM method in Fig. 1 (c) detected anomalies located almost at the same points and is effective for detecting anomalies in a multidimensional space using a hyperplane. Thus, this consistency between methods indicates their reliability.

Graphs (Fig. 2) of anomaly estimates for each method allow comparison of algorithm effectiveness, determine which is more sensitive to anomalies and which is more stable, and help identify which parameters need adjustment for better results.



a) b) c)

Figure 2 – Evaluation of anomaly scores of a) IF, b) LOF, c) OCSVM
Source: developed by the authors based on the data [5].

Fig. 2 (a) shows that IF algorithm detects numerous small deviations, with scores between 0.15 and 0.25 indicating moderate anomalous potential, suggesting sensor noise. A threshold can be set to identify stronger anomalies, such as scores above 0.25. In Fig. 2 (b) LOF method identifies most anomalies near 0, with sporadic significant outliers, indicating occasional deviations from the norm. In Fig. 2 (c), the OCSVM method maps anomalies within a narrow range, with peaks beyond ±10 indicating strong anomaly candidates, though frequent peaks suggest noise or model sensitivity.

Based on the analysis of both types of graphs on Fig. 1 and Fig. 2, LOF may be the most balanced method for detecting significant anomalies, reducing the risk of false positives. OCSVM can be used as a complementary method to provide broad anomaly detection, especially for large deviations. The IF method can be used for continuous monitoring with fine-tuned parameters to minimize minor anomaly detection.

In conclusion, having reliable automated systems that can detect faults in real time is crucial for enhancing the reliability and efficiency of production systems. Advanced data analysis methods for monitoring and diagnosing faults were explored to improve maintenance management. By integrating the advantages of IF, LOF, and OCSVM, the precision and reliability of fault detection in production systems can be greatly enhanced, reducing downtime and improving maintenance oversight.

References:

1. Amruthnath, N. and Gupta, T. (2018), “A research study on unsupervised machine learning algorithms for early fault detection in predictive maintenance”, 2018 5th International Conference on Industrial Engineering and Applications (ICIEA), pp. 355-361. https://dx.doi.org/10.1109/IEA.2018.8387124.

2. Isermann, R. (2009), “Fault Diagnosis Systems”, Springer, Berlin, Heidelberg, New York, 475 p. https://dx.doi.org/10.1007/3-540-30368-5.
3. Mallat, S.G. and Zhang, Z. (1993), “Matching pursuits with time-frequency dictionaries”, IEEE Transactions on Signal Processing, Vol. 41, No. 12, pp. 3397-3415. https://doi.org/10.1109/78.258082.
4. Perez, G.A. (2020), “Real-Time Fault Detection and Diagnosis Using Intelligent Monitoring and Supervision Systems”, Fault Detection, Diagnosis and Prognosis, IntechOpen. https://dx.doi.org/10.5772/intechopen.90158.
5. Schneider-Electric (2018), “Sensor Fault Detection Data”, available at: www.kaggle.com/datasets/arashnic/sensor-fault-detection-data (accessed 10 Sept. 2024).

UDK 004.9:37.091.2

Mykhailovska O.V.
student of higher education,
Educational and Scientific Institute of Computer Science and Artificial Intelligence of V. N. Karazin Kharkiv National University

SOFTWARE FOR ADDRESSING EDUCATIONAL NEEDS: TOOLS FOR STUDENT PERFORMANCE ANALYSIS

Introduction

In modern education, the analysis of student performance plays a key role in enhancing learning outcomes and fostering personalized teaching approaches. Software solutions designed to track and analyze student achievements allow educational institutions to monitor progress, identify learning gaps, and offer tailored support. Integrating such technologies into the educational environment increases the efficiency of academic processes and promotes data-driven decision-making.

Core Capabilities of Student Performance Analysis Software

Student performance analysis software collects data from various educational platforms, including grade books, attendance records, and learning management systems (LMS). This integration allows all critical information to be centralized, simplifying the monitoring process.

One of the main features is real-time progress tracking. This enables educators to quickly respond to changes in student performance and identify those who may need additional support. Modern platforms also utilize machine learning algorithms to predict academic outcomes based on attendance, participation, and past performance.

Advantages of Customizable Reports and Data Analysis

These software solutions offer customizable reports and dashboards, allowing educators and administrators to focus on specific data points, such as performance trends by subject or student engagement levels. The analysis of this data helps

identify problems early and adjust educational strategies accordingly. Teachers can adapt course content and teaching methods to meet the individual needs of students, creating personalized learning plans.

Examples of Popular Solutions

Among the software platforms facilitating student performance analysis are:

- *Edmodo Insights*, which combines LMS functions with performance analytics, offering tools for tracking exams and assignments while providing real-time academic insights.
- *Schoology Analytics*, which provides advanced analytics with customizable reporting options to assess student progress and course effectiveness.
- *Knewton*, which uses adaptive technology to personalize educational content based on student needs.
- *Illuminate Education*, which allows educators to collect and analyze both academic and behavioral data to identify problems and areas for growth.

Benefits of Implementing Student Performance Software

Using such tools provides numerous advantages, including:

- *Data-Driven Decision-Making* — Educators and administrators gain access to detailed reports that help them make informed decisions about adapting teaching strategies.
- *Enhanced Student Support* — Early identification of struggling students enables timely interventions and provides necessary support.
- *Transparency and Engagement* — These platforms give students, parents, and teachers access to comprehensive performance reports, fostering greater involvement in the learning process.

Challenges in Implementation

Despite clear benefits, the implementation of performance analysis software may face challenges such as:

- *High Costs and Integration Complexities* — Installing and configuring such software requires significant investments and time.
- *Data Privacy* — Ensuring platforms comply with data privacy regulations, such as FERPA, is critical.
- *Training Staff* — Successful implementation requires training educators and staff, which may demand additional resources.

Conclusion

Student performance analysis software is becoming an essential part of the modern educational process. It not only helps monitor academic progress but also personalizes learning plans, making the educational experience more adaptive to individual student needs. Despite challenges like cost and user training, the benefits of improving educational quality and efficiency far outweigh the difficulties. As technology continues to advance, the role of these software solutions will only grow, contributing to more personalized learning and better academic outcomes.

References:

1. BoldBI by Syncfusion. (2024). "*Educational Insights: Analyzing Student Performance with BI Dashboards*". [Online]. Available: https://www.boldbi.com/blog/educational-insights-analyzing-student-performance-with-bi-dashboards/
2. BROOKINGS. (2022). "*Digital tools for real-time data collection in education*". [Online]. Available: https://www.brookings.edu/articles/digital-tools-for-real-time-data-collection-in-education/
3. Kruger, D. (2020). Adaptive learning technology to enhance self-directed learning. *Self-Directed Multi-Modal Learning in Higher Education (NWU Self-Directed Learning Series), 5*, 93–116.Tempelaar, D. T., Rienties, B., & Giesbers, B. (2015). In Search for the Most Informative Data for Feedback Generation: Learning Analytics in a Data-Rich Context. Computers in Human Behavior, 47, 157-167. https://doi.org/10.1016/j.chb.2014.05.038

UDC 621.317

Skorin Yuriy
PhD, Associate Professor
Simon Kuznets Kharkiv National University of Economics
Zhu Huanyu
student of higher education
Simon Kuznets Kharkiv National University of Economics

APPLYING BUSINESS ANALYSIS TO IMPROVE INFORMATION SYSTEMS

In the current era of rapid development of information technology, information system has become the core tool to support enterprise operation and strategic decision-making.

These systems are not only responsible for the storage and processing of data, but also have a profound impact on business processes and customer experience.

With the deepening of digital transformation, enterprises are increasingly relying on information systems to improve efficiency, reduce costs and enhance competitiveness.

However, changing market demands, rapid advances in technology, and rising customer expectations have led many businesses to face the challenge that their information systems cannot effectively meet business needs.

The current information system often shows the problems of insufficient flexibility, poor integration and low user satisfaction.

These defects not only lead to the decline of operation efficiency, but also increase the waste of resources, which seriously affects the market competitiveness of enterprises.

To address these challenges, Business Analysis (BA), as a systematic methodology, is increasingly becoming an important tool for enterprises to solve information system problems.

Through in-depth requirements analysis, process optimization, and data-driven decision support, business analytics can help organizations identify critical issues in their information systems and develop targeted improvement strategies [1].

The core of business analytics is to understand and meet business needs, which can improve the adaptability and flexibility of information systems through a variety of means.

For example, through requirements analysis, business analysts are able to identify the real needs of users and ensure that the functional design of information systems is highly aligned with business objectives.

At the same time, process optimization can help enterprises re-examine existing workflows, eliminate redundancies and inefficiencies, and thus improve the overall performance of the system.

The application of data visualization technology provides intuitive decision support for management, helping them make fast and informed choices in a complex data environment.

This paper will explore the specific application of business analytics in information system improvement, in-depth analysis of how it can enhance the performance and adaptability of information systems through a series of practical methods, so as to create greater value for enterprises.

Through case study and theoretical analysis, this paper aims to provide strong support for enterprises to effectively use information systems in dynamic environment and promote their continuous innovation and development.

At the same time, this paper will also discuss the adaptability of business analytics in different industries, explore its effectiveness and flexibility in specific market environments, in order to provide theoretical basis and practical guidance for the future development of information systems, and help enterprises in the fierce market competition in an invincible position [2].

Purpose of work. The purpose of this paper is to optimize the performance of information systems in e-commerce platforms (taking Alibaba as an example), especially order management and logistics tracking systems, through the application of business analysis.

Through data-driven analysis methods, enterprises can improve their competitiveness in the market and improve the overall efficiency and user experience of information systems.

In addition, the paper aims to explore the application potential of big data, artificial intelligence and other technologies in enterprise information system optimization to help enterprises better respond to the rapid changes in market demand.

Research objects. The object of this study is the information system of e-commerce platform, especially the order management system (OMS) and logistics tracking system (LTS).

The research focuses on the performance of these systems in large-scale data processing and real-time response.

This paper chooses Alibaba as a case study to examine how the company improves its information system and improves operational efficiency through business analysis techniques and tools.

The research also covers platform users, order processes, inventory management and other system-related elements [1–4].

Research the topic.

The theme of the research is to improve the performance of information systems in e-commerce platforms through the application of business analytics techniques, especially for the optimization of order management and logistics systems.

The study explores how technical tools such as big data, artificial intelligence and machine learning can be used to identify bottlenecks in the system by analyzing order and logistics data and propose targeted optimization schemes.

Research topics include the improvement path of information systems, the impact of business analytics on system optimization, and the practical application of emerging technologies in information systems.

Research results. Through this research, the following results have been obtained. The key bottlenecks in e-commerce platform information system are identified, especially the efficiency of order management and logistics tracking system under high load operation.

This paper presents a specific method to optimize order management process by using business analysis tools, including data flow processing, predictive model application and automatic system resource adjustment scheme [7].

Through experimental verification, it is proved that after the introduction of machine learning model, the system performance is significantly improved during the peak order period, the order processing time is shortened, and the accuracy of logistics tracking is improved.

The results of this study provide a feasible optimization path for e-commerce platforms, and demonstrate the application effect of big data and artificial intelligence technology in actual business scenarios.

The results show that through the application of business analytics tools and technologies, enterprises can significantly improve the flexibility, responsiveness and scalability of information systems, thereby maintaining a leading position in a highly competitive market environment [1–6].

References

1. Davenport T. H. Artificial Intelligence for the Real World. / T. H. Davenport T. H.. Ronanki R. // Harvard Business Review, 96(1). – 2018. – pp. 108–116.

2. Chen H. Business Intelligence and Analytics: From Big Data to Big Impact / H. Chen, R. H. Chiang, V. C. Storey // MIS Quarterly, 36(4)). – 2012. – pp. 1165–1188.
3. Delen D., Demirkan, H. Data, Information and Analytics as Services / D. Delen, H. Demirkan // Decision Support Systems, 55(1) . – 2013. – pp. 359–363.
4. Shmueli G. Predictive Analytics in Information Systems Research / G. Shmueli, O. R. Koppius // MIS Quarterly, 35(3) . – 2011. – pp. 553–572.
5. Davenport T. H. Data Scientist: The Sexiest Job of the 21st Century / T. H. Davenport, D. J. Patil // Harvard Business Review, 90(10) . – 2012. – pp. 70–76.
6. Watson H. J. Tutorial: Big Data Analytics: Concepts, Technologies, and Applications / H. J. Watson // Communications of the Association for Information Systems, 34). – 2014. – pp. 1247–1268.
7. Mortenson M. J. Operational Research from Taylorism to Terabytes: A Research Agenda for the Analytics Age / M. J. Mortenson, N. F. Doherty, S. Robinson // European Journal of Operational Research, 241(3). – 2015. – pp. 583–595.
8. Gartner, W. B., Data-Driven Business Models for the Digital Economy / W. B. Gartner, K. Heine // Journal of Business Models, 3(2). – 2015. – pp. 1-13.
9. Wikipedia, the free encyclopedia. Management information system. URL : https://en.wikipedia.org/wiki/Management_information_system
10. What is Management Information Systems? URL : https://www.mtu.edu/business/what-is-mis/

UDC 621.317

Skorin Yuriy
PhD, Associate Professor
Simon Kuznets Kharkiv National University of Economics

DISTANCE LEARNING INFORMATION SYSTEMS FOR COMPUTER SUBJECTS

An analysis of modern methods and approaches to the problem of improving the quality of the educational process by creating distance learning information systems was conducted.

The most important tasks of increasing the level of computerization of the educational process were considered, the most appropriate areas of using information technology in the educational process were identified.

The most important role of information support for classes was noted, especially when using correspondence courses, as well as when students independently prepare for tests and examinations.

The purpose of the work is to justify the choice of software and methods for creating distance learning information systems, and practical suggestions for their use in the educational process were provided.

In modern conditions of intensive development of information technology, distance learning systems have found wide application in the process of training specialists.

Therefore, the development of distance learning courses is of considerable interest and the role of distance learning is difficult to overestimate.

Currently, a fairly large number of different manuals and teaching materials have been developed.

The analysis of existing systems and needs of distance learning allowed to form a nomenclature of requirements for the developed distance learning system, including all disciplines studied by students, on the basis of which the main functionality of the distance learning system was developed.

As a result of the analysis of the known software, the feasibility of using the Help&Manual software product as a software environment for creating distance learning information systems was substantiated, a version of the distance learning system was practically implemented and proposals for using the developed distance learning system in the educational process were developed.

The use of such distance learning systems in the educational process will effectively strengthen both traditional approaches to teaching academic disciplines and expand and even supplement the existing capabilities of both teachers and students.

It has been noted that at present, modern information systems and technologies are increasingly influencing the development of society.

In the system of higher education institutions, in their educational process, important and quite fundamental changes are taking place.

Thus, the introduction of a credit-modular system into the educational process has determined one of the most important tasks of building modern higher education, namely, the search for promising, rational ways to improve the level of training of specialists.

The introduction of modern computer systems and technologies into the educational process of higher education institutions, the development of modern computerized teaching aids, will significantly increase the efficiency of the educational process and provide significant information support for most of the classes conducted [1].

Thus, the effective computerization of the educational process will allow solving the following important tasks [1]:

- improving the professional knowledge and skills of students;
- increasing the level of mastering academic disciplines in the specialty;
- activating independent cognitive activity of students;
- improving the quality of assimilation of related disciplines by students;
- increasing the creative attitude of students to learning, etc.

The introduction of modern information technologies into the educational process will allow [1]:

- more effectively and efficiently use the latest achievements in the field of information technology in the educational process;
- conduct student training, including additional training, at a convenient time and in a convenient place;
- provide a real opportunity for simultaneous access of a significant number of students to databases;
- ensure more efficient use of both technical means and classroom space by teachers, etc.

It should be noted that computerization of the educational process will provide [1]:

- information support for classes using distance learning systems;
- conducting such types of classes as independent studies, preparation for exams and tests;
- information support for lectures on disciplines that require fairly large volumes of complex information in the form of graphic or text information.

Several users can participate in the creation of a project at the same time, i.e. the software has the ability to independently block the material that each specific user is currently editing.

The program provides a "read-only" mode for other users until the first user has completed their work.

The software allows you to store projects in a version control system, which provides additional security and the ability to work with different versions [5].

Based on the above, it can be argued that the Help&Mànuàl program is currently one of the best help file generators, on the basis of which it is possible to create quite powerful distance learning systems.

This is due to its versatility, convenient programming environment, wide range of tools, simple and understandable structure, and so on.

The developed system includes capabilities for both presenting educational material to students and for students to communicate with the teacher during the learning process and conducting quality control of knowledge [1].

In conclusion, I would like to note that the use of such distance learning systems in the educational process does not claim to replace the well-known traditional methods of teaching academic disciplines, but, on the contrary, only complements and expands the capabilities of both the teacher and the student [1].

References

1. Yu. I. Skorin. Improving the quality of the educational process through the development and testing of software for an information and simulation system based on virtual computer networks / Yu. I. Skopin, O. V. Shchebakov, I. O. Ushakova // Bulletin of the Kharkiv National Automobile and Road University. Collection of scientific papers. X.: I WILL. – 2022. – Issue 96. – pp. 141–145.

2. Korobko A.I. Virtual simulator of the accredited testing laboratory / A.I. Korobko, V.E. Shatikhina // Promising technologies and devices, No. 17 (December 24, 2020): pp. 72–78. URL : http://dx.doi.org/10.36910/6775-2313-5352-2020-17-11 http://htmleditors.ru/Ràsnoe/help/list2/help_&_mànuàl.html

3. Didenko O.K. Application of the method of controlled development behaviour for automation of web application testing // O. K. Didenko, D. Y. Holubnychyi // Proceedings of the International Scientific and Practical Conference of Young Scientists, Postgraduates and Students 'Information Technologies in the Modern World: Research of Young Scientists' 22 - 23 February 2024 - Kharkiv, 2024.

4. Help & Mànuàl overview - progràms for creàting help system files. URL : https://www.ixbt.com/soft/help-ànd-mànuàl.shtml

5. Virtual control and measuring devices and systems. URL : https://magnolia.lviv.ua/product/virtualni-kontrolno-vimiriuvalni-priladi-i-sistemi

6. Principles of development and use of virtual measuring tools URL : http://vtz.asv.gov.ua/article/view/174585

7. Theoretical foundations of modern Ukrainian pedagogy. URL : https://pedagogy.lnu.edu.ua/departments/pedagogika/library/vyshnevsky.pdf

8. Scientific novelty and theoretical significance of research results. URL : https://moodle.znu.edu.ua/mod/page/view.php?id=489528

9. Computer methods and means of solving engineering problems. URL : https://www.dstu.dp.ua/Portal/Data/3/21/3-21-mzs26.pdf

UDC 621.317

Skorin Yuriy
PhD, Associate Professor
Simon Kuznets Kharkiv National University of Economics

ENHANCING EDUCATIONAL EFFICIENCY THROUGH VIRTUAL SIMULATORS

An analysis of the current state of measuring technology and trends in its further development reveals that, alongside the advancement and enhancement of traditional measuring instruments, a relatively novel direction is emerging, namely the development of so-called virtual measuring instruments.

This is facilitated by three factors [1–4]:

- firstly, significant progress in the development of electronic computing equipment, as a result of which personal computers have become a common and even necessary tool for engineers, scientists, and teachers;
- secondly, the fleet of measuring equipment is often replenished and renewed not as fast as required by modern realities;
- and thirdly, the disruption of various integration links significantly complicates

the process of development and, most importantly, production of modern measuring instruments.

In this context of these considerations, it becomes evident that the search for alternative avenues to enhance the existing fleet of measuring instruments is imperative.

One such avenue is the development and creation of virtual measuring instruments.

In view of the progressive development of computing technology and the computerisation of all sectors of the economy, it seems reasonable to suggest that the powerful technological potential of computerisation could be harnessed to improve the measurement process in measuring systems.

The search for a solution has led to the creation of virtual instruments, which offer significant advantages over traditional instruments.

These advantages provide a rationale for the development of virtual computer simulators based on the virtualisation of the measurement process.

Such simulators could enhance the visibility and efficiency of the educational process, while also facilitating the expansion of the functionality of distance learning systems.

The relevance of this area is that [3; 4]:

- firstly, the composition of regular means of measuring equipment, which is available and necessary to ensure the quality of the learning process, as a rule, is limited, often requires repair, restoration or replacement, so the value of virtual computer simulators in such cases can hardly be overestimated;
- secondly, virtual computer simulators can provide practical skills in working with the most modern means of computer technology, which, due to limited technical or economic opportunities, are not yet used in teaching;
- thirdly, virtual computer simulators can be used by students during self-preparation for classes, because they are quite easy to operate, do not require special knowledge in the field of programming, are not critical to the hardware and software of a personal computer, contain hints and comments that practically guide the actions of the user, work out his mistakes;
- fourthly, virtual computer simulators, in our opinion, should be created, first of all, for the most modern devices that are not yet available in the laboratory and technical base of the university, also at the preliminary stage of preparation for work on regular equipment, during self-preparation for classes, in the case of distance learning, etc., that is, in cases where access to regular measuring equipment is limited or impractical;
- fifthly, a virtual computer simulator can be provided with additional functions that are not inherent in a real device, for example, to display physical processes that occur "inside" the device during a measurement experiment, inspection, as well as to provide reference information, to process and store measurement and diagnostic results, to test and monitor the level of knowledge of students, etc;
- sixthly, the virtual computer simulators considered in the article have an appearance that fully corresponds to the appearance of real devices, for this purpose,

non-standard ActiveX elements were created, which is also important in terms of the effectiveness of the learning process.

Hence, it is possible to formulate the objectives of the conducted research, which include substantiation of alternative ways to improve the fleet of measuring equipment by developing virtual measuring devices and improving the efficiency of the educational process by developing and implementing virtual computer simulators based on the created virtual devices.

This article puts forth the concept of implementing virtual simulators, based on virtual measuring instruments and the virtualisation of measurement processes, as a means of enhancing the educational process and improving the efficiency of advanced forms of professional training.

The research is based on an analysis of traditional measurement methods and tools, and it proposes the virtualisation of the measurement process as an alternative solution.

The study assesses the benefits and applications of virtual instruments.

It is observed that, in addition to their intended function as virtual measuring instruments, virtual devices demonstrate considerable potential for the development of virtual simulators. These simulators enhance the clarity and quality of education, particularly in instrument-based disciplines, thereby creating a foundation for their inclusion in existing or newly developed distance learning systems [1–4].

The research comprises an analysis and synthesis of the experience of utilising contemporary measurement methods and tools, an identification of the advantages and disadvantages of traditional measurement approaches, a substantiation of the selection of measurement process virtualisation as the most efficacious means of enhancing instrument equipment, an examination of the structure and methodologies employed in the construction of virtual instruments and an assessment of their applications, and a delineation of virtual instruments as a foundation for the development of virtual simulators that enhance the efficacy and clarity of the educational process and establish the prerequisites for the advancement and enhancement of distance learning systems.

References

1. Yu.I. Skorin Virtual devices in the measuring laboratory / Yu.I. Skorin, V.V. Stadnik, A.M. Klymenko // Bulletin of the National Technical University "KhPI". Collection of scientific papers. Series: Informatics and modeling. – Kharkiv: NTU "KhPI". – No. 38. – 2012. – P. 84–92.

2. Yu. I. Skorin. Improving the quality of the educational process through the development and testing of software for an information and simulation system based on virtual computer networks / Yu. I. Skopin, O. V. Shchebakov, I. O. Ushakova // Bulletin of the Kharkiv National Automobile and Road University. Collection of scientific papers. X.: I WILL. – 2022. – Issue 96. – pp. 141–145.

3. Yu. I. Skorin Virtual measuring and diagnostic devices / Yu. I. Skorin, O. V. Shcherbakov, T. I. Magdalits // Information processing systems. Collection of scientific papers. Issue 4(102), volume 1. Information technologies and information

protection. X.: HUPS. - 2012. - P. 65–68.
4. Yu.I. Skorin. Work program of the study discipline "Metrology and standardization" for students of the "Computer science" training direction of all forms of education / Yu.I. Skorin, V.V. Fedko, O. V. Shcherbakov. – Educational edition. Kharkiv: Ed. Khneu, 2012. – 48 p.
5. Virtual control and measuring devices and systems. URL : https://magnolia.lviv.ua/product/virtualni-kontrolno-vimiriuvalni-priladi-i-sistemi
6. Principles of development and use of virtual measuring tools URL : http://vtz.asv.gov.ua/article/view/174585
7. Theoretical foundations of modern Ukrainian pedagogy. URL : https://pedagogy.lnu.edu.ua/departments/pedagogika/library/vyshnevsky.pdf
8. Scientific novelty and theoretical significance of research results. URL : https://moodle.znu.edu.ua/mod/page/view.php?id=489528
9. Computer methods and means of solving engineering problems. URL : https://www.dstu.dp.ua/Portal/Data/3/21/3-21-mzs26.pdf
10. Korobko A.I. Virtual simulator of the accredited testing laboratory / A.I. Korobko, V.E. Shatikhina // Promising technologies and devices, No. 17 (December 24, 2020): pp. 72–78. URL : http://dx.doi.org/10.36910/6775-2313-5352-2020-17-11

UDC 621.317

Skorin Yuriy
PhD, Associate Professor
Simon Kuznets Kharkiv National University of Economics

THE MANAGEMENT OF SCALABILITY IN CLOUD-BASED APPLICATIONS MODULE

Today's world is characterised by the rapid development of information technology, which is having a significant impact on all aspects of human activity.

The automation of business processes is particularly important, as it allows companies to improve their efficiency, optimise costs and increase the speed of response to market changes.

The use of cloud technologies is becoming an answer to the need for flexibility and scalability of IT infrastructure, allowing resources to be dynamically scaled up and down according to business needs [1].

Growing volumes of data and the need to process it require monitoring systems to be highly efficient and able to scale quickly.

However, traditional approaches often prove too inflexible or costly to deploy, prompting the search for new solutions.

In this context, cloud technologies offer the opportunity to efficiently deploy and scale monitoring and resource management systems, enabling high availability and reliability of IT services.

The need to develop systems capable of automatically adapting to changing workloads and optimising resource utilisation is being driven by increasing demands for efficiency in processing large amounts of data and the need to reduce the cost of maintaining IT infrastructure.

The relevance of the study focuses on the critical need to improve and optimise cloud resource scalability management systems.

With the rapid development of technology and the increase in data volumes, effective management of cloud infrastructure resources is becoming a critical factor in ensuring high performance and availability of online services.

Cloud technologies offer great opportunities for scalability and elasticity, but also require granular control and adaptive management to ensure an optimal performance/cost ratio [2; 3].

Today's business requirements change frequently, requiring scalability monitoring and management systems to adapt quickly and automatically to these changes.

Developing a module that can analyse current performance and resource usage and automatically adjust system scaling based on this analysis meets these requirements.

This not only ensures business continuity, but also contributes to a significant reduction in IT infrastructure maintenance costs.

Thus, the relevance of this study lies in the need to develop effective solutions for dynamically managing the scalability of cloud resources that can ensure high availability and performance of services at optimal cost.

The aim of this paper is to implement a software module for monitoring and managing the scalability of a cloud application based on the AWS (Amazon Web Services) platform and managed by Terraform [3].

The main idea is to create a system capable of automatically analysing current resource usage and adaptively adjusting service scaling based on the data obtained.

This will help to increase system efficiency, reduce overall maintenance costs and increase end-user satisfaction by maintaining optimal application performance.

The following is an abstract of the article.

The article presents an analysis of the challenges associated with monitoring and managing the scalability of a cloud application.

To this end, a module for monitoring and managing the scalability of a cloud application has been developed as part of this study.

The development process included the introduction of automatic scaling, and monitoring using Prometheus and Grafana, which allows for a high level of availability and resource efficiency.

The study comprised a series of phases, including requirements analysis, system design, development, testing, and evaluation.

Consequently, the system's performance, stability, and capacity to scale in response to fluctuating workloads were enhanced.

The module exhibits a high degree of adaptability to changes in system requirements and load, which is a crucial attribute for the dynamic development of business applications.

This solution assists in optimizing the allocation of resources and reducing infrastructure costs.

The project has been found to fully meet the set goals and objectives, as well as the requirements for effective resource management of the Amazon Web Services cloud platform using Terraform, Prometheus, and Grafana.

The practical value of the developed module is evidenced by a significant improvement in resource efficiency, service stability and cost optimisation.

The module design has been subjected to rigorous testing and has been successfully implemented in a test environment, thereby demonstrating the sustainability and efficiency of the developed solution.

The experience gained in the implementation and operation of this solution may prove useful for further expansion and optimization of cloud solutions in other projects and companies specializing in the provision of cloud solutions [2–4].

The findings of this study were validated in a test environment at an IT company with a specialization in cloud technologies.

The objective was to ascertain the functionality and efficiency of the developed module in a real-world context of cloud infrastructure operation.

The testing process entailed the configuration of the module on pre-existing cloud infrastructure systems, its integration with Prometheus and Grafana for monitoring purposes, and the execution of a series of stress tests designed to assess the module's scalability.

As a result of this testing, a number of critical points were identified that required further optimization.

The results of the study and the issues identified during the project testing have enabled the identification of several areas for further improvement and development of the system.

First and foremost, the optimization of automatic scaling algorithms represents a crucial avenue for improvement.

The development of these algorithms should be oriented towards utilizing historical monitoring data to anticipate potential shifts in system load.

Another pivotal area for enhancement is the precision of monitoring systems.

The integration of supplementary tools and the expansion of existing monitoring systems' functionality will facilitate the acquisition of more comprehensive insights into the system's condition [2; 7].

This, in turn, will facilitate the expedient identification and eradication of potential issues.

References

1. Didenko O.K. Application of the method of controlled development behaviour for automation of web application testing // O. K. Didenko, D. Y. Holubnychyi // Proceedings of the International Scientific and Practical Conference

of Young Scientists, Postgraduates and Students 'Information Technologies in the Modern World: Research of Young Scientists' 22-23 February 2024 – Kharkiv, 2024.

2. Nystopad Yurii. Development of a module for monitoring and managing the scalability of a cloud application based on AWS and Terraform // Yurii Lystopad, Yurii Skorin // Proceedings of the International Scientific and Practical Conference of Young Scientists, Postgraduate Students and Students 'Information Technologies in the Modern World: Research of Young Scientists' 22-23 February 2024 – Kharkiv, 2024.

3. Yevhen Brykman. Terraform: infrastructure at the code level, 2024. URL : https://bambooks.com.ua/ua/p1809769909-kniga-terraform-infrastruktura.html

4. Jack Dwyer. Automating Cloud Infrastructure with Terraform CI CD: A Step-by-Step Guide, 2024. URL : https://zeet.co/blog/terraform-ci-cd

5. Aalok Trivedi. Leveraging high availability by creating an AWS Auto scaling group & application load balancer, 2023. URL : https://medium.com/@aaloktrivedi/leveraging-high-availability-by-creating-an-aws-auto-scaling-group-application-load-balancer-2ea1f31a746

6. Real-time Monitoring and Analysis of Edge and Cloud Resources, 2023. URL : https://dl.acm.org/doi/10.1145/3589010.3594892

7. Scalability as a software requirement, meaning and definition. URL : https://uk.itpedia.nl/2021/07/20/schaalbaarheid-als-software-requirement-betekenis-en-definitie

UDC 621.317

Skorin Yuriy
PhD, Associate Professor
Simon Kuznets Kharkiv National University of Economics

USABILITY TESTING FOR USER INTERFACES

The paper analyzes the problems of improving the quality of software, namely usability testing as one of the areas of ensuring this quality, analyzes publications that consider such methods as:

- electrooculography;
- electroretinography;
- mouse tracking;
- eye tracking

etc. and concludes that improving the quality of software directly depends on how effective the usability testing process will be [1].

An analysis of traditional tools and methods for testing software products was carried out and, as a result, mouse tracking technology and eye tracking technology were proposed as an alternative solution to the problem of improving the quality of software products.

Also, the criteria and metrics for assessing the usability of web applications were determined, and an analytical approach consisting of a comprehensive analysis of the research object was proposed as a methodological basis, classification and comparative analysis methods were also used, and the results were analyzed using standard statistical methods.

An assessment of the importance and necessity of usability testing of websites was also carried out.

The work considered generally accepted rules and recommendations in the field of usability testing, analyzed both quantitative and qualitative methods of analysis and evaluation of usability testing.

In order to study the object of study in more detail, the ergonomic interaction between the user and the information system, namely, with the web resource, was considered, important categories of users depending on a number of indicators were considered and analyzed, special attention was paid to the analysis of quality assessment criteria using existing standards and recommendations.

A thorough analysis of the usability testing process of software interfaces was carried out in order to analyze and evaluate methods for improving the quality of software and optimization by reducing the time of the usability testing process [2].

Also, conditions were prepared for an experimental study of the results considered theoretically based on eye tracking technology.

Today, a tendency for large-scale shifts has clearly emerged, both in scientific and applied areas, where the ergonomics of software is increasingly playing a key role.

This is the commercial attractiveness of software products, as well as the degree of their penetration into the market and the subjective satisfaction of users when working with these products.

The practical side of this study is closely related to the significant evolution of technological support, the rapid development of the Internet and the expansion of the scope of application of computer interfaces for a wide variety of user nomenclature [3].

A significant increase in the number of tasks that must be served by an ever-expanding range of users is due to an increasingly noticeable trend associated with computerization and the gradual replacement of personal information exchange between users and information systems in most professional areas.

Active improvement of standards that are designed to regulate the ergonomics of software is an important condition for achieving the required level of accessibility in the information environment.

Accessibility orchestration is organically integrated into a wider range of design and development processes, covering a methodical description of accessibility requirements, a quantitative assessment of accessibility indicators and the formulation of a distinguishable criterion for verification within the framework of user interaction [5].

The process of determining the degree of usability of software is of utmost importance, which is due to the complexity of the interaction between the user and the software, as well as other components of the software product.

Thus, any software product or device can have different degrees of usability for the user in different use cases, which plays a significant role, especially in scenarios involving different segments of users with certain disabilities [6].

In order to improve the quality and efficiency of the usability testing process, a comparative analysis of testing methods was carried out, namely:

- eye tracking method;
- mouse tracking method.

Using these technologies, the required conditions for performing experimental studies of theoretical results were established.

It was noted that, based on both the results of foreign and domestic studies, the selected method based on eye tracking is more effective for usability testing, primarily due to the significant, both quantitative and qualitative results obtained in one testing session.

It should be noted that the usability testing processes using the mouse tracking method and the eye tracking method have significant.

References

1. Dibrova T. G. Evaluation of the effectiveness of advertising by methods of physiological control / T. G. Dibrova, I. I. Garanina // Ekon. vistnyk of the National Technical University of Ukraine "KPI": collection of scientific papers – 2013. – Issue 10. – P. 316-320.

2. Kirilenko O. Methods for evaluating the usability of the user interface / O. Kirilenko, Y. Kuznetsova, E. Sokolova, G. Frolova // Bulletin of the National University "Lviv Polytechnic". – 2013. – № 751. – C. 244-256.

3. Kuznetsova Y. A. Visualisation of control algorithms in an automated testing system of a complex technical complex: PhD thesis: 05.13.06 / Y. A. Kuznetsova; National Aerospace University named after M. E. Zhukovsky – Kharkiv, 2015. 20 p.

4. Datsun N. M. Increasing the efficiency of the user interface of virtual laboratory work [Electronic resource] / N. M. Datsun, O. A. Goretsky // Scientific works of Donetsk National Technical University. Series: Informatics, Cybernetics and Computer Science. – 2012. – Vol. 15. – P. 239-244. – Access mode: http://nbuv.gov.ua/UJRN/Npdntu_inf_2012_15_36

5. New concepts of modern ergonomics [Electronic resource] / G.V. Migal. Myhal, O.F. Protasenko // Open information and computer integrated technologies. – 2018. – Issue 79, pp. 162-170. – URL : http://nbuv.gov.ua/UJRN/vikt_2018_79_20

6. Mouse Tracking. URL : https://en.ryte.com/wiki/Mouse_Tracking

7. Improving your website with Mouse Tracking. URL : https://zwebra.com.ua/uluchshenie-sajta-pri-pomoshhi-mouse-tracking.html

8. The Power of Eye Tracking Research: What Types of Research Can Be Conducted in Different Industries. URL :

https://eyeware.tech/uk/blog/%D0%B4%D0%BE%D1%81%D0%BB%D1%96%D0%B4%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F%D1%81%D0%BF%D0%BE%D1%81%D1%82%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F%D0%B7%D0%B0%D0%BE%D1%87%D0%B8%D0%BC%D0%B0/
9. Systems and methods of decision support. URL : https://ela.kpi.ua/bitstream/123456789/48418/1/Systemy_i_metody_pidtrymky_pryniattia_rishen.pdf
10. Usability testing. URL : https://en.wikipedia.org/wiki/Usability_testing

УДК 004.8:7.05

Андрющенко Т.Ю.
ст. викладач, кафедри медіасистем та технологій
Харківський національний економічний університет ім. Семена Кузнеця

АВТОМАТИЗАЦІЯ ДИЗАЙНУ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ: ГЕНЕРАЦІЯ ДИЗАЙНІВ

Актуальність теми полягає у швидкому розвитку технологій штучного інтелекту (ШІ) та їх впровадженні в усі сфери життя, включаючи дизайн. У сучасному світі компанії та дизайнерські агентства стикаються з необхідністю швидко створювати якісні та адаптивні графічні рішення для різних платформ і форматів, враховуючи при цьому зростаючі вимоги до персоналізації контенту.

Таким чином, автоматизація дизайну за допомогою ШІ є не лише інноваційним підходом, але й відповідає потребам сучасного бізнесу, підвищуючи продуктивність, знижуючи витрати та допомагаючи створювати більш персоналізований і якісний контент.

Мета дослідження – огляд сучасних можливостей ШІ в автоматизації дизайну, розгляд переваг та викликів.

ШІ не лише змінює підхід до створення дизайну, але й сприяє появі нових стандартів в індустрії. Завдяки інтелектуальним алгоритмам дизайнери можуть швидко створювати візуальні макети, прототипи, а також отримувати рекомендації, що базуються на даних про поведінку користувачів [1].

ШІ революціонізує процес проектування завдяки використанню алгоритмів машинного навчання. Наприклад, ці системи аналізують величезну кількість даних про історію модних тенденцій, уподобання споживачів і навіть культурні впливи. Це дозволяє дизайнерам передбачити, які візерунки та стилі стануть популярними в майбутньому, уникаючи ризиків, пов’язаних із сліпим дизайном. Крім того, генеративні моделі штучного інтелекту можуть створювати оригінальні моделі та концепції, які можуть використовуватися дизайнерами як натхнення. Цей інструмент стимулює творчість, допомагаючи

створювати унікальні колекції, які привертають увагу споживачів, які шукають сучасні та інноваційні рішення у світі моди [2].

Інструменти графічного дизайну зі штучним інтелектом змінюють умови праці дизайнерів, надаючи їм нові можливості для створення, налаштування та вдосконалення своєї роботи. Ці інструменти підвищують творчу продуктивність і роблять якісний графічний дизайн більш доступним. Завдяки автоматизації повторюваних дій, таких як видалення фону та поєднання шрифтів, вони створюють унікальні, персоналізовані зображення — навіть для тих, хто не є професійним дизайнером [3].

Переваги автоматизації дизайну за допомогою ШІ:

швидкість: Генерація великої кількості варіантів дизайнів за короткий час. ШІ здатний автоматично генерувати дизайни за лічені хвилини, що значно скорочує час, необхідний на розробку візуальних рішень, у порівнянні з традиційними методами;

творчість: Здатність генерувати нестандартні та оригінальні рішення;

персоналізація: Створення дизайнів, які відповідають індивідуальним потребам користувачів. ШІ може аналізувати великі обсяги даних і створювати персоналізовані дизайни, орієнтовані на конкретну аудиторію, що підвищує ефективність;

економія ресурсів: Зменшення витрат на наймання дизайнерів та ручну роботу. Завдяки автоматизації багатьох процесів, компанії можуть скоротити витрати на дизайн і одночасно підвищити продуктивність команд.

Виклики та обмеження:

якість: Не завжди можна досягти високої якості дизайнів, особливо для складних завдань;

творчий контроль: Відсутність повного контролю над процесом генерації. Дизайнери можуть зіткнутися з труднощами у внесенні особистих творчих ідей, оскільки автоматизовані процеси можуть обмежувати можливість для ручного втручання або індивідуальної адаптації;

етичні питання та авторське право: Можливість генерування стереотипних або образливих зображень. Проблеми визначення авторства та захисту інтелектуальної власності.

Отже, автоматизація дизайну за допомогою штучного інтелекту є потужним інструментом, що значно спрощує та прискорює процес розробки візуальних рішень. Хоча ШІ може автоматизувати певні етапи креативного процесу, створюючи унікальні дизайни на основі параметрів та аналізу даних, він не замінює людську творчість повністю. Це відкриває нові можливості для швидкої адаптації до ринкових змін та динамічних трендів, надаючи дизайнерам більше часу для зосередження на стратегічних та художніх аспектах роботи. ШІ виступає доповненням, підвищуючи ефективність та гнучкість дизайнерських рішень.

Таким чином, хоча автоматизація дизайну за допомогою ШІ відкриває широкі можливості для ефективності та оптимізації процесів, вона

супроводжується низкою обмежень, які вимагають обережного підходу до її впровадження.

Список використаних джерел:

1. Штучний інтелект для дизайнерів: топ-8 корисних інструментів для роботи. URL : https://proit.ua/shtuchnii-intieliekt-dlia-dizainieriv-top-8-korisnikh-instrumientiv-dlia-roboti/ (дата звернення 28.09.2024).

2. Про використання можливостей ШІ в дизайні та виробництві TCLF. URL : https://ukrlegprom.org/ua/news/pro-vykorystannya-mozhlyvostej-shi-v-dyzajni-ta-vyrobnycztvi-tclf/. (дата звернення 28.09.2024).

3. 14 інструментів штучного інтелекту для графічних дизайнерів. URL : https://thetransmitted.com/ai/14-instrumentiv-shtuchnogo-intelektu-dlya-grafichnyh-dyzajneriv-cherven-2024/. (дата звернення 28.09.2024).

УДК 005.8

Баришевський А.І.
аспірант
кафедри інтелектуальної власності та управління проєктами
Науковий керівник:
Петренко В.О.
д.т.н., проф.
Український державний університет науки і технологій

ОГЛЯД СУЧАСНИХ ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ ДАНИХ

В сучасному світі, коли всі процеси максимально оцифровані (завдяки цифровій трансформації) і їх проміжні й кінцеві результати фіксуються і зберігаються у вигляді даних, виникає потреба ці дані аналізувати. І як результат аналізу - робити якісь висновки, прогнози, або ж приймати рішення на основі даних. Це значно підвищує шанси прийняти вірне рішення.

Отже, Data-driven decisions (рішення, засновані на даних) — це процес прийняття рішень на основі аналізу й інтерпретації даних, а не на інтуїції, припущеннях чи особистому досвіді. Це підхід, коли всі кроки та вибір робляться після оцінки об'єктивної інформації, отриманої з різних джерел даних. Основними аспектами прийняття рішень на основі даних є:

1) Збір даних з різних джерел — бізнес-операцій, клієнтської поведінки, ринку, соціальних медіа тощо.

2) Аналіз даних може включати статистичний аналіз, машинне навчання та інші методи, що дозволяють виявляти патерни або тренди в даних.

3) Інсайти або висновки, які показують, що насправді відбувається в бізнесі, на ринку або з клієнтами.

4) Прийняття рішень після оцінки результатів аналізу. Це дозволяє уникнути суб'єктивності та помилок, які можуть виникати через обмеженість людської думки чи емоції.

5) Постійний моніторинг: Після прийняття рішень дані продовжують аналізувати, щоб перевірити, чи було прийняте рішення ефективним і чи потрібно його коригувати.

І наразі всі ці аспекти можуть бути об’єднані у програмних продуктах, які дозволяють також прогнозувати тренди (predictive analytics), та візуалізувати інформацію для кращого розуміння бізнес-процесів. Вибір конкретного інструменту залежить від потреб бізнесу, обсягів даних та спеціальних вимог до аналітики.

Нові програмні рішення для предиктивної аналітики використовують штучний інтелект (ШІ) і машинне навчання (МН) для прогнозування всього - від споживчого попиту і продуктивності робочої сили до непередбачуваних економічних подій.

Ось 3 найбільш потужні з них у 2024:

1) SAP Analytics Cloud допомагає підприємствам планувати, складати бюджети та прогнозувати, усуваючи потребу в окремих додатках для кожної функції. Функція сценарного планування дозволяє створювати бюджети та плани на основі змодельованих сценаріїв «що буде, якщо».

Завдяки функціям спільної роботи ви можете обговорювати плани з членами вашої команди. Потужні функції візуалізації даних допоможуть вам легко зрозуміти ваші сценарії та плани.

Нарешті, він також має попередньо створений бізнес-контент, заснований на різних найкращих практиках. Цей контент слугує шаблоном для прийняття рішень або відправною точкою для планування сценаріїв, таким чином прискорюючи темп, з яким ви можете будувати свої плани та прогнози.

2) Amazon QuickSight - це платформа бізнес-аналітики, яка є частиною Amazon Web Services (AWS). Функціонал предиктивної аналітики дозволяє створювати прогнози на основі декількох сценаріїв «що було б, якби», і він досить розумний, щоб автоматично виключати аномалії даних.

Створені прогнози також можна нанести на будь-який графік, який можна вбудувати у ваш аналіз. Потім ви можете відображати свої аналізи з графіками прогнозів на спеціальних інформаційних панелях проєктів, якщо ви хочете їх постійно відстежувати.

Ще однією важливою особливістю Amazon QuickSight є функція під назвою Q, яка стосується підтримки запитів на природній мові (NLQ). Функція Q дозволяє вам отримувати інформацію на основі даних з платформи, ставлячи запитання так само, як ви б поставили їх людині.

3) Oracle Analytics виділяється серед інструментів предиктивної аналітики тим, що може бути розгорнута трьома способами: у хмарі, локально або гібридно (тобто хмара + локально). Вона дозволяє створювати та навчати

власні прогнозні моделі, використовуючи різні алгоритми машинного навчання, вбудовані в платформу.

Платформа також має широкі можливості візуалізації даних. Ви можете створювати власні інформаційні панелі з діаграмами, тепловими картами, картами зображень та 42 іншими типами візуальних компонентів, щоб бачити свої прогнози саме так, як ви хотіли б.

Список використаних джерел

1) Stylianos Kampakis (2021). Data Science for Decision Makers & Data Professionals. Apress.

2) Tobias Zwingmann (2022). AI-Powered Business Intelligence. O'Reilly.

3) ClickUp engineering team (2024). Top 10 Predictive Analytics Software to Make Data-Driven Decisions.

4) Mike Fleckenstein, Lorenz Ebner (2022). Modern Data Strategy. Springer.

УДК 004:336

Бачинський Д. В.
здобувач вищої освіти,
Хмельницький університет управління та права імені Леоніда Юзькова
Науковий керівник
Фасолько Т. М.
к.е.н., доцент кафедри математики, статистики
та інформаційних технологій
Хмельницький університет управління та права імені Леоніда Юзькова

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ГОЛОВНИЙ ІНСТРУМЕНТ В УПРАВЛІННІ ФІНАНСАМИ

У сучасних умовах інформаційні технології відіграють важливу роль у всіх сферах суспільства: економіці, виробництві та управлінні підприємством. Сучасне управління фінансами не є виключенням. Воно все більш стає неможливим без активного використання інформаційних технологій (ІТ), зокрема за умов глобальної діджиталізації фінансового сектору. Тому варто звернути увагу на роль інформаційних технологій в ефективному управлінні фінансовими ресурсами.

Інформаційні технології виступають ключовим інструментом у різних аспектах управління фінансами. Останніми роками ІТ набули значного поширення завдяки здатності швидко й точно обробляти великі обсяги даних, порівняно з традиційними методами фінансового управління. ІТ змінюють підходи до фінансового менеджменту за допомогою таких інструментів, як автоматизація процесів, прогнозна аналітика, управління ризиками та оптимізація інвестиційних рішень. Автоматизовані системи обліку та

управління фінансами надають можливість бізнесам знижувати витрати, ефективніше контролювати фінансові потоки, а також приймати зважені рішення в умовах нестабільності ринку.

В Україні інформаційні технології активно впроваджуються у фінансовий сектор для підвищення його ефективності та прозорості. Зокрема, багато компаній використовують хмарні рішення для управління фінансами, що дозволяє зменшити витрати на інфраструктуру та забезпечити доступ до даних у реальному часі. Онлайн-банкінг набуває широкого поширення, а банки активно розвивають мобільні додатки для зручного управління фінансами клієнтів. Крім того, українські фінансові установи все частіше використовують Big Data та штучний інтелект для прогнозування фінансових ризиків і шахрайства. Впровадження блокчейн-технологій допомагає забезпечити безпеку транзакцій та знизити корупційні ризики. Однак, кібербезпека залишається значною проблемою, оскільки фінансові установи стикаються з постійними кіберзагрозами.

За прогнозами, роль інформаційних технологій у фінансовому секторі продовжуватиме стрімко зростати, досягнувши 170 мільярдів доларів до 2028 року. Основними рушійними силами цього зростання є штучний інтелект, блокчейн, машинне навчання та Big Data. Ці технології дозволяють знижувати витрати, підвищувати прозорість операцій і забезпечувати ефективне управління ризиками. Очікується, що глобальні збитки від кіберзлочинності у фінансовому секторі зростуть до 10,5 трильйонів доларів до 2025 року, що підвищує попит на безпечні IT-рішення. Штучний інтелект вже допомагає виявляти шахрайство в реальному часі, що знижує ризики фінансових втрат. Інвестиції у фінтех-сектор можуть зрости до 310 мільярдів доларів до 2027 року, зокрема для розвитку цифрових банків і роботизованих радників. Блокчейн-технології допоможуть скоротити витрати на транзакції, усуваючи посередників. Це може зекономити фінансовому сектору до 27 мільярдів доларів щороку. Аналітика на основі Big Data покращує прийняття рішень, допомагаючи управлінцям швидко реагувати на ринкові зміни.

Розглядаючи інформаційні технології в управлінні фінансами, вважаємо необхідним детальніший аналіз впливу кожної досліджуваної нами технології на конкретні аспекти управління фінансами, зокрема хмарні технології та онлайн-банкінг значно покращують управління фінансами, забезпечуючи доступ до даних і послуг у будь-який час і з будь-якої точки. Хмарні рішення дозволяють компаніям знижувати витрати на інфраструктуру та забезпечують гнучкість в управлінні фінансовими потоками. Онлайн-банкінг пришвидшує операції та робить фінансові послуги доступнішими, зокрема для малого і середнього бізнесу. Автоматизація на базі хмарних технологій допомагає уникати людських помилок, а розвиток мобільних додатків підвищує прозорість фінансових операцій.

Технології Big Data та штучний інтелект дають змогу обробляти великі обсяги даних для прогнозування фінансових результатів і управління ризиками. Big Data допомагає банкам точніше оцінювати кредитні ризики та прогнозувати

можливі економічні коливання. Штучний інтелект автоматизує фінансові процеси, включно з обробкою транзакцій і виявленням шахрайства в реальному часі. Завдяки AI компанії можуть швидше приймати рішення, знижуючи витрати та підвищуючи ефективність управління фінансами.

Використання інформаційних технологій у фінансовому управлінні не лише відкриває нові можливості, але й створює ряд викликів. Однією з основних проблем є необхідність постійного оновлення систем безпеки, оскільки кіберзлочинці постійно знаходять нові способи атак на фінансові установи. Важливо забезпечувати надійний захист від витоку даних і шахрайства, особливо враховуючи зростаючу кількість електронних транзакцій. Ще одним викликом є підтримка конфіденційності фінансових даних, адже зростання кількості операцій в інтернеті підвищує ризики витоку персональної та фінансової інформації клієнтів.

Контроль за прозорістю автоматизованих рішень також є важливою проблемою. Алгоритми, що приймають фінансові рішення, можуть бути складними для розуміння та не завжди прозорими, що може викликати недовіру у користувачів і регуляторів. Успішна інтеграція ІТ у фінансовий сектор також залежить від якості даних, які використовуються для аналізу. Якщо дані є неповними або неточними, це може призвести до неправильних рішень, що негативно вплине на ефективність фінансових операцій.

Технічна інфраструктура є ще одним ключовим аспектом, який визначає успішність впровадження ІТ у фінансове управління. У багатьох країнах, особливо тих, що розвиваються, технічна інфраструктура може бути недостатньо розвиненою для впровадження сучасних технологій. Це ускладнює доступ до інноваційних фінансових послуг і створює нерівні умови для учасників ринку.

Загалом, безперервний розвиток інформаційних технологій робить їх незамінним інструментом у сучасному управлінні фінансами. Використання автоматизованих систем і аналітичних інструментів підвищує ефективність і точність фінансових рішень, забезпечуючи їхню безпеку та прозорість. Однак, для повної інтеграції ІТ у фінансовий сектор необхідно вирішувати існуючі виклики та постійно вдосконалювати технології та інфраструктуру.

Список використаних джерел:

1. Грибовська Ю. М., Кононенко Ж. А. Застосування інформаційних систем в управлінні підприємством. *Економіка та суспільство*. 2023. URL: https://www.economyandsociety.in.ua/index.php/journal/article/view/2171/2098.

2. Парубець О. М., Сугоняко Д. О., Середюк І. О. Дослідження сучасного стану та перспектив розвитку штучного інтелекту у фінансовому секторі України. *Фінансові дослідження*. 2019. URL: https://fr.stu.cn.ua/tmppdf/183.pdf.

3. Стратегія розвитку штучного інтелекту в Україні: монографія / А. І. Шевченко, С. В. Барановський, О. В. Білокобильський, та ін. Київ: ІПШІ, 2023. 305 с.

УДК 336.7:004.8

Білий В. С.
здобувач вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Науковий керівник
Азаренкова Г.М
д.е.н, проф., зав. кафедри банківського бізнесу та фінансових технологій
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ У БАНКІВСЬКОМУ ОБСЛУГОВУВАННІ: РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ДИСТАНЦІЙНИХ ПОСЛУГАХ

Сучасний фінансовий сектор постійно змінюється під впливом стрімкого розвитку цифрових технологій. Однією з найперспективніших інновацій, яка революціонізує банківські процеси, є штучний інтелект. Впровадивши його в банківську сферу, можна підвищити ефективність обслуговування клієнтів, оптимізувати бізнес-процеси та значно підвищити якість дистанційного обслуговування. Загалом, тема розвитку штучного інтелекту та розвитку цифрових технологій стає все більш популярною. З кожним роком проводиться все більше досліджень. Наприклад: аналіз досвіду цифровізації українських банків навели у своїй роботі Баришевська І. В. та Сизоненко Ю. С. [1], А. С. Завербний і Н. Р. Сокульський [2], де автори зосередили увагу на окремих аспектах розвитку технологій штучного інтелекту в банківському секторі.

Головна перевага використання штучного інтелекту в банківській справі є автоматизація рутинних завдань. Тому багато банків активно використовують чат-боти для відповіді на поширені запити клієнтів, надання консультацій та підтримки у фінансових операціях. Це дозволяє безперервно обслуговувати клієнтів.

Крім того, штучний інтелект відіграє важливу роль у забезпеченні безпеки фінансових операцій. Банки використовують системи штучного інтелекту для автоматичного моніторингу транзакцій і виявлення підозрілої активності. Алгоритми можуть аналізувати поведінку клієнтів у реальному часі та виявляти можливі шахрайські транзакції. Це сприяє зниженню ризику фінансових злочинів і забезпечує вищий рівень довіри до банківських установ. Наприклад, системи розпізнавання обличчя або голосу на базі штучного інтелекту використовуються для ідентифікації клієнтів під час доступу до послуг онлайн-банкінгу, що забезпечує додатковий рівень захисту.

Проте, впровадження ШІ також пов’язане з власними ризиками та проблемами. Найбільш гострою проблемою є відсутність правового регулювання використання штучного інтелекту в банківській сфері. Наразі використання ШІ в Україні не врегульовано на законодавчому рівні (за винятком Концепції розвитку штучного інтелекту в Україні, ухваленої 2 грудня 2020 року) [3], схожа ситуація і в Європейському Союзі. Проте технології

продовжують швидко розвиватися, і це лише питання часу, коли національне та міжнародне законодавство почне адаптуватися до цих змін. Це створює правову невизначеність і може викликати етичні питання, зокрема щодо конфіденційності даних клієнтів і можливості штучного інтелекту приймати неправильні рішення.

Також, можливі технічні збої або недосконаліть алгоритмів ШІ, що можуть призвести до неправильних рішень. Наприклад, чат-боти можуть неправильно інтерпретувати запити клієнтів або надавати невірні консультації, що може негативно вплинути на репутацію банку.

Однак, незважаючи на ці виклики, перспективи використання штучного інтелекту в банківському обслуговуванні є надзвичайно обнадійливими. Запроваджуючи складніших алгоритмів та інтегруючі штучний інтелект у всі аспекти банківських операцій, фінансові установи можуть значно підвищити ефективність і якість надання послуг. Крім того, це може стати основою для створення нових фінансових продуктів і сервісів, що відповідатимуть потребам сучасного цифрового світу.

Отже, штучний інтелект вже стає невід'ємною частиною банківських послуг, особливо у сфері дистанційного обслуговування. Завдяки такому впровадженню банки мають можливість значно підвищити якість обслуговування, скоротити витрати та забезпечити безпеку своїх операцій. У той же час повне та безпечне використання штучного інтелекту потребує чіткості регуляторних питань та врахування ризиків, які можуть виникнути в результаті впровадження цієї технології.

Список використаних джерел:

1. Баришевська І. В., Штучний інтелект у банківській сфері в умовах глобалізації / І. В. Баришевська , Ю. С. Сизоненко// Обліково-аналітичне і фінансове забезпечення діяльності суб'єктів господарювання: національні, глобалізаційні, євроінтеграційні аспекти: матеріали VI Міжнародної науково-практичної конференції, Миколаїв, 2021. С. 87-91.

2. Завербний А. С., Пандемія як каталізатор цифровізації банківської системи в Україні / А. С. Завербний, Н. Р. Сокульський // Інвестиції: практика та досвід. - 2021. - № 2. - С. 5-9.

3. Концепція розвитку штучного інтелекту в Україні від 2 грудня 2020 р. № 1556-р. / [Електронний ресурс]. – Режим доступу: http://www.rada.gov.ua

УДК 004.45

Воробйов І.О.

здобувач вищої освіти, магістр
Науковий керівник
Кошова О.П.
к.п.н., доцент кафедри комп'ютерних наук та інформаційних технологій,
Полтавський університет економіки і торгівлі

РОЗРОБКА ТА ВИКОРИСТАННЯ ТЕЛЕГРАМ БОТУ

Тема використання Телеграм боту є актуальною в сучасних умовах, коли Телеграм є найпопулярнішою соціальною мережею в Україні. Враховуючи перехід ЗВО на дистанційну форму навчання, наявність Телеграм боту для інформування є оптимальним рішенням. Також не менш важливим є його використання в бізнесі, для комунікації та надання послуг клієнтам.

Методи комунікації, які можна реалізувати за допомогою Телеграм бота:

- інформування групи осіб певної категорії. Наприклад, в навчальному процесі можна використати для інформування групи чи потоку студентів денної або інших форм навчання, а також викладачів;
- інформування конкретної особи. Наприклад, в бізнесі, можна повідомити конкретну особу про певну подію, наприклад, про успішну доставку товару на певне відділення пошти;
- інформування конкретних Телеграм груп. Наприклад, додавши Телеграм бота в певний чат для інформування про знижки в конкретному магазині;
- використання функцій власного кабінету. Наприклад, відслідковування статусу замовлення;
- пошук інформації по відкритим джерелам інформації. Наприклад, пошук історії судових справ відносно певної особи;
- розподілення трафіку користувачів. Наприклад, для оптимізації роботи технічної підтримки компанії;
- автоматизація обслуговування клієнтів в бізнес процесах. Наприклад, для автоматизації відповіді на часто поставлені запитання;
- заповнення форми зворотного зв'язку. Наприклад, оцінка якості обслуговування.

Інформування може бути миттєвим або відкладеним. Наприклад, термінові оголошення можуть бути відправлені одразу всім особам певної групи, або ж відкладені повідомлення нагадування про закінчення дії подарункового сертифікату.

Для створення власного Телеграм боту потрібно його зареєструвати в головному боті Телеграм – BotFather. При створенні потрібно вказати ім'я та нікнейм, за яким його потім можна буде знайти. Для використання цього новоствореного бота у відповідь буде надано токен, який потрібно використовувати при написанні програмного коду для комунікації з прикладним

програмним інтерфейсом Телеграму. Найбільш поширеніші мови програмування для написання телеграм ботів – Java та Python.

Багато компаній починають створювати Телеграм боти для оптимізації та покращення підтримки своїх клієнтів. Часто він дублює існуючий функціонал в онлайн кабінетах, але має і переваги. Серед головних переваг можна виділити інформування про певні події незалежно від використовуваного девайсу. Наприклад, якщо ввімкнути інформування лише в браузері на персональному комп'ютері – повідомлення будуть надходити лише туди і, у випадку перебування в іншому місці, користувач може пропустити важливе повідомлення. У випадку з телеграм – потрібно лише підписатися на бота і він буде відправляти повідомлення незалежно від девайсу, будь-то телефон чи ноутбук. Враховуючи часову та фінансову важкість розробки власного програмного застосунку, необхідність встановлення цього застосунку на девайс – простіше і доцільніше використовувати готову платформу, яка має бути популярною.

Приклади компаній, які вже створили власного Телеграм бота:

- Укрпошта – є можливість авторизації за номером телефону для подальшого відслідковування посилок, а також знаходження відділення, розрахунок вартості доставки, зв'язок з центром онлайн підтримки;
- Монобанк – чат-бот створений для комунікації з центром підтримки користувачів;
- ПриватБанк – після авторизації є можливість здійснювати грошові перекази напряму з Телеграм бота.

Приклади популярних сервісів, реалізованих в телеграм ботах в Україні:

- OpenDataUABot – сервіс для отримання відкритих державних даних про юридичних та фізичних осіб, а також громадських об'єднань;
- RailwayBot – сервіс для знаходження залізничних квитків, який також має функціонал для попереднього інформування про відправлення потягу на вибраному маршруту в вибрану дату та час.

Приклад телеграм боту для оптимізації навчального процесу:

- KPI schedule – бот, який завчасно інформує про початок занять та місця проведення заняття.

Використання Телеграм бота з відповідним функціоналом зробить обслуговування користувачів більш ефективним, а також автоматизує бізнес процеси.

Список використаних джерел:

1. Чому Телеграм – це інноваційний напрям інтернет-маркетингу. URL: https://www.omgagency.me/
2. Telegram Push Notifications. URL: https://www.respond.io/
3. Setup Telegram bot. URL: https://www.medium.com/
4. Notification API. URL: https://core.telegram.org/
5. Як створити чат бот у Телеграм. URL: https://sendpulse.ua/

6. Introduction. Java Telegram Bot. URL: https://monsterdeveloper.gitbook.io/

УДК 330.4:004.9

Гладій А.Л.
здобувач початкової вищої освіти,
ВСП «Хмельницький торговельно-економічний
фаховий коледж Державного торгівельно-економічного університету»
Науковий керівник
Нестерук Г.В.
викладач ВСП «Хмельницький торговельно-економічний
фаховий коледж Державного торгівельно-економічного університету»

ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ ФІНАНСІВ

Використання програмного забезпечення у сфері фінансів є невід'ємною частиною діяльності підприємства, тому що застосування автоматизації економить час, підвищує тонкість операції, допомагає компаніям аналізувати та приймати обґрунтовані рішення.

Програмне забезпечення — сукупність програм системи оброблення інформації та програмних документів, потрібних для забезпечення роботи цієї системи. Це команди, які регулюють роботу комп'ютера, на відміну від апаратного забезпечення, яке виконує ці команди.

У фінансовій сфері програмне забезпечення виконує наступні функції:

− відбувається автоматизація процесів, до прикладу, механізація рутинних фінансових операцій, таких як облік, звітність, управління рахунками та платежами, що зменшує ймовірність помилок і підвищує ефективність роботи;

− швидкий аналіз даних, а саме, воно дозволяє збирати, зберігати та аналізувати великі обсяги фінансових даних, що допомагає приймати швидше обґрунтовані рішення на основі реальних даних і прогнозів;

− мінімізація ризиків, тобто програми допомагають ідентифікувати та зменшити ризики, забезпечуючи стабільність та безпеку фінансових операцій;

− створення планів та бюджетів, а саме, програмні рішення надають можливості ефективно планувати, прогнозувати доходи та витрати, а також стежити за виконанням фінансових планів;

− покращення взаємодії з клієнтами, наприклад, за допомогою мобільних банківських додатків та інших фінансових сервісі, вони дозволяють своїм споживачам зручно керувати своїми фінансами, здійснювати платежі та отримувати фінансові послуги в режимі онлайн.

− відповідність нормативним вимогам, тобто, програмне забезпечення допомагає підприємствам дотримуватися фінансових стандартів, що зменшує ризик штрафів і санкцій.

Одним з найпопулярніших програмних забезпечень є FinAP ® - (Financial Abuse Prevention, Запобігання Фінансових Зловживань). Він призначений для використання в банках, кредитних спілках та інших фінансових установах, страхових компаніях та організаціях, що є учасниками платіжних систем, операторах поштового зв'язку та установах, що надають послуги переказу коштів, а також в інших суб'єктів господарювання, що відповідно до законодавства є суб'єктами первинного фінансового моніторингу. Використання Програмних Комплексів FinAP – це запорука уникнення регулятивних санкцій (штрафів, припинення дії ліцензії тощо), скорочення витрат та оптимізація роботи, актуалізація інформації щодо легалізації та використання новітніх засобів щодо ідентифікації, виявлення, коректного визначення рівнів ризиків.

Також цінується QuickBooks online, — це бухгалтерське програмне забезпечення, спеціально розроблене для малого бізнесу та фрілансерів. Він спрощує складні облікові процеси. Крім того, що QuickBooks може створювати звіти про прибутки та збитки та торгівельні відомості, рахунки-фактури та виставлення рахунків, також автоматично онлайн синхронізує бізнес-профілі з єдиною інформаційною панеллю. Найбільшими його перевагами є забезпечення ефективного управління рахунками, доступність в інтернеті, безпека та резервне копіювання, регулярні вдосконалення.

Для малого бізнесу широко застосовуються doola Books – комплексне програмне забезпечення для ведення бухгалтерського обліку, призначене для покращення фінансового менеджменту компанії. У даній програмі інформаційна панель видає точний знімок прибутків та збитків, неоплачений рахунків та грошових потоків, відстежує фінансові записи в режимі реального часу, легко створюються та надсилаються рахунки-фактури клієнтам і спрощує оподаткування, шляхом полегшення керування та звітування.

У малому бізнесі використовують також Xero, яке було засноване в 2006 році, і є хмарним бухгалтерським програмним забезпеченням, що допомагає керувати своїми фінансами та оптимізувати свої облікові процеси. Має зручний інтерфейс, комплексні функції і доступні цінові плани. Головною перевагою клієнти вважають доступність через абсолютно будь-який пристрій, який підключений до Інтернету. Крім того, пропонуються автоматичні банківські канали. А надійна функція звітності надає інформацію про показники бізнесу в режимі реального часу Ці звіти допомагають визначити тенденції та сфери, які потрібно вдосконалити, щоб можна було приймати обґрунтовані бізнес-рішення.

FreshBooks – це хмарне програмне забезпечення для бухгалтерського обліку, спеціально розроблене для малого бізнесу та фрілансерів. Перевагою вважає те, що він зручний, інтуїтивно та добре зрозумілий і ефективний в управлінні всіма аспектами фінансових записів. У всьому світі зареєстровано близько 20 мільйонів користувачів, через що він стає одним з найпопулярніших

програм для ведення бухгалтерського обліку. Інтерфейс, що є його перевагою, розроблений таким чином, щоб навігація була простою та зручною навіть для тих, хто не знайомий із термінами та процесами бухгалтерського обліку. Інформаційна панель забезпечує огляд фінансів, що полегшує контроль за фінансовим станом бізнесу. Можна налаштовувати постійні рахунки-фактури для постійних клієнтів, щомісячно створюючи їх вручну.

Також широко використовуються такі сервіси, як:

- Dilovod – український онлайн-сервіс ведення обліку та подання звітності для підприємців, облік коштів, взаєморозрахунків, закупівлі, продажу, склад, простий кадровий облік та розрахунок зарплати, здавання звітності.
- Таксер – сервіс для реєстрації та складання електронних звітів в Україні, онлайн бухгалтерія для ФОП, здача звітності до податкової та пенсійного фонду, ведення бухгалтерії та електронний документообіг, актуальна інформація у довідниках, юридичні та бухгалтерські консультації.
- Бумажкин – сервіс бухгалтерського аутсорсингу України, поєднує в собі послуги бухгалтера, кадровика, юриста та фінансиста.

При виборі програмного забезпечення у фінансовій сфері варто дотримуватися наступних порад:

- врахування розміру та типу підприємства, різні підприємства мають різні облікові потреби;
- має бути легкість у використанні, необхідно, щоб система була зрозумілою та зі зручною навігацією;
- слід враховувати масштабованість та налаштування, тому що зі ростом бізнесу зростатимуть і його потреби в бухгалтерському обліку, якщо враховувати даний факт то можна уникнути перенавчання на нових платформах, заощадити час і гроші в довгостроковій перспективі;
- зайвими не будуть функціональні можливості, тобто автоматизація повторювальних дій, а саме, введення даних, звірка банківських рахунків
- легке в інтеграції, найзручніше вибирати те програмне забезпечення, яке легко поєднується з іншими інструментами та платформами, це дозволить уникнути потреби у подвійному введенні даних і зменшить кількість помилок;
- вартість є впливовим фактором, але перед прийомом рішення, варто уважно ознайомитися з функціями кожного варіанта.

Отже, програмне забезпечення є ключовим інструментом у сфері фінансів, тому що автоматизує процеси, прискорює аналіз даних, знижує ризики, покращує планування та ефективність управління фінансами. Автоматизація рутинних операцій, таких як облік та звітність, мінімізує ймовірність помилок і спрощує управління рахунками та платежами. Вибір програмного забезпечення повинен ґрунтуватися на розмірі компанії, зручності у використанні, масштабованості, можливості інтеграції з іншими платформами та відповідності бюджету.

Список використаних джерел:

1. Переходимо на українське: 7 програм для бухгалтерського обліку на заміну російському ПЗ. URL: https://finacademy.net/ua/materials/article/perehodimo-na-ukrayinske ;
2. Топ 10: Бухгалтерські програми для України. URL: https://www.livebusiness.com.ua/ua/tools/accounting/;
3. Як вибрати правильне програмне забезпечення для ведення бухгалтерського обліку для вашого бізнесу. URL: https://www.doola.com/uk/blog/how-to-choose-the-right-bookkeeping-software-for-your-business/.

УДК 004.77

Гринь Д.А.
здобувач вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Науковий керівник
Макарова Г.В.
к.ф.-м.н., доцент, доцент кафедри інформаційних технологій
та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

РОЛЬ НАВЧАЛЬНИХ СТАРТАПІВ У СУЧАСНОМУ ІТ-ПРОСТОРІ

Інформаційні технології глибоко інтегровані у всі сфери життя, створюючи нові можливості для бізнесу, виробництва та освіти. У рамках сучасних тенденцій, значну роль відіграють інноваційні стартапи, що пропонують програмні рішення для вирішення складних прикладних задач. Стартапи, зокрема, стають рушійною силою для автоматизації та покращення процесів в цих сферах.

Розглянемо вирішальний вплив стартапів на сучасні тренди у сфері інформаційних технологій та цифрового маркетингу. Стартапи відіграють важливу роль у розвитку сучасних технологій, зокрема в галузях програмного забезпечення для вирішення прикладних задач. Стартапи часто виступають каталізаторами інновацій, оскільки вони здатні швидко адаптуватися до змін ринку, експериментувати з новими ідеями та технологіями, а також швидше виводити продукти на ринок у порівнянні з великими корпораціями. Особливо важливим є їхній внесок у такі галузі, як штучний інтелект, великі дані та автоматизація бізнес-процесів. Ці підприємства здатні створювати рішення, які є більш гнучкими та персоналізованими для вирішення конкретних завдань у сфері бізнес-аналітики, освіти та виробництва.

Нами було досліджено особливості розвитку стартапів у сфері програмних рішень. А саме стартапи, що спеціалізуються на розробці програмних засобів для прикладних задач, мають свої особливості розвитку. Основними факторами успіху таких проектів є здатність швидко реагувати на потреби ринку, створювати інноваційні та конкурентоспроможні продукти, а також ефективне використання сучасних технологій, таких як хмарні обчислення, штучний інтелект та машинне навчання. Важливими етапами для стартапів є залучення інвесторів, розвиток MVP (minimum viable product), а також подальший масштаб продукту для різних ринкових сегментів. Успішні стартапи часто переходять до стадії масштабування, забезпечуючи автоматизацію та оптимізацію процесів як у бізнесі, так і в освітньому середовищі.

Розглянемо, які особливості стартап-рішень для різних сфер цифрової економіки:

1. Виробництво: Використання стартапів у створенні програмних систем для управління виробничими циклами дозволяє компаніям не тільки оптимізувати ресурси, але й автоматизувати виробничі процеси.
2. Освіта: Інтелектуальні платформи для дистанційного навчання, які мають корені в багатьох стартапах, дозволяють покращити навчальні процеси, роблячи їх більш інтерактивними та ефективними.
3. Бізнес-аналітика та прийняття рішень: Аналітичні платформи з функціями штучного інтелекту та великих даних дозволяють підприємствам приймати обґрунтовані рішення на основі ретельного аналізу ринкових тенденцій.
4. Інтелектуальна обробка даних: Штучний інтелект та великі дані стали ключовими інструментами для автоматизації рутинних процесів та пошуку рішень для складних задач.

Прикладом вдалого стартапу є проєкт: EduFlex — інтелектуальна платформа для автоматизації управління навчальними процесами та освітніми ресурсами.

Метою стартапу є створення платформи, яка дозволяє навчальним закладам автоматизувати управління освітніми процесами, інтегрувати штучний інтелект для персоналізації навчальних траєкторій та оптимізувати адміністрування освітніх ресурсів.

Основні компоненти платформи:

- Модуль адаптивного навчання: Платформа аналізує навчальні дані кожного студента, пропонуючи індивідуальні навчальні програми на основі їхніх успіхів, інтересів та потреб.

- Модуль автоматизованого адміністрування: Система дозволяє навчальним закладам автоматизувати процеси планування занять, оцінювання знань, а також управління викладачами та студентами.
- Інтерактивні навчальні матеріали: Платформа включає інтегровані інструменти для створення та використання інтерактивних освітніх матеріалів — відео, тестів, симуляцій, що робить навчання більш динамічним.
- Аналітичні інструменти: Платформа збирає та аналізує дані про навчальний прогрес, надаючи освітнім закладам можливість покращувати свої програми на основі реальних результатів студентів.

Інноваційність:

- Штучний інтелект для персоналізації навчання дозволяє адаптувати навчальні програми до індивідуальних потреб студентів у режимі реального часу.
- Модуль управління ресурсами дає змогу автоматично організовувати навчальні процеси, включаючи розклад, викладацький склад та інтеграцію з іншими системами (наприклад, Moodle або Google Classroom).
- Інтерактивні інструменти дозволяють викладачам створювати мультимедійні курси, які підвищують залученість студентів.

Впровадження та перспектива

- Цільова аудиторія: університети, школи, приватні навчальні центри, які прагнуть автоматизувати управлінські процеси та покращити навчальні траєкторії для своїх студентів.
- Можливості масштабування: Платформа може інтегруватися з існуючими освітніми системами, що робить її зручною для навчальних закладів різного розміру та специфіки.

Отже, EduFlex – це інноваційний стартап, що пропонує рішення для автоматизації та оптимізації освітніх процесів. Щодо перспективи розвитку, то можна сказати що з урахуванням зростання попиту на дистанційні та гібридні форми навчання, подальший розвиток платформ на основі штучного інтелекту та автоматизації дозволить навчальним закладам зробити освітній процес більш гнучким, ефективним і персоналізованим.

Список використаних джерел:

1. Сучасні тенденції цифровізації економіки: проблеми та перспективи розвитку. Міжнародний науковий журнал «Інтернаука»/ Н. Г. Гавриленко, 2021
2. Сучасне програмне забезпечення для здійснення бізнес-аналізу/ Н. Задорожнюк, 2021
3. Cisco Networking Academy. URL: https://www.netacad.com/

4. Бізнес аналітика та штучний інтелект. URL: https://julienflorkin.com/uk/business/business-intelligence/business-intelligence-and-ai/

УДК 377.3

Даценко О.О.
здобувачка вищої освіти
ХНПУ імені Г.С. Сковороди

ОСВІТА, ЯК РУШІЙНА СИЛА СТАБІЛЬНОГО ІННОВАЦІЙНОГО РОЗВИТКУ ДЕРЖАВИ

Для України, котра першочергове значення приділяє ретельному вивченню та раціональному ознайомленню передового світового досвіду в області формування розвиненого інноваційного середовища та використання сучасних інструментів фінансування інновацій, адже наша країна відстає за рівнем інноваційного розвитку від провідних країн світу. Всебічне дослідження особливостей і проблем функціонування національної інноваційної системи (НІС) України, моніторинг ефективних механізмів фінансування інноваційного розвитку національної економіки.

Об’єктивним наслідком помітного посилення ролі інновацій у розвитку провідних економік світу та питанням фінансування інноваційних нововведень знаходять все більше висвітлення у зарубіжній та вітчизняній науковій літературі.

В умовах економічної та політичної нестабільності, в період реформування вищої освіти перед університетами постає питання підготовки спеціаліста – особистості нового покоління гостро мислячого, творчо швидко реагуючого на запит ринку праці, де збільшується кількість безробітних освітян. Впровадження випереджального навчання належить університетам – це підготовка кваліфікованих спеціалістів для створення й раціонального використання інформаційних технологій у всіх сферах людської діяльності між університетами на національному та міжнародному рівнях. Тісна взаємодія фізичного та цифрового середовища, що полягає у переході з переважно матеріального світу в цифровий є особливістю сучасного етапу розвитку університетів в суспільстві.

Історико-культурний феномен має університетська освіта, яка має свої традиції та історію, реалізує себе в суспільстві та виконує функцію просвітницьку та наукову, готує кваліфікованих спеціалістів, передає культурний капітал. Університети змінювали свої напрями діяльності, структури, традиції згідно вимог та історичних потреб часу, виступаючи інструментом соціальних змін.

Як видно с рис. 1, 2 найбільша кількість бакалаврів на 01.01.2023 – 368 здобувачів, 99,46% осіб, що навчалися за рахунок коштів фізичних осіб, найменша – 01.07.2019 року 26 здобувачів освіти, де 92,31% бакалаврів, що навчались за кошти фізичних осіб.

Рисунок1. Відношення студентів, що навчаються за рахунок коштів державного забезпечення відносно загальної кількості бакалаврів, які навчаються на спеціальності 011 «Освітні, педагогічні науки» [1]

Рисунок 2. Відношення кількості студентів-контрактників до загальної кількості бакалаврів, спеціальності 011 "Освітні, педагогічні науки"[1]

Сьогодні ЗВО – це місце передачі й поширення знань, формування наукового пізнання та в майбутньому – бази для розвитку підприємництва, в умовах глобалізації культурний осередок, який виступає інструментом інноваційного розвитку освітнього процесу.

Освіта є рушійною силою економіки держави, дослідження державних витрат на освітній процес відображено у таблиці 1

Як видно з таблиці 1, питома вага державних витрат на освіту у ВВП України має тренд до зниження, що є несприятливим відображенням стану зацікавленості витрат на освіту. Найбільш привабливі роки для освітян – це 2014 рік, а найменші видатки відповідно до загальних витрат державного бюджету – у 2023 році.

Таблиця 1

Державні витрати на освіту у державному бюджеті, у ВВП України узагальнено [2]

Дата	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Видатки освіта, млн. грн	28677,9	30185,7	34825,4	41140,2	44323,4	51657,6	52857,3	63837,1	58508,1	60452,2	36206,9
Всього видатки, млн. грн	430217,8	576911,4	684743,4	839243,7	985842,0	1072891,5	1288016,7	1490258,9	2705423,3	4014418,1	2249701,5
Питома вага бюдж/ Всього, %	6.67	5.23	5.09	4.90	4.50	4.81	4.10	4.28	2.16	1.51	1.6
ВВП, млн. грн	1365123	1430290	2034430	2445587	3083409	3675728	3818456	4363582	3865780	5518062	-
Питома вага витрат на освіту до ВВП	2,10	2,11	1,71	1,68	1,44	1,41	1,38	1,46	1,51	1,10	

Не може вестися безсистемно підготовка кадрів наукових, технічних, які приймають участь в інноваційних процесах виробництва. Підготовка таких фахівців повинна складатися з пов’язаних між собою етапів вдосконалення компетенцій та знань, що супроводжуються науковим відбором. Держава виділяє кошти, щоб отримати від ринку праці кадровий потенціал, щоб розвивати свою економіку та допомогти людині стати щасливою, успішною, здатною до самореалізації в суспільстві. [3]

Список використаних джерел:

1. Офіційний сайт Єдиної державної електронної бази з питань освіти Державного підприємства «Інфоресурс» URL:https://registry.edbo.gov.ua/opendata/educators/

2. Офіційний сайт Міністерства Фінансів України URL:https://index.minfin.com.ua/ua/economy/gdp/

3. Інтернет-портал Інформаційне агентство «Главком» URL: https://glavcom.ua/country/science/jakikh-fakhivtsiv-potrebuvatime-ukrajina-pislja-peremohi-ministr-osviti-zrobiv-prohnoz-929130.html

УДК 004.8

Жерновий М. О.
здобувач вищої освіти,
ХНУМГ імені О. М. Бекетова
Братерська Н. М.
асистент кафедри комп'ютерних наук та інформаційних технологій
ХНУМГ імені О. М. Бекетова

ЗАСТОСУВАННЯ ШІ В ОСВІТНІЙ СФЕРІ ТА ЙОГО ПОТЕНЦІАЛ

Світова освіта переживає період безпрецедентних трансформацій, стимульованих стрімким розвитком технологій, зокрема штучного інтелекту (ШІ). ШІ, як ключова технологія Четвертої промислової революції (Klaus Schwab, 2017), має потенціал фундаментально змінити освітній ландшафт, пропонуючи нові підходи до навчання, оцінювання та управління освітнім процесом. Україна, яка прагне модернізувати свою освітню систему та інтегруватися в глобальний цифровий простір, має унікальну можливість скористатися перевагами ШІ, але одночасно стикається з низкою викликів.

В основі більшості сучасних систем ШІ лежать нейронні мережі – математичні моделі, натхненні будовою та функціонуванням людського мозку. Нейронна мережа складається з взаємопов'язаних вузлів (нейронів), організованих у шари (Goodfellow et al., 2014). Процес навчання нейронної мережі полягає в налаштуванні ваги зв'язків між нейронами для досягнення бажаного результату. Наприклад, AlphaGo, розроблений DeepMind, використовує глибинне навчання для досягнення рівня гри в Го, що перевершує людський (Silver et al., 2016).

Персоналізоване навчання залишається одним із найперспективніших напрямків застосування інноваційних технологій в освіті. Воно передбачає створення індивідуальних навчальних траєкторій та досвіду для кожного учня, що потенційно може підвищити їхню успішність і мотивацію. За даними дослідження, проведеного RAND Corporation у 2020 році, близько 60% вчителів старших класів у США повідомили про використання принаймні однієї практики персоналізованого навчання щотижня.

Зокрема, 39% вчителів регулярно надають учням можливість обирати, як демонструвати свої знання, а 36% дозволяють учням працювати у власному темпі. Хоча конкретні показники покращення успішності варіюються, дослідження демонструє, що персоналізоване навчання може сприяти значному

прогресу учнів у математиці та читанні порівняно з традиційними методами навчання.

Штучний інтелект аналізує дані про успішність учнів, їхній стиль навчання та інтереси, що дозволяє створити індивідуальні навчальні траєкторії. Прикладом такої системи є Khan Academy, яка адаптує складність завдань до рівня учня, надаючи можливість кожному учневі працювати в своєму темпі. Платформи, як-от DreamBox Learning і Smart Sparrow, також застосовують технології адаптивного навчання, що довели свою ефективність у підвищенні зацікавленості учнів і покращенні їхніх результатів.

Впровадження ШІ в освіту ставить перед нами низку викликів, які потрібно вирішити:

- Цифровий розрив: Необхідно забезпечити доступ до технологій та інтернету для всіх учнів, незалежно від їхнього місця проживання та соціального статусу.
- Підготовка вчителів: Вчителі потребують навчання з використання нових інструментів та технологій.
- Конфіденційність даних: Необхідно захистити персональні дані учнів та запобігти їх неправомірному використанню.
- Упередженість алгоритмів: ШІ-системи можуть бути упередженими, якщо навчальні дані містять упередження. Важливо розробити алгоритми, що забезпечують справедливість та інклюзивність.
- Відповідальність: Необхідно визначити, хто несе відповідальність за результати роботи ШІ та як вирішувати проблеми, пов’язані з помилками системи.

ШІ може автоматизувати рутинні завдання вчителів, такі як перевірка домашніх завдань та оцінювання есе (Shermis & Burstein, 2013). Це звільняє час для вчителів, що дозволяє їм зосередитися на розвитку творчих здібностей учнів. Дослідження показують, що автоматизоване оцінювання може бути настільки ж точним, як і людське, з точністю до 90% у деяких випадках (Baker et al., 2021). Крім того, ШІ може аналізувати дані про успішність учнів, виявляти прогалини в знаннях і пропонувати рекомендації щодо покращення навчального процесу.

Крім того, дослідження Кендис Уокінгтон і Метью Л. Бернакі, показало, що персоналізоване навчання з використанням ШІ може підвищити інтерес учнів і покращити результати. Вони використовували ШІ в інтелектуальній навчальній системі, щоб адаптувати завдання з алгебри до інтересів учнів (наприклад, спорт або відеоігри). Порівнюючи звичайне навчання з двома рівнями персоналізації (невеликою і глибокою), вони виявили, що навіть проста персоналізація покращує успішність, а глибока – значно підвищує інтерес.

ШІ-асистенти можуть стати надійними помічниками як для вчителів, так і для учнів. Для вчителів такі системи допомагають у плануванні уроків, пошуку навчальних матеріалів та організації навчального процесу. Учням ІІ-асистенти можуть надати персоналізовану підтримку, відповідати на запитання та пропонувати додаткові ресурси. Наприклад, система Wolfram Alpha не лише

відповідає на складні запитання, але й генерує навчальні матеріали, що робить навчання більш інтерактивним та ефективним.

Застосування штучного інтелекту в освіті не лише покращує навчальний процес, але й має суттєвий економічний потенціал. У світлі глобальних змін у навчанні та викладанні, інвестування в технології, пов'язані з персоналізованим навчанням, стає все більш привабливим для українських інвесторів.

Ринок штучного інтелекту в освіті демонструє значне зростання. За даними The Business Research Company, глобальний ринок ШІ в освіті оцінювався в 5,28 мільярда доларів США у 2024 році. Очікується, що він досягне 21,64 мільярдів доларів до 2030 року, зростаючи із сукупним річним темпом зростання (CAGR) 25,5% з 2024 по 2030 рік (рис. 1). Це відкриває численні можливості для інвестування в стартапи та технологічні рішення, пов'язані з освітою, які впроваджують штучний інтелект.

Рисунок 1 – Прогноз капіталізації ринку ШІ в освіті з 2024 по 2030 роки

Крім того, впровадження технологій ШІ в освіті може мати позитивний вплив на економіку в цілому. Відповідно до дослідження, проведеного ВБФ (Всесвітній банк), інвестиції в освіту можуть принести до 10% доходу протягом життя кожного учня. Це означає, що країни, які інвестують у навчання своїх громадян, зможуть підвищити свою продуктивність і конкурентоспроможність на світовій арені.

Штучний інтелект має величезний потенціал для трансформації освіти в Україні. Проте, для успішної інтеграції ШІ необхідно враховувати як можливості, так і виклики, а також дотримуватися етичних принципів. Важливу роль відіграє співпраця між державою, освітніми закладами, ІТ-компаніями та громадськістю. Тільки спільними зусиллями ми зможемо створити освітню систему, яка відповідає вимогам сучасного світу та готує майбутні покоління до успіху в цифрову епоху.

Список використаних джерел:

1. Steiner, Elizabeth D., Christopher Joseph Doss, and Laura S. Hamilton, High School Teachers' Perceptions and Use of Personalized Learning: Findings from the American Teacher Panel. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RRA322-1.html.
2. Walkington, C., Bernacki, M.L. Personalizing Algebra to Students' Individual Interests in an Intelligent Tutoring System: Moderators of Impact. *Int J Artif Intell Educ* **29**, 58–88 (2019). https://doi.org/10.1007/s40593-018-0168-1
3. Prof. Dr. Nirvikar Katiyar, Mr. Vimal Kumar Awasthi, Dr. Ram Pratap, Mr. Kuldeep Mishra, Mr. Nikhil Shukla, Mr. Raju singh, & Dr. Mamta Tiwari. (2024). Ai-Driven Personalized Learning Systems: Enhancing Educational Effectiveness. *Educational Administration: Theory and Practice*, *30*(5), 11514–11524. https://doi.org/10.53555/kuey.v30i5.4961
4. The Business Research Company. AI In Education Global Market Report 2024 URL: https://www.thebusinessresearchcompany.com/report/ai-in-education-global-market-report

УДК 004.056.53

Задворкін М.О.
здобувач вищої освіти,
Науковий керівник
Черненко О.О.
к .ф.-м. н., кафедри комп'ютерних наук
та інформаційних технологій
Полтавський університет економіки і торгівлі

ПРОГРАМНІ ІНСТРУМЕНТИ ДЛЯ РОЗВ'ЯЗАННЯ ОСВІТНІХ ПРИКЛАДНИХ ЗАВДАНЬ

З розвитком інформаційних технологій освіта отримала потужний інструмент для підвищення якості навчання та управління навчальними процесами. Програмні засоби активно використовуються для вирішення прикладних задач у освіті, сприяючи розвитку нових форм навчання, покращенню доступності знань та індивідуалізації підходу до кожного учня. У роботі розглянуто основні типи програмних засобів, що допомагають у вирішенні прикладних задач освіти, їхні переваги та перспективи використання [1].

Системи управління навчанням (LMS) – це програмні платформи, що забезпечують створення, управління та адміністрування навчальних курсів. Вони є основою для дистанційного навчання, надаючи доступ до навчальних

матеріалів, тестування, моніторингу прогресу студентів та організації комунікації між учнями і викладачами.

До популярних LMS можна віднести:

Moodle – відкрита платформа, яка дозволяє створювати курси різного рівня складності. Вона має гнучку структуру, що дозволяє адаптувати її під конкретні освітні потреби.

Google Classroom – інструмент для інтеграції у Google-екосистему, де учні та викладачі можуть легко обмінюватися файлами, завданнями, працювати з текстовими документами та презентаціями.

Canvas – платформа, що пропонує широкий функціонал для організації онлайн-навчання та управління курсами, а також підтримку інтерактивних елементів.

Переваги LMS:

- Доступність навчальних матеріалів у будь-який час і з будь-якого місця.
- Можливість індивідуалізувати навчальний процес, налаштовуючи темп та методи навчання для кожного студента.
- Полегшення адміністрування навчального процесу, наприклад, через автоматизоване оцінювання та моніторинг успішності.
- Підтримка дистанційної форми навчання, що є особливо актуальним в умовах пандемії чи обмеженого доступу до традиційної освіти.

Програмні засоби для тестування і оцінювання знань дозволяють викладачам створювати інтерактивні тести, анкети та інші форми перевірки знань. Вони дають можливість автоматизувати процес оцінювання, що значно знижує навантаження на викладачів і надає об'єктивніші результати.

Найбільш поширені програмні засоби для тестування і оцінювання знань:

Kahoot! – інтерактивна платформа для створення вікторин і тестів, що дозволяє залучати учнів у процес навчання через ігрові елементи.

Quizlet – інструмент для створення флеш-карток і тестів, який допомагає запам'ятовувати терміни та концепції.

Socrative – система для створення та проведення тестів у режимі реального часу з можливістю миттєвого оцінювання.

Переваги платформ для тестування [2]:

- Автоматизація оцінювання зменшує ризик суб'єктивності та зменшує час на перевірку.
- Можливість проводити тести онлайн, що забезпечує зручність як для викладачів, так і для студентів.
- Використання ігрових елементів стимулює залученість учнів у процес навчання.
- Миттєва зворотна реакція допомагає студентам швидко оцінювати свої знання та виправляти помилки.

Симулятори та моделювання використовуються для того, щоб учні могли практикувати реальні навички у віртуальному середовищі. Це особливо корисно

в таких сферах, як медицина, інженерія та природничі науки, де практика у реальному житті може бути складною або небезпечною.

Приклади освітніх симуляторів:

PhET Interactive Simulations – набір інтерактивних симуляцій для вивчення фізики, хімії, біології та математики, які допомагають учням візуалізувати абстрактні поняття.

3D Anatomy – програмні засоби для вивчення анатомії, які дозволяють студентам медицини детально вивчати людське тіло через віртуальні моделі.

AutoCAD – використовується для навчання інженерії та архітектури, дозволяючи студентам створювати точні креслення та моделі.

Переваги симуляторів:

- Можливість отримання практичних навичок без ризику для здоров'я або високих витрат на обладнання.
- Візуалізація складних концепцій допомагає краще засвоїти матеріал.
- Підтримка активного навчання через виконання практичних завдань у реальних умовах.

Програмні засоби для управління освітніми закладами (School Management Systems, SMS) дозволяють автоматизувати багато адміністративних процесів, таких як управління розкладами, фінансами, документами та комунікацією між викладачами, студентами і батьками [3].

Відомі інструменти:

Jenzabar – рішення для управління освітніми установами, що включає в себе функції адміністрування, фінансового обліку, управління кадрами та студентами.

Schoology – система, що поєднує в собі LMS і SMS, дозволяючи одночасно управляти як навчальним процесом, так і адміністративними завданнями.

PowerSchool – система управління для шкіл, яка спрощує ведення облікових записів учнів, управління успішністю та організацію навчального процесу.

До переваг систем управління навчальними закладами можна віднести автоматизацію рутинних процесів, таких як розклад занять, облік відвідуваності та управління фінансами.

Мобільні додатки відкривають нові можливості для навчання на ходу. Вони дозволяють студентам отримувати доступ до навчальних матеріалів у будь-який час, брати участь у вікторинах, вирішувати завдання та комунікувати з викладачами та іншими студентами.

Переваги мобільних додатків:

- Доступ до навчальних ресурсів у будь-який час і в будь-якому місці.
- Можливість персоналізованого навчання завдяки адаптивним алгоритмам.
- Залученість через ігрові елементи, мотиваційні системи та інтерактивні завдання.

Програмні засоби для вирішення прикладних задач освіти відіграють вирішальну роль у сучасному навчальному процесі. Вони надають можливість створювати ефективні системи навчання, індивідуалізувати підхід до кожного учня, автоматизувати адміністративні процеси та підвищувати залученість студентів через інноваційні інструменти. З розвитком технологій та інтеграцією новітніх досягнень, таких як штучний інтелект, майбутнє освіти виглядає ще більш інтерактивним, гнучким та доступним для всіх [4].

Список використаних джерел:

1.Спеціальність 122 «Комп'ютерні науки» [Електронний ресурс] – https://it.udau.edu.ua/ua/abiturientu/specialnist-kompyuterni-nauki.html – Назва з екрану.

2.Популярні LMS системи [Електронний ресурс] – https://shelfy.com.ua/categories/lms-systems/

3.Освітні симулятори та моделювання [Електронний ресурс] – https://learn.ztu.edu.ua/pluginfile.php/321353/mod_resource/content/1/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F7.pdf

4.Мобільні додатки для навчання [Електронний ресурс] – https://www.gostudy.cz/uk/blog/sovety-eksperta/mobilnye-prilozheniya-dlya-studentov

УДК 004.056.53

Запорожченко А.П.
аспірант,
Харківський національний університет радіоелектроніки
Науковий керівник
Гороховатський В.О.
д.т.н., професор кафедри Інформатики
Харківський національний університет радіоелектроніки

СТАТИСТИЧНІ ТА НЕЧІТКІ МОДЕЛІ ДАНИХ У СТРУКТУРНИХ МЕТОДАХ КЛАСИФІКАЦІЇ ЗОБРАЖЕНЬ

У сучасних системах комп'ютерного зору набули прикладного застосування методи розпізнавання об'єктів, що засновані на компонентних ознаках зображення у формі множини векторів. Ці методи базуються на визначенні множини ключових точок (КТ) зображення та їх опису у вигляді бінарного вектора – дескриптора, що відображає властивості функції яскравості зображення для локальних околів КТ [1-5].

Перспективною ідеєю у плані підвищення швидкодії реалізації методів класифікації є використання поняття «центру опису» для зображень із бази еталонів, який обчислюється шляхом статистичного узагальнення значень дескрипторів, представлених у вигляді рядку бітів [6]. Саме бітова структура дескрипторів опису, отриманих детекторами ORB або BRISK, дає можливість подальшого зменшення обсягів обчислень і спрощення апаратної реалізації автоматизованих систем класифікації зображень.

Одним із способів збереження достатньої результативності класифікації при узагальненні образу візуального об'єкта шляхом обчислення значень центрів описів є застосування числового вектору вагових коефіцієнтів для структури бітів, що складають центр еталонного опису.

Застосування більш універсальних методів статистичної класифікації із базуванням на еталонній інформації сприяє не тільки узагальненню подання образів, а також і більш детальному виявленню ступеня узгодженості аналізованих та еталонних образів.

Статистичні підходи дають можливість вирішити одну із ключових проблем при впровадженні структурних методів – скоротити достатньо великий обсяг обчислювальних витрат при обробленні об'ємних векторних масивів.

Процес класифікації з використанням статистичних моделей може бути реалізований як з використанням інтегрального розподілу компонентів, так і через визначення класу об'єкта за числом голосів (рис. 1).

Одним із ефективних статистичних засобів є кластерне подання та грануляція із використанням апарату нечітких множин [1, 7]. Однак, результативність цих методів суттєво залежить від складу даних, крім того, вони вимагають додаткових обчислювальних затрат на етапі класифікації.

Задача кластерування об'ємних масивів багатовимірних спостережень (векторів-образів) виникає у прикладних задачах комп'ютерного зору і вирішується рядом технологій [2, 8]. Наприклад, коли класи перетинаються, використовують методи нечіткого кластерного аналізу, одним з найпоширеніших методів є Fuzzy C-Means clustering (FCM) [1].

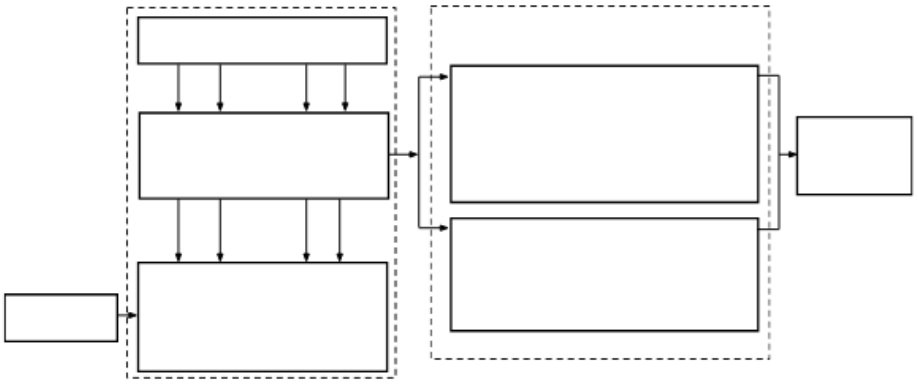


Рисунок 1 – Схема класифікації за статистичним описом

За рахунок нечіткої кластеризації можна не тільки розподілити дескриптори за кластерами, але і розрахувати суму значень функції належності

для елементів окремих еталонів, що сприяє формуванню інтегрованих еталонних образів аналогічно узагальненому дескриптору [9].

Важливою властивістю застосування апарату кластерування (звичайного і нечіткого) є незалежність сформованих просторів даних від порядку слідування дескрипторів у описі, так як це гарантує інваріантність значень трансформованих подань відносно групи геометричних перетворень [3].

Уявляється доцільним розвинення методів структурного розпізнавання на основі використання значень функції належності, отриманої за результатом нечіткої кластеризації, яка чисельно вираховує індивідуальні особливості ознак опису.

Конструкція перетворення бази дескрипторів для набору еталонів подана на рисунку 2.

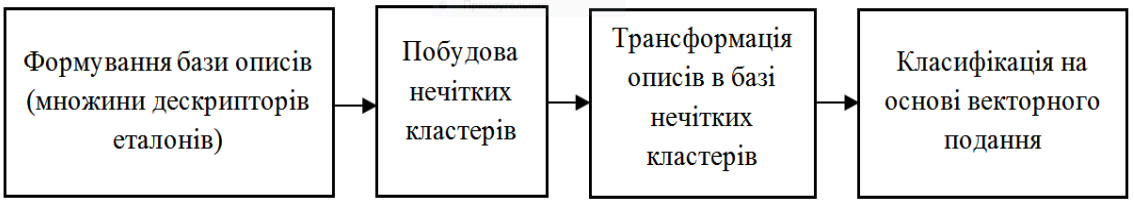


Рисунок 2 – Схема перетворення описів

Нечітке кластерне подання описів потребує дещо більшого часу оброблення у порівнянні з традиційною кластеризацією, але може демонструвати більшу гнучкість і ефективність розрізнення даних у задачах комп'ютерного зору.

Порівняльний аналіз результатів проведених експериментів із застосуванням нечіткого кластерування та традиційних підходів кластеризації показав наступні переваги залучення інструментарію нечітких множин для задачі класифікації.

1. Метод нечіткого кластерування не тільки забезпечує якість кластерування, але й суттєво скорочує час для розподілу множини дескрипторів на кластери за рахунок скорочення числа альтернатив попадання до кластеру до однієї можливої.

2. Ця техніка дає можливість досягти більш точного значення для центру кластеру, яке напряму впливає на результати класифікації.

3. За рахунок впровадження узагальненого дескриптору шляхом додавання коефіцієнтів можна додатково скоротити час класифікації за рахунок порівняння векторних подань для зображення і еталонів [1, 9].

Список використаних джерел

1. Гороховатський В.О., Творошенко І.С. Аналіз багатовимірних даних за описом у формі множини компонент: моногр. Харків, ХНУРЕ, 2022. – 124 с.

2. Гороховатський В.О., Гадецька С.В. (2020) Статистичне оброблення та аналіз даних у структурних методах класифікації зображень (монографія), Харків, ФОП Панов А.Н., 128 с.

3. Gorokhovatsky, V. (2014). Structural Analysis and Intellectual Data Processing in Computer Vision, SMIT, Kharkiv, 316 p.

4. Gorokhovatskyi V. Vlasenko N. (2021), The image description reduction in the set of descriptors on informativeness metric criteria base. Advanced Information Systems, 5 (4), 10–16. doi: https://doi.org/10.20998/2522-9052.2021.4.02

5. I. S. Tvoroshenko, and V. O. Gorokhovatsky. Intelligent classification of biophysical system states using fuzzy interval logic. Telecommunications and Radio Engineering 78.14 (2019): 1303-1315.

6. Гороховатський В.О., Гадецька С.В., Стяглик Н.І., Власенко Н.В. Класифікація зображень на підставі ансамблю статистичних розподілів за класами еталонів для компонентів структурного опису. Радіоелектроніка, інформатика, управління, 2020, №4 , с. 85–94.

7. Y. I. Daradkeh, V. Gorokhovatskyi, I. Tvoroshenko, and M. Zeghid. Improving the effectiveness of image classification structural methods by compressing the description according to the information content criterion. Computers, Materials & Continua 80.2 (2024): 3085-3106.

8. Gadetska, S.V., Gorokhovatskyi, V. O., Stiahlyk, N. I., Vlasenko, N.V. Statistical data analysis tools in image classification methods based on the description as a set of binary descriptors of key points. Radio Electronics, Computer Science, Control, 2021, №4, pp. 58-68. DOI 10.15588/1607-3274-2021-4-6

9. 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, doi: 10.1109/ACCESS.2024.3404371, https://ieeexplore.ieee.org/document/10536893

УДК 004.4:37.091.33:811.111

Зігура Т. М.
Здобувач вищої освіти
Одеський національний технологічний університет
Науковий керівник
Сакалюк О. Ю.
асистент кафедри інформаційних технологій та кібербезпеки
Одеський національний технологічний університет
Попков Д. М.
старший викладач кафедри інформаційних технологій та кібербезпеки
Одеський національний технологічний університет

РОЗРОБКА НАВЧАЛЬНО-ІГРОВОЇ СИСТЕМИ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАПАМ'ЯТОВУВАННЯ ЛЕКСИКИ АНГЛІЙСЬКОЇ МОВИ

У сучасному глобалізованому світі знання англійської мови є необхідним для успіху у різних сферах – від академічної діяльності до професійного розвитку. Вивчення лексики є ключовим аспектом в оволодінні мовою, і створення ефективних інструментів для її запам'ятовування відповідає потребам сучасного суспільства. Багато учнів стикаються з труднощами під час вивчення іноземних мов, особливо з великим обсягом нової лексики. Ігрові підходи можуть значно підвищити мотивацію учнів та допомогти їм ефективніше запам'ятовувати нові слова завдяки залученню до інтерактивних завдань.

Використання елементів гри в навчальному процесі (гейміфікація) довело свою ефективність в різних освітніх дисциплінах. Ігри допомагають не лише робити процес навчання цікавим, але й сприяють кращому засвоєнню матеріалу, залученню уваги та активізації процесу запам'ятовування через повторення в ігровій формі. Розвиток інформаційних технологій дає змогу створювати нові освітні продукти, які є інтерактивними та адаптивними до індивідуальних потреб учнів. Навчально-ігрові системи можуть адаптувати складність завдань відповідно до рівня знань учнів, що робить їх більш ефективними.

Лексика (грец. lexikos «словниковий») – це словниковий склад мови з фразеологією включно. За допомогою лексики ми членуємо навколишній та свій внутрішній світ на частини і кожній із них присвоюємо назву-замінник [1]. Усі слова мови становлять її лексику. В даній роботі буде йти мова про анаграми. Анаграми – це слова, які мають однакові літери з вхідним словом, але вони переставлені місцями. Наприклад, анаграма до слова «мова» – «вамо». Гравець в анаграми повинен скласти саме вхідне слово.

Ігри в навчальних закладах іноді розглядаються як діяльність, де учні можуть лише розважатися, не маючи з цього нічого навчитися. Сучасний вчитель усвідомлює, що ігри можуть бути використані як навчальний засіб у процесі вивчення англійської мови, особливо у викладанні лексики. Зараз все

більше викладачів під час викладання матеріалу користуються інтерактивними дошками, проєкторами, комп'ютерами тощо. Крім того, за умов пандемії кілька років тому та військового положення зараз, велика кількість учнів/студентів навчаються онлайн. Тим самим роблячи телефон та персональний комп'ютер головними інструментами отримання освіти.

Основна проблема полягає в тому, що учні/студенти вже мають певну концепцію про вивчення англійської. На їхню думку, ця мова нецікава та складна. Крім того, примусове «зазубрювання» словникового складу лише підсилює їхнє негативне ставлення до навчання. Усі вищезазначені фактори впливають на мотивацію студента, а її низький рівень стає головною перешкодою під час навчання. Саме тому застосування новітніх технологій необхідне для підвищення інтересу до предмету.

Гра в анаграми була вигадана близько 2 тис. років тому. Давньогрецький граматик Лікофон придумав переставляти літери в слові, щоб утворилося нове [2]. З того часу гра була автоматизована. Зараз у мережі можна знайти багато веб-сайтів та застосунків, які реалізують цю гру. Усі вони мають одну й ту ж саму ідею, але їх відрізняє дизайн, платформа та функціональні можливості.

Наш проект було вирішено реалізувати у вигляді веб-сторінки, яку зможе відкрити будь-який охочий за посиланням. Для створення користувацького інтерфейсу застосовувалася мова програмування JavaScript, а саме її бібліотека – React. JavaScript – це мова сценаріїв або програмування, яка дозволяє реалізувати складні функції на веб-сторінках [3]. JavaScript разом з мовою розмітки HTML та CSS утворюють групу стандартних веб-технологій. React, а точніше його компоненти, поєднує у собі HTML та JavaScript. У цій реалізації гри замість CSS використовується препроцесор SASS. SASS має свій синтаксис, але на виході з цього коду генерується CSS-код, який зрозумілий для браузера.

Будь-яка розробка програмного продукту починається з визначення вимог. Варіант до розрахунково-графічного завдання описав наступні вимоги:

– слова обираються з текстового файлу;

– на вгадування слова виділяється певний час, який можна змінювати;

– забезпечити мінімум 10 рівнів;

– усі гравці додаються у таблицю рекордів.

На наступному етапі відбувається проєктування системи. В даному випадку створюється прототип сторінок, обирається кольорова гама сайту та створюється структура сайту. Також на цьому етапі було створено текстовий файл, який містить 50 слів, тобто 50 раундів. Надалі цей список можна розширювати, щоб забезпечити більшу кількість раундів.

Далі почалася розробка основних функцій програмного продукту. Середовищем розробки стала IntelliJ IDEA. Під час цього етапу відбувається також програмування основних функцій проєкт. Реалізуються події після натискання на кожну кнопку, під час вписування тексту в поле та після завершення гри. Останнім етапом розробки програмного продукту буде його тестування та впровадження (див. розділ 3 цієї записки). На цьому етапі виявляються баги, лексичні та синтаксичні помилки та інші неточності. Під

впровадженням програмного продукту розуміють введення його робочої версії в експлуатацію.

Далі про роботу навчальної гри. Коли сайт відкривається, користувач бачить головну сторінку. На цій сторінці можна ввести ім’я гравця та вказати кількість секунд на один раунд. Після натискання кнопки «START» почнеться гра. Гравець буде вгадувати слова, вводячи своє слово у поле введення. Воно відображатиметься на так званій «дошці» (див. рис.1). Щоб підтвердити відповідь, користувач натисне на кнопку «ENTER». Якщо слово вгадано – йому буде присвоєно 100 балів і слово зміниться, а таймер оновиться.

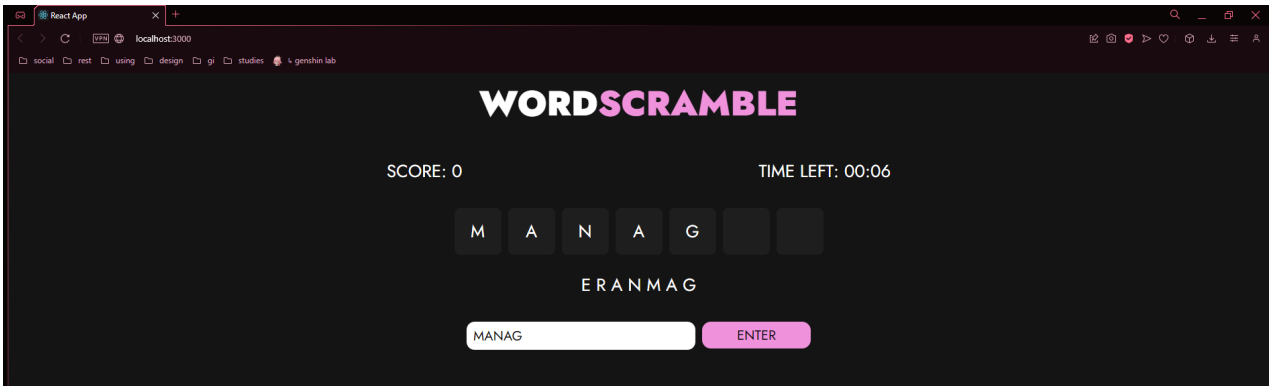


Рисунок 1 – Сторінка відгадування слів

Після того, як гра завершиться відобразиться вікно з результатами та варіантами наступних: «TRY AGAIN» – гра почнеться спочатку с тим же ім’ям; «NEW GAME» – поверне на головний екран, де можна ввести нового гравця.

Після розміщення сайту на сервері, його можна буде запустити на будь-якому пристрої з будь-якого веб-браузера. Головна умова – це наявність під’єднання до Інтернету.

Отже, результатом цієї роботи є веб-сторінка, яка пропонує пограти у гру розгадування анаграм. Проєкт було реалізовано засобами бібліотеки React та мови стилів SASS. Було створено прототип дизайну сайту, розглянуто основні етапи розробки програмного продукту та детально описано основні функції проєкту.

Список використаних джерел

1. Лексика і лексикологія Офіційний сайт Української мови. Офіційний сайт Української мови. URL: http://ukrainskamova.com/publ/chinnij_pravopis/leksika/leksika_i_leksikologija/5-1-0-44 (дата звернення: 11.11.2023).

2. Навіщо школяру розгадувати анаграми. «Світ Чекає Крилатих» – Сайт Освітньої системи А. Цимбалару. URL: https://svitchekaiekrylatykh.com/новини/навіщо-школяру-розгадувати-анаграми. (дата звернення: 11.11.2023).

3. MDN Web Docs. MDN Web Docs. URL: https://developer.mozilla.org/en-US/ (accessed at: 11.11.2023).

УДК 004.67

Кирилюк М.В.
здобувач бакалаврського рівня вищої освіти
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна;
Стяглик Н. І.,
к.п.н., доцент, завідувач кафедри інформаційних технологій
та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

СИСТЕМИ ОБРОБЛЕННЯ ДАНИХ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ БІЗНЕС-ПРОЦЕСІВ У МАЛОМУ ТА СЕРЕДНЬОМУ БІЗНЕСІ.

У сучасному динамічному бізнес-середовищі малий та середній бізнес стикається з численними викликами, серед яких особливе місце займає необхідність оптимізації бізнес-процесів. Ефективне управління даними є ключовим фактором, що визначає успіх підприємств у цій категорії. Системи оброблення даних забезпечують підприємствам можливість швидко аналізувати інформацію, виявляти тренди та ухвалювати обґрунтовані рішення, що, у свою чергу, сприяє підвищенню продуктивності, зменшенню витрат і поліпшенню обслуговування клієнтів.

В даній роботі розглянемо різноманітні програмні рішення та технології, які допомагають малим і середнім підприємствам інтегрувати дані у свої бізнес-процеси, а також дослідимо приклади їх впровадження, що демонструють позитивний вплив на загальну ефективність діяльності.

В процесі свого функціонування бізнес стикається з різноманітними задачами, які вимагають використання спеціалізованого програмного забезпечення. Ось лише деякі з них: управління фінансами, аналіз даних, керування проєктами, автоматизація кампаній, управління персоналом, оптимізація виробничих процесів, електронна комерція, маркетингові дослідження, внутрішня комунікація та багато іншого.

Здійснимо огляд основних програмних засобів, що дозволяють вирішувати прикладні задачі виробництва.

SCADA (Supervisory Control and Data Acquisition) – це програмне забезпечення для моніторингу та контролю виробничих процесів. SCADA-системи забезпечують збір даних з різних сенсорів та їх аналіз у реальному часі, що дозволяє оптимізувати роботу підприємства.

ERP-системи (Enterprise Resource Planning) – інтегровані платформи для управління всіма ресурсами підприємства, такими як фінанси, людські ресурси, постачання, виробництво та ін. Серед найпопулярніших ERP-систем можна виділити SAP, Oracle та 1С.

Програмні засоби для бізнес-аналітики. BI-системи (Business Intelligence) – це набори інструментів для збору, обробки та аналізу даних для ухвалення бізнес-рішень. Відомі системи: Power BI (Microsoft), Tableau, QlikView. Вони

дозволяють створювати інтерактивні звіти та візуалізувати дані для полегшення прийняття рішень.

CRM-системи (Customer Relationship Management) – це інструменти для управління взаємовідносинами з клієнтами. CRM допомагає збирати та аналізувати дані про клієнтів для поліпшення продажів і маркетингових стратегій. Найвідоміші CRM: Salesforce, Bitrix24, Zoho CRM

Програмні засоби для інтелектуальної обробки даних. Системи для машинного навчання та штучного інтелекту (ML/AI) – використовуються для автоматизації процесів аналізу великих обсягів даних, прогнозування тенденцій та пошуку прихованих закономірностей. Найпоширеніші середовища для роботи з AI: TensorFlow, Keras, PyTorch.

Інструменти для Big Data – Hadoop, Apache Spark, Google BigQuery – дозволяють обробляти і аналізувати масиви даних у режимі реального часу.

Більшість програм є безкоштовними. Але також більшість програм має платні послуги або версії, якими професіонали своєї справи і користуються, не тільки для свого комфорту, але і для більш зручної, точної та приємної роботи.

Список використаних джерел

1. Оптимізація бізнес-процесів: як допомагають IT-рішення. URL: https://intecracy.com/ua/news/optimizacia-biznes-procesiv-ak-dopomagaut-it-risenna.html
2. Огляд програмних засобів статистичного аналізу даних. URL: http://www.economy.nayka.com.ua/?op=1&z=5676
3. SCADA. URL: https://uk.wikipedia.org/wiki/SCADA
4. Планування ресурсів підприємства. URL: https://uk.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D0%BD%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D1%96%D0%B2_%D0%BF%D1%96%D0%B4%D0%BF%D1%80%D0%B8%D1%94%D0%BC%D1%81%D1%82%D0%B2%D0%B0
5. Управління відносинами з клієнтами. URL: https://uk.wikipedia.org/wiki/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D0%B2%D1%96%D0%B4%D0%BD%D0%BE%D1%81%D0%B8%D0%BD%D0%B0%D0%BC%D0%B8_%D0%B7_%D0%BA%D0%BB%D1%96%D1%94%D0%BD%D1%82%D0%B0%D0%BC%D0%B8

УДК 004.056.53

Кошелев М.О.
здобувач базової фахової середньої освіти,
Харківський Фаховий Комп'ютерний Коледж
Науковий керівник
Наугольна Л.М.
викладач програмування
Харківський Фаховий Комп'ютерний Коледж

ШТУЧНИЙ ІНТЕЛЕКТ ТА ЙОГО ВПЛИВ НА РОЗРОБКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Штучний інтелект (ШІ) стрімко стає невід’ємною частиною сучасної розробки програмного забезпечення, він формує нові підходи до розробки, тестування та навіть дизайну програмного забезпечення. Нещодавно впровадження ШІ у програмуванні розглядалось як щось далеке та не вивчене, проте сьогодні ця технологія стає однією із найзручніших та найефективніших. Сьогодні розробнику програмного забезпечення пропонується велика кількість сервісів в основі яких покладено технології і алгоритми ШІ, наприклад, GitHub Copilot, Tabnine, Replit Ghostwriter, CodeT5, OpenAI Codex та інші. Саме завдяки використанню таких сервісів, які розроблені на базі можливостей ШІ, вдається автоматизувати рутинні процеси і знаходити оптимальні рішення там, де розробнику бракує часу чи ресурсів. ШІ у прямому сенсі прискорює розробку та підвищує якість програмного продукту.

Застосування штучного інтелекту в розробці програмного забезпечення відкриває численні перспективи: автоматичне генерування коду, виявлення помилок, оптимізація програмного коду та багато іншого. Але, незважаючи на всі ці плюси та переваги, виникають нові питання, які потребують глибшого розуміння: чи може ШІ повністю замінити розробників-програмістів у майбутньому? Який буде штучний інтелект через 10 років, і як його розвиток вплине на IT індустрію?

Але на сьогодні можна стверджувати, що однією з ключових переваг застосування ШІ у розробці програмного забезпечення є автоматизація рутинних процесів, що не тільки підвищує продуктивність розробників, але й зменшує ймовірність помилок. ШІ може аналізувати великі обсяги коду, виявляючи та виправляючи баги набагато швидше, ніж це могли б зробити фахівці. Також штучний інтелект сприяє поліпшенню якості тестування.[1] З його допомогою можна автоматизувати процеси тестування, забезпечуючи глибший та всебічний аналіз продукту. Це дозволяє виявляти проблеми на

ранніх стадіях розробки, що позитивно впливає на технологічні процеси розробки програмного забезпечення, зменшує витрати ресурсів компанії та підвищує якість кінцевого продукту.

Аналізуючи процес розробки програмного забезпечення, треба зауважити, що це не лише написання коду, але й вирішення складних проблем, розуміння потреб користувачів та адаптація до умов, які еволюціонують і змінюються. Саме розробники, особливо з великим досвідом, мають здатність мислити нестандартно, знаходити інноваційні рішення та адаптуватися до нових технологій або умов. ШІ, незважаючи на свою вражаючу здатність до обробки великих обсягів даних, все ще не володіє повною мірою креативністю та інтуїцією, що є важливими рисами розробників програмного забезпечення. Крім того, у багатьох ситуаціях розробникам доводиться працювати в умовах невизначеності або недостатньої інформації. Фахівці можуть приймати рішення на основі неповних даних, використовуючи досвід та інтуїцію. ШІ, навпаки, залежить від якісних даних і може бути обмежений у своїх можливостях у ситуаціях, де точних даних недостатньо або вони не відповідають контексту. Таким чином, хоча ШІ відіграє важливу роль у трансформації ТІ індустрії, його функції спрямовані на допомогу, а не на заміну фахівці з розробники у повному обсязі.[2]

Штучний інтелект має значний вплив на ринок праці, що викликає багато дискусій, як на глобальному рівні, так і в Україні. Автоматизація процесів та впровадження ШІ змінюють традиційні уявлення про роботу, що створює як нові можливості, так і виклики для працівників у різних галузях.

Автоматизація й впровадження ШІ, особливо в галузях, де рутинні завдання складають значну частину роботи, наприклад, логістика, виробництво, обслуговування клієнтів, фінансові послуги та інше, має великий вплив. Дослідження прогнозують, що значна частина робочих місць у цих сферах зникне або трансформується, що буде вимагати перекваліфікації працівників.[3] Проте водночас ШІ створює нові можливості, відкриваючи ринки для спеціалістів, які можуть працювати з цими технологіями. Сфери розробки штучного інтелекту та програмного забезпечення, управління даними, кібербезпеки, також інноваційні галузі, як біотехнології чи робототехніка, потребуватимуть висококваліфікованих фахівців. Таким чином, глобальний ринок праці буде поступово зміщуватися від завдань, що виконуються вручну, до знань та навичок, пов'язаних з технологіями, аналітикою даних та управлінням вже автоматизованими системами.

Список використаних джерел:

1. Інтернет ресурс Freshtech – URL: https://freshtech.global/ua/blog/leveraging-ai-for-business-process-automation
2. Інтернет ресурс ITVDN – URL: https://itvdn.com/ua/blog/article/will-artificial-intelligence-replace-developers#nsfkargoz7p2
3. Штучний Інтелект Budni robota.ua – URL: https://budni.robota.ua/career/shtuchniy-intelekt-ta-rinok-pratsi-osnovni-vikliki-ta-mozhlivosti

УДК 005.95.96

Ломоносов О.С.
здобувач вищої освіти
ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА»
Головний спеціаліст відділу з питань кримінального та кримінального процесуального законодавства Головного управління кримінальної юстиції Директорату правосуддя та кримінальної юстиції Міністерства юстиції України
Науковий керівник:
Латишева О.В.
кандидат економічних наук, доцент кафеди Цифрових технологій та проєктно-аналітичних рішень,
ТОВ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА»

ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ДЛЯ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ПІДБОРУ ПЕРСОНАЛУ: ЕФЕКТИВНІСТЬ ТА ПЕРСПЕКТИВИ

Інтелектуальне оброблення даних та прийняття рішень відіграють важливу роль у сучасних системах управління персоналом. Зі зростанням кількості претендентів на вакансії та обсягів даних про них, використання програмних засобів стає ключовим для автоматизації процесів аналізу та швидкого прийняття ефективних рішень.

Актуальність використання програмних засобів у сфері добору персоналу полягає в тому, що застосування інтелектуальних систем у процесі добору персоналу значно покращує ефективність та точність найму. Завдяки використанню штучного інтелекту (далі – ШІ) та машинного навчання (ML), можна автоматизувати обробку великих масивів резюме та оптимізувати процес відбору, забезпечуючи відповідність кандидатів вимогам вакансій. Зростаюча кількість претендентів на робочі місця та необхідність швидкого прийняття рішень роблять програмні засоби невід'ємною частиною сучасних процесів найму, що сприяє скороченню часу на пошук і підбір персоналу.

Серед таких засобів важливе місце займають системи управління кандидатами, інструменти на базі штучного інтелекту та машинного навчання.

Системи управління кандидатами (Applicant Tracking Systems, ATS) є основними інструментами для автоматизації процесу найму. Вони дозволяють ефективно управляти процесом добору персоналу, починаючи від аналізу резюме до організації співбесід. Популярні платформи, такі як Workday, Greenhouse та BambooHR, автоматизують завдання HR-відділу, надаючи можливість зберігати та обробляти інформацію про кандидатів у зручному форматі, забезпечуючи ефективну співпрацю між рекрутерами та керівництвом.

Workday – хмарна платформа, що забезпечує управління даними про кандидатів, спрощує процеси пошуку та відбору персоналу, а також інтегрується з іншими HR-системами [1].

Greenhouse – одна з провідних платформ ATS, що спеціалізується на автоматизації процесу відбору кандидатів, зокрема на етапах оцінки навичок та організації інтерв'ю [2].

BambooHR – проста у використанні система, орієнтована на малий і середній бізнес, яка дозволяє легко керувати процесом найму, аналізувати резюме та відслідковувати статус кандидатів [3].

Варто зауважити, що штучний інтелект все більше інтегрується в процес добору персоналу, дозволяючи автоматизувати обробку резюме та виконувати складніші завдання, такі як аналіз поведінкових даних кандидатів або проведення первинних інтерв'ю за допомогою чат-ботів. Серед найпоширеніших інструментів з використанням ШІ – HireVue та XOR.

HireVue використовує ШІ для проведення відеоінтерв'ю з кандидатами, аналізуючи не лише їхні відповіді, але й невербальну поведінку (жести, вираз обличчя), щоб надати рекрутерам більш повну оцінку кандидатів [4].

XOR – це чат-бот, що використовує ШІ для автоматизації комунікації з кандидатами, проведення первинного відбору та надання рекомендацій для подальших етапів найму [5].

Разом з тим, машинне навчання дозволяє створювати моделі, які прогнозують успішність кандидатів на основі історичних даних. Ці моделі враховують попередній досвід, досягнення та інші фактори, що дозволяють підвищити точність процесу найму. Деякі з провідних платформ, що використовують ML, включають Pymetrics та Recruitee.

Pymetrics використовує ігрові алгоритми машинного навчання для оцінки когнітивних та емоційних характеристик кандидатів, допомагаючи компаніям підбирати працівників, які найбільше відповідають вимогам та культурі організації [6].

Recruitee – платформа, що поєднує ATS та інструменти для прогнозування успішності кандидатів на основі аналізу їхніх даних та попередніх результатів роботи, що забезпечує кращу відповідність між вимогами вакансії та навичками претендентів [7].

Говорячи про вплив інтелектуальних систем на прийняття рішень у сфері найму (IDSS), то вони відіграють також ключову роль у модернізації процесу

добору персоналу на сучасних підприємствах. Оскільки, IDSS аналізують комплексні набори даних, що охоплюють широкий спектр інформації про кандидатів. Наприклад, системи на базі машинного навчання можуть використовувати історичні дані для побудови моделей прогнозування, які допомагають визначити, чи буде кандидат відповідати вимогам підприємства. Такий підхід знижує ризики неправильної оцінки потенційних співробітників та дозволяє зосередитись на найбільш підходящих кандидатах [8].

Також інтелектуальні системи дозволяють проводити більш глибокий аналіз даних про кандидатів. Завдяки цьому HR-фахівці отримують можливість виявляти неочевидні закономірності, що можуть бути важливими для прийняття рішення про найм. Наприклад, експертні системи, такі як ті, що використовуються у платформах на основі ШІ, здатні аналізувати поведінкові особливості кандидатів під час співбесід або їхню здатність до адаптації в новому колективі [9]. Це особливо корисно для великих компаній, де вручну обробляти подібні дані надзвичайно складно.

Що стосується розробки індивідуальних стратегій найму та розвитку персоналу, то це також можливо за допомогою експертних систем. Такі системи здатні враховувати різні фактори, включаючи довгострокові плани розвитку підприємства та індивідуальні особливості кожного кандидата. Вони допомагають HR-менеджерам не тільки у процесі підбору, але й у розробці планів професійного зростання для нових співробітників, що підвищує їхню мотивацію та продуктивність. Наприклад, експертні системи можуть визначати, які навчальні програми будуть найбільш ефективними для певного кандидата, виходячи з його сильних сторін та професійних навичок [10].

Можна дійти висновку, що інтелектуальні системи у сфері добору персоналу значно підвищує ефективність процесу найму, скорочуючи час на відбір кандидатів і покращуючи точність прийнятих рішень. Автоматизація рутинних завдань та глибокий аналіз даних забезпечують більш об'єктивний підхід до вибору персоналу, що позитивно впливає на результативність та ефективність HR-відділів. Враховуючи низку позитивних аспектів від використання таких систем з часом можливий повний перехід до використання програмних засобів та штучного інтелекту.

Список використаних джерел:

1. Workday. (n.d.). *Хмарна платформа для управління персоналом.* https://www.workday.com .
2. Greenhouse. (n.d.). *Програмне забезпечення для управління кандидатами та рекрутингу.* https://www.greenhouse.io .
3. BambooHR. (n.d.). *Програмне забезпечення для HR для малого та середнього бізнесу.* https://www.bamboohr.com .
4. HireVue. (n.d.). *Платформа для відеоінтерв'ю на базі ШІ.* https://www.hirevue.com .
5. XOR. (n.d.). *Чат-бот для рекрутингу на базі ШІ.* https://www.xor.ai .

6. Pymetrics. (n.d.). *Платформа для оцінки когнітивних та емоційних характеристик на базі ШІ.* https://www.pymetrics.com .
7. Recruitee. (n.d.). *Програмне забезпечення для спільного підбору персоналу.* https://recruitee.com .
8. Artificial Intelligence in HR: Data-Driven Decision Making for Recruitment. New York: Springer.
9. Machine Learning in Human Resources: Enhancing Decision-Making Processes. London: Oxford University Press.
10. Artificial Intelligence for Recruitment: Strategic Implementation and Best Practices. Harvard Business Review.

УДК 338.42

Лось Д.В.
здобувач вищої освіти,
Хмельницький університет управління та права імені Леоніда Юзькова
Науковий керівник:
Ткачук Н.М.
к.е.н., доцент, доцент кафедри фінансів, банківської справи, страхування та фондового ринку
Хмельницький університет управління та права імені Леоніда Юзькова

РОЗВИТОК ДИСТАНЦІЙНИХ БАНКІВСЬКИХ ПОСЛУГ В УКРАЇНІ

Поширення цифрових технологій і зростання популярності онлайн сервісів призвело до широкого використання населення і бізнесом дистанційного банківське обслуговування. Останні роки, зокрема період пандемії COVID-19 та події, пов'язані з російським вторгненням у 2022р., значно прискорили процес діджиталізації банківської сфери. Українські банки сьогодні пропонують клієнтам широкий спектр дистанційних послуг, активно впроваджуючи інноваційні рішення, розширюючи онлайн-функціонал та вдосконалюючі системи безпеки, що дозволяє ефективно управляти фінансами, задовольняти зростаючі потреби в дистанційному обслуговуванні та зменшити час на відвідування банківських відділень.

Дистанційні банківські послуги – це можливість користуватися послугами банку, не відходячи від мобільного пристрою чи комп’ютера. За допомогою інтернет-банкінгу, мобільного додатку чи телефону, клієнти можуть переказувати кошти, перевіряти баланси на рахунку та здійснювати різноманітні платежі. Однією з переваг дистанційних банківських послуг є можливість швидко та легко проводити операції з будь-якого місця та в будь-який час доби. Незважаючи на віддаленість від банку, клієнти можуть здійснювати операції, а також ділитися своїми даними та реквізитами з відповідними особами, тим самим знижуючи ризик втрати коштів. Крім того, дистанційне банківське

обслуговування безпечне та надійне, адже банк забезпечує високий рівень захисту персональних даних клієнтів та їх фінансових операцій, тому клієнти можуть бути впевнені, що їхні кошти та інформація захищені від несанкціонованого доступу [1].

На сьогоднішній день в Україні багато банків надають дистанційні фінансові послуги різного спрямування, але лідерами з надання таких послуг є наступні:

1. Приват24 – онлайн-банкінг Приватбанку, який розробив широкий спектр мобільних додатків для віддаленого обслуговування клієнтів, включаючи: «Privat24», «Приват 24 для бізнесу», «Скарбничка», «Термінал», «Мої вклади», «Кредитна історія», «Приватагент» [3]. Приват24 пропонує широкий спектр послуг, включаючи платежі та перекази коштів, оплату послуг, поповнення мобільного, управління картками та депозитами, тощо.

2. PUMB Online – онлайн-банкінг від Першого Українського Міжнародного Банку (ПУМБ). Банк надає повний спектр банківських послуг через мобільний додаток та веб-інтерфейс, включаючи управління рахунками, кредитами та депозитами, а також можливість здійснювати платежі та перекази. Система відрізняється надійністю та зручністю використання для приватних та корпоративних клієнтів.

3. Monobank – перший в Україні повністю мобільний банк без фізичних відділень, який пропонує зручний мобільний додаток з широким функціоналом, включаючи миттєві перекази, кешбек, віртуальні та фізичні картки, кредитні ліміти та можливість використовувати бонусні програми.

4. UKRSIB online – онлайн-банкінг Укрсиббанку, який пропонує широкий спектр онлайн-послуг, включаючи управління рахунками, картками, кредитами та депозитами, здійснення платежів і переказів, оплата низки послуг та поповнення мобільного телефону.

Зазначені пропозиції банків є дуже популярними в Україні та мають низку переваг, оскільки дозволяють клієнтам: економити час та ресурси, здійснювати операції цілодобово без вихідних, уникати відвідування відділень та черг, контролювати фінанси в режимі реального часу, швидко переказувати кошти та оплачувати послуги, керувати рахунками та депозитами дистанційно, отримувати миттєві сповіщення про операції, користуватися послугами з будь-якої точки світу, мати доступ до детальної історії транзакцій та отримувати оперативну онлайн-підтримку.

В Україні останніми роками спостерігається швидка зміна платіжних звичок. Громадяни все частіше почали користуватись послугами електронної комерції та віддають перевагу безготівковим розрахункам, особливо безконтактним. Поряд з цим, спостерігається тенденція до збільшення популярності безконтактних платіжних методів та використання їх для проведення розрахунків.

Оскільки ринок платіжних карток є важливою складовою дистанційного банківського обслуговування, доцільно проаналізувати ринок електронних платіжних засобів. Для розуміння тенденцій на ринку карток ключовим

показником є зростання частки безготівкових операцій за період 2019-2023 рр., що зображено на рис. 1.

Рис. 1. Динаміка структури розрахункових операцій банків в Україні у 2019-2023 рр. [2].

Аналізуючи дані, що наведені на рис. 1., можна побачити, що частка безготівкових операцій зростає щорічно, в той час, як питома вага готівкових операцій, відповідно, зменшуються. Навіть під час війни українці продовжують надавати перевагу безготівковим розрахункам за допомогою платіжних карток. Так, у 2023р. майже 68% операцій з картками були безготівковими, що значно вище, ніж у 2021р., коли цей показник становив майже 61%.

Загалом, це свідчить про зростання ролі безготівкових розрахунків в Україні, що є безсумнівно позитивним фактором для банківської системи. Хоча обсяги операцій зі зняття готівки за допомогою електронних платіжних засобів зростають, їхня частка поступово зменшується. Виходячи з цього можна зробити висновок, що населення з кожним роком все більше віддає перевагу безготівковим розрахункам і можна припустити, що така тенденція продовжиться, а частка готівкових операцій буде зменшуватися й надалі.

Отже, дистанційні банківські послуги є важливою складовою розвитку системи банківських розрахунків, популярність яких швидко зростає. Цей факт підтверджується різноманітністю доступних віртуальних банківських продуктів та сервісів, що, безумовно, є позитивним, оскільки зарубіжний досвід показує, що майбутнє банківської сфери тісно пов'язане з цифровою трансформацією й саме це стає визначальним фактором конкурентоспроможності та ефективності банківських послуг у майбутньому.

Список використаних джерел:

1. Аврамчук, Л., Ясковець, І., Дистанційний банкінг в Україні. *Scientific Collection «InterConf»*. 2023. С 48–52.

2. Операції з використанням платіжних карток в Україні та за кордоном, IV квартал 2023 року. Національний банк України. URL: https://bank.gov.ua/ua/news/all/operatsiyi-z-vikoristannyam-platijnih-kartok-v-ukrayini-ta-za kordonom-iv-kvartal-2023-roku

3. Мобільні додатки Приватбанку. URL: https://privat-bank.ua/apps

УДК 004.4`2

Лукаш Д.І.
здобувач вищої освіти, магістр
Науковий керівник
Ольховська О.В.
к.ф.-м.н, зав.кафедри комп'ютерних наук та інформаційних технологій,
Полтавський університет економіки і торгівлі

РОЗРОБКА МОБІЛЬНИХ ДОДАТКІВ: СУЧАСНІ ІНСТРУМЕНТИ ТА ТЕХНОЛОГІЇ

У сучасному світі мобільні додатки стали невід'ємною частиною повсякденного життя. В тому є потреба створювати нові, та вдосконалювати старі. З розвитком технологій користувачі очікують від додатків швидкої, зручної та стабільної роботи на різних пристроях. Сучасні інструменти для розробки мобільних додатків, такі як Flutter, React Native та Xamarin, дозволяють значно пришвидшити процес створення програмного забезпечення, забезпечуючи його кросплатформенність і високу продуктивність.

Серед основних інструментів для розробки мобільних додатків можна виділити наступні [1-3]:

Flutter – це фреймворк від Google для створення нативних інтерфейсів на iOS та Android. Використовуючи мову програмування Dart, Flutter надає можливість розробникам створювати додатки з високою продуктивністю. Однією з ключових переваг Flutter є гарячий перезапуск (Hot Reload), який дозволяє розробникам миттєво бачити зміни в коді без перезапуску програми. Це значно прискорює процес розробки та тестування.

React Native – це JavaScript-бібліотека від Facebook для розробки нативних мобільних додатків. Використовуючи React, цей інструмент дозволяє створювати мобільні додатки з єдиним кодом для iOS та Android. React Native є популярним серед розробників через його ефективність і гнучкість, а також можливість використання готових компонентів та інтеграції з існуючими бібліотеками.

Xamarin – це фреймворк від Microsoft, що дозволяє використовувати мову C# для розробки кросплатформених мобільних додатків. Основна перевага Xamarin полягає в тому, що він забезпечує високу продуктивність за рахунок прямої компіляції в нативний код. Xamarin також підтримує використання єдиного базового коду для різних платформ, що зменшує час та ресурси на розробку.

Розглянемо програми, створені за допомогою Flutter, React Native, Xamarin:

Alo.ua – це мобільний додаток від інтернет-магазину побутової техніки та електроніки ALO.ua. Створений на Flutter, додаток забезпечує швидку навігацію, зручний пошук та кросплатформенну стабільність.

MEGOGO – це українська платформа для перегляду фільмів, серіалів та телебачення. Використання Flutter допомогло створити стабільний і зручний додаток для мобільних пристроїв із багатим функціоналом для потокового відео.

Sushiya – це офіційний додаток популярної української мережі ресторанів японської кухні. Використання React Native дозволило створити мобільний додаток, що працює як на iOS, так і на Android, з однаковим інтерфейсом і функціональністю.

Uklon – це сервіс таксі. Uklon використовує React Native для свого мобільного додатка, що забезпечує швидкий і зручний інтерфейс для замовлення таксі, відстеження авто та інших послуг, доступний на різних платформах.

Приват24 – це один із найбільш популярних банківських додатків в Україні. За допомогою Xamarin було створено стабільний кросплатформенний додаток для управління рахунками, платежами та іншими банківськими операціями.

Нова Пошта – це додаток для відстеження посилок та оформлення доставки. Використовується Xamarin що дозволяє компанії забезпечувати користувачів однаковим функціоналом на Android і iOS з високою продуктивністю.

Основними перевагами сучасних інструментів для розробки мобільних додатків є: кросплатформенність, використовуючи єдиний код для різних платформ, розробники можуть значно зменшити час та витрати на створення додатків; швидкість розробки, інструменти, як-от Flutter та React Native, дозволяють використовувати гарячий перезапуск, що прискорює процес тестування та налагодження додатків; гнучкість**,** використання бібліотек і готових компонентів дозволяє швидко додавати нові функції та розширювати можливості додатків.

Незважаючи на численні переваги, інструменти для кросплатформенних додатків мають і свої обмеження. Наприклад, продуктивність таких додатків може бути нижчою порівняно з нативними додатками, розробленими для конкретної платформи. Також іноді виникають проблеми з підтримкою нових функцій і оновлень операційних систем.

Сучасні інструменти для розробки мобільних додатків, такі як Flutter, React Native та Xamarin, значно спрощують процес створення кросплатформених рішень, дозволяючи забезпечити швидку, стабільну та зручну роботу додатків на різних операційних системах. Їх використання дозволяє скоротити час та витрати на розробку завдяки можливості створення єдиного коду для різних платформ. При цьому гарячий перезапуск (Hot Reload) та готові компоненти допомагають прискорити тестування та налагодження додатків, забезпечуючи гнучкість в управлінні функціональністю.

Проте варто пам'ятати про певні обмеження цих інструментів. Продуктивність кросплатформених додатків може бути нижчою порівняно з нативними рішеннями, розробленими спеціально для однієї платформи. Крім

того, іноді виникають труднощі з підтримкою нових функцій та оновлень операційних систем.

Тож вибір інструмента для розробки мобільного додатка повинен залежати від конкретних вимог проєкту, зокрема від потреб у кросплатформенності, продуктивності та можливостях швидкої інтеграції нових функцій. Популярні приклади, такі як Alo.ua, Приват24, Нова Пошта, MEGOGO, Uklon та Sushiya, демонструють успішне використання цих технологій в Україні.

Список використаних джерел:

1. Google Developers. Flutter Documentation. URL: https://flutter.dev/docs
2. Facebook Developers. React Native Documentation.URL: https://reactnative.dev/docs/getting-started
3. Microsoft. Xamarin Documentation. URL: https://docs.microsoft.com/en-us/xamarin

УДК 004.4:37.091.33:91

Мурзак І. В.
Здобувач вищої освіти
Одеський національний технологічний університет
Науковий керівник
Сакалюк О. Ю.
асистент кафедри інформаційних технологій та кібербезпеки
Одеський національний технологічний університет
Попков Д. М.
старший викладач кафедри інформаційних технологій та кібербезпеки
Одеський національний технологічний університет

РОЗРОБКА ПРОГРАМНОГО ЗАСОБУ ДЛЯ НАВЧАЛЬНОЇ ГРИ З ГЕОГРАФІЇ «ВГАДАЙ ПРАПОР»

Сучасні освітні методики все частіше використовують ігри та інтерактивні засоби для залучення учнів і підвищення ефективності навчання. Гра «Вгадай прапор» викликає інтерес до географії через захоплюючі завдання та сприяє кращому засвоєнню інформації. Включення ігрових елементів стимулює креативність і допомагає легко закріпити знання. Оскільки географічна грамотність залишається важливою складовою освіти, ця гра допоможе швидше запам'ятати прапори, розташування та інші важливі дані про країни.

Метою даної роботи є розробка та реалізація комп'ютерної гри «Вгадай прапор», яка буде сприяти розвитку культурного та географічного світогляду, а також когнітивних навичок користувачів. Така гра буде спрямована на

покращення знань про різноманітність національних прапорів світу, сприяючи активнішому вивченню географії та культури різних країн.

У ході пошукової роботи в українському сегменті інтернету було виявлено декілька варіантів ігрових застосунків, які носили деякі характеристики гри «Вгадай прапор», але жоден з них не був повноцінним продуктом. Один із найближчих за семантикою до цієї гри є фрагмент, вбудований на сайті «Join the Travel». Варто відзначити, що ця програма, хоч і має деякі позитивні особливості, все ж таки має свої обмеження, які потрібно врахувати для подальшого вдосконалення майбутньої гри [1]. Розробка браузерної гри «Вгадай прапор» може бути розділена на кілька етапів (див. табл. 1)

Таблиця 1

Етапи розробки гри «Вгадай прапор»

№	Етап	Опис
1.	Збір вимог	– визначення цільової аудиторії; – визначення правил гри та механіку.
2.	Проектування	– розробка макетів інтерфейсу користувача; – вибір технологічного стеку (мова програмування, бібліотеки, інструменти розробки).
3.	Розробка	– написання коду для графічного інтерфейсу та логіки гри; – реалізація системи рекордів і опцій таймеру.
4.	Інтеграція бази даних	– збереження і відновлення рекордів гравців; – управління набором даних прапорів.
5.	Тестування	– перевірка функціональності; – виправлення помилок та оптимізація продуктивності.

Джерело: узагальнено автором

При розробці веб-гри «Вгадай прапор» можна стикнутися з рядом викликів. Однією з головних проблем є збір та управління великою кількістю зображень прапорів, їх оптимізація для швидкого завантаження без втрати якості. Також необхідно забезпечити сумісність зображень з різними браузерами та пристроями, включаючи мобільні. Крім технічних аспектів, є проблеми з UX/UI дизайном, такі як створення інтуїтивного інтерфейсу, який був би зрозумілим і простим у використанні для користувачів різного віку та досвіду. Розробка системи рекордів вимагає створення надійної бази даних та механізмів захисту від шахрайства.

Для розробки даної гри було обрано JavaScript фреймворк React. React є однією з найпопулярніших бібліотек JavaScript для створення користувацьких інтерфейсів, особливо для веб-додатків. React дозволяє створювати інтерактивні UI з високою продуктивністю за допомогою декларативного підходу, що робить код легшим для розуміння та підтримки. Компонентна архітектура React ідеально підходить для ігор, де різні елементи інтерфейсу, як-от прапори та

кнопки, можуть бути побудовані як окремі, повторно використовувані компоненти.

Даний фреймворк ефективно керує оновленнями DOM, що є важливим для ігор, де потрібно часто оновлювати інтерфейс без втрати продуктивності. Використання віртуального DOM мінімізує кількість взаємодій з реальним DOM, що дозволяє швидко відображати зміни на сторінці, такі як перевірка відповідей гравця або оновлення книги рекордів.

Крім того, React може бути інтегрований з іншими бібліотеками та фреймворками, які можуть забезпечити додаткову функціональність для таймерів, анімації та управління станами, що робить його гнучким рішенням для розробки гри [2].

Розглянемо етапи реалізації програмного продукту:

1. налаштування середовища розробки (створення нового проекту, потім було встановлено додаткові необхідні залежності для розробки ПЗ – встановлення Firebase SDK,а також деякі додаткові бібліотеки React, необхідні для реалізації певних функціональних можливостей);

2. розробка інтерфейсу користувача (використання сервісу flagcdn.com для отримання адрес зображень, а також використання CSS-стилів для стилізації інтерфейсу та забезпечення привабливого вигляду гри);

3. розробка функціоналу гри (реалізований механізму випадкового вибору п'яти прапорів для відображення на екрані гравця, а також механізм перевірки правильності відповідей та оновлення рахунку користувача);

4. реалізація книги рекордів (впровадження основного функціоналу гри було інтегровано збереження рекордів користувачів у Firebase).

Результат роботи гри представлено на рис.1 та рис.2.

Рисунок 1 – Інтерфейс гри

Рисунок 2 – Виведення результатів

Після закінчення гри гравець бачить вікно з кінцевим результатом та дві кнопки за допомогою яких можна зіграти ще раз або перейти до головної сторінки.

У ході реалізації даного проєкту було успішно виконано поставлені завдання з розробки гри "Вгадай прапор". Завдання, визначені на початку роботи, були виконані у повному обсязі, і результатом став функціональний та інтерактивний застосунок, який дозволяє гравцям тестувати свої знання та навички вгадування прапорів різних країн.

Отриманий результат виглядає не лише як виконане завдання, але й як продукт, що може зацікавити та задовольнити користувачів. Гра «Вгадай прапор» відкриває можливості для подальшого розвитку та вдосконалення, включаючи додаткові функції та елементи гейміфікації, що можуть зробити гру ще привабливішою для широкого кола гравців.

Список використаних джерел

1. Гра Прапори світу // Join the Travel: [Веб-сайт]. URL: https://jointhetravel.com/uk/world-flags-game/ (дата звернення: 10.09.2024).
2. Learn React // React Dev: [Веб-сайт]. URL: https://react.dev/learn (accessed at: 11.09.2024).

УДК 05:[378.147.091.3:004]

Петриківа Т.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

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПРИ ПІДГОТОВЦІ МАЙБУТНІХ МЕНЕДЖЕРІВ

Сучасний менеджер, виконуючи професійні обов’язки, має використовувати вміння щодо пошуку необхідної інформації, аналізу, обробки даних та їх інтерпретації для подальшої роботи. Крім того, менеджери доволі часто самостійно створюють потрібну інформацію, поширюють її з метою професійного використання, а також використовують новітні інформаційно-комунікаційні технології. Саме тому оволодіння теоретичними знаннями та практичними навичками в сфері інформаційних технологій є актуальним в освіті майбутніх менеджерів.

З огляду на прискорені темпи розвитку інформаційних технологій, освітній процес намагається адаптуватися до використання нових інструментів, що застосовуються в сфері управління та бізнесу. Так, сучасною освітньою програмою підготовки здобувачів першого (бакалаврського) рівня «Цифровий менеджмент в бізнесі» зі спеціальності 073 «Менеджмент» передбачено формування навичок використання інформаційних і комунікаційних технологій [1]. Тобто майбутній менеджер володітиме особливостями використання електронної пошти, корпоративних месенджерів, відеоконференцій, інструментами планування, аналізу та інтерпретації інформації, які дозволятимуть проводити якісний та кількісний аналіз, а також приймати на їх базі рішення, наближені до реальних. Зауважимо, що управлінцям у сучасному світі діджиталізації дуже важливо адаптуватися до нових технологій та управляти процесом змін у колективі.

Формування ІКТ-компетентності є цінним активом, яким повинен володіти сучасний менеджер, якщо він хоче ефективно та результативно виконувати свої обов'язки. Метою інтеграції ІКТ у професійну діяльність є покращення та підвищення якості, доступності та рентабельності управлінської діяльності, а також це стосується переваг мережевого об'єднання організацій для вирішення викликів сучасної глобалізації [2].

На особливу увагу при підготовці майбутніх менеджерів заслуговує навчання інформаційно-комунікаційним технологіям. Зокрема, викладачі ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна використовують віртуальні навчальні середовища, онлайн – курси, платформи, які сприяють засвоєнню нового матеріалу під час навчального процесу, а також поза ним із урахуванням персональної траєкторії навчання для кожного студента. За допомогою таких платформ, як Moodle, Google Classroom є можливість створювати інтерактивні курси, проводити різні форми контролю знань, такі як тестування, контрольні роботи, а також відстежувати успіхи здобувачів в режимі реального часу. Такий інструмент як інтерактивний засіб навчання зарекомендував себе в якості методу, що покращує засвоєння матеріалу, розвиває критичне мислення, комунікативні навички через можливість дозволяти здобувачам не лише бути пасивними слухачами, а й брати участь у інтерактивних вправах, набувати практичних умінь та оволодівати професійними навичками. Електронні підручники, форуми, чати, відеоконференції, моделі – все це робить процес навчання ефективнішим та більш цікавим і сучасним.

Отже, впровадження технологій в навчальний процес при підготовці майбутніх менеджерів є важливою умовою підготовки компетентних, конкурентоспроможних та затребуваних на ринку праці менеджерів.

Список використаних джерел:

1.Освітньо-професійна програма «Цифровий менеджмент в бізнесі» першого бакалаврського рівня вищої освіти спеціальності 073 Харківського

національного університету імені В.Н. Каразіна. URL: http://kbi.karazin.ua/wp-content/uploads/2024/06/4.OPP_073_B.pdf

2.Мукан Н., Гелеш А., Бондін Д. Формування ІКТ‑компетентності майбутніх менеджерів у закладах вищої освіти. *Академічні візії*. Випуск 21/2023 DOI: http://dx.doi.org/10.5281/zenodo.8177327

УДК 004.8:004.9

Проценко Н.М.
к.е.н., доцент, доцент кафедри інформаційних технологій, кібернетики та захисту інформації
Державний біотехнологічний університет
Бутенко Т.А.
к.е.н., доцент, доцент кафедри інформаційних технологій, кібернетики та захисту інформації
Державний біотехнологічний університет

СИМБІОЗ ШТУЧНОГО ІНТЕЛЕКТУ ТА СУЧАСНИХ ТЕХНОЛОГІЙ ОБРОБКИ ДАНИХ

У сучасному світі технології розвиваються неймовірно швидко: те, що до недавно виглядало як фантастика або може з’явитися в далекому майбутньому, сьогодні стає невід’ємною частиною багатьох сфер життя. У світі, де кожну секунду хтось натискає клавішу або робить клік мишею, настає нова ера − ера нейромереж та штучного інтелекту.

Штучний інтелект (англ. AI) не є зовсім новим явищем. Цей термін вперше ввів у 1956 році Джон Маккарті (математик, який працював асистентом професора у Дартмутському коледжі) і застосовувався для опису нової області дослідження: можливості моделювати міркування, інтелект та творчі процеси за допомогою обчислювальних машин. Проте лише запуск генеративної платформи штучного інтелекту OpenAI, відомої як ChatGPT (2022 р.), привернуло широку увагу до цієї технології та сприяло більш інтенсивному її використанню.

Ринок штучного інтелекту бурхливо розвивається: за даними дослідницької компанії MarketsandMarkets до 2027 року його обсяг із середньорічним темпом зростання 36,2 % досягне 407 млрд доларів США. У 2024 році інструменти штучного інтелекту використовують майже 314 млн осіб, тобто кожна 27-ма людина у світі [1]. Зміни, які відбуваються завдяки штучному інтелекту, фіксуються в науці, виробництві, творчості, зокрема у процесі створення текстів.

Перші програми, що використовували штучний інтелект (ШІ) для написання текстів, автоматично генерували прості звіти та статистичні дані. Згодом цей підхід змінився: ШІ не лише автоматизує процеси, а й пропонує нові

способи структурування та форматування текстів, відкриває можливості застосовувати різні стилі та форми. На сьогодні існують системи, які здатні створювати тексти, до складу яких можуть входити статті з новинами та літературні твори. Прикладом такого прогресу є розвиток моделей, заснованих на GPT (Generative Pretrained Transformer). Головна особливість нейромережі складається з двох компонент: 1) здатності запам'ятовувати та аналізувати інформацію; 2) можливості створювати на основі цієї інформації логічно-пов'язаний текст. Потужна модель обробки природної мови з архітектурою «трансформер» створює фрази та речення за тим самим алгоритмом, як це робить людина у розмові чи листі.

У листопаді 2022 року компанія OpenAI представила свій новий продукт – чат-бот ChatGPT із штучним інтелектом. Ця версія нейромережі дуже швидко перетворилася у побутовий інструмент, який використовують люди різних вікових груп і професії. Користувацькі моделі ChatGPT дозволяють створити більш персоналізований та цілеспрямований розмовний досвід, який адаптується до відповідної галузі чи сфери використання. По суті, такі моделі надають користувачам можливість редагувати та навчати власні версії моделі ChatGPT відповідно до своїх особистих потреб.

Наприклад, CapCut VideoGPT дозволяє перетворити текстові концепції на аудіовізуальні сценарії та спростити виробництво відео. Дуже ефективною зарекомендувала себе користувацька модель Video Summarizer, що здатна інтерпретувати запити на мові, яку вказує користувач, і концентруватися на свіжому відеоконтенті, забезпечуючи актуальність представлених резюме та аналізів. Фахівцям, які працюють у сфері будівництва, архітектури чи певних творчих професій, цікавим буде DALL-E, який генерує зображення на основі текстових описів і створює візуальні образи.

Швидке створення якісного контенту є однією із вимог сьогодення. Копірайтинг для компаній, що працюють на іноземний ринок, робоче листування та звіти в міжнародних компаніях, журналістика в закордонних ЗМІ − безліч професій пов'язані з необхідністю писати тексти мовами, носіями яких вони не є. Hemingway Editor – це набір інструментів, призначений для покращення та доопрацювання текстів за допомогою перевірених принципів редагування. Програма оптимізує заплутані речення, замінює прислівники точними дієсловами, підтримує єдиний стиль, зводить до мінімуму зайву пунктуацію та негативні висловлювання. Завдяки такому алгоритму досягається створення ясного і всеосяжного тексту для максимального впливу.

Не можна обійти увагою й такий напрям, як e-commerce (електронна комерція), що давно стала звичною частиною нашого життя, але інтерес до неї з кожним роком зростає. У 2024 році більшість ресторанів мають можливість доставки, салони краси пропонують клієнтам запис через сайт, а сотні магазинів одягу існують тільки на маркетплейсі. За даними UNCTAD, загальний обсяг електронної торгівлі у світі вже вищий за 26,6 трлн доларів США [2]. У 2020 році частка e-commerce становила 17 % світової торгівлі, і прогнози говорять про те, що до 2025 року вона збільшиться до 25 % [3], і вже до 2032

року досягне неймовірної планки 57 трлн доларів США [4]. Проте сьогодні ринок електронної комерції став висококонкурентним і власникам сайтів необхідно, щоб саме їх ресурс займав найвищу позицію у видачі Google за цільовими запитами. Але це вимагає цілого комплексу заходів для покращення видимості сайту в пошукових системах, тобто оптимізації сайтів або SEO (Search Engine Optimization). Для виконання таких непростих завдань корисним буде Julian Goldie GPT, що пропонує експертні рекомендації та ефективні рішення для SEO. Цей спеціалізований сервіс надає практичні рекомендації за такими ключовими напрямками SEO, як побудова посилань, розробка контенту та використання SEO-інструментів.

Крім того, для успішного просування свого продукту потрібна правильна маркетингова політика, тобто наскільки глибоко розуміння бренду чи продукту. Це передбачає оцінку бренду, цільового ринку, аналіз сильних та слабких сторін конкурентів. Помічником у вирішенні цих питань може стати GPT Pro Marketer – віртуальний експерт з маркетингу, який запропонує стратегічне управління з різних маркетингових аспектів.

Якісний аналіз це обов'язкова умова для зрозумілих висновків на основі даних. Проте, щодня створюється 2,5 10^{18} байт інформації [5]. Ця інформація настільки велика та різноманітна, що її складно проаналізувати за допомогою звичайних засобів аналізу даних (наприклад, реляційних баз даних). Тому був введений окремий термін Big Data. Саме поєднання технології штучного інтелекту та аналізу даних дозволяє отримувати прогнози на основі цих нових даних і все частіше у наукових джерелах зустрічаються назви цих двох технологій у вигляді стійкої абревіатури BD&AI. Великі дані акумулюють цінну інформацію про чисельні унікальні об'єкти, структурні закономірності, аномалії та прийняття рішень у різноманітних цифрових додатках. ШІ будує прогнози, розробляє рекомендації та здійснює моделювання процесів. Методи штучного інтелекту, такі як машинне навчання, глибоке навчання, обробка природної мови – дозволяють переглянути ці дані набагато швидше, ніж будь-яка людина. Переваги штучного інтелекту великих даних досить очевидні: швидке отримання аналітичної інформації, точна інформація, точність та визначення тонкощів. Увесь цей комплекс дій сприяє прийняттю зважених та обґрунтованих рішень. Наразі практично всі онлайн-ресурси впровадили цю технологію. Сукупний потенціал цих двох технологій у таких секторах, як уряд та державне управління, кібербезпека, охорона здоров'я, транспорт тощо може значно підвищити швидкість організаційних процесів і якісно покращити автоматизоване управління.

Підсумовуючи вище розглянуте, можемо відмітити, що завдяки штучному інтелекту відбулися революційні зміни в багатьох сферах людського життя. Сьогодні ШІ не просто інструмент для спрощення завдань, а й партнер, здатний збагатити людську творчість унікальними можливостями і діапазон його застосування безмежний: від бізнес-звітів до літературних творів. Поєднання штучного інтелекту та технологій обробки даних відкриває нові горизонти, допомагаючи впоратися з рутинною роботою та стимулюючи творчі процеси.

Список використаних джерел:

1. Artificial Intelligence. URL: https://www.marketsandmarkets.com.
2. Global Trade Data. URL: https://tradeint.com/insights/search-for-importers-and-exporters.
3. Top Trends to Watch in 2024. URL: https://www.emarketer.com/content/top-trends-watch-2024.
4. Що таке електронна комерція? URL: https://wezom.com.ua/blog/elektronnaya-kommertsiya.
5. BIG DATA (великі дані): Що, навіщо і як? URL: https://klona.ua/uk/blog/artificial-intelligence-uk/big-data-velyki-dani-shho-navishho-i-yak.

УДК 004.8.37

Ракітін Н.М.
здобувач вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Науковий керівник
Петренко О. Є.
к.т.н., доцент, доцент кафедри інформаційних технологій
та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ НАВЧАЛЬНОГО ПРОЦЕСУ

Штучний інтелект (далі ШІ) поступово стає невід'ємною частиною нашого життя, і освіта не є винятком. ШІ пропонує безліч інструментів та можливостей, які можуть значно покращити процес навчання як для студентів, так і для викладачів. Створені програмні продукти дозволяють знайти миттєві та вичерпні відповіді на питання з різноманітних галузей, що в свою чергу надає можливості підвищити рівень знань студентів при підготовки домашнього завдання. ШІ покращує роботу викладача, дозволяючи йому витрачати менше часу на підготовку до занять. Викладачі мають можливість вдосконалити свої заняття шляхом огляду проблеми з різних точок зору, отримати матеріал, що доповнений різними експериментами. ШІ може розробляти персоналізовані навчальні плани, враховуючи сильні та слабкі сторони кожного студента. ШІ може автоматично перевіряти прості завдання, звільняючи викладачів для більш творчої роботи. ШІ може створювати різноманітні навчальні матеріали, такі як тести, вправи, презентації. ШІ може аналізувати великі обсяги даних про успішність учнів, допомагаючи викладачам виявляти труднощі та розробляти ефективні стратегії навчання.

Важливо зазначити, що ШІ не замінює викладача, а є його помічником. Роль викладача полягає в тому, щоб керувати навчальним процесом, мотивувати студентів та створювати сприятливе навчальне середовище. ШІ може взяти на себе рутинні завдання, звільнивши викладача для більш творчої роботи та індивідуальної роботи з студентами. З огляду на існуючі переваги, застосування ШІ має також певні недоліки, а саме є загроза його застосування студентами не для отримання нових знань, а пошуку легкого шляху виконання домашнього завдання, не оволодіваючи знаннями та навичками.

Метою дослідження є виявлення переваг та недоліків інструментів ШІ на основі здійснення їх порівняльно аналізу.

В роботі розглянуто наступні інструменти ШІ, а саме: Course Hero, Cognii, Socrat.

Course Hero створено для покращення академічного навчання та ефективності. Він надає допомогу в домашніх завданнях на базі штучного інтелекту, що значно прискорює процес пошуку миттєвих відповідей і детальних пояснень для широкого спектру навчальних матеріалів. Вказаний інструмент дозволяє отримувати запитання на відповіді, запитання з заповненням бланку, відкриті запитання в режимі реального часу.

Socrat – це інструмент штучного інтелекту, який покращує викладання та навчання, надаючи викладачам можливості створення курсів, керування завданнями та відстеження прогресу студентів. Студенти використовують інструменти на основі ШІ, щоб покращити свої результати навчання.

Третім інструментом штучного інтелекту є Cognii. Він має в своєї конфігурації віртуального помічника у навчанні, який покладається на розмовну технологію, щоб допомогти студентам формувати відповіді у відкритому форматі та вдосконалювати навички критичного мислення. Окрім цього, віртуальний помічник також забезпечує індивідуальне навчання та зворотний зв’язок у реальному часі, налаштований для кожного студента.

Для аналізу інструментів ШІ було введено наступні критерії:

- можливість створення курсів та завдань викладачем;
- підтримка можливостей індивідуального навчання;
- керування діяльністю студентів в режимі реального часу
- підтримка можливості групової роботи.

Результати проведеного аналізу наведено у табл.1.

Згідно з проведеним аналізом, інструмент Socrat має переваги в порівнянні з Course Hero та Cognii, що робить його привабливим для застосування в освітньому процесі. Крім зазначених в таблиці 1 критеріїв, інструмент Socrat дозволяє здійснювати контроль в процесі навчання з боку викладача, може бути застосований на всіх освітніх рівнях, дозволяє підключення з будь-якого пристрою та має зручний інтерфейс.

Таблиця 1.

Порівняльний аналіз інструментів ШІ.

Назва інструменту ШІ	можливість створення курсів та завдань викладачем	Підтримка можливостей індивідуального навчання	Керування діяльністю з боку викладача студентів в режимі реального часу	Підтримка можливості групової роботи
Course Hero	ні	підтримує	ні	не підтримує
Socrat	так	підтримує	так	підтримує
Cognii	так	підтримує	ні	не підтримує

За допомогою інструменту Socrat викладач може зберегти час на перевірку відвідування занять з боку студентів, може миттєво оцінювати подані студентами завдання, виділяючи проблемні питання та надаючи відгуки. Він дозволяє викладачам негайно втручатися, коли студент стискається з проблемами в навчанні, може передбачити, які студенти знаходяться в групі ризику.

Висновки. Штучний інтелект має великий потенціал для трансформації освіти. Завдяки своїм можливостям, ШІ може зробити навчання більш персоналізованим, ефективним та доступним. Однак, важливо розуміти, що ШІ є лише інструментом, його успішне використання залежить від того, як він інтегрується в освітній процес викладачем.

Список використаних джерел:

1. Teach Start Up School: https://tsus.org/node/399
2. На урок: https://naurok.com.ua/post/shtuchniy-intelekt-v-osviti-ide-dlya-vikoristannya-na-urokah
3. Unite.AI – 10 найкращих інструментів ШІ для освіти (вересень 2024 р.)https://www.unite.ai/uk/10-best-ai-tools-for-education/

УДК 004.4

Рибалка Р.А.
здобувач вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Наукові керівники
Ковальчук Д.М.
к.т.н., старший викладач
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Самородов Б.В.
д.е.н., к.т.н., професор
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВИКОРИСТАННЯ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ В СИСТЕМАХ АВТОМАТИЗОВАНОГО ДОКУМЕНТООБІГУ

Системи електронного документообігу – це спеціалізовані програмні рішення, призначені для автоматизації процесів створення, обробки, зберігання, передачі та контролю документів у цифровій формі. Вони допомагають підприємствам і організаціям ефективно управляти документацією, забезпечують зручність доступу до даних, підвищують продуктивність роботи та знижують ризики втрати інформації. Використання мікросервісної архітектури в системах автоматизованого документообігу дозволяє суттєво підвищити гнучкість, масштабованість і надійність таких систем.

Мікросервісна архітектура – це підхід до організації архітектури, що ґрунтується на ряді незалежних сервісів. Кожен із цих сервісів має свою бізнес-логіку та базу даних, орієнтуючись на конкретну мету. Оновлення, тестування, розгортання та масштабування здійснюються всередині кожного сервісу. Мікросервіси дозволяють розбивати великі бізнес-задачі на кілька самостійних баз коду. Хоча вони не зменшують загальної складності, вони роблять її більш помітною і керованою, розділяючи завдання на менші процеси, які працюють незалежно один від одного та вносять свій вклад у загальну мету.

Основні переваги мікросервісної архітектури полягають в наступному:

- гнучкість: кожен мікросервіс може розвиватися і змінюватися незалежно від інших, що дозволяє швидше адаптуватися до змін в бізнес-вимогах;
- масштабованість: мікросервіси можна масштабувати окремо, в залежності від потреб, що дозволяє ефективніше використовувати ресурси;
- надійність: у випадку збоїв одного сервісу решта системи залишається працездатною. Це підвищує загальну надійність системи;
- технологічна різноманітність: мікросервіси можуть бути реалізовані з використанням різних технологій і мов програмування, що дозволяє вибрати оптимальні рішення для кожного конкретного сервісу;

- швидкість розробки: незалежні команди можуть працювати над різними мікросервісами одночасно, що скорочує час розробки та впровадження нових функцій;
- зручність обслуговування: оскільки кожен мікросервіс автономний, зміни або оновлення можна виконувати без впливу на всю систему;
- покращений контроль версій: окремі мікросервіси можна оновлювати без необхідності синхронізації з усією системою, що спрощує управління версіями.

Ці переваги роблять мікросервісну архітектуру привабливим вибором для реалізації автоматизованої системи електронного документообігу.

В роботі пропонується розробити автоматизовану систему електронного документообігу, яка складається з таких функціональних компонентів:

1. обробка документів: мікросервіси для сканування, розпізнавання тексту (OCR), аналізу і категоризації документів;
2. зберігання та архівування: мікросервіси які відповідають за зберігання документів у різних форматах, забезпечення швидкого доступу до них;
3. управління доступом: контроль прав доступу до документів, впровадження механізмів автентифікації та авторизації;
4. інтеграція з іншими системами: мікросервіси, які забезпечують інтеграцію з CRM, ERP та іншими системами, можуть автоматизувати обмін даними.

Для комунікації між мікросервісами пропонується використати такі моделі обміну:

- HTTP/REST: найбільш популярний спосіб взаємодії між мікросервісами, що забезпечує простоту та зрозумілість;
- масиви повідомлень: використання брокерів повідомлень (наприклад, RabbitMQ, Kafka) для асинхронної взаємодії між сервісами, що може покращити продуктивність і надійність.

Для контейнеризації мікросервісів, пропонується використання Docker, що спрощує розгортання і управління мікросервісами.

Отже, мікросервісна архітектура має значний потенціал для впровадження в системи автоматизованого документообігу, дозволяючи підвищити їх гнучкість, масштабованість і надійність. Хоча впровадження цього підходу пов'язане з певними викликами, такі як управління складністю та безпекою, належна реалізація мікросервісів може значно покращити ефективність і продуктивність документообігу в організаціях.

Список використаних джерел:

1. Карпенко М. Ю. Системи електронного документообігу : конспект лекцій для студентів усіх форм навчання першого (бакалаврського) рівня вищої освіти спеціальності 122 – Комп’ютерні науки / М. Ю. Карпенко; Харків. нац. університет міського господарства ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2021. – 68 с.

2. Microservices vs Monolithic. URL: https://ncube.com/blog/microservices-vs-monolithic-which-architecturesuits-best-for-your-project.
3. Мікросервіси. URL: https://uk.wikipedia.org/wiki/%D0%9C%D1%96%D0%BA%D1%80%D0%BE%D1%81%D0%B5%D1%80%D0%B2%D1%96%D1%81%D0%B8.

УДК 004.72

Романов Р.Р.
здобувач вищої освіти,
ННІ «Комп'ютерних наук та штучного інтелекту» ХНУ імені В.Н. Каразіна

МОДЕЛЬ КЛАСИФІКАЦІЇ СТАНУ КОМП'ЮТЕРНИХ МЕРЕЖ

Інформаційно-обчислювальні мережі, будучи основою сучасної індустрії обробки інформації, висувають високі вимоги до ефективного використання засобів зв'язку та характеристик обслуговування мережевих абонентів. У зв'язку з цим однією з найважливіших проблем, яку доводиться вирішувати при практичному втіленні мережевих проєктів та їх експлуатаційному супроводі, є проблема адмініструванні та організації ефективної роботи мережі у різних умовах функціонування. Тому актуальною є задача побудови комп'ютерної моделі класифікації стану комп'ютерних мереж, що є важливим інструментом для аналізу, моніторингу та управління мережевими ресурсами.

В роботі запропонована комп'ютерна модель класифікації стану комп'ютерних мереж на основі алгоритмів машинного навчання. Вона використовується для визначення поточного стану мережі, ідентифікації потенційних проблем та їхньої природи (наприклад, перевантаження, несправності, атаки) та прийняття рішень щодо оптимізації мережевої інфраструктури.

Класифікація стану мережі зазвичай ґрунтується на зібраних даних, таких як трафік, затримки, помилки передачі, час відгуку системи, використання пропускної здатності тощо. За допомогою алгоритмів машинного навчання або традиційних статистичних методів ці дані обробляються та аналізуються для виявлення аномалій та визначення нормальних і критичних станів мережі.

Запропонована комп'ютерна модель, може класифікувати чотири стани комп'ютерної мережі, такі як:

- нормальний стан: мережа працює стабільно, всі компоненти функціонують правильно, трафік проходить без затримок;
- перевантаження: збільшення обсягу трафіку, що призводить до затримок або втрат пакетів. Може виникати через недостатні ресурси або атаки на мережу;

- помилки в передачі: виникають через проблеми з обладнанням, конфігурацією або зовнішніми факторами (наприклад, перешкоди в бездротових мережах);
- аварійний стан: мережа або її компоненти перестають функціонувати (наприклад, збій сервера, відключення каналу зв'язку).

В комп’ютерній моделі класифікації стану комп’ютерних мереж, пропонується представити комп’ютерну мережу на основі графової моделі. Кожен вузол мережі є вершиною графа, дуга – канал зв’язку з певною пропускною спроможністю. Вхідними даними буде масив, який визначає пропускну спроможність кожної дуги. Якщо дуги не існує, її пропускна спроможність дорівнює нулю. Модель враховує такі метрики для класифікації:

- пропускна здатність: вимірює, скільки даних може бути передано через мережу за одиницю часу;
- затримка: час, необхідний для передачі даних від джерела до призначення. Включає затримку передачі, обробки та черги;
- втрати пакетів: відсоток пакетів, які не досягають свого призначення. Високий рівень втрат свідчить про проблеми в мережі.
- час відмови: час, протягом якого мережа або її компоненти не функціонують.

Прогнозування стану мережі відбувається на основі алгоритмів машинного навчання та моделей прийняття рішень. Алгоритми машинного навчання використовують алгоритми для аналізу історичних даних та прогнозування можливих станів мережі на основі виявлених патернів. Моделі прийняття рішень – застосовують статистичні методи для оцінки ризиків і планування заходів щодо покращення стану мережі.

В роботі досліджено такі алгоритми класифікації, як: дерева прийняття рішень (Decision Tree), метод k-найближчих сусідів (k-Nearest Neighbors), метод опорних векторів (Support Vector Machine) та логістична регресія.

Отже, класифікація стану комп’ютерних мереж є критично важливим аспектом управління мережами. Застосування моделей, метрик і інструментів моніторингу дозволяє оперативно виявляти проблеми, покращувати продуктивність і забезпечувати надійність мережевих ресурсів. Ця інформація допомагає організаціям ухвалювати обґрунтовані рішення щодо оптимізації мережі та покращення її стану.

Список використаних джерел:

1. Жураковський Б. Ю., Зенів І.О. Комп’ютерні мережі. Частина 1: навчальний посібник для студентів спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології. КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.
2. Харченко В.О. Основи машинного навчання : навчальний посібник. – Суми : Сумський державний університет, 2023. – 264 с.

3. Задерейко О. В. Комп’ютерні мережі : навчально-методичний посібник [Електронне видання] / О. В. Задерейко, Багнюк Н.В., А. А. Толокнов. – Одеса : Фенікс, 2023. – 210 с. – URL: http://hdl.handle.net/11300/25951

УДК 004.43

Свинаренко А.А.
здобувачка вищої освіти,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Науковий керівник
Чеканова Н.М.
к.фіз.-м.наук
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

КЛЮЧОВІ АСПЕКТИ ВПРОВАДЖЕННЯ АДАПТИВНОЇ ВІЗУАЛІЗАЦІЇ НА БАЗІ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У СТАРТАПАХ

Стартап – бізнес-компанія, орієнтована на інноваційні та ризиковані проєкти, має і може залучати зовнішнє фінансування для швидкого зростання. Для стартапу характерне швидке виведення продукту на ринок та завоювання його частини. Через схильність до ризиків команді стартапу необхідно ухвалювати обґрунтовані рішення в умовах невизначеності за короткий проміжок часу.

Для коректності таких процесів як аналіз даних і прийняття рішень важливо використовувати ефективні інструменти. Одним з них є візуалізація, яка покликана виконувати завдання трансформації великих обсягів інформації у наочну форму. Цей інструмент є одним з популярних, доступних і дієвих, його застосовують компанії різних розмірів на багатьох стадіях своєї роботи.

Доказами того, що візуалізація даних відіграє важливу роль для підтримки прийняття рішень, є наступні твердження:

- доносити інформацію простіше завдяки використанню графіків, дашбордів, діаграм;
- людський мозок краще утримує в пам’яті кольорові зображення, аніж текст;
- є можливість наочного відслідковування трендів і аномалій.

Адаптивна візуалізація відрізняється від інтерактивної тим, що здатна автоматично змінюватися та підлаштовуватися під потреби користувача або зміни в даних. У розрізі цього типу візуалізації під поняттям штучний інтелект мається на увазі платформи чи інструменти, що використовують алгоритми машинного навчання або прогнозування для автоматичного аналізу даних і побудови адаптивних візуалізацій. Прикладами таких інструментів є:

- Tableau з інтеграцією ШІ для створення адаптивних візуалізацій;

- Power BI з вбудованими можливостями ШІ для автоматичного аналізу даних;
- Google AI в поєднанні з BigQuery може використовуватися для аналізу великих обсягів даних, а Data Studio – для створення адаптивних візуалізацій;
- бібліотеки Python, такі як TensorFlow, Scikit-learn або Keras, можуть бути використані для побудови AI-моделей, а візуалізація може реалізовуватися за допомогою таких бібліотек, як Matplotlib або Plotly.

Для ефективного і грамотного впровадження адаптивної візуалізації важливо враховувати такі фактори:

- Якість вхідних даних: для точності прогнозів системі необхідно, щоб дані відповідали критеріям цілісності, повноті, валідності.
- Регулярний моніторинг: встановлення чіткого графіку для забезпечення систематичного оновлення та перевірки наявної інформації.
- Вибір відповідної AI-технології: необхідно враховувати специфіку даних та задач, які стартап прагне вирішувати за допомогою ШІ. Це можуть бути як моделі машинного навчання, так і моделі глибоко навчання, в залежності від обсягу та складності даних.
- Прозорість результатів: Інтерпретацію прогнозів у графічному вигляді потрібно подавати в зрозумілому форматі для всіх, хто буде з нею взаємодіяти.
- Відповідність стандартам безпеки: Система повинна відповідати вимогам законодавства про захист даних.

Впровадження адаптивної візуалізації на основі штучного інтелекту є важливим елементом для успішної діяльності стартапів. Це допомагає компанії ухвалювати більш обґрунтовані рішення в умовах ризику і мінливості ринку. Правильна інтеграція ШІ-технологій дозволяє не лише автоматизувати процеси, але й підвищити точність аналізу, забезпечуючи підприємство важливою інформацією для швидкого та ефективного прийняття рішень.

Список використаних джерел:

1. Анналін Нг, Кеннет Су. Опануй числа! Наука про дані для нефахівців. Фабула. – 2024 . –184 с.
2. Stuart J. Russell and Peter Norvig. Artificial Intelligence A Modern Approach Third Edition. 2018. – 1151 с.
3. What Is Data Visualization? Definition, Examples, And Learning Resources. URL: https://www.tableau.com/learn/articles
4. Microsoft. Microsoft-365 URL: https://www.microsoft.com/uk-ua/microsoft-365
5. TensorBoard: TensorFlow's visualization toolkit. URL: https://www.tensorflow.org

УДК 004

Сидоренко В.О.
здобувачка вищої освіти,
Сумський державний університет
Науковий керівник
Антипенко В.П.
к.т.н., доцент, доцент кафедри інформаційних технологій,
Сумський державний університет

ВЕБОРІЄНТОВАНА ІНФОРМАЦІЙНА СИСТЕМА ПІДТРИМКИ ДІЯЛЬНОСТІ БАЙЄРА ОДЯГУ

Веборієнтована інформаційна система для байєрів одягу [1] – це інноваційний інструмент, який забезпечує ефективну організацію закупівлі вбрання й аксесуарів світових брендів та управління асортиментом для відповідних спеціалістів в індустрії моди. Такий програмний продукт насамперед створюється для спрощення здійснення пошуку, аналізу та придбання товарів із-за кордону. Також його використання забезпечить зручним каналом комунікації всіх учасників даного процесу.

Особливо актуальним даний інструмент є в умовах складної економічної ситуації в Україні. Сьогодні багато брендів залишили наш ринок або значно підвищили ціни на свою продукцію. Це змушує байєрів шукати альтернативні варіанти постачань відповідного одягу та аксесуарів із-за кордоном. Оскільки покупки у такий шлях стали вигіднішими. Завдяки інтеграції з іншими онлайн сервісами, наприклад, такими як закордонні інтернет-магазини, запропонована веборієнтована система для байєрів дозволить ефективно управляти ланцюгом придбання товарів поза межами України. Це дозволить відповідним продавцям адаптуватися до нових умов сучасного ринку.

Тому метою даного проєкту є створення веборієнтованої платформи, застосування якої дозволить байєрам автоматизувати процес отримання запиту на здійснення замовлення в структурованому електронному вигляді, а також сприятиме удосконаленому управлінню товарними запасами та плануванню закупівель. У свою чергу клієнти отримуватимуть актуальну інформацію щодо цін, знижок та наявності товарів світових брендів в реальному часі. Це дозволить мінімізувати вірогідність виникнення помилок, пов’язані з людським фактором, та налагодити процес шопінгу з інших країн [2].

Представлена веборієнтована система передбачає автоматизацію таких процесів, як розміщення товару, опрацювання замовлень, сортування за постачальником, створення відповідних звітів. Також надається зручний канал комунікації з клієнтами. Її використання забезпечує можливість зберігання та аналізу даних про доступну продукцію, ціни та постачальників. Це допомагає байєрам приймати обґрунтовані рішення щодо подальшого кар’єрного розвитку [3].

Таким чином, розробка веборієнтованої інформаційної системи підтримки діяльності байєра одягу є важливим кроком у напрямку удосконалення здійснення процесів закупівлі товарів із-за кордону. Її впровадження дозволить скоротити час клієнтів при здійсненні такого виду шопінгу, знизити витрати на доставку придбаної продукції та забезпечити конкурентну перевагу на ринку моди, що є особливо вагомим фактором у сучасних умовах високого економічного суперництва.

Список використаних джерел:

1. Shklar, L., Rosen, R. Архітектура веб-додатків: принципи, протоколи та практики. – 2-е вид. – Чічестер: Wiley, 2009. – 480 с.
2. Laudon, K.C., Traver, C.G. Електронна комерція: бізнес, технології, суспільство. – 15-е вид. – Бостон: Pearson, 2018. – 912 с.
3. 20 Top eCommerce Trends to Watch in 2024 URL: https://blog.contactpigeon.com/ecommerce-trends-2024/#top10

УДК 004.9

Скорін Ю.І.
к.т.н., доцент, доцент кафедри інформаційних систем
Харківський національний економічний університет імені Семена Кузнеця
Листопад Ю.Р.
здобувач вищої освіти,
Харківський національний економічний університет імені Семена Кузнеця

ІНСТРУМЕНТИ ВЕБ-ПАРСИНГУ ДЛЯ АНАЛІЗУ ВИМОГ ДО КАНДИДАТІВ НА РИНКУ ПРАЦЕВЛАШТУВАННЯ В ІТ СФЕРІ

Актуальність розробки інструменту веб-парсингу для аналізу вимог до кандидатів на ринку працевлаштування в ІТ сфері полягає в необхідності покращення ефективності процесу підбору кандидатів та відповідності їхніх навичок та досвіду робочим вимогам. Завданням дослідження є збір та аналіз інформації про вакансії та їхні вимоги, що дозволить автоматизувати процес збору та фільтрації даних, а також забезпечить централізований доступ до актуальної інформації як для кандидатів, так і роботодавців.

Метою цього дослідження є автоматизований збір інформації із джерел подачі вакансій на ІТ ринку України та подальше представлення інформації у зручному вигляді з можливістю перегляду статистичних даних на основі збережених даних про вакансії.

Ринок праці в галузі інформаційних технологій представляє собою динамічний та конкурентоспроможний сегмент, який визначається численними факторами. За останні роки ІТ-індустрія стала важливим каталізатором технологічного розвитку та ключовим учасником на ринку праці. Низка

особливостей визначає його унікальні риси та тенденції. Швидкий розвиток технологій, таких як штучний інтелект, блокчейн та хмарні обчислення, створює постійний попит на фахівців, що володіють актуальними навичками. Висока конкуренція за талановитими працівниками призводить до зростання заробітних плат та удосконалення систем бонусів.

Глобалізація також впливає на ринок, відкриваючи доступ до міжнародних можливостей та створюючи глобальний басейн талантів. Постійний дефіцит кваліфікованих фахівців заохочує компанії до активного конкурування за кращих працівників. Разом із технологічними змінами змінюються й вимоги до кандидатів. Індивідуальний підхід до розвитку кар'єри, вміння адаптуватися та володіння не лише технічними, але й м'якими навичками стають ключовими факторами. Тенденція до гібридної моделі роботи, де поєднуються віддалена та офісна робота, впливає на критерії вибору роботодавців та відкриває нові можливості для працівників. Культурні та економічні особливості різних регіонів також впливають на структуру та динаміку ринку праці в галузі інформаційних технологій.

Моніторинг ринку праці з використанням веб-парсингу є ключовим елементом стратегічного рекрутингу в галузі інформаційних технологій. За допомогою цього інструменту рекрутери можуть отримувати актуальні дані та аналізувати їх для ефективного взаємодії з динамікою ринку праці. Також, враховуючи попит на конкретні технології, можна визначити тенденції у вимогах до кандидатів. Наприклад, за даними вебпарсингу, збільшення кількості вакансій, де потрібні навички в області штучного інтелекту чи розробки мовою програмування Python, може вказувати на актуальні та важливі напрямки у сфері IT.

Зокрема, у випадку вебпарсингу популярних робочих платформ, таких як Indeed чи Glassdoor, можна взнати не лише про вакансії, але і про середні зарплати, вимоги до досвіду та інші ключові параметри. Це дозволяє рекрутерам здійснювати аналіз конкурентоспроможності пропозицій власної компанії на ринку праці.

Для вирішення завдання та досягнення поставлених цілей у дослідженні, був обраний стратегічний підхід – розробити методологію, яка відповідає унікальним вимогам та специфіці нашого проєкту з аналізу вимог до кандидатів на ринку працевлаштування в галузі інформаційних технологій. Створення власної методології дозволяє не лише точно адаптуватися до конкретних особливостей дослідження, але й акцентує на нашій індивідуальній концепції та підходах. Одним із ключових аспектів розробленої методології є вибір мови програмування та інструментів, що оптимально відповідають завданням вебпарсингу та аналізу вимог до кандидатів.

Для проєкту з розробки інструментарію для вебпарсингу та аналізу даних, були розглянуті різні мови програмування та інструменти. Серед варіантів, які розглядалися, були Python, JavaScript (Node.js), Java, Ruby та C#. Кожна мова має свої переваги та підходить для різних сценаріїв. Python є популярною мовою для вебпарсингу завдяки бібліотеці BeautifulSoup та

фреймворку Scrapy. JavaScript, особливо в середовищі Node.js, дозволяє асинхронно обробляти запити, що є важливим для ефективного взаємодії з великою кількістю даних.

У кінцевому результаті було обрано Node.js. Ця мова має численні переваги, такі як асинхронність, велика кількість доступних бібліотек, зокрема Cheerio та Request, а також активну спільноту розробників. Node.js забезпечує ефективність та гнучкість для успішної реалізації наших завдань у вивченні вимог кандидатів на ринку праці в галузі інформаційних технологій. Необхідно побудувати серверний застосунок, що буде виконувати роботу по збору (парсингу), аналізу та збереженню інформації із сайтів джерел у базу даних MySQL. Використання MySQL у дослідженні та розробці вебпарсера для аналізу вимог до кандидатів на ринку праці в інформаційних технологіях обумовлено кількома обґрунтованими перевагами. MySQL славиться своєю надійністю та стабільністю, що робить його відмінним вибором для забезпечення надійності та стійкості у зберіганні та обробці великого обсягу даних. Його висока швидкодія сприяє ефективному використанню у великих обсягах даних, що буде актуально для мого дослідження. SQL-мова та зручний синтаксис MySQL роблять його досить зрозумілим та легким у використанні. Це спрощує роботу з базою даних та дозволяє ефективно виконувати різноманітні запити для аналізу даних. Гнучкість та розширюваність MySQL важливі для адаптації до зростаючих потреб дослідження та проєкту, забезпечуючи масштабованість. Його активна спільнота та підтримка роблять його надійним та дозволяють швидко вирішувати будь-які труднощі чи питання. Також важливо відзначити, що MySQL легко інтегрується з іншими технологіями, що спрощує роботу та поліпшує ефективність розробки вебпарсера та аналітичного інструментарію в цілому.

До серверного застосунку ще необхідно додати вебзастосунок для перегляду зібраних даних у двох представленнях: табличне із можливістю пошуку; графічне із побудованими графіками для відображення статистичних даних за тими що були зібрані. У списковому відображені має бути можливість сортування списку за будь-яким із стовпчиків та має бути можливість використання фільтрів для зручного пошуку потрібних вакансій, що нададуть найбільш точні результати для вибору роботи. У графічному представлені має бути відображено декілька графіків та діаграм що, дозволять користувачеві переглядати зібрані дані у вигляді зручної статистики. Додатковою можливістю може бути додана фільтрація для графіків та діаграм за різними даними, щоб збільшити кількість видимих даних на одному й тому ж розмірі екрану.

Для розроблення вебзастосунка було обрано Node.js як основу для серверної частини та MySQL для забезпечення надійності бази даних. Розроблення включає в себе backend на Node.js, зосереджуючись на ефективній обробці HTTP-запитів та взаємодії з базою даних. На стороні клієнта ми використовуємо React для створення інтерфейсу, який буде не тільки функціональним, але й забезпечуватиме зручність взаємодії з користувачем. Інтегруємо обидві частини, після чого проводимо ретельне тестування та

оптимізацію, спрямовані на підвищення продуктивності та забезпечення стабільної роботи. Також для виконання роботи було обрано використання Next.js для представлення графічних даних та Redux для інтерфейсу користувача.

Практична значущість даного дослідження полягає в його потенційній здатності сприяти підвищенню ефективності процесу пошуку та відбору кандидатів на ринку працевлаштування в IT сфері. Розроблений інструмент вебпарсингу дозволить кандидатам швидше та зручніше знаходити вакансії, що відповідають їхнім кваліфікаційним вимогам, а роботодавцям забезпечить доступ до більш об'єктивних та актуальних даних про потенційних працівників.

Таким чином, вирішення поставленої наукової задачі є важливим кроком у покращенні процесу підбору кандидатів на ринку працевлаштування в IT сфері, сприяє підвищенню ефективності та точності відбору працівників, а також сприяє зменшенню часових та ресурсних затрат у цьому процесі.

Список використаних джерел:

1. NodeJS ES6 – NodeJS. URL : https://nodejs.org/uk/docs/es6/
2. NextJS Measuring Performance. URL : https://nextjs.org/docs/advanced-features/measuring-performance
3. Стрілочні функції – Developers. URL : https://developer.mozilla.org/ru/docs/Web/JavaScript/Reference/Functions/Arrow_functions

УДК 004.9

Скорін Ю.І.

к.т.н., доцент, доцент кафедри інформаційних систем

Харківський національний економічний університет імені Семена Кузнеця

Мартиненков Д.С.

здобувач вищої освіти,

Харківський національний економічний університет імені Семена Кузнеця

ОПТИМІЗАЦІЯ ВЕБ-ПОРТАЛУ ДЛЯ ПОШУКУ РОБОТИ В IT-СФЕРІ З ВИКОРИСТАННЯМ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

У сучасних умовах ринок праці в IT-сфері зазнає значного розвитку.

Це зумовлено постійним зростанням попиту на висококваліфікованих спеціалістів, що спричиняє збільшення кількості вакансій і необхідність у спеціалізованих знаннях.

Виникають нові виклики як для роботодавців, так і для кандидатів.

Останні стикаються з проблемою ефективного пошуку вакансій, які відповідають їхнім навичкам і досвіду, в умовах великої кількості варіантів.

Сучасні платформи для пошуку роботи, такі як LinkedIn, Indeed, Glassdoor, Dice, намагаються спростити цей процес.

Вони пропонують стандартні пошукові механізми, які базуються на фільтрах та ключових словах.

Однак такі системи часто не враховують індивідуальних потреб і вподобань користувачів.

Це може призводити до отримання нерелевантних результатів, що значно знижує ефективність пошуку.

У цьому контексті актуальним стає застосування нових підходів, зокрема алгоритмів машинного навчання, для автоматизації підбору вакансій та підвищення точності персоналізованих рекомендацій.

Використання алгоритмів машинного навчання дозволяє не лише покращити персоналізовані рекомендації, а й суттєво підвищити точність відповідності між кандидатами та вакансіями.

Такі системи можуть враховувати попередні взаємодії користувачів із платформою, їхній досвід та поведінкові патерни.

Попередній аналіз існуючих платформ показав, що традиційні пошукові системи не повністю використовують потенціал даних про користувачів.

Як зазначено в статті "Recommender Systems: A Primer" [1], сучасні рекомендаційні системи часто ігнорують поведінкові аспекти користувачів, що призводить до недостатньої точності рекомендацій.

Одним із найбільш ефективних алгоритмів для поліпшення персоналізованих рекомендацій є SVD (Singular Value Decomposition).

Він дозволяє розкладати матрицю взаємодій між користувачами і вакансіями, виявляючи приховані патерни в поведінці користувачів.

Це дає можливість передбачати нові вакансії на основі аналізу дій інших користувачів із подібними професійними інтересами.

Такий підхід був успішно впроваджений на платформі LinkedIn, де використання SVD дозволило надавати персоналізовані рекомендації навіть для нових користувачів, які ще не мали активної взаємодії з системою.

Зважаючи на технічний характер IT-сфери, для забезпечення точних рекомендацій важливо застосовувати не лише колаборативне фільтрування, а й контентну фільтрацію.

Цей підхід дозволяє аналізувати текстові описи вакансій та резюме, порівнюючи їх за змістом. Метод TF-IDF (Term Frequency-Inverse Document Frequency) є одним із найбільш ефективних інструментів для аналізу текстових даних.

У статті "Learning job embeddings for job recommendation in a practical setting" [2] обґрунтовано, як векторизація тексту допомагає підвищити релевантність рекомендацій, порівнюючи вимоги вакансій з навичками кандидатів.

Наприклад, на платформах, таких як Hired, застосування TF-IDF дозволяє системам краще співвідносити технічні навички кандидатів з вимогами до вакансій, що робить процес підбору більш точним.

Інтеграція алгоритмів машинного навчання в пошукові системи передбачає також використання складніших моделей, таких як RandomForest.

Ці моделі дозволяють аналізувати складні взаємозв'язки між навичками кандидатів, вимогами до вакансій та іншими чинниками.

У статті "A hybrid job recommendation algorithm based on user behavior and job features" [3] розглядається гібридний підхід, що поєднує аналіз поведінкових аспектів із характеристиками вакансій.

Це дозволяє підвищити точність рекомендацій на платформах, таких як Indeed та Glassdoor, де важливо враховувати як технічні параметри, так і поведінкові чинники, що впливають на вибір користувачів.

Одним із важливих аспектів впровадження систем на основі машинного навчання є зручність використання для користувачів.

Досвід провідних платформ, таких як LinkedIn, свідчить про те, що добре продуманий UX/UI має вирішальне значення для успіху системи.

Оптимізація користувацького інтерфейсу сприяє зменшенню кількості кроків, необхідних для пошуку роботи та подачі резюме.

У статті "Building Recommender Systems with Python" [4] підкреслюється, що інтуїтивна взаємодія з системою може значно підвищити ефективність рекомендацій.

Це особливо важливо для користувачів IT-платформ, які прагнуть швидко знайти релевантні вакансії.

Практичне значення цього дослідження полягає в тому, що інтеграція інтелектуальних систем для покращення роботи пошукових платформ в IT-сфері дозволяє досягти значного підвищення точності та релевантності рекомендацій.

Використання гібридного підходу, що поєднує колаборативне фільтрування та контентну фільтрацію, дозволить поліпшити загальний користувацький досвід.

Як показано на прикладі "Building Recommender Systems with Python" [4], розвиток рекомендаційних систем, орієнтованих на користувача, є важливим кроком у підвищенні ефективності платформ для пошуку роботи.

Таким чином, розробка та впровадження алгоритмів машинного навчання і оптимізація пошукових систем на платформах пов'язаних з пошуком роботи, дозволить значно покращити персоналізовані рекомендації для користувачів.

Це не лише знизить витрати часу на пошук роботи, але й спростить процес підбору кандидатів для роботодавців, забезпечуючи вищу ефективність та релевантність результатів пошуку.

Список використаних джерел:

1. Recommender Systems: A Primer. URL : https://arxiv.org/abs/2302.02579

2. Learning job embeddings for job recommendation in a practical setting. URL : https://arxiv.org/pdf/1905.13136

3. A hybrid job recommendation algorithm based on user behavior and job features. URL : https://www.researchgate.net/publication/276350987_A_Hybrid_Recommender_System_Based_on_User-Recommender_Interaction
4. Building Recommender Systems with Python. URL : https://www.researchgate.net/publication/365269049_Automating_the_design_of_recommender_systems_from_foundational_aspects_to_actual_developme
5. Матеріал з Вікіпедії — вільної енциклопедії. URL : https://uk.wikipedia.org/wiki/%D0%9C%D0%B0%D1%88%D0%B8%D0%BD%D0%BD%D0%B5_%D0%BD%D0%B0%D0%B2%D1%87%D0%B0%D0%BD%D0%BD%D1%8F
6. Що таке машинне навчання: як працює та де використовується. URL : https://gigacloud.ua/blog/navchannja/scho-take-mashinne-navchannja-jak-pracjue-ta-de-vikoristovuetsja
7. Що таке машинне навчання? Усе, що вам потрібно знати. URL : https://incrypted.com/ua/mashynne-navchannja/
8. Дослідження алгоритмів машинного навчання для побудови математичних моделей задач класифікації мультимодальних даних. URL : https://science.lpnu.ua/uk/jcpee/vsi-vypusky/vypusk-11-nomer-2-2021/doslidzhennya-algorytmiv-mashynnogo-navchannya-dlya

УДК 004.9

Скорін Ю.І.
к.т.н., доцент, доцент кафедри інформаційних систем
Харківський національний економічний університет імені Семена Кузнеця
Негер Д.М.
здобувач вищої освіти,
Харківський національний економічний університет імені Семена Кузнеця

ВЕБЗАСТОСУНОК ДЛЯ СТРИМІНГОВОГО ПРОСЛУХОВУВАННЯ МУЗИЧНОГО КОНТЕНТУ

У сучасному цифровому світі музичний контент став невід'ємною частиною щоденного життя. Зростаюча популярність стримінгових платформ свідчить про постійний попит на зручні та доступні сервіси для прослуховування музики.

Однак, на українському ринку ще не існує повноцінної платформи, яка б відповідала потребам місцевих слухачів та сприяла популяризації української музики і підтримці місцевих виконавців.

Попереднє оцінювання сучасного стану ринку музичних платформ показало, що існуючі рішення недостатньо уважно ставляться до української

музики та виконавців. Багато з них концентруються на іноземному контенті, залишаючи український аудіо-фонд на обраному місці.

У зв'язку з цим, актуальність розроблення вебзастосунка для стримінгового прослуховування музичного контенту полягає в заповненні цієї прогалини на ринку, створюючи платформу, яка не лише надасть можливість зручного доступу до української музики, але й активно сприятиме її популяризації та підтримці українських виконавців.

Метою даного дослідження є розроблення вебплатформи для стримінгового прослуховування музики з акцентом на український контент.

Завдання включають в себе:

- реалізацію зручного інтерфейсу для користувачів, інтеграцію з платіжною системою Stripe для оплати передплати;
- використання бази даних PostgreSQL для зберігання музичного контенту та інформації про користувачів;
- використання Supabase для управління базою даних, а також використання бібліотеки React та фреймворку Next.js для створення вебзастосунка.

Це дослідження має важливе значення у контексті дослідження та популяризації української музичної культури.

Практичне значення полягає в створенні функціонального і конкурентоспроможного продукту на ринку стримінгових платформ.

Наразі в літературі і інтернет-джерелах зазначено дефіцит інформації щодо створення вебплатформ, що спеціалізуються на українській музиці.

Однак, існують публікації про технології розробки вебзастосунків, використання платіжних систем, та реалізацію стримінгових сервісів, які стали корисними в процесі цієї роботи.

Таким чином, можна сформулювати цілі для розроблення вебзастосунку:

- підтримка українських виконавців та популяризація української музики;
- спрощення процесу реєстрації та авторизації користувачів за допомогою інтеграції зі службами Discord і GitHub, що сприяє зручності та доступності вебзастосунку;
- посилення усвідомленості користувачів про значимість музичного прослуховування та його вплив на їхнє життя, надаючи інформацію про переваги музики та її вплив на настрій та емоційний стан;
- покращення ефективності та зручності взаємодії користувачів з вебзастосунком шляхом оптимізації функцій пошуку, відтворення та зберігання в свій плейлист обрані треки;
- забезпечення можливості додавання власних треків користувачами для подальшого їхнього прослуховування без потреби завантаження, зберігаючи їх у базі даних.

Виходячи з вище поставлених цілей можна сформувати такі завдання для розроблення:

- інтеграція українського музичного контенту;

- реалізація системи реєстрації та авторизації користувачів з інтеграцією з Discord і GitHub;

- розроблення функціоналу для запису користувачів на преміум-підписку для доступу до всіх можливостей застосунку;

- створення інтерфейсу для музичного програвання, пошуку та зберігання в плейлист обраних треків;

- створення інтерфейсу для додавання власних треків користувачами та їхнього подальшого зберігання у базі даних.

У сучасному світі музики спостерігається значущий розквіт, що є результатом стрімкого розвитку музичної індустрії.

Протягом останніх кількох років стримінгові сервіси перетворилися на необхідну та навіть ключову частину повсякденного життя.

Важко переоцінити їхню популярність, оскільки вони не лише задовольняють музичні пристрасті користувачів, а й стали невід'ємною складовою їхнього рутинного щодення.

З урахуванням зазначеного розквіту в сучасній музичній індустрії та загальної популярності стримінгових сервісів, виникає важлива задача розроблення вебзастосунка.

У поточний період існують конкретні труднощі та виклики, пов'язані з функціональністю та зручністю існуючих музичних вебзастосунків для стрімінгу музики.

Частина цих сервісів не завжди повністю відповідає потребам користувачів у зручному та ефективному використанні.

Такі недоліки у функціоналі та зручності можуть ускладнювати користування музичними платформами та обмежувати задоволення від їх використання.

Отже, враховуючи вищезазначені виклики та недоліки наявних музичних вебзастосунків, стає актуальною необхідність розробки нового вебінструменту.

Ця необхідність виникає із прагнення поліпшити користувацький досвід та відповісти на потреби і очікування сучасного споживача.

Створення нового інструменту є важливим завданням, оскільки воно має на меті виправити та усунути недоліки існуючих рішень та надати користувачам нові можливості та враження у сфері стримінгового прослуховування музики.

Практичне значення цієї роботи полягає в створенні ефективного та зручного вебзастосунку для стримінгового прослуховування музики.

Заплановано розробити застосунок, використовуючи передові технології веброзробки, такі як Next 13.4, React, Stripe, Supabase, PostgreSQL та Tailwind [1–6].

React – це JavaScript бібліотека для створення інтерфейсів користувача. У проєкті React використовується для реалізації компонентного підходу та створення інтерактивного та ефективного інтерфейсу вебзастосунка.

Next.js є фреймворком для розробки вебзастосунків на базі React. В проєкті використовується Next 13.4 для забезпечення серверного рендерингу,

оптимізації завантаження сторінок та іншими перевагами, які пропонує цей фреймворк [1].

Використання TypeScript із його статичною типізацією сприяє виявленню та виправленню помилок на етапі розробки, а також поліпшує читабельність та розширюваність коду [3].

Stripe використовуватиметься для оброблення платежів, Supabase та PostgreSQL – для зберігання даних, а Tailwind – для стилізації вебінтерфейсу [3; 5; 6].

Процес розроблення зосереджений на впровадженні автоматизації та вдосконаленні користувацького досвіду.

Ключові переваги вебзастосунка будуть включати швидку та зручну можливість вибору музики, підвищену продуктивність та оперативне обслуговування користувачів.

Список використаних джерел:

1. Next.js Documentation URL : https://nextjs.org/docs
2. React Documentation URL : https://reactjs.org/docs/getting-started.html
3. Stripe Documentation URL : https://stripe.com/docs
4. Supabase Documentation URL : https://supabase.io/docs
5. PostgreSQL Documentation URL : https://www.postgresql.org/docs
6. Tailwind CSS Documentation URL : https://tailwindcss.com/docs

УДК 004.9

Скорін Ю.І.
к.т.н., доцент, доцент кафедри інформаційних систем
Харківський національний економічний університет імені Семена Кузнеця
Пирог Д.О.
здобувач вищої освіти,
Харківський національний економічний університет імені Семена Кузнеця

МОДУЛЬ ОБЛІКУ РЕЄСТРАЦІЇ ПАЦІЄНТІВ ПОЛІКЛІНІКИ НА БАЗІ ВЕБТЕХНОЛОГІЙ

Сучасна медична сфера зазнає сталого розвитку та постійної необхідності вдосконалення систем управління медичними даними.

Цифрова трансформація є важливою ознакою сьогодення.

Більшість як приватних, так і державних установ починають користуватися системами електронного обігу документів.

На жаль, деякі галузі діяльності не мають таких важливих технологій. Саме система охорони здоров’я є однією з таких сфер.

Згідно з результатами проведеного аналізу можемо дійти висновку, що кількість медичних кадрів є недостатньою для гідного забезпечення потреб населення у медичному обслуговуванні [6].

Отож, на вказані результати впливають різноманітні чинники, наприклад рівень технічного забезпечення медичних закладів, а це, в свою чергу може значно ускладнювати роботу лікаря і збільшувати робоче навантаження на нього.

Також, маємо досить велику кількість проблем, з якими доводиться стикатися і саме пацієнтам.

Розглянемо ситуацію та спробуємо з'ясувати с чим це пов'язано. Річ у тому, що щоб отримати власні медичні дані пацієнт змушений щоразу знову звертатися до лікаря, а це, в свою чергу, викликає нескінчені черги, що суттєво гальмують процеси отримання такої необхідної медичної допомоги.

Виходом з цієї складної ситуації може бути розроблення модуля обліку реєстрації пацієнтів поліклініки на базі вебтехнологій.

Сьогодні саме клієнт-серверні застосунки набувають досить масового поширення. Такі застосунки все частіше використовуються у більшості галузей народного господарства і, як результат, значно спрощують та оптимізують широку номенклатуру видів робіт.

Але ж, розроблення таких застосунків виявляється досить важким та високовартісним, що викликає потребу у значної кількості і кваліфікації розробників, проте створений програмний продукт у повній мірі виправдає як кошти так і ресурси, що були витрачені на його розроблення.

Досить ключовим аспектом є процес оптимізації процедури саме реєстрації пацієнтів, стратегічну важливим для надання надійної та оперативної медичної допомоги, важко переоцінити.

Це дозволяє сформулювати в якості головного завдання - саме розроблення клієнт-серверного застосунку для здійснення обліку пацієнтів у медичному закладі. А це, в свою чергу значно допоможе вирішити більшу частину з проблем, які були наведені раніш.

Основними можливостями запропонованого застосунку можна виділити такі:

- можливість лікаря здійснювати контроль за ходом лікування хворого, причому протягом всього лікування, тобто від першого звернення до лікаря і аж до завершального візиту;
- можливість лікаря призначати необхідні, як діагностичні, так і лікувальні заходи;
- можливість лікаря зручно складати повний, але зрозумілий перелік призначень.

При цьому пацієнт отримує можливість:

- дистанційно, що є дуже важливим, записатись на прийом до потрібного йому медичного працівника, тим самим оминути можливі черги;
- дистанційно отримати доступ до своєї медичної картки, тобто своїх медичних даних;

- дистанційно отримати доступ до повного списку фармацевтичних засобів, які були призначені лікарем, це стосується, в першу чергу, людей досить похилого віку;

- суттєво спростити процес комунікації між пацієнтом та лікарем;

- забезпечити можливість переходу системи охорони здоров'я до електронного документообігу [6].

Саме цей напрямок обумовлений необхідністю покращення обслуговування пацієнтів та оптимізації робочих процесів для медичного персоналу [1].

Упровадження передових технологій у реєстраційні процедури поліклініки має велике значення для оптимізації обробки та зберігання обсягових медичних даних пацієнтів.

Нещодавно працівникам медичних закладів доводилося опиратися на сотні папок з історіями захворювань пацієнтів, однак з появою вебтехнологій ситуація змінилася радикально.

Тепер ми маємо можливість легко та ефективно керувати цими даними. Цей модуль не лише забезпечує потужний інструмент для зберігання медичних інформацій, але також перетворює важкодоступні файли в безпечну та доступну електронну форму.

Технологічна платформа для реєстрації пацієнтів та управління їхньою медичною історією у вебсередовищі забезпечує лікарям та медичному персоналу ефективний та зручний доступ до даних пацієнтів.

Система реєстрації пацієнтів дозволяє вести докладну медичну історію кожного пацієнта, включаючи збереження важливих даних про захворювання, прийоми до лікарів та відстеження поточного стану пацієнта, і надає широкий спектр переваг у сучасному світі.

Серед них варто відзначити оптимізацію робочих процесів, можливість індивідуального підходу до обслуговування кожного пацієнта, зручний і точний доступ до необхідної інформації, а головне - швидкий доступ, що стає важливим фактором для ефективного виконання завдань.

Таким чином, однією з найважливіших та відповідальних частин організації медичного закладу є належна система реєстрації пацієнтів, спрямована на безперебійний, швидкий та точний облік медичних даних, управління їхньою історією та надання високоякісних медичних послуг.

У процесі виконання завдань щодо розроблення вебдодатка, використовуються передові вебтехнології, зокрема:

- React.js;
- HTML;
- CSS;
- JavaScript;
- Redux для фронтенду:
- Node.js;
- MySQL.

Ці інструменти є одними з найпопулярніших у світі веброзробка, надаючи можливість створення високопродуктивних та масштабованих вебдодатків.

Так, наприклад, React.js - це потужний фреймворк для створення інтерфейсів користувача, який дозволяє розробникам побудувати складні односторінкові додатки з великою швидкодією та ефективністю.

В свою чергу, Redux використовується для ефективного керування станом додатка, що робить процес розроблення більш організованим та легким для розширення.

У бекенді використовується Node.js яка є – потужною платформою для розроблення високопродуктивних та масштабованих вебдодатків.

MySQL виступає у ролі системи управління базами даних, забезпечуючи зберігання та оптимізацію обробки даних.

Також буде використаний інструмент контролю версій Git для управління кодом та роботи з репозиторієм. Він дозволить ефективно контролювати версії коду та забезпечить надійність у процесі розробки [1–3].

Практичне значення роботи полягає в створенні системи, що забезпечить швидкий доступ до медичних даних, поліпшить обробку інформації та забезпечить ефективність роботи медичного персоналу.

Ця система покликана підвищити якість медичних послуг через вчасне виявлення патологій та забезпечення точного обліку медичних даних кожного пацієнта.

Список використаних джерел:

1. Створення, реєстрація та редагування пацієнта на прикладі системи "eHealth". URL : https://info.elife.com.ua/pages/viewpage.ction?pageId=17465695

2. React – JavaScript-бібліотека для створення інтерфейсів користувача. URL : https://uk.legacy.reactjs.org

3. Розробка додатків на Node.js URL : https://kitapp.pro/uk/rozrobka-dodatkiv-na-node-js/

4. Діденко О. К. Застосування методу керованої поведінки розробки для автоматизації тестування вебзастосунків // О. К. Діденко, Д. Ю. Голубничий // Матеріали Міжнародної науково-практичної конференції молодих учених, аспірантів та студентів “Інформаційні технології в сучасному світі: дослідження молодих вчених” 22 – 23 лютого 2024 р. – Харків, 2024. – С.3.

5. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання / Нац. стандарт України. – Київ : ДП «УкрНДНЦ», 2016. – 18 с.

6. Клієнт-серверний застосунок обліку пацієнтів у лікарні. URL : https://ela.kpi.ua/server/api/core/bitstreams/f5577b2a-6b72-42cc-a38e-6196d8735e3c/content

УДК 004.9

Скорін Ю.І.
к.т.н., доцент, доцент кафедри інформаційних систем
Харківський національний економічний університет імені Семена Кузнеця
Рудь І.А.
здобувач вищої освіти,
Харківський національний економічний університет імені Семена Кузнеця

ЧАТ-БОТ ДЛЯ СТРИМІНГОВОЇ ПЛАТФОРМИ TWITCH

У сучасному світі стрімінгові платформи відіграють важливу роль у сфері розваг та комунікацій.

Однією з найбільш популярних платформ є Twitch, яка надає можливість користувачам транслювати свій контент у режимі реального часу, взаємодіючи з аудиторією через чат.

Враховуючи стрімке зростання популярності таких платформ, ефективне адміністрування стрімів стає все більш актуальним завданням.

Адміністрування стрімінгових каналів на Twitch включає в себе безліч рутинних завдань, таких як:

- модерація чату;
- управління підписниками;
- відповіді на часті запитання та інші дії, які потребують значних зусиль та часу з боку стрімерів.

З метою автоматизації цих процесів і полегшення роботи стрімерів, доцільно використовувати чат-ботів.

Розроблення чат-боту для адміністрування стрімінгової платформи Twitch дозволяє вирішити низку важливих завдань. Чат-бот може автоматично виконувати модерацію, надавати інформацію глядачам, керувати інтерактивними функціями стріму та виконувати багато інших корисних функцій.

Це дозволяє стрімерам зосередитись на створенні контенту та взаємодії зі своєю аудиторією, залишаючи рутинні завдання на чат-бота.

Тому є дуже важливим розробити такий чат-бот, який не лише автоматизує рутинні завдання, але й покращує загальний досвід як для стрімерів, так і для їх глядачів.

Був проведений аналіз предметної області, визначено функціональні та нефункціональні вимоги до системи, здійснено проектування та розроблення чат-боту, а також проведено його тестування і розгортання.

Таким чином, основною метою є створення ефективного інструменту для адміністрування стрімінгової платформи Twitch, який сприятиме підвищенню якості та зручності стрімів, що у свою чергу підвищить задоволеність користувачів платформи

Створення та розгортання бота для чату на платформі Twitch настійно рекомендується і є критично необхідним у контексті вдосконалення всього

користувацького досвіду та підвищення ступеня інтерактивності в рамках цієї віртуальної спільноти.

Відмінна риса Twitch як провідної платформи для стримінгу в реальному часі полягає не тільки в потоковому передаванні ігрового контенту, а й у формуванні інтенсивних обговорень, живої взаємодії між глядачами та стримерами, а також у створенні спільнот зі спільними інтересами [1–2].

Перше, що робить бот, це забезпечує модерацію, що дає змогу підтримувати порядок і запобігати порушенням у чаті.

Вони можуть автоматично видаляти небажані повідомлення, блокувати спам і стежити за дотриманням правил спільноти.

Це значно полегшує завдання стримеру та його модераторам, дозволяючи їм зосередитися на контенті та взаємодії з аудиторією.

Крім того, боти сприяють інтерактивності чату.

Вони можуть надавати інформацію про стрімера, організовувати голосування, запускати різні ігри та розіграші призів, що робить перегляд стріму захопливим і різноманітним для глядачів.

Основні переваги використання чат-боту для адміністрування платформи Twitch:

- спрощення модерації: чат-бот дозволяє автоматично виявляти та видаляти неприйнятний контент, запобігати спаму, управління заборонами користувачів. Це спрощує роботу модераторів та підвищує якість модерації;
- підвищення взаємодії з користувачами: бот може відповідати на часті запитання, організовувати голосування, проводити інтерактивні ігри та заходи, що підвищує залученість аудиторії та покращує користувацький досвід;
- автоматизація інформаційних сповіщень: чат-бот може автоматично надсилати сповіщення про початок стріму, нагадування про важливі події, тим самим спрощуючи роботу модераторів та стрімера, які можуть зосередитись на інших задачах замість постійних нагадувань у чаті.

Наприклад, бот чату на платформі Twitch може бути використаний для створення інтерактивних ігор з аудиторією.

Уявімо, що бот пропонує глядачам брати участь у грі "Вгадай число", де глядачі можуть робити припущення про загадане число в певному діапазоні.

Бот збирає пропозиції глядачів і повідомляє результати.

Ця гра може бути активована протягом стріму. Щойно стрімер оголошує початок гри, глядачі починають надсилати свої числа в чат.

Бот відстежує числа і наприкінці часового відрізка, зазначеного стрімером, оголошує переможця, тобто, того глядача, чий варіант був найближчий до загаданого числа.

Переможець може отримати якийсь приз або особливу згадку від стрімера.

Цей приклад демонструє, як бот може залучати глядачів до інтерактивних моментів стріму, роблячи перегляд більш захопливим і захопливим.

Такі ігри не тільки розважають аудиторію, а й зміцнюють взаємодію між стрімером і глядачами, стимулюючи їхню активну участь у трансляції.

Боти також допомагають в автоматизації певних завдань, наприклад, інформуванні про правила чату, розклад стрімів, посилання на соціальні мережі стримера та інші корисні ресурси.

Це скорочує час, що витрачається на повторювані дії та забезпечує більш гладку і зручну взаємодію зі спільнотою.

Таким чином, створення бота для чату Twitch є необхідним кроком для підтримання порядку, стимулювання інтерактивності та поліпшення загального досвіду користувачів на цій платформі.

Java є привабливим вибором для розробки бота для чату Twitch з кількох причин.

По-перше, Java має високу переносимість, що дає змогу запускати програми на різних платформах без змін коду. Це важливо для забезпечення роботи бота на різних операційних системах.

Крім того, Java пропонує великий набір бібліотек та інструментів, що сприяють зручному розробленню та підтримці застосунків, а також забезпечує високу продуктивність і надійність, що істотно для безперебійної роботи бота під час стрімів і спілкування в чаті Twitch [1–9].

Практичне значення даної роботи полягає у створенні бота для полегшення роботи з аудиторією, автомодерації, автоматизації сповіщень і спрощення роботи стрімера з чатом.

Список використаних джерел:

1. Twitch Chat & Chatbots. URL : https://dev.twitch.tv/docs/irc/
2. Twitch API Reference URL : https://dev.twitch.tv/docs/api/reference/
3. Learn Java URL : https://dev.java/learn/
4. Java Tutorial URL : https://www.w3schools.com/java/default.asp
5. Next.js Documentation URL : https://nextjs.org/docs
6. React Documentation URL : https://reactjs.org/docs/getting-started.html
7. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання / Нац. стандарт України. – Київ : ДП «УкрНДНЦ», 2016. – 18 с.
8. Лунтовський А. Проєктування та дослідження комп'ютерних мереж / А. Лунтовський, І. Мельник. – Львів: Університет "Україна", 2020. – 362 с.
9. Алгоритми та структури даних : робоча програма для студентів спеціальності 122 "Комп'ютерні науки та інформаційні технології" першого (бакалаврського) рівня [Електронний ресурс] / уклад. О. В. Щербаков, Ю. Е. Парфьонов, В. М. Федорченко. – Харків : ХНЕУ ім. С. Кузнеця, 2017. – 58 с.

УДК 004.9

Скорін Ю.І.
к.т.н., доцент, доцент кафедри інформаційних систем
Харківський національний економічний університет імені Семена Кузнеця
Самилкін К.Р.
здобувач вищої освіти,
Харківський національний економічний університет імені Семена Кузнеця

ВЕБЗАСТОСУНОК ДЛЯ АДМІНІСТРУВАННЯ СПОРТИВНОГО ЦЕНТРУ

В сучасному світі, постійних розробок та нових технологій, постійних змін у вимогах споживачів треба раціонально оцінити можливості та зробити все можливе для реалізації цієї цілі.

Так само була поставлена ціль розробити вебзастосунок для придбання абонементів та послуг спортивного центру.

Головною проблемою цього бізнесу було і залишається те що в нього по цей час немає свого вебзастосунка чи сайту.

Наслідками цих проблем для клієнтів може бути:

- складність запису на заняття: клієнти змушені дзвонити або приходити особисто, щоб записатися на заняття, це може бути незручно, особливо для людей з щільним графіком;
- відсутність актуальної інформації: клієнти не завжди можуть отримати актуальну інформацію про розклад занять, вартість послуг, зміни в роботі спортивного центру;
- неможливість онлайн-оплати: клієнти змушені оплачувати послуги готівкою або через термінал, це може бути незручно, а також небезпечно в умовах, наприклад пандемії.

Для організації, у цьому випадку можуть бути ось такі наслідки:

- втрата клієнтів: спортивний центр може втрачати клієнтів, які шукають більш зручні способи запису на заняття та отримання інформації;
- зниження ефективності роботи: персонал спортивного центру, змушений витрачати час на прийом телефонних дзвінків та запис клієнтів;
- неможливість масштабування: спортивному центру буде складно масштабувати діяльність без вебзастосунка.

Метою досліджень буде внесення новаторських рішень у структуру дизайну інтерфейсу користувача та розроблення інтуїтивно зрозумілого застосунку.

Цільовою аудиторією застосунку є дуже великий спектр клієнтів, починаючи від звичайних любителів спорту, які прагнуть лише тримати себе в тонусі до справжніх спортсменів які постійно женуться за новими рекордами та бажають показати найкращий результат.

Застосунок буде розроблений з урахуванням всіх цільових груп, гарантуючи кожному користувачеві зручний та зрозумілий інтерфейс.

Розроблення вебзастосунка буде включати в себе комплексний підхід, в складі якого буде аналіз вимог, конкурентоспроможність на ринку, проєктування та розроблення користувацького інтерфейсу.

Важливим пунктом буде створення системи для онлайн-замовлень послуг або купівлі абонемента на тренування. Вже після цього всього застосунок буде наповнений контентом та перейде у стадію тестування.

Дослідження є досить актуальним, оскільки воно відповідає потребам сучасних спортивних центрів, реалізуючи одну із основних їх проблем.

Результатом розроблення стане сучасний вебзастосунок, що зможе вплинути на розвиток та масштабування спортивного центру.

У сучасному світі, де швидкість, зручність та доступність стали важливими аспектами для бізнесу будь-якого формату, спортивні центри також активно впроваджують технології для покращення своєї діяльності та забезпечення зручності для клієнтів.

Розроблення та впровадження онлайн-системи оплати та адміністрування абонементів та квитків через вебзастосунок стало кроком до нової ери управління спортивним бізнесом.

Ця інноваційна платформа дозволяє клієнтам здійснювати оплату за послуги спортивного центру онлайн, безпосередньо через їхній веббраузер або мобільний застосунок [1].

Онлайн-система оплати та адміністрування абонементів та квитків відкриває нові можливості для спортивного центру у взаємодії з клієнтами.

Вона спрощує процеси оплати та адміністрування, забезпечуючи швидкий та зручний доступ до послуг, що стає ключовим фактором у залученні та утриманні клієнтів.

Цей застосунок є не просто інструментом для спрощення операцій реєстрування нових клієнтів або оновлення вже існуючих профілів.

Він є стратегічним кроком до цифрової трансформації спортивного бізнесу, що сприяє підвищенню конкурентоспроможності спортивних центрів, покращенню взаємодії з клієнтами та забезпеченню високого рівня обслуговування.

Розроблення онлайн-системи оплати та адміністрування абонементів та квитків для спортивного центру – це не просто нововведення в управлінні, це новий стандарт в обслуговуванні клієнтів та управлінні спортивними послугами.

Ця система дозволяє клієнтам отримати доступ до послуг спортивного центру в будь-який зручний для них час, відбувається це онлайн через вебсайт чи мобільний додаток.

Переваги цього рішення виявляються вже на початковому етапі взаємодії з клієнтом. Користувачі можуть ознайомитися з послугами, розкладом тренувань, обрати та оплатити абонемент або квиток на потрібну послугу у всьому зручному для них режимі.

Це створює безперервний потік доступу до послуг спортивного центру, що сприяє збільшенню задоволення клієнтів та їх лояльності.

Додатковою перевагою системи є її здатність забезпечити ефективне адміністрування.

Менеджери спортивного центру отримують доступ до зручної адміністративної панелі, де вони можуть легко відстежувати оплати, керувати абонементами, а також аналізувати дані про використання послуг.

Це дозволяє ефективно планувати роботу спортивного центру, реагувати на попит клієнтів та пропонувати їм більш персоналізований підхід.

Технологічна складність розробки такої системи вимагає використання передових інструментів.

Laravel і Vue.js, в якості основних фреймворків, забезпечують стабільну роботу системи та забезпечують швидкість та надійність взаємодії з користувачами.

Використання передових вебтехнологій, таких як Laravel і Vue.js, було обрано для створення цієї системи. Laravel, як масштабований та прогресивний фреймворк, забезпечує надійну та ефективну роботу з базою даних, а Vue.js надає зручний та інтуїтивно зрозумілий інтерфейс для користувачів [1–3].

В цілому, впровадження онлайн-системи оплати та адміністрування абонементів та квитків в спортивному центрі є кроком до майбутнього.

Це не лише зручний інструмент для клієнтів, але й стратегічна інвестиція в розвиток бізнесу, що підвищує його конкурентоспроможність та впливає на ріст лояльності клієнтів.

Список використаних джерел:

1. Автоматизація бізнес-процесів – Softex. URL : https://www.softex.if.ua/services/proektne-vprovadzhennya/avtomatizatsiya-biznes-protsesiv/

2. Laravel – The PHP Framework For Web Artisans. URL : https://laravel.com/

3. TechCrunch | Startup and Technology News. URL : https://techcrunch.com

4. The PHP Framework for Web Artisans. URL : https://www.binarcode.com/services/laravel-development

5. For Web Artisans. URL : https://entwickler.de/php/for-web-artisans

6. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання / Нац. стандарт України. – Київ : ДП «УкрНДНЦ», 2016. – 18 с.

7. Золотухіна О.А. Якість та тестування інформаційних систем: навч. посіб. / О.А. Золотухіна. – Київ: ННІІТ ДУТ, 2020. – 128 с.

8. Моделюва́ння бі́знес-проце́сів. URL : https://uk.wikipedia.org/wiki/Моделювання_бізнес-процесів

9. Основи програмування з HTML, CSS та JavaScript. URL : https://prometheus.org.ua/course/course-v1:DukeUniversity+PFW101+2023_T3

10. Організація баз даних: інформаційна система, СКБД, SQL/NoSQL та мотивація. URL : https://www.youtube.com/watch?v=MRLzJDOl0fk

УДК 004.9

УДК 004:005

Скорін Ю.І.
к.т.н., доцент, доцент кафедри інформаційних систем
Харківський національний економічний університет імені Семена Кузнеця
Сухоруков В.С.
здобувач вищої освіти,
Харківський національний економічний університет імені Семена Кузнеця

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ ПІДПРИЄМСТВА ШЛЯХОМ ВПРОВАДЖЕННЯ ГНУЧКИХ МЕТОДІВ УПРАВЛІННЯ ПРОЄКТАМИ

У сучасному світі, де технології швидко розвиваються, управління проєктами стає все більш складним завданням. Традиційні методи управління проєктами часто не можуть ефективно впоратися з цими викликами, що призводить до затримок, перевищення бюджету та незадовільних результатів.

В цьому контексті, гнучкі методи управління проєктами, такі як Scrum, Kanban та Agile, стають все більш популярними, оскільки вони дозволяють командам краще адаптуватися до змін та ефективно реагувати на проблеми [1; 4].

Однак, незважаючи на очевидні переваги гнучких методів, багато підприємств все ще використовують традиційні методи управління проєктами, які можуть бути менш ефективними в сучасних умовах.

Тому головною метою є дослідження можливостей впровадження гнучких методів управління проєктами на підприємствах, аналіз їхньої ефективності та виявлення перешкод, які можуть виникнути під час цього процесу.

Для досягнення цієї мети необхідно вирішити такі завдання [2; 5]:

- ознайомитися з основними гнучкими методами управління проєктами, їхніми принципами та особливостями;
- дослідити досвід впровадження цих методів на підприємствах;
- провести аналіз ефективності використання гнучких методів у порівнянні з традиційними.

Таким чином, об’єктом дослідження є процес впровадження гнучких методів управління проєктами на підприємствах та їх вплив на ефективність роботи підприємства.

Важливим аспектом впровадження гнучких методів управління проєктами є розуміння їхньої сутності та принципів роботи.

Гнучкі методи управління проєктами базуються на ітеративному підході, коли проєкт розбивається на невеликі частини, які розробляються паралельно.

Це дозволяє швидко вносити зміни в проєкт і адаптуватися до змін у бізнес-середовищі [3].

Однак, впровадження гнучких методів управління проєктами може стикнутися з рядом перешкод.

Наприклад, може бути важко знайти кваліфікованих спеціалістів, які знають, як працювати з цими методами.

Також може бути важко змінити застарілі підходи до управління проєктами, які вже були використані в культурі підприємства раніше.

Тому, одним з основних завдань цієї роботи є дослідження перешкод, які можуть виникнути під час впровадження гнучких методів управління проєктами, та розробка рекомендацій щодо їх подолання.

Крім того, важливо провести аналіз ефективності використання гнучких методів у порівнянні з традиційними.

Це дозволить визначити, чи дійсно гнучкі методи дозволяють підвищити ефективність роботи підприємства, та які саме переваги вони дають.

Отже, у результаті можна сподіватися отримати вичерпну інформацію про можливості впровадження гнучких методів управління проєктами на підприємствах.

Це включає в себе розуміння різних типів гнучких методів, таких як Agile, Scrum, Kanban та інших, а також їх застосування в різних галузях промисловості [1; 3].

Необхідно дослідити їхні переваги, такі як підвищення продуктивності, покращення комунікації в команді, здатність швидко реагувати на зміни та інше.

Але також важливо зрозуміти їхні недоліки, наприклад, можливі проблеми з плануванням, необхідність високого рівня самоорганізації команди, ризик вигорання та інше.

Наприклад, основні принципи гнучкого управління проєктами викладені в Маніфесті Agile, який робить акцент на людях та взаємодії, а не на процесах та інструментах.

Гнучкі методи управління проєктами передбачають використання гнучких методологій та впровадження спільних практик у командах.

Так, Agile надає пріоритет співпраці з клієнтом над переговорами щодо контракту, гарантуючи, що кінцевий продукт відповідає потребам користувача. Іншим ключовим принципом є реагування на зміни за фіксованим планом, що дозволяє командам швидко адаптуватися до нової інформації або мінливих вимог.

Agile також надає перевагу робочому програмному забезпеченню, а не вичерпній документації, зосереджуючись на наданні функціональних продуктів на ранніх стадіях і часто.

Регулярна рефлексія та коригування є невід’ємною частиною, команди аналізують свою роботу та процеси в кінці кожного спринту, щоб визначити сфери для вдосконалення.

Цей безперервний цикл зворотного зв'язку сприяє створенню середовища постійного зростання та вдосконалення.

У сукупності ці принципи створюють гнучку та оперативну структуру, яка покращує результати проєкту та динаміку команди.

Практична значущість даного дослідження полягає в можливості підвищення ефективності роботи підприємства за допомогою впровадження гнучких методів управління проєктами.

Результати цього дослідження можуть бути використані підприємствами, які шукають способи оптимізації своїх процесів управління проєктами.

Крім того, дане дослідження може слугувати посібником для менеджерів проєктів, які хочуть запровадити гнучкі методи у своїй практиці. Воно надає детальний огляд гнучких методів, їхніх переваг та недоліків, а також рекомендації щодо їх впровадження.

Нарешті, результати цього дослідження можуть бути використані в академічних цілях для подальших досліджень у цій області.

Це може сприяти розвитку наукових знань про гнучкі методи управління проєктами та їх вплив на ефективність роботи підприємства.

Це дослідження буде корисним для підприємств, які прагнуть підвищити ефективність своєї роботи за допомогою сучасних методів управління проєктами.

Це може допомогти їм краще розуміти, як вони можуть використовувати ці методи для досягнення своїх цілей, покращення процесів та забезпечення високої якості своєї роботи.

Список використаних джерел:

1. Сазерленд Д. Scrum. Революційний метод управління проєктами. / Д. Сазерленд, 2014. – 329 с. URL: https://balka-book.com/ua/razrabotka_programnogo_obespecheniya-366/scrum_revolyutsionnyiy_metod_upravleniya_proektami-34833
2. Грін Д. Цінності, принципи, методології / Д. Грін, Е. Стіллман, 2018. – 240 с. URL: https://balka-book.com/ua/upravlenie_it_proektami-364/postigaya_agile_tsennosti_printsipyi_metodologii-40664
3. Ries M. Agile Project Management: A Complete Beginner’s Guide To Agile Project Management / M. Ries, 2018. URL: https://www.medimops.de/marcus-ries-agile-project-management-a-complete-beginner-s-guide-to-agile-project-management-taschenbuch-M01539877302.html
4. Anderson David J., Kanban: Successful Evolutionary Change for Your Technology Business / David J. Anderson, 2010. URL: https://kanbanbooks.com/kanban-successful-evolutionary-change-for-your-technology-business
5. Kerzner H., Project Management: A Systems Approach to Planning, Scheduling, and Controlling / H. Kerzner, 2017. URL: https://books.google.de/books/about/Project_Management.html?id=B1u9e0Dgx80C&redir_esc=y

УДК 004.9

Скорін Ю.І.
к.т.н., доцент, доцент кафедри інформаційних систем
Харківський національний економічний університет імені Семена Кузнеця
Терентьєв О.О.
здобувач вищої освіти,
Харківський національний економічний університет імені Семена Кузнеця

КАТЕГОРИЗАЦІЯ РЕЗУЛЬТАТІВ АВТОМАТИЧНОГО ТЕСТУВАННЯ З ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ МАШИННОГО НАВЧАННЯ

Сучасним стандартом в розробці програмних продуктів стає процес випуску нових версій з високою частотою [2].

Проміжок між версіями може складати місяць, тиждень, а деколи й один день. Основною мотивацією для таких частих релізів є високе конкурентне середовище.

Комерційному підприємству треба випереджати конкурентів у задовільнені нових запитів від клієнтів. Запізнення може коштувати відтоком клієнтів та наступним за цим зниженням прибутків.

З іншого боку цього процесу знаходиться якість програмного забезпечення.

Неякісний продукт з великою кількістю помилок зменшить кількість клієнтів ще швидше ніж відсутність нового функціоналу.

Існують різноманітні схеми організації перевірки якості програмних продуктів, але кінцевим агентом, котрий приймає рішення стосовно придатності програми виконувати описаний новий функціонал на прийнятному рівні є людина.

Цю роль можуть виконувати розробники, менеджери проєктів, або окремі спеціалісти. Для подальшого розгляду будемо називати людину, котра виконує цю роль тестувальником.

З ростом розміру проєкту потреба в тестувальниках зростає. А також зростає кількість операцій, котрі вони повинні виконати аби дізнатись наявний стан відносно відповідності продукту заявленій якості.

А з ростом частоти випуску, робота по перевірці стає монотонною і це збільшує кількість помилок самих тестувальників.

Тому починаючи з певного розміру проєкту, кількості часу, необхідного на перевірку однієї версії продукту та частоти випусків, компанії починають автоматизування процесу тестування.

Що дуже сильно скорочує час котрий тестувальники витрачають на перевірки [2].

На жаль програмне забезпечення не рідка теж має помилки, котрі приводять до невірного визначення придатності системи.

Також робота систем в тестовому середовищі пов’язана з певними неполадками в фізичному обладнані, котре неможливо або дуже коштовно передбачити в автоматичних тестах.

Це призводить до ситуацій, коли знову тільки тестувальник, переглянувши результати тестів, що завершились з помилками, зможе визначити чи це реальний дефект продукту, чи це проблема з автоматичним тестом, або це проблема тестового середовища.

З ростом функціональності продукту, росте і кількість автоматичних тестів, а з ними й кількість помилок, котрі треба перевіряти тестувальникам.

Одним з варіантів розв'язання цієї проблеми може бути автоматичне визначення джерела проблеми.

Тобто по наявним записам сценарію тестування та відповідям системи й історії попередніх тестувань ми маємо автоматично визначити причину помилки.

Для вирішення такого класу проблем останнім часом набули популярності методи машинного навчання, котрі при певній кількості вхідних даних надають досить високу точність результатів [2].

Хоча методи для вирішення такого класу задач існують достатньо давно, лише в останні роки вони почали демонструвати прийнятну якість [2–4].

Основними факторами стали: загальний розвиток методів машинного навчання, збільшення об’єму даних для навчання, а також збільшення обчислюваної потужності сучасної техніки.

Існує дві основні категорії тестування програмного забезпечення: ручне та автоматизоване.

Ручне тестування займає багато часу, трудомісткість, а зі складним програмним забезпеченням воно також може бути дорогим, якщо ви використовуєте його виключно.

Автоматизоване тестування оптимізує процеси, скорочує час, необхідний для тестування, і усуває неефективність, наприклад розробники програмного забезпечення витрачають виснажливі години на тестування функціональності програмного забезпечення [1].

Автоматизоване тестування це процес використання програмних інструментів, які запускають нещодавно розроблене програмне забезпечення або оновлення через низку тестів для виявлення потенційних помилок кодування, вузьких місць та інших перешкод продуктивності.

Засоби автоматизації тестування програмного забезпечення виконують такі функції [1]:

- впровадження та виконання тестів;
- аналіз результатів;
- порівняння результатів з очікуваними результатами;
- формування звіту про продуктивність програмного забезпечення розробки.

Автоматизовані тести можуть допомогти швидше виявляти збої з меншим ризиком людської помилки. Крім того, їх легше запускати кілька разів для кожної зміни або до досягнення бажаних результатів.

Автоматизація також прискорює процес виведення програмного забезпечення на ринок. Автоматизація дозволяє проводити ретельне тестування в певних областях, щоб ви могли вирішити загальні проблеми, перш ніж переходити до наступного етапу [1].

Піраміда автоматизації тестування допомагає зрозуміти, як часто потрібно виконувати кожен тип тесту.

Піраміда автоматизації тестування поділяє тестування на чотири рівні. Нижній шар представляє тести, які ви повинні виконувати найчастіше.

Рівні стають меншими, чим ближче вони до вершини піраміди, тобто тести, які вам слід виконувати рідше [1].

Ось типи тестів, які слід виконати за пірамідою автоматизації тестування, від найбільшого до найменшого [1]:

- модульні тести;
- інтеграційні тести;
- тести API;
- тести інтерфейсу користувача.

Таким чином мета полягає в дослідженні застосування методів машинного навчання для категоризації результатів автоматичного тестування.

Необхідно провести аналіз наявних рішень. Визначити критерії вибору.

На прикладі обраного рішення провести моделювання, та визначити ефективність зазначеної методики.

Список використаних джерел:

1. Що таке автоматизація тестування? URL: https://www.zaptest.com/uk/%D1%89%D0%BE%D1%82%D0%B0%D0%BA%D0%B5%D0%B0%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F%D1%82%D0%B5%D1%81%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%D0%B1%D0%B5%D0%B7
2. Arnon Axelrod. Complete Guide to Test Automation: Techniques, Practices, and Patterns for Building and Maintaining Effective Software Projects. / Axelrod // Arnon New York, NY, USA: Apress, 2018. – 558 с.
3. Ian Goodfellow. Deep Learning. / Goodfellow Ian, Bengio Yoshua, Courville Aaron // Cambridge, MA, USA: The MIT Press, 2016. – 800 с.
4. Машинне навчання простими словами. URL: http://www.mmf.lnu.edu.ua/ar/1739
5. Розробка програмного забезпечення для розв'язання задачі категоризації текстових документів. URL: https://repository.kpi.kharkov.ua/-server/api/core/bitstreams/d19690b8-9fb7-41bf-ac34-e7016d1fa62b/content

УДК 004.9

Скорін Ю.І.
к.т.н., доцент, доцент кафедри інформаційних систем
Харківський національний економічний університет імені Семена Кузнеця
Федосенко В.О.
здобувач вищої освіти,
Харківський національний економічний університет імені Семена Кузнеця

ВПРОВАДЖЕННЯ ТАКСОНОМІЙ У СФЕРІ ФІНАНСОВИХ ТЕХНОЛОГІЙ

В сучасному світі фінансові технології швидко розвиваються, відображаючи постійні зміни в економіці.

Однак для підтримки стійкого розвитку фінансових установ і підприємств важливо впроваджувати таксономії, які надають основи і принципи для систематизації та розуміння складних структур і взаємозв'язків у фінансовій сфері.

Це можуть бути основні концепції, методології або системи класифікації, які допомагають організувати інформацію та розкривати взаємозв'язки між різними фінансовими об'єктами або поняттями [2].

Таксономія – наука про принципи та способи класифікації й номенклатури складно-організованих ієрархічних систем дійсності.

Завдання таксономії – визначення і теоретичне обґрунтування класифікаційних одиниць – таксонів, їх системи, супідрядності, співвідношення та обсягу.

Основним завданням систематики, або таксономії є класифікація об’єктів, тобто розміщення в більш або менш близьких однорідних груп на основі їх спорідненості. У системі об’єктів ці групи розміщують (класифікують) в серію підпорядкованих споріднених таксономічних рангів [1].

Процес впровадження таксономій у фінансові технології потребує комплексного підходу та оптимізації з метою максимізації ефективності та зниження витрат.

Це включає розробку, впровадження та постійне вдосконалення таких систем, що може бути складним через їхню складність та потребу відповідності стандартам та регулятивним вимогам.

Інтеграція таксономій у фінансові технології передбачає кілька етапів, включаючи аналіз даних, створення структури таксономії, впровадження та тестування системи, а також постійне вдосконалення та адаптацію до змінних умов ринку.

Для оптимізації цього процесу можна використовувати сучасні методи управління проєктами та технологіями, такі як методи штучного інтелекту, аналіз даних та автоматизація процесів.

Це допомагає підвищити швидкість впровадження, зменшити ризики та забезпечити високу якість результуючої системи.

Оптимізація процесу впровадження таксономій у сфері фінансових технологій є ключовим етапом для забезпечення ефективності та стабільності фінансових установ та підприємств в умовах стрімкого розвитку сучасного фінансового ринку та постійних технологічних інновацій.

Впровадження таксономій дозволяє систематизувати та структурувати дані, що допомагає у зробленні обґрунтованих стратегічних рішень та прогнозуванні розвитку фінансових ринків.

Таксономі́чна катего́рія (таксономічний ранг) – поняття, що застосовується в систематиці для позначення підпорядкування різних груп живих організмів, що відрізняються одна від одної ступенем спорідненості.

Таксономічні категорії різного рівня, або рангу, присвоюють реальним відокремленим групам об’єктів – таксонам, тобто категорії є сукупностями таксонів одного рангу.

На відміну від таксонів, таксономічні категорії позначають не реальні організми, а визначений ранг чи рівень класифікації, тобто ступінь ієрархії [1].

Існує два види таксономії:

- природна, тобто індуктивно виведена з аналізу властивостей об'єктів;
- штучна (логічна), що базується на деякому єдиному логічному принципі, що вводиться апріорно.

У лінгвістиці застосовуються обидва типи таксономії; приклад природної таксономії – генеалогічна класифікація мов, приклад штучної таксономії – типологічна класифікація.

Змістовно одна й та сама таксономія може бути в одних випадках природною, в інших – штучною.

Природна таксономія дає більш жорстке і, як правило, єдине угруповання об'єктів.

За характером таксономічної процедури розрізняються:

якісна таксономія (угруповання об'єктів за наявністю чи відсутності вони таксономічних ознак);

кількісна таксономія (угруповання об'єктів за рівнем володіння таксономічними ознаками, тобто за числової величини близькості об'єктів друг до друга).

Якісна таксономія дає чітко розмежовані таксони – класи.

Кількісна таксономія може містити як класи, і поля, т. е. таксони, які мають чітких кордонів і дифузно змикаються коїться з іншими таксонами.

Один з викликів у процесі впровадження таксономій полягає у їхній складності та потребі відповідати вимогам стандартів та регулятивних органів.

Це може вимагати розробки спеціалізованих технологічних рішень та впровадження новаторських підходів у фінансову сферу.

Для досягнення оптимальних результатів у впровадженні таксономій необхідно використовувати сучасні методи управління проєктами та технологіями.

Застосування методів штучного інтелекту, аналізу даних та автоматизації процесів дозволяє підвищити ефективність впровадження, знизити ризики та забезпечити високу якість результуючої системи.

Оптимізація процесу впровадження таксономій у фінансовій сфері є складним завданням, проте з використанням сучасних підходів та інструментів вона може бути успішно вирішена.

Важливою є системна та комплексна підготовка, а також гнучкість у вирішенні виникаючих завдань та проблем [3].

Метою даного дослідження є ретельний аналіз та систематизація методів оптимізації процесу впровадження таксономій у сфері фінансових технологій.

Дослідження спрямоване на вивчення кращих практик у цій галузі, а також розробку рекомендацій щодо оптимального використання цих методів у конкретних умовах.

Об'єктом дослідження є процес впровадження таксономій у сфері фінансових технологій.

Дослідження спрямоване на вивчення етапів, методів та інструментів, які використовуються для ефективного впровадження таксономій, а також на визначення факторів успіху та перешкод, які можуть вплинути на його результативність.

Список використаних джерел:

1. Матеріал з Вікіпедії — вільної енциклопедії. URL: https://uk.wikipedia.org/wiki/%D0%A2%D0%B0%D0%BA%D1%81%D0%BE%D0%BD%D0%BE%D0%BC%D1%96%D1%8F

2. Tsai C. The FinTech Revolution and Financial Regulation: The Case of Online Supply Chain Financing. Asian Journal of Law and Society / C. Tsai. – 2017. Vol. 4. Issue 1. P. 109–132.

3. Вовчак О. Д. Вплив фінансових технологій на забезпечення конкурентоспроможності банку / О. Д. Вовчак, В. М. Пронько // Вісник Університету банківської справи. – 2020. – № 1. – С. 86-91.

4. Vartsaba V. Fintech industry in Ukraine: problems and prospects for the implementation of innovative solutions / V. Vartsaba, O. Zaslavska // Baltic Journal of Economic Studies. 2020. Vol. 6, № 3. P. 46-55.

5. Ковблюк М. М. Основи номенклатури та систематики / М. М. Ковблюк. — Сімферополь: ДІАЙПІ, 2008.- 148 с.

УДК 004.41

Стяглик В.В.
здобувач бакалаврського рівня вищої освіти
Національний технічний університет «Харківський політехнічний інститут»
Науковий керівник
Асландуков М.О.
Старший викладач кафедри КМАД
Національний технічний університет «Харківський політехнічний інститут»

РОЛЬ ПРОГРАМНОЇ ІНЖЕНЕРІЇ У СТВОРЕННІ МАСШТАБОВАНИХ ІТ-РІШЕНЬ

В умовах стрімкого розвитку інформаційних технологій, здатність компаній швидко адаптувати свої системи до зростання обсягів даних та користувачів стає однією з ключових конкурентних переваг. Масштабованість ІТ-рішень є критичним фактором для забезпечення стабільної роботи сервісів у динамічному бізнес-середовищі. Програмна інженерія виступає основою для розробки таких рішень, забезпечуючи ефективну архітектуру, яка здатна підлаштовуватися під потреби зростання. Спробуємо дослідити роль програмної інженерії у створенні масштабованих ІТ-рішень через аналіз ключових принципів, підходів та успішних прикладів.

Почнемо із визначення поняття “масштабованість”. Це здатність системи збільшувати свої ресурси та продуктивність у відповідь на збільшення навантаження. Це може бути досягнуто шляхом вертикальної масштабованості (збільшення потужностей одного сервера) або горизонтальної масштабованості (додавання нових серверів). Масштабованість є важливою для будь-якого бізнесу, оскільки дозволяє ефективно реагувати на зростання попиту без втрати продуктивності. Для стартапів це означає можливість швидко розширювати свої сервіси, для великих компаній – підтримувати високу якість обслуговування мільйонів користувачів.

Розглянемо основні принципи програмної інженерії. Програмна інженерія забезпечує систематичний підхід до розробки програмного забезпечення, орієнтованого на масштабованість. Одним з ключових принципів є використання архітектурних патернів, таких як мікросервіси. Мікросервісна архітектура дозволяє будувати систему на основі сукупності незалежних сервісів, що можуть працювати автономно, що полегшує їх масштабування. Інші підходи включають контейнеризацію, що дозволяє запускати окремі компоненти системи незалежно від інфраструктури, і використання хмарних технологій для гнучкого розподілу ресурсів.

Методології розробки, такі як Agile та DevOps, забезпечують ефективне управління процесом створення програмного забезпечення. DevOps, зокрема, фокусується на автоматизації процесів тестування та розгортання, що дозволяє скоротити час виходу нових версій продукту. Інструменти для автоматизації, такі як Jenkins, Docker та Kubernetes, допомагають командам розробників

швидко впроваджувати зміни, забезпечуючи стійкість та масштабованість системи.

Схарактеризуємо вплив програмної інженерії на масштабованість ІТ-рішень. Програмна інженерія допомагає створювати архітектуру, яка сприяє масштабованості через чітке розмежування компонентів системи та гнучкість у їх керуванні. Застосування хмарних рішень, таких як Amazon Web Services (AWS) чи Microsoft Azure, дозволяє динамічно змінювати кількість ресурсів, що виділяються для системи залежно від поточного навантаження. Це особливо важливо для проєктів, що стикаються з раптовими піками навантаження, наприклад, під час маркетингових кампаній або запуску нових продуктів.

Інший важливий аспект – це оптимізація використання ресурсів. Розробники можуть використовувати балансування навантаження для рівномірного розподілу трафіку між серверами, що знижує ризик перевантаження одного з них. Автоматизація процесів у рамках DevOps дозволяє командам забезпечити безперервне оновлення та моніторинг систем, що підвищує ефективність їх масштабування.

Наведемо приклади масштабованих ІТ-рішень. Прикладом успішної реалізації масштабованих рішень є Google, де використовується мікросервісна архітектура для підтримки мільярдів запитів щодня. Компанія побудувала свою інфраструктуру на базі хмарних технологій, що дозволяє їй гнучко керувати ресурсами та швидко реагувати на зростання навантаження.

Інший приклад – Netflix, який використовує архітектуру на базі AWS для забезпечення безперебійної роботи свого стримінгового сервісу. Завдяки масштабованій інфраструктурі компанія може обслуговувати мільйони користувачів у режимі реального часу, забезпечуючи високу якість передачі даних навіть під час пікових навантажень.

Проте, питання масштабування ІТ-рішень не обходить наявність проблем та викликів. Незважаючи на переваги масштабованих рішень, існує ряд викликів, з якими стикаються компанії. Перш за все, це вартість впровадження таких рішень. Масштабована архітектура вимагає значних інвестицій в інфраструктуру, а також у забезпечення безпеки та відмовостійкості. Наприклад, необхідність дублювання даних або створення резервних серверів може суттєво збільшити витрати.

Ще один виклик – це забезпечення стабільності та безпеки системи. Зі збільшенням масштабів зростає складність управління безпекою, оскільки більша кількість компонентів означає більше можливих точок вразливості. Програмна інженерія вирішує ці проблеми шляхом впровадження інструментів моніторингу та виявлення загроз у реальному часі.

Попри всі труднощі, що супроводжують програмну інженерію в цілому та питання масштабування зокрема, маємо зазначити перспективи розвитку програмної інженерії для масштабованих рішень.

У майбутньому, програмна інженерія продовжить розвиватися у напрямку забезпечення більшої гнучкості та адаптивності ІТ-рішень. Тенденції, пов'язані зі штучним інтелектом та машинним навчанням, відкривають нові можливості

для автоматизації процесів управління масштабованими системами. Наприклад, системи, що самостійно аналізують навантаження та адаптують свої ресурси, можуть значно знизити потребу у втручанні людини в процес масштабування.

Крім того, розвиток таких технологій, як безсерверна архітектура (serverless), дозволить створювати ще більш гнучкі рішення, що можуть автоматично масштабуватися залежно від потреб бізнесу. Це змінить підхід до розробки та управління системами, відкриваючи нові перспективи для ефективного використання ресурсів.

Отже, програмна інженерія відіграє вирішальну роль у створенні масштабованих IT-рішень, забезпечуючи інструменти та методології для гнучкої адаптації систем до зростання навантаження. Використання хмарних технологій, мікросервісної архітектури та інструментів автоматизації дозволяє бізнесу не тільки підтримувати високу продуктивність, але й ефективно використовувати ресурси. Незважаючи на виклики, такі як витрати та безпека, перспективи розвитку програмної інженерії відкривають нові горизонти для подальшого вдосконалення масштабованих IT-систем.

Список використаних джерел

1. Киселевич, В., Усата, О., Сікора, Я., Вербівський, Д., Іванов, Д. (2024). Мікросервісна архітектура: переваги та недоліки її практичного застосування. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2, 50–59, doi: https://doi.org/10.32782/IT/2024-2-7

2. Ю.В. Рогушина, І.Ю. Гришанова (2022). Проблеми масштабування семантичних інформаційних ресурсів зі складною структурою *Проблеми програмування*. № 3-4. С. 171-182. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/188641/18-Rogushina.pdf?sequence=1

3. Цибульник С.О., Барандич К.С. (2022) Технології розроблення програмного забезпечення частина 1. життєвий цикл програмного забезпечення. КПІ ім. Ігоря Сікорського. 270 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/9521e5f9-421a-4874-a17d-f0853f942856/content

УДК 004.8+336

Стяглик І. В.
здобувач освіти
Харківський кооперативний торгово-економічний фаховий коледж
Науковий керівник
Москаленко О. В.
викладач
Харківський кооперативний торгово-економічний фаховий коледж

МАЙБУТНЄ ШТУЧНОГО ІНТЕЛЕКТУ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ В СУЧАСНОМУ СЕРЕДОВИЩІ ФІНАНСОВИХ УСТАНОВ

Штучний інтелект (ШІ) стрімко трансформує фінансовий сектор, відкриваючи нові можливості для автоматизації процесів, аналізу великих обсягів даних і прийняття рішень на основі алгоритмів. Впровадження ШІ змінює підходи до роботи з клієнтами, управління ризиками та боротьби з шахрайством. Проте, цей процес також супроводжується рядом викликів: від кібербезпеки до етичних питань і необхідності розвитку законодавчої бази. Спробуємо дослідити, як фінансові установи можуть використовувати потенціал ШІ, подолавши існуючі перешкоди, щоб залишатися конкурентоспроможними в епоху цифрової трансформації.

Розглянемо сучасний стан розвитку технологій у фінансових установах. Можна стверджувати, що наряду з іншими галузями, фінансові установи вже активно використовують інструменти ШІ для підвищення ефективності обслуговування клієнтів, управління операційними процесами, автоматизації виконання рутинних завдань. Наприклад, чат-боти, такі як AI-асистенти, полегшують роботу з клієнтами, обробляючи тисячі запитів в автоматичному режимі. Алгоритми машинного навчання дозволяють аналізувати великі обсяги фінансових даних, виявляти тренди та прогнозувати поведінку ринку. Завдяки цим інноваціям банки можуть швидше ухвалювати рішення, оптимізувати внутрішні процеси та знижувати витрати.

Проте, маємо і суттєві виклики впровадження ШІ у фінансово-кредитній сфері. Незважаючи на численні переваги, впровадження ШІ у фінансових установах супроводжується рядом проблем. Одним з ключових факторів є кібербезпека. Оскільки фінансові установи обробляють велику кількість конфіденційних даних, автоматизація процесів може підвищити вразливість систем до кібератак. Також, занепокоєння викликають й етичні питання використання новітніх інструментів цифрових технологій. Автоматизація рішень може призвести до дискримінації або неправильних результатів через помилки чи неточності в алгоритмах. Ще один виклик – це відсутність чіткої законодавчої бази для регулювання використання ШІ у фінансовій сфері, що може створювати певні правові та регуляторні ризики.

Та попри всі ці складності та утруднення, впевнені, що існують перспективи розвитку інструментів ШІ у фінансово-кредитній та банківській

сфері. Наприклад, ШІ може оптимізувати процеси оцінки та управління ризиками, забезпечуючи більш точні прогнози щодо можливих фінансових втрат і допомагаючи уникати збитків та необґрунтованих рішень. Крім того, використання ШІ може сприяти персоналізації банківських послуг, що дозволяє установам пропонувати індивідуальні рішення для кожного клієнта на основі його поведінки, уподобань, витрат та фінансових операцій. А ще, ШІ відіграє важливу роль у боротьбі з шахрайством, допомагаючи виявляти підозрілі транзакції на основі відомих патернів та сценаріїв поведінки.

Маючи такий потенціал, інструменти штучного інтелекту вже мають і матимуть надалі вирішальний вплив на трансформацію бізнес-моделей фінансових установ. Застосування ШІ сприяє перетворенню традиційних бізнес-моделей. Зокрема, інтеграція ШІ в процеси прийняття рішень дозволяє швидко реагувати на зміни ринкових умов і мінімізувати вплив людського фактору. Автоматизація таких процесів, як оцінка кредитоспроможності, ризик-менеджмент або клієнтський сервіс, змінює підходи до управління і дозволяє фінансовим установам залишатися конкурентоспроможними у світі, який так стрімко змінюється.

Спробуємо сформувати деякі прогнози щодо подальшого впровадження ШІ у кредитно-фінансову сферу. Аналітики та фахівці цієї галузі стверджують, що у найближчі 5-10 років очікується значне зростання впровадження ШІ у фінансових та банківських установах. Прогнозується, що нові інструменти на основі ШІ все більше використовуватимуться для автоматизації процесів аналізу великих даних, що дозволить фінансовим установам приймати рішення на основі складних моделей прогнозування. Крім того, інтеграція з іншими технологіями, такими як блокчейн та Big Data, може посилити здатність кредитно-фінансових установ ефективніше управляти операціями та забезпечувати безпеку даних. Проте, через ризики таких загроз, як кібератаки, установи та організації мають бути готовими інвестувати значні кошти в посилення кібербезпеки та розвиток персоналу, створення безпечного інформаційного середовища та комфортного і безпечного цифрового простору.

Отже, ШІ має величезний потенціал для трансформації фінансово-кредитної сфери, надаючи можливості для оптимізації процесів, персоналізації обслуговування клієнтів та покращення управління ризиками. Однак, для повноцінного використання переваг ШІ, фінансові установи мають подолати ряд викликів, таких як забезпечення кібербезпеки, адаптація законодавства та розвиток кваліфікованих фахівців. У майбутньому ті установи та організації, які зможуть успішно інтегрувати ШІ у свої процеси, матимуть значні конкурентні переваги.

Список використаних джерел

1. Autor, D., & Salomons, A. (2018). Is automation labor-displacing? Productivity growth, employment, and the labor share. *Brookings Papers on Economic Activity*. URL: https://www.jstor.org/stable/26506212

2. Arner, D. W., Barberis, J. N., & Buckley, R. P. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business*. URL: https://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2/

3. Кулініч Т., Стернюк О. Аналіз використання штучного інтелекту в цифровому фінансовому середовищі в Україні. *Економіка та суспільство*. Випуск 63 / 2024. URL: https://economyandsociety.in.ua/index.php/journal/article/view/4086/4015

УДК 658.115.4:339.92

Сунцова О.О.
д. е. н., професор, академік Академії економічних наук України,
професор кафедри міжнародної економіки,
Національний університет харчових технологій
Карандюк О.Г.
старший вчитель, Тарасівський ліцей

СИСТЕМИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ТРАНСНАЦІОНАЛЬНИХ КОРПОРАЦІЙ: ОСОБЛИВОСТІ І ВИКЛИКИ В УМОВАХ ГЛОБАЛІЗАЦІЇ

Системи прийняття рішень для транснаціональних корпорацій (ТНК) є критичним компонентом їхньої здатності успішно функціонувати у сучасних умовах глобалізації. Складність та динамічність глобального середовища вимагають від ТНК ефективного управління інформаційними потоками, швидкої адаптації до змін ринку та зваженого врахування багатьох факторів. Основною проблемою є необхідність інтеграції глобальних та локальних чинників, що часто входять у конфлікт, зокрема через різні культурні та економічні реалії.

Транснаціональні корпорації відіграють ключову роль у глобальній економіці, створюючи глобальні виробничі мережі, які охоплюють кілька країн. За даними досліджень (Szulanski, 2020), особливістю систем прийняття рішень у ТНК є необхідність врахування відмінностей між ринками. Це включає регуляторні вимоги, культурні традиції та специфіку бізнес-практик, що значно ускладнює процес прийняття рішень. Важливим аспектом є й управління транснаціональними командами, що потребує високого рівня комунікації та взаємодії між підрозділами у різних країнах.

Метою цього дослідження є аналіз особливостей систем прийняття рішень у ТНК та виявлення основних викликів, які виникають в умовах глобалізації. Основними завданнями є: визначити ключові фактори, що впливають на прийняття рішень у ТНК; проаналізувати виклики, з якими стикаються корпорації під час інтеграції рішень на глобальному та локальному рівнях; оцінити роль сучасних інформаційних систем у покращенні процесу

прийняття рішень. Методи дослідження включають аналіз літературних джерел, кейс-стаді та порівняння практик управління в ТНК різних секторів.

Процеси прийняття рішень у ТНК зазнають значного впливу як внутрішніх, так і зовнішніх факторів. Важливою складовою є необхідність врахування регіональних особливостей ринків. Наприклад, ТНК, що працюють в Азії, мають адаптувати свої стратегії до регуляторних норм і культурних практик регіону, що часто відрізняються від стандартів на західних ринках. Ця адаптація ускладнює процес прийняття рішень та потребує розвинених інформаційних систем.

Інформаційні системи відіграють важливу роль у модернізації процесів управління, дозволяючи топ-менеджменту ТНК обробляти великі обсяги даних і приймати швидкі рішення. Проте використання таких систем ставить нові виклики у сфері кібербезпеки, оскільки зростає ризик витоку конфіденційної інформації. Як зазначає Prakash (2022), успішне впровадження інформаційних технологій значно підвищує ефективність управління в ТНК, але потребує постійного моніторингу та забезпечення безпеки.

В табл. 1 розглянемо факти застосування систем прийняття рішень різними ТНК та відомі виклики їх запровадження в умовах глобалізації.

Таблиця 1. Аналітика кейсів застосування систем прийняття рішень різними транснаціональними корпораціями (ключові стратегії та виклики в умовах глобалізації)

ТНК	Система прийняття рішень	Ключові особливості	Основні виклики	Результати
Google	Інтеграція локальних рішень у глобальну стратегію	Використання даних від локальних команд для прийняття адаптованих рішень	Культурні відмінності, труднощі у реалізації єдиної стратегії на різних ринках	Зростання присутності на міжнародних ринках, покращена адаптивність продуктів
Toyota	Тотальна якість управління (Total Quality Management – TQM)	Фокус на децентралізованих рішеннях і впровадженні інновацій у виробничі процеси	Забезпечення відповідності глобальним стандартам якості та водночас врахування регіональних специфікацій	Підвищення ефективності виробництва, зниження витрат, покращення якості продукції
Nestlé	Централізоване управління з місцевою адаптацією	Використання глобальних стратегічних ініціатив із можливістю	Конфлікт між глобальними цілями компанії та потребами локальних	Підвищення локальної конкурентоспроможності, задоволення потреб різних ринків

ТНК	Система прийняття рішень	Ключові особливості	Основні виклики	Результати
		адаптації до місцевих ринків	ринків, регуляторні обмеження в різних країнах	
Unilever	Інформаційні системи для управління ланцюгами постачання	Застосування інформаційних систем для оптимізації ланцюгів постачання та логістичних процесів	Висока складність управління даними та процесами в глобальних масштабах, кіберзагрози	Оптимізація витрат на логістику, покращення координації між регіональними офісами та глобальними командами
Volkswagen	Стратегічне планування на основі "зеленої" мобільності	Прийняття рішень щодо екологічної стійкості та переходу на електромобілі	Регуляторні вимоги щодо викидів у різних регіонах, адаптація виробництва до нових технологічних стандартів	Зниження викидів, покращення екологічного іміджу, зростання частки ринку електромобілів
Samsung	Інноваційне планування та R&D	Інвестиції в дослідження і розробки, стратегія продуктового лідерства	Висока конкуренція, необхідність швидкої адаптації до змін ринку та технологій	Підвищення інноваційної конкурентоспроможності, лідерство у сфері технологічних продуктів
Coca-Cola	Локалізація маркетингових рішень	Адаптація глобальних маркетингових стратегій до особливостей різних регіональних ринків	Відмінності у споживчих перевагах, культурних традиціях та регуляторних нормах різних країн	Покращення глобальної впізнаваності бренду, локалізація продуктів відповідно до потреб споживачів у різних регіонах

Source: independently compiled by the author

Важливою складовою управління є інтеграція глобальних рішень на локальному рівні, що часто стикається з опором через відмінності у регіональних умовах. У таких випадках ТНК повинні розвивати гнучкі стратегії, що дозволяють адаптувати глобальні рішення до місцевих умов, зберігаючи при цьому загальну стратегічну лінію. Також виникають питання стосовно відповідальності ТНК перед різними стейкхолдерами, що вимагає

розширення корпоративної соціальної відповідальності, зокрема в умовах екологічних і соціальних ризиків.

Системи прийняття рішень у ТНК повинні бути адаптовані до умов глобалізації та враховувати численні виклики, що пов'язані зі складністю управління транснаціональними структурами. Використання сучасних інформаційних технологій може значно покращити цей процес, проте залишається необхідність вирішення питань кібербезпеки та інтеграції регіональних рішень у загальну стратегію компанії. Перспективним напрямом досліджень є розробка нових моделей прийняття рішень, які будуть враховувати не лише економічні, а й соціально-екологічні фактори в умовах глобальних викликів.

Список використаних джерел:

1. Prakash, A. (2022). The Role of Information Systems in Enhancing Decision-Making Efficiency in Global Corporations. *International Journal of Business and Management*, 17(2), 129-145. https://doi.org/10.2139/ssrn.3859765

2. Suntsova, O. (2024) Impact of public-private partnership assets on economic growth in Ukraine. *Financial and Credit Systems: Prospects for Development*, 2(13), 68-84. https://doi.org/10.26565/2786-4995-2024-2-07

3. Сунцова О. Роль технології блокчейн в зміні структури монетарної бази та ВВП країни. *Фінансово-кредитні системи: перспективи розвитку*. No1(12) 2024. С. 24-36.DOI: https://doi.org/10.26565/2786-4995-2024-1-03

4. Szulanski, G. (2020). Decision-Making Processes in Multinational Corporations: A Global Perspective. *Journal of International Business Studies*, 51(3), 457-475. https://doi.org/10.1057/s41368-020-00035-9

УДК 378.018

Холіна П.В.
здобувачка вищої освіти
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна
Науковий керівник
Галич Р.В.
к.ю.н., доцент, доцент кафедри банківського бізнесу та фінансових технологій
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ПЕРЕДОВІ ТЕХНОЛОГІЇ: ОСОБЛИВОСТІ ГІБРИДНОГО НАВЧАННЯ

Сьогодення ознаменоване швидкоплинним розвитком інноваційних технологій. Рушійною силою таких процесів стають як глобальні виклики, так і еволюційний хід сучасних трансформацій. Освітнє середовище також знаходиться не осторонь технологічного прогресу, а інколи і очолює його, розвиваючи інновації. Ключовими рисами змін, що характерні для освіти визнаються: впровадження нових форм, моделей і методів навчання. А це, справедливо відмітити, відбувається завдяки як негативним факторам (пандемії, війни і конфлікти, природні катаклізми), так і позитивним (технологічний прогрес), наслідком яких є глобальні зміни в системі комунікацій в соціумі. Зважаючи на це, запровадження нових дистанційних форм роботи, змішаних, гібридних методів і онлайн-технологій є звичайним сьогоденням освіти, як у високотехнологічних країнах Європи, так і в усьому світі загалом [1]. Це підтверджує і досвід в діджитал освіті Німеччини (Саарландский Університет), Іспанії (Університет Короля Хуана Карлоса, Міжнародний університет Ла-Ріохи), Італії (Університет Палермо) тощо.

При цьому, як вбачається, є кілька обов'язкових складників, які мають бути збережені або досягнуті в такому форматі освітніх процесах. І мова йде, в першу чергу, про якість і рівень освіти, доступність, рівність і безперервність навчання. Крім того, забезпечення високих стандартів перебуває в фокусі обрання оптимальних моделей. Денна, заочна і дистанційна форми, різні види занять, асинхронні і синхронні процеси, змішані форми – все це потребує універсальної моделі, так званого гібриду. Моделі, яка є спробою забезпечити «найкраще з обох світів», тобто переваги онлайн-навчання в поєднанні з усіма перевагами традиційного класу [2]. Справедливо відмічено, гібрид являє собою поєднання нової, передової технології зі старою технологією і створення інновації стосовно старої технології [3]. До того ж, визначаючи дефініцію гібридне навчання, відмічено, гібридне навчання is a diverse and expanding area of design and inquiry that combines face-to face and online [4]. Отже, гібридне навчання – формат навчання, за якого навчальне заняття відбувається в аудиторії і одночасно (синхронно) для учасників освітнього процесу поза аудиторією, за допомогою інноваційних технологій. Як і будь-яке явище,

гібридне навчання має свої очевидні переваги, але також і певні пересторогі, що підтверджують і дослідження цієї теми. Серед інших, називають: і збільшення участі студентів, гнучкість навчання, доступ до освіти, слабкий зв'язок між учнем і викладачем, технічні проблеми, неефективну педагогіку тощо [5]. Безумовно, це питання треба розглядати комплексу. І з погляду держави – на рівні регулювання, стандартів впровадження (якісних і кількісних); університету – регулювання, матеріально-технічні умови, підвищення кваліфікації персоналу; викладача – підвищення професійних здібностей в умовах використання високих технологій; здобувача – здатність бути повноцінним учасником процесу, обрання оптимального формату навчання. На наш погляд, у разі вирішення юридичної і фінансової частин, гібридне навчання відповідатиме вже згаданим високим стандартам та успішно об'єднає віддалених і очних студентів у режимі реального часу для синхронних занять, причому з відсутньою різницею між тими, хто знаходиться особисто чи віддалено.

Отже, гібридне навчання є цілком повноцінною формою і одним з найбільш ефективних форматів, де використовуються передові технології. Саме такий формат не тільки виключно забезпечує навчальний процес в певних умовах, а й активізує, стимулює швидкоплинний розвиток всіх учасників процесу – студента, викладача, адміністративний персонал, університет і державу загалом. Така модель потребує подальшого аналізу і в найближчому майбутньому формалізованої імплементації в нову сучасну модель освіти України і Європи.

Список використаних джерел:

1. Johnson, J. (2023, 10).Internet penetration rate worldwide 2023, by region. Retrieved 11 25, 2023, from Statista: https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/

2. Clayton M. Christensen, Michael B. Horn, Heather Staker(May 22, 2013).An introduction to the theory of hybrids.11,26, 2023. https://www.christenseninstitute.org/publications/hybrids.

3.Кухаренко В.М. (2015) Системний підхід до змішаного навчання.Інформаційні технології в освіті. № 24. дата звернення 27.11.2023.Режим доступу: http://nbuv.gov.ua/UJRN/itvo_2015_24_6

4.Singh, Abtar Darshan. (May2021).Conceptualisingand implementing hybrid learning models.UNESCO.No. 47. 28.11.2023 https://unesdoc.unesco.org/ark:/48223/pf0000377807

5.E.Idrizi, S.Filiposka,Vl. Trajkovik (May 2022). Hybrid Learning -the new normal.Green Economy and Technological Change for Sustainability-5th international Scientific Conference on Business and Information Technologies SEE University, Tetovo, North Macedonia. 29.11.2023. https://www.researchgate.net/publication/360783732_Hybrid_Learning_-the_new_normal

УДК 374.72:004(447.54-25)

Ягло В.О.
здобувач вищої освіти, перший (бакалаврський) рівень вищої освіти
ННІ «Каразінський банківський інститут» ХНУ ім. В.Н. Каразіна
Єрмакова Н.А.
старший викладач кафедри інформаційних технологій та математичного моделювання
ННІ «Каразінський банківський інститут» ХНУ ім. В.Н. Каразіна

НАВЧАННЯ ДОРОСЛИХ МОБІЛЬНІЙ ГРАМОТНОСТІ: ДОСВІД ТА РЕЗУЛЬТАТИ НА БАЗІ ОСВІТНЬОГО ЦЕНТРУ ПРИ SNC MUSEUM

В умовах цифровізації всі сфери життя вимагають від людини навичок роботи з мобільними пристроями та програмним забезпеченням. Проте дорослі, особливо літні люди, часто стикаються з труднощами в освоєнні нових технологій через недостатню мобільну грамотність. Здатність користуватися мобільними додатками, такими як соціальні мережі, месенджери, навігаційні системи та браузери, стає не просто побутовою необхідністю, а важливим аспектом для підтримання соціальної взаємодії, доступу до інформації, управління фінансами та інших важливих життєвих сфер. Тому навчання дорослих мобільній грамотності стає актуальним соціально-освітнім завданням.

Основною метою навчання було забезпечити дорослих учнів навичками мобільної грамотності, необхідними для комфортного використання сучасних мобільних технологій у щоденному житті. Зокрема, курс включав вивчення базових функцій смартфонів, роботи з популярними додатками (Instagram, Telegram, Viber, Zoom), а також навігацію в інтернеті за допомогою Google Chrome та Google Maps.

Завданнями курсу стали:

- ➢ Ознайомлення з основами роботи з мобільними пристроями (загальний інтерфейс телефону, налаштування, безпека).
- ➢ Розвиток навичок використання комунікаційних додатків (Telegram, Viber, Zoom).
- ➢ Навчання базовим функціям соціальних мереж (Instagram).
- ➢ Опановування навичками користування Google Maps для навігації та Google Chrome для інтернет-серфінгу.
- ➢ Залучення дорослих учнів до активного використання мобільних додатків для покращення якості життя.

Для навчання дорослих були застосовані інтерактивні та адаптивні методики, орієнтовані на індивідуальні потреби кожного учасника. У процесі викладання використовувалися різноманітні методи. Розглянемо їх детальніше.

1. Інтерактивне навчання: Кожен учень мав можливість самостійно виконувати практичні завдання на власних телефонах під час занять. Це допомагало не лише закріпити теоретичний матеріал, але й сприяло активному засвоєнню нових знань через практику.

2. Індивідуальний підхід: Завдяки волонтерському характеру проєкту кількість учасників була невеликою, що дало змогу забезпечити персональну увагу до кожного учня, враховуючи його попередній рівень знань та темп освоєння інформації.

3. Візуалізація: Для пояснення складних моментів використовувалися наочні матеріали – презентації, відеоінструкції та покрокові інструкції, що полегшували розуміння та сприяли кращому запам'ятовуванню.

4. Групова робота: Літні учні активно взаємодіяли один з одним, допомагаючи у вирішенні технічних питань, що посилювало командний дух і мотивацію до навчання.

5. Практичні завдання: Кожне заняття завершувалося виконанням конкретних дій (створення акаунта в Instagram, додавання контактів у Viber, створення груп та каналів зв'язку тощо), що закріплювало отримані знання та навички.

Після завершення курсу було проведено опитування учнів, яке показало високий рівень задоволення та позитивні результати навчання. Основними показниками якості навчання стали:

- *збільшення впевненості у використанні смартфонів*: Більшість учасників зазначили, що стали відчувати себе набагато впевненіше під час користування мобільними додатками та пристроями.
- *розширення можливостей для соціальної взаємодії:* Учні активно почали використовувати Viber і Telegram для комунікації з родиною та друзями, що позитивно вплинуло на їхній соціальний зв'язок.
- *підвищення рівня незалежності:* Опановування базовими навичками роботи з Google Maps та Google Chrome допомогло учасникам стати більш незалежними у повсякденному житті.
- *сприяння професійній активності:* У деяких випадках здобуті навички були використані для професійних цілей – учасники змогли брати участь у відеоконференціях через Zoom, вести особисті блоги в Instagram, а також шукати важливу інформацію через Google.

Окрім побутових переваг, навчання мобільній грамотності сприяло також особистісному та професійному розвитку учасників. Завдяки отриманим знанням і навичкам, дорослі учні змогли активно використовувати смартфони для підвищення своєї професійної активності. Наприклад, викладачі елегантного віку мали змогу організовувати онлайн-зустрічі через Zoom, що забезпечило їхню залученість до освітнього процесу в умовах пандемії COVID-19 та повномасштабного вторгнення.

На особистісному рівні учасники відзначили зростання впевненості у власних силах, що позитивно вплинуло на їхнє самопочуття та самооцінку. Можливість опанувати нові технології сприяла подоланню страху перед новими викликами та дала відчуття успішності.

Зважаючи на позитивні результати навчання, необхідно продовжувати впровадження подібних програм для дорослих на регулярній основі. Перспективними напрямками розвитку освітньої діяльності є:

Розширення географії проєкту: створення подібних освітніх ініціатив у малих містах і сільських місцевостях, де доступ до технологій обмежений.

Розробка онлайн-курсів: упровадження дистанційних програм навчання, які дозволять охопити більшу аудиторію та надавати навчання у більш зручний спосіб.

Інтеграція навчання у загальноосвітні програми для дорослих: навчання мобільній грамотності може бути частиною програм підвищення кваліфікації або перекваліфікації дорослих, особливо в контексті професій, що вимагають активного використання цифрових технологій.

Загалом, мобільна грамотність є ключовою складовою сучасного суспільства, і навчання дорослих цим навичкам – важливий крок до забезпечення їхньої повноцінної участі в соціальному та професійному житті.

Список використаних джерел:

1. Єрмакова Н.А. Навчання дорослих комп'ютерній і мобільній грамотності в Освітньому центрі при Музеї Софту та комп'ютерів в умовах сьогодення України // Матеріали III Міжнародної науково-практичної конференції “Освіта дорослих: світові тенденції, українські реалії та перспективи”, 13-14 червня 2024 р.

2. Марцинюк А.Ю. Цифрова грамотність у контексті освіти дорослих // Молодіжна наука у контексті суспільно-економічного розвитку країни: матеріали III Міжнародної учнівсько-студентської конференції., м. Черкаси: СУЕМ, 22 лист. 2019 р. Черкаси, 2019. С. 280-282.

ЗМІСТ

Електронне наукове видання
комбінованого використання
Можна використовувати в локальному та мережному режимах

ІТ-ПРОСТІР СЬОГОДЕННЯ: ТЕНДЕНЦІЇ, ІННОВАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Збірник тез доповідей
Всеукраїнської науково-практичної студентської конференції

(16 жовтня 2024 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-класса; ОС Windows 7/10;
дисковод CD-ROM; Acrobat Reader 10.
Об’єм даних 3,8 Мб. Замовлення № 113/23.

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.