Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Інститут цифровізації освіти НАПН України
Національний технічний університет України
«Київський політехнічний інститут» ім. І. Сікорського
Вінницький національний технічний університет
Житомирський військовий інститут імені С.П. Корольова
Тернопільський національний технічний університет імені Івана Пулюя
Харківський національний університет радіоелектроніки
Уманський державний педагогічний університет імені Павла Тичини
Національний університет біоресурсів і природокористування України
Інститут геохімії навколишнього середовища НАН України
Черкаський державний технологічний університет
Державний університет «Київський авіаційний інститут»

Комп'ютерні технології: інновації, проблеми, рішення

Тези доповідей VIII Всеукраїнської науково-технічної конференції

м. Житомир, 02-03 грудня 2025 р.

2025

УДК 004
К63

Рекомендовано Вченою радою Державного університету «Житомирська політехніка» (протокол № 20 від 18.12.2025 р.)

К63 Комп'ютерні технології: інновації, проблеми, рішення: тези доповідей VIII Всеукраїнської науково-технічної конференції, м. Житомир, 02-03 грудня 2025 р. – Житомир: Житомирська політехніка, 2025. – 468 с.

ISBN 978-966-683-721-2

Представлено доповіді учасників VIII Всеукраїнської науково-технічної конференції. Наведено аналіз та результати досліджень сучасних проблем інформаційних технологій, математичного моделювання та розробки програмного забезпечення, інформаційних систем, комп'ютерної інженерії та кібербезпеки, цифрової обробки сигналів та зображень, комп'ютерно-інтегрованих технологій, робототехніки та приладобудування, інформаційних технологій в телекомунікаціях та біомедицині, інформаційно-комунікаційних технологій в освіті.

УДК 004

ISBN 978-966-683-721-2

Секція 1
МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

УДК 004

Терещук В. О., магістрант,
Чижмотря О. В., ст. викладач
Державний університет «Житомирська політехніка»

ТЕХНОЛОГІЇ ОПТИЧНОГО РОЗПІЗНАВАННЯ СИМВОЛІВ ТА ЇХ ЗАСТОСУВАННЯ

Сфера документообігу сьогодні переживає активну цифровізацію, традиційні паперові документи замінюються їх електронними версіями, а нові матеріали переважно створюються одразу в цифровому форматі. Важко уявити собі державну установу чи будь яке підприємство, де не використовуються інформаційні технології для спрощення та систематизації обліку.

Для переходу у цифровий формат паперові документи сканують чи фотографують, після чого працюють фактично із зображеннями, що нерідко мають низьку якість, шуми чи спотворення. Через усі такі перешкоди безпосередній аналіз їхнього вмісту є складним завданням для звичайних інформаційних систем.

Технології оптичного розпізнавання символів допомагають вирішити цю проблему, надаючи можливість перетворити зображення з текстом у цифровий формат, зрозумілий комп'ютеру, готовий до редагування чи обробки. Технологія OCR ґрунтується на цифровій обробці рисунків, а також поєднанні систем комп'ютерного зору та інструментів штучного інтелекту [1]. Будь-яке зображення проходить через низку етапів перед розпізнаванням тексту на ньому та перетворенням його у цифровий формат. До них належать: попередня обробка, безпосереднє розпізнавання тексту різними способами, аналіз макету та постобробка результату.

Сучасні системи оптичного розпізнавання символів можуть відрізнятися за рівнем складності та інтелектуальності. Алгоритми, що лежать в основі систем оптичного розпізнавання символів, можуть реалізовувати різні підходи до розпізнавання, тому виділяють чотири основні типи таких технологій, серед яких посимвольне порівняння шаблонів, оптичного розпізнавання позначок, інтелектуальне розпізнавання символів та інтелектуальне розпізнавання слів [1].

Системи, що здійснюють розпізнавання тексту за принципом посимвольного порівняння шаблонів вважаються найпростішими. У таких рішеннях кожен символ зі сканованого зображення співставляється з еталонним зразком з бази даних. Таким чином, якщо форма символу збігається з одним із шаблонів – система визначає його як конкретну літеру або цифру. Проте цей метод вважається малоефективним, адже його застосування обмежене текстами, що написані стандартними шрифтами, які попередньо були “відомі” системі.

Часто виникають ситуації, коли важливо швидко розпізнати певні шаблони на документі, без проведення глибокого аналізу тексту. Для цього використовується підхід оптичного розпізнавання позначок. Він орієнтований саме на виявлення графічних елементів, зокрема відміток у формах і анкетах, позначок у тестових бланках, підписів, логотипів, водяних знаків, тощо.

У свою чергу, інтелектуальне розпізнавання символів використовує алгоритми машинного навчання й штучного інтелекту, зокрема навчається розпізнавати символи самостійно, аналогічно до того, як це роблять люди. Нейронні мережі аналізують тисячі зразків тексту, поступово навчаючись знаходити характерні риси кожної окремої літери. Алгоритми враховують розташування прямих та кривих ліній, їх перетинів – усе це дозволяє працювати не лише з друкованими, а й з рукописними текстами, а також з тими шрифтами, що ще не зустрічались у системі раніше.

На вищому рівні займає своє місце метод інтелектуального розпізнавання слів. Він вважається продовженням попередньої технології, але замість роботи з окремими символами, проводиться аналіз слів як цілісних графічних об’єктів, завдяки чому збільшується швидкість розпізнавання та її точність. Використання моделей глибокого навчання дозволяє системам враховувати також контекст, граматичну структуру речень та навіть ймовірні лексичні зв’язки між словами.

Підсумовуючи викладене, технології оптичного розпізнавання символів можна вважати невід’ємною складовою сучасних систем цифрового документообігу. Вони забезпечують автоматизацію введення даних, скорочують час, потрібний на обробку документів та підвищують точність інформаційних процесів.

Список використаних джерел:

1. Holdsworth J. What is OCR? [Електронний ресурс] / J. Holdsworth. – Режим доступу: https://www.ibm.com/think/topics/optical-character-recognition

UDC 004

Mykola Turchyn, Master's Student,
Olena Chyzhmotria, Senior Lecturer,
Iryna Dmytrenko, Senior Lecturer
Zhytomyr Polytechnic State University

SEABORN AS A TOOL FOR EFFECTIVE WORK WITH CATEGORICAL DATA

In the fields of data science and machine learning, visualization is a key tool for identifying patterns and presenting results. This is especially true when working with categorical data, which represents discrete groups. The Seaborn library, based on Matplotlib, has become one of the most popular solutions for creating such graphics. It simplifies the creation of aesthetic statistical diagrams, integrates closely with Pandas DataFrames, and provides high-level functions that reduce code volume compared to Matplotlib [1].

Categorical Data

Categorical data represents discrete groups or categories, such as gender, product types, or geographic regions. Adequate visualization of categorical data allows us to identify distributions, compare values across categories, and draw meaningful insights. Bar plots, box plots, and violin plots are the most effective tools for this purpose [2]. An example is shown in Fig. 1.

Bar plots are a very popular way for visualizing categorical data, where one axis represents the categories, and the other shows the corresponding numerical values. They make it easy to compare values across groups and identify trends or differences. On the other hand, count plots display the frequency of each category, which is particularly useful for interpretation of the distribution and prevalence of different groups.

Another way to examine the distribution of the numerical values across categories is through the use of box plots and violin plots. Box plots summarize data using the median, the quartiles, and a limit (or indicator) of the outliers, thus permitting the observation of variation or deviations from the data. In a similar line, box plots supplemented with kernel density estimates called violin plots which provide information on several cases and their distribution across categories. Seaborn is a very relevant tool for the interpretation of trends and variations at a group level, thanks to its ability to provide detailed and versatile analysis of categorical data.

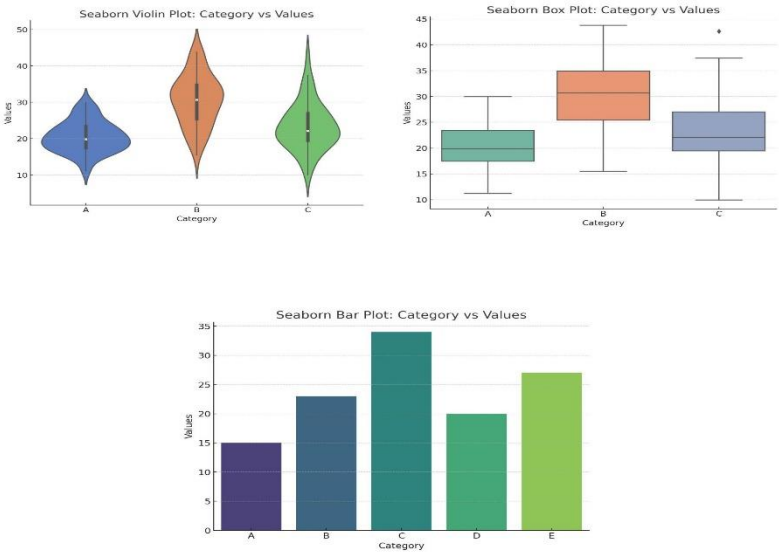


Fig. 1 – Example of visualization of categorical data

Summary

Seaborn can be useful for visualizing and analyzing categorical data. It features friendly syntax, integrates well with Pandas, and has good high-level plotting functions, making things easier when creating informative visualizations. If you are interested in studying data distributions or comparing values across categories, Seaborn has the tools to expose and present interesting findings. By learning the essential functions for categorical data, such as bar plots, box plots, and violin plots, you will be able to convert unorganized data into clear and compelling messages that aid in making decisions.

References:

1. Wes M. Python for Data Analysis Data Wrangling with pandas, NumPy, and Jupyter / McKinney Wes., 2022. – 561 c.

2. A Beginner's Guide to Seaborn for Data Visualization in Python [Information resource] / DataCamp – Resource access mode: https://www.datacamp.com/tutorial/seaborn-python-tutorial.

UDC 004

Mykola Turchyn, Master's Student,
Olena Chyzhmotria, Senior Lecturer,
Iryna Dmytrenko, Senior Lecturer
Zhytomyr Polytechnic State University

SEABORN AS A TOOL FOR EFFECTIVE WORK WITH NUMERICAL DATA

Effective data visualization is indispensable in modern analysis, helping researchers confirm theories and communicate ideas. When working with numerical data, such as age or income, graphical representation makes it easy to detect trends and relationships. Seaborn, a powerful library based on Matplotlib, offers excellent tools for this purpose. Due to its system-oriented implementation, it appeals to users as it works seamlessly with Pandas DataFrames and offers high-level functions for better visualization readability [1].

Numerical Data

Entities such as age, income, or sales can be considered as numerical data. Graphical representation of numbers makes it easy to detect trends and relations within data sets. Understanding how frequently, uniformly, or how many modes a data set contains in its frequency distribution can be done through the aid of histograms. In this way, they enable analysts to see at a glance how counts or measurements smear overall and so are significant for defining of the attributes of the data [2]. An example is shown in Fig. 1.

Scatter plots are another key visualization tool for numerical data, allowing analysts to explore relationships between two variables. By plotting numerical values on both axes, scatter plots highlight correlations, clusters, and trends by plotting numerical values on both axes enabling insights into linear or non-linear relationships. This visualization is particularly valuable for identifying whether two numerical variables influence one another.

However, *line plots* are commonly deployed to visualize changes over time. They are especially helpful in the performance of time series studies, for instance, in analyzing sales, variations in temperature or the stock market. Many data points are connected with lines and thus have definite trends and fluctuations, making them suitable for temporal analysis and forecasting.

Pair plots, are a useful tool given by Seaborn, as they allow the user to visualize multiple scatter plots of numerical relationships within groups at once. Pair plots help the user visualize scatter plots and histograms of all variable combinations, allowing the user to more thoroughly investigate pairwise relationships in an effort to locate correlations, clusters, or outliers in massive data sets.

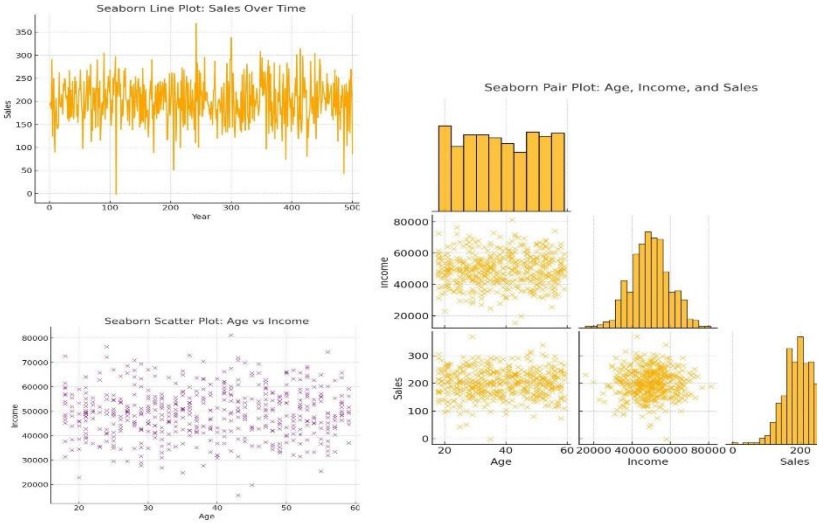


Fig. 1 – Example of visualization of numerical data

Summary

Seaborn can be useful for visualizing and analyzing numerical data. It features friendly syntax, integrates well with Pandas, and has good high-level plotting functions, making things easier when creating informative visualizations. If you are interested in studying data relations or trends, Seaborn provides the tools, such as histograms, scatter plots, and line plots, to expose and present interesting findings. By learning the essential functions for numerical data, you will be able to convert unorganized data into clear and compelling messages that aid in making decisions and guiding narratives.

References:

1. Wes M. Python for Data Analysis Data Wrangling with pandas, NumPy, and Jupyter / McKinney Wes., 2022. – 561 c.

2. Rishabh S. Seaborn: A comprehensive guide to statistical data visualization in Python [Information resource] / Singh Rishabh. - 2024. - Resource access mode: https://medium.com/@RobuRishabh/seaborn-a-comprehensive-guide-to-statistical-data-visualization-in-python-60f0d7c1de33.

UDC 004

Roman Kormysh, Master's Student,
Olena Chyzhmotria, Senior Lecturer,
Iryna Dmytrenko, Senior Lecturer
Zhytomyr Polytechnic State University

THE ROBUSTNESS OF THE NAIVE BAYES CLASSIFIER TO DATA IMBALANCES IN FIRST AID DATASETS

The increasing use of machine learning models in critical domains like healthcare and emergency response necessitates a deep understanding of their performance on non-ideal data. First aid datasets often suffer from severe data imbalance, where minor injuries are common but life-threatening events are rare. This skew can compromise a classifier's accuracy, particularly for the critical minority classes. The Naive Bayes classifier is a computationally efficient algorithm, but its core assumption of feature independence can make it vulnerable to data imbalance when the training data disproportionately favors one class over another [1]. This study conducts a comprehensive investigation into the robustness of the Naive Bayes classifier on imbalanced first aid datasets, evaluating its predictive performance and reliability on both majority and minority classes under a range of conditions.

Naive Bayes is rooted in Bayes' Theorem, which computes the posterior probability for a class given a feature vector. The algorithm's "naive" assumption of conditional independence simplifies calculations, making it fast. However, in the presence of severe class imbalance, the algorithm's prior probability estimation can become heavily skewed. A model might learn to classify all instances as the majority class to achieve high overall accuracy, effectively ignoring the critical minority class [2]. This is catastrophic in first aid applications, where misclassifying a rare but critical emergency could lead to delayed or inappropriate treatment. Therefore, our analysis will use more robust performance metrics, including precision, recall, and the F1-score, and a detailed confusion matrix to quantify the model's ability to correctly identify true positives and avoid false negatives, which is paramount for safety-critical systems.

To systematically evaluate the classifier's robustness, this research will use a simulated first aid dataset with varying degrees of class imbalance, from moderate (10:1) to extreme (100:1). The dataset will mimic realistic scenarios, including features like patient vitals, reported symptoms, and external factors. A series of controlled experiments will be conducted to measure the impact of different mitigation strategies, including both data-level and algorithm-level approaches.

Data-level techniques will include re-sampling methods like random undersampling of the majority class and oversampling of the minority class using SMOTE (Synthetic Minority Oversampling Technique) [3]. We will also investigate algorithm-level techniques, specifically cost-sensitive learning, which modifies the algorithm to assign a higher misclassification cost to errors on the minority class. A false negative (failing to identify a critical condition) can be assigned a cost much greater than a false positive. We will conduct several key experiments: first, we will evaluate the Naive Bayes classifier on the raw, imbalanced dataset to establish a baseline performance. Next, we will compare its performance on datasets modified with undersampling and SMOTE. We will then analyze the impact of cost-sensitive learning. Finally, we will explore a hybrid approach by combining the most effective data and algorithm-level methods to determine if they yield superior performance. [4]. By understanding the specific limitations of the Naive Bayes classifier, we can make informed decisions about its suitability for various applications.

In conclusion, the robustness of the Naive Bayes classifier to data imbalances is a critical consideration for its application in real-world first aid and medical datasets. This study provides a comprehensive framework for assessing its performance and evaluating various mitigation techniques. By focusing on metrics beyond overall accuracy, we can gain deeper insights into the algorithm's behavior, particularly concerning the correct identification of rare yet critical events. The outcomes of this research will provide actionable, data-driven insights for building reliable and trustworthy AI systems in the emergency response domain, ensuring that artificial intelligence enhances, rather than compromises, patient outcomes [5]. Future work could extend this study to evaluate the performance of other classifiers on similar imbalanced datasets, offering a broader comparative analysis to guide model selection in critical applications.

References:

1. Wu S. & He S. C., The Impact of Class Imbalance on Machine Learning Classifiers: A Comparative Study. – 2023. – P. 45-50.

2. Li Q. & Zhang Y., Understanding and Mitigating the Effects of Class Imbalance on Naive Bayes Classifiers. – 2022. – P. 112-118.

3. Chawla N. V., Bowyer K. W., Hall L. O. & Kegelmeyer W. P., SMOTE: Synthetic Minority Oversampling Technique. – 2002. – P. 321-331.

4. Brown A., Chen J. & Wang L., Performance of Machine Learning Models in Emergency Medical Systems: A Critical Review. – 2021. – P. 78-85.

5. Miller K. & Jones T., Building Trustworthy AI for Healthcare: Ethical and Technical Considerations. – 2024. – P. 20-25.

UDC 004

Roman Kormysh, Master's Student,
Olena Chyzhmotria, Senior Lecturer,
Iryna Dmytrenko, Senior Lecturer
Zhytomyr Polytechnic State University

THE ROLE OF SYMPTOM SEVERITY IN IMPROVING NAIVE BAYES-BASED FIRST AID DIAGNOSIS ACCURACY

The increasing adoption of machine learning in critical domains, such as first aid and emergency medicine, introduces unique challenges, particularly concerning the quality and nature of training data. Medical datasets are often characterized by severe class imbalance, where common, non-life-threatening conditions vastly outnumber rare but critical emergencies. While the Naive Bayes classifier is prized for its simplicity and speed, this data skew can significantly compromise its predictive accuracy, especially for the vital minority classes, as detailed in a critical review of machine learning models in emergency systems [1].

Standard implementations of the algorithm may learn to ignore rare symptoms that could indicate a serious condition, instead defaulting to the most probable, benign diagnosis. This study proposes and evaluates a method to enhance the Naive Bayes classifier's performance by incorporating symptom severity as a key feature, thereby providing a stronger signal for the model to correctly identify critical first aid situations and improve overall diagnostic reliability [2]. A fundamental vulnerability of the Naive Bayes classifier is its reliance on prior probabilities derived directly from the training data. This reliance can lead to an unacceptably high rate of false negatives for critical cases, a common issue with imbalanced data that has been studied extensively.

By introducing a symptom severity score, we move beyond a simple binary representation of "symptom present" or "symptom absent." Instead, a feature like "pain level" could be graded on a scale, or a symptom like "bleeding" could be qualified as "minor" or "severe." This added layer of information provides the model with a more nuanced understanding of the clinical context, allowing it to correctly weight the importance of certain symptom combinations that may point to a rare, but serious, condition. To test this hypothesis, this research will use a simulated first aid dataset representative of real-world class distributions. The dataset will be carefully annotated to include a severity score for each symptom, allowing for a direct comparison of models. We will train two separate Naive Bayes classifiers: a baseline model trained on the raw, imbalanced data, and a second model that includes the engineered severity feature [3]. The performance of both models

will be critically assessed using metrics beyond simple accuracy, specifically focusing on the recall and F1-score for the minority class, which are crucial for understanding and mitigating the effects of class imbalance on classifiers.

A detailed analysis of the confusion matrices will also be conducted to pinpoint any reduction in false negatives, which is the primary objective of this research. The outcomes of this study hold significant potential for practical application in emergency response systems. If our findings demonstrate that the symptom severity feature substantially improves the Naive Bayes classifier's ability to detect critical conditions, it will provide a simple yet powerful design pattern for developers [4].

Ultimately, this research aims to contribute to the development of more effective automated diagnostic tools in healthcare, where the accuracy of a diagnosis can directly impact patient safety and survival. While this study focuses on the Naive Bayes classifier, the methodology of incorporating a severity feature can be extended to other machine learning models. Future work could explore the application of this approach to more complex algorithms, such as support vector machines or neural networks, to determine if similar gains in performance can be achieved [5].

In conclusion, the data imbalance inherent in first aid datasets is a major obstacle for the Naive Bayes classifier. However, by strategically incorporating symptom severity as a feature, we can provide the model with the necessary information to overcome its biases and make more accurate predictions, a concept similar to over-sampling techniques designed for imbalanced data.

References:

1. Brown, A., & Chen, J. (2021). Performance of Machine Learning Models in Emergency Medical Systems: A Critical Review. *Journal of Medical AI*, 11(2), 78-85.

2. Wu, S., & He, S. C. (2023). The Impact of Class Imbalance on Machine Learning Classifiers: A Comparative Study. *International Conference on Machine Learning Applications*, 45-50.

3. Li, Q., & Zhang, Y. (2022). Understanding and Mitigating the Effects of Class Imbalance on Naive Bayes Classifiers. *Journal of Data Science*, 11(3), 112-118.

4. Miller, K., & Jones, T. (2024). Building Trustworthy AI for Healthcare: Ethical and Technical Considerations. *Health Informatics Review*, 15(1), 20-25.

5. Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic Minority Over-sampling Technique. *Journal of Artificial Intelligence Research*, 16, 321-357.

УДК 004.7

Башманівський М. О., магістрант,
Чижмотря О. В., ст. викладач,
Дмитренко І. А., ст. викладач
Державний університет «Житомирська політехніка»

АРХІТЕКТУРА FULL-STACK ЗАСТОСУНКУ ДЛЯ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ REDDIT З ВИКОРИСТАННЯМ ЛОКАЛЬНИХ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Стрімкий розвиток великих мовних моделей (LLM) відкриває нові можливості для обробки неструктурованого контенту, однак покладання на комерційні хмарні API створює суттєві недоліки, зокрема високу вартість, затримки та ризики конфіденційності. Ці обмеження формують нагальну проблему створення архітектур, здатних безпечно та автономно інтегрувати локально розгорнуті LLM, що особливо актуально для аналізу динамічних платформ, як-от Reddit. Метою даної роботи є представлення багаторівневої архітектури full-stack застосунку, розробленого для інтелектуального аналізу контенту Reddit. Запропонована система реалізує повний цикл оброблення даних — від ініціації запиту та збору до аналітичної інтерпретації та візуалізації, — спираючись на локально розгорнуту велику мовну модель. Такий підхід дозволяє мінімізувати залежність від зовнішніх сервісів і забезпечує контроль над усім процесом обробки даних, що є критично важливим у контексті захисту інформації. Крім того, він відкриває можливості для адаптації моделі під специфіку конкретного домену або завдання.

Для представлення фізичної архітектури та взаємодії компонентів системи була розроблена діаграма розгортання (рис. 1). Вона ілюструє розміщення програмних артефактів на фізичних або віртуальних вузлах. На самому WebServer одночасно розгорнуто декілька ключових процесів, що забезпечують його функціональність. Середовище виконання Node.js / Express API реалізує всю бізнес-логіку, обробку запитів, інтеграцію з API та оркестрацію аналізу. Поруч із ним функціонує локальний AI-сервер LM Studio, що надає доступ до моделі openai/gpt-oss-20b. Важливо, що зв'язок з ним відбувається через локальний інтерфейс http://127.0.0.1:1234, гарантуючи, що дані аналізу не залишають межі сервера. Також на сервері розгорнуто in-memory сховище Redis, яке використовується для кешування проміжних результатів NLP-обробки та керування чергами завдань.

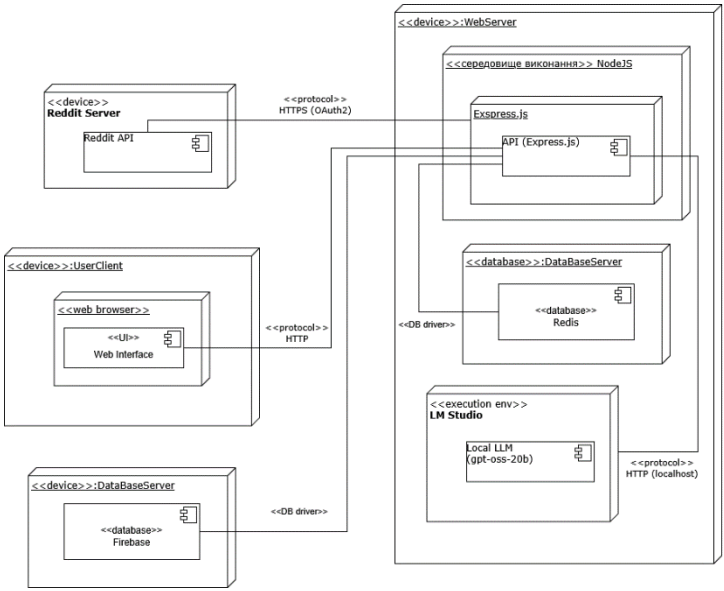


Рисунок 1 – Діаграма розгортання застосунку для інтелектуального аналізу

Зовнішній вузол Firebase Cloud надає два критичні артефакти: Firebase Authentication для безпечної автентифікації користувачів та Firestore для зберігання результатів аналізу. Інший зовнішній вузол, Reddit API, виступає джерелом даних, до якого сервер звертається через протокол OAuth2.

Запропонована багаторівнева архітектура є гнучким рішенням для інтеграції локальних LLM в full-stack застосунки. Ключова перевага полягає у використанні локального AI-двигуна, що гарантує повну конфіденційність даних на відміну від хмарних API [1]. Серверний рівень на Node.js виступає оркестратором повного циклу обробки, від збору даних з Reddit API до збереження результатів у Firebase. Розроблений підхід є життєздатною, безпечною та відмовостійкою моделлю для інтелектуальних систем, орієнтованих на приватність.

Список використаних джерел:

1. Zeng A., Liu J., Zhang H., et al. LLM Application Architectures: A Survey and Design Pattern Analysis. *arXiv preprint,* arXiv:2404.02852, 2024. URL: https://arxiv.org/abs/2404.02852

УДК 004.7

Башманівський М. О., магістрант,
Чижмотря О. В., ст. викладач,
Дмитренко І. А., ст. викладач
Державний університет «Житомирська політехніка»

ГІБРИДНА МЕТОДОЛОГІЯ АНАЛІЗУ КОНТЕНТУ REDDIT: ПОЄДНАННЯ КЛАСИЧНОГО NLP ТА ГЕНЕРАТИВНИХ МОДЕЛЕЙ ДЛЯ УЗАГАЛЬНЕННЯ ТА ВИЯВЛЕННЯ ТОНАЛЬНОСТІ

Аналіз Reddit, як масштабного джерела суспільних настроїв, ускладнений обсягами, динамічністю та неструктурованістю даних. Традиційні методи нездатні впоратися зі складністю мови, сарказмом та контекстуальними нюансами при спробах виявити тональність чи узагальнити дискусії, що вимагає нових, гнучких методологій аналізу.

Існуючі підходи мають суттєві обмеження. Класичні методи NLP, такі як статистичний аналіз (TF-IDF) чи лексикон-орієнтовані підходи до тональності , ефективні для виявлення частотних закономірностей, але демонструють низьку точність при роботі зі складними семантичними явищами та нездатні до абстрактного узагальнення дискусій. З іншого боку, сучасні великі мовні моделі (LLM) чудово розуміють контекст та можуть генерувати змістовні резюме, однак їх пряме застосування до всього масиву сирих даних є обчислювально дорогим та може призводити до втрати фактичної точності без належної "доказової канви".

Метою даної роботи є представлення гібридної методології аналізу, яка вирішує ці проблеми шляхом поєднання сильних сторін обох підходів. Запропонований аналітичний конвеєр використовує класичні NLP-алгоритми для швидкої попередньої обробки, фільтрації та виділення ключових статистичних ознак (n-грам, тем). Далі, ці структуровані дані разом із репрезентативними фрагментами тексту подаються до генеративної моделі, яка виконує високорівневі завдання: абстрактивне узагальнення (TL;DR) та глибоке семантичне визначення тональності. Такий гібридний підхід дозволяє досягти балансу між обчислювальною ефективністю, точністю та глибиною аналізу.

Запропонована методологія ґрунтується на послідовному аналітичному конвеєрі, що поєднує швидкість класичної обробки природної мови (NLP) з семантичною глибиною генеративних моделей. На першому етапі закладається NLP-фундамент. Після збору даних через офіційний Reddit API, весь текстовий контент проходить жорсткий процес попередньої обробки. Цей процес включає

нормалізацію (усунення HTML-артефактів, емодзі, вирівнювання регістру), визначення мови, токенізацію та лематизацію для зменшення варіативності словоформ. Важливою частиною цього етапу є фільтрація шумів: застосовуються евристики та швидкі класифікатори для виявлення та видалення спаму, дублікатів та низькоінформативних повідомлень.

Після очищення база нормалізованих текстів проходить етап статистичного аналізу для формування так званого "профілю" дискусії. На цьому кроці розраховується частотність n-грам (наприклад, зважених за TF-IDF), виділяються ключові фрази та сутності, а також оцінюються базові показники, такі як лексична різноманітність . Результатом цього фундаменту є структурований набір даних: ключові теми, статистичні розподіли та "доказова канва", що складається з найбільш репрезентативних фрагментів тексту. Цей структурований профіль є основою для наступного, інтерпретаційного етапу.

Отримані структуровані дані використовуються для формування "розумного" запиту (промпту) до локальної великої мовної моделі. Замість того, щоб подавати на вхід весь масив сирого тексту, модель отримує комбінований запит, що містить ключові NLP-показники, такі як теми чи ключові фрази, та репрезентативні приклади оригінальних коментарів . При вирішенні задачі узагальнення, LLM, спираючись на надану "доказову канву", генерує змістовне резюме (TL;DR), що зменшує ризик "галюцинацій" моделі . Для аналізу тональності, LLM виходить за межі простих класифікаторів, надаючи більш тонку оцінку емоційного фону та ідентифікуючи сарказм, що важко для класичних методів [1].

Класичний NLP надає LLM фактичну основу, що "заземлює" її генеративні здібності та підвищує точність узагальнень. Водночас LLM збагачує сухі статистичні дані якісною, людсько-читабельною інтерпретацією, надаючи користувачу готові аналітичні висновки та інсайти, а не лише графіки. Крім того, досягається значна обчислювальна ефективність, оскільки основна маса даних обробляється швидкими NLP-алгоритмами, а ресурсоємна LLM залучається лише на фінальному етапі для інтерпретації вже підготовлених даних.

Список використаних джерел:

1. Katta K. Analyzing User Perceptions of Large Language Models (LLMs) on Reddit: Sentiment and Topic Modeling of ChatGPT and DeepSeek Discussions. *arXiv preprint*, arXiv:2502.18513, 2025. URL: https://arxiv.org/abs/2502.18513

УДК 004

Груницький Д. С., магістрант,
Чижмотря О. В., ст. викладач,
Дмитренко І. А., ст. викладач
Державний університет «Житомирська політехніка»

ВИДІЛЕННЯ І СТРУКТУРИЗАЦІЯ КЛЮЧОВИХ ПОНЯТЬ У ТЕКСТОВИХ НАВЧАЛЬНИХ МАТЕРІАЛАХ

У сучасному навчальному середовищі люди потребують нові способи обробки великої кількості тексту [1] для кращого розуміння, запам'ятовування та загалом, навчання. Як всім нам відомо, студенти навчальних закладів, користувачі на різних платформах часто працюють із книгами, статтями або презентаціями, де важливо виділити ключові поняття даного матеріалу. Автоматичне виділення та структуризація ключових слів, термінів і основних ідей допомагає покращити навчальний процес та підвищити його ефективність.

Основна ідея полягає у створенні інструменту, який автоматично аналізуватиме текстовий матеріал різних форматів, таких як книги, статті, документи або презентації. Під час аналізу система використовуватиме спеціальні алгоритми для визначення ключових понять, термінів та інших важливих фраз, які є основою змісту тексту. Виділена інформація не лише буде зібрана, але й упорядкована у структурований формат, що зробить її більш доступною та зрозумілою для будь-якого користувача. Це дозволить значно скоротити час на обробку великих обсягів текстової інформації та спростить ознайомлення з матеріалом.

Для досягнення цієї мети використовуватимуться сучасні методи обробки текстових даних. Зокрема, TF-IDF (Term Frequency-Inverse Document Frequency) [2] допомагає знаходити важливі слова у тексті, відкидаючи непотрібні і виділяючи ті, які краще підходять для розуміння змісту, використовуючи наступні формули:

$$TF(t,d) = \frac{number\ of\ times\ t\ appears\ in\ d}{total\ number\ of\ terms\ in\ d} \quad (1)$$

$$IDF(t) = log\frac{N}{1+df} \quad (2)$$

$$TF - IDF(t,d) = TF(t,d) * IDF(t), \quad (3)$$

де:

t – термін (слово або фраза, що аналізується);

d – окремий документ у колекції;

N – загальна кількість документів у колекції;

df – кількість документів, у яких зустрічається термін t.

Методи токенізації та лематизації допомагають розбити текст на окремі слова й привести слова до базової форми, що полегшує їх подальший аналіз. Додатково буде використовуватись аналіз змісту, щоб знайти основні ідеї та зв'язки в тексті. Ключові поняття будуть згруповані за темами, щоб інформація була чіткою та легкою для розуміння. Загалом, комплексне використання цих методів забезпечить ефективну обробку текстових даних і створення зручного для сприйняття результату.

Практична реалізація інструменту дозволятиме користувачам завантажувати текстові файли у різних форматах (DOC, DOCX, PDF тощо) або вставляти посилання на статті, книги та інші джерела. Система автоматично аналізує завантажений або введений матеріал, виділяє ключові слова, фрази та терміни, а також знаходить основні ідеї та визначення. Отримана інформація обробляється та структурується у зручному форматі, наприклад, у вигляді списку термінів, коротких підсумків або згрупованих термінів за темами. Це дозволятиме користувачам швидко знайти необхідну інформацію та отримати чітке уявлення про основний зміст тексту.

Розроблений інструмент дозволятиме ефективно обробляти великі об’єми тексту автоматично, створюючи структуровані конспекти, виділяти найважливіші терміни та поняття. Це значно спрощує процес засвоєння навчального матеріалу, оскільки користувачам стає легше знаходити необхідну інформацію та отримувати чітке уявлення про зміст документа. Завдяки такому інструменту можна економити час, уникати необхідності переглядати великі тексти та швидко зосередитися на ключових аспектах. Однак є і певні недоліки. Автоматичне виділення інформації може іноді бути неточним, особливо у складних текстах або при використанні специфічної термінології. Також інструмент може не завжди точно визначати терміни та фрази, що впливає на якість підсумованої інформації.

Отже, автоматичне виділення та упорядкування ключових понять допомагає краще обробляти текстові матеріали, роблячи навчання швидшим та зручнішим для будь-якого користувача.

Список використаних джерел:

1. Що таке НЛП? Як це працює, переваги, проблеми, приклади [Електронний ресурс] – Режим доступу до ресурсу: https://uk.shaip.com/blog/what-is-nlp-how-it-works-benefits-challenges-examples/.

2. Understanding TF-IDF for Machine Learning [Електронний ресурс] – Режим доступу до ресурсу: https://www.capitalone.com/tech/machine-learning/understanding-tf-idf/.

УДК 004

Груницький Д. С., магістрант,
Чижмотря О. В., ст. викладач,
Дмитренко І. А., ст. викладач
Державний університет «Житомирська політехніка»

ІНТЕГРАЦІЯ ЧАТ-БОТІВ

У сучасному світі все більше набирає популярності тренд на автоматизацію багатьох процесів. Наразі відбувається прагнення – передати прості та звичайні для людей задачі технологіям, які дозволяють заощадити час та ресурси. Особливо помітною стала тенденція до використання так званих «ботів», тобто програм, які можуть взаємодіяти з користувачами в реальному часі. Замість звичайного терміну «робот», який у багатьох асоціюється з фізичними машинами, слово «бот» стало більш звичним. Для когось це співрозмовник, для інших – це автоматизована програма, яка допомагає вирішувати різні питання швидко та без консультації людей.

На перший погляд, це чудово, але вони також мають свої переваги та недоліки, насправді, без цього нікуди, і це нормально. Чат-боти [1] мають низку значних переваг, що дозволяє пояснити їхню популярність. По-перше, вони працюють 24/7 без необхідності відпочинку, як цього потребує людина для продуктивної праці. Це дає користувачам постійний доступ до інформації та послуг. По-друге, розроблені алгоритми, за якими працюють боти, дозволяють швидко обробляти запити та надавати відповіді без затримок. Це значно покращує користувацький досвід та підвищує якість та ефективність обслуговування. Однак, як було сказано раніше, є й свої недоліки. По-перше, боти часто не здатні коректно обробляти складні або нестандартні запити, що призводить до необхідності втручання операторів. По-друге, вони не можуть замінити емоційний контакт або емпатію, що дійсно важливо при спілкуванні з людьми.. Більшість користувачів віддають перевагу спілкуванню з живими людьми.

З технічної точки зору, чат-боти – це звичайні програми, які інтегруються через API в платформи, такі як Telegram, Viber або в інші масштабні системи та вебсайти. Вони можуть бути написані на різних мовах програмування, зокрема Python, Java, JavaScript тощо, із застосуванням фреймворків, таких як Flask [2], Express.js [3] або Nest.js [4], для спрощення розробки. Система чат-бота [5] складається з обробника запитів, що аналізує вхідні дані, розпізнає відповіді та генерує відповідь (рис. 1). Для складніших ботів використовується обробка природної мови (NLP [6]) для кращого розуміння тексту. API

дозволяє взаємодіяти з різними зовнішніми сервісами, обмінюватися даними та розширювати можливості бота. Крім того, такі системи часто інтегруються з базами даних для зберігання даних користувачів.

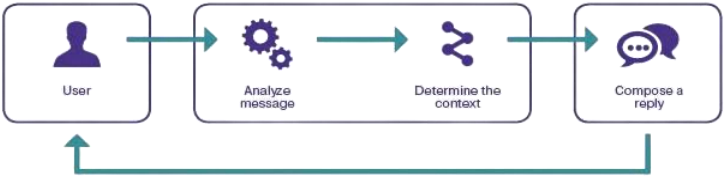


Рисунок 1 – Схема роботи звичайного чат-боту

Зараз чат-боти використовуються в різних галузях. У бізнесі вони допомагають автоматизувати спілкування з клієнтами, прийом замовлень та бронювання. У сфері освіти – сприяють доступу до навчальних матеріалів та проведенню онлайн-тестів. У медичній сфері вони можуть нагадувати пацієнтам про прийом ліків або збирати медичні дані для лікарів. У сфері фінансів вони допомагають клієнтам з інформацією про банківські рахунки, платежі та кредитні умови.

Отже, інтеграція чат-ботів є важливою частиною цифрового розвитку, і їх роль буде тільки зростати в майбутньому. Вони спрощують життя користувачів, автоматизуючи звичайні процеси та задачі. Відтак, чат-боти стають невід'ємною частиною нашого життя.

Список використаних джерел:

1. Що таке чат-бот: секрети використання та основні переваги для бізнесу [Електронний ресурс] – Режим доступу до ресурсу: https://helpcrunch.com/blog/uk/shcho-take-chat-bot/.

2. Flask [Електронний ресурс] – Режим доступу до ресурсу: https://flask.palletsprojects.com/en/stable/.

3. Express.js [Електронний ресурс] – Режим доступу до ресурсу: https://expressjs.com/uk/.

4. Nest.js [Електронний ресурс] – Режим доступу до ресурсу: https://nestjs.com/.

5. How chatbots benefit higher education [Електронний ресурс] – Режим доступу до ресурсу: https://www.ellucian.com/blog/how-chatbots-benefit-higher-ed.

6. What is natural language processing (NLP)? [Електронний ресурс] – Режим доступу до ресурсу: https://www.coursera.org/articles/natural-language-processing.

УДК 004

Груницький Д. С., магістрант,
Чижмотря О. В., ст. викладач,
Дмитренко І. А., ст. викладач
Державний університет «Житомирська політехніка»

СИСТЕМА СТВОРЕННЯ ПЕРСОНАЛІЗОВАНИХ КОНСПЕКТІВ

Сучасний світ характеризується стрімким розвитком інформаційних технологій та постійним зростанням кількості доступної нам інформації. У цих умовах виникає потреба у нових підходах до навчання, які допомагатимуть користувачам швидко знаходити, структурувати й засвоювати знання відповідно до їхніх індивідуальних потреб. Традиційні методи навчання часто не враховують особливості кожного користувача та не дозволяють ефективно працювати з великим обсягом інформації [1]. Персоналізовані навчальні системи, які адаптують всю необхідну інформацію під конкретного користувача, є актуальними та необхідними інструментами для підвищення ефективності навчального процесу. Враховуючи це, тема «Система створення персоналізованих конспектів» є важливою та актуальною як з наукової точки зору, так і для практичного використання в освітніх процесах.

Дана тема є досить розповсюдженою та популярною, але те, що буде виконувати ця система не є тією «звичайною темою, яка буде допомагати дітям або студентам в навчанні». Система має стати універсальним інструментом для користувачів, допомагаючи їм знаходити, чітко формулювати та структурувати інформацію, яку вважатиме за потрібне.

Щодо архітектури, для створення системи було обрано мікросервісну архітектуру (рис.1) [2]. Це архітектурний стиль, у якому додаток складається з низки незалежних сервісів, що працюють окремо та взаємодіють між собою за допомогою швидких і простих протоколів передачі даних, таких як HTTP. Такий підхід зробить систему більш легкою та гнучкою для подальшого розвитку.

На сьогодні існує декілька платформ і додатків, які пропонують персоналізовані підходи до навчання. Найбільш поширеними серед них є **Coursera**, **Khan Academy** та **Duolingo**. Ці платформи використовують алгоритми адаптивного навчання для підбору матеріалів відповідно до рівня знань та інтересів користувачів. Однак ці системи переважно орієнтовані на задані набори курсів і не дозволяють користувачам самостійно додавати власні навчальні матеріали.

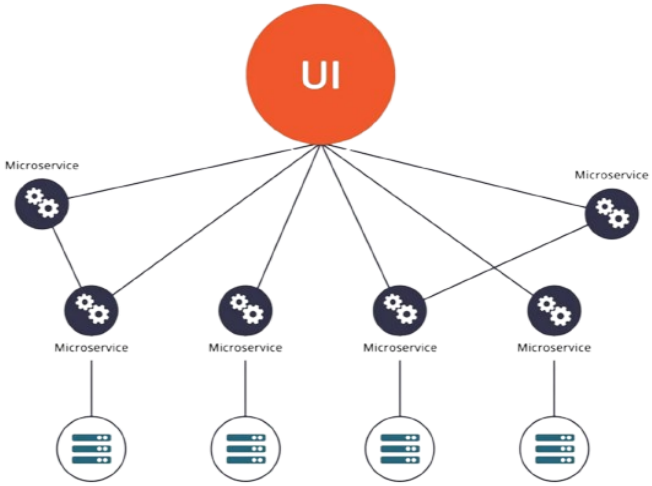


Рисунок 1 – Схема роботи мікросервісної архітектури

Інші платформи, такі як **Notion** або **Obsidian**, дозволяють користувачам самостійно створювати і структурувати інформацію, але вони не пропонують можливості автоматичної обробки навчальних матеріалів або виділення ключових термінів і визначень.

Результатом дослідження повинна стати система, яка поєднуватиме функції автоматизованої обробки текстових даних і надання користувачу зручних інструментів для доступу до навчальної інформації. Система дозволить користувачам завантажувати документи або вводити посилання на джерела (статті, книги, презентації), після чого здійснюватиметься аналіз вмісту, виділення ключових термінів та визначень. Отримані результати можна буде завантажити на пристрій у вигляді структурованого тексту. Ця система стане новим інструментом, який полегшить доступ до знань і зробить навчальний процес більш ефективним та простішим.

Список використаних джерел:

1. Великі дані [Електронний ресурс] – Режим доступу до ресурсу: https://termin.in.ua/big-data-velyki-dani/.

2. The What, Why, and How of a Microservices Architecture [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/hashmapinc/the-what-why-and-how-of-a microservices-architecture-4179579423a9.

УДК 004

Shostak Anatoliy, Ph.D., Associate Professor
National Aerospace University «Kharkiv Aviation Institute»

ON MODIFICATION OF THE ALGORITHM FOR CONSTRUCTING AN AVL TREE

The AVL tree data structure is widely used in data processing system software as a height-balanced structure that provides logarithmic speed for search, insertion, and deletion operations [1-3].

Let there be a set of integers S of power N. It is necessary to construct an AVL tree based on S. Classically [1-3], the A1 algorithm for constructing an AVL tree is used for this task, and the construction of the tree depends on the order of the elements in S. In algorithm A1, after inserting the next node, the height balance of the nodes is checked and, if necessary, the tree is balanced in height by means of single and double left and right rotations of the subtrees. The result is an AVL tree with a height of approximately $\log_2 N$. The complexity of such an algorithm for constructing an AVL tree is $O(N\log N)$.

For the sequence SA consisting of elements (1, 2, 3, 4, 5, 6, 7), the AVL tree is shown in Fig. 1, and four left rotations were required to balance it in height.

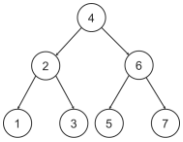


Fig. 1 – AVL tree for a sequence of elements (1, 2, 3, 4, 5, 6, 7)

For the sequence SB (4, 2, 6, 1, 3, 5, 7) of the same numbers, but in a different order, the AVL tree has the same appearance (Fig. 1), but does not require a single rotation during construction. That is, the order of the SB sequence is such that, as a result of inserting keys into the binary search tree, an AVL tree will ultimately be constructed without the need to check the balance of nodes and left and right rotations.

A distinctive feature of SB-type sequences is that the median of the entire sequence is in the first place, the median of the left subtree is in the second place, the median of the right subtree is in the third place, and so on. That is, if you preprocess the initial sequence before constructing the AVL tree and obtain an SB-type key sequence, the result will be the construction of an AVL tree without the need to check the balance of nodes after each insertion and perform left and right rotations.

It is proposed to use algorithm A2 to construct the AVL tree, which performs the following steps:

1) based on the set of integers S, obtain the ascendingly sorted sequence S1 (the complexity of such sorting can be O(N), for example, for the counting sort algorithm),

2) select the median of the sorted sequence S1 and place it in the first position in the sequence S2 — this will later be the root of the AVL tree being constructed (the complexity of searching for the median in this case is O(1)), the left part of S1 relative to the median forms the nodes of the left subtree of the AVL tree, and the right part of S1 relative to the median forms the nodes of the right subtree,

3) recursively continue selecting medians for the left and right parts of S1 and thus form a sequence S2 of N integers (the complexity of forming S2 is O(N)).

4) construct an AVL tree based on S2 (obviously, it is not necessary to check the balance of nodes and balance by height for S2).

The complexity of constructing an AVL tree using algorithm A2 is also O(NlogN), but algorithm A2 has a significantly lower multiplicative constant for the following reasons. Algorithm A2 uses a more efficient and optimised sorting operation compared to the more complex and slower operations of traversing the tree, checking its balance, recursive returns to update the tree balance, and the complex rotation logic of algorithm A1. Algorithm A2 also uses faster access to data in a dense array compared to access via links to tree nodes, which may be scattered across different memory locations, in algorithm A1.

References

1. Cormen Thomas H., Leiserson Charles E., Rivest Ronald L., Clifford Stein. Introduction to algorithms: / Thomas H Cormen. – MIT Press, 2022. – 1312 pp. ISBN: 9780262046305

2. Brown Russell A. Comparative Performance of the AVL Tree and Three Variants of the Red-Black Tree. Software: Practice and Experience, 2025, Vol. 55(9). P. 1607-1615. https://doi.org/10.1002/spe.3437

3. Bounif L., Zegour D. Toward a Unique Representation for AVL and Red-Black Trees. Computación y Sistemas, 2019, Vol. 23, No. 2, P. 435–450. https://doi.org/10.13053/cys-23-2-2840

УДК 004.8

Кирилова Є. В., магістрант,
Шушура О. М., д.т.н.,
Соломаха С. А., к.е.н.
Державний університет інформаційно-комунікаційних технологій

АНАЛІТИЧНИЙ ОГЛЯД СУЧАСНИХ АРХІТЕКТУР DNN, CNN, RNN ТА TRANSFORMER У ЗАДАЧАХ РЕГРЕСІЇ ТА КЛАСИФІКАЦІЇ

Зростання складності реальних даних, їх багатовимірність та нелінійність зумовлюють потребу у моделях, здатних забезпечувати високу точність апроксимації залежностей у задачах класифікації та регресії. Сучасні архітектури глибоких нейронних мереж (Deep Neural Networks, DNN) демонструють значні переваги у моделюванні складних функцій та роботі з великими наборами даних. Особливої актуальності набувають такі архітектури, як згорткові нейронні мережі (Convolutional Neural Networks, CNN), рекурентні мережі (Recurrent Neural Networks, RNN), мережі LSTM, а також моделі на основі механізму самоуваги (Transformers) [1]. Необхідність визначення ефективності цих архітектур у регресійних і класифікаційних задачах різних типів мотивує виконання комплексного аналітичного огляду.

Метою дослідження є порівняльний аналіз сучасних архітектур нейронних мереж, визначення їх внутрішньої структури, обчислювальних властивостей, здатності до узагальнення, ефективності у задачах з різними типами даних, а також виокремлення перспектив розвитку та застосування.

Глибокі нейронні мережі (DNN) — це багатошарові моделі прямого поширення сигналу, що містять кілька прихованих шарів з нелінійними функціями активації та здатні апроксимувати складні функції завдяки властивості універсального наближення.

Згорткові нейронні мережі (CNN) — архітектури, створені для обробки просторово структурованих даних. Основою CNN є згорткові шари, що виконують фільтрацію з використанням спільних ваг, що значно зменшує кількість параметрів та підвищує стійкість до варіацій у вхідних даних. CNN забезпечують автоматичне виділення ознак різного рівня, що дозволяє ефективно розв’язувати задачі комп’ютерного зору та обробки сигналів [2].

Рекурентні нейронні мережі (RNN) моделюють залежності у послідовних даних за допомогою внутрішнього стану, який оновлюється покроково. Основним недоліком класичних RNN є

проблема зникання градієнтів, що ускладнює їх застосування для довгих послідовностей.

LSTM (Long Short-Term Memory) покращують базову архітектуру RNN завдяки гейтовим механізмам, що дозволяють зберігати релевантну інформацію протягом тривалих інтервалів. Це забезпечує високу точність у задачах прогнозування часових рядів, обробки текстів та визначення трендів [3].

Трансформерні архітектури (Transformers) замінили рекурентність механізмом самоуваги (self-attention). Структура Encoder–Decoder дозволяє моделювати глобальні залежності між елементами послідовності та паралелізувати обчислення. Механізм Multi-Head Self-Attention забезпечує аналіз даних у кількох підпросторах ознак, що робить трансформери ефективними у задачах класифікації й регресії, особливо на великих масивах даних.

Сучасні модифікації, такі як ResNet, дозволяють стабілізувати навчання глибоких CNN, тоді як оптимізатори AdamW покращують збіжність DNN. Використання Batch Normalization та Dropout знижує ризик перенавчання. У регресійних задачах найвищу точність демонструють трансформери, а у класифікаційних задачах зображень — CNN. У задачах з вираженими часовими залежностями LSTM зберігають значну перевагу.

Аналіз показує, що кожна архітектура нейронних мереж має власні оптимальні області застосування. CNN переважно використовуються для просторових даних, LSTM — для послідовностей, DNN — для табличних даних, а Transformers — для задач з глобальними залежностями та великими обсягами інформації. Перспективи подальших досліджень пов’язані з оптимізацією обчислювальної складності трансформерних моделей, створенням гібридних архітектур CNN–Transformer та впровадженням методів pruning, quantization і distillation для зменшення ресурсних витрат.

Список використаних джерел:

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016. 800 p..

2. LeCun Y., Bengio Y., Hinton G. Deep learning. Nature. 2015. Vol. 521, No. 7553. P. 436–444.

3. Hochreiter S., Schmidhuber J. Long short-term memory. Neural Computation. 1997. Vol. 9, No. 8. P. 1735–1780.

УДК 004

Рябко О.Д., здобувач,
Єфремов Ю. М., к.т.н., доцент
Державний університет «Житомирська політехніка»

АКТУАЛЬНІСТЬ РОЗРОБКИ СИСТЕМИ УПРАВЛІННЯ ЗАКЛАДАМИ ХАРЧУВАННЯ

На сьогоднішній день, сфера громадського харчування посідає одне з найдинамічніших галузей світової економіки. За даними компанії Grand View Research, світовий ринок програмного забезпечення для управління ресторанами у 2023 році оцінювався у понад 5,6 мільярда доларів США, а до 2030 року передбачається його зростання до 13,4 мільярда доларів США. Така динаміка вказує на те, що зараз відбувається активне впровадження цифрових технологій у галузі харчової індустрії. І як стверджує платформа SUPY, сучасні інновації у мережах ресторанів цілеспрямлені на автоматизацію багатьох процесів, аналітику даних та використання штучного інтелекту, що допомагатиме покращувати вже існуючі аспекти та розвивати їх у довгостроковій перспективі.

Український комерційна діяльність також демонструє поступове зростання у стійкість і вміння адаптуватися до сучасних умов. За інформацією Forbes Україна, кількість кав'ярень зросла на 35 % , якщо порівнювати 2021 та 2024 роки, а разом із цим зросла чисельність закладів з фастфудом приблизно на 15%. Ці аспекти свідчать про гнучкість та високу адаптивність бізнесів в нашій країні.

Не дивлячись на позитивні тенденції , значна частина закладів харчування досі стикається з труднощами через використання застарілих та не інтегрованих між собою програмних рішень, що ускладнюють роботу, а особливо внутрішні процеси закладу. Тому створення інноваційної системи управління, яка здатна об'єднати всі фундаментальні процеси в одному рішенні, обробляти дані і слідкувати за поточною інформацією, а також підвищувати роботу персоналу і обслуговування клієнтів, є надзвичайно актуальним завданням. На ринку праці вже існують такі автоматизовані системи у вигляді хмарних рішень та POS-технологій, які вже активно використовуються великою кількістю підприємців.

У процесі розробки необхідно знайти оптимальне поєднання технологій, яке забезпечить стабільну, гармонійну роботу та взаємодію клієнтської частини, серверного компонента, зручного інтерфейсу та бази даних, відповідно до вимог сучасних систем.

На етапі фронтенд-розробки для створення сучасного, швидкого та інтуїтивно-зрозумілого інтерфейсу слушно обрати React. Так як ця технологія дозволяє оновлювати дані без перевантаження сторінки, що є суттєвим для роботи з замовленнями. Однією з переваг React - підтримка адаптивного дизайну, який підходить для використання системи з ряду різних гаджетів. Для частини бекенду було доречно використати Node.js, що буде забезпечувати стабільну взаємодію між клієнтською частиною та сервером, а поміж цього ще й миттєве реагування на запити. Для збереження даних про замовлення, асортимент та ще додаткової інформації варто використати MySQL, адже вона виступає надійною реляційною базою даних, яка забезпечує безпеку та підтримує аналітичні функції для створення звітів.

Підсумком розробки стане система управління закладами харчування, спрямована на вдосконалення роботи, усіх процесів та підвищення продуктивності підприємств. Розроблене програмне рішення дозволятиме ефективно керувати такими процесами, як: обліком замовлень та контролем їхніх статусів, управління фінансами та персоналом , перевірка складу. Завдяки використанню підходящих сучасних технологій система матиме швидку, надійну роботу та забезпечить зручну та інтуїтивно-зрозумілу взаємодію з інтерфейсом.

Програмне рішення поєднає в собі гнучкість і можливість подальшого впровадження та потенційне розширення функціоналу, відповідно до потреб та запитів відповідних закладів. Використання системи сприятиме ефективнішій організації роботи закладу, покращенню клієнтського обслуговування та дозволить зменшити витрати часу на виконання повторюваних завдань. З часом подібні рішення можуть стати важливою частиною розвитку закладів харчування, допомагаючи їм бути більш сучасними, конкурентоспроможними та стабільними в умовах швидких технологічних змін.

Список використаних джерел:

1. Grand View Research. Restaurant Management Software Market Size, Share & Trends Analysis Report 2023–2030 URL: https://www.grandviewresearch.com/industry-analysis/restaurant-management-software-market (дата звернення: 09.11.2025).

2. SUPY. Fostering Innovation in Restaurant Chains. 2024. URL: https://supy.io/blog/fostering-innovation-in-restaurant-chains/

3. Forbes Україна. Кількість кав'ярень під час війни зросла на 35% – Poster. 2024. URL: https://forbes.ua/news/kilkist-kavyaren-pid-chas-viyni-zrosla-na-35-poster-09052024-21057

УДК 004

Рябко О.Д., здобувач,
Єфремов Ю. М., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ІСНУЮЧИХ СИСТЕМ УПРАВЛІННЯ ЗАКЛАДАМИ ХАРЧУВАННЯ

На сьогодні сфера закладів харчування стрімко розвивається та вдосконалюється аби автоматизувати більшість процесів, щоб задовільнити потреби споживачів. Рівень конкуренції невпинно зростає в даній області, тому власники все більше потребують ефективних програмних рішень з інноваційними підходами спрямованих на автоматизацію. Такі рішення підвищують рівень ефективності роботи закладу та покращують якість обслуговування клієнтів. Тобто, система повинна мати багатофункціональні можливості та бути зручною для користувачів. Програма має приймати та прослідковувати статус замовлення, контролювати запаси й закупівлі, вести точний обліку продажів та фінансів, а також аналізувати вподобання відвідувачів та впроваджувати різні механізми для заохочення. Нині вже існує багато таких систем автоматизації закладів харчування, серед яких є Poster POS та Syrve Україна, які є гарним прикладом для реалізування власної системи.

Poster POS – це сучасна хмарна система управління закладами харчування, вона об’єднує простоту та зручність використання, працює на сучасних гаджетах без потреби використання складного обладнання [1]. Система дозволяє управляти меню, персоналом та базою клієнтів, забезпечує облік продажів та можна прослідкувати за фінансовою складовою, а також інтегрується з сервісами онлайн доставки. Завдяки хмарній структурі системи власник може контролювати роботу закладу в режимі реального часу. На рис. 1 представлено інтерфейс системи Poster POS, який є надзвичайно зручним у способі подання інформації для користувачів.

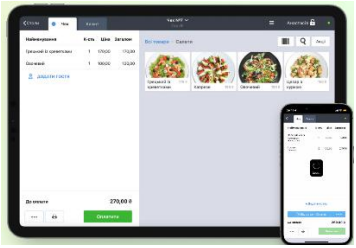


Рисунок 1 – Інтерфейс хмарної системи Poster POS

Syrve Україна – це хмарна платформа, орієнтована на середні та великі підприємства, яка забезпечує ведення та контроль роботи закладів харчування [2]. Основними перевагами є широкий функціонал пов'язаний з прийняттям замовлень, оплатою та роботою з касовими апаратами, підтримкою програми лояльності, а також розвинена аналітика та ведення обліку, підтримка роботи із сервісами доставки, централізований контроль та доступ онлайн. На рис. 2 зображено інтерфейс багатофункціональної системи Syrve Україна.

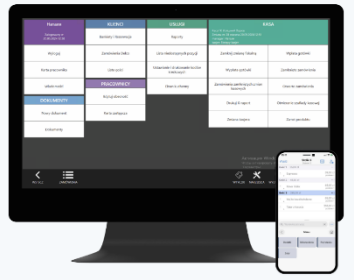


Рисунок 2 – Представлення інтерфейсу системи Syrve Україна

Аналіз обох аналогів продемонстрував, що перелічені системи налічують високий рівень автоматизації необхідних та основних процесів у закладах харчування. Вони дозволяють власникам повноцінно керувати роботою закладу координувати продажі, нововведення, склад та персонал, а для клієнтів швидко отримувати якісне обслуговування ,що формує позитивне враження та спонукає їх повернутися знову.

Poster POS відзначається зручністю для користування з простими налаштуваннями і підходить для невеликих закладів харчування, кав'ярень, тощо. В той час, як Syrve Україна має ширший набір можливостей, дає можливість управління мережею ресторанів та взаємодію з різними онлайн сервісами. Отже, Poster POS орієнтована на швидкість та легкість роботи, а Syrve Україна має більш розширені можливості та набір інструментів для керування бізнесом.

При створені власної систему доцільно поєднати сильні сторони обох аналогів, а також додати аналітичні та CRM-модулі аби отримати максимально зручне та універсальне рішення для підприємств у сфері закладів харчування.

Список використаних джерел:

1. Poster POS. URL: https://joinposter.com/ua (дата звернення: 08.11.2025).
2. Syrve Україна. URL: https://ua.restasystem.com/ (дата звернення: 08.11.2025).

УДК 004.02

Новічков Є. М., магістрант,
Чижмотря О. В., ст. викладач
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ BI-LSTM МОДЕЛІ З МЕХАНІЗМОМ УВАГИ ДЛЯ АВТОМАТИЧНОГО ТЕГУВАННЯ ТЕКСТУ

Для побудови системи автоматичного тегування тексту, нам потрібно побудувати рекурентну нейронну мережу, головна відмінність якої – наявність «пам'яті», що формується через подачу виходу попереднього кроку часу як входу у наступний крок.

Звичайні рекурентні нейронні мережі мають проблему зникнення градієнту, що заважає їм вивчати довготривалі зв'язки між словами. Натомість, Long short-term memory (LSTM), одна із різновидів рекурентних мереж, має структуру комірок пам'яті [1]. Ця структура підходить для завдань, де результат залежить від аналізу семантики всього тексту. Архітектура такої моделі починається з шару вкладень, що подає слова як числові вектори. У цьому векторному просторі слова зі схожими значеннями розташовані ближче одне до одного. Ми можемо скористатися вже навченою моделлю вкладень, даючи змогу моделі узагальнювати синоніми навіть якщо даних для тренування небагато.

Ядром такої архітектури є LSTM комірка, що керує потоком інформації за допомогою трьох механізмів: вхідний вентиль, вентиль забуття та вихідний вентиль. Ці вентилі використовують сигмоїдні функції активації для видачі значень від нуля до одиниці [1]. Вентиль забуття вирішує, яка інформація з попереднього стану комірки більше не є актуальною та має бути відкинута. Вхідний вентиль визначає, яка нова інформація є достатньо значущою для оновлення стану комірки, а вихідний вентиль контролює, яка інформація передається до наступного прихованого стану.

Проте лінійна обробка тексту «зліва направо» не є найкращою для завдань класифікації, де весь документ доступний одночасно. У складних текстах процес визначення значення слова часто залежить від контексту навколо нього. Тому кращою архітектурою для даної задачі є двонапрямлена LSTM (Bi-LSTM). Вона передбачає тренування двох окремих шарів LSTM: прямого та зворотного LSTM, які обробляють послідовність від початку до кінця й від кінця до початку відповідно. На кожному конкретному часовому кроці приховані стани цих двох шарів об'єднуються. Це гарантує, що кінцеве представлення слова містить повний контекст до та після нього [2].

Незважаючи на ефективність Bi-LSTM, її стандартна архітектура має обмеження, відоме як інформаційне вузьке місце (information bottleneck). Мережа стискає семантичний вміст усього документа в кінцевий вектор прихованих станів, що призводить до втрати деталей. Щоб вирішити цю проблему, можна додати механізм уваги. Цей шар дозволяє моделі брати до уваги усі попередні приховані стани, а не лише кінцевий. Механізм працює шляхом обчислення оцінки для кожного часового кроку, які потім нормалізуються для отримання вагових коефіцієнтів уваги [1]. Це дозволяє моделі присвоювати високу значущість найбільш релевантним словам, практично ігноруючи стоп-слова. Це усуває проблему вузького місця та спрощує доступ до

Оскільки тегування тексту є завданням класифікації з кількома мітками, де документ може належати до кількох не взаємовиключних категорій, стандартна softmax функція активації є недоречною. Замість неї краще використати сигмоїдну функцію активації. Вона обчислює кінцеві значення незалежно для кожного класу від нуля до одиниці. Потім застосовується поріг ймовірності для визначення приналежності класу до документа. Щоб зменшити ризик перенавчання алгоритм повинен використовувати шари dropout для випадкового вимкнення нейронів під час навчання, запобігаючи коадаптації, та batch нормалізацію для стабілізації розподілу вхідних даних. Процес навчання повинен керуватися оптимізатором adam для ефективної конвергенції, використовуючи бінарну перехресну ентропію як функцію втрат для належного покарання за помилки.

Використання описаного підходу забезпечує створення ефективної системи автоматичного тегування тексту, що спирається не лише на частотність термінів, а й на їхнє контекстуальне значення.

Список використаних джерел:

1. Liriam Enamoto, Andre R.A.S. Santos, Ricardo Maia, Li Weigang and Geraldo P. Rocha Filho. Multi-label legal text classification with BiLSTM and attention. International Journal of Computer Applications in Technology. 2022. Vol. 68, No. 4. P. 369-378. URL: https://www.researchgate.net/publication/363244291_Multi-label_legal_text_classification_with_BiLSTM_and_attention (дата звернення: 19.11.2025).

2. Understanding Bidirectional LSTM for Sequential Data Processing. URL: https://medium.com/@anishnama20/understanding-bidirectional-lstm-for-sequential-data-processing-b83d6283befc (дата звернення: 19.11.2025).

УДК 004.738.5

Трибюк В.О., здобувач,
Фант М.О., к.філол.н., доцент
Державний університет «Житомирська політехніка»

СТЕК ТЕХНОЛОГІЙ ДЛЯ РЕАЛІЗАЦІЇ ПЛАТФОРМИ ДЛЯ КОСМЕТИЧНИХ КОЛЕКЦІЙ ТА БЛОГУ

Соціальні мережі сьогодні займають значну частку повсякденного часу користувачів. Переглядаючи огляди та рекомендації від контент-крієйторів, люди формують свої споживчі вподобання, створюють списки бажань і приймають рішення щодо вибору косметичних продуктів. За прогнозами аналітичних звітів, глобальний ринок б'юті-індустрії продовжує демонструвати стабільну тенденцію зростання і за оцінками, може досягти близько 677,19 млрд доларів США у 2025 році [1]. Саме тому розвиток технологій у цій сфері є прибутковою можливістю, а створення платформи, де користувачі можуть керувати власними косметичними колекціями, формувати добірки під конкретні потреби та ділитися власним досвідом у форматі блогу, є актуальним напрямком для створення єдиного простору роботи з б'юті-контентом.

Для створення проєкту необхідно визначити, який стек технологій буде використано під час розробки. При цьому варто враховувати такі ключові аспекти, як продуктивність, безпека та стабільність розвитку, адже саме вони забезпечують ефективність, надійність і довговічність програмного продукту.

Для серверної частини обрано ASP.NET Core Web API, оскільки він вирізняється високою продуктивністю, суворою типізацією та надійними механізмами безпеки.

Для зберігання даних вибрано PostgreSQL, що відзначається високою продуктивністю, безпекою, розширюваністю та відповідністю стандарту SQL, що забезпечує стабільну роботу й зручність у розробці застосунку [3].

Для взаємодії бази даних та Web API найкраще підходить фреймворк Entity Framework Core – технологія, що дозволяє працювати з базою даних за допомогою .NET об'єктів (моделей). Вона складається з класів сутностей та об'єкта контексту, який забезпечує зв'язок між моделями й базою даних [2]. EF Core забезпечує спрощене керування даними, потужні можливості запитів, автоматичне відстеження змін і підтримку міграцій, що значно підвищує продуктивність розробки та гарантує цілісність і безпеку даних.

Клієнтську частину застосунку реалізована на основі React із використанням мови програмування TypeScript, що забезпечує швидке й динамічне оновлення інтерфейсу, компонентний підхід до розробки, а також зручність у масштабуванні та повторному використанні коду.

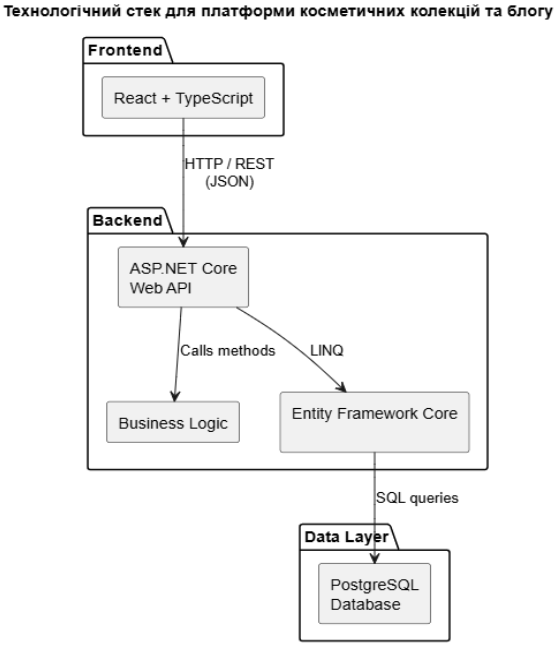


Рисунок 1 – Діаграма технологічного стеку

Отже, обраний стек технологій (рис. 1) – це поєднання безпеки, продуктивності та відповідності сучасним стандартам розробки. Такий підхід дозволяє створювати масштабовані, стабільні й зручні у підтримці вебзастосунок, що відповідають вимогам сучасної індустрії.

Список використаних джерел:

1. Beauty industry statistics 2025 (cosmetic market size). DemandSage [Електронний ресурс] – Режим доступу до ресурсу: https://www.demandsage.com/beauty-industry-statistics/

2. Overview of entity framework core - EF core. Microsoft Learn: Build skills that open doors in your career [Електронний ресурс] – Режим доступу до ресурсу: https://learn.microsoft.com/en-us/ef/core/

3. What is postgresql? Databases explained. Google Cloud [Електронний ресурс] – Режим доступу до ресурсу: https://cloud.google.com/discover/what-is-postgresql

УДК 004.738.5

Козлик С.О., здобувач,
Фант М.О., к.філол.н., доцент
Державний університет «Житомирська політехніка»

ТЕХНОЛОГІЧНИЙ СТЕК ДЛЯ СИСТЕМИ КЕРУВАННЯ ПРОЦЕСАМИ ВИДАВНИЦТВА

У робочих процесах видавництва книг застосовують велику кількість різноманітного програмного забезпечення для вирішення варіативних задач, наприклад, для написання, редагуваннння та форматування текстів книги використовують Microsoft Word або Scrivener, для верстки макету до друку – Affinity Publisher чи Adobe InDesign, а для управління проектами, відслідковування таймлайнів та надання завдань працівникам – Trello, Asana тощо. Така різноманітність інструментів ускладнює роботу над проектом, потребує багато часу на навчання користування ними. Тому було вирішено розробити єдину систему керування процесами видавництва, яка зекономить час та підвищить ефективність роботи у видавництві.

Для реалізації даного застосунку було обрано сучасний технологічний стек, який відповідає актуальним тенденціям розробки, орієнтований на роботу зі значними обсягами текстових матеріалів та забезпечує зручність розробки, підтримки і розширення системи.

У процесі розробки системи керування процесами видавництва було обрано клієнт-серверну архітектуру [1], в якій клієнтська частина взаємодіє з серверною, передаючи запити користувача та отримуючи сформовані на них відповіді від сервера.

Серверна частина застосунку побудована на ASP.NET Core Web API [3]. Він є кросплатформенним, має легку та модульну структуру, зручну маршрутизацію, легко інтегрується з сучасними інструментами для роботи з базами даних, що робить його гарним та надійним варіантом для створення REST API.

Для автентифікації та авторизації у системі використовується ASP.NET Core Identity у поєднанні з JWT, завдяки якому відбувається безпечна передача та перевірка даних користувачів без потреби збереження стану на сервері. Identity відповідає за керування та перевірку особистих даних, відновлення доступу та надає можливість розширювати стандартні моделі і встановлювати ролі для користувачів. Інформацію про користувача та його роль JWT передає у вигляді claims під час взаємодії клієнтської та серверної частин.

Для збереження інформації системи було обрано СУБД PostgreSQL, оскільки вона підтримує транзакції, розширення, індекси та паралельне

виконання запитів, а також забезпечує стабільність і надійне зберігання даних. Її пропонується використовувати для збереження наступної інформації: дані користувачів, видавництв; створені проекти, пов'язані з ними книги, матеріали; встановлені для проектів етапи, додані до них завдання.

Для взаємодії з базою даних використовується Entity Framework Core, яка має об'єктно-орієнтований підхід, гнучку конфігурацію, підтримує створення та виконання міграцій.

Текстові та графічні матеріали вирішено зберігати не в базі даних, а завантажувати у хмарне сховище Amazon S3, тому що це дозволить покращити продуктивність БД. Також хмарні сховища оптимізовані для зберігання файлів великих обсягів, забезпечують автоматичне резервне копіювання та відновлення файлів у разі їхньої втрати чи пошкодження, мають низьку вартість зберігання. У БД будуть зберігатися лише посилання на файли, дати створення, а їх завантаження та видалення буде здійснюватися через API хмарного сервісу.

Для написання інтерфейсу користувача було вирішено застосувати бібліотеку React [2]. Вона має компонентно-орієнтований підхід, тобто React дозволяє створювати та перевикористовувати незалежні компоненти при побудові UI. Також він дозволяє створити віртуальний DOM, тобто спрощену копію DOM; завдяки цьому реальний DOM буде оновлювати і відображати лише ті змінені частини, які виявлені у віртуальному DOM. На відміну від Angular, в React компоненти можна створювати без використання класів, застосовуючи лише функції; дані в них передаються зверху вниз, тобто від батьківського компонента до дочірніх, що зменшує можливість виникнення будь-яких неочікуваних змін стану.

Таким чином, було обрано технологічний стек для розробки системи керування процесами видавництва, який забезпечить гнучкість, масштабованість, безпеку та продуктивність кінцевого продукту. У сукупності ці технології повністю відповідають вимогам системи для реалізації її функціоналу.

Список використаних джерел:

1. Bass L., Clements P., Kazman R. Software Architecture in Practice. 4-те вид. Addison-Wesley Professional, 2021. 464 с.

2. Rippon C. Learn React with TypeScript. 2-ге вид. Packt Publishing, 2023. 474 с.

3. Tanure A. S. ASP.NET Core 9 Essentials. Packt Publishing, 2025. 402 с.

УДК: 004.8:004.4

Бойко О.Р. к.т.н., доцент,
Хрущак С.В. к.т.н., доцент
Вінницький національний аграрний університет

VIBE CODING: СУЧАСНІ ІНСТРУМЕНТИ ТА ПІДХОДИ ДО ПРОГРАМУВАННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасні тенденції у галузі програмування демонструють швидкий перехід від традиційних підходів до методологій, у яких ключову роль відіграють системи штучного інтелекту. Одним із таких напрямів є **vibe coding** - парадигма, що передбачає створення програмного забезпечення не через ручне написання коду, а шляхом формулювання намірів, вимог та очікувань природною мовою. Ключовою перевагою vibe coding є **зниження технічного порогу входу**, скорочення часу на реалізацію типових модулів і пришвидшення ітераційної розробки [1,2].

На даний момент кількість AI-систем, що пропонують можливість vibe кодінга вже налічує більше 100. В той же час, всі такі системи містять велику кількість недоліків, які не дають можливість говорити про те, що робота програмістів буде замінена AI найближчими роками [1].

Нами було проведено дослідження декількох таких систем, зокрема **Base44** та **Loveable.**

Система **Base44** позиціонується як інструмент для комплексного AI-асистованого проєктування, який може працювати з великими проєктами, генерувати цілі модулі та виконувати глибинний рефакторинг.

Система **Lovable** позиціонується як інструмент для надшвидкої AI-орієнтованої розробки, що дозволяє створювати повноцінні веб-застосунки та прототипи «під ключ» на основі коротких текстових інструкцій.

За допомогою вказаних систем було реалізовано два проекти:
- Сторінка-візитка дитячого спортивного клубу з адаптивним дизайном, адмін сторінкою та підтримкою мультимовності.
- Система - планувальник задач та робочих змін для працівників підприємства.

Обидва проекти були успішно реалізовані та впроваджені в робочі процеси замовників. Для обох проектів були використані платні версії vibe систем, але не зважаючи на це – витрачені бюджети значно нижчі ніж оплата спеціаліста за виконання тієї ж роботи. Загальний час витрачений на створення промптів для системи, аналіз отриманих

результатів та виправлення помилок за нашими оцінками в 3 рази менший ніж ідентична робота програміста та тестувальника.

Водночас під час процесу розробки нам довелось стикнутися з рядом недоліків та труднощів, що сповільнювали процес розробки унеможливлювали його для людей не знайомих з основами web розробки.

Нижче наведено основні проблеми, з якими довелося стикнутися:
- Створені продукти розміщуються на серверах системи та використовують загальну базу даних – так звану SuperBase, що унеможливлює редагування даних та створення копії БД на інших ресурсах.

- Модель в результаті роботи часто видає помилки, що потребують виправлення шляхом аналізу вихідного коду і подальших пояснень через промти. На даний момент це унеможливлює роботу з подібними системами людей, що не мають навиків та знань з основ програмування

- Існують великі проблеми з версійністю продукту. Часто система при черговому запиті повністю переписує код певної сторінки чи навіть модуля замість того, щоб виправити невелику помилку а доробити певний функціонал.

Проведене дослідження підтверджує, що системи вайб кодінгу демонструють значний потенціал у прискоренні створення програмних продуктів, зниженні технічного порогу входу та оптимізації рутинних етапів роботи. Разом із тим, виявлені обмеження показують, що vibe coding наразі не може розглядатися як самодостатня технологія для створення складних систем без участі досвідченого спеціаліста. Проблеми з версійністю, помилками генерації, залежністю від центральної інфраструктури та неможливістю роботи без розуміння базових принципів програмування свідчать про незрілість підходу. Це також наголошує на потребі у змішаній моделі роботи, де ключові етапи контролюються людиною, а AI виступає інструментом прискорення, а не повної автоматизації.

Список використаних джерел:

1. Vibe Coding in Practice: Motivations, Challenges, and a Future Outlook. Ahmed Fawzy, Amjed Tahir, Kelly Blincoe. https://doi.org/10.48550/arXiv.2510.00328 (дата звернення: 23.11.2025)

2. The Role of Artificial Intelligence in Software Development: A Literature Review. Nitesh Upadhyaya. https://www.researchgate.net/publication/385781688_The_Role_of_Artificial_Intelligence_in_Software_Development_A_Literature_Review (дата звернення: 23.11.2025)

УДК 004.7

Дрожак В.Т., здобувач,
Єфремов Ю.М., к.т.н.,доцент
Державний університет «Житомирська політехніка»

ВЕБ ПЛАТФОРМА ДЛЯ ПОШУКУ ТА ОРГАНІЗАЦІЇ СТУДЕНТСЬКИХ СТАЖУВАНЬ

У сучасних умовах цифрової трансформації якість підготовки молодих фахівців дедалі більше залежить від можливості здобути практичний досвід під час навчання. Роботодавці оцінюють кандидатів не лише за знаннями, а й за вмінням застосовувати їх на практиці, працювати в команді, адаптуватися та користуватися сучасними технологіями. Стажування дозволяє студентам зануритися в професійну діяльність, закріпити знання, розвинути компетентності та підвищити шанси на успішне працевлаштування.

Попри високий попит на стажування, процес їх пошуку все ще залишається розрізненим і неефективним. Інформація розміщена на різних платформах – від соцмереж до сайтів компаній і порталів вакансій, де важко виокремити саме пропозиції стажувань. Часто бракує засобів для порівняння умов, вимог чи перспектив розвитку. Компанії отримують неструктуровані резюме та витрачають багато часу на первинний відбір і комунікацію.

Освітні установи використовують власні системи практик, але вони не завжди узгоджені з потребами ринку й залишаються частково паперовими або розрізненими між різними інструментами.Усе це підкреслює потребу створення єдиного цифрового середовища, де студенти, роботодавці та координатори практик могли б взаємодіяти швидко, структуровано й зручно. Веб-платформа, що поєднує пошук стажувань, подачу заявок, управління кандидатами та контроль їх проходження, здатна суттєво модернізувати процес.

Студенти отримують доступ до релевантних пропозицій, персональних рекомендацій і можливість зручно подавати заявки та відстежувати їхній статус. Компанії – інструменти для створення описів стажувань, систематизації кандидатів, фільтрації заявок і швидкого прийняття рішень. Координатори можуть переглядати аналітику, відстежувати активність і керувати інформаційним наповненням.

Розробка платформи вимагає аналізу функціональних вимог, вивчення аналогів, вибору сучасних технологій і проєктування архітектури для забезпечення стабільності, безпеки та масштабованості. Вона повинна гарантувати захист даних, високу швидкодію, зручність і адаптивність інтерфейсу. Платформа також сприяє новим моделям

взаємодії між університетами та бізнесом: швидке поширення інформації про програми й проєкти формує довгострокові зв'язки, а прозора система відгуків допомагає студентам обирати стажування з кращими умовами, а компаніям – удосконалювати програми.

Важливою перевагою є використання розширеного пошуку та рекомендаційних алгоритмів, які допомагають студентам швидко знаходити релевантні можливості відповідно до їхніх навичок і цілей. Компанії отримують ефективні інструменти відбору, оцінювання компетентностей та формування бази майбутніх працівників. Для адміністратора платформа слугує універсальним засобом контролю й аналітики – від модерації вакансій до перегляду статистики та динаміки розвитку стажувальних програм.

Під час розробки системи приділено увагу зручності інтерфейсу: простій навігації, швидкій подачі заявок, отриманню оновлень і використанню комунікаційних інструментів. Архітектура проєкту забезпечує підтримку зростання користувачів, інтеграцію зовнішніх сервісів (зокрема авторизацію через соцмережі) та стабільну роботу навіть при високому навантаженні.

Запропонована веб-платформа є сучасним і перспективним рішенням, яке покращує взаємодію між усіма учасниками процесу стажувань. Вона створює прозоре та структуроване цифрове середовище, сприяє розвитку професійного потенціалу студентів, підвищує ефективність компаній і відкриває нові можливості співпраці між освітою та бізнесом.

Список використаних джерел:

1. Марусик О. В. Роль цифрових платформ у професійному розвитку студентів. Інформаційні технології і засоби навчання. 2022. Т. 87, № 5. С. 54–66.

2. Литвин Н. А. Використання веб-платформ для організації виробничої практики студентів. Педагогічний процес: теорія і практика. 2021. № 3. С. 37–43.

3. Філіпенко А. Системи управління практикою студентів на основі цифрових сервісів. Сучасні інформаційні технології в освіті. 2023. № 4. С. 102–109.

4. Європейська комісія. Digital Education Action Plan 2021–2027: Resetting education and training for the digital age. Brussels : EC, 2021. 54p.

УДК 004.7

Волинець А.Ю., магістрант
Вакалюк Т.А., д.пед.н., професор
Державний університет «Житомирська політехніка»

АБСТРАКТНА МАТЕМАТИЧНА МОДЕЛЬ ДЛЯ ПОБУДОВИ РЕАКТИВНИХ СИСТЕМ

Програмні системи, що функціонують на основі автоматичного поширення змін, називають реактивними. Їх суть полягає в тому, що зміна стану одного елемента автоматично ініціює каскад змін у всіх пов'язаних компонентах. Такий підхід дозволяє уникнути явного керування залежностями між окремими частинами системи та істотно спрощує логіку її функціонування.

Реактивність має направлений характер, оскільки передавання змін відбувається від причини до наслідку. Тому в якості абстрактної моделі найчастіше використовується направлений ациклічний граф (DAG). Вершини такого графа відповідають станам, подіям або обчислювальним вузлам, а ребра — причинно-наслідковим зв'язкам між ними. Відсутність циклів у структурі забезпечує однозначність порядку обробки змін та запобігає нескінченним ітераціям оновлення.

Однак, як підкреслюється у дослідженні «*Sheaf Theory: From Deep Geometry to Deep Learning*» (2025), прості направлені графові структури обмежені двома рівнями часткового впорядкування (posetal order) та, таким чином, не здатні повною мірою відобразити складні багаторівневі відносини, що виникають у реальних динамічних системах [1]. У таких структурах практично відсутні механізми для опису контекстуальних, асинхронних та взаємозалежних процесів, які є характерними для сучасних розподілених та реактивних середовищ.

Формально класична реактивна модель на основі DAG описується як

$$G = (V, E), \qquad E \subseteq V \times V,$$

де V — множина станів (вузлів), а E — множина направлених залежностей між ними [2]. У таких графах допускаються лише відносини типу «нижче → вище», що зумовлює обмежений характер часткового впорядкування та знижує здатність моделі представляти складні багатовимірні взаємозв'язки.

При поширенні зміни від вузла v_i до залежного вузла v_j, де $(v_i, v_j) \in E$, новий стан формується на основі локальних даних та попереднього стану джерела. У загальному вигляді це може бути подано як

$$S(v_j) = F(v_j, S(v_i)).$$

Проте така модель не враховує контексту виконання, часових характеристик, рівня активності вузла та інших параметрів, які впливають на реальну поведінку системи.

Для подолання зазначених обмежень кожному вузлу $v \in V$ може бути поставлений у відповідність локальний обчислювальний простір:

$$L(v) = \{S(v), C(v)\},$$

де $S(v)$ — локальний стан вузла, а $C(v)$ — сукупність контекстних параметрів (локальна епоха, версія, умови виконання, пріоритет, активність тощо) [3]. У такому випадку поширення змін визначається не лише структурою графа, а й взаємодією локальних просторів, що дозволяє розглядати багаторівневі та контекстно-залежні відношення.

Запропонений підхід відкриває можливість моделювання більш складних реактивних систем, зокрема:

- систем з асинхронними подіями;
- багатоконтекстних середовищ;
- систем із динамічною зміною структури зв'язків;
- розподілених обчислювальних процесів [4].

Використання локальних контекстів дозволяє уникнути необхідності глобальної синхронізації та підвищує масштабованість моделі за рахунок ізоляції обчислювальних процесів у межах окремих вузлів і підграфів.

Таким чином, сучасні програмні системи, які реалізують реактивність, спираючись виключно на модель направленого ациклічного графа, є обмеженими у своїй здатності адекватно відображати складні причинно-топологічні взаємозв'язки. Розширення класичної моделі шляхом введення поняття локального обчислювального простору створює передумови для побудови більш гнучких, адаптивних та формально обґрунтованих реактивних систем.

Список використаних джерел:

1. Ayzenberg A., Gebhart T., Magai G., Solomadin G. Sheaf theory: from deep geometry to deep learning [Електронний ресурс]. – 2025. – 369 с. (arxiv: 2502.15476). – Режим доступу: https://arxiv.org/pdf/2502.15476, (дата звернення: 24.11.2025).

2. Harel D. Algorithmics: The Spirit of Computing. – 3rd ed. – London: Pearson Education, 2004. – 528 p.

3. Abadi M., Cardelli L. A Theory of Objects. – New York: Springer-Verlag, 1996. – 172 p.

4. Lee E. A., Seshia S. A. Introduction to Embedded Systems: A Cyber-Physical Systems Approach. – Cambridge: MIT Press, 2017. – 560 p.

УДК 004.7

Єфремов Ю.М., к.т.н., доцент,
Коломієць А.О., магістрант
Державний університет «Житомирська політехніка»

ГІБРИДНІ АЛГОРИТМИ У РЕКОМЕНДАЦІЙНИХ СИСТЕМАХ: ПОЄДНАННЯ КОНТЕНТНОГО ТА КОЛАБОРАТИВНОГО ПІДХОДІВ

Рекомендаційні системи давно стали невід'ємною частиною цифрових сервісів, зокрема інтернет-магазинів, стрімінгових платформ і соціальних мереж. Вони допомагають користувачам орієнтуватися у величезних обсягах інформації, пропонуючи саме той контент, який може бути цікавим чи корисним. Такі системи формують персональні добірки фільмів на Netflix, плейлисти на Spotify або товари, схожі на вже переглянуті, на Amazon. У їхній основі лежать алгоритми, що аналізують попередню поведінку користувачів і властивості об'єктів, аби знайти подібність між ними [1].

Попри активний розвиток, класичні методи побудови рекомендацій мають свої обмеження. Контентне фільтрування працює лише тоді, коли система має детальні описи об'єктів, а колаборативне - коли накопичено достатньо даних про користувацькі взаємодії. Проблема "cold start", коли новий користувач або новий товар ще не має історії оцінок, робить ці методи малоефективними в ізольованому вигляді. Для подолання цих труднощів розробники дедалі частіше звертаються до гібридних моделей, які комбінують кілька принципів одночасно [2].

Сучасні рекомендаційні системи все частіше орієнтуються не лише на статичні дані, а й на динаміку зміни інтересів користувача. Люди можуть змінювати свої вподобання залежно від контексту, часу доби, дня тижня або навіть настрою, тому алгоритми мають здатність адаптивно оновлювати моделі й аналізувати короткострокові сигнали. Це дозволяє пропонувати більш релевантний контент, а не тільки базуватися на історичній поведінці, яка може частково втратити актуальність.

Крім того, зростає роль мультиканальних даних, що надходять із різних джерел: пошукових запитів, переглядів сторінок, кліків, поведінки в мобільних додатках, інтеракцій у соціальних мережах тощо. Розуміння того, як користувач пересувається між платформами й способами взаємодії, дає змогу будувати більш комплексний профіль та формувати точні рекомендації навіть у складних сценаріях. Такі системи здатні враховувати не лише окремі дії, а й загальну траєкторію користувацького досвіду.

У наукових дослідженнях останніх років простежується тенденція до створення систем, здатних адаптивно змінювати вагу різних методів залежно від контексту. У статті “Hybrid Recommender Systems: A Systematic Literature Review” [3] зазначено, що такі системи можуть застосовувати як послідовне злиття результатів різних моделей, так і ансамблеве об’єднання, де кожен алгоритм відповідає за певний аспект користувацької поведінки. Наприклад, одна модель прогнозує інтерес до товарів за схожими описами, а інша враховує історію покупок схожих користувачів.

Водночас у практичних реалізаціях усе частіше використовують графові нейронні мережі (GNN), які дозволяють формалізувати зв’язки між користувачами й об’єктами у вигляді графів. Це робить модель чутливою до контексту та структури даних. У роботі “Hybrid Recommendation System using Graph Neural Network and BERT Embeddings” [4] продемонстровано, що комбінація GNN з мовною моделлю BERT здатна враховувати не лише поведінкові дані, а й семантику описів товарів або контенту.

Таким чином, гібридні системи відкривають новий етап еволюції рекомендаційних алгоритмів. Вони дозволяють інтегрувати різнорідні дані, підвищують стійкість моделі до шумів і зменшують залежність від обмежених даних про користувачів. У майбутньому розвиток таких систем сприятиме більш точній персоналізації, а також допоможе компаніям підвищити рівень задоволеності клієнтів та ефективність бізнес-процесів.

Список використаних джерел:

1. Review-based Recommender Systems: A Survey of Approaches, Challenges and Future Perspectives. arXiv preprint arXiv:2405.05562, 2024. URL: https://arxiv.org/abs/2405.05562 (дата звернення: 04.10.2025).

2. A Deep Hybrid Model for Recommendation Systems. arXiv preprint arXiv:2009.09748, 2020. URL: https://arxiv.org/abs/2009.09748 (дата звернення: 04.10.2025).

3. Zamanzadeh Darban Z., Valipour M. H. GHRS: Graph-based Hybrid Recommendation System with Application to Movie Recommendation. arXiv preprint arXiv:2111.11293, 2021. URL: https://arxiv.org/abs/2111.11293 (дата звернення: 06.10.2025).

4. A Survey on Multimodal Recommender Systems. arXiv preprint arXiv:2502.15711, 2025. URL: https://arxiv.org/abs/2502.15711 (дата звернення: 07.10.2025).

УДК 004.7

Єфремов Ю.М., к.т.н., доцент,
Коломієць А.О., магістрант
Державний університет «Житомирська політехніка»

ОПТИМІЗАЦІЯ ТОЧНОСТІ РЕКОМЕНДАЦІЙ ЗА ДОПОМОГОЮ МЕТОДІВ ГЛИБИННОГО НАВЧАННЯ

Сучасний світ продукує гігантські обсяги інформації - від переглядів відео до відгуків у соцмережах. У цьому середовищі глибинне навчання стало одним із найефективніших інструментів для аналізу складних взаємозв'язків і побудови рекомендацій. Алгоритми цього типу здатні не лише виявляти приховані патерни у взаємодії користувачів із контентом, а й навчатися на неструктурованих даних - текстах, зображеннях або аудіо. Це дає можливість створювати багатокомпонентні моделі, які розуміють контекст споживання контенту [1].

У роботі "A Deep Hybrid Model for Recommendation Systems" [2] запропоновано архітектуру, яка поєднує ID-embedding користувачів і товарів із зовнішніми атрибутами (опис, категорія, рейтинг). Такий підхід дозволяє моделі не просто узагальнювати закономірності, а й розпізнавати відмінності між сегментами користувачів. Це особливо важливо для великих маркетплейсів, де поведінка покупців відрізняється залежно від регіону чи демографії.

Окрему увагу дослідники приділяють графовим архітектурам, де користувачі та об'єкти розглядаються як вершини, а їхні взаємодії - як ребра. У статті "GHRS: Graph-based Hybrid Recommendation System with Application to Movie Recommendation" [3] наведено приклад того, як поєднання графових структур із автоенкодером дозволяє суттєво покращити точність рекомендацій у кінематографічній сфері.

Сьогодні все більше уваги приділяється мультимодальним системам, які поєднують різні джерела інформації: опис товару, фотографії, текстові відгуки. У дослідженні "A Survey on Multimodal Recommender Systems" [4] наголошується, що такі моделі забезпечують кращу персоналізацію, оскільки враховують не лише кількісні дані, а й контекстуальну семантику.

Глибинне навчання робить рекомендаційні системи гнучкішими, точнішими та здатними до самонавчання. У перспективі поєднання нейронних мереж із графовими моделями та мультимодальними даними створить передумови для побудови «розумних» систем, що

зможуть прогнозувати потреби користувача ще до того, як він сам їх усвідомить.

Одним із ключових практичних викликів упровадження глибинних моделей у рекомендаційні системи є забезпечення їхньої масштабованості в умовах високонавантажених платформ. Оброблення мільярдів взаємодій потребує не лише складних архітектур, а й оптимізованих механізмів розподілених обчислень, інкрементального навчання та ефективного керування пам'яттю. У цьому контексті дедалі більше уваги приділяється компромісам між точністю та обчислювальною вартістю, а також інтеграції моделей у виробничі середовища, де час відгуку та стабільність мають критичне значення.

Суттєвим аспектом сучасних рекомендаційних систем є підвищення рівня інтерпретованості моделей, що базуються на глибинному навчанні. Попри високу прогностичну здатність, такі моделі часто залишаються малопрозорими, що ускладнює їх використання у сферах, де обґрунтованість рекомендації є критичною передумовою довіри. У зв'язку з цим актуальним напрямом досліджень стає розроблення підходів до пояснюваності, які дають змогу зрозуміти, які фактори вплинули на формування конкретної рекомендації та наскільки ці фактори є валідними.

Узагальнюючи, розвиток рекомендаційних систем на основі глибинного навчання залежить не лише від удосконалення моделей, а й від здатності розв'язувати пов'язані питання масштабованості, прозорості та етичного використання даних. Сукупне врахування цих аспектів формує основу для створення стійких і персоналізованих систем, які можуть адаптивно реагувати на потреби користувачів у сучасному цифровому середовищі.

Список використаних джерел:

1. Review-based Recommender Systems: A Survey of Approaches, Challenges and Future Perspectives. arXiv preprint arXiv:2405.05562, 2024. URL: https://arxiv.org/abs/2405.05562 (дата звернення: 03.10.2025).

2. A Deep Hybrid Model for Recommendation Systems. arXiv preprint arXiv:2009.09748, 2020. URL: https://arxiv.org/abs/2009.09748 (дата звернення: 04.10.2025).

3. Zamanzadeh Darban Z., Valipour M. H. GHRS: Graph-based Hybrid Recommendation System with Application to Movie Recommendation. arXiv preprint arXiv:2111.11293, 2021. URL: https://arxiv.org/abs/2111.11293 (дата звернення: 05.10.2025).

4. A Survey on Multimodal Recommender Systems. arXiv preprint arXiv:2502.15711, 2025. URL: https://arxiv.org/abs/2502.15711 (дата звернення: 08.10.2025).

УДК 004

Обміняний Д. С., магістрант,
Чижмотря О. В., ст. викладач
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ МОДЕЛЕЙ ПРОГНОЗУВАННЯ РИЗИКІВ У ЖИТТЄВОМУ ЦИКЛІ ІТ-ПРОЄКТІВ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

Управління ризиками є однією з ключових складових успішної реалізації ІТ-проєктів, оскільки програмні системи характеризуються складністю, високою вартістю та значним рівнем невизначеності протягом усього життєвого циклу. З огляду на зростання масштабів цифровізації, в умовах жорсткої конкуренції та вимог до якості програмних продуктів, виникає необхідність застосування інтелектуальних методів прогнозування ризиків, здатних підвищити ефективність управлінських рішень.

Традиційні методи оцінювання ризиків базуються на експертних оцінках і статистичному аналізі, однак вони не здатні забезпечити необхідну точність у середовищі, де змінюються пріоритети, вимоги та доступні ресурси. Сучасні дослідження доводять, що застосування інтелектуальних систем дозволяє прогнозувати можливі затримки проєктних робіт, визначати ймовірність перевищення бюджету, втрату якості продукту та виникнення технічних проблем [1].

Інтелектуальні технології у сфері ризик-менеджменту ІТ-проєктів охоплюють використання алгоритмів нечіткої логіки, нейронних мереж, дерев рішень, методів кластеризації та багатокритеріального аналізу. Завдяки навчанню на основі даних попередніх проєктів такі системи враховують закономірності, які складно визначити традиційними способами. Це дозволяє моделювати ризики не лише на визначеному етапі, а й прогнозувати їхній вплив на подальші фази життєвого циклу: аналіз вимог, проєктування, розробку, тестування та супровід [2].

Особливістю ризиків у життєвому циклі ІТ-проєктів є їхня динамічна природа. Наприклад, неякісний аналіз вимог призводить до помилок у проєктуванні, що викликає перевитрати ресурсів під час розробки та затримки при тестуванні. Таким чином, прогнозування має враховувати причинно-наслідкові зв’язки між ризиками. Інтелектуальні системи дають можливість будувати такі взаємозалежності за допомогою моделей, що адаптуються до нових умов та уточнюються зі зростанням обсягів даних.

Серед типових ризиків, що підлягають прогнозуванню, виділяють: технологічні - некоректний вибір технологій, організаційні - неоптимальний розподіл ролей і ресурсів, фінансові - перевищення бюджету, часові - затримки виконання робіт, а також ризики якості, пов'язані з некоректним тестуванням або технічним боргом. Інтелектуальні системи, орієнтовані на автоматизоване прогнозування, здатні ранжувати ризики за рівнем критичності, оцінювати їхню ймовірність та пропонувати стратегії мінімізації. Ці стратегії можуть включати перерозподіл ресурсів, перегляд технічних рішень, зміну пріоритетів завдань або коригування плану проєкту. Завдяки цьому команди отримують можливість оперативніше реагувати на відхилення та приймати обґрунтовані управлінські рішення, зменшуючи ймовірність виникнення критичних ситуацій [3].

Отже, впровадження інтелектуальних систем прогнозування ризиків у життєвому циклі ІТ-проєктів сприяє підвищенню точності аналітики, мінімізації наслідків невизначеності, зменшенню ймовірності критичних відхилень та забезпеченню стійкості процесів розробки. Поєднання експертних підходів з інтелектуальними алгоритмами дозволяє створювати адаптивні системи управління ризиками, які підвищують конкурентоспроможність підприємств та сприяють успішному впровадженню програмних продуктів у динамічному ринковому середовищі.

Крім того, такі системи можуть автоматично виявляти приховані закономірності в даних, що недоступні традиційним методам аналізу. Вони підтримують безперервний моніторинг ключових показників, забезпечуючи оперативне реагування на потенційні загрози. Деякі інтелектуальні моделі також дозволяють проводити симуляції різних сценаріїв, що допомагає оптимізувати стратегії розвитку проєкту. Завдяки цьому управління ризиками стає більш системним та ефективним у довгостроковій перспективі.

Список використаних джерел:

1. Марусей Т. В. Моделі та методи оцінки ризиків в управлінні ІТ-проєктами. Сучасні інформаційні технології в управлінні. 2021. № 2. С. 56–63.

2. Гриценко О. А. Інтелектуальні методи аналізу ризиків у складних інформаційних системах. Київ: НТУУ «КПІ ім. І. Сікорського», 2020. 148 с.

3. Бутченко О. О. Штучний інтелект у системах прогнозування та оцінювання ризиків управління проєктами. Публічне управління та адміністрування у цифровій економіці України. 2022. № 4. С. 90–98.

УДК 004

Обміняний Д. С., магістрант,
Чижмотря О. В., ст. викладач
Державний університет «Житомирська політехніка»

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ПЛАНУВАННЯ ТА ОПТИМІЗАЦІЇ РЕСУРСІВ ІТ-ПРОЄКТІВ

Сучасні ІТ-проєкти характеризуються високою динамічністю вимог, обмеженістю ресурсів та необхідністю прийняття оперативних управлінських рішень у нестабільних умовах. Тому створення та впровадження інтелектуальних систем підтримки прийняття рішень, що здатні автоматизувати планування та оптимізувати використання ресурсів, є однією з актуальних задач у сфері управління інформаційними технологіями.

У зв'язку зі зростанням конкурентності ринку ІТ-послуг ефективне управління ресурсами проєктів набуває вирішального значення для їх своєчасної реалізації, дотримання бюджету та забезпечення необхідної якості продукту. Актуальні дослідження свідчать, що застосування інтелектуальних технологій значно підвищує точність прогнозування, скорочує витрати та сприяє раціональному розподілу людських, матеріальних і часових ресурсів [1].

Системи підтримки прийняття рішень у сфері ІТ-проєктів використовують математичні моделі, експертні системи, алгоритми машинного навчання та методи аналізу багатокритеріальних альтернатив. Ключовою метою таких систем є оцінювання стану проєкту, прогнозування можливих ризиків та автоматичне або рекомендаційне формування оптимальних рішень щодо планування ресурсів.

Сучасні інструменти забезпечують інтеграцію з системами управління проєктами, що дозволяє оперативно отримувати актуальні дані. Вони також підтримують візуалізацію ключових показників ефективності, що допомагає менеджерам швидше реагувати на зміни. Системи здатні враховувати архівні дані для побудови точніших прогнозів. Завдяки цьому прийняття рішень стає більш обґрунтованим.

Інтелектуальні системи можуть аналізувати структуру задач, складність програмних модулів, рівень кваліфікації виконавців, а також залежності між операціями. Це дає змогу підвищити точність оцінювання тривалості робіт, визначити критичні шляхи, а також збалансувати навантаження між членами команди. Важливою особливістю таких систем є можливість навчання на основі

накопичених даних, що дозволяє поступово підвищувати точність рішень [2].

Одним із ключових напрямів оптимізації ресурсів в ІТ-проєктах є застосування багатокритеріальних моделей, які враховують не лише вартісні та часові показники, але й ризики, пріоритетність завдань, компетенції виконавців та ступінь невизначеності зовнішніх факторів. У вітчизняних дослідженнях наголошується, що використання таких моделей сприяє мінімізації людського фактора, зменшенню помилок планування та підвищенню ефективності управлінських рішень [3].

Найбільш поширеними проблемами у плануванні ресурсів ІТ-проєктів є: неточне оцінювання трудомісткості завдань, недооцінювання ризиків, перевантаження виконавців, нерівномірність розподілу робочого часу та неефективне використання бюджету. ІСППР дозволяє усунути зазначені недоліки шляхом застосування адаптивних механізмів оцінювання, автоматизації аналітичних процесів й побудови прогнозних моделей з урахуванням реальних даних попередніх проєктів.

Таким чином, використання інтелектуальних систем підтримки прийняття рішень у процесі планування й оптимізації ресурсів ІТ-проєктів сприяє підвищенню ефективності управління, зменшенню проєктних ризиків, забезпеченню збалансованого розподілу ресурсів та досягненню заданих показників якості. Для максимізації результатів доцільним є комбіноване застосування математичних методів, аналітичних моделей та інтелектуальних технологій, а також постійне оновлення баз знань і адаптація систем до змін у проєктному середовищі.

Застосування описаних підходів забезпечить оптимізацію проєктних ресурсів, підвищить точність планування та сприятиме успішній реалізації ІТ-проєктів у конкурентних умовах.

Список використаних джерел:

1. Системи і методи підтримки прийняття рішень. П. І. Бідюк, О. Л. Тимощук, А. Є. Коваленко, Л. О. Коршевнюк. Київ: КПІ ім. Ігоря Сікорського, 2020. 259 с.

2. Інтелектуальні системи підтримки прийняття рішень. Київ: Національна академія управління при Президентові України, 2016. 188 с.

3. Запорожець Т. В. Застосування інтелектуальних технологій та систем штучного інтелекту для підтримки прийняття управлінських рішень. Публічне управління та регіональний розвиток. 2020. № 2. С. 113–120.

УДК 004.7

Лупашина А.А., здобувач,
Фант М.О., к.філол.н., доцент,
Громський О.О., асистент,
Нерода С.І., асистент
Державний університет «Житомирська політехніка»

АРХІТЕКТУРА ТА ТЕХНІЧНА РЕАЛІЗАЦІЯ ВЕБ-СИСТЕМИ УПРАВЛІННЯ СТУДЕНТСЬКИМ ГУРТОЖИТКОМ

Розроблення сучасних веб-систем потребує поєднання формальних методів моделювання, гнучких архітектурних рішень та технологій, орієнтованих на масштабованість і безпеку. Система управління студентським гуртожитком є прикладом складної предметної області, де необхідно координувати численні взаємодіючі сутності: студентів, кімнати, гуртожитки, адміністративний персонал, заявки, бронювання та технічне обслуговування. Коректне математичне моделювання таких процесів дозволяє створити структуровану та передбачувану архітектуру програмного забезпечення.

На етапі проєктування виконано декомпозицію предметної області на підсистеми та побудовано UML-діаграми відповідно до стандартів OMG. Діаграма прецедентів описує ролі та сценарії взаємодії (реєстрація студента, бронювання кімнати, управління поселеннями, обробка заявок). Діаграма класів формалізує структуру сутностей із чітким виділенням атрибутів, асоціацій та обмежень цілісності. Діаграми активностей та послідовності дозволили сформувати математичну модель потоків даних і логічних станів системи, що мінімізує можливість виникнення суперечностей у бізнес-логіці.

На рисунку 1 наведено приклад UML діаграми прецедентів.

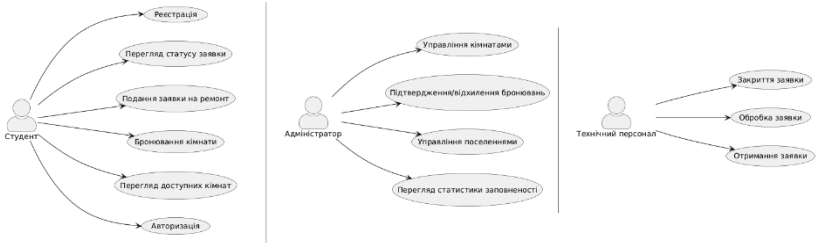


Рисунок 1 – Діаграма прецедентів системи управління гуртожитком

Архітектура системи реалізована у відповідності до принципів багаторівневого (Layered) та модульного підходу. Серверна частина побудована на NestJS, який забезпечує інверсію залежностей, модульність та суворе структурування бізнес-логіки. Система використовує RESTful API, а в перспективі передбачена можливість інтеграції GraphQL для оптимізації вибірок даних. Для зберігання даних обрано PostgreSQL, яке поєднує ACID-властивості, підтримку транзакцій, складні індекси та JSONB-поля для змішаних моделей даних. Взаємодія із СУБД реалізована через TypeORM, що забезпечує автоматичні міграції, lazy/eager loading та репозиторний підхід.

Для логування та моніторингу застосовано Winston і Prometheus, що дозволяє відслідковувати продуктивність, помилки та поведінку системи під навантаженням. У межах математичного аналізу продуктивності виконано оцінку часової складності основних операцій, зокрема пошуку доступних кімнат та оптимізації розподілу студентів за критеріями (курс, факультет, статус пільги).

Фронтенд реалізовано з використанням React, що дозволяє впроваджувати компонентний підхід та декларативну логіку побудови інтерфейсу. Для керування станом можуть бути використані Redux Toolkit або Zustand, залежно від складності глобальної логіки. Для оптимізації рендерингу застосовуються React.memo та динамічне завантаження модулів. Комунікація з сервером реалізована через Axios, а роутинг — за допомогою React Router 6.

Інтеграція формальних методів моделювання, сучасних JavaScript-технологій та архітектурних патернів дозволяє створити масштабовану, продуктивну й безпечну систему. Запропонована архітектура може бути розширена за рахунок мікросервісного підходу, контейнеризації у Docker та оркестрації через Kubernetes, що відкриває можливість адаптації системи для великих освітніх комплексів.

Список використаних джерел:

1. TypeORM Official Documentation. TypeORM Team [Електронний ресурс] – Режим доступу до ресурсу: https://typeorm.io

2. Kubernetes Documentation. Cloud Native Computing Foundation [Електронний ресурс] – Режим доступу до ресурсу: https://kubernetes.io/docs/

3. Design patterns: elements of reusable object-oriented software. Gamma E., Helm R., Johnson R., Vlissides J. [Електронний ресурс] – Режим доступу до ресурсу: https://www.oreilly.com/library/view/design-patterns/0201633612/

УДК 004.7

Харченко Ю.В., магістрант,
Вакалюк Т.А., д.пед.н., професор
Державний університет «Житомирська політехніка»

ПРОБЛЕМА ХОЛОДНОГО СТАРТУ В РЕКОМЕНДАЦІЙНИХ АЛГОРИТМАХ ДЛЯ КНИЖКОВИХ ВЕБ-ДОДАТКІВ

У сучасному цифровому середовищі користувачі зіштовхуються з великою кількістю інформації, зокрема з безліччю книжкових видань у електронному форматі. Рекомендаційні системи стають важливим інструментом для подолання інформаційного перевантаження, тому що вони допомагають користувачам швидко знаходити літературу, що відповідає їхнім інтересам та потребам [1]. Завдяки використанню алгоритмів машинного навчання такі системи формують персоналізовані добірки книг, що значно покращує користувацький досвід і підвищує ефективність пошуку контенту.

У той же час однією з найсуттєвіших складнощів у розробці таких систем є так звана проблема холодного старту. Це ситуація, коли алгоритм не володіє достатнім обсягом даних для формування точних і персоналізованих рекомендацій. Наприклад, коли користувач вперше взаємодіє з платформою, система ще не знає його вподобань, а тому не може створити релевантні рекомендації.

Проблема холодного старту є типовою для систем, які тільки починають накопичувати дані про користувачів або контент. Вона проявляється у трьох основних формах: коли у системі з'являється новий користувач, новий елемент або нова сама система. У випадку нового користувача платформа не має історії його дій, оцінок чи відгуків, тому не може точно визначити коло його інтересів. Якщо ж додається нова книга, то алгоритм не має достатньої кількості оцінок чи відгуків, щоб зрозуміти яким користувачам вона може бути цікавою. Проблема нового середовища виникає тоді, коли вся система перебуває на початковій стадії і база даних ще недостатньо наповнена для ефективного навчання моделей [2].

Особливо ця проблема відчувається у книжкових веб-додатках, орієнтованих на персоналізацію. Це пов'язано з тим, що рекомендаційні алгоритми часто базуються на колаборативній фільтрації, яка вимагає значного обсягу даних про взаємодії користувачів з контентом. У таких випадках результати рекомендацій можуть бути неточними або занадто

загальними, що знижує рівень задоволеності користувачів, лояльність до платформи та частоту повторних відвідувань.

Для подолання проблеми холодного старту застосовуються різні підходи. Одним із найефективніших вважається гібридизація алгоритмів, тобто поєднання контентно-орієнтованих і колаборативних методів. Контентна фільтрація використовує характеристики самих книг, наприклад жанр, автора, ключові слова, опис або тематичні категорії. Це дозволяє формувати початкові рекомендації навіть без наявності оцінок користувачів. Колаборативна фільтрація, у свою чергу, поступово підвищує точність результатів у міру накопичення даних про вподобання та поведінку читачів.

Важливу роль у вирішенні цієї проблеми відіграють і методи машинного навчання, у тому числі і технології обробки природної мови, які дозволяють аналізувати описи книг, відгуки користувачів і створювати семантичні зв'язки між творами. Такі алгоритми допомагають будувати змістовніші моделі подібності між книгами, що забезпечує більш точні рекомендації навіть за мінімальної кількості даних.

Деякі сучасні дослідження також пропонують використання методів глибокого навчання для автоматичного вилучення ознак із текстових описів або метаданих. У поєднанні з гібридними методами такі системи здатні динамічно адаптуватися до нових користувачів і контенту, що значно зменшує вплив холодного старту.

Таким чином, проблема холодного старту залишається однією з головних перешкод у створенні персоналізованих рекомендаційних систем для книжкових платформ. Її ефективне вирішення можливе шляхом комбінування різних підходів до рекомендацій, використання додаткових джерел даних, впровадження гібридних алгоритмів і методів глибокого навчання. Це дозволяє підвищити точність рекомендацій, покращити користувацький досвід і забезпечити індивідуальний підхід до кожного читача навіть на початкових етапах роботи системи.

Список використаних джерел:

1. Zhang, W., Bei, Y., Yang, L., Peng Zou, H., Zhou, P., Liu, A., Bu, J.: Cold-Start Recommendation towards the Era of Large Language Models (LLMs): A Comprehensive Survey and Roadmap. 2025. arXiv preprint arXiv:2501.01945. URL: https://arxiv.org/abs/2501.01945

2. Panteli, A., Boutsinas, B.: Addressing the Cold-Start Problem in Recommender Systems Based on Frequent Patterns. 2023. Algorithms, Vol. 16, No. 4: pp. 182. URL: https://www.mdpi.com/1999-4893/16/4/182

УДК 004.7

Харченко Ю.В., магістрант,
Вакалюк Т.А., д.пед.н., професор
Державний університет «Житомирська політехніка»

ГІБРИДНІ РЕКОМЕНДАЦІЙНІ АЛГОРИТМИ ДЛЯ ПЕРСОНАЛІЗОВАНОГО ПІДБОРУ КНИЖОК

У сучасних веб-додатках для персоналізованого підбору книжок важливу роль відіграють рекомендаційні алгоритми, які здатні аналізувати великі обсяги даних і пропонувати користувачам відповідний контент. Різноманітність літературних жанрів, різна кількість відгуків та оцінок користувачів роблять задачу підбору оптимальних рекомендацій досить складною. Традиційні алгоритми, які застосовуються в таких системах, зазвичай поділяються на два основні типи: контентно-орієнтовані та колаборативні.

Контентно-орієнтовані підходи аналізують властивості книг, такі як жанр, автор, опис або ключові слова, і на основі цього пропонують користувачу схожі твори. Однак вони не враховують соціальний контекст, спільні вподобання інших користувачів або тенденції популярності, що може обмежувати якість рекомендацій, особливо якщо користувач прагне знайти щось несподіване або нове.

Колаборативна фільтрація, навпаки грунтується на поведінці інших користувачів та їхніх оцінках, формуючи рекомендації на основі схожості вподобань. Вона здатна виявляти приховані закономірності, які важко помітити при контентному аналізі. Проте для ефективної роботи колаборативних методів потрібні великі обсяги даних про користувачів і їхні взаємодії, що створює проблему на ранніх етапах запуску платформи або для нових користувачів. Через ці обмеження жоден із традиційних підходів не є універсальним і не може забезпечити стабільно високий рівень персоналізації. Саме тому все більшої популярності набувають гібридні рекомендаційні системи, які поєднують переваги обох методів, намагаючись компенсувати їхні недоліки та підвищити точність рекомендацій [1].

Гібридні алгоритми дозволяють суттєво підвищити ефективність системи рекомендацій. Наприклад, на початкових етапах роботи система може формувати профіль нового користувача, аналізуючи не тільки його оцінки книг, а й додаткові фактори, такі як демографічні дані, теми, які цікавлять користувача, або ключові слова з опису вподобаних творів. У міру накопичення інформації про його поведінку система поступово переходить до колаборативної фільтрації,

враховуючи схожість із іншими користувачами та закономірності їхніх оцінок [2]. Такий підхід дозволяє створювати персоналізовані рекомендації, які постійно адаптуються до змін інтересів читача, забезпечуючи більш плавний і природний перехід від загальних до більш точних рекомендацій, а також підвищуючи рівень довіри користувачів до платформи.

Сучасні гібридні системи активно інтегрують методи машинного навчання, зокрема кластеризацію, глибокі нейронні мережі та обробку природної мови. Методи обробки природної мови дозволяють аналізувати опис книги, рецензії користувачів, ключові слова та інші текстові дані, перетворюючи їх у векторні представлення, які можна порівнювати між собою. Глибокі нейронні мережі здатні будувати спільний простір ознак для користувачів та книг, виявляючи складні семантичні взаємозв'язки між творами, навіть якщо вони не мають спільних оцінок або належать до різних жанрів. Це дозволяє системі робити "розумні припущення" щодо смаків користувачів і забезпечує більш релевантні та точні рекомендації.

Ще одним перспективним напрямом є використання багаторівневої архітектури гібридних систем, де різні алгоритми працюють на окремих етапах обробки даних. Один модуль може відбирати потенційно цікаві книги на основі контентного аналізу, інший - ранжувати їх з урахуванням уподобань подібних користувачів, а третій - оптимізувати результати на основі зворотного зв'язку та активності користувача [1,2].

Таким чином, гібридні рекомендаційні алгоритми відкривають широкі можливості для розвитку персоналізованих книжкових платформ. Вони поєднують точність контентного аналізу з гнучкістю колаборативних методів, забезпечуючи високий рівень адаптивності та персоналізації. Завдяки цьому користувач отримує більш індивідуалізований досвід взаємодії з системою, бо рекомендації постійно оновлюються відповідно до його вподобань і поведінки.

Список використаних джерел:

1. Çano, E., & Morisio, M.: Hybrid Recommender Systems: A Systematic Literature Review. 2019. arXiv:1901.03888. URL: https://arxiv.org/abs/1901.03888

2. Wayesa, F.: Pattern-based hybrid book recommendation system using data mining rules. 2023. Scientific Reports, 13(1), 12345. URL: https://www.nature.com/articles/s41598-023-30987-0

УДК 004

Затилюк Д.О., здобувач,
Локтікова Т.М., ст. викладач
Державний університет «Житомирська політехніка»

ОСОБЛИВОСТІ РОЗРОБКИ ОНЛАЙН-БІБЛІОТЕКИ З ПЕРСОНАЛІЗОВАНИМИ ФУНКЦІЯМИ ЧИТАННЯ

Сучасні електронні бібліотеки та онлайн-системи для читання активно розвиваються, однак більшість із них залишається функціонально обмеженими, яким притаманні такі недоліки: недостатня персоналізація, відсутність повноцінної синхронізації прогресу читання між пристроями, обмежені можливості перекладу та відсутність інтегрованого озвучування тексту. Це викликає потребу в глибокому аналізі наявних рішень для визначення напрямів розвитку електронних бібліотек нового покоління.

Для аналізу було розглянуто дві популярні українські онлайн-платформи: https://booknet.ua/, https://uabook.com.ua/. Кожна з них має свої особливості, однак загальний огляд демонструє повторювані проблеми, пов'язані зі зручністю читання, синхронізацією та кастомізацією.

https://booknet.ua/ – одна з найбільших в Україні платформ для читання художньої літератури, яку щомісяця відвідує понад пів мільйона унікальних користувачів. Як і будь-який сервіс, вона має свої переваги та недоліки [1].

Перевагами можна вважати її масштабність – близько 20 000 книжок, присутні активні блоги для авторів, конкурси та зручні інструменти організації власної бібліотеки. Також наявні нічний режим (але лише в мобільній версії) та зміна розміру шрифтів.

Водночас, недоліками є те, що можливості персоналізації досить вузькі: немає вибору шрифтів, зміни кольорів чи гнучких параметрів відображення. Десктопна версія виглядає менш адаптивною порівняно з мобільною.

https://uabook.com.ua/ – це онлайн-платформа для читання літератури різних напрямів, від художніх творів до професійних посібників, зокрема й з програмування [2].

Її перевагами можна вважати: наявність корисних функцій, а саме пошук, фільтри та базові налаштування відображення – зміна розміру шрифту й нічний режим; підтримка декількох форматів завантаження, включаючи PDF та EPUB; наявність порівняно великого книжкового фонду – близько тисячі книжок.

Як недолік можна відзначити те, що система перегортання сторінок реалізована незручно: перехід на наступну сторінку не прокручує текст угору автоматично, що дратує користувача і ускладнює читання. Персоналізація також обмежена – неможливо змінити фон, колір тексту чи шрифт.

Після проведених огляду й аналізу було визначено низку вимог, яким повинна відповідати онлайн-платформа нового покоління.

Насамперед, це розширені можливості персоналізації інтерфейсу читання, включно з вибором шрифту, кольорової схеми, розміру та міжрядкового інтервалу. Користувач повинен мати змогу гнучко налаштовувати зовнішній вигляд тексту відповідно до власних потреб.

Також важливо забезпечити зручну та інтуїтивну навігацію між розділами й сторінками. Це дозволяє уникнути ситуацій, коли механіка перегортання ускладнює взаємодію з текстом.

Окремим критерієм вважається стабільність роботи інструментів пошуку та фільтрації. Саме вони формують перше враження про платформу і визначають швидкість доступу до необхідного матеріалу.

У якості подальшого розвитку й удосконалення функціональності доцільно передбачити інтеграцію інструментів машинного перекладу та синтезу мовлення. Це забезпечить багатомовний доступ до контенту та можливість озвучування текстів.

Перспективним напрямом також є впровадження інтелектуальних рекомендацій на основі історії читання. Крім того, корисними будуть системи виділення та коментування фрагментів, а також можливість збереження налаштувань інтерфейсу як окремих профілів користувача.

Додатково варто розглянути підтримку різних режимів читання – посторінкового, безперервного та інших адаптивних форматів. Це дозволить платформі відповідати різним стилям роботи з текстом і підвищить комфорт користувача.

Результатом розробки з урахуванням визначених особливостей стане повнофункціональна веб-платформа, що поєднує можливості електронної бібліотеки, інтерфейсу для читання, персоналізованого налаштування та технологій штучного інтелекту. Такий проєкт може бути використаний у комерційних сервісах електронних книг, освітніх ресурсах, онлайн-видавництвах або як універсальний інструмент для організації доступу до цифрової літератури.

Список використаних джерел:

1. Booknet – платформа для електронного читання книг. URL: https://booknet.ua/ (дата звернення: 24.11.2025).

2. UA Book – онлайн-платформа для електронних книг. URL: https://uabook.com.ua/ (дата звернення: 24.11.2025).

УДК 004

Пилипенко Є.В., здобувач,
Локтікова Т.М., ст. викладач,
Кушнір Н.О., ст. викладач
Державний університет «Житомирська політехніка»

СУЧАСНИЙ СТАН І ТЕНДЕНЦІЇ РОЗВИТКУ СЕРВІСІВ ДЛЯ БРОНЮВАННЯ ЖИТЛА

Ринок онлайн-сервісів для бронювання житла переживає значні трансформації через новітні технології та зміни в уподобаннях споживачів. Такі платформи, як Airbnb, Booking.com та Agoda, займають провідні позиції на ринку, забезпечуючи зручний доступ до різноманітних варіантів житла. Мобільні додатки, відгуки та рейтинги допомагають користувачам швидко вибирати найкращі варіанти, а впровадження безпечних платіжних систем підвищує рівень зручності і довіри [1].

Суттєво вплинула на зміну уподобань споживачів, підвищивши попит на приватне житло, яке дозволяє уникати контактів із іншими людьми, пандемія COVID-19. Це змусило платформи адаптуватися, впровадивши гнучкі умови скасування бронювань і можливості для довгострокової оренди. У той же час, важливу роль відіграють нові технології, зокрема штучний інтелект, який дозволяє прогнозувати ціни, персоналізувати пропозиції та покращувати загальний досвід користувачів. Наприклад, Booking.com використовує алгоритми для підбору варіантів житла, які відповідають інтересам і попереднім виборам користувачів, що значно підвищує ефективність і зручність процесу бронювання [2].

Також зростає попит на екологічно чисте житло та сталий туризм. Споживачі все частіше шукають варіанти, що відповідають екологічним стандартам, таким як низький рівень вуглецевого сліду та енергоефективність. Платформи, які підтримують принципи сталого розвитку і екологічної відповідальності, стають все більш популярними серед свідомих мандрівників. Наприклад, платформа Ecobnb пропонує лише екологічно чисті варіанти, що відповідають суворим стандартам, і сприяє зростанню екологічного туризму [3].

Особлива увага приділяється використанню в сучасних сервісах для бронювання житла блокчейн-технологій, які значно підвищують безпеку транзакцій і роблять процес бронювання більш прозорим. Впровадження смарт-контрактів здатне зменшити роль посередників, автоматизувати більшість операцій та знизити витрати для учасників

ринку. Такі інновації дозволяють платформам створювати більш ефективні моделі співпраці та взаємодії [4].

У сучасних умовах зростаючого попиту на житло для «цифрових кочівників», які працюють віддалено, обумовлює зміну вимог до оренди [2]. Платформи адаптуються, пропонуючи житло на довший термін і додаючи до нього робочі простори, швидкісний Інтернет та інші послуги, що дозволяють поєднувати роботу з відпочинком у комфортних умовах. Це, в свою чергу, стимулює зростання попиту на житло в нестандартних локаціях – селищах, екологічних поселеннях, навіть на маленьких островах. Розширення гнучкості в роботі, можливість працювати з будь-якої точки світу надає нові можливості для розвитку таких напрямів.

Ще однією важливою тенденцією є підвищення персоналізації досвіду користувачів. Платформи бронювання активно використовують великі дані для створення персоналізованих рекомендацій, що допомагають клієнтам знаходити варіанти житла, які відповідають їхнім інтересам та вимогам. Це не тільки підвищує рівень задоволеності користувачів, а й зміцнює лояльність клієнтів до платформи [3].

Таким чином, ринок онлайн-сервісів для бронювання житла продовжує змінюватися і адаптуватися до нових технологій та змін у вимогах споживачів. Платформи, які вміють передбачати ці зміни і впроваджувати новітні рішення, збережуть свою конкурентоспроможність та стануть лідерами на ринку.

Список використаних джерел:

1. Mordor Intelligence. Online Accommodation Booking Market Size & Share Analysis – Growth Trends and Forecasts (2025–2030). 2025.
URL:https://www.mordorintelligence.com/industry-reports/global-online-accommodation-booking-market.

2. Fortune Business Insights. Online Accommodation Booking Market Size, Share & Industry Analysis, By Category…, And Regional Forecast, 2025–2032. 2024.
URL:https://www.fortunebusinessinsights.com/online-accommodation-booking-market-105007.

3. BCD Travel. Traveler insights: Hotel booking trends. 2025.
URL: https://www.bcdtravel.com/resources/traveler-insights-hotel-booking-trends/.

4. HOTREC. Digital Trends in Accommodation: Hotels, Booking.com and DMA. 2024.
URL:https://www.hotrec.eu/en/news/digital_trends_in_accommodation_hotels_booking-com_and_dma_.html.

УДК 004

Купрієнко М.С., здобувач,
Варганова Д.О., ст. викладач
Державний університет «Житомирська політехніка»

МОДЕЛЮВАННЯ ПЕРЕТИНУ ДВОХ ПРЯМИХ У ПРОСТОРІ ЗАСОБАМИ ПРОГРАМУВАННЯ

Проблеми просторової геометрії лежать в основі багатьох сучасних технологій та наукових досліджень. Зокрема, у таких сферах як комп'ютерна графіка, робототехніка, мехатроніка, системи автоматизованого проектування (САПР). В багатьох задачах важливим завданням є визначення взаємного положення об’єктів у тривимірному просторі одне відносно одного.

Однією з головних цілей є визначення взаємного розташування прямих у тривимірному просторі, а саме чи перетинаються вони, паралельні, чи є мимобіжними, або збігаються. Якщо прямі перетинаються, то потрібним є визначення координат точки перетину для подальших обчислень та побудов.

Математична модель:

Параметричне рівняння, яке задає координати всіх точок прямої у тривимірному просторі:

$$x = l\,t + x_0;\ y = m\,t + y_0;\ z = n\,t + z_0,$$

де (x_0, y_0, z_0) – координати точки, що лежить на прямій:

$\{l; m; n\}$ – координати напрямного вектора прямої.

Розглянемо дві прямі, які задані параметрично:

Пряма L_1: $x_1 = l_1 * t + x_{01}$; $y_1 = m_1 * t + y_{01}$; $z_1 = n_1 * t + z_{01}$.

Пряма L_2: $x_2 = l_2 * s + x_{02}$; $y_2 = m_2 * s + y_{02}$; $z_2 = n_2 * s + z_{02}$.

Точка перетину цих прямих повинна задовольняти дві системи рівнянь одночасно, що утворює систему трьох рівнянь з двома невідомими і змінними t і s [1].

$l_1 * t + x_{01} = l_2 * s + x_{02}$;

$m_1 * t + y_{01} = m_2 * s + y_{02}$;

$n_1 * t + z_{01} = n_2 * s + z_{02}$.

Розглянемо алгоритм розв'язку:

1. Ініціалізація та вхідні дані. Користувач задає координати точок та компоненти напрямних векторів для двох прямих.

2. Перевірка на паралельність. Здійснюється перевірка на колінеарність векторів за допомогою порівняння їхніх векторних добутків. Обчислюється векторний добуток напрямних векторів. Якщо його довжина близька до нуля (з урахуванням заданої похибки EPS = 1e-9), вектори вважаються паралельними. Якщо вектори паралельні,

алгоритм перевіряє, чи належить точка першої прямої другій прямій. Якщо істина – прямі збігаються, якщо ні – паралельні.

3. Верифікація. Знайдені параметри t і s підставляються в третє рівняння. Якщо воно також справджується, прямі перетинаються. Знаходимо значення координати z для кожної з прямих в знайдених точках. Якщо різниця між цими значеннями не перевищує задану точність EPS, прямі перетинаються.

4. Пошук точки перетину. Якщо вектори не паралельні, система розв'язується відносно параметрів t і s за методом Крамера, використовуючи перші два рівняння. Таким чином знаходимо точки перетину даних прямих.

5. Визначення мимобіжності. Якщо на етапі верифікації рівність для z-координати не виконується, прямі ввважаємо мимобіжними [2].

Фрагмент реалізації програми на мові С (частина задачі, коли вже знайдено, що прямі перетинаються, знаходження координат точки перетину):

```
if (fabs(z1_check - z2_check) < EPS)
{
double x_int = l1 * t + x01;
double y_int = m1 * t + y01;
double z_int = n1 * t + z01;
printf("Точка перетину: (%.2f, %.2f, %.2f)\n", x_int, y_int, z_int);
}
```

Отже, реалізація даного алгоритму надає можливість ефективно зрозуміти взаємне розташування двох прямих у тривимірному просторі. Розроблений програмний модуль є універсальним інструментом, який можна використовувати не лише для базових геометричних задач, а й може бути інтегрований у складніші обчислення для розв’язання прикладних задач у робототехніці, комп'ютерній графіці та архітектурі, інших галузях, де необхідний просторовий аналіз.

Список використаних джерел:

1. Onlinemschool: Рівняння прямої [Електронний ресурс] – Режим доступу до ресурсу: https://ua.onlinemschool.com/math/library/analytic_geometry/line/.

2. GeeksforGeeks: How to check if two given line segments intersect? [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/dsa/check-if-two-given-line-segments-intersect/.

УДК 004

Паламарчук І.С., здобувач,
Локтікова Т.М., ст. викладач,
Лисогор Ю.І., ст. викладач
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ПРИНЦИПІВ ПОБУДОВИ ТА ПРОЄКТУВАННЯ СИСТЕМИ УПРАВЛІННЯ ВИРОБНИЦТВОМ КРАФТОВИХ М'ЯСНИХ ВИРОБІВ

Малі підприємства стикаються з низкою викликів в управлінні виробничими процесами. Відсутність автоматизації призводить до зниження ефективності процесів на підприємстві. Розв'язком цієї проблеми слугують ERP-системи [1]. Але для бізнесів з малими потужностями виробництва впровадження громіздких систем є проблемою через їхню складність та високі витрати.

ERP (Enterprise Resource Planning) – це комплексна система, що дозволяє планувати та управляти всіма ресурсами компанії, об'єднаними в одному програмному рішенні [2].

Такі програмні системи складаються з основних модулів.

Модуль "Центральна база даних" є основою системи, де зберігається інформація про контрагентів, товари, склади та іншу номенклатуру.

Модуль "Фінанси" контролює бюджет, формує управлінський баланс між прибутками та збитками.

Модулі "Закупівлі" та "Продажі" підтримують процес управління запасами та автоматизують процеси замовлення та продажу продукції.

Модуль "Управління запасами" дозволяє керувати рухом товарів і матеріалів.

Модуль "Кадри та зарплатня" спрощує кадровий облік, автоматизує розрахунок заробітної платні.

Модуль "Виробництво" керує циклом випуску продукції, від планування завантаження ресурсів до випуску готової продукції.

Модуль "Система звітності" дозволяє швидко отримувати інформацію про стан бізнесу, забезпечує візуалізацію даних та прогнозування.

Не всі зазначені модулі обов'язково впроваджуються в системі, яка розробляється, оскільки кожне підприємство має унікальні потреби. Тому важливо визначити вимоги конкретного підприємства, щоби коректно сформулювати функціональні вимоги до програмного продукту.

Пропонується веборієнтована ERP-система для автоматизації управління виробництвом крафтових м'ясних виробів, яка забезпечить комплексне управління складським обліком, виробничими процесами та документообігом для малого бізнесу.

Функціональні можливості програмного забезпечення включають: облік надходження та списання сировини, списання сировини на виробництво, розробку специфікацій продукції, запуск виробничих процесів, формування документів переміщення між складами та цехами, реалізацію готової продукції через видаткові накладні, ведення довідників контрагентів, складів, цехів.

Архітектура системи базується на принципах Domain-Driven Design з чітким розділенням на шари: бізнес-логіка, сервіси, інфраструктура бази даних, контролери.

Domain-Driven Design (DDD) – це стратегічний підхід до розробки програмного забезпечення, який ставить у центр уваги реальні бізнес-процеси [3]. Цей шаблон підходить до великих систем, до яких належить запропоноване рішення.

Одним з інструментів цього підходу є “Уніфікована мова”. Це практика створення спільної, чіткої мови між розробниками та користувачами. Тобто, кодова база програми має використовувати термінологію бізнесу, щоби відображати його реальні процеси.

Також використовуються агрегати, об’єднання сутностей та об’єктів-значень, які розглядаються як єдиний об’єкт. Кожен агрегат має кореневу сутність. Тільки через цей об’єкт відбувається доступ до підпорядкованих об’єктів. Це забезпечує консистентність системи та цілісність даних.

Сутність – це об'єкт, який має унікальну ідентичність, незалежно від змін його атрибутів, тоді як об'єкти-значення слугують для опису характеристик сутностей.

Пропонована система забезпечує автоматизацію управління виробництвом крафтових м'ясних виробів, підвищує продуктивність підприємства, знижує ризики помилок та створює основу для масштабування бізнесу.

Список використаних джерел:

1. ERP система для малого бізнесу: необхідність чи примха? Камала Софт. URL: https://kamala-soft.com/uk/blog/erp-sistema-dlya-malogo-biznesa/.

2. Власова А. Повний гайд по ERP-системах: що це, приклади та структура сучасних рішень. Brander. 22.08.2025. URL: https://brander.ua/blog/povnyy-hayd-po-erp-systemakh-shcho-tse-pryklady-ta-struktura-suchasnykh-rishen.

3. Domain-Driven Design (DDD). Sensidev. URL: https://sensidev.com/glossary/domain-driven-design/.

УДК 004.932

Голенко М.Ю., аспірант
Державний університет «Житомирська політехніка»

АНАЛІЗ МЕТОДІВ ФОРМУВАННЯ ТЕПЛОВИХ КАРТ ДЛЯ АДАПТИВНОГО ПОКРАЩЕННЯ ЗОБРАЖЕНЬ З БПЛА

Теплові карти нейронних мереж використовуються для візуалізації регіонів, які модель вважає найбільш інформативними. Вони можуть слугувати індикатором інформативності кадру або окремого його фрагмента. Це забезпечує можливість активувати суперрезолюцію (SR) лише там, де її використання виправдане, оскільки вона потребує значних обчислювальних ресурсів.

Адаптивна логіка використання SR передбачає вибіркове застосування покращення лише в тих випадках, коли зображення містить регіони, здатні принести користь для подальшого розпізнавання. Оскільки SR підсилює локальні ознаки, вона є ефективною тоді, коли в кадрі присутні структури, які модель може використати. Для визначення таких регіонів можуть застосовуватися теплові карти, що відображають, які частини зображення модель вважає важливими у своїх внутрішніх ознаках.

Для формування теплових карт широко застосовуються методи Grad-CAM та Eigen-CAM:

1. Grad-CAM формує теплову карту на основі градієнтів виходу моделі за певним класом щодо активацій вибраного шару [1]. Підхід узгоджує середні значення градієнтів з каналами активацій, створюючи карту важливості, яка відображає регіони, що найбільше впливають на прогноз моделі. Оскільки такий механізм напряму пов’язаний із конкретним класом, теплова карта є класово-залежною і показує лише ті ділянки, які модель використовує саме для відповідного передбачення. Якість карти залежить від стабільності градієнтного сигналу. Якщо модель не впевнена у прогнозі або не розпізнає об’єкт, карта стає фрагментованою або слабко вираженою. Крім того, обчислення Grad-CAM потребує виконання зворотного проходу, що підвищує обчислювальну вартість і ускладнює застосування методу в режимах з жорсткими обмеженнями продуктивності. Підхід добре підходить для аналізу класових ознак та пояснення рішень моделі, однак не є ефективним для оцінки загальної інформативності кадру, оскільки повністю залежить від класових прогнозів.
2. Eigen-CAM використовує активації проміжного шару моделі як матрицю ознак та визначає їх найбільш характерний напрямок зміни за допомогою методу головних компонент [2]. Теплова карта формується

на основі першої головної компоненти, що відображає домінантну структуру активацій без прив'язки до класу. Такий підхід є класово-незалежним і формує карту важливості, що показує інформативність зображення загалом, а не його зв'язок із певним прогнозом. Eigen-CAM залишається стабільним навіть на кадрах низької якості, оскільки не потребує чіткого класового сигналу і не покладається на градієнти. Метод працює на основі прямого проходу моделі, що забезпечує низьку обчислювальну вартість і робить його придатним для використання в режимах реального часу. Оскільки теплова карта відображає загальну інформативність зображення, Eigen-CAM може слугувати надійним індикатором для вирішення, чи варто застосовувати суперрезолюцію, тобто чи містить кадр ознаки, підсилення яких покращує розпізнавання. Відсутність класової прив'язки може бути недоліком у завданнях, де необхідно аналізувати важливість саме конкретного класу, проте в контексті адаптивної суперрезолюції це не є критичним.

Порівняння двох методів показує, що Grad-CAM та Eigen-CAM суттєво відрізняються за принципом формування теплових карт і характером інформації, яку вони відображають. Grad-CAM є класово-залежним і демонструє максимальну ефективність тоді, коли модель має стабільний прогноз, що робить його корисним для аналізу класових ознак, але обмежує у випадках, коли необхідно оцінити загальну інформативність. Eigen-CAM, натомість, формує класово-незалежну карту важливості та зберігає стійкість на кадрах низької якості.

З огляду на ці властивості, Eigen-CAM є більш практичним для адаптивної суперрезолюції, де потрібно визначити, чи має кадр структури, підсилення яких може покращити результативність детекції. Застосування такого підходу забезпечує більш точне визначення інформативності та дає змогу раціональніше використовувати суперрезолюцію, що загалом підвищує ефективність детекції та якість обробки зображень з БПЛА.

Список використаних джерел:

1. Selvaraju R. R., Cogswell M., Das A., Vedantam R., Parikh D., Batra D. Grad-CAM: Visual Explanations from Deep Networks via Gradient-based Localization // Proceedings of the IEEE International Conference on Computer Vision (ICCV 2017). – Венеція, 2017. – С. 618–626.

2. Muhammad M. B., Yeasin M. Eigen-CAM: Class Activation Map using Principal Components // Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN). – Глазго, 2020. – С. 1–7.

СЕКЦІЯ 2
КОМП'ЮТЕРНА ІНЖЕНЕРІЯ, КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.7

Держанівська А.О., здобувач,
Покотило О.А., ст. викладач,
Щур Н.О., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ КРИПТОГРАФІЧНИХ ЗАВДАНЬ У CTF- ЗМАГАННЯХ

Capture The Flag (CTF) - це формат змагань у сфері кібербезпеки, який моделює реальні сценарії кібератак і захисту інформаційних систем. Оскільки криптографія відіграє важливу роль у кібербезпеці, забезпечуючи конфіденційність та цілісність даних, майже у всіх змаганнях з CTF існує категорія «Крипто» або «Криптографія» [1].

Такі змагання набули значної популярності серед студентів технічних спеціальностей, оскільки дозволяють перевіряти теоретичні знання на практиці. У контексті криптографії участь у CTF сприяє розвитку аналітичного мислення, розумінню принципів роботи шифрів і навчанню нестандартних способів пошуку вразливостей у реалізаціях алгоритмів.

Метою цього дослідження є аналіз та класифікація типових завдань криптографії у CTF-змаганнях, що дозволить студентам та початківцям, які планують брати участь у CTF-змаганнях, краще розуміти принципи побудови таких завдань та ефективніше готуватися до їх розв'язання.

У межах змагань CTF криптографічні завдання можна умовно поділити на кілька типів залежно від принципів шифрування, складності та підходів до розв'язання [2].

Завдання з класичними шифрами. До цієї категорії належать завдання, що базуються на історичних методах шифрування, таких як шифр Цезаря, шифр Віженера, Playfair, Rail Fence тощо. Розв'язання таких завдань зазвичай передбачає частотний аналіз, пошук повторюваних сегментів у тексті та автоматизацію дешифрування за допомогою простих скриптів або утиліт.

Завдання із сучасними алгоритмами шифрування. Ці завдання пов'язані із вивченням та експлуатацією сучасних криптосистем, зокрема RSA, AES, ECC. Учасникам може бути запропоновано знайти вразливість у реалізації алгоритмів шифрування. Такі завдання

допомагають зрозуміти, як навіть стійкі алгоритми можуть бути зламані через помилки в реалізації.

Завдання з хешування. Завдання цієї групи вимагають відновлення вихідних даних із хеш-значення або виявлення колізій. Найчастіше використовуються алгоритми MD5, SHA-1, SHA-256. Основні методи розв'язання - brute-force, словникові атаки або використання попередньо обчислених таблиць (rainbow tables). Для цього застосовуються такі інструменти, як Hashcat та John the Ripper.

Завдання з кодування та декодування. У таких завданнях необхідно розпізнати формат кодування (Base64, Hex, URL-encoding тощо) та відновити початкові дані. Ці задачі часто використовуються як підготовчий етап до складніших криптоаналізів. Найпопулярнішими інструментами є CyberChef та Python-скрипти для автоматизації декодування.

З огляду на практичне виконання цих завдань, на сучасних CTF-платформах учасники працюють в ізольованому середовищі Linux- або Docker-контейнерів. Для розв'язання криптографічних задач часто створюються спеціальні Python-скрипти, які автоматизують рутинні обчислення - наприклад, аналіз підключів, пошук періодів у шифрах потокового типу або підбір відкритих експонент у RSA. У деяких випадках завдання передбачають комбінацію кількох технік - наприклад, кодування, шифрування та хешування в одному файлі, що вимагає від учасників комплексного підходу до розв'язання.

Окрему категорію становлять завдання на криптоаналіз власних або нестандартних реалізацій шифрів, створених авторами завдань спеціально для CTF. Такі задачі дають змогу відпрацьовувати навички аналізу невідомих алгоритмів, виявлення логічних помилок у побудові та тестування гіпотез щодо способів дешифрування. Часто саме цей тип завдань є найскладнішим і вимагає поєднання знань із лінійної алгебри, теорії чисел та програмування.

Проведений аналіз узагальнює типові криптографічні завдання у CTF-змаганнях, визначає основні підходи до їх розв'язання та сприяє розвитку практичних навичок застосування криптографії. Отримані результати можуть бути використані при підготовці навчальних тренажерів з прикладної криптології та формуванні банку завдань для освітніх CTF-платформ.

Список використаних джерел:

1. Cyber University. CTF Practice: Cryptography. URL: https://cyberuniversity.tech/cryptography/ctf-practice

2. cywf. Cryptography Challenges – cywf/ctf-kit GitHub Wiki. URL: https://github-wiki-see.page/m/cywf/ctf-kit/wiki/Cryptography-Challenges

УДК 004.056

Нарольський Т.М., здобувач,
Балацька В.С., д-р філ., ст. викладач,
Полотай О.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ РІВНЯ ДОВІРИ В ДЕЦЕНТРАЛІЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ КСЗІ НА ОСНОВІ БЛОКЧЕЙН-ТЕХНОЛОГІЙ

Інформаційні системи, особливо ті, що функціонують у державному секторі, стикаються з проблемою втрати довіри до джерел та процесів обробки даних. Централізовані структури керування доступом, навіть за умови побудови комплексних систем захисту інформації (КСЗІ), залишаються вразливими до людського фактора, зловживань правами адміністратора та внутрішніх загроз.

В умовах децентралізації даних усе більшої актуальності набувають механізми математичного формалізування довіри, які дозволяють оцінювати поведінку кожного елемента системи не лише за його технічними параметрами, а й за історією взаємодій.

Метою дослідження є створення математичної моделі, яка дозволяє формалізувати процес формування довіри між вузлами в децентралізованій архітектурі КСЗІ. В основі запропонованої моделі лежить поєднання поведінкового аналізу, теорії графів та ймовірнісних функцій ризику. Такий підхід дає можливість системі автоматично виявляти аномалії, прогнозувати можливі загрози та реагувати ще до того, як вони реалізуються.

Для вузла i у момент часу t рівень довіри визначається функцією:

$$T_i t = \alpha P_i t + \beta H_i t + \gamma S_i t,$$

де $P_i(t)$ – ймовірність коректної поведінки; $H_i(t)$ – історичний показник дотримання політик безпеки; $S_i(t)$ – структурна взаємодія з іншими вузлами; α, β, γ – вагові коефіцієнти $(\alpha+\beta+\gamma=1\alpha + \beta + \gamma = 1\alpha+\beta+\gamma=1)$, що визначають вплив кожного параметра.

Якщо рівень довіри вузла падає нижче порогового значення Tcrit, система автоматично активує політику підвищеного контролю, багатофакторну аутентифікацію або перевірку транзакцій через смарт-контракт.

Для кількісного опису ризику використовується експоненціальна залежність: $R_i(t) = 1 - e^{(-\lambda(Tcrit - T_i(t)))}$, де λ – параметр чутливості системи. Зі зменшенням довіри ризик зростає нелінійно, що дозволяє більш точно реагувати на небезпечні зміни у поведінці користувачів.

Модель тестувалася в середовищі Python із використанням бібліотек *NetworkX* і *SymPy*. Для мережі з 50 вузлів при наявності 20 % зловмисних елементів середній рівень довіри зберігався вище 0,75, що свідчить про стійкість системи до внутрішніх аномалій. Алгоритмічна складність розрахунку матриці довіри становила $O(n^2)$, що є прийнятним для permissioned blockchain-мереж середнього масштабу.

Практична цінність запропонованого підходу полягає в тому, що він дозволяє перейти від статичних правил доступу до динамічної системи довіри, де кожна дія користувача впливає на його поточний статус у мережі. Такий механізм може бути реалізований на рівні permissioned blockchain (наприклад, Hyperledger Fabric, Quorum), де вузли виступають рівноправними учасниками з формалізованими математичними атрибутами довіри.

Використання блокчейн як реєстру довірчих взаємодій забезпечує прозорість і незмінність журналів подій, а математичне моделювання довіри – гнучкість і прогнозованість поведінки системи. У сукупності це створює основу для формування пояснюваної безпеки – коли кожне управлінське рішення (блокування, попередження, зміна прав доступу) може бути обґрунтоване формулою або моделлю.

Отже, запропонований підхід дозволяє поєднати переваги блокчейн-технологій із класичними методами оцінки ризику та забезпечення конфіденційності. Його застосування у КСЗІ державних реєстрів, освітніх або банківських систем дозволяє мінімізувати людський фактор, підвищити рівень довіри між користувачами та забезпечити відповідність міжнародним стандартам ISO/IEC 27001, ISO/IEC 27701 і GDPR.

Список використаних джерел:

1. Балацька В. С., Опірський І. Р. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну // Кібербезпека: освіта, наука, техніка. 2023. № 4 (20). С. 6–19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619

2. Balatska V., Opirskyy I. Blockchain as a tool for transparency and protection of government registries // Ukrainian Scientific Journal of Information Security. 2024. Vol. 30, issue 2. P. 221–230. DOI: https://doi.org/10.18372/2225-5036.30.19211

3. Балацька В., Ткачук Р., Маслова Н. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних систем України // Кібербезпека: освіта, наука, техніка. 2025. № 2(30). С. 316–332. DOI: https://doi.org/10.28925/2663-4023.2025.30.975

УДК 004.056.5:005.334

Нарепеха Д.Ю., здобувач,
Полотай О.І., к.т.н., доцент,
Балацька В.С., д-р філ., ст. викладач
Львівський державний університет безпеки життєдіяльності

АНАЛІЗ ВИКОРИСТАННЯ МІТИГАЦІЇ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ НА ПІДПРИЄМСТВІ

Проблематика інформаційної безпеки значною мірою визначається характером ризиків та масштабом їх можливих наслідків. У невеликих локальних системах створення ефективної системи управління ризиками є відносно простішим завданням, ніж у розподілених системах, що зумовлено їх специфічними особливостями [2].

У сучасних умовах цифровізації економіки питання забезпечення інформаційної безпеки стає одним із ключових аспектів ефективного функціонування підприємства. Ризики інформаційної безпеки охоплюють широкий спектр загроз – від несанкціонованого доступу до корпоративних даних до збоїв у роботі інформаційних систем, витоків конфіденційної інформації чи кібератак. Такі ризики можуть призвести до значних фінансових втрат, зниження репутації, втрати клієнтів і порушення стабільності бізнес-процесів. Саме тому мітигація ризиків інформаційної безпеки є критично важливою складовою системи управління ризиками підприємства.

Мітігація (або митігування) ризиків - це термін, що походить від англійського слова mitigation, що означає "пом'якшення" або "пом'якшення наслідків". Прямий переклад з англійської вже частково описує суть мітигації ризиків – це зниження наслідків їх реалізації. Спочатку термін «мітігація» застосовувався щодо різноманітних катастроф і надзвичайних ситуацій (у розумінні способів зниження тяжкості їх наслідків), але останнім часом він нерідко використовується і в теорії управління ризиками. Особливо часто останнім часом цей термін застосовується в таких галузях як інформаційна та кібербезпека. Мітигація – це процес здійснення заходів, спрямованих на зменшення ймовірності настання ризикової події та/або зменшення тяжкості наслідків, якщо вона все ж станеться. Це proactive-стратегія, яка передбачає активні дії для попередження негативних наслідків, а не просто реагування на них після того, як вони сталися [2].

Процес мітигації ризиків інформаційної безпеки передбачає кілька основних етапів: ідентифікацію, оцінювання, розроблення заходів

реагування, реалізацію та постійний моніторинг. На етапі ідентифікації визначаються потенційні загрози, такі як фішингові атаки, шкідливе програмне забезпечення, помилки персоналу чи вразливості програмного забезпечення. Оцінювання ризиків дозволяє визначити ймовірність їх виникнення та рівень впливу на бізнес-процеси, що є основою для формування пріоритетів у захисті інформаційних активів.

Одним із практичних прикладів мітигації ризиків інформаційної безпеки у локальних комп'ютерних мережах підприємства є впровадження системи контролю доступу та сегментації мережі для зниження ризику несанкціонованого доступу до конфіденційних даних.

Наприклад, на підприємстві існує спільна локальна мережа, до якої підключені всі комп'ютери працівників різних відділів – бухгалтерії, відділу кадрів, технічного відділу тощо. У разі відсутності розмежування прав доступу, співробітники можуть потенційно отримати доступ до інформації, яка не стосується їхніх обов'язків, або ж зовнішній зловмисник, потрапивши до внутрішньої мережі, отримає змогу вільно пересуватися між сегментами системи.

Щоб мінімізувати цей ризик, підприємство впроваджує політику мітигації ризику шляхом сегментації мережі – кожен відділ отримує власний підмережевий сегмент із чітко визначеними правилами взаємодії між ними. Доступ до критично важливих ресурсів, наприклад до бази даних бухгалтерії, надається лише авторизованим користувачам із багатофакторною аутентифікацією. Додатково застосовується система моніторингу та журналювання подій, яка дозволяє відстежувати спроби несанкціонованого доступу.

Завдяки таким заходам ризик компрометації даних зменшується: навіть якщо зловмисник отримає доступ до однієї з ділянок мережі, він не зможе легко проникнути до інших частин системи або отримати доступ до конфіденційної інформації. Такий підхід демонструє ефективну мітигацію ризику шляхом технічного, організаційного та процедурного посилення системи інформаційної безпеки.

Список використаних джерел:

1. Мітигація ризиків. URL: https:// https://qamania.org/blog/risk-mitigation//

2. Тичина Ю., Ящук В., Полотай О. Модель системи управління інцидентами інформаційної безпеки. Зб. тез доп. V Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів "Інформаційна безпека та інформаційні технології". (м. Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. С. 108–111.

УДК 004.8

Дорогий Я. Ю., д.т.н., професор,
Донецький національний технічний університет
Цуркан В. В., к.т.н., доцент,
Інститут спеціального зв'язку та захисту
інформації КПІ ім. Ігоря Сікорського
Дорога-Іванюк О. О., вчитель вищ. кат.,
Пологівський ліцей Ковалівської територіальної громади
Білоцерківського району Київської області

ЗАСТОСУВАННЯ ШІ ПРИ ВИВЧЕННІ ДИСЦИПЛІН З КІБЕРБЕЗПЕКИ

Інтенсифікація кіберзагроз останніми роками викликає зростаючий попит на висококваліфікованих фахівців з кібербезпеки. Університети адаптують освітні програми, включаючи актуальні інструменти ШІ, щоб забезпечити студентам практичні навички захисту інформаційних систем. Наразі ШІ все частіше використовується не лише для автоматизованого виявлення атак, але й для навчання: наприклад, студенти можуть тренуватися в безпечному симульованому середовищі з імітацією реальних атак і відповідей.

В університетській освіті з кібербезпеки ШІ використовується для забезпечення реалістичних практичних вправ та персоналізації навчального процесу. Різноманітність ШІ-технологій у цьому контексті охоплює кілька напрямів:

- *Генеративні AI-моделі*. Інструменти на кшталт ChatGPT широко застосовуються для створення навчальних сценаріїв та пояснень складних тем. Наприклад, generative AI показує високу ефективність у допомозі студентам-початківцям при підготовці до CTF-змагань: ChatGPT узагальнює і пояснює базові поняття (шифрування, мережеві атаки тощо) на доступному рівні [1]. Університетські курси використовують такі моделі для генерації завдань та автоматичного зворотного зв'язку, що підвищує залученість студентів та глибину розуміння. При цьому важливо, щоб учасники навчання критично оцінювали AI-результати, а викладачі коригували їхню роботу.
- *Моделі симуляції та кіберарені*. ШІ-інструменти покращують якість симуляцій «живих атак». Наприклад, концепція Red Team/Blue Team широко використовується для відпрацювання реалістичних сценаріїв: IT-інфраструктура моделюється віртуально, і студенти у ролі нападників (Red) і захисників (Blue) змагатимуться за контроль. Системи штучного інтелекту можуть генерувати сценарії атак, створювати автоматизованих агентів-опонентів або оцінювати

результати дій студентів. У цій категорії активно розвиваються технології цифрових двійників – віртуальних копій мережевих систем (DT), які дозволяють проводити високодеталізовані симуляції кібератак у безпечному середовищі. Так, згадуваний «Red Team Knife» інтегрується з DT-екосистемою для послідовного практичного вивчення всіх фаз атаки та захисту [2].

- *Гейміфікація та адаптивне навчання*. ШІ-системи дозволяють реалізувати адаптивні навчальні шляхи: наприклад, програма виявляє слабкі місця студента і автоматично пропонує додаткові вправи або теоретичні матеріали. Аналізують греп-інформацію про спосіб вирішення задачі, модифікують складність. Хоча конкретні університетські кейси описані переважно у внутрішніх звітах, поєднання AI з гейміфікацією (змагання в режимі он-лайн, персональний прогрес, рейтинги) рекомендується практиками, оскільки підвищує конкурентний дух і ефективність засвоєння матеріалу.

Таким чином, широке застосування ШІ – від глибоких нейромереж до генеративних мовних моделей і реалістичних симуляцій – робить вивчення кібербезпеки більш інтерактивним і наближеним до реальності.

Висновки. Використання технологій штучного інтелекту в університетських курсах з кібербезпеки відкриває нові можливості для інтерактивного і практично орієнтованого навчання. Поєднання нейронних мереж для виявлення загроз, генеративних моделей для створення освітнього контенту та платформ симуляції атак сприяє тому, що студенти набувають практичних навичок у безпечному середовищі зворотного зв'язку. Зі зростанням ролі ШІ у реальних кібероперація освітніх програм із включенням цих технологій стає незаперечною вимогою для підготовки конкурентоспроможних фахівців.

Список використаних джерел:

1. Lam L. Capturing the Flag with ChatGPT: Generative AI for Cyber Education. Center for Security and Emerging Technology (CSET), Georgetown University, 2023. URL: https://surli.cc/aoymhp.

2. Barletta V.S., Bavaro V., Calvano M., Curci A., Piccinno A., Posa D.P. Enabling Cyber Security Education through Digital Twins and Generative AI. arXiv:2507.17518, 2025. URL: https://surli.cc/xggzvx.

УДК 004.7

Боднарашик А. О., здобувач,
Покотило О. А., ст. викладач
Державний університет «Житомирська політехніка»

ВІДМИВАННЯ КОШТІВ У КРИПТОВАЛЮТНИХ МЕРЕЖАХ ТА МЕТОДИ ЇХ АНАЛІЗУ

З розвитком цифрових технологій та зростанням популярності цифрових валют фінансові правопорушення, зокрема відмивання коштів, набули стрімкого розвитку. «Відмивання» грошей (Money-laundering) – це складна процедура непрозорих транзакцій для приховування походження статків [1]. Складність виявлення слідів «брудних» грошей випливає з унікальної архітектури блокчейн (blockchain), що лежить в основі криптовалют. Створення адреси займає кілька секунд і є безкоштовним, а кількість таких рахунків на користувача не обмежується.

На відміну від традиційних фінансових систем, у криптовалютах відсутній централізований контроль, що ускладнює ідентифікацію учасників грошових потоків. Децентралізація та можливість створення необмеженої кількості адрес сприяють використанню цифрових активів для приховування транзакцій і уникнення фінансового моніторингу.

Першим етапом у відмиванні статків є переказ незаконно отриманих коштів на депозитну адресу: блокчейн гаманець, приватну організацію, або міксер («mixer»). Анонімність цифрових валют не дозволяє вийти на конкретних осіб, однак публічний характер блокчейн транзакцій залишає цифровий слід, який можливо відстежити. На наступному етапі міксери змішують криптовалюти різних осіб на одній адресі, які звідти розсилаються на різні рахунки меншими частинами. Процес можна повторити декілька разів до досягнення кінцевого пункту призначення – пов’язати їх з першоджерелом надходження буде майже неможливо. Після завершення процесу міксування кошти надсилають на основну біржу або P2P платформу, де їх можна конвертувати назад у фіатну валюту. Враховуючи стрімке зростання курсів обміну, виправдати несподіване збагачення («відмити» гроші) стає дуже легко. Деякі криптовалюти демонструють збільшення вартості на десятки тисяч відсотків [2], слугуючи стимулом їх використання у злочинних цілях.

Володіння криптовалютою в Україні є законним, але законним платіжним засобом вона не визнається. Після початку повномасштабного вторгнення обмеження Національного банку України спричинило зростання у використанні криптовалюти

українцями для обходу контролю за рухом статків. Громадяни у скрутному фінансовому становищі можуть надавати свої адреси для операцій сумнівного характеру за невелику винагороду. Банки намагаються боротися з цим (за 2024 рік було заблоковано 80 000 таких адрес [3]), проте частина користувачів може не знати справжньої мети щахраїв.

Для боротьби з криптозлочинами необхідно усунути основну перешкоду – відсутність правової бази в галузі. Регулювання криптовалютного ринку сприятиме правоохоронним органам у виявленні шахраїв, обмеженні відмивання грошей та залученні потенційних податкових надходжень від діяльності криптобірж.

У рамках дослідження було проведено аналіз випадкових криптовалютних транзакцій. Зафіксовано транзакції, де сотні тисяч доларів з одного вхідного гаманця розщеплюються на близько десяти вихідних адрес. Такі підозрілі ознаки, як розсіювання коштів однією великою транзакцією та повернення останнього виходу на нову адресу відправника, вказують на потенційні схеми відмивання та розсіювання (dispersion) активів для ускладнення відстеження. Для попереднього виявлення подібних аномалій можуть застосовуватися методи графового аналізу та кластеризації адрес, що дозволяє автоматично відстежувати транзакційні зв'язки та виявляти нетипові маршрути руху активів. Подальше застосування алгоритмічних методів до таких транзакційних патернів є критичним для розробки ефективних моделей виявлення фінансових злочинів у криптовалютному середовищі.

Список використаних джерел:

1. How illicit actors launder money through crypto exchanges. sanctions.io [Електронний ресурс]. – Режим доступу: https://www.sanctions.io/blog/how-illicit-actors-launder-money-through-crypto-exchanges (дата звернення: 10.11.2025).

2. Money laundering through cryptocurrencies. United Nations : UN Toolkit on Synthetic Drugs [Електронний ресурс]. – Режим доступу: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html (дата звернення: 10.11.2025).

3. Криптовалютні злочини щороку відбирають в України мільярди втрачених доходів – звіт RUSI. mind.ua [Електронний ресурс]. – Режим доступу: https://mind.ua/news/20293934-kriptovalyutni-zlochini-shchoroku-vidbirayut-v-ukrayini-milyardi-vtrachenih-dohodiv-zvit-rusi (дата звернення: 10.11.2025).

УДК 681.518

Сарапин В.Є., магістрант,
Шабала Є.Є., к.т.н., доцент
Київський національний університет будівництва і архітектури

ГІБРИДНИЙ ПІДХІД ДЛЯ ДІАГНОСТИКИ МЕРЕЖЕВИХ АНОМАЛІЙ ЧЕРЕЗ ПАРАМЕТР ХЕРСТА ТА QOS-МЕТРИКИ

Мережеві відмови є будь-яким порушенням роботи системи, які призводять до зниження продуктивності або повного припинення надання послуг. Для діагностики критично важливо їх класифікувати:

Апаратні відмови – це збої фізичних компонентів (комутатор, кабель, мережева карта) і виявляються через моніторинг стану портів та логів обладнання.

Програмні відмови пов’язані з помилками у мережевому ПЗ, драйверах чи операційній системі пристроїв, які спричиняють непередбачувану поведінку протоколів.

Відмови протоколів з’являються коли несправності пов'язані з некоректною конфігурацією маршрутизації (OSPF, BGP) або транспортних протоколів (TCP-таймаути).

Візантійські відмови вважаються особливим класом відмов, де один або кілька вузлів поводяться зловмисно або непослідовно, надсилаючи суперечливі дані різним частинам розподіленої системи. З позиції мережевої кібербезпеки це може виражатися через:

Для того, щоб встановити нормальний базовий рівень трафіку та спрогнозувати його поведінку використовуються математичні моделі. Моделювання дозволяє відрізнити нормальні коливання навантаження від справжніх аномалій.

Модель Пуассона традиційно використовується для моделювання надходження подій або пакетів. Вона передбачає, що прибуття пакетів є незалежним і відбувається з постійною середньою інтенсивністю. Для варіанту M/G/1 вхідний процес характеризується розподілом Пуассона зі швидкістю надходження повідомлень λ [1] .

Самоподібний (фрактальний) трафік є більш точною моделлю для високошвидкісних мереж. Вона враховує, що сплески трафіку виглядають однаково на різних часових масштабах (від мілісекунд до годин). Моделювання з використанням параметру Херста (H) є критичним для точного прогнозування перевантажень. Якщо $H=0.5$, трафік відповідає моделі Пуассона. Якщо $0.5<H<1$, трафік є самоподібним, що вказує на сильні залежності та довший час перебування в черзі.

Ланцюги Маркова, особливо приховані Марковські моделі, успішно застосовуються для класифікації різних протоколів і типів трафіку [2].

Для моніторингу та діагностики пропонується трирівнева архітектура, що забезпечує масштабованість та поділ відповідальності. Алгоритм використовує поєднання класичного моніторингу QoS та моделі самоподібності для підвищення точності виявлення, особливо для прихованих атак, як-от Slowloris або Low-Rate DDoS, які не завжди викликають різке перевищення традиційних порогів.

Формування базового рівня. Протягом встановленого періоду (наприклад 7 днів) збираються дані QoS-метрик та розраховується середнє значення параметра Херста для трафіку в кожному сегменті. Встановлюються статистичні діапазони нормального функціонування

Розрахунок ознак у реальному часі. Для кожного часового вікна (наприклад 5 секунд) розраховуються поточні значення:

(затримка, втрата пакетів, джитер).

(поточний параметр Херста).

Система виявляє мережеві аномалії завдяки генерації сигналів тривоги типу А, коли поточні показники якості обслуговування виходять за межі статистичного діапазону та сигналів типу Б, якщо зростання параметру самоподібності . Це є показником традиційних несправностей або потенційних прихованих загроз.

Верифікація та кореляція. Сигнали тривоги типу А та Б від різних сенсорів, що відбуваються одночасно, піддаються кореляційному аналізу. Якщо сигнал типу Б походить від вузла, який одночасно надсилає суперечливі дані іншим сенсорам, це підтверджує візантійську відмову або компрометацію.

Список використаних джерел:

1. Моделювання процесів керування у корпоративних комп’ютерних мережах / упоряд. Посашков О. Ю., Безкоровайний В. В. Харків : ХНАДУ, 2021. URL: https://dspace.khadi.kharkov.ua/server/api/core/bitstreams/a6ec3c97-37e3-4e8b-ba0f-651fa0f67e30/content (дата звернення: 18.11.2025).

2. Клюшник В.В., Чернецький Є.В., Онищенко О.В. Ідентифікація трафіку мереж передачі даних у реальному часі. Вісник Приазовського державного технічного університету. Серія: Технічні науки. 2025. Вип. 50. С. 18-24. DOI: https://doi.org/10.31498/2225-6733.50.2025.336234

УДК 004.056.53

Палагін В.В., д.т.н., професор,
Яковлєв Б.В., магістрант,
Гуржій І.В., магістрант
Черкаський державний технологічний університет

ІНТЕГРАЦІЯ SIEM-СИСТЕМИ WAZUH В ДЕРЖАВНИХ ФІНАНСОВИХ УСТАНОВАХ

Актуальність теми зумовлена стрімкою цифровізацією державного сектору та одночасним зростанням кількості кіберзагроз. Державні фінансові установи, що оперують критичними бюджетними даними та персональною інформацією, є пріоритетними цілями для зловмисників. Впровадження ефективних систем моніторингу подій та управління інформаційною безпекою (SIEM) є нагальною потребою. Проте, обмеженість бюджетів державних установ вимагає пошуку гнучких та економічно ефективних рішень, яким є open-source платформа Wazuh.

Метою роботи є аналіз особливостей впровадження SIEM-системи Wazuh в інформаційну інфраструктуру державних фінансових установ для підвищення загального рівня їх кіберзахисту.

Для досягнення мети було проаналізовано типову архітектуру IT-систем в державних установах та запропоновано модель інтеграції Wazuh. Вона базується на трьох основних компонентах:

1. **Wazuh Server:** центральний компонент, що відповідає за аналіз отриманих логів, кореляцію подій та генерацію сповіщень;
2. **Wazuh Indexer:** кластер на базі OpenSearch, що забезпечує зберігання, індексацію та швидкий пошук великих обсягів даних про події безпеки;
3. **Wazuh Agents:** легковагі клієнти, що встановлюються на кінцеві точки (сервери, робочі станції) для збору системних журналів, моніторингу файлів та виявлення аномалій.

Процес інтеграції передбачає налаштування агентів для збору специфічних для фінансових установ подій, зокрема логів банківського ПЗ, систем електронного документообігу та баз даних.

Основними результатами впровадження запропонованої моделі є:

- **централізований моніторинг:** забезпечення єдиної точки збору та аналізу журналів подій з усієї інфраструктури, що є ключовим для розслідування інцидентів;
- **виявлення загроз в реальному часі:** автоматичне спрацювання правил кореляції на відомі техніки атак (напр., спроби підбору паролів, підвищення привілеїв, несанкціоноване ПЗ);

- **моніторинг цілісності файлів (FIM):** контроль за змінами у критичних системних файлах та конфігураціях фінансових додатків, що запобігає несанкціонованому втручанню;
- **аудит вразливостей:** автоматизоване сканування активів на наявність відомих вразливостей (CVE), що дозволяє встановити пріоритети оновлення.

Окрему увагу приділено тонкому налаштуванню правил кореляції (ruleset). Реалізовано моніторинг специфічних загроз (доступ до БД, UBA) та інтеграцію з каталогом MITRE ATT&CK для класифікації інцидентів.

В ході підготовки було протестовано ключові функції моніторингу. Зокрема, модуль **моніторингу цілісності файлів (FIM)** був налаштований на відстеження критичних системних файлів. Під час тестування система коректно ідентифікувала **всі** тестові спроби зміни цих файлів, генеруючи відповідні сповіщення. Це підтверджує готовність системи до захисту важливих даних та конфігурацій.

Перспективи подальшого розвитку системи полягають у її інтеграції з платформами класу SOAR (Security Orchestration, Automation and Response) для автоматизації типових сценаріїв реагування, а також у поглибленому використанні модулів машинного навчання для проактивного виявлення загроз.

Висновки. Інтеграція SIEM-системи Wazuh є ефективним та економічно обґрунтованим рішенням для державних фінансових установ. Вона дозволяє не лише швидко реагувати на інциденти, але й виявляти слабкі місця в захисті, забезпечуючи належний рівень інформаційної безпеки в умовах обмежених ресурсів. Впровадження даного рішення також сприяє виконанню вимог національних стандартів у сфері кібербезпеки та захисту інформації.

Список використаних джерел:

1. Wazuh: The Open Source Security Platform. [Електронний ресурс]. URL: https://wazuh.com (дата звернення: 12.11.2025).

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-viii (дата звернення: 12.11.2025).

УДК 004.056.55:519.21

***Шоломинський Ю.Р.,* здобувач,**
Маслова Н.О., к.т.н., доцент,
Балацька В.С., д-р філ.
Львівський державний університет безпеки життєдіяльності

КРИПТОГРАФІЧНІ АСПЕКТИ ГЕНЕРАЦІЇ БЕЗПЕЧНИХ ПРОСТИХ ЧИСЕЛ

Безпечні прості числа (safe primes) – це спеціальний клас простих чисел, що забезпечує максимальну криптографічну стійкість групових протоколів. Їх використання зменшує ризики атак на малі підгрупи й гарантує, що порядок групи має великий простий дільник, що є критично важливим для безпечного обміну ключами та цифрових підписів. Тож безпечне просте число – це просте число p, для якого виконується умова: $p = 2q+1$, де q також є простим числом [1,2].

Наприклад: $q = 11$ – просте; тоді $p = 2\times11 + 1 = 23$ – також просте, отже, $p=23$ – безпечне просте.

У криптографічних протоколах, таких як Diffie–Hellman або DSA, ми працюємо у мультиплікативній групі за модулем простого числа p:

$\mathbb{Z}^*_p = \{1,2,3,\ldots,p-1\}$.

Порядок цієї групи дорівнює $p-1$. Якщо $p=2q+1$, то:

$|\mathbb{Z}^*_p|=2q$. Тобто група має великий простий підгруповий порядок q.

Це дуже важливо, бо:

- робить дискретний логарифм складнішим (менше вразливостей через малі підгрупи);
- забезпечує відсутність коротких циклів;
- дозволяє будувати надійний генератор (primitive root) для створення криптографічних ключів.

Безпечні прості числа затосовуються у сучасних крипографічних протоколах. Так, у протоколі Diffie–Hellman затосовується алгорим:

1. обирається велике безпечне просте p=2q+1.
2. вибирається генератор g, який має порядок q у групі $\mathbb{Z}^*_p$. Ключі користувачів обчислюються за формулами:

$A=g^a \bmod p$, $B=g^b \bmod p$, і спільний ключ: $K = g^{ab} \bmod p$.

Якщо p не є безпечним простим, можливі атаки через підгрупи малого порядку (small subgroup attacks).

В той же час алгорим DSA (Digital Signature Algorithm) використовує ті самі параметри p,q,g, де $p=2q+1$. Але безпечність підпису гарантується складністю обчислення дискретного логарифма в підгрупі порядку q. Прикладами безпечних простих чисел є, наприклад, для q= 5,11,23,29,83; p = 2q+1 = 11,23,47,59,167 відповідно.

У реальних криптографічних системах q і p мають сотні або тисячі біт (наприклад, $q \approx 256$ біт, $p \approx 2048$ біт), тож приклади безпечних простих чисел є демонстраційними.

Наведемо алгоритм пошуку Safe prime:

1) генеруємо випадкове непарне просте q;

2) обчислюємо p=2q+1;

3) перевіряємо, чи p також просте (наприклад, тестом Міллера–Рабіна). Якщо обидва прості – p є безпечним простим. Результати роботи алгоритму й частотний розподіл безпечних простих чисел в інтервалі [1-2000] наведено на рисунку 1.

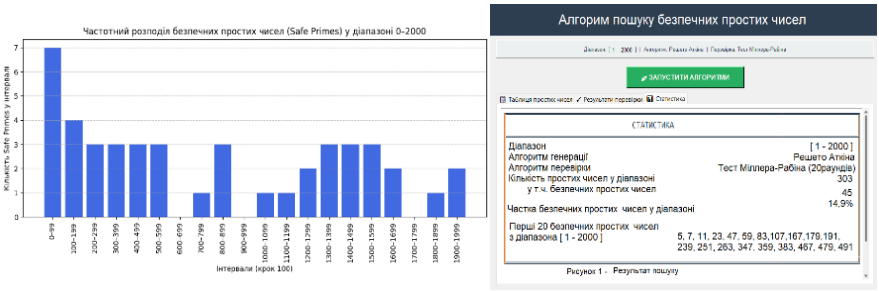


Рисунок 1 – Результати роботи алгоритму

Кількість простих чисел, наприклад, на інтервалі від 1 до 2000 дорівнює 303, тоді як Safe primes – усього сорок п’ять.

Реалізація дозволяє поєднати генерацію простих чисел та пошук безпечних простих чисел в одному проході, й цим знизити обчислювальні витрати.

Новий аспект полягає в тому, що решето Аткіна застосовано не лише для пошуку простих чисел в діапазоні, а й для фільтрації їх підмножини вигляду p=2q+1, релевантної криптографічним протоколам (Diffie–Hellman, DSA).

Список використаних джерел:

1. Gathen J., Shparlinski I. E. Generating safe primes // Journal of Mathematical Cryptology. – 2013. – Vol. 7, № 4. – P. 333–365. – DOI 10.1515/jmc-2013-5011.

2. Sieve of Atkin Revisited: Algorithmic Enhancements” // Scientific Bulletin of the „Politehnica” University of Bucharest, Series A. Applied Mathematics and Physics. – 2021. – Vol. 83, Issue 3. – P. 15-26.

УДК 004.056.5

Нечипорук М.В., здобувач,
Саган Б.В., здобувач,
Скальська А.Р., здобувач,
Чешун В.М., к.т.н., доцент,
Хмельницький національний університет

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ІНТЕРНЕТ-ПРОВАЙДЕРА

Інформаційна безпека в умовах стрімкого розвитку цифрових технологій та зростаючих загроз у кіберпросторі є однією з пріоритетних задач [1]. Надійна система захисту інформаційних ресурсів має гарантувати безперервну роботу сервісів [2], захист персональних даних користувачів [3], а також здатність своєчасно виявляти та нейтралізовувати потенційні атаки [4].

В межах проведених робіт вирішувалось завдання проєктування, реалізації та тестування інформаційної системи інтернет-провайдера, що здатна виявляти та протидіяти базовим видам кіберзагроз.

На першому етапі проведено ґрунтовний теоретичний аналіз стану проблеми, визначено основні види шкідливого програмного забезпечення (віруси, трояни, скриптові ін’єкції, програми-шпигуни тощо) та проаналізовано сучасні підходи до побудови систем захисту на рівні прикладного програмного забезпечення, баз даних і мережевої інфраструктури. Особливу увагу приділено аналізу відкритих вразливостей, таких як SQL-ін’єкції, XSS-атаки, обхід автентифікації та підміна запитів.

На другому етапі спроєктовано структуру бази даних для обліку користувачів та супутніх дій, яка містить такі компоненти:

- основна таблиця users для зберігання облікових записів;
- logs для фіксації усіх дій користувачів (входів, помилок, спроб доступу);
- alerts для зберігання зафіксованих інцидентів безпеки;
- access_tokens для управління авторизаційними сесіями;
- roles і user_roles для реалізації рольової моделі доступу;
- security_settings як механізм конфігурації параметрів безпеки без втручання в код.

Реалізація бази даних здійснювалася за допомогою середовища phpMyAdmin, а логіка обробки даних – за допомогою мови PHP. Застосовано алгоритм хешування SHA-256 для паролів користувачів, що гарантує незворотність та захист від компрометації облікових даних. Для захисту персональної інформації реалізовано шифрування поля full_name з використанням симетричного алгоритму AES-256, що

забезпечує конфіденційність у випадку несанкціонованого доступу до бази даних.

Окремо розглянуто реалізацію фільтрації вхідних даних користувача. Запити, які містять шкідливі патерни (наприклад, SQL-ін'єкцію або XSS), розпізнаються засобами регулярних виразів і не обробляються, а їхній вміст автоматично записується у таблицю alerts. Це дозволяє фіксувати всі підозрілі дії та потенційні загрози для подальшого аналізу.

Також реалізовано рівневе управління доступом: користувачам можуть бути призначені різні ролі, що обмежують або розширюють їхні можливості в системі. Такий підхід відповідає принципу мінімальних привілеїв та забезпечує сегментацію доступу до критично важливих компонентів.

Система успішно протестована за допомогою низки імітаційних сценаріїв, у тому числі – моделювання входу користувача, шкідливих запитів, перевищення дозволених спроб входу та завершення сесій. Під час тестування підтверджено:

- правильність обробки персональних даних;
- коректність дій системи при виявленні атак;
- стабільність при багаторазовому доступі;
- працездатність функціоналу автоматичного логування та шифрування;
- гнучкість системи налаштувань безпеки.

Результати показали, що реалізована система відповідає сучасним вимогам до інформаційної безпеки для веб-застосунків та може слугувати прототипом для впровадження у провайдерських середовищах, корпоративних мережах та малих IT-інфраструктурах.

Список використаних джерел:

1. Зубок В.Ю., Мохор В.В. Кібербезпека топології INTERNET : монографія. К. : ІПМЕ ім. Г.Є.Пухова, 2022. 191 с.

2. Геєць В.М. Соціальна реальність у цифровому просторі. Економіка України. 2022. №1. С. 3-28. DOI: https://doi.org/10.15407/economyukr.2022.01.003

3. Бакаєв О.О., Суський Г.В. Методи захисту персональної інформації в інформаційних системах Телекомунікаційні та інформаційні технології. 2024. №2(83). С. 68-77. DOI: 10.31673/2412-4338.2024.028190

4. Шторгін Б. Дослідження та програмна реалізація системи надання доступу до мережі Internet сервіс провайдера. Збірник праць молодих науковців ЦНТУ. 2024. Вип.14. С. 318-328.

УДК 004.056.5

Декалюк Б.О., здобувач,
Ханін Н.В., здобувач,
Чешун Д.В., викладач
Хмельницький фаховий економіко-технологічний коледж УЕП

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Вибір методу виявлення вразливостей залежить від багатьох факторів, зокрема від етапу життєвого циклу, наявності вихідного коду та типу вразливостей, які очікується знайти. Існують три основні автоматизовані підходи (SAST, DAST, IAST) та ручне тестування [1-3].

Для класифікації загроз часто використовують загальновизнані стандарти, такі як OWASP Top 10 [4].

Ці стандарти забезпечують єдину мову та методологію для ідентифікації, класифікації та реагування на загрози, роблячи процес тестування безпеки додатків (Application Security Testing) більш структурованим та результативним, а також дозволяють робити порівняльну оцінку ефективності методів виявлення проти класів вразливостей (таблиця 1).

Таблиця 1 – Оцінка ефективності методів проти класів вразливостей

Клас вразливостей	SAST	DAST	IAST	Ручне тестування
Вразливості коду: SQL Ін'єкція, XSS(Cross-Site Scripting) [5]	Висока	Середня / Висока	Середня / Висока	Висока
Вразливості часу виконання, помилки конфігурації сервера, слабке управління сесіями.	Низька	Висока	Висока	Висока
Маніпуляції цінами, обхід етапів авторизації, IDOR [6]	Низька	Низька	Низька	Висока

Базуючись на аналізі методів та враховуючи технічні можливості інфраструктури можна сформулювати практичні пропозиції та рекомендації для ефективного виявлення вразливостей програмного забезпечення, що полягають у впровадженні циклічного процесу тестування безпеки.

Практичне застосування DAST є першим кроком для розгорнутого застосунку. В умовах лабораторії це реалізується розгортанням навмисно вразливого вебзастосунку у ізольованій «пісочниці» Кіберполігону.

Використання утиліти OWASP ZAP, яка надсилає тисячі тестових запитів до всіх виявлених точок входу, намагаючись знайти поширені вразливості є другим етапом. Після завершення роботи утиліти, фахівець має вручну перевірити кожну знайдену вразливість "високого" та "середнього" ризику, підтвердивши її реальну експлуатованість.

Застосування SAST та IAST буде ефективним, якщо є доступ до вихідного коду досліджуваного ПЗ. Паралельно запускається SAST-інструмент SonarQube або Snyk. Це дозволяє знайти вразливості, які DAST міг пропустити, що найважливіше – точно вказати на проблемний рядок коду, що значно прискорює виправлення.

Для запобігання XSS всі дані, що надходять від користувача, мають проходити валідацію на дозволені символи. Всі дані, що відображаються на сторінці, мають проходити контекстно-залежне кодування HTML, URL та JavaScript.

Автоматизація запуску SAST та DAST-сканерів у процесі безперервної інтеграції дозволяє виявляти вразливості при кожній зміні коду, що відповідає сучасним підходам до кіберзахисту.

Список використаних джерел:

1. Understanding Industry Perspectives of Static Application Security Testing (SAST) / Yuan Li et al. Proceedings of the ACM on Software Engineering. Volume 2, Issue FSE. Article № FSE134. P.3033-3056. DOI: https://dl.acm.org/doi/abs/10.1145/3729404.

2. DAST: Difficulty-Adaptive Slow-Thinking for Large Reasoning Models / Yi Shen et al. arXiv. 2025. №2503.04472v2. DOI: https://arxiv.org/abs/2503.04472.

3. Anoop Gupta, Sivakumar Ponnusamy. Cybersecurity and Ethical Hacking Harnessing AI. IJGIS. November 2024. DOI: https://doi.org/10.21428/e90189c8.35100e4b.

4. System approach to web application security: analysis of threats and methods of cyber protection. A. Ilienko et al. Ukrainian Information Security Research Journal. 2024. Vol. 26, №2. P. 277-293. URL: https://h7.cl/1iBLW.

5. Advancing XSS Detection in IoT over 5G: A Cutting-Edge Artificial Neural Network Approach / Rabee Alqura'n et al. IoT. 2024. №5(3). P. 478-508. DOI: https://www.mdpi.com/2624-831X/5/3/22.

6. Bhutani V., Ghassemi Toosi F., Buckley J. Analysing the Analysers: An Investigation of Source Code Analysis Tools. Applied Computer Systems. 2024. Vol. 29, Is. 1. DOI: https://h7.cl/1iC7i.

УДК 004.056.5:004.75:004.8

Денега А.Р., здобувач,
Ящук В.І., к.екон.н., доцент,
Полотай О.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

КОМПЛЕКСНИЙ ПІДХІД ДО ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ІНСАЙДЕРСЬКИМ ЗАГРОЗАМ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Інсайдерські загрози становлять один із найнебезпечніших чинників порушення інформаційної безпеки, оскільки виникають усередині системи та часто маскуються під легітимну діяльність користувачів. Ефективний кіберзахист у таких умовах потребує поєднання поведінкової аналітики, технологічних інструментів моніторингу й організаційних заходів контролю доступу. Комплексний підхід базується на аналізі аномалій у діях користувачів, застосуванні машинного навчання, багаторівневих політиках автентифікації та принципах Zero Trust, що забезпечує підвищення кіберстійкості корпоративних мереж.

Більшість інцидентів інсайдерського характеру пов'язана не лише зі зловмисними намірами, а й із людськими помилками, низьким рівнем кіберобізнаності та нехтуванням політиками безпеки. У зв'язку зі зростанням цифрової складності організаційних інфраструктур ефективна протидія інсайдерам потребує поєднання технічних, поведінкових та організаційних методів контролю. Комплексний підхід до аналізу та запобігання інсайдерським загрозам дозволяє підвищити рівень кіберстійкості й забезпечує захист критичних даних у динамічному цифровому середовищі.

Інсайдерська діяльність здатна завдати системам значної шкоди через легітимність доступу та глибоке знання внутрішньої структури мережі. Типовими проявами таких загроз є несанкціоноване копіювання конфіденційних даних, ексфільтрація інформації через електронну пошту чи хмарні сервіси, маніпуляція критичними конфігураціями, зловживання привілейованими обліковими записами та маскування шкідливих дій у системних логах.

Ключову роль у своєчасному виявленні інсайдерської активності відіграють засоби поведінкової аналітики. Системи UEBA формують базові профілі нормальної діяльності користувачів і визначають відхилення, характерні для спроб порушення політик безпеки. Додаткову точність забезпечують SIEM-рішення, які корелюють події з різних сегментів мережі й фіксують послідовності дій, що не узгоджуються зі стандартними бізнес-процесами.

У складних інфраструктурах значущу роль відіграють алгоритми машинного навчання, здатні виявляти тонкі аномалії у патернах доступу, створювати прогнозні моделі ризику та зменшувати ймовірність хибних спрацьовувань. Важливим компонентом протидії є контроль доступу: принцип мінімальних привілеїв, сегментація мережі, регулярний аудит прав користувачів, управління привілейованими записами та застосування багатофакторної автентифікації. Zero Trust-архітектура доповнює ці механізми, оскільки передбачає постійну перевірку ідентичності користувачів, пристроїв і контексту їхніх дій.

Організаційні заходи також мають суттєвий вплив на зменшення ризиків інсайдерської активності. До них належать систематичне навчання персоналу принципам кібергігієни, моделювання соціотехнічних інцидентів, впровадження політик відповідальності та моніторинг інформаційних потоків усередині організації. Синергія технічних та організаційних інструментів створює стійку архітектуру безпеки, здатну протистояти різним формам інсайдерських загроз.

Інсайдерські загрози відзначаються високим рівнем складності через наявність у порушників легітимних прав доступу та можливість маскування шкідливої активності. Ефективна протидія вимагає застосування комплексної системи, що включає поведінкову аналітику, кореляційні механізми моніторингу, алгоритми машинного навчання, жорсткі політики контролю доступу та організаційні заходи формування культури безпеки. Інтегроване поєднання цих елементів забезпечує своєчасне виявлення аномалій, зменшує ризики витоку інформації та підвищує загальну кіберстійкість корпоративних мереж.

Список використаних джерел:

1. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations : NIST Special Publication 800-53. Gaithersburg : NIST, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2. National Institute of Standards and Technology. Zero Trust Architecture : NIST Special Publication 800-207. Gaithersburg : NIST, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final

3. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2023. Athens : ENISA, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

4. Microsoft Security. Digital Defense Report 2023–2024. Microsoft Corporation, 2024. URL: https://www.microsoft.com/security/business/microsoft-digital-defense-report

УДК 004.056.5:004.75:004.8

Дмитрук Б. О., здобувач,
Ящук В.І., к.екон.н., доцент,
Ткаченко А.М., викладач
Львівський державний університет безпеки життєдіяльності

КОМПЛЕКСНИЙ АНАЛІЗ ВЕКТОРІВ ІНФІКУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ШКІДЛИВИМ ПРОГРАМНИМ КОДОМ ТА РОЗРОБЛЕННЯ БАГАТОРІВНЕВОЇ СТРАТЕГІЇ КІБЕРЗАХИСТУ

Шкідливий програмний код залишається одним з найпоширеніших та найбільш руйнівних засобів реалізації кібератак, спрямованих на порушення конфіденційності, цілісності й доступності інформаційних систем. Його проникнення здійснюється через широкий спектр векторів, що охоплюють як технічні, так і соціоінженерні методи. Комплексний аналіз таких векторів є необхідною передумовою для створення ефективної стратегії кіберзахисту сучасних цифрових інфраструктур.

До ключових векторів інфікування належать соціотехнічні атаки (phishing, spear-phishing, smishing), що базуються на використанні психологічних маніпуляцій для примушування користувачів виконати шкідливі дії; експлуатація вразливостей ПЗ та обладнання, включно з помилками в бібліотеках, драйверах, протоколах та некоректними конфігураціями серверів; компрометація ланцюгів поставок (supply chain attacks), зокрема у процесі оновлення програмного забезпечення, драйверів та контейнеризованих застосунків; використання незахищених мережевих сегментів, зокрема відкритих портів, хибно налаштованих VPN, незашифрованих протоколів взаємодії; зловживання легітимними інструментами системи (living-off-the-land techniques), коли зловмисники застосовують штатні утиліти, такі як PowerShell, WMI чи PsExec, мінімізуючи сліди активності.

У сучасних умовах класичні засоби антивірусного захисту часто виявляються недостатніми, оскільки шкідливий код дедалі частіше використовує поліморфізм, обфускацію, ін’єкції в пам’ять та безфайлові механізми. Це зумовлює необхідність переходу до багаторівневих систем захисту, що здатні реагувати не лише на відомі сигнатури, а й на поведінкові аномалії.

На рис. 1 - наведена пропонована багаторівнева стратегія кіберзахисту.

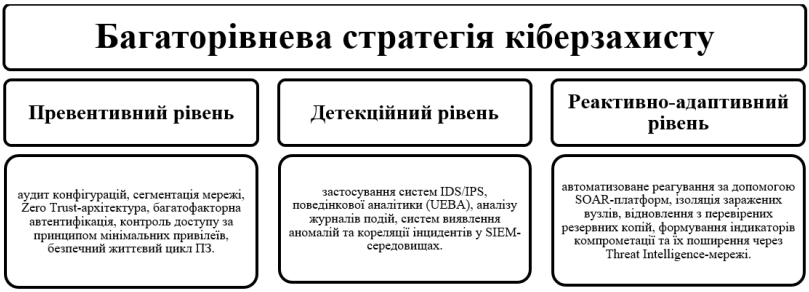


Рисунок 1 – Багаторівнева стратегія кіберзахисту

Особлива увага приділяється взаємодії між рівнями безпеки, що забезпечує стійкість системи до багатовекторних атак. Комбінація машинного навчання, аналізу поведінкових патернів і Zero Trust-підходу дозволяє мінімізувати площу атаки, обмежити рух шкідливого коду та забезпечити своєчасне виявлення навіть обфускованих або безфайлових загроз.

Комплексний аналіз векторів інфікування інформаційних систем демонструє, що сучасні атаки набувають багатокомпонентного та прихованого характеру. Ефективна протидія можливе лише за умов упровадження багаторівневого, адаптивного та проактивного кіберзахисту, що поєднує технологічні, поведінкові та політико-організаційні механізми. Запропонована стратегія дає змогу швидко виявляти шкідливий код, локалізувати наслідки інцидентів та підвищувати стійкість критично важливих цифрових інфраструктур до атак нового покоління.

Список використаних джерел:

1. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations : NIST Special Publication 800-53. Gaithersburg : NIST, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2. National Institute of Standards and Technology. Zero Trust Architecture : NIST Special Publication 800-207. Gaithersburg : NIST, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final

3. MITRE Corporation. MITRE ATT&CK Framework : Adversarial Tactics, Techniques, and Common Knowledge. McLean : MITRE, 2023. URL: https://attack.mitre.org

4. European Union Agency for Cybersecurity (ENISA). Threat Landscape Report 2023. Athens : ENISA, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

УДК 004.056.5:004.75:004.8

Краєвський Ю.Р., здобувач,
Ящук В.І., к.екон.н., доцент,
Полотай О.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

МЕТОДОЛОГІЯ ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ ФІШИНГОВИХ АТАК ІЗ ВИКОРИСТАННЯМ СИСТЕМИ ЗАХИСТУ ЕЛЕКТРОННОЇ ПОШТИ MICROSOFT DEFENDER FOR OFFICE 365

Фішингові атаки залишаються одним із найрезультативніших методів компрометації інформаційних систем, оскільки спрямовані на людський фактор і широко застосовуються для викрадення облікових даних, розповсюдження шкідливого ПЗ та здійснення фінансових шахрайств. У корпоративному середовищі ефективність протидії фішингу залежить від здатності системи безпеки аналізувати контент листів, перевіряти достовірність відправника, виявляти маніпулятивні або підозрілі елементи й блокувати шкідливу активність до взаємодії користувача з повідомленням. Microsoft Defender for Office 365 інтегрує набір механізмів, що базуються на машинному навчанні, сигнатурному аналізі та поведінкових алгоритмах, забезпечуючи багаторівневий захист поштової інфраструктури.

Фішингові кампанії ґрунтуються на підробці легітимної комунікації, модифікації заголовків та доменів, використанні шкідливих вкладень і гіперпосилань, що перенаправляють користувача на фальшиві ресурси. Виявлення таких листів потребує аналізу контексту повідомлення, автентичності доменів, структури тіла листа, конфігурації вкладень і параметрів мережевої взаємодії.

Система Microsoft Defender for Office 365 забезпечує багатовекторний захист електронної пошти завдяки поєднанню механізмів перевірки автентичності доменів, аналізу поведінки відправника та динамічної оцінки ризикових ознак листів у режимі реального часу. Microsoft Defender for Office 365 забезпечує глибоку перевірку вхідної кореспонденції шляхом застосування технологій anti-phishing policies, які оцінюють доменну репутацію, перевіряють SPF, DKIM і DMARC, аналізують ризикові шаблони поведінки відправника та виявляють підміну імені або адреси. Алгоритми машинного навчання моделюють сотні ознак електронного листа, включно з семантикою тексту, структурою HTML, характеристиками вкладень і метаданими, що дозволяє розпізнавати навіть складні таргетовані атаки.

Додаткову лінію захисту формує механізм Safe Links, який виконує динамічний аналіз URL-адрес у режимі реального часу та блокує доступ

до фішингових сайтів, навіть якщо початковий лист пройшов первинну перевірку. Функція Safe Attachments ізолює вкладення у віртуальному середовищі й досліджує їхню поведінку для виявлення ознак шкідливих скриптів, макросів або експлойтів.

Системи автоматизованого реагування (Automated Investigation and Response, AIR) виконують кореляцію інцидентів, ізолюють скомпрометовані листи у поштових скриньках, ініціюють блокування небезпечних відправників та виявляють взаємопов'язані загрози у масштабі всієї організації.

Поєднання технологічних механізмів із політиками доступу та навчанням користувачів формує цілісну систему протидії фішингу. Важливе значення має регулярне оновлення поштових політик, моделювання фішингових атак, контроль репутаційних атрибутів доменів та застосування багатофакторної автентифікації.

Методологія протидії фішинговим атакам у середовищі Microsoft Defender for Office 365 ґрунтується на багаторівневому аналізі електронних листів, поєднанні сигнатурних та поведінкових методів, використанні машинного навчання та ізоляції підозрілих елементів у спеціалізованих середовищах. Технології Safe Links та Safe Attachments дозволяють виявляти приховані форми фішингу та блокувати їх до того, як вони становитимуть ризик для користувача. Інтелектуальні механізми автоматизованого реагування забезпечують швидке усунення інцидентів і мінімізацію наслідків атак. Комплексність підходу створює основу для підвищення кіберстійкості організаційної поштової інфраструктури та зменшує ймовірність успішної компрометації користувачів.

Список використаних джерел:

1. Microsoft. Microsoft Defender for Office 365 Technical Documentation. Microsoft Docs, 2024. URL: https://learn.microsoft.com/microsoft-365/security/office-365-security/

2. National Institute of Standards and Technology. Trustworthy Email : NIST Special Publication 800-177. Gaithersburg : NIST, 2020. URL: https://csrc.nist.rip/publications/detail/sp/800-177/rev-1/draft

3. European Union Agency for Cybersecurity (ENISA). Phishing Threat Landscape 2023. Athens : ENISA, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

4. Mandiant Intelligence. Phishing Trends and Techniques Report 2024. Mandiant, 2024. URL: https://www.mandiant.com/resources

УДК 004.056.5:004.738.5

Черкас С.А., здобувач,
Ящук В.І., к.екон.н., доцент,
Пановик У.П., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ БЕЗПЕКИ ДЛЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ IOT-СИСТЕМ У ПОБУТОВОМУ СЕРЕДОВИЩІ

Стрімке зростання кількості IoT-пристроїв у побутових мережах створює нові вектори кібератак і підвищує ризики несанкціонованого доступу до персональних даних користувачів. Існуючі стандарти безпеки, зокрема ENISA, NIST та OWASP, здебільшого орієнтовані на корпоративний сектор, що ускладнює їх застосування в умовах обмежених ресурсів побутових систем. Автори сформували інтегровану модель кіберзахисту, яка враховує специфіку домашнього середовища, динамічність підключень та економічні аспекти реалізації безпечного життєвого циклу пристроїв.

Методологічна основа дослідження включає системний підхід до оцінки кіберстійкості IoT-систем, моделювання тестових середовищ (honeypots, sandbox, digital twins), використання емпіричних методів перевірки захисних механізмів і побудову кількісних метрик за п’ятьма доменами: апаратна безпека, мережевий захист, життєвий цикл, приватність і операційна стійкість**.** Вагові коефіцієнти для кожного домену дозволяють адаптувати оцінку під конкретні сценарії – критичні або комфортні пристрої.

Запропонована модель підтримує уніфікований процес тестування: інвентаризація пристроїв, базове сканування вразливостей, функціональні та атакуючі тести, вимірювання показників відновлення (MTTR), детекції інцидентів та ефективності контрзаходів. Верифікація здійснюється через повторні експерименти та кореляцію результатів. Особливу увагу приділено етичним аспектам проведення експериментів, забезпеченню конфіденційності даних і дотриманню принципів відповідального розкриття вразливостей (responsible disclosure).

Економічна складова дослідження базується на поєднанні моделей Total Cost of Ownership (TCO) і Cost–Benefit Analysis, що дає змогу оцінити економічну доцільність заходів кіберзахисту. Передбачено впровадження маркування рівня безпеки («security label»), яке стимулює виробників до пролонгованої підтримки продуктів і підвищення довіри користувачів. Пілотне дослідження включає 20–30

пристроїв п’яти типів, охоплює типові топології домашніх мереж та різні сценарії атак (brute-force, MITM, експлуатація CVE, DDoS тощо).

Результати валідації підтверджують відтворюваність запропонованої методології та її ефективність у кількісній оцінці безпеки IoT-екосистем. Формування стандартизованих рейтингів безпеки пристроїв створює передумови для розвитку регуляторних вимог, а відкритий науковий репозиторій результатів забезпечує прозорість і доступність методики для подальших досліджень.

Запропонована комплексна модель захисту IoT-пристроїв у побутовому середовищі поєднує технічні, поведінкові та економічні підходи до забезпечення кіберстійкості. Її основою є кількісно-орієнтована методологія оцінки безпеки, що дозволяє уніфікувати процес тестування, формувати порівняльні рейтинги пристроїв і розробляти практичні рекомендації для виробників, користувачів і регуляторних органів. Впровадження запропонованої моделі сприятиме підвищенню конфіденційності, цілісності та доступності даних у побутових IoT-мережах, а також розвитку стандартів і політик кіберзахисту споживчих технологій.

Список використаних джерел:

1. ENISA – Guidelines for Securing the Internet of Things (2020) doi: 10.2824/314452.

2. NIST – Cybersecurity for IoT / Consumer IoT Cybersecurity (SP-серія, 2022 і суміжні документи). Електронне видання. Режим доступу: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program.

3. OWASP – Internet of Things Project / IoT Top 10 Електронне видання. Режим доступу: https://owasp.org/www-project-internet-of-things/

4. Пановик У. П., Кутас С.А. Інтернет речей для інтелектуального поліграфічного виробництва. Поліграфія і видавнича справа, № 1(87),2024, С. 61–74. URL: https://doi.org/10.32403/0554-4866-2024-1-87-61-74.

5. Пановик У. П. Кібербезпека в телекомунікаційних мережах та системах. Наукові записки, № 1(68), 2024, С. 122–135. URL: https://doi.org/10.32403/1998-6912-2024-1-68-122-135

7. Пановик У. П. Стандартизація інтернету речей: сучасний стан та перспективи розвитку. Поліграфія і видавнича справа. 2023. № 1 (85). С. 51–64. URL: https://doi.org/10.32403/0554-4866-2023-1-85-51-64.

УДК 004.8:004.9

Щерб'як М.Т., здобувач,
Ящук В.І., к.екон.н., доцент,
Шклярський Р.А., викладач
Львівський державний університет безпеки життєдіяльності

РОЗРОБЛЕННЯ КОНЦЕПТУАЛЬНОЇ МОДЕЛІ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ТОВ «ІНФО ПРОСТІР ПЛЮС» ВІД НЕСАНКЦІОНУВАНОГО ДОСТУПУ НА ОСНОВІ БАГАТОРІВНЕВОЇ АРХІТЕКТУРИ БЕЗПЕКИ

У сучасному цифровому середовищі корпоративні мережі перебувають під постійним впливом широкого спектра кіберзагроз, зокрема несанкціонованих спроб доступу, атак на автентифікаційні механізми, експлуатації мережевих вразливостей і маніпуляцій із конфігураційними параметрами систем. Стійкість інформаційної інфраструктури організації залежить від здатності вчасно протидіяти зовнішнім і внутрішнім ризикам, забезпечуючи захист на кожному рівні взаємодії користувачів і сервісів.

Для ТОВ «ІНФО ПРОСТІР ПЛЮС» важливою є побудова моделі, яка поєднує структуровані механізми контролю доступу, сегментацію мережевих ресурсів, інструменти моніторингу та автоматизоване реагування на інциденти. Багаторівнева архітектура безпеки дає змогу реалізувати комплексний підхід до захисту, у якому кожен рівень функціонує як автономна лінія оборони та взаємодіє з іншими для формування єдиної системи. Таке поєднання технічних засобів, політик конфіденційності й організаційних заходів створює умови для мінімізації ризиків несанкціонованого доступу та забезпечує стабільне функціонування ІТ-інфраструктури підприємства.

Несанкціонований доступ виникає внаслідок комп'ютерних атак, компрометації облікових даних, помилок користувачів або неправильно налаштованих компонентів мережі. Уразливість може з'являтися як на рівні фізичної інфраструктури, так і в логічній конфігурації систем, що зумовлює необхідність комплексного контролю.

Побудова концептуальної моделі системи захисту передбачає використання принципів «глибинної оборони». Першим рівнем виступає автентифікація користувачів, включно з багатофакторною перевіркою, біометричними ідентифікаторами, політиками складності паролів та обмеженням доступу на основі ролей. Другий рівень включає сегментацію корпоративної мережі. Розділення інфраструктури на логічні зони за допомогою VLAN, фільтрації трафіку на межах сегментів та виділення окремих контурів для критично важливих

ресурсів підвищує контрольованість інфраструктури та знижує ризик поширення атак. Третій рівень моделі ґрунтується на технологіях виявлення аномалій та вторгнень. IDS/IPS-системи аналізують мережевий трафік, визначають характерні відхилення та блокують підозрілу активність. SIEM-рішення забезпечують централізований збір логів, кореляцію подій, аналіз дій користувачів і пристроїв, формуючи цілісну картину стану безпеки. Четвертий рівень – системи управління конфігураціями, аудит інфраструктури та контроль цілісності. Регулярна перевірка прав доступу, журналів змін і конфігураційних файлів зменшує ризики, пов'язані з помилками адміністрування та непоміченими модифікаціями.

Важливу роль відіграє також організаційний компонент: розроблення регламентів, політик безпеки, проведення навчання для співробітників та підтримання культури відповідальної роботи з даними. У поєднанні з концепцією Zero Trust, яка передбачає постійну перевірку користувачів, пристроїв, місця розташування та контексту запиту, така архітектура створює високий рівень захищеності корпоративної мережі ТОВ «ІНФО ПРОСТІР ПЛЮС».

Багаторівнева архітектура безпеки забезпечує системну протидію несанкціонованому доступу та дозволяє охопити всі ключові складові корпоративної інфраструктури – від автентифікації до моніторингу й аналізу поведінкових патернів. Ефективність захисту визначається узгодженою роботою механізмів контролю доступу, сегментації мережі, моніторингу трафіку та кореляції подій, а також відповідністю політик безпеки сучасним стандартам кіберзахисту. Комплексна модель створює передумови для підвищення кіберстійкості підприємства, знижує ймовірність успішної компрометації критичних ресурсів і гарантує надійне функціонування інформаційних процесів. Реалізація інтегрованого підходу особливо важлива для ТОВ «ІНФО ПРОСТІР ПЛЮС», оскільки забезпечує захист бізнес-процесів, мінімізує ризики внутрішніх і зовнішніх загроз та відповідає сучасним вимогам корпоративної безпеки.

Список використаних джерел:

1. Ящук В. І. Методика забезпечення безпеки інформаційних систем та реагування на кіберінциденти кібербезпековими центрами // Scientific Collection «InterConf+». 2024. Vol. 45(201) : Proceedings of the 8th International Scientific and Practical Conference «International Scientific Discussion: Problems, Tasks and Prospects», May 19–20, 2024, Brighton, United Kingdom / comp. LLC SPC «InterConf». Brighton : A.C.M. Webb Publishing Co Ltd., 2024. P. 632–641. DOI: https://doi.org/10.51582/interconf.19-20.05.2024

УДК 004.7

Маруняк С.Т., аспірант,
Кирик М.І., д.т.н., професор,
Національний університет «Львівська політехніка»

ІНТЕРПРЕТОВАНИЙ АНАЛІЗ ОЗНАК ДЛЯ ПІДВИЩЕННЯ ТОЧНОСТІ КЛАСИФІКАЦІЇ АНОМАЛІЙ BGP

Протокол BGP забезпечує обмін маршрутизованою інформацією між автономними системами (AC), тому його стабільність є критичною для безперебійної роботи Інтернету. Помилки в конфігурації, підміна префіксів або масові виходи з ладу можуть призводити до дестабілізації глобальних маршрутів. Для зменшення наслідків таких інцидентів важливо не лише виявити факт аномалії, а й визначити її тип – збій у мережі (outage), підміна маршруту (hijack) чи інші форми порушень. Це дозволяє обрати відповідну реакцію: від технічного відновлення до втручання операторів.

Для автоматизованої класифікації BGP-аномалій використовують десятки ознак, сформованих на основі потоків повідомлень BGP. Проте надлишкова кількість або слабоінформативні параметри можуть знижувати якість класифікації. Щоб виявити найбільш релевантні ознаки, застосовують методи пояснення моделей – Explainable AI (XAI). Одним із таких методів є SHapley Additive exPlanations (SHAP) [1], який дозволяє оцінити вплив кожної ознаки на результат класифікації як загалом, так і для окремих класів аномалій.

На рисунку 1 представлено результат глобального аналізу ознак за допомогою SHAP для базової моделі. Найбільший вплив мають характеристики, пов’язані з топологією маршрутів та географічною відстанню. Натомість дві ознаки, пов’язані з довжиною префіксів IPv4, показали найменші значення важливості.

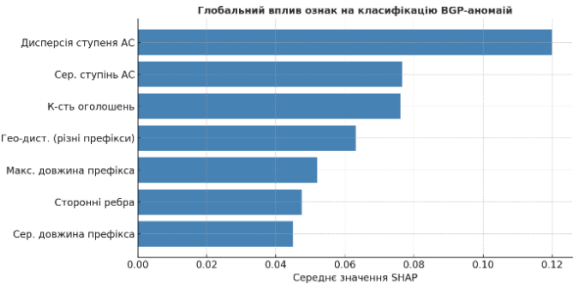


Рисунок 1 – Глобальний вплив ознак на класифікацію аномалій

Для перевірки впливу цих ознак на продуктивність моделі було проведено два вимірювання: з повним набором ознак (табл. 1) та після їх часткового видалення (табл. 2). Модель класифікує три типи аномалій: прямі (direct), непрямі (indirect) та відключення (outage). Ключові метрики: точність (Precision), повнота (Recall), F1-score. Вони характеризують частку правильно класифікованих тестових даних, повноту виявлення об'єктів певного класу та баланс між ними відповідно.

Таблиця 1 – Метрики класифікації вихідної моделі

Class	Precision	Recall	F1-score
Direct	1.00	1.00	1.00
Indirect	0.87	1.00	0.93
Outage	1.00	0.67	0.80

Таблиця 2 – Метрики класифікації моделі після вилучення ознак

Class	Precision	Recall	F1-score
Direct	1.00	1.00	1.00
Indirect	0.91	0.99	0.95
Outage	0.97	0.77	0.86

Після вилучення двох найменш значущих ознак модель почала точніше ідентифікувати випадки відключень: показник повноти для цього класу зріс з 0.67 до 0.77. Це означає, що система стала виявляти більшу частку реальних інцидентів типу збій, не пропускаючи їх. При цьому важливо, що якість класифікації інших типів аномалій залишилася на високому рівні – тобто вилучення ознак не спричинило зменшення точності або зростання хибнопозитивних спрацювань у цих класах. Такий підхід дозволяє не лише оптимізувати модель, а й підвищити її стійкість до шуму у вхідних даних. Подібні інтерпретовані методи можна використовувати і для подальшої оптимізації складніших моделей.

Список використаних джерел:

1. Al-Musawi B., Branch P., Armitage G. BGP anomaly detection techniques: A survey // IEEE Communications Surveys & Tutorials. 2016. Vol. 19, No. 1. P. 377–396. DOI: https://doi.org/10.1109/COMST.2016.2622240

2. Kyryk M., Maruniak S., Tandrukhiv M. SHAP-based Feature Contribution Analysis for Robust BGP Anomaly Classification // Telecommunications and Radio Engineering. 2025. Vol. 84, No. 4. P. 391–400.

УДК 35:004.056.5

Бень Д.Ю., здобувач,
Ткачук Р.Л., д.т.н., професор,
Ящук В.І., к.екон.н., доцент
Львівський державний університет безпеки життєдіяльності

АДМІНІСТРАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Стрімка цифровізація та зростання кіберзагроз, особливо в умовах гібридної агресії проти України, роблять критично важливим ефективне адміністративно-правове врегулювання діяльності суб'єктів сектору безпеки і оборони, оскільки узгодженість їхніх повноважень визначає здатність держави забезпечувати кіберстійкість та оперативно реагувати на кіберінциденти.

Нормативно-правову основу формують Закон України «Про основні засади забезпечення кібербезпеки України» (2017), Закон України «Про національну безпеку України» (2018), Стратегія кібербезпеки України (2021), Закон України «Про основи національного спротиву» (2021), а також численні підзаконні акти: Положення про Держспецзв'язку, Положення про Службу безпеки України, нормативи НЦКБ при РНБО. Попри розширення нормативного масиву, чинне законодавство все ще містить колізії й прогалини, що стосуються розмежування функцій державних органів. Найбільш проблемними є питання дублювання повноважень між Держспецзв'язку (як технічним регулятором), СБУ (як контррозвідувальним органом), Кіберполіцією та Міністерством оборони. Невизначеність меж компетенції створює «сірі зони» у державному управлінні, що негативно впливає на координацію та швидкість реагування на кіберінциденти.

Особливого значення набуває уточнення адміністративно-правового статусу суб'єктів сектору безпеки в умовах воєнного стану, оскільки ефективність протидії кібератакам (WhisperGate, HermeticWiper, NotPetya, Deface 2022–2024) залежить насамперед від чіткості алгоритмів взаємодії та нормативного визначення компетенції органів.

Дослідження зосереджувалося на комплексному адміністративно-правовому аналізі статусу та компетенції суб'єктів сектору безпеки і оборони у сфері кібербезпеки з урахуванням національного законодавства, галузевих стандартів і міжнародних підходів НАТО та ЄС. Особлива увага приділяється нормативно-правовим механізмам організації кіберзахисту та розподілу повноважень між СБУ, Держспецзв'язку, НЦКБ, Міноборони та іншими ключовими суб'єктами.

На підставі проведених досліджень, на нашу думку, ключові проблемні аспекти можна сформулювати наступним чином:

– відсутність чіткого розмежування між функціями кіберзахисту (Держспецзв'язку), кіберрозвідки та контррозвідки (СБУ, ГУР МОУ) створює правові прогалини, які можуть бути використані противником;

– діяльність НЦКБ потребує розширення адміністративно-правових механізмів впливу та підпорядкування єдиній вертикалі рішень щодо реагування на критичні кіберінциденти;

– євроатлантична інтеграція має охоплювати не лише технічну, а й правову сумісність із підходами НАТО, зокрема відповідно до NATO Cyber Defence Policy, Tallinn Manual 2.0, EU Cybersecurity Act та Директиви NIS2.

Таким чином, удосконалення адміністративно-правових механізмів, усунення законодавчих колізій та впровадження єдиного стратегічного підходу до міжвідомчої координації є ключовим для формування ефективної та стійкої системи кіберзахисту України. Це забезпечує чітке визначення компетенцій органів, оперативне реагування на загрози та гармонізацію національних стандартів із практиками НАТО та ЄС.

Список використаних джерел:

1. Законодавство України. Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua

2. Regulation (EU) 2019/881 of the European Parliament and of the Council «Cybersecurity Act». URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj

3. NATO. Comprehensive Cyber Defence Policy. 2021. URL: https://www.act.nato.int/activities/cyber/

4. NATO. How NATO-Accredited Cyber Defence Centre of Excellence Advances Legal Interoperability. 2025. URL: https://www.act.nato.int/article/ccdcoe-2025/

5. Івануса А. І., Ткачук Р. Л., Брич Т. Б. Удосконалення методів управління процесами інформаційної безпеки // Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : матеріали III Міжнар. наук.-практ. конф., Хмельницький, 21 листопада 2024 р. Хмельницький : НАДПСУ, 2024. С. 1136–1138.

УДК 327.56:004.056.5

Зеленчук А.Р., здобувач,
Ткачук Р.Л., д.т.н., професор,
Федина Б.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

ІНФОРМАЦІЙНА БЕЗПЕКА В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Інформація у сучасному суспільстві є ключовим ресурсом розвитку економіки, науки та технологій, використовується для управління процесами та міжособистісної взаємодії, а її цінність визначається достовірністю, корисністю та доступністю. На макрорівні вона забезпечує державну потугу, ефективне управління економікою та оборонними системами, на мікрорівні – ефективність діяльності підприємств і органів влади.

Інформаційна безпека як складова національної безпеки забезпечує захист даних та інфраструктури, охоплюючи доступність, цілісність і конфіденційність інформації, і стосується захисту інтересів держави, особистості та суспільства, запобігаючи маніпуляціям, дезінформації та інформаційно-психологічним впливам.

Основні загрози інформаційній безпеці виникають як внутрішні (недосконаліть правової системи, низька інформаційна культура, внутрішні комп'ютерні злочини), так і зовнішні (політичний та економічний тиск, діяльність іноземних спецслужб, міжнародний кібертероризм). Вони включають неякісну або фальшиву інформацію, несанкціонований доступ, відмови технічних засобів і порушення прав на інформацію. Особливе значення має кібертероризм, що швидко адаптується до нових технологій, а його транснаціональний характер ускладнює контроль.

Для підвищення рівня інформаційної безпеки (ІБ) держави, суспільства та окремих організацій рекомендується комплексний підхід, який включає наступні напрямки:

Технічні заходи – передбачають впровадження систем виявлення і запобігання вторгнень (IDS/IPS), багатофакторної автентифікації (MFA), розширеного шифрування даних, систем контролю мобільних пристроїв та захисту електронної пошти. Ці засоби дозволяють запобігти несанкціонованому доступу, зберегти цілісність інформації та забезпечити надійність функціонування інформаційної інфраструктури.

Інноваційні підходи – включають застосування штучного інтелекту (ШІ) та методів машинного навчання для прогнозування загроз, виявлення аномалій у великих масивах даних та автоматичного

реагування на інциденти. Використання таких технологій підвищує швидкість і ефективність захисту інформаційних систем у динамічному кіберпросторі.

Організаційні заходи – полягають у підготовці та навчанні персоналу, розмежуванні доступу за принципом мінімальних привілеїв, регулярних тренуваннях із кібербезпеки, а також розробці внутрішніх політик і процедур реагування на інциденти. Ці заходи забезпечують підвищення культури інформаційної безпеки і мінімізацію людського фактору як джерела ризиків.

Криптографічний захист та блокчейн – включає використання сучасних криптографічних алгоритмів і технології блокчейн для забезпечення цілісності, достовірності та незмінності даних. Технологія блокчейн підвищує надійність фінансових транзакцій та зберігання інформаційних ресурсів, запобігає маніпуляціям і несанкціонованим змінам, забезпечуючи прозорість та контроль за потоками даних.

Міжнародна співпраця – передбачає інтеграцію у глобальні системи забезпечення інформаційної безпеки, обмін інформацією про загрози та інциденти, координацію спільних заходів із запобігання кібератакам і протидії транснаціональним інформаційним загрозам. Це дозволяє країні не лише захистити власні ресурси, а й підвищити ефективність міжнародних механізмів реагування на глобальні виклики.

Таким чином, інформаційна безпека є багатогранним процесом управління загрозами, що включає технічні, організаційні, правові та інноваційні складові. Забезпечення ІБ вимагає системного підходу, де поєднуються сучасні технології, нормативно-правова база, організаційні заходи та міжнародна кооперація, що гарантує стабільність, надійність і розвиток інформаційного простору держави.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» : Указ Президента України. від 16.02.2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text

2. Івануса А. І., Ткачук Р. Л., Брич Т. Б. Удосконалення методів управління процесами інформаційної безпеки. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : матеріали III Міжнародної науково-практичної конференції (Хмельницьк, 21 листопада 2024 р.). Хмельницький: НАДПСУ, 2024. С. 1136–1138.

УДК 327.56:004.056.5

Кривий Р.А., здобувач,
Ткачук Р.Л., д.т.н., професор,
Балацька В.С., д-р. філ., ст. викладач
Львівський державний університет безпеки життєдіяльності

КІБЕРБЕЗПЕКА БАНКІВСЬКОГО СЕКТОРУ: СУЧАСНІ ЗАГРОЗИ ТА РОЛЬ ШІ У ПРОТИДІЇ

Зростання кіберзагроз у фінансовому секторі підвищує потребу в постійному оновленні систем захисту банківської інформації. Українські банки загалом захищені від існуючих загроз, проте сучасні виклики, зокрема пов'язані із застосуванням ШІ, потребують впровадження передових технічних рішень та розвитку культури інформаційної безпеки. Сфера ІБ в Україні базується на національних законах («Про інформацію», «Про захист персональних даних», «Про електронні комунікації») та міжнародних стандартах GDPR і ISO/IEC 27001. Технічний захист реалізується через нормативні вимоги, організаційну інфраструктуру та матеріально-технічні засоби, ключову роль серед яких відіграють системи DLP. Основні технічні канали витоку – акустичні, радіотехнічні, оптичні, електричні та матеріально-речові – нейтралізуються комплексом інженерно-технічних заходів.

Банківська система є критичною складовою економіки, а її стійкість визначає рівень фінансової безпеки держави. Цифровізація фінансових послуг супроводжується збільшенням обсягів даних, що містять персональну інформацію клієнтів, комерційні відомості та банківську таємницю, підвищуючи вразливість до кібератак (фішинг, DDoS, атаки на платіжні системи), внутрішніх загроз та інформаційно-психологічного впливу на співробітників і клієнтів.

Опираючись на проведений аналіз, основні сучасні виклики можна узагальнити у вигляді наступних загроз:

– кіберзлочинність – фішинг, шкідливе програмне забезпечення, несанкціонований доступ до баз даних та крадіжку фінансових ресурсів;

– штучні загрози, створені із застосуванням ШІ, які дозволяють автоматизувати атаки, обходити традиційні системи безпеки та прогнозувати поведінку користувачів;

– внутрішні ризики, пов'язані з людським фактором та порушенням процедур доступу;

– інформаційні обмеження, які впливають на своєчасність виявлення загроз та реагування на них.

Ці чинники ускладнюють забезпечення конфіденційності, цілісності та доступності даних банківської системи, що робить її вразливою до матеріальних, репутаційних і стратегічних втрат.

Ефективні заходи захисту на наш погляд мають включати:

Технічні засоби: впровадження систем виявлення вторгнень (IDS/IPS), багатофакторної автентифікації (MFA), розширеного шифрування даних, а також систем захисту електронної пошти та контролю мобільних пристроїв.

Інноваційні підходи: використання ШІ та методів машинного навчання для прогнозування загроз, аналізу великих обсягів даних та автоматичного реагування на аномалії.

Організаційні заходи: навчання персоналу, розмежування доступу за принципом найменших привілеїв та регулярні кібервійськові тренування.

Криптографічний захист: застосування квантового шифрування для підвищення стійкості систем до сучасних атак.

Технологія блокчейн: впровадження децентралізованих реєстрів для забезпечення прозорості, незмінності та додаткового рівня захисту даних, що знижує ризики шахрайства та несанкціонованого втручання.

Комплексне поєднання технічних, організаційних і криптографічних заходів, а також активне використання ШІ дозволяє забезпечити високий рівень стійкості банківських інформаційних систем, знижує ризики матеріальних та репутаційних втрат і підвищує готовність до реагування на новітні кіберзагрози.

Список використаних джерел:

1. Про затвердження Положення про використання засобів криптографічного захисту інформації Національного банку України : Постанова від 14.04.2023р. № 49. URL: https://zakon.rada.gov.ua/laws/show/v0049500-2

2. Ткачук Р. Л., Полотай О. І., Балацька В. С., Брич Т. Б., Кухарська Н. П. Моделювання захисту операційних систем від реалізації кібератак з використанням критерію Пірсона. Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. пр. Львів : ЛДУ БЖД, 2025. № 31. С. 117–125. DOI: https://doi.org/10.32447/20784643.31.2025.12

3. Балацька В.С., Ткачук Р.Л., Маслова Н.О. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних системи України. Кібербезпека: освіта, наука, техніка. Спеціальний випуск : електронне фахове наукове видання Київ, 2025. № 2 (30). С. 316–332. DOI: https://doi.org/10.28925/2663-4023.2025.30.975

УДК 35:004.056.5

Панченко Н.А., здобувач,
Ткачук Р.Л., д.т.н., професор,
Полотай О.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

КІБЕРТЕРОРИЗМ, ДЕЗІНФОРМАЦІЯ ТА ІНФОРМАЦІЙНІ ОБМЕЖЕННЯ ЯК ЗАГРОЗИ ДЕРЖБЕЗПЕЦІ

У сучасних умовах цифровізації та зростання ролі інформаційного простору забезпечення інформаційної безпеки держави набуває стратегічного значення. Інформація перетворилась на критичний ресурс, від ефективного захисту якого залежить стабільність політичних інститутів, функціонування державних систем та довіра суспільства. З урахуванням інтенсивного розвитку гібридних форм протидії, держава стикається з новими типами загроз, серед яких ключовими виступають кібертероризм, дезінформація та штучні обмеження доступу до публічної інформації. Ці фактори здатні порушувати цілісність інформаційного простору, маніпулювати суспільною думкою та підривати національну безпеку, що зумовлює необхідність їх комплексного аналізу та системної протидії.

Важливо розуміти, що інформаційна безпека є однією зі складових національної безпеки держави нарівні з економічною, енергетичною, військовою, соціальною та іншими. При цьому цілком очевидно, що роль інформаційної безпеки та її місце в системі національної безпеки держави стає все значнішою.

У сучасних умовах цифрової трансформації кібербезпека є ключовим компонентом державної безпеки, що забезпечує захист кіберпростору та критичної інфраструктури від зовнішніх і внутрішніх кібервпливів. Зростання кіберзлочинності, інтенсифікація гібридних атак та використання ІКТ, як інструментів впливу формують спектр загроз, серед яких найбільш небезпечними виступають кібертероризм, дезінформація та штучні обмеження доступу до публічної інформації. Ці явища здатні дестабілізувати систему державного управління, впливати на суспільну свідомість, порушувати функціонування критичних сервісів та підривати національну безпеку.

В умовах триваючої гібридної війни Україна накопичила значний досвід протидії кібератакам та інформаційно-психологічному впливу, однак ефективна нейтралізація сучасних загроз вимагає запровадження комплексної моделі національної кіберстійкості. Така модель має спиратися на принципи управління ризиками та поєднувати

превентивні, технічні, організаційні й правові заходи, що мають реалізуватися за чотирма ключовими напрямами:

1. *Розвиток національної кіберінфраструктури та кіберстійкості*: посилення захисту критичних об'єктів; впровадження систем раннього виявлення та реагування на кібератаки; регулярний аудит та тестування безпеки.

2. *Превентивні та правові заходи:* удосконалення законодавства у сфері кібербезпеки та інформаційного захисту; посилення механізмів відповідальності за кібератаки й інформаційні диверсії; формування єдиної державної політики протидії дезінформації.

3. *Інформаційна стійкість суспільства*: розвиток медіаграмотності населення; підвищення прозорості державних комунікацій для мінімізації ризиків інформаційних маніпуляцій; створення ефективних механізмів перевірки та спростування фейкових повідомлень.

4. *Міжнародна кооперація*: участь у глобальних програмах кіберзахисту; обмін даними про кіберзагрози з країнами-партнерами та міжнародними організаціями; уніфікація стандартів і процедур реагування на кібератаки.

Таким чином, ефективне протистояння кібертероризму, дезінформації та інформаційним обмеженням можливе лише за умови формування комплексного, багаторівневого механізму, який поєднує технологічні рішення, правове регулювання, інституційну взаємодію та підвищення стійкості суспільства до інформаційних впливів.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 15.10.2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

2. Крикун В., Бауліна Т. Дезінформація як засіб гібридної війни : сутність і наслідки. Вісник Київського національного університету імені Тараса Шевченка. Філософія. 2022, Вип. 2. С. 30–33. URL : http://nbuv.gov.ua/UJRN/ VKNUF_2022_2_7

3. Івануса А. І., Ткачук Р. Л., Брич Т. Б. Удосконалення методів управління процесами інформаційної безпеки. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : матеріали III Міжнародної науково-практичної конференції (Хмельницьк, 21 листопада 2024 р.). Хмельницький: НАДПСУ, 2024. С. 1136–1138.

УДК 327.56:004.056.5

Ціфринець В.М., здобувач,
Ткачук Р.Л., д.т.н., професор,
Івануса А.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

ВПЛИВ ДЕЗІНФОРМАЦІЇ НА НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ

Розповсюдження недостовірної інформації стало критичним викликом сучасного інформаційного суспільства, впливаючи на громадську думку та процеси прийняття рішень.

Наслідки дезінформації включають політичні конфлікти, погіршення стану громадського здоров'я та загрозу національній безпеці. В умовах гібридної агресії проти України дезінформація застосовується як традиційний метод ведення війни, спрямований на дестабілізацію суспільства та послаблення державних структур.

Одночасно Україна використовує власні інформаційні інструменти для захисту населення від маніпуляцій та підтримки демократичних принципів, зберігаючи баланс між свободою слова та інформаційною безпекою. Ефективна протидія дезінформації потребує комплексного підходу, що поєднує технологічні, правові та просвітницькі заходи.

Проведений аналіз засвідчує, що дезінформація є одним із ключових чинників, які істотно впливають на внутрішню та зовнішню стабільність функціонування держави. Її поширення генерує комплекс загроз, що проявляються у соціальній, політичній, інформаційній та безпековій сферах. Серед основних негативних наслідків виявлено:

1. Вплив дезінформації на внутрішню стабільність держави, які зводяться до: провокування штучних конфліктів і загострення наявних поділів; активізації стереотипів і поширення атмосфери ворожнечі; зростанні емоційної напруги, що може викликати протести; поглиблення дезорієнтації та недовіри між групами; посилення політичної й етнічної поляризації; формування образу «ворога» та соціальної фрагментації; підриву довіри до влади й інститутів, зниженні легітимності; негативного впливу на психологічний стан суспільства.

2. Вплив дезінформації на зовнішню стабільність держави, які зводяться до: зниження довіри союзників; ускладнення дипломатичної взаємодії; формування негативного міжнародного іміджу; зростання ризиків напруги й конфліктів; провокування суперечок і регіональної дестабілізації; використання як інструменту зовнішнього тиску.

Проведене дослідження підтверджує, що дезінформація є системною загрозою, яка одночасно підриває внутрішню стійкість

держави та її зовнішньополітичні позиції. У цьому контексті визначено ключові напрями підвищення ефективності протидії дезінформаційним впливам. Насамперед необхідно вдосконалити законодавчу базу, чітко визначивши поняття, критерії та процедури виявлення дезінформації й механізми відповідальності. Важливо також посилити міжвідомчу координацію структур безпеки, медіарегуляторів і аналітичних центрів для оперативного обміну інформацією. Значну роль відіграє розвиток національних систем моніторингу на основі штучного інтелекту та аналізу великих даних. Потребує інституційної підтримки діяльність фактчекінгових ініціатив та впровадження механізмів швидкого спростування фейків. Підвищення медіаграмотності через освітні програми й суспільні кампанії посилює стійкість населення. Важливим є також розширення міжнародної співпраці з партнерами ЄС і НАТО та впровадження найкращих практик. Підвищення відкритості державних органів сприятиме зменшенню впливу маніпуляцій і відновленню суспільної довіри.

Список використаних джерел:

1. Звоздецька О. Дезінформація як загроза національній безпеці Європейського Союзу : проблеми та підходи Історико-політичні проблеми сучасного світу : Збірник наукових статей. 2021, № 43. С. 30–39.

2. Про рішення Ради національної безпеки і оборони України від 15.10.2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

3. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» : Указ Президента України. від 16.02.2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text

4. Крикун В., Бауліна Т. Дезінформація як засіб гібридної війни : сутність і наслідки. Вісник Київського національного університету імені Тараса Шевченка. Філософія. 2022, Вип. 2. С. 30–33. URL : http://nbuv.gov.ua/UJRN/ VKNUF_2022_2_7

5. Івануса А. І., Ткачук Р. Л., Брич Т. Б. Удосконалення методів управління процесами інформаційної безпеки. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : матеріали ІІІ Міжнародної науково-практичної конференції (Хмельницьк, 21 листопада 2024 р.). Хмельницький: НАДПСУ, 2024. С. 1136–1138.

УДК 004.75

Шелуха О.О., к.т.н., ст. викл.
Овсянніков Д.В., магістрант
Державний університет «Житомирська політехніка»

МЕТОДИ ТА ТЕХНОЛОГІЇ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ДОСТУПУ КОРПОРАТИВНОЇ МЕРЕЖ

В умовах зростаючої гібридної інфраструктури комп'ютерних мереж назріла необхідність переходу від застарілих VPN-рішень, що створюють єдині точки відмов і є складними для масштабування, до сучасних захищених архітектур. Авторами проведено дослідження, аналіз та практичне впровадження методів організації захищеного доступу до корпоративної мережі.

В ході дослідження було здійснено порівняльний аналіз методів поєднання віддалених підмереж та основних VPN протоколів (PPTP, OpenVPN, IPsec, IKEv2, L2TP), на основі якого було обгрунтувано вибір WireGuard, як оптимальної основи для створення віртуальних тунелів для віддалених хостів. Основні переваги обраної технології полягають у високій швидкості та високому рівню криптографічної безпеки, що стає можливим з використанням алгоритму ChaCha20 [1]. Розглянуто можливості технологію Mesh VPN-рішення Tailscale [2], що побудовано на основі зазначеного алгоритму, та досліджено можливості його застосування у поєднанні із технологією WireGuard. Зазначений підхід, на відмінну від більшості традиційних VPN-рішень, використовує децентралізовану однорангову топологію. Ще одним напрямом забезпечення безпеки мережі стала інтеграція Tailscale з дотримання концепції Zero Trust Networking.

На основі теоретичних даних, було проведено моделювання захищеної корпоративної мережі, яка базується на ієрархічній трирівневій моделі та складається з головного офісу, філіалу та віддаленого працівника. Зазначений проєкт було налаштовано в емуляційному середовищі GNS3, включаючи налаштування контролера домену, базових мережевих служб та інтеграцію Tailscale. Було розроблено і впроваджено підсистему захисту з використанням маршрутизаторів на базі дистрибутиву VyOS з можливістю налаштування міжмережевого екрану. Крім того, виконано розробку списків контролю доступу у Tailnet та налаштовано аутентифікацію клієнтів Tailscale через Single Sign-On із використанням системи автентифікації Google. Всі впроваджені засоби дозволять реалізувати гнучку мікросегментацію прав доступу з дотримання суворого принципу мінімальних привілеїв.

Практичне тестування розробленої моделі мережевої інфраструктури та впроваджених рішень показали коректність її функціонування. В ході роботи було отримано наступні результати:

1. Застосування списків доступу на рівні Tailnet дозволили провести блокування передачі трафіку між віддаленим користувачем та філією, тим самим підтвердивши реалізацію принципу мінімальних привілеїв в Tailscale.

2. Аналіз перехопленого трафіку за допомогою Wireshark дозволив зафіксувати наявність наскрізного шифрування всього корпоративного трафіку з використанням протоколу WireGuard, що зрештою гарантує повну конфіденційність переданої інформації через публічні мережі.

3. Практичне тестування інформаційного обміну між сегментами мережі продемонстрували наявність прямих підключень між віддаленими вузлами мережі, тим самим підтверджуючи факт забезпечення високої швидкості та надійності з'єднань в децентралізованій Mesh-топології Tailscale.

4. Перевірка можливості віддаленого користувача отримувати доступ до внутрішніх ресурсів корпоративної мережі довела те, що Tailscale здатний забезпечувати зв'язок між пристроями навіть з приватних мереж.

5. Впровадження Single Sign-On із використанням автентифікації Google дало можливість використовувати один створений обліковий запис для декількох сервісів, зокрема в Tailscale. Це, в поєднанні з автоматичним присвоєнням IP-адрес в мережі Tailscale, мінімізує кількість ручних налаштувань мережі, що є важливим для ефективного масштабування топології.

На основі розробленої моделі корпоративної інфраструктури та впроваджених рішень було перевірено ефективність застосування рішення Tailscale для організації захищеного доступу в корпоративній мережі, зокрема використання списків доступу, наявність наскрізного шифрування корпоративного трафіку і та коректність роботи методу Single Sign-On для зручної і безпечної автентифікації користувачів. Також було протестовано можливість підключення кінцевих вузлів з приватних мереж та наявність прямих підключень між сегментами Tailscale.

Список використаних джерел:

1. The ChaCha family of stream ciphers. URL: https://cr.yp.to/chacha.html

2. What is Tailscale? URL: https://tailscale.com/kb/1151/what-is-tailscale

УДК 004.738.5

Ретивих К.О., магістрант,
Колощук М.С., ст. викладач
Державний університет «Житомирська політехніка»

МОНІТОРИНГ І ВІЗУАЛІЗАЦІЯ МЕРЕЖЕВОГО ТРАФІКУ ЗА ДОПОМОГОЮ ZENARMOR DASHBOARD

Сучасні комп'ютерні мережі постійно зіштовхуються зі зростаючим обсягом трафіку та підвищеною кількістю кіберзагроз. Особливо це ускладнюється тим, що значна частина трафіку передається з використанням протоколу HTTPS і відповідно є зашифрованою, що зрештою ускладнює процес аналізу та виявлення прихованого шкідливого контенту. Ця проблематика вимагає використання технології глибокого аналізу мережевого трафіку, яка часто є ключовою функцією рішень класу Next-Generation Firewall (NGFW), до яких належить і Zenarmor [1].

Метою дослідження є аналіз можливостей системи Zenarmor для моніторингу та візуалізації мережевого трафіку в умовах зростання обсягу зашифрованих даних та кіберзагроз.

Zenarmor позиціонується, як високопродуктивне та гнучке рішення NGFW, розроблене для ефективного протидії сучасним загрозам, особливо прикладного рівня [2]. Ключовою особливістю Zenarmor є його здатність здійснювати глибокий аналіз трафіку і надавати розширені можливості, такі як контроль додатків, веб-фільтрація на основі категорій, аналіз загроз у реальному часі і здійснювати агрегацію та візуалізацію зібраних даних.

В рамках дослідження, з використанням середовища емуляції GNS3, було створено проєкт невеликої локальної комп'ютерної мережі, що складається з робочої станції Windows та маршрутизатора на базі дистрибутива OPNsense зі встановленим плагіном Zenarmor. Zenarmor заздалегідь був налаштований на максимальні безпекові параметри, що включає автоматичне блокування всіх потенційно підозрілих і небезпечних сайтів, недавно створених доменів, азартних ігор, піратських сайтів, соціальних мереж та інших подібних ресурсів.

Для отримання репрезентативного набору даних з браузера робочої станції Windows було здійснено перехід на різноманітні веб-ресурси як дозволених, так і заборонених політиками Zenarmor категорій. Після цього, було переглянуто вкладку зі звітами (Рисунок 1 -). З цього рисунка можна отримати загальну статистику по розподілу трафіку за загальними категоріями додатків (наприклад Secure Web Browsing чи Media Streaming) і конкретними застосунками (YouTube, Bing, Facebook). Дана візуалізація дозволяє визначити загальний характер

навантаження на мережу й ідентифікувати додатки, які найчастіше використовуються кінцевими пристроями мережі.

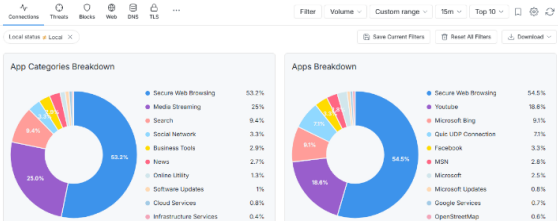


Рисунок 1 – Візуалізація розподілу мережевого трафіку за категоріями

На панелі Threats в Zenarmor (рис. 2) можна переглянути загальне співвідношення категорій заблокованих ресурсів (наприклад, Potentially Dangerous, Malware/Virus), тоді як графік праворуч надає інформацію про конкретні домени та URL-адреси (наприклад, fastway01.biz чи itorrents-igruha.org), які були блоковані системою. Це є важливим для швидкого отримання ситуаційної обізнаності та застосування відповідних протидій.

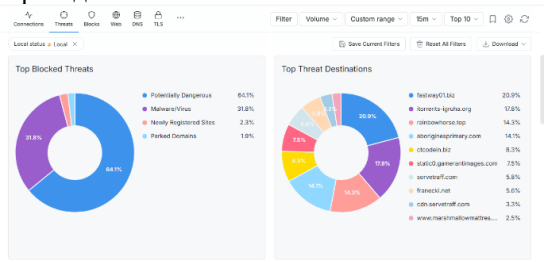


Рисунок 2 – Графічне відображення заблокованих загроз на панелі Zenarmor

Отже, проведене практичне дослідження підтвердило ефективність використання Zenarmor у проактивному захисті мережі від загроз прикладного рівня. Система успішно ідентифікувала та заблокувала ресурси категорій Potentially Dangerous та Malware/Virus, включно з доменами fastway01.biz та itorrents-igruha.org. Панель візуалізації забезпечила зручне групування трафіку як за загальними категоріями (Secure Web Browsing, Media Streaming), так і за конкретними застосунками (YouTube, Bing, Facebook), що дозволяє адміністраторам оперативно оцінювати мережеву активність та приймати обґрунтовані рішення щодо політик безпеки.

Список використаних джерел:

1. What is a Next-Generation Firewall (NGFW)? URL: https://www.zenarmor.com/docs/category/ngfw

2. About Zenarmor. URL: https://www.zenarmor.com/docs/opnsense

УДК 004.738

Ференз А.Р., магістрант,
Фальковський І.Г., ст. викладач
Державний університет «Житомирська політехніка»

ОГЛЯД МЕРЕЖЕВИХ ПРОТОКОЛІВ, ЩО ВИКОРИСТОВУЮТЬСЯ ДЛЯ МОНІТОРИНГУ

Ефективний моніторинг мережевої інфраструктури забезпечується спеціалізованими протоколами, які дозволяють збирати дані про стан пристроїв, продуктивність і безпеку мережі. Їхнє комбіноване використання забезпечує комплексний підхід до управління мережею, дозволяючи виявляти несправності, оптимізувати трафік і підвищувати безпеку.

1) Ping – базовий метод активного моніторингу, що використовує протокол ICMP. Система надсилає Echo Request і очікує Echo Reply, перевіряючи доступність пристрою та вимірюючи затримку з'єднання. Простота та вбудованість у більшість операційних систем роблять Ping основним інструментом для генерації аварійних сповіщень.

2) SNMP (Simple Network Management Protocol) – широко використовуваний протокол для активного (GET-запити) та пасивного (traps, informs) моніторингу. Існують три версії SNMP:

- SNMP v1 (1988): базова версія з обмеженою функціональністю та слабкою безпекою (автентифікація через community string).
- SNMP v2c (1993): покращена продуктивність, підтримка 64-бітних лічильників, але без змін у безпеці.
- SNMP v3 (2002): додано шифрування, автентифікацію користувачів і контроль доступу, що значно підвищило безпеку.

3) Syslog, стандартизований у RFC 5424, передає текстові лог-повідомлення через UDP до центрального сервера. Повідомлення містять Facility, Severity та опис події (наприклад, помилки чи зміни конфігурації). Централізоване зберігання логів полегшує аналіз подій і діагностику проблем, хоча доставка не гарантується.

4) Протоколи мережевих потоків (NetFlow, sFlow, IPFIX) призначені для збору даних про IP-потоки для подальшого аналізу трафіку та безпеки.

- NetFlow: розроблений Cisco, забезпечує детальний збір даних про мережеві потоки, фіксуючи такі параметри, як IP-адреси джерела та призначення, порти, протоколи, обсяг трафіку та часові мітки. NetFlow v9 розширює можливості завдяки підтримці IPv6, MPLS і гнучких шаблонів. Є пропрієтарним протоколом.

- sFlow: застосовує вибірковий підхід (sampling), відбираючи зразки пакетів і даних інтерфейсів, що значно знижує навантаження на мережеве обладнання порівняно з NetFlow. Це робить sFlow ідеальним для моніторингу великих і високонавантажених мереж. Однак через вибірковий характер збору даних деталізація інформації нижча, що може обмежувати точність аналізу. Є відкритим стандартом.
- IPFIX: стандартизована IETF еволюція NetFlow (на основі NetFlow v9), вирізняється гнучкістю та адаптивністю завдяки підтримці кастомних шаблонів для збору даних. Це дозволяє налаштовувати протокол для специфічних потреб, що робить його універсальним для сучасних мереж, включаючи хмарні та SDN-середовища.

5) Cisco Discovery Protocol (CDP) та Link Layer Discovery Protocol (LLDP). CDP – пропрієтарний протокол Cisco, який виявляє сусідні пристрої, надаючи дані про ідентифікатор, IP-адресу, тип і модель обладнання, версію ПЗ, активні інтерфейси, VLAN та споживання енергії в PoE-середовищах. LLDP – відкритий стандарт, що працює на канальному рівні, сумісний із пристроями різних виробників. Він передає дані про тип пристрою, порт, VLAN ID і адреси управління. Використання LLDP ідеально підходить для гетерогенних мереж.

6) WMI (Windows Management Instrumentation (WMI) – це інструмент Microsoft для моніторингу та управління Windows-системами. Він дозволяє отримувати дані про стан операційної системи, апаратного забезпечення та програм через простий інтерфейс. WMI підтримує автоматизацію завдань (наприклад, моніторинг диска чи налаштування мережі), централізоване управління через єдину консоль, інтеграцію з PowerShell і System Center, а також забезпечує захист даних завдяки вбудованим механізмам безпеки.

В доповіді буде представлено огляд вищезгаданих мережевих протоколів для моніторингу з акцентом на їхні особливості, переваги та сфери застосування.

Список використаних джерел:

1. Ultimate Guide to Network Monitoring? URL: https://www.dnsstuff.com/network-monitoring
2. Types of Network Management Protocols. URL: https://www.liveaction.com/resources/blog-post/types-of-network-management-protocols/
3. Network Monitoring Protocols. URL: https://www.kentik.com/kentipedia/network-monitoring-protocols/

УДК: 004.056.5:004.021

Хавер Анюта Вячеславівна, аспірант,
Державний університет інформаційно-комунікаційних технологій

КОЛЬОРОВІ СІТКИ ПЕТРІ ЯК МАТЕМАТИЧНИЙ ЗАСІБ МОДЕЛЮВАННЯ КІБЕРАТАК В ТЕХНОЛОГІЧНИХ СИСТЕМАХ ПРОМИСЛОВИХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кольорові сітки Петрі належать до розділу дискретної математики та поєднують елементи кількох її підрозділів. Вони є формальною моделлю дискретних подійно-орієнтованих систем, що ґрунтується на апараті орієнтованих графів. Незважаючи на наявність широкого спектра графових інструментів – алгоритмів пошуку шляхів (алгоритм Дейкстри), Марківських ланцюгів, Байєсівських мереж, класичних графів станів – жоден з них не забезпечує достатнього рівня деталізації, не враховує неоднорідність вузлів, формальності та динамічності для моделювання складних кібератак у середовищі технологічних систем промислових об'єктів критичної інфраструктури (ПОКІ). Кольорові сітки Петрі є найбільш придатним інструментом для вирішення завдання імітаційно-аналітичного моделювання кібератак, оскільки дозволяють одночасно відображати стани та властивості вузлів, моделювати паралельні процеси (зокрема поширення ШПЗ), визначати логічні умови переходів, а також формально аналізувати поведінку системи. Крім того, стохастичні моделі (Марківські ланцюги, Байєсівські мережі) моделюють переважно ймовірнісний аспект процесу, але не дозволяють явно враховувати структурно-логічні зв’язки, умовні переходи, паралельність та ресурсні характеристики кібератак, в той час як кольорові сітки Петрі забезпечують повноцінне імітаційно-аналітичне моделювання всього досліджуваного процесу кібератаки.

Основними елементами кольорової сітки Петрі є 9-ти кортеж:

$$CPN= (P, T, A, \Sigma, V, C, G, E, I) \quad (1)$$

де: P- множина місць; T – множина переходів; A – множина дуг; Σ – кольорові множини (типи); V – змінні; C – функція типів місць; G – guard- вирази; E – вирази дуг; I – початкове маркування.

Спрощений графічний приклад кольорової сітки Петрі, яка відображає реагування Safety instrumented system (SIS) на фіксацію небезпечного стану сенсором в технологічній системі ПОКІ наведено на Рис.1.1. Така модель відтворює стандартну структуру Safety Instrumented Function (SIF) згідно IEC 61508/IEC 61511: сенсор → логічний вирішувач (PLC SIS) → актуатор.

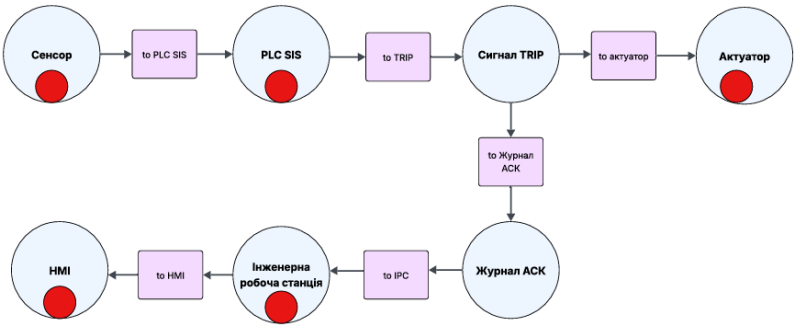


Рисунок 1 – Спрощений графічний приклад кольорової сітки Петрі, яка відображає реагування SIS на фіксацію небезпечного стану сенсором

Практичне використання вищезазначеного імітаційно-аналітичного математичного підходу з використанням кольорових сіток Петрі дозволяє розрахувати кількість вузлів (місць) та дає змогу розрахунку ресурсів (людських, часових, фінансових) для реалізації тої чи тої тактики проведення кібератаки суб'єктом кіберзагрози (сформувати так званий інтегральний "ресурсний профіль" кібератаки). Разом з тим, змодельовану кольорову сітку Петрі можна використати для побудови інтерактивного програмного прототипу в середовищі ПЗ "CPN Tools". Підхід може використовуватися підрозділами Cyber Threat Intelligence ПОКІ для моделювання потенційних кібератак та їх обґрунтування у моделі загроз (кіберзагроз) технологічної систем. Результати такого імітаційно-аналітичного моделювання можуть використовуватися для прийняття рішень щодо пріоритезації кіберзахисту в технологічній системі та створення стратегії кіберзахисту на коротку (для нейтралізації загроз від тактик з найменшими ресурсними затратами для суб'єкта кіберзагрози) та довгу перспективу (для нейтралізації загроз від тактик найбільш ресурсовитратних для суб'єкта кіберзагрози).

Список використаних джерел:

1. Kurt Jensen, Lars M. Kristensen "Coloured Petri Nets: Modelling and Validation of Concurrent Systems", 2009 p., P. 1-56.;

2. Савченко В.А., Хавер А.В. "Оцінка впливу програмних інструментів на основі технологій штучного інтелекту на ресурсну ефективність щодо проведення деструктивних кібероперацій по відношенню до об'єктів критичної інфраструктури", Сучасний захист інформації № 3, ДУІКТ, м. Київ, 2025 р. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/3317.

УДК 004.7

Сарапин В.Є., магістрант
Київський національний університет будівництва і архітектури

ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ ЗАСОБАМИ АНАЛІЗУ ТРАФІКУ

Сучасні комп'ютерні мережі функціонують у високодинамічному середовищі, де зростання обсягів трафіку, ускладнення транспортних протоколів та інтенсивність мережевих викликів створюють підґрунтя для появи аномальних поведінкових патернів. Виявлення мережевих аномалій є одним із ключових завдань кібербезпеки, оскільки саме на ранніх етапах аномалії сигналізують про присутність загроз, експлуатацію уразливостей або функціональні збої систем. Аналіз трафіку як метод діагностики дозволяє досліджувати поведінку мережі у реальному часі, здійснювати її класифікацію та встановлювати відхилення від нормальних режимів роботи.

Мережеві аномалії можуть проявлятися у вигляді нетипових сплесків активності, надмірної фрагментації пакетів, перевищення порога затримок, порушення порядку доставки пакетів або зміни інтенсивності міжвузлової взаємодії. До поширених класифікаційних категорій аномалій належать поведінкові, структурні, протокольні та змішані. Поведінкові аномалії пов'язані зі змінами трафіку в часі, структурні – з порушенням узгодженості пакетів, а протокольні – з неправильним формуванням заголовків та нестандартними запитами. Виявлення таких аномалій вимагає наявності інструментів, здатних точно аналізувати характеристики потоків.

Для детального аналізу аномалій використовуються засоби пакетного аналізу, такі як Wireshark, які дозволяють вивчати структуру мережевих кадрів, визначати нестандартні поля та виявляти аномальні сигнатури. Засоби низькорівневого моніторингу tcpdump забезпечують збирання трафіку у середовищах з обмеженими ресурсами, що робить їх ефективними у випадках, коли потрібен мінімальний вплив на систему. Потокові протоколи NetFlow та IPFIX дозволяють аналізувати статистику потоків, що є надзвичайно корисним при пошуку аномалій, пов'язаних із тривалими атаками, скануванням портів або горизонтальним переміщенням загроз.

Виявлення аномалій також ґрунтується на побудові математичних моделей, що описують нормальну поведінку мережі. Значну роль відіграють статистичні підходи, зокрема дисперсійний аналіз, кореляційні методи та кластеризація поведінкових патернів. Методи машинного навчання, такі як алгоритми ізоляційних лісів, автоенкодери

та моделі часових рядів, дозволяють автоматично виявляти приховані закономірності у великих масивах трафіку. Використання таких методів забезпечує можливість раннього попередження про аномалії без необхідності попереднього визначення сигнатур або точних правил поведінки.

Не менш важливою складовою є оцінка якості обслуговування. Збільшення затримок, нерівномірність навантаження, коливання пропускної здатності, поява джитеру та збільшення втрат пакетів можуть бути маркерами некоректної роботи мережі або наслідком цілеспрямованої атаки. Моніторинг цих показників дозволяє визначити вузькі місця, встановити причини погіршення продуктивності та виявити неузгодженість у роботі механізмів маршрутизації.

У практичних мережах комплексна діагностика аномалій потребує використання як програмних, так і апаратних інструментів. Апаратні TAP-пристрої та SPAN-порти дозволяють отримувати копії трафіку у чистому вигляді, забезпечуючи безперервний моніторинг без впливу на роботу інфраструктури. Дані, отримані такими засобами, можуть бути інтегровані у системи SIEM, де здійснюється їх кореляція, нормалізація та детальний аналіз. Поєднання таких методів дозволяє створювати комплексні системи раннього виявлення інцидентів.

Отже, виявлення мережевих аномалій на основі аналізу трафіку є фундаментальним напрямом кібербезпеки, який забезпечує захист інформаційних систем від прихованих та активних загроз. Використання сучасних інструментів аналізу, статистичних методів та алгоритмів машинного навчання створює передумови для побудови стійких та адаптивних систем захисту, здатних забезпечити безперервне функціонування мережі.

Список використаних джерел:

1. Wireshark Foundation. Wireshark User Guide. URL: https://www.wireshark.org/docs/

2. Cisco Systems. NetFlow Services Export Version 9 : RFC 3954. IETF, 2004. URL: https://datatracker.ietf.org/doc/html/rfc3954

3. Lakhina A., Crovella M., Diot C. Characterization of Network-Wide Anomalies // ACM Internet Measurement Conference (IMC). 2004. URL: https://dl.acm.org/doi/10.1145/1028788.1028794 4. Barford P., Plonka D. Flow Analysis Techniques for Network Monitoring. IEEE Communications Magazine, 2001.

5. Tanenbaum A. Computer Networks. 5th ed. Upper Saddle River : Prentice Hall, 2010.

УДК 004.7

Пирч О.В., асистент,
Коробко Р.М., здобувач,
Панько Р.М., здобувач,
Державний університет «Хмельницький національний університет»

ОСОБЛИВОСТІ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ МАЛОЇ ІНТЕНСИВНОСТІ

Сучасні системи моніторингу безпеки мереж здебільшого орієнтовані на аналіз великих обсягів трафіку, адже у переважній більшості досліджень з виявлення аномалій опрацьовуються саме великі масиви мережевого трафіку: терабайти логів, довгі часові ряди, та багатогодинні сесії., де статистичні закономірності чітко виражені. Такий підхід традиційно формується навколо хмарних інфраструктур, великих корпоративних мереж або дата-центрів. Однак у випадках малої інтенсивності передавання даних, зокрема у сегментах IoT, промислових мережах або малих корпоративних інфраструктурах, класичні методи виявлення аномалій втрачають ефективність через нестачу даних і високу варіативність поведінкових характеристик. Саме там аномалії ховаються найкраще. У тих поодиноких пакетах важче знайти закономірність, але у той же час і легше непомітно приховати атаку.

Ключовими особливостями та проблемами аналізу трафіку малої інтенсивності є нестача статистично значущих значень, нерегулярність трафіку, домінування «квазіаномалій», та проблема високої чутливості алгоритмів. Коли активність низька, це призводить до того що кількість пакетів недостатня для побудови надійної моделі. У класичних методах (наприклад, сигнатурних або статистичних IDS) це призводить до високої похибки і неможливості формування репрезентативного профілю системи. У таких умовах кожен пакет стає важливим, і система повинна працювати з мінімальним набором інформації, не втрачаючи контексту.

Варто підкреслити, що потоки малої інтенсивності не мають чітких ритмів, що означає що пакети можуть надходити рідко, неформально, і без стабільного інтервалу. Це ускладнює побудову часових моделей і зменшує ефективність методів, що покладаються на регулярність (LSTM, ARIMA тощо). Інколи поведінка пристрою змінюється просто тому, що він працює в іншому режимі, і система, яка є досить чутлива о будь-яких змін, може сприйняти це як атаку і відповідним чином підкреслити це у системі безпека, що є false-positive відповіддю і може призупинити роботу системи поки ця проблема не буде вирішеною, що у свою чергу може завдати збитків компанії.

У трафіку малої інтенсивності з’являється багато подій, які формально відхиляються від норми, але не є шкідливими. Прикладами таких подій може бути повторна ініціалізація пристрою, коли працівник використовує

систему з іншого девайсу не завершивши сеанс на іншому пристрої, зміна інтервалу передачі даних, або ж короткотривала нестабільність мережі, яка може вплинути на те як трафік приймається, і може бути також сприйнята як аномальна зміна трафіку.

Для подолання цих проблем запропоновано використовувати комбіновані методи машинного навчання, зокрема автоенкодери для реконструкції нормальної поведінки та непараметричні алгоритми кластеризації (DBSCAN, k-NN) для виділення потенційно аномальних зразків. Крім того, ефективним виявився підхід із динамічним формуванням часових вікон, що враховує реальну активність мережевих вузлів, а не лише фіксовані інтервали часу. Аналіз особливостей трафіку малої інтенсивності засвідчує, що традиційні IDS-моделі не є ефективними для таких умов. Для підвищення якості виявлення аномалій необхідно застосовувати адаптивні підходи машинного навчання, здатні працювати з обмеженими та нестабільними даними.

Поєднання автоенкодерів, непараметричних алгоритмів та динамічної сегментації даних утворює модель, що успішно працює з неповними та нерегулярними потоками; знижує рівень false-positive спрацьовувань; виявляє як одиничні, так і групові аномалії; зберігає адаптивність у середовищах, де поведінка нормального трафіку змінюється. Усе це створює основу для побудови ефективних систем захисту в малих мережах, де тиша й повільні ритми трафіку не повинні вводити в оману: саме там найдовше ховається загроза.

Практична цінність дослідження полягає у можливості впровадження запропонованого методу в системи моніторингу безпеки корпоративних мереж, інфраструктури інтернету речей, промислові сегменти та віддалені вузли, де обсяг трафіку є обмеженим і нестійким. Запропонований підхід забезпечує підвищену точність виявлення аномалій за умов малої інтенсивності передавання даних, що дозволяє значно зменшити ризики непомічених атак, прихованих мережевих взаємодій та несанкціонованого доступу. Завдяки адаптивності та здатності працювати з мінімальними вибірками метод може бути використаний для зміцнення кіберзахисту у критично важливих інформаційних середовищах та інфраструктурах, де традиційні IDS-рішення втрачають ефективність.

Список використаних джерел:

1. Stephanie N. Anomaly Detection in Network Traffic Using Advanced Machine Learning Techniques. URL https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10833631

2. Félix I.V. Analysis of network traffic features for anomaly detection. URL https://www.researchgate.net/publication/269420763_Analysis_of_network_traffic_features_for_anomaly_detection

УДК 004.7

Жеребцов Д.В., здобувач,
Кухар А.А., здобувач,
Сергійко В.М., здобувач,
Рудюк Б.М., асистент
Державний університет «Житомирська політехніка»

МІГРАЦІЯ З IPV4 НА IPV6: ПРОБЛЕМИ, РИЗИКИ ТА ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ

Глобальне зростання Інтернету поставило під сумнів подальшу придатність протоколу IPv4 з його 32-бітним адресним простором (приблизно 4,3 млрд адрес). Вже у 2011 році Міжнародне агентство з присвоєння адрес IANA, вичерпало запас IPv4-адрес, що спричинило використовувати необхідність впровадження проміжних механізмів, зокрема NAT для продовження життєвого циклу IPv4. Ці обхідні рішення збільшили складність мереж та створили вузькі місця в продуктивності. Натомість розроблений ще у 1990-х роках протокол IPv6 має 128-бітний адресний простір (близько $3{,}4\times10^{38}$ адрес), фактично необмежений для потреб теперішнього і майбутнього Інтернету. Перехід на IPv6 став нагальною необхідністю для підтримки масштабування мережі, появи нових технологій, таких як IoT, 5G, тощо, та усунення обмежень IPv4.

Головною причиною міграції є вичерпання адресного простору IPv4. Регіональні Інтернет-реєстри у різних частинах світу поступово повідомили про відсутність вільних IPv4-адрес протягом 2011–2015 років. Це призвело до різкого зростання вартості IPv4-адрес на вторинному ринку та залежності від NAT-технологій, що створюють затримки і проблеми з продуктивністю. IPv6 повністю розв’язує проблему нестачі адрес завдяки колосальному адресному простору, достатньому для потреб людства на непередбачуване майбутнє.

Окрім адрес, IPv6 пропонує переваги в продуктивності та маршрутизації. Зокрема, спрощений заголовок пакетів і ієрархічна адресація дають змогу зменшити таблиці маршрутизації та прискорити передачу даних, що в реальних впровадженнях дозволило знизити затримки завантаження веб-сторінок на 15–30%. Автоматична конфігурація адрес у IPv6 полегшує управління мережею, усуваючи ручне налаштування для кожного вузла. Покращення безпеки є ще одним аргументом на користь IPv6: протокол спроектовано з урахуванням безпеки, з обов’язковою підтримкою шифрування IPsec для кожного вузла, що підвищує конфіденційність і цілісність даних та зменшує ризики кібератак. Відмова від масового використання NAT

також усуває низку проблем фрагментації мережі і спрощує встановлення прямого кінцевого з'єднання між вузлами.

Перехід на IPv6 є складним багатоетапним процесом, що стикається з технічними та організаційними перешкодами. Перш за все, несумісність протоколів: IPv4 і IPv6 суттєво відрізняються, тому безпосередньо не взаємодіють між собою. Це означає, що пристрої або додатки, що підтримують лише IPv4, не можуть спілкуватися з вузлами IPv6 без спеціальних механізмів переходу. Багато застарілих мережевих пристроїв і програмного забезпечення не підтримують IPv6 або підтримують його частково. Отже, для впровадження нового протоколу часто потрібне оновлення прошивки чи заміна обладнання, що особливо складно в галузях з довгим життєвим циклом пристроїв.

Інфраструктурні виклики включають необхідність модернізації мереж: провайдерам і підприємствам доводиться налаштовувати мережеві пристрої на підтримку двох протоколів одночасно або впроваджувати шлюзи та тунелі. Це ускладнює архітектуру мережі та висуває підвищені вимоги до IT-персоналу. Важливим фактором є економічні витрати.

Окрім того, людський фактор теж грає роль: існує брак фахівців, добре обізнаних з IPv6, і необхідність навчати персонал новим протоколам, що потребує часу і ресурсів. У багатьох організаціях спостерігається опір змінам: поки IPv4 працює, керівники не завжди бачать негайну вигоду від впровадження IPv6. Така інерція та побоювання з приводу потенційних збоїв або проблем під час міграції уповільнюють процес переходу.

Процес впровадження IPv6 супроводжується низкою ризиків та загроз, які потребують уваги. Безпека мережі під час переходу є подвійною проблемою.

З одного боку, IPv6 покращує безпеку за рахунок вбудованого IPsec та усунення потреби в NAT. З іншого боку, поява нового протоколу відкриває нові вектори атак. Наприклад, протокол сусіднього виявлення NDP у IPv6 може бути об'єктом специфічних атак, як-то підробка оголошень сусідів або переповнення таблиць сусідства, що раніше не загрожували IPv4. Під час одночасної роботи двох протоколів зловмисники можуть шукати вразливості як в IPv4-, так і в IPv6-стеках.

Якщо IT-персонал менш досвідчений з налаштуваннями безпеки IPv6, існує ризик помилкової конфігурації брандмауерів або пропуску фільтрації IPv6-трафіку, що відкриває шлюзи для атак.

Операційні ризики включають можливі збої в роботі сервісів під час переходу. Некоректно налаштовані тунелі або шлюзи можуть призвести до перебоїв у зв'язку, втрати пакетів чи збільшення затримок.

Фінансові ризики пов’язані зі значними первинними інвестиціями: організація може витратити великі кошти на модернізацію, але не отримати негайної віддачі. Це вимагає стратегічного планування бюджету, щоб перехід не вплинув негативно на поточну діяльність.

Ресурсні та кадрові ризики виникають через брак спеціалістів з досвідом IPv6. Потрібно врахувати час на навчання персоналу та можливі помилки через людський фактор.

Таким чином, ефективне управління ризиками в проєктах міграції на IPv6 вимагає комплексного підходу. Він передбачає ретельне планування, тестування в безпечних сегментах, поступове впровадження та постійний моніторинг безпеки і продуктивності.

Перехід від IPv4 до IPv6 – це не просто технічне оновлення, а стратегічний імператив для глобальної мережевої інфраструктури. Сучасний Інтернет вже не може розвиватися на базі обмеженого IPv4, адже вимоги адресації, продуктивності і безпеки зросли багаторазово.

IPv6 пропонує необхідні рішення:

- практично невичерпну адресацію;
- вбудовані засоби безпеки;
- ефективнішу маршрутизацію.

Водночас цей перехід потребує значних зусиль і передбачає подолання згаданих труднощів – від технічних проблем сумісності до економічних витрат і навчання кадрів.

Отже, IPv6 однозначно стає невід’ємною частиною майбутнього Інтернету. Своєчасна та продумана міграція на IPv6 є критичною умовою для забезпечення стійкого функціонування, безпеки та конкурентоспроможного розвитку мережевих ресурсів у світовому масштабі.

Список використаних джерел:

1. Kane A. Challenges and Benefits of Shifting from IPv4 to IPv6 // Scientific Research Publishing. 2025. DOI: https://doi.org/10.4236/ijids.2025.72002

2. Gundarwala Y., Deputy M., Patel P. Transitioning from IPv4 to IPv6: Strategies, Challenges, and Adoption Status // International Journal of Engineering Research & Technology. 2024. URL: https://www.ijert.org/transitioning-from-ipv4-to-ipv6-strategies-challenges-and-adoption-status

УДК 004.7

Гавриш О.С., доцент,
Сімонов В.О., здобувач,
Черкаський державний технологічний університет

РОЗРОБКА ТА ВПРОВАДЖЕННЯ РАЦІОНАЛЬНИХ ПОЛІТИК ДОСТУПУ ДЛЯ МЕРЕЖІ ПРИВАТНОЇ КОМПАНІЇ

Сучасні корпоративні мережі характеризуються високою складністю, багаторівневою архітектурою та неоднорідними інформаційними сегментами, що підтримують бізнес-процеси різного масштабу. У цих мережах використовується значна кількість інформаційних ресурсів, доступ до яких регулюється політиками безпеки. Однак у багатьох приватних компаніях доступ до цих ресурсів часто налаштовується за принципом «за замовчуванням», однаковим для всіх співробітників, що створює значні ризики для безпеки даних.

Ця проблема ускладнюється тим, що внутрішні загрози вважаються одними з найнебезпечніших у сучасному кіберпросторі. Погано налаштовані політики доступу можуть призвести до несанкціонованого використання, копіювання або поширення інформації співробітниками, які не повинні мати доступу. У випадку приватних компаній це може мати фінансові та правові наслідки, особливо коли це стосується персональних даних клієнтів, конфіденційної інформації або інформації, пов'язаної з внутрішніми службами.

У дослідженні проаналізовано корпоративну мережу приватної компанії «Brain Basket», де інформаційні ресурси демонструють різний рівень критичності. Основною метою цієї роботи була розробка ефективного механізму політики доступу на основі об'єктивного аналізу інформаційних потоків, характеристик бізнес-процесів та статистики інцидентів інформаційної безпеки.

Для досягнення цієї мети було проведено ретельний аналіз організаційної структури компанії. Були визначені основні групи користувачів, їхні функціональні обов'язки та фактичні потреби в доступі до ресурсів. На основі цього інформаційні активи були ранжовані за важливістю та чутливістю, а також визначені ключові елементи, що потребують посиленого контролю доступу. Особлива увага була приділена персональним даним клієнтів та співробітників.

Вибір методів реалізації політики доступу базувався на характеристиках корпоративної мережі, яка побудована на платформі Windows. Були враховані функціональні можливості інтегрованих інструментів управління доступом, включаючи об'єкти групової політики (GPO), контроль доступу NTFS, розділення прав користувачів,

управління ролями та обмежені правила безпеки. Для кожного типу ресурсу була створена матриця доступу, що регулює взаємодію користувачів з інформаційними об'єктами відповідно до принципів найменших привілеїв та необхідності знати.

Впровадження запропонованого підходу оптимізувало розподіл прав доступу між користувачами, зменшило кількість непотрібних дозволів та посилило контроль за обробкою конфіденційної інформації. Ця модель дозволяє гнучко та масштабовано керувати політикою безпеки, враховуючи зміни в структурі організації та її інформаційних ресурсах.

Практична користь від такої еволюції полягає в можливості адаптувати впроваджені методологічні підходи до інших організацій з подібною мережевою структурою. Запропоновані політики доступу сприяють значному зниженню ризиків порушень конфіденційності, цілісності та доступності даних, а також посилюють дотримання компанією вимог інформаційної безпеки та стандартів захисту персональних даних.

Список використаних джерел:

1. BrainBasket Foundation. 2019. URL: https://brainbasket.org/ru/homepage/

2. Закон України «Про інформацію» від 01 липня 2015 р. № 2657-XII // Відомості Верховної Ради України. 1992. № 48. Ст. 650.

УДК 004.7

Жеребцов Д.В., здобувач,
Кухар А.А., здобувач,
Сергійко В.М., здобувач,
Рудюк Б.М., асистент
Державний університет «Житомирська політехніка»

РОЛЬ FIREWALL В СУЧАСНИХ МЕРЕЖАХ

Firewall (міжмережевий екран) від початків Інтернету є ключовим інструментом кібербезпеки, формуючи бар'єр між внутрішньою довіреною мережею та зовнішніми загрозами. Він контролює та фільтрує трафік відповідно до визначених правил безпеки, дозволяючи проходити лише легітимним даним. Сьогодні міжмережевий екран залишається першою лінією оборони проти кібератак як у традиційних, так і в сучасних мережах, захищаючи внутрішні системи від несанкціонованого доступу ззовні. Така система захисту є глобально визнаною і застосовується всюди – від персональних мереж до корпоративних центрів обробки даних і публічних мереж Wi-Fi.

Функціонально міжмережевий екран виконує фільтрацію та моніторинг мережевого трафіку, блокуючи небезпечні або неприпустимі з'єднання і пропускаючи лише дозволені пакети даних. Він може бути реалізований як апаратний пристрій на межі мережі або як програмне забезпечення на сервері чи кінцевому пристрої. Залежно від середовища використання розрізняють мережеві та хостові екрани. Перші працюють на виділеному обладнанні та захищають цілі сегменти мережі, тоді як другі встановлюються безпосередньо на комп'ютерах або серверах, у тому числі хмарних і контролюють трафік окремого вузла

Сучасний глобальний контекст мережевої безпеки ставить перед міжмережними екранами нові завдання. Попри появу додаткових засобів безпеки, міжмережні екрани продовжують еволюціонувати, щоб відповідати загрозам і умовам сьогодення.

Масовий перехід на хмарні сервіси змінив звичну модель безпеки та побудови корпоративних мереж. Критично важливі застосунки та дані тепер розміщені у публічних хмарах, а компанії використовують мультимодельні середовища. У результаті трафік все менше проходить через одну точку контролю, і потребується захист одразу в кількох периметрах. Сучасні міжмережеві екрани відповідають на цей виклик шляхом віртуалізації: з'явилися хмарні міжмережеві екрани, які можна розгортати в хмарній інфраструктурі, а також концепція Firewall-as-a-

Service, що дозволяє централізовано керувати політиками безпеки у хмарному середовищі.

Зростання кількості IoT-пристроїв формує новий фронт кібератак. Ці пристрої, часто зі слабким захистом, генерують великі обсяги даних і працюють у режимі постійного зв'язку, підвищуючи ризик компрометації. Тому мережеві екрани критично необхідні для їхньої безпеки. Сучасні екрани мають бути проактивними. Їхнє використання разом із сегментацією мережі дозволяє ізолювати небезпечний трафік та мінімізувати вплив потенційних атак.

Перехід до віддаленої роботи та концепції BYOD (Bring Your Own Device) призвів до того, що багато співробітників і пристроїв тепер знаходяться поза межами корпоративної мережі. Це кидає виклик традиційним підходам безпеки, адже потрібно захищати доступ до внутрішніх ресурсів із зовнішніх мереж. Новітні рішення дають змогу розширити периметр безпеки на будь-яке місце розташування користувача. Зокрема, модель Firewall-as-a-Service дозволяє охопити всіх авторизованих користувачів незалежно від їхнього місця перебування, часто у поєднанні з VPN, тим самим забезпечуючи захист віддалених офісів і працівників. Такий підхід підтримує концепцію нульової довіри, коли кожне з’єднання перевіряється, а міжмережевий екран виконує роль центрального пункту контролю політик доступу навіть поза межами фізичної офісної мережі.

Незважаючи на швидку еволюцію IT-інфраструктури, міжмережеві екрани продовжує відігравати провідну роль у захисті персональних, корпоративних і публічних мереж. Водночас, сучасні міжмережні екрани значно розширили свої можливості: вони поєднують функції глибокої інспекції пакетів, виявлення вторгнень, веб-фільтрації та інших сервісів, аби протидіяти передовим загрозам.

Отже, міжмережеві екрани продовжують бути ключовим елементом кібербезпеки, адаптуючись до глобальних викликів і залишаючись ефективним інструментом захисту для мереж користувачів у сучасну епоху.

Список використаних джерел:

1. Raja Waseem Anwar, Tariq Abdullah and Flavio Pastore. Multidisciplinary Digital Publishing Institute. Firewall Best Practices for Securing Smart Healthcare Environment. 2021. https://doi.org/10.3390/app11199183

2. Cisco. The Future of the Firewall White Paper. 2019. URL: https://www.cisco.com/c/en/us/products/collateral/security/firewalls/ngfw-futureoffirewalling-wp.html

УДК 004.8

Рій А.І., аспірант,
Заблоцький С. О., аспірант,
Кирик М. І., д.т.н., професор,
Національний університет «Львівська політехніка»

ГІБРИДНА МОДЕЛЬ ISOLATION FOREST-GAN-TRANSFORMER ДЛЯ АНАЛІЗУ МЕРЕЖЕВИХ АНОМАЛІЙ

Вступ

Виявлення аномалій у багатовимірних часових рядах мережевого трафіку вимагає нових підходів, здатних адаптуватися до динамічних змін середовища. У цій роботі представлено гібридну архітектуру IF-DGT, яка поєднує методи статистичного аналізу та глибинного навчання. Такий комплексний підхід дозволяє підвищити точність детектування, ефективно ідентифікуючи як явні аномалії, так і складні, замасковані загрози, що залишаються непомітними для традиційних методів.

Архітектура та принцип роботи

Запропонований метод Isolation Forest-Dropout-GAN-Transformer (IF-DGT) є гібридною ансамблевою архітектурою, що аналізує трафік у двох паралельних потоках, як показано на (Рисунок 1 -).

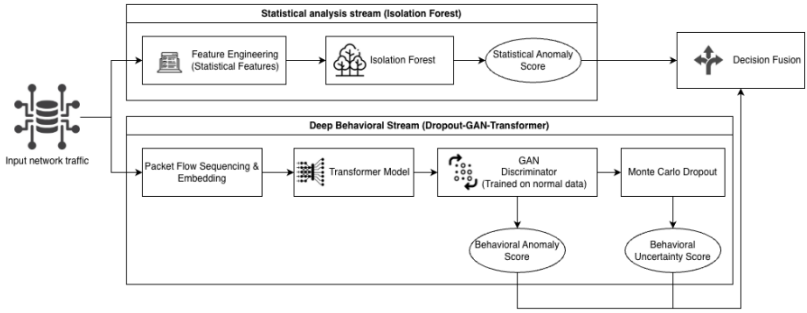


Рисунок 1 – Архітектура комбінованого методу

Перший потік використовує Isolation Forest для високоточного визначення явних статистичних викидів, з якими класичні методи справляються краще та стабільніше. Паралельний DGT-потік працює з прихованими залежностями: Transformer аналізує контекст послідовності, GAN [1] виявляє відхилення від нормального патерну, а MC Dropout оцінює надійність прогнозу [2]. Фінальне рішення формується шляхом об'єднання (стекінгу) цих сигналів. Це дозволяє

системі використовувати сильні сторони обох підходів: Isolation Forest гарантує виявлення "грубих" атак, а DGT розпізнає складні, замасковані вторгнення.

Експериментальні результати

Ефективність IF-DGT оцінено на датасеті CIC-IDS2017 та порівняно з двома базовими моделями: Isolation Forest (класичний ML) та Autoencoder (глибоке навчання). Валідація на спектрі атак (зокрема DDoS та Botnet) підтвердила стійкість методу в умовах реального дисбалансу даних. Результати оцінено за метриками F1-Score, Precision та Recall (Таблиця 1).

Таблиця 1 – Оцінка метрик ефективності запропонованих моделей

Модель	Precision	Recall	F1-Score
Isolation Forest	0.82	0.71	0.76
Autoencoder	0.89	0.86	0.87
IF-DGT (Наша модель)	0.91	0.88	0.89

IF-DGT перевершує базові методи за F1-Score, доводячи ефективність поєднання статистичного та поведінкового аналізу для виявлення складних загроз. Високий Precision (0.91) підтверджує мінімум хибних тривог, необхідний для практичного застосування. Водночас, зростання показника Recall до 0.88 (проти 0.71 у Isolation Forest) свідчить про здатність архітектури розпізнавати замасковані низькоінтенсивні аномалії, які губляться на фоні легітимного трафіку при використанні виключно статистичних підходів.

Висновки

Запропоновано гібридну архітектуру IF-DGT, що поєднує Isolation Forest та ансамбль Dropout-GAN-Transformer. Експерименти на датасеті CIC-IDS2017 демонструють суттєві переваги методу, показуючи високу точність та повноту виявлення. Здатність до адаптації дозволяє моделі ефективно ідентифікувати навіть нові, невідомі раніше типи загроз у динамічному трафіку. Це робить IF-DGT перспективним рішенням для захисту комп'ютерних мереж.

Список використаних джерел:

1. Schlegl T., Seeböck P., Waldstein S. M., Schmidt-Erfurth U., Langs G. Unsupervised anomaly detection with generative adversarial networks to guide marker discovery // International Conference on Information Processing in Medical Imaging (IPMI). 2017. P. 146–157.

2. Shukla A., Jureček M., Stamp M. Social media bot detection using Dropout-GAN // Journal of Computer Virology and Hacking Techniques. 2024. Vol. 20, No. 4. P. 669–680.

UDC 004.056.2

Valentyn Yanchuk, PhD, professor,
Anna Humeniuk, PhD, professor
Zhytomyr Polytechnic State University

DATA AND APPLICATION SECURITY ASPECTS FOR INTERNATIONAL E-COMMERCE SOLUTIONS IN EUROPE AND UKRAINE FROM THE PERSPECTIVE OF DATA PROTECTION AND SUPPLY CHAIN MAINTENANCE

Accelerated integration of the Ukrainian digital economy into the European Single Market has created unprecedented opportunities for cross-border e-commerce. However, scaling operations across these jurisdictions introduces complex challenges at the intersection of data protection compliance, advanced application architecture security, and physical and digital supply chain integrity. Unlike domestic operations, international e-commerce solutions must navigate a bifurcated regulatory landscape while maintaining seamless operational continuity against an evolving threat landscape. This thesis examines the technical and organizational imperatives for securing these cross-border platforms, extending beyond basic transactional security to include complex product configuration systems and international logistics data flows.

The research on this subject is performed in the frame of fellowship under the Polish National Commission for UNESCO 2025/2026 Ref. 205/E/2025 JM.4020.54.2025

The foundation of international e-commerce security in this context lies in harmonizing regulatory requirements. While Ukraine is actively aligning its legislation with European standards, significant operational gaps remain between domestic laws and the General Data Protection Regulation (GDPR). For e-commerce entities operating between Ukraine and the EU, the primary challenge is ensuring lawful cross-border data transfer mechanisms. The architecture must support strict data localization requirements where necessary, while facilitating the flow of transactional data essential for commerce. This requires implementing robust "Privacy by Design" principles directly into the application architecture, ensuring that data subject rights can be executed technically across distributed databases located in different jurisdictions [1].

From an application security perspective, the reliance on monolithic architectures is rapidly becoming a liability in international trade. Modern cross-border e-commerce relies heavily on microservices and extensive API integrations connecting storefronts in one country with logistics providers, payment gateways, and warehousing services in others. Consequently, API

security has emerged as the critical attack surface. Traditional perimeter defenses are insufficient when data constantly flows between Ukrainian specialized services and EU fulfilment centers. Security measures must shift towards rigorous API gateway controls, implementing mutual TLS (mTLS) for service-to-service authentication across borders, and adhering strictly to standards such as the OWASP API Security to prevent broken object level authorization and excessive data exposure in transit [2].

A significant development in modern e-commerce is the rise of complex product configurators, allowing customers to customize goods prior to ordering. These sophisticated frontend tools introduce unique security vectors often overlooked in traditional threat models. Complex configurators frequently rely heavily on client-side logic for interactivity, making them vulnerable to business logic manipulation, such as price tampering or inventory bypass attacks, if client-side validation is trusted blindly. Furthermore, the configuration data itself –representing manufacturing specifications –constitutes sensitive intellectual property. Securing these systems requires rigorous server-side re-validation of complex configuration data structures and ensuring state integrity throughout the customization process to prevent the injection of malicious parameters into the manufacturing workflow [3].

Furthermore, the concept of supply chain maintenance in international e-commerce has expanded to include both the digital software supply chain and the physical logistics data chain. E-commerce platforms depend on a complex ecosystem of third-party libraries and SaaS integrations. A vulnerability in a third-party module used by a Ukrainian vendor can compromise data integrity for European customers, necessitating rigorous Vendor Risk Management (VRM) programs [4].

Simultaneously, the physical aspect of supply chain maintenance – logistics between Ukraine and the EU –presents critical data protection challenges regarding problem-solving in transit. The integration of Ukrainian carriers with pan-European logistics networks requires real-time data exchange regarding customs declarations, routing optimization, and IoT-based tracking. The integrity of this data is paramount; manipulation of shipping manifests or customs data in transit can lead to severe operational disruptions, regulatory penalties at the border, and fraud. Securing these logistics data flows requires immutable audit trails for custody transfer and ensuring that IoT devices used for tracking shipments across borders are secured against compromise to prevent them from becoming entry points into the wider logistics network [5].

In conclusion, securing international e-commerce solutions between Europe and Ukraine requires a holistic strategy that transcends basic compliance. It demands an architectural shift towards Zero Trust principles

for cross-border API interactions, deep visibility into both software and logistics data supply chains, and robust validation mechanisms for complex frontend configurators. Only by integrating these advanced data protection measures directly into the technical fabric of the platform can organizations maintain the trust and operational integrity necessary for sustained international growth.

References:

1. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121–135. DOI: https://doi.org/10.1093/cybsec/tyw001. Last access: 24/11/2025

2. Alshaikh, M. (2020). Developing cybersecurity culture to influence cybersecurity policy compliance: A conceptual framework. Computers & Security, 98, 102003. DOI: https://doi.org/10.1016/j.cose.2020.102003. Last access: 24/11/2025.

3. Quintus, M., Mayr, K., Hofer, K. M., & Chiu, Y.-T. (2024). Managing consumer trust in e-commerce: Evidence from advanced versus emerging markets. International Journal of Retail & Distribution Management, 52(10-11), 1038-1056. DOI: 10.1108/IJRDM-10-2023-0609. Last access: 24/11/2025.

4. Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. Frontiers in Psychology, 13, Article 927398. DOI: 10.3389/fpsyg.2022.927398. Last access: 24/11/2025.

5. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134–153. DOI: https://doi.org/10.1016/j.clsr.2017.05.015. Last access: 24/11/2025.

УДК 004.056:004.451.3

Гребенюк Д. М., магістрант
Черкаський державний технологічний університет

HONEYPOT-ПЛАТФОРМА ДЛЯ ВИЯВЛЕННЯ АТАК

Актуальність. Honeypot-системи - це «приманки» в кібербезпеці, що імітують важливі ресурси - сервери або сервіси з відкритими вразливостями з метою привабити зловмисників. Вони ізольовані від продуктивної мережі і постійно моніторяться, в результаті все, що робить атакуючий фіксується та аналізується. Основна мета - відволікти атаки від реальних критичних систем і визначити методи та інструменти зловмисників [1]. Витяги з активності в Honeypot допомагають отримати цінну розвідувальну інформацію про техніки зловмисників та оновити сигнатури захисту, виправити виявленні вразливості, одночасно зменшуючи кількість хибних спрацювань у системах виявлення. Сучасні дослідження підтверджують, що застосування honeypot-підходів дає змогу своєчасно виявляти реальні загрози та покращувати захист інформаційних ресурсів [5; 7].

Мета і завдання дослідження. Метою роботи є розробка комплексної Honeypot-системи на базі Ruby on Rails для реєстрації та аналізу мережевих атак. Завдання включають:

- розробку архітектури і реалізацію веб-інтерфейсу для налаштування пасток та перегляду логів;
- запуск відповідних служб (HTTP, SSH, FTP) для взаємодії з нападниками [4; 6];
- забезпечення зручного адміністрування на основі фреймворку Avo [3];
- організацію управління життєвим циклом пасток за допомогою бібліотеки Actor [4];
- проведення експериментів з реальними атаками та отримання емпіричних результатів (типи атак і поведінки зловмисників).

Архітектура системи. Система побудована на основі фреймворку Ruby on Rails, що забезпечує стандартні MVC-підходи і швидку розробку веб-додатків [2]. Rails надає готові структури для роботи з базою даних, веб-сервісами й сторінками, а також підтримує зручні механізми міграцій і генерації основних моделей/контролерів для швидкого запуску проекту. Загальна архітектура включає:

- Веб-модуль (HTTP) - декілька Rails-контролерів і маршрутів, що обробляють всі вхідні HTTP-запити (до фіктивних сторінок/інтерфейсів). Кожен запит (URL, заголовки, тіло)

фіксується у відповідних лог-файлах в базі даних для подальшого аналізу.

- Honeypot служби (SSH, FTP) - система запускає окремі фонові сервіси, які імітують реальні SSH- та FTP-сервери з фіктивними обліковими записами. Усі спроби підключення, введення пароля, виконання команд тощо ретельно записуються.
- База даних і моделі - у сховищі зберігається інформація про події (HTTP-запити, SSH/FTP-сесії), налаштування пасток і метадані. Rails-моделі представляють користувачів, пастки і логи.
- Менеджмент процесів - для керування запуском та зупинкою пасток використано бібліотеку Ruby-гем actor, що дозволяє описувати сервіси як поетапні об'єкти (service objects) з можливістю обробки помилок. Це спрощує послідовне виконання дій (запуск демона, налаштування) і їх відкат у разі помилок [4].
- Адміністративний інтерфейс (Avo) - поверх Rails реалізовано зручну панель керування з використанням фреймворку Avo. Avo дозволяє декларативно описати ресурси (моделі) і автоматично генерує CRUD-інтерфейс із зручним UX. Це суттєво скорочує час розробки панелі адміністрування: Avo позиціонує себе як «фреймворк адміністрування для Rails, який економить командам місяці розробки» [3].

Експериментальні результати. Після розгортання на сервері були проведені тестові атаки та збір реального трафіку. Основні спостереження:

- HTTP: зафіксовано численні сканування веб-додатків (перевірка шляхів /admin, /login, /phpinfo тощо), а також атаки на форми (SQL-ін'єкція у полях логіна, XSS-ключі).
- SSH: домінують brute-force-атаки - автоматизовані ботнети підбирали комбінації для ідентифікації за зразками root:password, admin:admin тощо. У вдалих випадках системи відслідковували запуск сценарію та передачу шкідливих бінарних файлів (інколи різних архітектур).
- FTP: аналогічні шаблони - багато підборів логінів/паролів, спроби завантаження сценаріїв, що є класичною поведінкою ботів із використанням стандартних словників.

Висновки. Отримані результати демонструють, що система успішно виконує роль «пастки» для зловмисників. Зібрані дані дозволяють детально аналізувати тактики атак і коригувати захист. В цілому, Honeypot-підхід довів високу ефективність, що обумовлено генеруванням малої кількості хибних спрацювань. Передбачається, що

легітимні користувачі навряд чи навмисно потрапляють у пастку (на відміну від IDS, яка іноді може давати хибні спрацьовування - сигналізувати про небезпеку і у випадках нормального трафіку). Таким чином, презентована Honeypot-система підтвердила практичну користь застосування Ruby on Rails у сфері кібербезпеки. Подальший розвиток може включати додавання штучного інтелекту для автоматичного аналізу зібраних атак, розширення переліку пасток на інші служби (Telnet, IoT-пристрої тощо) та інтеграцію з SIEM-аналізаторами загроз. Такі кроки дозволять перетворити атаку на цінну розвідку і зроблять захист більш проактивним.

Список використаних джерел:

1. The Honeynet Project. Know Your Enemy: Honeynets. URL: https://www.honeynet.org (дата звернення: 20.11.2025).

2. Ruby on Rails Guides. Ruby on Rails Documentation. URL: https://guides.rubyonrails.org (дата звернення: 20.11.2025).

3. Avo. Avo Admin Panel for Ruby on Rails. URL: https://avohq.io (дата звернення: 20.11.2025).

4. Sunny. Actor Ruby Gem: Lightweight Actor Model Implementation. URL: https://github.com/sunny/actor (дата звернення: 20.11.2025).

5. Kaur M., Singh S. Analysis of Honeypot Systems for Network Security. International Journal of Computer Applications. 2014. Vol. 96, No. 18. P. 1-4.

6. Gonzalez A., Smith J. Techniques for HTTP Attack Detection Using Application-Layer Honeypots. Journal of Cybersecurity Research. 2020. Vol. 12(3). P. 45-57.

7. Brown L., Patel R. Deployment of Multi-Protocol Honeypots for Attack Profiling. International Journal of Information Security Science. 2019. Vol. 8(2). P. 63-74.

УДК 004.056.5:004.738.5:004.42

Череватий Б.С., магістрант,
Шушура О.М., д.т.н., професор,
Соломаха С.А., к.е.н., доцент
Державний університет інформаційно-комунікаційних технологій

СИСТЕМА ЗАБЕЗПЕЧЕННЯ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНИХ TELEGRAM-ЧАТІВ

Активне поширення цифрових інструментів комунікації в корпоративному середовищі зумовило зростання ролі месенджерів як основного засобу оперативної взаємодії між співробітниками. Однією з найбільш універсальних платформ є Telegram, що завдяки високій продуктивності, гнучкій інфраструктурі та можливостям інтеграції через боти все частіше використовується в організаціях різного масштабу. Проте збільшення обсягів обміну інформацією у таких середовищах супроводжується підвищенням ризиків витоку конфіденційних даних, несанкціонованого доступу, внутрішніх інцидентів та помилок користувачів. Це формує об'єктивну необхідність створення спеціалізованих систем контролю та моніторингу інформаційної безпеки корпоративних чатів.

Постановка задачі

Telegram став одним із провідних інструментів корпоративної комунікації завдяки простоті використання, можливості автоматизації процесів та підтримці швидкого обміну даними. Однак відсутність централізованих механізмів контролю безпеки, неконтрольоване поширення службової інформації, ризики соціальної інженерії та користувацькі помилки створюють загрозу для інформаційної безпеки підприємств.

Проблема полягає у відсутності ефективного інструменту, який би забезпечував комплексний моніторинг дотримання політик безпеки в корпоративних чатах Telegram та дозволяв би своєчасно виявляти потенційні інциденти без необхідності ручного контролю з боку адміністратора.

Мета дослідження

Метою роботи є розроблення системи моніторингу інформаційної безпеки для корпоративних чатів Telegram, що забезпечує автоматизований контроль за дотриманням політик безпеки, виявлення порушень та інформування відповідальних осіб у режимі реального часу.

Для досягнення цієї мети визначено такі основні завдання:

- дослідити Telegram як платформу корпоративної взаємодії;
- ідентифікувати ключові загрози та ризики інформаційної безпеки;
- сформувати архітектуру системи моніторингу та розробити відповідні алгоритми обробки подій;
- створити та протестувати робочий прототип системи на основі Telegram Bot API.

Результати дослідження

У ході дослідження розроблено архітектуру системи моніторингу інформаційної безпеки, що включає такі ключові модулі:

- модуль збору даних;
- модуль аналізу безпеки;
- модуль логування та сповіщення.

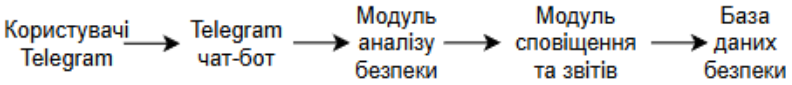


Рисунок 1 - Схема архітектури системи моніторингу

Висновки та перспективи

Розроблена система моніторингу інформаційної безпеки корпоративних чатів Telegram забезпечує можливість оперативного контролю за дотриманням політик безпеки без втручання у приватне листування користувачів. Отримані результати демонструють потенціал такого рішення для інтеграції у корпоративні середовища з метою зменшення ризиків витоку даних, запобігання загрозам та підвищення загального рівня кібербезпеки.

Подальші перспективи роботи включають:

- розширення можливостей аналізу з використанням NLP і машинного навчання;
- адаптацію моделі моніторингу до інших месенджерів;
- впровадження механізмів автоматичного реагування на інциденти.

Список використаних джерел:

1. Горовий В. М. Інформаційні фактори розвитку інформаційних ресурсів у контексті сучасного національного інформаційного комплексу // Національна бібліотека України імені В. І. Вернадського. 2024. URL: https://irbis-nbuv.gov.ua/E_LIB/PDF/er-0004857.pdf

2. Bahramali A., Soltani R., Houmansadr A., Goeckel D., Towsley D. Practical Traffic Analysis Attacks on Secure Messaging Applications. URL: https://arxiv.org/abs/2005.00508.

UDC 004

Karyna Polishchuk, Master's Student,
Oleksii Chyzhmotria, Senior Lecturer,
Tetiana Vakaliuk, Dr. Sc., prof.
Zhytomyr Polytechnic State University

WHY CAMELLIA FAILED TO BECOME A WIDESPREAD CRYPTOGRAPHIC STANDARD

The selection of cryptographic standards shapes the foundation of the global information security infrastructure. Although technical excellence should ideally guide the adoption of standards, the case of the Camellia cipher demonstrates that market success depends on a complex combination of technical, political, and economic factors. This research investigates why Camellia, despite possessing security and performance characteristics comparable to AES, achieved only regional adoption, primarily within Asian markets.

Developed in 2000 through collaboration between NTT and Mitsubishi Electric, Camellia represents a highly sophisticated cryptographic solution. The algorithm is a 128-bit block cipher supporting key lengths of 128, 192, and 256 bits. Its architecture employs a modified Feistel network consisting of 18 or 24 rounds and incorporates FL/FL^{-1} functions for additional security [1]. Independent security evaluations conducted by CRYPTREC and NESSIE confirmed that Camellia offers resistance to differential and linear cryptanalysis equivalent to AES, which led to its certification under ISO/IEC 18033-3 [2].

Performance benchmarks reveal several technical advantages of Camellia. The algorithm demonstrates superior efficiency on 8-bit microcontrollers through optimized lookup table operations and lower memory requirements. Power consumption analysis shows reduced energy usage compared to AES in resource-constrained environments, providing notable benefits for IoT and mobile applications [3]. However, these technical merits were insufficient to ensure global standardization and market dominance.

The key factor that undermined Camellia's international adoption was timing. AES obtained NIST standardization through FIPS 197 in 2001, securing a decisive first-mover advantage during the transition from DES. By the time Camellia pursued international standardization, AES had already achieved substantial market penetration and deep integration within industry solutions. Cryptographic standards exhibit strong network effects, where early adoption creates self-reinforcing advantages through compatibility requirements and ecosystem development [4].

Geopolitical influences also played a crucial role. The U.S. government's mandate requiring AES in federal systems immediately legitimized the standard and stimulated wide-scale adoption across the private sector. In contrast, Camellia received official backing primarily from Japan, which limited its credibility and exposure in Western markets. Moreover, the transparent, globally oriented AES selection process managed by NIST contrasted with Camellia's domestic evaluation in Japan, raising concerns among international stakeholders [5].

Infrastructure-related and linguistic factors further hindered adoption. Major processor manufacturers developed AES-specific optimizations, such as Intel AES-NI and ARM Cryptography Extensions, providing AES with unmatched performance advantages and embedding it deeply into hardware ecosystems [6]. Simultaneously, early documentation for Camellia was available mainly in Japanese, restricting evaluation and understanding among Western cryptographers. Although English translations were later released, these initial accessibility barriers reduced awareness during the critical early adoption phase [7].

In summary, the experience of Camellia emphasizes that even robust algorithms may remain regionally confined if these strategic factors are not addressed effectively. Successful adoption requires synchronized political support, optimal timing, ecosystem readiness, and international outreach.

References:

1. Aoki K., Ichikawa T., Kanda M. Specification of Camellia - a 128-bit Block Cipher. NTT and Mitsubishi Electric Corporation, 2000. 56 p.

2. Cryptrec. Cryptrec report 2002: Evaluation of cryptographic techniques. Information-technology Promotion Agency, Japan, 2003. 331 p.

3. Matsui M., Nakajima J. Performance analysis and parallel implementation of Camellia // IEICE Transactions. 2008. Vol. E91-A, No. 1. P. 172-180.

4. Anderson R. Security engineering: A guide to building dependable distributed systems. 2nd ed. Wiley, 2008. 1088 p.

5. Schneier B. The politics of cryptographic standards // Crypto-Gram Newsletter. April 2002. URL: https://www.schneier.com/crypto-gram/archives/2002/0415.html

6. Gueron S. Intel advanced encryption standard (AES) instructions set. Intel Corporation, 2010. 94 p.

7. Nessie Consortium. Nessie security report. IST-1999-12324. Version 2.0. 2003. 94p.

УДК 004.7

Ліщинський В.В., здобувач,
Романець О. А., здобувач,
Марчук Я. В., здобувач,
Рудюк Б.М., асистент
Державний університет «Житомирська політехніка»

РОЛЬ DHCPv6 У АВТОМАТИЧНІЙ КОНФІГУРАЦІЇ IPv6-АДРЕС У КОРПОРАТИВНИХ МЕРЕЖАХ

Швидке зростання кількості мережевих пристроїв у корпоративних інфраструктурах та перехід до IPv6 створили потребу у гнучких та керованих механізмах автоматичної конфігурації мережевих параметрів. Одним з ключових інструментів, який забезпечує централізоване та масштабоване налаштування хостів в IPv6-середовищі, є протокол DHCPv6.

На відміну від IPv4-версії, DHCPv6 тісно взаємодіє з протоколами SLAAC та Neighbor Discovery, що дозволяє створювати комбіновані методи конфігурації. DHCPv6 підтримує як stateful, так і stateless режими роботи. У stateful-режимі сервер повністю керує видачею IPv6-адрес і зберігає записи про клієнтів, що важливо для аудиту, журналювання та доступності. Stateless-режим дозволяє надавати додаткову інформацію (DNS, доменні параметри), залишаючи призначення адрес механізмам SLAAC. Такий підхід робить DHCPv6 гнучким інструментом, який може бути адаптований під різні корпоративні сценарії.

Використання DHCPv6 дозволяє легко масштабувати мережу: великі IPv6-префікси можуть ефективно розподілятися між тисячами хостів без додаткових ускладнень, що є критично важливим для швидкозростаючих корпоративних середовищ. У динамічних середовищах, де постійно додаються IoT-пристрої, робочі станції або сервери, DHCPv6 забезпечує автоматичне надання необхідних параметрів, роблячи такі зміни прозорими та керованими.

DHCPv6 має важливе значення у підвищенні рівня безпеки корпоративної інфраструктури. По-перше, кожен клієнт ідентифікується унікальним DUID, що унеможливлює конфлікт адрес та дозволяє відстежувати активність конкретних пристроїв. По-друге, централізована конфігурація DNS-серверів допомагає впроваджувати політики фільтрації, моніторингу та захисту від фішингу. По-третє, у поєднанні з Relay-агентами DHCPv6 дозволяє контролювати видачу параметрів між сегментами мережі, що знижує ризик підробки конфігураційних повідомлень.

Додатково DHCPv6 сприяє побудові сегментованих і керованих мереж відповідно до концепцій Zero Trust та Network Access Control, забезпечуючи співпрацю з механізмами 802.1X, firewall-політиками та ACL.

У великих мережах DHCPv6 часто поєднується з системами керування (Cisco Prime, SolarWinds, Zabbix), забезпечуючи повний контроль над адресним простором.

Попри численні переваги, використання DHCPv6 має деякі обмеження:

- потребує додаткової інфраструктури (сервери, relay-агенти);
- складніша конфігурація, особливо при комбінуванні зі SLAAC; затримки у видачі параметрів у великих мережах, якщо сервери перевантажені;
- залежність від довіреної взаємодії з Router Advertisements, оскільки саме вони визначають, чи використовуватиметься DHCPv6;
- повільніше відновлення після збоїв, якщо сервер DHCPv6 є єдиною точкою конфігурації без резервування.

Однак ці недоліки можуть бути мінімізовані за рахунок використання кластерів DHCPv6, резервування та коректної сегментації мереж.

DHCPv6 відіграє ключову роль у побудові сучасних корпоративних мереж на базі IPv6, забезпечуючи централізовану, гнучку та безпечну автоматичну конфігурацію мережевих параметрів. Його інтеграція з іншими компонентами IPv6 дозволяє ефективно масштабувати інфраструктуру, підвищувати рівень безпеки та покращувати мережеве управління.

Список використаних джерел:

1. John RFC 8415: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). *IETF Datatracker*. URL: https://datatracker.ietf.org/doc/html/rfc8415
2. What is an IPv6 Address?. *Bright Data*. URL: https://surl.lu/hpehxx
3. DHCPv6 Server | Junos OS | Juniper Networks. *Juniper Networks, Now Part of HPE – Leading the Convergence of AI & Networking*. URL: https://www.juniper.net/documentation/us/en/software/junos/dhcp/topics/topic-map/dhcpv6-server.html

УДК 004.7

Ліщинський В.В., здобувач,
Романець О.А., здобувач,
Марчук Я.В., здобувач,
Рудюк Б.М., асистент
Державний університет «Житомирська політехніка»

БЕЗПЕКА DHCPv6: МЕТОДИ ЗАХИСТУ ВІД АТАК ТА НЕПРАВОМІРНОГО РОЗПОДІЛУ АДРЕС

У сучасних мережевих інфраструктурах із широким впровадженням протоколу IPv6 автоматизовані механізми конфігурації мережевих параметрів набувають особливої важливості. Протокол DHCPv6 відіграє ключову роль, оскільки забезпечує масштабований та гнучкий розподіл IPv6-адрес, налаштувань DNS, інформації про шлюзи та інших параметрів, необхідних для функціонування мережевих вузлів. Проте робота DHCPv6 у відкритому мережевому середовищі створює значні виклики безпеці, адже неконтрольований процес призначення адрес може стати інструментом для різних кібератак, здатних порушити цілісність і доступність корпоративної мережі.

Базовою проблемою DHCPv6 є відсутність механізмів автентифікації між клієнтом і сервером, що відкриває можливість для запуску несанкціонованих серверів, здатних нав’язувати хибні параметри конфігурації. Такі сервери, маскуючись під легітимні, можуть спричинити спрямування трафіку через шкідливі шлюзи, перенаправлення DNS-запитів до сторонніх серверів або повне блокування мережевої доступності.

Ще однією загрозою є перехоплення та модифікація DHCPv6-повідомлень під час передавання. Оскільки традиційна реалізація протоколу не містить механізмів криптографічного захисту, зловмисник може втрутитися в мережевий трафік, змінити конфігураційні параметри або повторно відправити застарілі повідомлення. У мережах, де одночасно застосовуються SLAAC та DHCPv6, з’являються додаткові можливості для маніпуляцій, оскільки зміна RA-повідомлень безпосередньо впливає на те, яким чином клієнт обирає спосіб конфігурації адреси.

Для протидії цим загрозам у корпоративних мережах застосовується комплекс механізмів, які дозволяють контролювати джерела DHCPv6-повідомлень, обмежувати діяльність підозрілих вузлів і запобігати несанкціонованому впливу на конфігураційні процеси. Одним із найбільш дієвих рішень є використання технологій DHCPv6 Shield, що реалізуються на мережевому обладнанні. Вони дозволяють фільтрувати

DHCPv6-трафік залежно від того, з якого порту він надходить, блокуючи відповіді від можливих фальшивих серверів і запобігаючи їхньому впливу на клієнтів. У поєднанні з механізмами RA Guard, які перехоплюють підозрілі оголошення маршрутизаторів, створюється надійний бар'єр для атак, що використовують взаємодію SLAAC і DHCPv6.

Поступово в інфраструктурних рішеннях з'являються можливості використання автентифікації DHCPv6-повідомлень. Цей підхід базується на криптографічних методах перевірки достовірності джерела та цілісності даних, що значно ускладнює підміну серверів або модифікацію трафіку. Додатково важливим засобом є контроль доступу на рівні комутаторів, що передбачає обмеження кількості пристроїв, які можуть ініціювати DHCPv6-запити з одного фізичного порту. Це унеможливлює атаки на виснаження адресного пулу та знижує ризик масових підроблених запитів.

Значну роль у комплексній безпеці відіграють системи моніторингу мережевого трафіку. Інструменти IDS/IPS, журнали DHCPv6-серверів, аналіз аномалій та збір телеметрії дозволяють швидко виявляти підозрілу активність, визначати джерела атак та реагувати на них у реальному часі. IT-адміністратори отримують можливість оперативно блокувати несанкціоновані порти, ізолювати підозрілі пристрої або змінювати конфігураційні політики з метою локалізації загрози.

Таким чином, безпека DHCPv6 є ключовим елементом побудови надійної IPv6-інфраструктури. Наявність кібератак, спрямованих на процеси призначення адрес, вимагає впровадження узгоджених захисних механізмів, які охоплюють фільтрацію трафіку, автентифікацію, моніторинг та розмежування доступу. Застосування таких методів дозволяє організаціям захищати критичні сегменти мережі від підміни конфігураційних сервісів, збоїв у роботі та перенаправлення трафіку. У результаті створюється стійке до атак середовище, у якому процес автоматизованої конфігурації мережевих параметрів залишається керованим, надійним і відповідним сучасним вимогам кібербезпеки.

Список використаних джерел:

1. John RFC 8415: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). *IETF Datatracker*. URL: https://datatracker.ietf.org/doc/html/rfc8415

2. RFC 4861: Neighbor Discovery for IP version 6 (IPv6). *IETF Datatracker*. URL: https://datatracker.ietf.org/doc/html/rfc4861

УДК 004.7

Єфіменко А. А., здобувач,
Єфіменко А.А., к.т.н., доцент,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

МОДЕЛЬ ПОБУДОВИ SOC З ВИКОРИСТАННЯМ ІНТЕГРАЦІЙ ВІДКРИТИХ ПРОГРАМНИХ РІШЕНЬ

У сучасних умовах стрімкого розширення цифрового простору та зростання інтенсивності кіберзагроз особливої актуальності набуває формування ефективних механізмів забезпечення інформаційної безпеки. Збільшення технологічного периметру, розвиток розподілених інфраструктур та зростання кількості векторів атак вимагають постійного моніторингу подій безпеки та оперативного реагування на інциденти. Операційні центри безпеки (SOC) є ключовими елементами такої інфраструктури, проте традиційні комерційні рішення залишаються недоступними для значної частини малих і середніх організацій через високу вартість впровадження та підтримки. У цьому контексті використання відкритих програмних рішень є перспективним напрямом, що забезпечує можливість створення адаптивних, масштабованих і економічно доцільних моделей SOC.

Аналіз наукових і технічних джерел свідчить про зростаючий інтерес до застосування інструментів із відкритим кодом для логування, аналізу подій, управління інцидентами та автоматизації реагування. Разом з тим, у науковій літературі недостатньо представлено комплексні підходи до побудови SOC на основі повністю відкритого технологічного стеку. Потребують уточнення питання інтеграції компонентів різного призначення, узгодження архітектурних принципів їх взаємодії, формалізації інформаційних потоків та визначення моделей, що описують структурну та функціональну організацію процесів моніторингу і реагування. На практичному рівні існує дефіцит методичних рекомендацій щодо впровадження SOC в умовах обмежених ресурсів і відсутності стандартизованих технологічних підходів.

Метою роботи є розроблення моделі SOC із використанням відкритих рішень, визначення її архітектурних характеристик та побудова прототипу, який забезпечує виявлення, кореляцію та автоматизоване реагування на інциденти інформаційної безпеки. Основна ідея полягає у створенні концептуальної моделі, що інтегрує функціональні можливості відкритих систем SIEM, SOAR та IR у єдине середовище моніторингу та реагування, а також у формулюванні

положень, які визначають функціональні взаємозв'язки компонентів SOC та логіку їх взаємодії в межах цілісної архітектури.

Дослідження виконано в лабораторному середовищі на базі VirtualBox з використанням програмних рішень Wazuh, TheHive, Cortex та Shuffle. Архітектура моделі ґрунтувалася на узгодженні процесів аналізу телеметрії, обробки інцидентів та реалізації автоматизованих реакцій. Для теоретичного обґрунтування використовувалися методики структурного аналізу, системного підходу та моделювання типових сценаріїв загроз, що визначаються за MITRE ATT&CK.

Отримані результати дозволили узагальнити принципи побудови SOC на основі відкритих технологій, визначити архітектурні та функціональні параметри інтегрованої системи, а також сформулювати положення, які описують логіку організації потоків даних і взаємодії між основними підсистемами. Практичне значення дослідження полягає у можливості застосування розробленої моделі для створення доступних рішень у сфері кіберзахисту, формування навчальних і тренувальних середовищ, а також у використанні отриманих результатів як методичної бази для впровадження SOC у організаціях різного масштабу.

Таким чином, використання відкритих програмних рішень може слугувати ефективною основою для побудови доступного SOC, що забезпечує базову автоматизацію, зниження вартості впровадження та адаптованість до потреб організацій. Перспективи подальших досліджень включають розроблення контейнеризованих рішень для розгортання SOC, інтеграцію механізмів машинного навчання для виявлення аномалій та удосконалення автоматизованих сценаріїв реагування.

Список використаних джерел:

1. MITRE. 11 Strategies of a World-Class Cybersecurity Operations Center. 2022. 452 с

2. AT&T Business. How to Build a Security Operations Center (on a Budget). 2019. 35 с.

УДК 004.459

Фальковський І.Г., ст. викладач
Карп'юк І.В., магістрант
Державний університет «Житомирська політехніка»

МОДЕЛЬ ОПТИМІЗАЦІЯ УПРАВЛІННЯ КІНЦЕВИМИ ТОЧКАМИ НА БАЗІ MECM У WINDOWS-ІНФРАСТРУКТУРІ

Стрімке масштабування сучасних IT-інфраструктур та перехід до гібридних моделей роботи формують нові виклики для системних адміністраторів. Зі збільшенням кількості робочих станцій у корпоративній мережі, побудованій на базі Windows, критичного значення набуває проблема ефективного управління кінцевими точками. Ручне виконання рутинних операцій, таких як інсталяція операційних систем, розгортання прикладного програмного забезпечення та встановлення оновлень безпеки, стає не лише економічно недоцільним через високі часові витрати, але й створює суттєві ризики для інформаційної безпеки підприємства. Затримка в оновленні навіть одного вузла може призвести до компрометації всієї системи.

Вирішення цієї проблеми полягає у переході від децентралізованого до повністю автоматизованого централізованого керування. У даній роботі досліджується підхід до побудови такої системи на основі Microsoft Endpoint Configuration Manager у тісній інтеграції зі службами каталогу Active Directory. Цей інструментарій дозволяє розглядати інфраструктуру не як набір розрізнених пристроїв, а як єдиний керований організм, де політики безпеки та конфігурації застосовуються глобально або до цільових груп.

Ключовим технічним аспектом, що дозволяє вирішити проблему навантаження на мережеві канали при масовому розгортанні "важкого" контенту, є впровадження та налаштування Boundary Groups. У роботі продемонстровано, що правильна конфігурація цих параметрів дозволяє локалізувати трафік та оптимізувати маршрути отримання оновлень клієнтськими машинами. Це вирішує проблему "вузьких місць" у мережі під час планових оновлень, забезпечуючи стабільність бізнес-процесів навіть у періоди пікового навантаження на IT-інфраструктуру.

Практична реалізація запропонованої моделі у тестовому середовищі довела свою ефективність. На прикладі автоматизованого розгортання програмного забезпечення, зокрема медіаплеєра VLC та агентів управління було показано, як застосування сценаріїв MECM мінімізує людський фактор та гарантує уніфікацію програмного

середовища на всіх робочих станціях. Впровадження автоматизованих політик оновлення сприяє зменшенню обсягу ручної роботи, дозволяючи фахівцям зосередитися на стратегічних завданнях. Крім того, інтеграція засобів моніторингу дозволяє адміністраторам отримувати превентивні сповіщення про технічні проблеми, такі як нестача дискового простору для баз даних SQL, що забезпечує проактивне реагування на інциденти.

У перспективі модель може бути масштабовано шляхом інтеграції з Microsoft Defender for Endpoint та впровадження багатофакторної автентифікації, що посилить загальний контур безпеки корпоративної мережі .

Отже, впровадження MECM із застосуванням розроблених сценаріїв налаштування Boundary Groups та політик оновлення дозволяє досягти якісно нового рівня керованості інфраструктурою. Це забезпечує баланс між оперативністю обслуговування користувачів та дотриманням суворих стандартів корпоративної безпеки .

Список використаних джерел:

1. Microsoft. Microsoft Endpoint Configuration Manager Documentation. URL: https://learn.microsoft.com/en-us/mem/configmgr/

2. Smith J. Practical Guide to Integrating MECM with Active Directory. IT Pro Publishing, 2020. 450 c.

3. Microsoft. Automatic Deployment of Software Updates. URL: https://learn.microsoft.com/en-us/intune/configmgr/sum/deploy-use/automatically-deploy-software-updates

УДК 004.7

Слободянюк А.О., магістрант
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ТА РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ БАГАТОРІВНЕВОГО ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ

Стабільність функціонування локальних мереж є ключовою умовою безперервності роботи сучасних організацій, оскільки більшість бізнес-процесів прямо залежить від доступності сервісів та збереження цілісності інформації. Зростання кількості кіберзагроз і ускладнення методів атак підсилюють потребу у системах багаторівневого мережевого захисту, здатних забезпечити раннє виявлення порушень і мінімізувати ризики компрометації інфраструктури. Особливої уваги потребують гібридні атаки, які поєднують технічні та соціальні методи впливу й долають традиційні механізми захисту. Це підкреслює важливість систем, що дозволяють отримувати цілісне уявлення про стан мережевої безпеки.

Аналіз сучасних підходів до організації мережевої безпеки показує, що значна частина технічних засобів захисту застосовується ізольовано. Міжмережні екрани, системи моніторингу, IDS/IPS або SIEM-платформи часто працюють автономно, без узгодженого обміну даними. Це породжує фрагментацію захисту: фаєрволи забезпечують фільтрацію трафіку, але не мають контексту поведінкових подій, тоді як системи моніторингу фіксують загрози, однак не можуть самостійно вплинути на трафік або блокування доступу. Це призводить до того, що частина інцидентів фіксується лише після реалізації атаки, що значно збільшує час реагування та масштаби можливих наслідків.

Порівняльний аналіз функціональних можливостей міжмережних екранів та засобів моніторингу безпеки дає можливість виокремити їх ключові переваги й обмеження. Фаєрволи характеризуються високою ефективністю у контролі доступу, сегментації мережі та фільтрації пакетів, проте їхні можливості щодо аналітики обмежені. Натомість SIEM/IDS-системи забезпечують глибокий аналіз подій, кореляцію логів і виявлення потенційних атак, але не можуть самостійно виконувати превентивні дії на рівні мережевого трафіку. Основне протиріччя полягає в тому, що жоден із цих інструментів окремо не забезпечує комплексного захисту, тоді як їхня потенційно ефективна взаємодія на практиці залишається недостатньо узгодженою.

Результати аналізу показують, що найбільш ефективною є модель, у якій фаєрвол виконує функції первинної фільтрації та контролю

доступу, а система моніторингу забезпечує збір і кореляцію подій, виявлення аномалій та формування єдиного інформаційного поля безпеки. Такий підхід рекомендується для інтеграції систем, оскільки у ізольованих реалізаціях, взаємодія між компонентами відсутня, що обмежує швидкість реагування на інциденти та повноту інформації про загрози.

На основі проведеного аналізу сформульовано рекомендації щодо організації багаторівневого захисту локальної мережі:

– забезпечити логічну сумісність міжмережного екранування та систем моніторингу через уніфіковані політики безпеки;

– застосовувати централізований збір журналів подій із мережевих пристроїв, що підвищує повноту інформаційної картини;

– використовувати кореляцію подій для раннього виявлення загроз, які не фіксуються на рівні фільтрації трафіку;

– упроваджувати сегментацію мережі як базову передумову багаторівневого захисту;

– доповнювати систему моніторингу правилами поведінкового аналізу для виявлення складних та малопомітних атак.

Окремо слід розглянути впровадження регулярного аудиту безпеки та тестування політик доступу, оскільки це дозволяє оперативно виявляти конфігураційні помилки та зменшувати площу атаки.

Таким чином, результати аналітичного дослідження свідчать, що комбінований підхід до формування багаторівневої системи захисту є найбільш ефективним з погляду підвищення стійкості мережевої інфраструктури. Поєднання міжмережного екранування та моніторингу подій дозволяє мінімізувати обмеження кожного окремого інструмента й створити узгоджену систему протидії сучасним кіберзагрозам.

Перспективним напрямом подальших досліджень є впровадження адаптивних механізмів автоматизованого реагування та використання інтелектуальних методів аналізу поведінки мережі, що забезпечить вищий рівень автономності та точності виявлення інцидентів.

Список використаних джерел:

1. Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. 3rd ed. Boston: Prentice Hall, 2014, 848 p.

2. Whitman M., Mattord H. Principles of Information Security. 7th ed. Boston: Cengage Learning, 2021. 672 p.

3. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання Cisco: навч. посіб. Київ: КНУТД, 2020. 168 с.

УДК 004.056

Томасов Р.О., магістрант,
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ НАЙПОШИРЕНІШИХ ТИПІВ ВРАЗЛИВОСТЕЙ У WORDPRESS

Актуальність дослідження даної теми зумовлена домінуючим положенням Wordpress на ринку. Станом на 2025 рік понад 43% усіх вебсайтів світу працюють на WordPress, що робить платформу найбільш привабливою ціллю для автоматизованих і цілеспрямованих атак [1].

Враховуючи таку популярність даної CMS, важливим є систематизувати типові вразливості, які найчастіше експлуатуються зловмисниками. За даними аналітиків безпеки, понад 96% компрометацій сайтів на WordPress пов'язані з недоліками в сторонніх плагінів і темах, тоді як ядро системи залишається відносно захищеним [2]. Нижче наведено огляд найпоширеніших типів вразливостей, з акцентом на їх механізми роботи та потенційні наслідки [3].

Міжсайтовий скриптинг (Cross-Site Scripting, XSS) залишається одним із найпоширеніших типів вразливостей у WordPress. Він виникає через недостатнє екранування вхідних даних користувачів при виведенні на сторінку, що дозволяє зловмиснику додавати та виконувати довільний JavaScript-код в браузері інших користувачів. Найнебезпечнішим серед цього лишається збережений XSS, коли шкідливий код зберігається в базі даних (наприклад, у коментарях чи контенті) і автоматично запускається для кожного відвідувача або адміністратора сайта.

SQL-ін'єкції, попри наявність захищених механізмів у ядрі WordPress, продовжують зустрічатися у сторонніх плагінах. Вразливість з'являється внаслідок неправильного формування SQL-запитів, зокрема через конкатенацію невідфільтрованих даних користувача. Наслідком успішної атаки може бути повне отримання вмісту бази даних, зміна або повне знищення всіх даних.

Підробка міжсайтових запитів (Cross-Site Request Forgery, CSRF) становить серйозну загрозу для дій, що змінюють стан системи. Вразливість виникає через відсутність або некоректного використання токенів при обробці POST-запитів. Зловмисник таким чином може змусити автентифікованого користувача виконати небажану дію (наприклад, змінити пароль чи видалити певний контент).

Довільне завантаження файлів є поширеною вразливістю в плагінах, що відповідають за імпорт, резервне копіювання або роботу з

файлами. Через недостатню перевірку типу та вмісту завантажених файлів зловмисник отримує можливість розмістити на сервері виконуваний скрипт (веб-шел або бекдор), що забезпечує стійкий доступ до системи жертви для хакера.

Порушення контролю доступу є критичною проблемою в темах та плагінах, де некоректно реалізована перевірка прав користувача. Вона проявляється через дозвіл на виконання адміністративних дій (наприклад, редагування налаштувань чи видалення контенту) для користувачів з низькими привілеями. Потенційні наслідки включають несанкціоноване маніпулювання сайтом, встановлення бекдорів або навіть повне перехоплення контролю.

Ескалація привілеїв часто зустрічається в плагінах для керування користувачами та реєстрації, де вразливість дозволяє неавтентифікованому зловмиснику створювати облікові записи з правами адміністратора. Механізм базується на помилках у функціях обробки реєстрації без належного контролю ролей. Успішна експлуатація вразливості призводить до переходу повного контролю над сайтом в руки зловмисника.

Таким чином проведений аналіз показав, що попри відносну стійкість ядра, безпека WordPress все ще вкрай залежить від якості сторонніх розширень, які лишаються головним вектором атак. Найпоширеніші вразливості, а також недоліки в контролі доступу та обробці завантажень файлів виникають через фундаментальні помилки під час розробки плагінів, що включає некоректну валідацію вхідних даних та недостатнє розмежування прав доступу. Успішна експлуатація цих недоліків може призвести до несанкціонованого виконання зловмисного коду, викрадення даних або повного захоплення контролю над сайтом, що вимагає від власників ресурсів налаштування процесу постійного моніторингу, регулярного оновлення та вибору лише перевірених сторонніх плагінів і тем.

Список використаних джерел:

1. Usage statistics and market share of WordPress. URL: https://w3techs.com/technologies/details/cm-wordpress

2. 2024 Annual WordPress Security Report by Wordfence. URL: https://www.wordfence.com/blog/2025/04/2024-annual-wordpress-security-report-by-wordfence/

3. WordPress vulnerability guide. URL: https://www.liquidweb.com/wordpress/security/vulnerability/

УДК 004.7

Качур В.В., здобувач,
Рудюк Б.М., асистент
Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ TELNET ТА SSH ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ МЕРЕЖЕВОГО ОБЛАДНАННЯ

У процесі експлуатації сучасних комп'ютерних мереж критично важливим аспектом є можливість віддаленого керування мережевим обладнанням – маршрутизаторами, комутаторами та серверами. У сучасних комп’ютерних мережах питання безпечного віддаленого адміністрування є одним із ключових для підтримання стабільної та захищеної роботи інфраструктури. Для віддаленого доступу до мережевого обладнання застосовуються різні протоколи, серед яких найбільш поширеними є Telnet та SSH. Незважаючи на схожість функціональних можливостей, їх рівень безпеки суттєво відрізняється.

Telnet (Telecommunication Network) – це один із найстаріших мережевих протоколів, розроблений у 1969 році для віддаленого доступу до комп'ютерних систем. Протокол працює на прикладному рівні моделі OSI та використовує TCP-з'єднання через порт 23. Основним недоліком Telnet є передача всіх даних, включаючи облікові дані користувача, у відкритому вигляді без будь-якого шифрування. Це робить протокол вразливим до атак типу «людина посередині» та перехоплення трафіку, що створює серйозні ризики для безпеки мережі.

SSH (Secure Shell) – це криптографічний мережевий протокол, розроблений у 1995 році як безпечна альтернатива Telnet. SSH забезпечує шифрування всього трафіку між клієнтом і сервером, використовуючи асиметричну криптографію для автентифікації та симетричну криптографію для передачі даних. Протокол працює через порт 22 і підтримує різні методи автентифікації, включаючи парольну автентифікацію та автентифікацію на основі ключів.

Основні переваги SSH над Telnet включають:

1. шифрування всіх даних, що передаються;
2. захист від атак перехоплення та підміни даних;
3. підтримку тунелювання та переадресації портів;
4. можливість передачі файлів через безпечний канал;
5. гнучкі механізми автентифікації.

SSH використовує тришарову архітектуру безпеки: транспортний рівень забезпечує шифрування та цілісність даних, рівень автентифікації підтверджує особу користувача, а рівень з'єднання

мультиплексує кілька логічних каналів через одне захищене з'єднання. Сучасні версії SSH підтримують алгоритми шифрування AES, ChaCha20 та інші, що забезпечують високий рівень криптографічної стійкості.

Telnet продовжує використовуватися лише в ізольованих мережах або для застарілого обладнання, яке не підтримує SSH. Однак навіть у таких випадках рекомендується розглянути можливість оновлення обладнання або використання додаткових засобів захисту, таких як VPN-тунелі.

Порівняльний аналіз продуктивності показує, що додаткові обчислювальні витрати на шифрування в SSH є мінімальними на сучасному обладнанні і цілком виправдані з точки зору забезпечення безпеки. Затримка, викликана процесами шифрування та дешифрування, становить лише кілька мілісекунд і не впливає на ефективність адміністративних операцій.

Порівняння цих протоколів показує, що SSH має суттєві переваги над Telnet за всіма ключовими показниками безпеки. Хоча Telnet може використовуватися в закритих або тестових середовищах, у виробничих мережах застосування цього протоколу недоцільне. SSH, у свою чергу, забезпечує високий рівень захисту і відповідає сучасним вимогам кібербезпеки.

Таким чином, хоча обидва протоколи виконують функцію надання віддаленого доступу, з точки зору інформаційної безпеки вони не є рівнозначними. Використання Telnet у виробничому середовищі створює неприйнятні ризики для безпеки і суперечить сучасним практикам кібербезпеки. Telnet є застарілим протоколом, який не відповідає сучасним вимогам захисту інформації. SSH є галузевим стандартом для адміністрування, оскільки забезпечує комплексний захист від прослуховування, підміни даних та несанкціонованого доступу. Повний перехід на SSH є обов’язковим кроком для забезпечення кіберстійкості будь-якої організації.

Список використаних джерел:

1. William S. Data and Computer Communications. Pearson, 2013. 912 p.

2. Ylonen T., Lonvick C. The Secure Shell (SSH) Protocol Architecture. IETF RFC 4251, 2006.

УДК 004.7

Мосійчук Р.І., здобувач,
Рудюк Б.М., асистент
Державний університет «Житомирська політехніка»

ВІДДАЛЕНИЙ ДОСТУП У МЕРЕЖАХ IPV6

У сучасних комп'ютерних мережах, де кількість пристроїв постійно збільшується, а потреба у швидкому та безпечному дистанційному підключенні набуває особливої актуальності, важливу роль відіграє перехід на протокол IPv6. Його впровадження не лише розширює адресний простір, але й значно впливає на організацію віддаленого доступу. У ситуаціях, коли традиційні схеми на базі IPv4 та NAT обмежують можливості прямого підключення до обладнання, IPv6 пропонує простіший та ефективніший механізм для створення захищених каналів комунікації.

Однією з ключових переваг IPv6 у контексті віддаленого доступу є глобальна унікальна адресація. Кожен пристрій може отримати власну адресу, доступну напряму з Інтернету, без використання трансляції адрес. Це усуває необхідність пробросу портів, складних NAT-схем або проміжних сервісів для доступу до серверів, робочих станцій, маршрутизаторів, камер чи IoT-пристроїв.

Однак така доступність потребує високого рівня уваги до безпеки. Пристрої з глобальними IPv6-адресами можуть бути доступні з будь-якої точки світу, тому правильно налаштовані політики фільтрації стають обов'язковими. На відміну від IPv4, де внутрішні підмережі часто ховались за NAT, в IPv6 важливо забезпечити коректну роботу службових механізмів, без яких мережа не функціонуватиме. Зокрема, необхідно правильно поводитися з такими компонентами, як:

- коректна робота ICMPv6;
- протокол Neighbor Discovery (ND);
- механізми SLAAC та DHCPv6.

Ці механізми не можна блокувати бездумно, оскільки це може порушити маршрутизацію або унеможливити встановлення віддалених з'єднань. Саме тому правила доступу в IPv6-інфраструктурі мають формуватися з урахуванням специфічного функціонування цього протоколу.

У забезпеченні захищеного віддаленого доступу важливу роль відіграє IPsec, який спочатку був інтегрований у стандарт IPv6. Це дає змогу будувати нативні тунелі між клієнтом та сервером без

додаткових протоколів. Сучасні рішення також активно використовують:

- WireGuard – простий, швидкий і безпечний тунель;
- TLS-VPN (OpenVPN, SSTP) – підходить для гнучкого керування доступом;
- SSH-технології – для адміністративного підключення та безпечного переносу даних.

Ці методи забезпечують:

- конфіденційність переданих даних;
- цілісність трафіку;
- можливість обмеження доступу до окремих сегментів мережі.

IPv6 робить віддалений доступ простішим і прозорішим, оскільки усуває потребу у складних схемах маршрутизації та NAT-трансляції.

Питання приватності теж залишається важливим, адже глобальні адреси можуть бути статичними. Для цього в IPv6 існують Privacy Extensions, які дозволяють генерувати тимчасові випадкові адреси, мінімізуючи можливість відстеження пристрою під час роботи у віддалених сесіях.

Перехідний період між IPv4 та IPv6 супроводжується використанням таких механізмів, як NAT64, DNS64 та тунелювання. Хоча вони забезпечують сумісність між стеком протоколів, ці технології можуть ускладнювати налаштування віддаленого доступу, оскільки додають додаткові шари трансляції.

Організація віддаленого доступу в IPv6-мережах потребує комплексного підходу: правильного планування адресного простору, налаштування сучасних механізмів автентифікації, багатофакторного захисту, контролю ICMPv6, сегментації мережі, коректної роботи Neighbor Discovery та застосування IPsec або інших сучасних технологій шифрування.

Таким чином, IPv6 формує нову архітектуру мережевої взаємодії, у якій віддалений доступ стає більш прямим, стабільним і масштабованим. Проте це також накладає додаткові вимоги до безпеки та налаштування. Правильне впровадження IPv6 дозволяє повністю реалізувати його потенціал і забезпечити надійний та безпечний віддалений доступ у сучасних мережах.

Список використаних джерел:

1. RFC 8200. Internet Protocol, Version 6 (IPv6) Specification. Internet Engineering Task Force (IETF), 2017. 55 p. URL: https://datatracker.ietf.org/doc/html/rfc8200

УДК 004.7

Лещенко Б.С., аспірант,
Єфіменко А.А., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЗМЕНШЕННЯ РОЗМІРУ КОНТЕЙНЕРНИХ ОБРАЗІВ ЯК СТРАТЕГІЯ ЗНИЖЕННЯ ПОВЕРХНІ АТАКИ

Одним з основних переваг використання контейнеризованих образів, порівняно з віртуальними машинами, стало зменшення розмірів образів. Зростання використання контейнерних технологій спровокувало розвиток досліджень, зосереджених на мінімізації розміру образів *Docker* для підвищення ефективності розгортання та зменшення безпекових ризиків.

Мінімізація кількості вбудованих компонентів та бібліотек сприяє звуженню «поверхні атаки», що, відповідно, обмежує потенційний вектор для експлуатації вразливостей.

Утиліта *BusyBox* [1] була одним з найперших рішень для створення надлегких образів. *BusyBox* об'єднує численні базові *Unix*-команди в одному виконуваному файлі. Образ, що містить лише *BusyBox* та мінімальну реалізацію libc, компактний і підходить для запуску простих бінарних застосунків з мінімальною кількістю залежностей.

Наступним кроком стала поява *Alpine Linux*. *Alpine* є «легким» дистрибутивом, який з самого початку був спроектований для мінімізації свого розміру. *Alpine* використовує *musl-libc* і, той же, набір утиліт *BusyBox*, та власний пакетний менеджер. Однак, слід зауважити, що стандартний Alpine-образ може містити CVE, які не одразу фіксуються традиційними сканерами.

Наступний етап в еволюції безпеки контейнерних образів привніс концепцію так званих *«distroless»* [2] образів, розроблених компанією Google. Distroless образи не тільки виключають непотрібні утиліти, як попередні приклади, а також застосовують радикальне скорочення компонентів, включно з інтерпретатором командного рядка (*shell*) та менеджером пакетів.

Появу декларативних інструментів для побудови мінімальних образів можна назвати новим етапом розвитку контейнеризації. Наприклад, утиліта *apko* від *Chainguard* приймає конфігураційний *YAML*-файл з переліком пакетів та автоматично вирішує залежності, формуючи кінцевий образ.

Ubuntu Chiseled реалізує концепцію package slicing. Package slicing деконструкція Debian пакетів на логічні підмножини залежностей, якими можна легко керувати для створення образів.

У 2025 році також розширено увагу до мінімальних образів на рівні інструментів безпеки. Зокрема, *Amazon* оголосила [3], що *Amazon Inspector* навчають сканувати *distroless* та *Chainguard* образи нарівні з іншими образами. Крім того, нові версії *Docker* та *BuildKit* пропонують додаткові можливості [4]: підтримку стиснення шарів через Zstd/estargz, оптимізацію шарів контейнеру та інші поліпшення, що сприяють створенню ще компактніших образів. Хоч ці новації орієнтовані радше на продуктивність, вони також підвищують безпеку за рахунок зменшення розміру і кращої відтворюваності збірки (в невеликих образах простіше відстежувати зміни).

```
docker images | sort -k7 -h -r
debian                                        latest    8f6a88feef3e   8 days ago      206MB
registry.access.redhat.com/ubi9/ubi-minimal   latest    61d5ad475048   8 days ago      153MB
ubuntu                                        latest    c35e29c94501   5 weeks ago     139MB
debian                                        12-slim   b4aa902587c2   8 days ago      136MB
alpine                                        latest    4b7ce07002c6   6 weeks ago     26.1MB
busybox                                       latest    e3652a00a2fa   14 months ago   13MB
cgr.dev/chainguard/static                     latest    d44809cee093   2 weeks ago     6.41MB
gcr.io/distroless/static                      nonroot   e8a4044e0b4a   N/A             6.23MB
REPOSITORY                                    TAG       IMAGE ID       CREATED         SIZE
```

Рисунок 1 - Порівняння розмірів різних базових образів

На рисунку 1 зображено градацію контейнерних образів за їхнім розміром, показуючи еволюцію від повнофункціональних дистрибутивів до максимально спрощених середовищ.

Таким чином, еволюція підходів до безпеки мінімальних контейнерних образів пройшла шлях від повноцінних дистрибутивів до радикально мінімізованих рішень із суворим контролем вхідних/вихідних даних. Ці сучасні підходи базуються на ідеї обмеження кількості компонентів та наданні розробникам інструментів для декларативного контролю складу образів.

Список використаних джерел:

1. Docker. Busybox. URL: https://hub.docker.com/_/busybox.
2. Google Container Tools. Distroless images. URL: https://github.com/GoogleContainerTools/distroless.
3. Docker. Docker’s developer innovation: unveiling performance milestones. URL: https://www.docker.com/blog/dockers-developer-innovation-unveiling-performance-milestones/.
4. AWS. Amazon inspector enhances container security by mapping amazon ECR images to running containers. URL: https://aws.amazon.com/blogs/aws/amazon-inspector-enhances-container-security-by-mapping-amazon-ecr-images-to-running-containers/.

УДК 004.4:003.26:681.326.3

Омельчук І.А., викладач,
Пількевич І.А., д.т.н., професор,
Мірошніченко С.І., викладач
Житомирський військовий інститут ім. С.П. Корольова

МЕТОДИ МАТЕМАТИЧНОГО ПРОГНОЗУВАННЯ ДЛЯ ВИКОРИСТАННЯ В СИСТЕМАХ УПРАВЛІННЯ РОБОТИЗОВАНИМИ КОМПЛЕКСАМИ

Інтенсифікація розвитку сучасних вимірювальних та інформаційних систем дозволяють автоматизувати і дистанціювати процеси управління різноманітними об'єктами. Саме тому XXI сторіччя принесло людству чергову технологічну революцію. Мікроконтролери, смартфони, системи передачі даних, стрімкий розвиток інформаційних мереж істотним чином змінив буття кожної країни та родини. За минулі 10-15 років в багатьох країнах світу інтенсивно почали з'являтися різноманітні зразки роботизованих комплексів наземного базування або в обмеженому розумінні UGV (unmanned ground vehicles), що стало результатом розвитку сучасних інформаційно вимірювальних технологій. Роботизовані системи широко впроваджуються і в військовій сфері. Значна потреба поширення застосування роботизованих систем наявна в сухопутних військах, які є найбільш «контактними» (переувають у постійній бойовій взаємодії з військовими підрозділами супротивника) і при цьому зазнають найбільш відчутних втрат у військових діях.

Розвиток сучасних військових інформаційних технологій зумовлює швидке впровадження в практику бойового застосування широкого спектру наземних керованих систем різного спектру застосувань, однак вирішення проблематики автоматизації керування цими комплексами на рівнях управління оператором, та адаптації їх до умов застосування в бойових умовах безпосередньо в місцях виконання ними поставлених задач є актуальним питанням сьогодення.

Останнім часом з'являються потужні світові школи та проекти щодо розробки та впровадження автоматичних роботизованих систем та їх складових компонентів.

Велика кількість закладів наукового, військового та цивільного спрямування працюють над розробкою та вдосконаленням роботизованих комплексів [1], їх тягових і маневрових характеристик [2], розробці систем керування рухомими апаратами [3].

Метою даної роботи є розробка алгоритму стабілізації курсової стійкості наземних рухомих апаратів під час їх руху. В основу дії запропонованого алгоритму покладено аналізування виміряних значень відцентрових сил які виникають під час руху комплексу та побудову на

основі цих даних лінії прогнозного тренду щодо їх подальшої поведінки та розвитку. На основі замірів та математичних обрахунків проводиться програмний аналіз стабільності існуючої траєкторії, та обирається варіант реагування на поведінку колісного агрегату при можливій зміні траєкторії, що була спричинена характеристиками дорожнього покриття чи особливостями рельєфу.

Також маючи результати замірів сил що виникають під час руху агрегату на початку маневру є можливість побудувати математичну модель тренду для даного моменту руху з прогнозуванням розвитку подій. Отже володіючи масивом результатів замірів сил реакції на початку виконання маневру можна провести математичне прогнозування розвитку траєкторії руху рухомого апарата [4].

Математичний апарат прогнозування розвитку сил реакції, що виникатимуть під час виконання маневру побудовано на основі методу статистичної обробки результатів вимірювання відцентрових сил що виникають рід час руху апарату.

Методи статистичного моделювання широко розповсюджені та використовуються при прогнозуванні в різних сферах діяльності [5]. Враховуючи систематичність проведення вимірювань під час руху наземного роботизованого копплексу, результати вимірювань отримані під час руху можуть бути розглянуті у вигляді дискретного стохастичного часового ряду з певним кроком в часі. Виміряні значення сил що діють на апарат який рухається є змінною величиною, відповідно часовий ряд в конкретних дорожніх умовах також є різним і визначає траєкторію рухомого об'єкта в конкретний момент часу. Цілком очевидним є те, що для кожного відрізку шляху і особливостей маневру цей ряд є індивідуальним.

Як вказано в [5], значення експонентної середньої S_t можна виразити через значення часового ряду x

$$S_t = \alpha x_t + \beta S_{t-1} = \alpha x_t + \alpha\beta x_{t-1} + \beta^2 S_{t-2} = \ldots =$$
$$= \alpha x_t + \alpha\beta x_{t-1} + \alpha\beta^2 x_{t-2} + \ldots + \alpha\beta^l x_{t-i} + \ldots + \beta^N S_0 = \alpha \sum_{i=0}^{N-l} \beta^l x_{t-i} + \beta^N S_0 , \quad (1)$$

де N – кількість членів ряду; S_0 – деяка величина, що характеризує початкові умови з яких починається застосування формули при $t = 1$; α – параметр згладжування ряду, $\alpha = \text{const}, 0 \le \alpha \le 1; \beta = 1 - \alpha$.

Отже,

$$S_t = \alpha \sum_{i=0}^{\infty} \beta^i x_{i-t} . \quad (2)$$

Таким чином, величина S_t є зваженою сумою всіх членів часового ряду. Причому питома вага обрахованого значення експоненційно зменшується залежно від тривалості проведених спостережень. Саме цей фактор пояснює, назву величини S_t експонентною середньою.

Отже, запровадиши запропоновану математичну модель можна з достатньою ступінню імовірності оцінити розвиток сил реакції які можуть виникати під час виконанні маневру наземним комплексом в умовах цього застосування і зреагувати завчасно щодо коригування його курсу.

Такими діями може бути або швидка коригуюча зміна положення керованих коліс, або коригуванням курсової стійкості динамічним способом [5].

Висновки. Використовуючи запропонований алгоритм є можливість суттєво покращити тактико технічні характеристики наземних роботизованих комплексів.

Також, при застосуванні математичного прогнозування, та застосування коригуючих керувальних дій завчасно, є можливість підвищити швидкість виконання маневрів наземними комплексами що значно ускладнить виявлення та ураження комплексу на полі бою, і дасть змогу підняти його показники живучості.

Список використаних джерел:

1. Перспективи використання мобільних роботизованих комплексів в широкому спектрі вирішення задач мілітарного спрямування / Зінько Р. В., Ванкевич П. І., Черненко А. Д. та ін. // Збірник наукових праць Військової академії. Одеса, 2018. Вип. № 1 (9). С. 17–27. URL:http://zbirnyk.vaodessa.org.ua/images/zbirnyk_9/03.pdf

2. Грубель М. Г., Крайник Л. В., Боднар М. Ф. Оцінка тягово-швидкісних характеристик військової автомобільної техніки за умов руху бездоріжжям методами імітаційного моделювання // Озброєння та військова техніка, 2019. № 3. С. 46–52. URL: http://nbuv.gov.ua/UJRN/ovt_2019_3_6.

3. Папуша Д., Чепюк Л. Автоматизована система управління рухом робота для дослідження небезпечних приміщень // Комп'ютерні технології: інновації, проблеми, рішення – 2017 : тези доп. II Міжнар. наук.-техн. конф. URL: https://conf.ztu.edu.ua/wp-content/uploads/2017/11/154.pdf.

4. Бобошко О. А. Наукові основи підвищення показників маневреності автомобілів: дис. на здобуття ступеня доктора технічних наук за спец. 05.22.02 – Автомобілі і трактори / Харківський нац. автомобільно-дорожній університет. Харків, 2019. 332 с. URL:https://uacademic.info/ua/document/0519U001087

5. Бідюк П. І. Ймовірнісно-статистичні методи моделювання і прогнозування : [монографія] / П. І. Бідюк, О. П. Гожий. – Миколаїв : Чорноморський державний університет ім. Петра Могили, 2014. – 440 с. URL:https://dspace.chmnu.edu.ua/jspui/bitstream.pdf

UDC 004.056.55

Maksym Manko, student,
Viacheslav Tuz, professor,
Cherkasy State Technological University

COMPARATIVE ANALYSIS OF CLASSICAL, POST-QUANTUM, AND QUANTUM CRYPTOGRAPHIC METHODS FOR SECURE MILITARY COMMUNICATIONS

Abstract. This paper provides a structured comparison of classical cryptosystems (symmetric and public-key), post-quantum cryptography (PQC), and quantum key distribution (QKD) with respect to their suitability for secure military communications. We analyze threat models (classical supercomputer vs. quantum-capable adversary), secrecy properties, channel requirements (fiber-optic and free-space optics), and the impact on latency, throughput, and key-lifecycle management. We show that AES-256 in authenticated modes remains the foundation for bulk traffic, while public-key schemes based on factorization/discrete logarithms require migration to PQC standards. QKD delivers physics-grounded key establishment for critical routes but requires specialized infrastructure and careful integration with key management systems (KMS). We propose a phased hybrid architecture (QKD+PQC+AES) and outline a deployment roadmap for Ukraine's security and defense sector.

Introduction and Motivation. Resilience of secure communications amid long-term warfare and increasingly sophisticated cyber operations is a national priority. Classical symmetric ciphers (AES) provide high-throughput confidentiality, while public-key schemes (RSA/ECC) support key establishment and digital signatures. Large-scale quantum computing undermines trust in many public-key algorithms (Shor's algorithm) and moderately affects symmetric ciphers (Grover's algorithm), which can be countered by parameter increases. Two complementary lines of response are emerging: post-quantum cryptography (PQC) – standardized, quantum-resistant algorithms deployable without changing the physical medium; and quantum key distribution (QKD) – a physical-layer method for establishing keys with security guaranteed by quantum mechanics [4–6].

Objective. To justify the cryptographic choices for military communications by comparing classical, post-quantum, and quantum approaches and proposing a viable model for their combined use [8–10].

***Methodology and Comparison Criteria*.** We evaluate along: (i) security model (classical/quantum adversary, forward/backward secrecy, resistance to "record-now-decrypt-later"), (ii) key establishment mechanisms and refresh rates, (iii) latency/throughput and hardware acceleration, (iv)

channel requirements and delivery reliability (BER, atmospheric effects for FSO), (v) compatibility with existing MACsec/IPsec and KMS, (vi) CAPEX/OPEX and lifecycle assurance, (vii) alignment with standards and security policies.

Technical Overview.

1. Symmetric cryptography. AES-256-GCM/CTR as the baseline for bulk data encryption; low latency, broad hardware support, and manageable "quantum overhead" via parameter scaling.

2. Public-key / post-quantum cryptography. Traditional RSA/ECC are vulnerable to Shor's algorithm; migration to standardized PQC KEMs/signatures (e.g., ML-KEM, ML-DSA, SLH-DSA) is recommended. Their advantages include software compatibility and scalability across existing networks [4–6].

3. Quantum key distribution (QKD) Protocols BB84/E91/MDI-QKD; channels include optical fiber and free-space/satellite; required components are single-photon sources/detectors, QRNG, synchronization, and error-correction/privacy-amplification stacks [6–10]. QKD feeds fresh key material into the KMS for use by symmetric protocols (IPsec/MACsec/one-time pad on critical routes) [6–10].

Comparative Analysis

Table 1 – Comparative analysis of cryptographic approaches for military communications.

Criterion	**AES-256 (symmetric)**	**RSA/ECC (classical PK)**	**PQC (ML-KEM / ML-DSA / SLH-DSA)**	**QKD**
Security basis	Computational hardness; Grover mitigated via larger parameters [1,3].	Computational hardness; vulnerable to Shor's algorithm [2].	New hardness assumptions (lattices / hashes) designed to resist quantum attacks [4–6].	Laws of quantum physics (no-cloning, measurement disturbance) [7–10].
Role in system	Bulk encryption + authentication [1].	Key exchange/signatures (legacy paradigm) [2].	Key exchange/signatures (soft-rollout migration) [4–6].	Supplies keys to KMS/OTP [8-10].
Performance	Very high; low latency [1].	Moderate/high with acceleration [2].	Better than RSA at comparable security; larger keys/sigs [4–6].	Channel-limited; key rates are distance-/loss-limited [8-10].
Infrastructure	Existing [1].	Existing [2].	Existing (SW/FPGA/NIC updates) [4–6].	Quantum modules, fiber/FSO, trusted nodes required [9-10].

Best use	Any links and storage [1].	Legacy/transition [2].	Broad interagency use [4–6].	Highest-value corridors (HQ↔DC, government backbone) [7-10].

Note: "PQC standards used: FIPS 203/204/205; QKD profiles/interfaces: ITU-T Y.3800 series, ETSI GS QKD. [4–6] Threat model includes harvest-now-decrypt-later; QKD keys consumed by MACsec/IPsec via KMS [6–10]."

Regulatory and Standards Context (Ukraine/International).

• National cybersecurity policy and requirements for cryptographic protection in the public sector; current orders and message-format requirements for cryptographic tools.

• National encryption standards (including the Ukrainian block cipher "Kalyna"), algorithm identifiers, integration with trust services. [6, 10].

• International standards: profiles and interfaces for QKD networks (ETSI/ITU-T); PQC standards (FIPS) for KEM and signatures. [4–6] *Note.* QKD deployment must be aligned with existing KMS (REST key delivery, key-lifecycle policies, audit) [6–10].

Architecture and Roadmap for Ukraine's Security and Defense Sector.

1. Architectural principles. Trust-domain segmentation; attack-surface minimization; separation of quantum and classical channels. QKD-KMS integration with MACsec/IPsec (fresh key delivery, accounting, rotation). PQC for all interagency transits and signatures, with protocol compatibility.

2. Roadmap (phases). 1) PQC migration –transition to ML-KEM/ML-DSA/SLH-DSA and upgrade of cryptomodules and certification chains; 2) QKD pilot –link between two strategic facilities (dark fiber with FSO backup) integrated with departmental KMS; 3) Trusted-node network –backbone scaling and key-lifecycle policy alignment; 4) Expansion –evaluate satellite segments and ensure multi-vendor interoperability via open profiles.

Practical Significance and Novelty. We propose a unified model for cryptographic transformation of defense networks that combines the strengths of QKD and PQC while remaining deployable on existing infrastructure. The novelty lies in an applied focus on key lifecycle, integration interfaces, and phased implementation aligned with Ukraine's regulatory environment.

Conclusions. In the course of this work, classical (AES/RSA/ECC), post-quantum (ML-KEM/ML-DSA/SLH-DSA), and quantum (QKD) approaches for defense-grade communications were assessed. We conclude

that AES-256 (authenticated modes) is optimal for bulk traffic, public-key functions should migrate to standardized PQC, and QKD should be applied selectively on the most sensitive fixed routes to supply physics-grounded keys. The roadmap is: PQC migration across PKI/gateways → a dark-fiber QKD pilot with KMS integration and FSO backup → expansion to a trusted-node backbone with strict key-lifecycle governance. This hybrid posture strengthens forward secrecy, lowers record-now-decrypt-later risk, and scales on existing MACsec/IPsec networks.

References:

1. National Institute of Standards and Technology. (2001). FIPS 197: Advanced Encryption Standard (AES). https://doi.org/10.6028/NIST.FIPS.197

2. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

3. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th ACM Symposium on Theory of Computing (STOC '96), 212–219. https://doi.org/10.1145/237814.237866

4. National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-based Key-Encapsulation Mechanism (ML-KEM). https://doi.org/10.6028/NIST.FIPS.203

5. National Institute of Standards and Technology. (2024). FIPS 204: Module-Lattice-based Digital Signature Algorithm (ML-DSA). https://doi.org/10.6028/NIST.FIPS.204

6. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175–179. https://doi.org/10.48550/arXiv.2003.06557

7. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301

8. ETSI Industry Specification Group (ISG) QKD. (2019). ETSI GS QKD 014 V1.1.1: Quantum Key Distribution (QKD); Protocol and data format of REST- based key delivery API.

https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf

9. IEEE. (2018). IEEE Std 802.1AE-2018: IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Security (MACsec). https://standards.ieee.org/standard/802_1AE-2018.html

10. DSTU 7624:2014. (2015). Information technologies – Cryptographic protection of information – Symmetric block transformation algorithm. Kyiv: State Enterprise "UkrNDNC". https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=109736

УДК 004.056.53

Коровайченко Ю.Ю., аспірант
Нікітін А.М., аспірант
Державний університет інформаційно-комунікаційних технологій

МОДЕЛЬ БАГАТОШАРОВОГО АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ТА РОЛЬ АЛГОРИТМУ RANDOM FOREST У ІЄРАРХІЇ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОГО ВИЯВЛЕННЯ АНОМАЛІЙ

У сучасних комп'ютерних мережах обсяг і складність трафіку демонструють постійне зростання, що суттєво ускладнює процес виявлення аномалій у таких системах як IPS/IDS (попередження та виявлення вторгнень). Традиційні монолітні методи аналізу виявляються недостатньо ефективними для обробки різнорівневого контексту мережевих даних, який охоплює спектр від сирих пакетів до складних поведінкових патернів. У цьому аспекті багатошаровий підхід аналізу пропонує ієрархічну модель, яка інтегрує сигнатурні, статистичні та методи машинного навчання на пакетному, потоковому й поведінковому рівнях, забезпечуючи комплексне та послідовне виявлення потенційних загроз.

На пакетному рівні аналізу акцент робиться на необроблених даних: прапорцях, значенні часу життя пакета (TTL) та протоколах передачі. Домінуючими тут є сигнатурні методи, призначені для оперативного фільтрування відомих типів атак; водночас застосування методів машинного навчання обмежене високою динамікою обробки та низькою структурованістю інформації. Потоковий рівень передбачає агрегацію даних у форми NetFlow чи IPFIX, з фокусом на таких ознаках, як тривалість з’єднання та обсяг переданих даних, що дозволяє впроваджувати статистичні моделі та базові методи машинного навчання для ефективної редукції шумів. Поведінковий рівень, у свою чергу, орієнтований на вивчення патернів користувацької активності та контекстних відхилень, де методи машинного навчання досягають найвищої продуктивності завдяки здатності моделювати нелінійні залежності в даних.

У загальній ієрархії методів аналізу мережевого трафіку алгоритм Random Forest посідає одне з пріоритетних місць серед ансамблевих підходів у рамках машинного навчання, перевершуючи сигнатурні методи за адаптивністю та евристичні - за стійкістю до варіацій у трафіку. Зокрема, Random Forest виявляється оптимальним для потокового та поведінкового рівнів: він ефективно обробляє

високовимірні набори ознак без ризику перенавчання завдяки механізму баггінгу. Алгоритм характеризується стійкістю до шумів, притаманних мережевим потокам, та забезпечує інтерпретованість через аналіз важливості ознак. На пакетному рівні застосування Random Forest є менш доцільним через обмежену кількість доступних ознак та суворі вимоги до обробки в реальному часі. Алгоритм Random Forest переважає метод опорних векторів (SVM) за швидкістю обчислень на великих масивах даних і градієнтний бустинг - за простотою параметризації, хоча й поступається глибоким нейронним мережам у здатності захоплювати вкрай складні патерни. Таким чином, він забезпечує оптимальний баланс для гібридних систем виявлення вторгнень.

Запропонована багатошарова модель інтегрує алгоритм Random Forest як вершину ієрархії методів, що, за оцінками літературних джерел, демонструє підвищення ефективності на значному рівні. Подальші перспективи розвитку пов'язані з гібридизацією Random Forest та методів глибокого навчання для формування автономних систем кібербезпеки.

Список використаних джерел:

1. Awotunde J. B., Ayo F. E., Panigrahi R., Garg A., Bhoi A. K., Barsocchi P. A Multi-level Random Forest Model-Based Intrusion Detection Using Fuzzy Inference System for Internet of Things Networks // International Journal of Computational Intelligence Systems, 2023. URL: https://link.springer.com/article/10.1007/s44196-023-00205-w

2. Agate V., De Paola A., Ferraro P., Lo Re G. MIDES: A multi-layer Intrusion Detection System using ensemble machine learning // International Journal of Intelligent Networks, 2025. URL: https://www.sciencedirect.com/science/article/pii/S2666603025000156

УДК 004.7

Цевчук В.С., магістрант
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

ПРОЄКТУВАННЯ HONEYPOT-ПІДСИСТЕМИ ДЛЯ ЗАХИСТУ ПУБЛІЧНИХ ПОРТІВ КОРПОРАТИВНИХ МЕРЕЖ

Сучасні тенденції розвитку цифрових мереж в Україні передбачають суттєве посилення захисту публічних портів корпоративних мереж. Концепція Honeypot використовується для створення оманливих сервісів, в яких ключова роль відводиться проактивному моніторингу та блокуванню загроз. Саме проєктна реалізація Honeypot з інтеграцією в MS Active Directory є важливим чинником підвищення безпеки, оскільки традиційні методи (фаєрволи, IDS/IPS) не забезпечують проактивного моніторингу та збору threat intelligence. Згідно з даними звіту Cybersecurity Ventures, кількість кібератак на корпоративні мережі зросла на 50% у 2024 році, що підкреслює необхідність інноваційних рішень, таких як Honeypot, для збору даних про атаки в реальному часі. У контексті українських підприємств, де MS Active Directory є поширеним інструментом управління, відсутність адаптованих honeypot-підсистем призводить до вразливостей у публічних портах, як SSH, Telnet, HTTP/HTTPS, що експлуатуються для несанкціонованого доступу.

У мережах на базі MS Active Directory публічні порти (SSH, Telnet, HTTP/HTTPS) вразливі до несанкціонованого доступу, що призводить до компрометації домену та витоку даних. Проблема посилюється відсутністю інтегрованих honeypot-підсистем з блокуванням IP, обмеженням віртуальним середовищем, браком кількісного аналізу ефективності та фокусу на сучасних загрозах (AI-driven attacks, zero-day exploits). Аналіз застосування схожих технологій виявив сильні сторони в теорії та реалізації, але слабкості в емпіричних даних.

Тому метою дослідження є розробка honeypot-підсистеми для виявлення і блокування зловмисних IP-адрес на публічних портах мережі на базі MS Active Directory, підвищивши рівень кібербезпеки через моніторинг загроз.

Модель прототипу підсистеми розроблялася в середовищі VirtualBox на базі програмного забезпечення Oracle VirtualBox як гіпервізора, Ubuntu Server як шлюзу, Windows Server для MS Active Directory, Cowrie для емуляції SSH/Telnet, Honeyhttpd для HTTP/HTTPS та Kali Linux для симуляції атак, застосовуючи методи експериментального тестування та аналізу логів JSON та Fail2Ban.

В результаті проєктування отримана модель honeypot-підсистеми з інтеграцією в AD через Ubuntu-шлюз з iptables для блокування IP. Прототип розробленої підсистеми є результативним і дійсно виконує функцію виявлення атак (SSH/HTTP) з низьким відсотком помилкових спрацювань.

Таким чином, у доповіді буде представлено модель яка відображає прототип honeypot-підсистеми для мереж MS Active Directory.

Теоретична та практична значимість проведеного дослідження полягає в розширенні знань про застосування honeypot, обґрунтовуючи віртуальну інтеграцію для моніторингу загроз та розвитку теорії кібербезпеки з акцентом на емуляцію сервісів і аналіз threat intelligence, а також у запропонованих рекомендаціях щодо налаштування інструментів Cowrie, Honeyhttpd та Fail2Ban, що суттєво зменшує ризики без значних витрат ресурсів. Запропоновану модель доцільно впроваджувати в корпоративні мережі, що забезпечить на погляд авторів підвищення ефективності виявлення атак, блокування IP-адрес та оптимізації політик Active Directory. Практична значимість полягає в

В перспективі подальше дослідження буде орієнтуватися на масштабування до реальних продуктивних мереж з інтеграцією традиційних IDS/IPS систем, на розширення на додаткові протоколи (FTP, RDP), а також тестування в хмарних середовищах, таких як Azure AD.

Список використаних джерел:

1. Honeypots: tracking hackers. Boston : Addison-Wesley, 2002. 452 с.

2. Blue team handbook: incident response edition : a condensed field guide for the cyber security incident responder. 2-ге вид. CreateSpace Independent Publishing Platform, 2014. 146 с.

3. Public-Facing infrastructure – threatng security - external attack surface management (EASM) - digital risk protection - security ratings. ThreatNG Security. URL: https://www.threatngsecurity.com/glossary/public-facing-infrastructure.

4. Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024. Cybersecurity Ventures. URL: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

УДК 004.7

Приходько Д.С., здобувач,
***Петросян Р.В.**, ст. викладач*
Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ ТЕХНОЛОГІЙ MPLS ТА SD-WAN ПРИ ПОБУДОВІ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

У сучасних умовах масового переходу до хмарних сервісів традиційна архітектура глобальних мереж демонструє свою неефективність. MPLS (багатопротокольна комутація за мітками), який довгий час був основним стандартом, сьогодні характеризується високою вартістю та недостатньою гнучкістю. Альтернативою виступає технологія SD-WAN (програмно-визначені глобальні мережі), яка передбачає відокремлення плоскості управління від плоскості передачі даних. Ключові відмінності між цими двома підходами полягають у рівні операційної гнучкості та відмовостійкості мережі [1-3].

Головним недоліком MPLS є використання застарілої топології Hub-And-Spoke. В неї весь трафік, включно з інтернет-трафіком від віддалених філій, спрямовується через центральний вузол, навіть якщо це не є необхідним. Це явище, відоме як «ефект тромбона», призводить до надмірних затримок та зниження продуктивності мережі через неефективні маршрути. Крім того, залежність від єдиного провайдера та складність масштабування є суттєвими операційними обмеженнями.

SD-WAN є надбудовою, яка може функціонувати поверх будь-якої транспортної мережі, включаючи MPLS, широкосмуговий інтернет або канали LTE. Така архітектура надає значні переваги: дозволяє організувати прямий вихід у інтернет з периферійних відділень, що знижує затримки при роботі з хмарними сервісами. Керування всією інфраструктурою централізоване через єдиний контролер, що дозволяє впроваджувати політики на тисячах пристроїв швидко та послідовно. На противагу, MPLS значною мірою покладається на динамічні протоколи маршрутизації, такі як OSPF, який, хоч і надійний, відрізняються повільною реакцією на зміни. У SD-WAN пристрої не обмінюються маршрутною інформацією безпосередньо, а отримують політики від контролера, що зменшує їхнє обчислювальне навантаження та спрощує управління.

Що стосується ефективності передачі даних, технологія MPLS характеризується мінімальними накладними витратами (4-байтова мітка), тоді як архітектура SD-WAN додає значно більше службові інформації до пакетів. Однак ця втрата ефективності компенсується економічними перевагами. Історично MPLS обирали через гарантії якості обслуговування. SD-WAN подолав це обмеження завдяки

механізму Application-Aware Routing, який дозволяє в реальному часі моніторити стан каналів і автоматично перенаправляти критичний трафік на резервні шляхи при погіршенні якості. Також є можливість відновлення втрачених пакетів, що забезпечує стабільність зв'язку навіть при використанні ненадійних каналів.

Архітектура безпеки MPLS ґрунтується на захисті довіреного периметра, де внутрішня мережа вважається довіреною зоною, а трафік між філіями часто передається без шифрування. На противагу цьому, архітектура SD-WAN реалізує модель «нульової довіри» із обов'язковим шифруванням всього трафіку. Глибока мікросегментація в SD-WAN ізолює мережеві сегменти, запобігаючи горизонтальному пересуванню загроз. Інтеграція з архітектурою Secure Access Service Edge дозволяє перенести інспекцію трафіку в хмарні шлюзи.

Фінансова складова є вирішальним аргументом: перехід з дорогих виділених каналів MPLS на стандартний широкосмуговий інтернет дозволяє скоротити операційні витрати на зв'язок практично вдвічі. Додаткову економію забезпечує механізм Zero Touch Provisioning, що автоматизує процес розгортання обладнання шляхом завантаження конфігурації з хмари, усуваючи необхідність у виїздах обслуговуючого персоналу.

Показовим прикладом переваг архітектури SD-WAN став досвід України в умовах бойових дій [4]. Мережі з MPLS продемонстрували вразливість через прив'язку до фізичної інфраструктури, яка легко пошкоджується внаслідок обстрілів. Натомість SD-WAN забезпечив високу відмовостійкість завдяки оперативній інтеграції терміналів Starlink у мережеву інфраструктуру. Система балансувала трафік між супутниковими каналами, мобільними мережами та вцілілими наземними лініями.

Висновки. SD-WAN – закономірний етап еволюції мереж, що пропонує кращий баланс вартості та функціональності. Попри збереження ролі MPLS у спеціалізованих сегментах, майбутнє належить гібридним моделям, у яких SD-WAN об’єднує різнорідні канали зв’язку в єдину керовану інфраструктуру.

Список використаних джерел:

1. Kernitskyi A. MPLS vs. SD-WAN: Is MPLS Dead?. *Obkio.* URL: https://obkio.com/blog/mpls-vs-sd-wan/.

2. The Foundations of SD-WAN and MPLS Technologies. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/sd-wan-vs-mpls.

3. SD-WAN and Local Internet Breakouts. *Zscaler*. URL: https://www.zscaler.com/resources/solution-briefs/sd-wan-security.pdf.

4. How Starlink Became Ukraine’s Lifeline in War. *UNITED24 Media*. URL: https://united24media.com/war-in-ukraine/how-starlink-became-ukraines-lifeline-in-war-5774.

УДК 004.056:004.8

Боцанюк І.М, магістрант,
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

АДАПТИВНА МОДЕЛЬ ПІДВИЩЕННЯ СТІЙКОСТІ СИСТЕМ ВИЯВЛЕННЯ ФІШИНГУ

Стрімка еволюція соціотехнічних атак формує потребу у створенні засобів кіберзахисту, здатних гнучко реагувати на нові техніки обходу фільтрації. Незважаючи на прогрес у сфері інформаційної безпеки, фішингові атаки залишаються одним із головних векторів початкового проникнення в корпоративні мережі [1], тоді як статичні моделі поступово втрачають ефективність унаслідок появи адаптивних методів маскування та контекстної маніпуляції [2]. Особливо вразливою залишається ділова електронна пошта, де зловмисники експлуатують семантику й поведінкові патерни, що ускладнює виявлення та призводить до значних економічних втрат [3]. Додаткову складність становить те, що сучасні атаки часто не містять шкідливих вкладень, а базуються на створенні переконливих підроблених сценаріїв комунікації. Основна проблема полягає у неможливості статичних систем своєчасно відображати зміни в поведінці атакуючих.

Метою роботи є розроблення адаптивної моделі виявлення фішингу, що поєднує гнучке зважування ризиків, аналіз поведінкових характеристик та механізми активного навчання. У ролі базової архітектури для оброблення тексту використано трансформерну модель DistilBERT, що забезпечує збалансоване співвідношення між точністю класифікації та швидкодією.

У межах дослідження створено архітектуру гібридної системи, яка інтегрує результати різних модулів аналізу в єдине адаптивне рішення. Центральним елементом є коефіцієнт адаптивної довіри - механізм, що коригує вагу прогнозу моделі відповідно до рівня впевненості; у разі низької визначеності посилюється роль евристичних перевірок та системних правил безпеки. Якщо в листі виявлено критичні індикатори ризику, такі як приховані символи, аномальна структура тексту чи ознаки соціальної інженерії, повідомлення автоматично маркується як підозріле.

Особливу увагу приділено модулю поведінкового аналізу, який формує персоналізований профіль користувача, враховуючи часові закономірності листування, історію попередніх комунікацій і сталість довірених доменів. Коли новий лист суттєво відхиляється від звичних патернів, система підвищує ризикову оцінку за рахунок додаткових

штрафних факторів. Це дозволяє виявляти технічно коректні, але поведінково аномальні повідомлення, які легко обходять класичні сигнатурні та контентні фільтри.

Для забезпечення безперервної адаптації впроваджено механізм активного навчання на основі локального зворотного зв'язку: виправлення користувача автоматично використовуються для донавчання моделі на пристрої. Такий підхід зменшує кількість хибнопозитивних спрацьовувань і забезпечує поступове удосконалення системи відповідно до реального середовища без передавання конфіденційних даних на зовнішні сервери.

Модуль очищення та нормалізації вхідного тексту додатково захищає систему від маніпулятивних впливів, виявляючи приховані символи та спроби прихованої модифікації контенту. Крім того, інтегрований модуль пояснення рішень формує інтерпретований звіт про причини блокування або маркування листа, підвищуючи прозорість і керованість процесу виявлення.

Запропонована адаптивна модель усуває основні обмеження статичних систем шляхом поєднання динамічного зважування ознак, поведінкового аналізу та локального активного навчання, що суттєво підвищує стійкість системи до нових технік атак і водночас забезпечує конфіденційність обробки даних. Перспективним напрямом розвитку є розроблення методів колективного захищеного навчання, що дозволить поширювати інформацію про загрози між користувачами без розкриття змісту приватної кореспонденції.

Список використаних джерел:

1. 2024 Data Breach Investigations Report [Електронний ресурс] / Verizon. – New York : Verizon, 2024. – URL: https://www.verizon.com /business/resources/reports/dbir/.

2. Lu J. Learning under Concept Drift: A Review / J. Lu, A. Liu, F. Dong // IEEE Transactions on Knowledge and Data Engineering. – 2018. – Vol. 31, № 12. – P. 2346–2363.

3. Internet Crime Report 2023 [Електронний ресурс] / Federal Bureau of Investigation. – Washington, D.C. : Internet Crime Complaint Center, 2023. – 33 p. –URL: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Re port.pdf.

УДК 004.7

Гаврилюк В.А., магістрант
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ТА РЕКОМЕНДАЦІЇ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ РОЗПОДІЛЕНИХ КОРПОРАТИВНИХ МЕРЕЖ

Для надання найкращого рівня послуг корпорації дедалі частіше відкривають регіональні представництва. Це дозволяє не лише прискорити обслуговування, але й краще розуміти потреби локальних клієнтів. Разом з цим, компанії беруть на себе додаткову відповідальність за збереження конфіденційної інформації, розуміючи, що довіра – це найцінніший актив, тому безпеці даних надається вищий пріоритет. Саме тому в умовах зростання кількості філій та поширення гібридних моделей роботи, основним завданням стає забезпечення безпечної взаємодії між географічно розподіленими офісами та впровадження суворого контролю доступу до внутрішніх ресурсів.

Проблемним питанням залишається невідповідність нинішнього стану захисту багатьох корпоративних мереж сучасним кіберзагрозам. В процесі організації зв'язку між філіями, в яких відсутній належний рівень шифрування, а також централізовані механізми аутентифікації та авторизації, виникають суттєві ризики несанкціонованого доступу, перехоплення та модифікації конфіденційних даних. Крім зовнішніх загроз, актуальною залишається проблема неконтрольованого доступу в межах локальної мережі, що вимагає впровадження гранулярного контролю на рівні портів комутаторів. Необхідність аналізу методів захисту від загроз визначає основний напрям даного дослідження.

Метою дослідження є аналіз та розробка рекомендацій щодо проектування підсистем захисту корпоративних мереж із використанням технологій GRE over IPSec, RADIUS.

У процесі дослідження проведено порівняльний аналіз протоколів автентифікації RADIUS та TACACS+. Визначено, що, хоча TACACS+ забезпечує шифрування всього тіла пакета та розділення процесів авторизації й аутентифікації, RADIUS є відкритим стандартом (RFC 2865), що гарантує кращу сумісність у гетерогенних мережах та є єдиним вибором для реалізації мережевого доступу за стандартом 802.1x.

Також розглянуто типи VPN-технологій (Site-to-Site, Remote Access) та здійснено детальне порівняння GRE over IPsec із звичайним IPsec тунелюванням. Встановлено, що класичний IPsec не підтримує multicast-трафік, що унеможливлює коректну роботу протоколів

динамічної маршрутизації (OSPF, EIGRP) без значного ускладнення конфігурації. Використання комбінації GRE over IPsec нівелює цей недолік: GRE інкапсулює службовий та multicast-трафік у unicast-пакети, які потім надійно шифруються IPsec, забезпечуючи гнучкість та безпеку каналу.

Як приклад, в доповіді буде продемонстровано прототип рекомендованої інтегрованої моделі підсистеми захисту, яка поєднує тунелювання GRE over IPsec, щоб забезпечити захищений зв'язок між офісами та механізми 802.1x для контролю доступу.

Моделювання мережевої інфраструктури та відпрацювання сценаріїв захисту виконувалося у середовищі емуляції GNS3. Як програмно-апаратну основу задіяно віртуальні образи маршрутизаторів та комутаторів Cisco, а також обладнання Mikrotik. З метою реалізації централізованої політики AAA розгорнуто сервери RADIUS, а тестування клієнтського доступу виконується за допомогою віртуальних машин з ОС Windows.

Аналіз розробленого прототипу підтвердив, що система забезпечує конфіденційність передачі даних, коректну роботу протоколів динамічної маршрутизації через захищений канал та ефективне блокування неавторизованих пристроїв на рівні комутації, що доводить практичну життєздатність моделі для використання в корпоративних мережах.

На основі проведеного аналізу було розроблено рекомендації з метою забезпечення комплексного захисту корпоративної мережі, підвищення ефективності та безпеки бізнес-процесів. Однією з головних функцій запропонованої моделі є синергетичне поєднання надійного шифрування каналів зв'язку та централізованого, гранулярного контролю доступу до ресурсів, що дозволяє ефективно протидіяти сучасним загрозам.

Список використаних джерел:

1. Stallings W. Network Security Essentials: Applications and Standards. Pearson, 2016. 464 с..

2. Stewart M., Kensey D. Network Security, Firewalls, and VPNs. 3rd ed. Jones & Bartlett Learning, 2020.

УДК 004:7

Сердійчук І.С., магістрант
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

ШЛЯХИ УДОСКОНАЛЕННЯ ЗАХИСТУ ГЕТЕРОГЕННОЇ МЕРЕЖІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ КОМПЛЕКСУ VPN-ТЕХНОЛОГІЙ

Стабільність та безпека функціонування корпоративних мереж є ключовою умовою безперервності бізнес-процесів сучасних організацій. Стрімка цифровізація призвела до трансформації класичних локальних мереж у складні гетерогенні системи, які об'єднують різнорідні компоненти: серверні кластери, стаціонарні робочі станції, мобільні пристрої співробітників та датчики інтернету речей. Кожен із цих елементів має відмінні обчислювальні можливості та працює під управлінням різних операційних систем, що створює нові виклики для систем захисту інформації.

Основним механізмом забезпечення конфіденційності даних при передачі через відкриті канали зв'язку залишаються технології віртуальних приватних мереж (VPN). Проте аналіз сучасних підходів до їх впровадження виявляє суттєву проблему: застосування уніфікованих стандартів тунелювання для всіх учасників мережі є неефективним. «Важкі» протоколи створюють критичне навантаження на мережу, що призводить до значних затримок у передачі даних. Водночас, спрощені рішення, орієнтовані на швидкість, можуть не забезпечувати достатнього рівня криптографічної стійкості для захисту конфіденційної корпоративної інформації.

Метою роботи є підвищення рівня захищеності та продуктивності гетерогенної мережі шляхом розробки методу адаптивного використання VPN-технологій. В рамках дослідження проведено порівняльний аналіз провідних протоколів. Встановлено, що новітні протоколи, такі як WireGuard, демонструють значно менші затримки завдяки оптимізованій кодовій базі, тоді як класичний IPSec забезпечує кращу сумісність із наявним мережевим обладнанням. Теоретична значущість дослідження полягає в обґрунтуванні гібридної моделі, де вибір технології захисту відбувається динамічно, виходячи з параметрів кінцевого вузла.

За результатами аналізу сформульовано рекомендації щодо удосконалення захисту гетерогенної мережі:

- впровадити класифікацію мережевих вузлів за рівнем обчислювальної потужності та вимогами до безпеки;

- застосовувати адаптивний підхід до вибору протоколу: використовувати WireGuard або оптимізований IKEv2 для мобільних пристроїв для зменшення затримок, та OpenVPN/IPSec з посиленими алгоритмами шифрування для зв’язку між філіями;
- розробити модель загроз, специфічну для гетерогенного середовища, враховуючи вразливості кінцевих точок з обмеженими ресурсами;
- використовувати засоби автоматизованого керування конфігураціями для динамічного перемикання параметрів тунелювання.

Окрему увагу в процесі реалізації цих рекомендацій слід приділити питанням відмовостійкості та балансуванню навантаження. Оскільки запропонований гібридний підхід передбачає одночасне функціонування кількох шлюзів або різних конфігурацій на одному пристрої, критично важливо забезпечити постійний моніторинг ресурсів маршрутизатора.

Таким чином, результати аналітичного дослідження свідчать, що відмова від монолітної архітектури VPN на користь адаптивної моделі дозволяє досягти синергетичного ефекту. Комбінований підхід забезпечує зниження навантаження на клієнтські пристрої та на саму мережу, що прямо корелює з підвищенням загальної продуктивності праці співробітників за рахунок зменшення часу відгуку інформаційних систем. При цьому рівень захищеності мережевого периметра залишається високим, оскільки інші алгоритми не застосовуються для передачі критично важливих даних. Перспективним напрямом подальших досліджень є розробка алгоритмів автоматичного перемикання протоколів тунелювання в реальному часі на основі поточного стану каналу зв'язку.

Список використаних джерел:

1. Оліфер В. Г., Оліфер Н. А. Комп'ютерні мережі. Принципи, технології, протоколи. Київ : Каравела, 2020. 992 с.

2. Столлінгс В. Криптографія та мережева безпека: принципи та практика. Москва : Вільямс, 2018. 750 с.

3. Goralski W. The Illustrated Network: How TCP/IP Works in a Modern Network. Morgan Kaufmann, 2017. 866 p.

УДК 004.85

Івченко О.В., к.т.н., доцент,
Єфименко Д.В., здобувач,
Черкаський державний технологічний університет

РОЗРОБКА ТА ВПРОВАДЖЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ МЕРЕЖІ НА ОСНОВІ ФАЄРВОЛІВ CISCO НОВОГО ПОКОЛІННЯ (NGFW)

Сучасні корпоративні мережі піддаються зростаючому спектру кіберзагроз, включаючи DoS/DDoS, складні багаторівневі атаки (APT) та експлуатацію 0-day уразливостей[1]. Класичні фаєрволи, що базуються на фільтрації пакетів, є недостатніми для забезпечення належного рівня захисту, оскільки вони не здатні аналізувати трафік на рівні додатків чи протидіяти шифрованим атакам.

Фаєрволи нового покоління (NGFW) [2], зокрема рішення компанії Cisco, поєднують функції міжмережевого екрану, системи запобігання вторгнень (IPS), контролю застосунків та інтеграції з антивірусним захистом.

Об'єктом дослідження в роботі є процеси забезпечення інформаційної безпеки корпоративних мереж. Предметом дослідження є методи та засоби побудови комплексної системи захисту мережі на основі фаєрволів Cisco NGFW (ASA, Firepower).

Мета роботи полягає у розробці та впровадженні комплексної системи захисту корпоративної мережі з використанням фаєрволів Cisco нового покоління, дослідження ефективності їх застосування для протидії сучасним кіберзагрозам.

В результаті виконання роботи було проведено аналіз сучасних кіберзагроз та методів їх нейтралізації. Досліджені функціональні можливості Cisco NGFW (ASA, Firepower Threat Defense – FTD), розроблено архітектуру системи захисту корпоративної мережі на базі Cisco NGFW, налаштувано політики безпеки (контроль доступу, IDS/IPS, фільтрація застосунків, URL-фільтрація). В тестовому середовищі змодельовані типові атаки (SQL-ін’єкції, brute-force, DoS) і оцінена ефективність системи захисту.

Порівняльний аналіз показав, що класичні підходи мають переваги у простоті та низькому впливі на продуктивність, але критично обмежені через відсутність аналізу вмісту трафіку (Layer 7) та неефективність проти сучасних багатовекторних атак.

NGFW (Cisco, Fortinet, Palo Alto, Check Point) [2,3] забезпечують глибоку інспекцію трафіку (DPI), контроль додатків (App-ID),

інтегрований IPS/IDS, SSL/TLS-інспекцію та Sandboxing. Недоліками сучасних рішень є висока вартість та складність налаштування.

Запропонована система захисту побудована на базі Cisco Firepower Threat Defense (FTD) [4], яка об'єднує класичні функції Cisco ASA (міжмережевий екран, VPN) із передовими можливостями NGFW.

Управління системою здійснюється централізовано через Firepower Management Center (FMC), що забезпечує моніторинг, аналітику та інтеграцію із зовнішніми системами SIEM (Security Information and Event Management) та SOC (Security Operations Center).

Проєктування архітектури системи захисту базується на принципах багаторівневого захисту (Defense in Depth) та включає: периметровий NGFW, ізольовану DMZ та захист критичних внутрішніх сегментів.

В рамках практичної частини було розроблено політики доступу, що включають:

• Розмежування прав доступу на основі ролей користувачів та сегментації.

• Реалізація засобів захисту від типових атак: DoS/DDoS захист, захист від SQL-ін'єкцій та інших атак на додатки через інспекцію HTTP/S запитів (WAF), Brute-force prevention: блокування IP-адрес після невдалих спроб аутентифікації.

У тестовому середовищі, що включало сегменти LAN, DMZ, Internet та VPN-клієнтів, було змодельовано атаки (наприклад, сканування портів nmap, SQL-ін'єкції sqlmap) для перевірки ефективності налаштованих IPS-політик та роботи Cisco AMP.

Впровадження комплексної системи захисту на основі Cisco NGFW (FTD) забезпечує багаторівневий захист корпоративної мережі, що є необхідним в умовах сучасних кіберзагроз. Завдяки інтеграції функцій DPI, IPS, AMP та централізованому управлінню через FMC, система демонструє високу точність виявлення загроз та ефективність проти складних шифрованих атак та zero-day експлойтів.

Список використаних джерел:

1. Cisco Talos Intelligence. Threat Research Reports. – Cisco, 2023. – URL: https://talosintelligence.com

2. Anderson, B. Next-Generation Firewall Architectures: Comparative Analysis and Trends // Journal of Cybersecurity. – 2023. – Vol. 12, № 4. – P. 55–72.

3. Sharma, R. Deep Packet Inspection and Application Identification in Modern NGFW Systems // IEEE Security & Privacy. – 2022. – P. 48–57.

4. Cisco Secure Firewall Threat Defense Configuration Guide. – Cisco Systems. – 2024. – URL: https://www.cisco.com

УДК 004.85

Івченко О.В., к.т.н., доцент,
Бочаров П.І., здобувач,
Черкаський державний технологічний університет

АНАЛІЗ ТА ОПТИМІЗАЦІЯ АЛГОРИТМІВ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ В МЕРЕЖАХ З ВЕЛИКОЮ КІЛЬКІСТЮ ВУЗЛІВ

Сучасні IP-мережі (хмарні сервіси, IoT) стрімко зростають за розміром і складністю, що висуває жорсткі вимоги до пропускної здатності, надійності та затримки. Традиційні алгоритми маршрутизації (RIP, OSPF) у великих мережах демонструють обмеження: погіршується час конвергенції, зростає обсяг службового трафіку та вимоги до ресурсів маршрутизаторів [1]. Дослідження присвячене системній оцінці цих обмежень та розробці практичних методів оптимізації, зокрема шляхом впровадження Segment Routing, Fast Reroute та елементів машинного навчання.

В роботі проведений комплексний аналіз ефективності існуючих алгоритмів динамічної маршрутизації (OSPF, EIGRP, RIP, BGP) у великих IP-мережах, виявленню їхніх обмеженнь при масштабуванні та розробці практичних методів оптимізації з метою підвищення швидкодії, надійності й ефективності використання ресурсів мережі.

Об'єктом дослідження в роботі є процес маршрутизації даних у великих IP-мережах. Предмет дослідження – алгоритми динамічної маршрутизації (OSPF, EIGRP, RIP, BGP) та методи їхньої оптимізації з урахуванням масштабованості та часу конвергенції. Для дослідження використано аналітичні методи, математичне та експериментальне моделювання. Експерименти проводилися у симуляційному середовищі Cisco Packet Tracer, де були побудовані тестові топології на 50, 200 та 1000 вузлів.

Основні результати та наукова новизна

1. Порівняльний аналіз протоколів. Проведено порівняльне дослідження поведінки алгоритмів Link State (OSPF, IS-IS), Distance Vector (RIP) та Hybrid (EIGRP) у залежності від масштабу мережі. Виявлено, що для топологій до 50 вузлів прийнятний RIP, для 200–500 вузлів оптимальними є OSPF та EIGRP, а для 1000+ вузлів необхідні ієрархічні підходи (IS-IS, BGP)[2].

2. Оптимізація таблиць маршрутизації. Удосконалено підхід до побудови ієрархічної маршрутизації (OSPF multi-area) з використанням агрегації маршрутів. Моделювання показало, що такий підхід забезпечує скорочення обсягу таблиць маршрутизації на 60–85% на

маршрутизаторах ядра в мережі на 1000 вузлів, знижуючи навантаження на обчислювальні ресурси.

3. Підвищення відмовостійкості (Fast Reroute). Доведено ефективність застосування технології Fast Reroute (FRR), зокрема механізму Loop-Free Alternate (LFA). Експерименти показали, що FRR дозволяє зменшити час відновлення зв'язності після відмови лінка до < 50 мс (порівняно з 4–6 с без FRR), що є критично важливим для сервісів реального часу.

4. Впровадження Segment Routing (SR). Розроблено концептуальну модель використання Segment Routing (SR-MPLS) як сучасного методу оптимізації. SR-MPLS забезпечує централізоване керування потоками. Моделювання показало, що SR призводить до зменшення розміру таблиць маршрутів на 76% та зниження середньої затримки на 55% завдяки мінімізації стану в проміжних вузлах.

Отримані результати та розроблені рекомендації можуть бути використані при проектуванні та оптимізації мереж великого масштабу (корпоративних, операторських). Розроблені лістинги конфігурацій (RIP, OSPF, IS-IS, EIGRP, BGP, FRR, SR-MPLS) можуть бути застосовані для лабораторних робіт та практичних занять зі спеціальності «Кібербезпека та захист інформації».

На основі аналізу встановлено, що корпоративним мережам (середнього/великого масштабу) рекомендується використовувати OSPF multi-area у поєднанні з Fast Reroute (FRR) для забезпечення відновлення зв'язку менш ніж за 50 мс, операторським мережам (великі магістралі) рекомендується впроваджувати Segment Routing (SR-MPLS / SRv6), інтегруючи його зі SDN-контролерами та ML-прогнозуванням для досягнення максимальної масштабованості та адаптивного управління трафіком.

У роботі отримано нові наукові результати, що підтверджують можливість підвищення ефективності динамічної маршрутизації у масштабних мережах за рахунок комбінування ієрархічної структури, технологій Fast Reroute, Segment Routing та SDN-контролю, скорочуючи час конвергенції та зменшуючи навантаження на мережеві ресурси.

Список використаних джерел:

1. Байда С. В., Соловйов І. В. Маршрутизація в комп’ютерних мережах: теорія та практика. Київ : Ліра-К, 2021.

2. Rekhter Y., Li T., Hares S. A Border Gateway Protocol 4 (BGP-4) : RFC 4271. IETF, 2006. URL: https://datatracker.ietf.org/doc/html/rfc4271

УДК 004

Кожухівський А. Д., професор
Ганусяк С. І., аспірант
Державний університет інформаційно-комунікаційних технологій

ПРОГНОЗУВАННЯ БОТНЕТ-АКТИВНОСТІ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА ЗА ДОПОМОГОЮ РЕГРЕСІЙНИХ МОДЕЛЕЙ

Ботнети – це розподілені мережі скомпрометованих пристроїв, які потрапили під контроль зловмисників і використовуються ними для виконання різноманітних шкідливих дій. До складу таких мереж можуть входити персональні комп'ютери, сервери, мобільні пристрої, а в умовах стрімкого розвитку Інтернету речей – навіть розумні телевізори, побутова техніка та системи відеоспостереження. Усі ці пристрої об'єднуються під централізованим або децентралізованим управлінням, що дозволяє зловмисникам координувати масовані кібератаки – зокрема, розповсюдження шкідливого програмного забезпечення, виконання DDoS-атак, розсилку спаму, крадіжку персональних даних або збір облікової інформації [3].

В умовах активної цифровізації та автоматизації виробничих процесів підприємств різного профілю зростає ризик того, що ботнет-активність спричинить значні економічні збитки. Зокрема, вона може призвести до втрати критично важливої або конфіденційної інформації, зупинки роботи окремих інформаційних систем, порушення логістичних процесів і навіть репутаційних втрат компанії. Особливо актуальною ця загроза є для великих корпорацій, банківських установ, промислових підприємств та органів державної влади.

З огляду на складність виявлення ботнетів у реальному часі та їхню здатність до швидкої зміни шаблонів поведінки, особливої актуальності набуває завдання прогнозування ботнет-активності. Ефективне прогнозування надає можливість виявляти загрозу ще до її реалізації – зменшуючи потенційні ризики для інформаційної безпеки [2].

Одним із найбільш перспективних підходів до вирішення цього завдання є застосування методів машинного навчання, зокрема регресійного аналізу, що дозволяє працювати з часовими рядами та знаходити аномальні закономірності в мережевому трафіку, які можуть вказувати на приховану ботнет-активність.

Регресійний аналіз – це метод статистичного моделювання, що полягає у визначенні залежності між змінною-ціллю (у цьому випадку – рівнем ботнет-активності) та незалежними змінними (ознаками, які впливають на неї) [1]. Серед таких ознак можуть бути:

- загальний обсяг вхідного і вихідного трафіку;
- кількість встановлених з'єднань за одиницю часу;
- частота звернень до нестандартних портів;
- тип використаного мережевого протоколу (TCP, UDP, ICMP тощо);
- географічне розташування джерела трафіку;
- повторюваність підозрілих шаблонів активності [2].

Регресійні моделі дозволяють не лише прогнозувати розвиток ситуації, але й виявляти приховані взаємозв'язки між параметрами, які людина може не побачити під час звичайного аналізу.

У сфері кібербезпеки ці моделі широко використовуються для:

- моделювання поведінки користувачів та пристроїв у мережі для виявлення аномалій;
- аналізу трафіку з метою прогнозування пікових навантажень;
- виявлення нетипових змін у поведінці системи, які можуть свідчити про приховану активність ботнетів;
- розрахунку ймовірності виникнення інцидентів у майбутньому [4].

Найчастіше використовуються наступні типи регресій:

- лінійна регресія – проста, але ефективна при стабільних і передбачуваних даних;
- поліноміальна регресія – підходить для моделювання складних, нелінійних взаємозв'язків;
- регресії з регуляризацією (Ridge, Lasso) – корисні для роботи з великими наборами ознак, де існує ризик перенавчання та мультиколінеарності [5].

Методика дослідження:

1. Збір даних. На першому етапі проводиться збір логів мережевого трафіку підприємства. Вони можуть бути отримані з систем захисту, міжмережевих екранів, роутерів або SIEM-систем. До даних зазвичай входять:

- IP-адреси джерела і призначення;
- часові мітки;
- обсяги переданих пакетів;
- використані порти та протоколи;
- кількість з'єднань та їхня тривалість;
- напрямок трафіку (вхідний або вихідний).

2. Попередня обробка. Отримані дані нормалізуються, видаляються пропуски, проводиться агрегація за часовими вікнами (наприклад, кожні 5 хвилин або 1 годину). Формуються часові ряди, а також проводиться маркування даних – визначення, яка активність є

типовою, а яка потенційно пов'язана з ботнет-діяльністю (на основі експертної оцінки або знань про інциденти в минулому).

3. Побудова моделей. У дослідженні використовуються:

- Лінійна регресія – як базовий інструмент для аналізу залежностей.
- Поліноміальна регресія – для моделювання випадків із різкими змінами навантаження.
- Ridge/Lasso-регресія – для побудови стійких моделей за умов високої варіативності.

4. Оцінка ефективності моделей. Для перевірки якості прогнозування використовуються стандартні метрики:

- MAE (середня абсолютна похибка) – показує середню різницю між прогнозом і фактичним значенням.
- RMSE (корінь середньоквадратичної похибки) – дає більше ваги великим відхиленням.
- R^2 (коефіцієнт детермінації) – демонструє, яка частка варіацій пояснюється моделлю [3].

Також проводиться тестування моделей на нових, раніше не бачених даних, щоб оцінити їхню здатність адаптуватися до змін у поведінці ботнетів.

Результати експериментів показали, що:

- лінійна регресія добре справляється в умовах стабільного трафіку, але має обмеження в умовах складних змін;
- поліноміальна регресія другого або третього ступеня краще моделює стрибкоподібні навантаження;
- регуляризовані моделі є найбільш гнучкими та стійкими до шуму й надлишкових змінних [3].

Загалом, інтеграція регресійного аналізу в системи кіберзахисту підприємств дозволяє вчасно виявляти відхилення в мережевій поведінці, що потенційно пов'язані з ботнет-мережами. Це, своєю чергою, підвищує рівень кіберстійкості та дозволяє діяти на випередження.

У майбутньому доцільним є розширення даного підходу шляхом використання глибоких нейронних мереж, зокрема LSTM (Long Short-Term Memory) або GRU (Gated Recurrent Unit). Ці моделі краще адаптовані для роботи з часовими рядами та дозволяють враховувати довгострокові залежності, контекст попередніх атак, сезонність трафіку та інші складні характеристики поведінки мереж.

Список використаних джерел:

1. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. К.: Видавнича група BHV, 2009. 608с

2. Жилін А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.

3. Захист від ботнетів. URL: https://www.eset.com/ua/support/information/entsyklopediya-zahroz/zakhyst-vid-botnetiv/?srsltid=AfmBOop5nxAw5V0fXFktltYE3qK47Cr-yXSHhIlTsDN42MTLrIt_Olsi

4. Остапов С. Е. Технології захисту інформації: навчальний посібник. Х.: Вид. ХНЕУ, 2013. 476 с

5. Ткаченко М. П., Кучеренко Є. А., Журавська І. М. Автоматизована система виявлення бот-атак на основі аналізу користувацьких профілів у соціальних мережах. Інформаційні технології та інженерія: тези доп. Всеукр. наук.-практ. конф. Миколаїв, 8–11 лютого 2022 р. Миколаїв: Чорном. нац. ун-т ім. Петра Могили, 2022. С. 28–31.

УДК 004

Макаревич С.О., здобувач
Дячук О.Ю., ст. викладач
Колощук М.С., ст. викладач
Державний університет «Житомирська політехніка»

HONEYPOT/HONEYNET У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ: СТРАТЕГІЯ ЗБОРУ ЕМПІРИЧНИХ ДАНИХ ДЛЯ ПРОГНОЗНОЇ БЕЗПЕКИ

У сучасних умовах зростання кількості кібератак та автоматизованих ботнет-кампаній корпоративні мережі перебувають у стані постійної загрози. Масові сканування, брутфорс-атаки та канали керування (Command and Control, C2) суттєво збільшують навантаження на служби безпеки. Традиційні методи, засновані на сигнатурах або статичних правилах, дедалі частіше демонструють недостатню ефективність у виявленні нових типів атак. Це зумовлює перехід від реактивної моделі захисту до прогнозної, що ґрунтується на аналізі поведінки зловмисників і закономірностей еволюції загроз.

У цьому контексті технології honeypot та honeynet виступають стратегічним елементом системи прогнозної безпеки. Вони дозволяють досліджувати реальну активність атакуючих агентів у контрольованому середовищі, формувати емпіричні бази даних і створювати моделі для передбачення загроз [1]. Їх наукова цінність полягає у можливості отримання автентичних даних про нові техніки атак та формування індикаторів компрометації (IoC), що збагачують системи виявлення (SIEM, SOAR).

Особливо актуальною є проблема нестачі якісних публічних датасетів із поведінкою ботнетів. Без них неможливе ефективне навчання алгоритмів ШІ та машинного навчання – основи адаптивних систем безпеки майбутнього [1]. Використання honeynet як контрольованого середовища здатне заповнити цю прогалину, забезпечуючи отримання реальних даних без ризику для продуктивних систем.

Концептуальна модель підходу передбачає гібридну архітектуру сенсорів. Сенсори низької взаємодії дають широку картину атакувальної активності, фіксують сканування та типові спроби вторгнення. Сенсори середнього й високого рівня взаємодії дозволяють досліджувати поведінку ботів, командні сесії, шкідливі файли та механізми C2-з'єднань [2], [3]. Отримані дані можуть бути використані для побудови поведінкових моделей виявлення загроз із застосуванням методів класифікації, машинного навчання та алгоритмів на кшталт

Random Forest, XGBoost чи LSTM, що підвищує точність прогнозної аналітики [3].

Наукова новизна підходу полягає у формалізації процесу створення репрезентативних honeynet-датасетів і методики оцінки переносності моделей між лабораторним та операційним середовищами. Важливим результатом є рекомендації щодо інтеграції даних із пасток у корпоративні системи моніторингу без істотного підвищення операційного ризику. Це створює основу для внутрішніх репозиторіїв загроз, що підсилюють аналітику в сучасних Security Operation Center (SOC).

Ключовим аспектом реалізації таких досліджень є дотримання етичних і правових вимог. Розгортання honeynet повинно супроводжуватися політикою data governance, що регламентує отримання дозволів, зберігання й анонімізацію даних та контроль вихідного трафіку для запобігання поширенню шкідливих артефактів. Практична імплементація має здійснюватися у співпраці з юридичними та кібербезпековими фахівцями, що гарантує технічну безпеку й відповідність міжнародним нормам.

Отримані результати важливі як для науки, так і для практики. Вони формують теоретичне підґрунтя розвитку поведінкової аналітики та підвищують ефективність систем моніторингу й реагування у корпоративних мережах. Honeynet як платформа прогнозного аналізу відкриває перспективи створення адаптивних систем кіберзахисту, здатних не лише реагувати на атаки, а й передбачати їх розвиток.

Дослідження підкреслює необхідність переходу до прогнозних моделей безпеки, де центральним елементом є збір та аналітика емпіричних даних. Використання honeypot/honeynet у корпоративних середовищах є науково обґрунтованим шляхом до формування нової парадигми кіберзахисту. Запропонована методологія дозволяє створювати безпечні експериментальні середовища для дослідження ботнет-активності, розвивати інструменти виявлення загроз і формувати основу для систем прогнозної безпеки наступного покоління.

Список використаних джерел:

1. Franco M., Abhishta A., Nieuwenhuis L., Joosten R. A Survey of Honeypots and Honeynets for Internet Security. arXiv:2308.10212, 2023. URL: https://arxiv.org/pdf/2108.02287

2. Fan W., Du Z., Smith-Creasey M., Fernández D. HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design // IEEE Journal on Selected Areas in Communications. 2019. Vol. 37, No. 3. P. 683–697. URL: https://arxiv.org/pdf/2402.06516

3. Yang X., Yuan J., Yang H., Kong Y., Zhang H., Zhao J. A Highly Interactive Honeypot-Based Approach to Network Threat Management // Future Internet. 2023. Vol. 15, No. 4. Article 127. URL: https://doi.org/10.3390/fi15040127

УДК 004.7

Млинський Б.М., здобувач
Дячук О.Ю., ст. викладач
Державний університет «Житомирська політехніка»

АРХІТЕКТУРА ТА ВІДМОВОСТІЙКІСТЬ СТЕКІВ CISCO CATALYST 2960-SF: АНАЛІЗ FLEXSTACK/FLEXSTACK-PLUS

Сучасні корпоративні мережі потребують високої доступності та масштабованості, що особливо важливо у сегменті рівня доступу. Комутатори Cisco Catalyst 2960-SF залишаються поширеним рішенням у державних, освітніх і корпоративних мережах, де необхідна оптимізація інфраструктурних витрат при одночасному забезпеченні відмовостійкості. Технології FlexStack і FlexStack-Plus дозволяють об'єднати кілька фізичних комутаторів у єдиний логічний пристрій з централізованою керованістю, що є актуальним для мереж зі швидким зростанням навантажень. Додаткову актуальність дослідженню надає практичний аспект – наявність зібраного стеку Cisco 2960-SF, представленного на Рисунок 1 - , що дозволяє підтвердити теоретичні положення на реальній інфраструктурі.

Рисунок 1 - Стек комутаторів Cisco Catalyst 2960-SF

Метою роботи є аналіз архітектури стекування Cisco Catalyst 2960-SF із використанням FlexStack та FlexStack-Plus, з урахуванням механізмів резервування, ролей Master, Standby та Member, особливостей передачі керування в разі відмов та поведінки стеку в топології redundant ring. Додатково виконано огляд практичного зібраного стенду для демонстрації працездатності механізмів стекування у реальних умовах експлуатації.

Технологія FlexStack забезпечує побудову єдиної логічної структури з загальною таблицею MAC-адрес та централізованою конфігурацією. Розподіл ролей Master і Standby дозволяє забезпечити безперервність керуючої площини: Standby-комутатор зберігає повнорозмірну копію стану стеку та автоматично перебирає роль Master у разі його виходу з ладу. Топологія у вигляді кільця (redundant stack ring) забезпечує транспортну відмовостійкість: при обриві одного зі стекових лінків стек продовжує функціонувати через альтернативний шлях, запобігаючи split-stack та зберігаючи логічну цілісність.

Практична частина дослідження включала аналіз роботи зібраного стеку комутаторів Cisco 2960-SF (Рисунок 1 -), що дозволило експериментально підтвердити коректність теоретичних положень щодо роботи механізмів election-процесів, синхронізації конфігурацій, актуалізації MAC-таблиці та передачі керування між Master та Standby вузлами. На практичному стенді було реалізовано кільцеву топологію стекових з'єднань (рис. 2), що забезпечило стабільність під час вимкнення окремого пристрою й підтвердило ефективність моделі резервування FlexStack.

Рисунок 2 - Кільцева топологія стеку Cisco Catalyst 2960-SF

Наукова новизна дослідження полягає у поєднанні теоретичного аналізу стекових технологій Cisco з практичною валідацією на реальному обладнанні. Це дозволило систематизувати фактори надійності стекових архітектур рівня L2 та розширити існуючі підходи до моделювання відмовостійкості стеків у корпоративних мережах. Результати мають прикладне значення для модернізації інфраструктури в організаціях, які використовують обладнання Cisco попередніх поколінь, але потребують забезпечення високої доступності без переходу на модульні шасі.

У підсумку показано, що стекування Cisco Catalyst 2960-SF на базі FlexStack та FlexStack-Plus забезпечує ефективний баланс між вартістю, масштабованістю та надійністю. Централізоване управління, логічна консолідація, резервування ролей та кільцева архітектура з'єднань дозволяють гарантувати стабільну роботу мереж навіть у разі часткових відмов компонентів. Практичне тестування підтвердило ефективність даної архітектури у реальних умовах.

Список використаних джерел:

1. Cisco Systems. Data sheet Catalyst-2960-S Series Switches. 2019. URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.pdf

2. Cisco Systems. Consolidated configuration guide for Catalyst 2960-XR Series Switches. 2021. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960xr/software/15-2_3_e/consolidated_guide/b_1523e_consolidated_2960xr_cg/b_1522e_consolidated_2960xr_cg_chapter_0110010.pdf

3. LANCOM Systems. Switch Design Guide — Redundancy Concepts. 2020. URL: https://www.lancom-systems.fr/fileadmin/download/techpaper/LANCOM-Techpaper-Switch-design-guide-redundancy-concepts.pdf

УДК 004.75

Ожго Ю. А., здобувач
Миколайчук В. В., ст. викладач
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ПОПУЛЯРНИХ CONTAINER RUNTIME

Сьогоденний процес розробки програмного забезпечення вимагає використання найсучасніших та найактуальніших технологій, методологій та підходів, що дозволяють створювати якісні та практичні рішення. Одним із таких ключових підходів є застосування контейнеризації. Контейнеризація – це метод запакування програми з усіма їй необхідними залежностями, бібліотеками та файлами конфігурації в єдину, ізольовану від навколишнього середовища сутність, яку називають контейнером[1]. Контейнери використовуються при розробці, тестуванні, доставці та розгортанні продукту і де-факто є стандартом для більшості етапів життєвого циклу ПЗ.

Середовище виконання контейнера (Container Runtime) – це програмне рішення, що реалізує стандарти OCI (Open Container Initiative) та відповідає за створення, запуск і керування контейнерами [2]. Воно забезпечує ізоляцію й контроль ресурсів на низькорівневому рівні(low-level) та керування образами й життєвим циклом на високорівневому рівні(high-level).

До найбільш поширених low-level середовищ виконання відносять [3]:

- runc – еталонна реалізація специфікації OCI Runtime Specification для запуску OCI-сумісних контейнерів у Linux. Він обробляє пакет із файловою системою та конфігурацією і використовує механізми ядра ОС, такі як namespaces та cgroups, для ізоляції процесу та управління ресурсами контейнера;
- crun – мінімалістична та високопродуктивна альтернатива runc, що також реалізує специфікації OCI. Розроблений на мові C, цей runtime забезпечує швидший запуск контейнерів і оптимізоване використання ресурсів порівняно з runc. Активно розвивається спільнотою Red Hat;
- runhcs – це розгалуження runc, створене Microsoft для запуску контейнерів на платформі Windows. Він підтримує контейнери у форматі OCI і є реалізацією OCI Runtime Specification для Windows. На відміну від runc, який працює тільки в Linux і використовує механізми ядра Linux, runhcs взаємодіє з HCS і призначений виключно для Windows-середовища;
- containerd – середовище виконання з відритим кодом, яке

підтримується на Linux і Windows та полегшує управління життєвим циклом контейнерів за допомогою API. Насправді, дане програмне забезпечення можна віднести, як до низькорівневих так і до високорівневих середовищ, за рахунок його можливостей керувати образами та життєвим циклом, проте, оскільки ми не взаємодіємо з ним безпосередньо, то його прийнято вважати низькорівневим.

До найбільш поширених high-level середовищ виконання відносять [4]:

- Docker – це платформа для роботи з контейнерами, що надає інструменти для розробки, розгортання та управління контейнеризованими застосунками. У складі платформи інтегровано containerd, який відповідає за управління контейнерними образами та виконання контейнерів. Крім того, Docker включає засоби, що забезпечують взаємодію з Kubernetes;
- Podman – це програмне забезпечення з відкритим вихідним кодом,

розроблене компанією Red Hat, яке пропонує більш безпечну модель роботи з контейнерами порівняно з оригінальною реалізацією Docker. На відміну від Docker, Podman не потребує фонової служби (демона) і дозволяє запускати контейнери без прав суперкористувача (root), забезпечуючи більш безпечне та гнучке середовище виконання;

- CRI-O – це легке та мінімалістичне середовище виконання

контейнерів з відкритим кодом, спеціально розроблене для Kubernetes. Воно реалізує стандарт CRI, дозволяючи Kubernetes запускати та керувати контейнерами відповідно до OCI стандартів, і є оптимізованою альтернативою Docker у контексті оркестрації.

Вибір container runtime залежить від потреб проєкту і є критично важливим для забезпечення ефективної, надійної та безпечної роботи контейнеризованих застосунків. Основними критеріями оцінки є сумісність зі стандартами OCI, інтеграція з оркестраторами, а також продуктивність, витрати ресурсів і рівень безпеки.

Список використаних джерел:

1. Container Runtimes Explained: Security, Types & Best Practices. URL: https://www.akamai.com/glossary/what-is-a-container.
2. What Is a Container Runtime?. URL: https://www.aquasec.com/cloud-native-academy/container-security/container-runtime/.
3. What are Container Runtimes. URL: https://www.sysdig.com/learn-cloud-native/what-are-container-runtimes.
4. Most Popular Container Runtimes. URL: https://www.cloudraft.io/blog/container-runtimes.

Секція 3
ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УДК 004.92

Тетерук Д.О., магістрантка
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ТА ОЦІНЮВАННЯ ВПЛИВУ ВИКОРИСТАННЯ ДОПОВНЕНОЇ РЕАЛЬНОСТІ НА ЕФЕКТИВНІСТЬ ОРІЄНТУВАННЯ КОРИСТУВАЧІВ У МІСЬКОМУ СЕРЕДОВИЩІ

Під час надзвичайних ситуацій у місті вирішальною стає здатність людини швидко та безпомилково знайти безпечне місце. Застосування класичних засобів навігації (плоскі карти, текстові інструкції) потребує додаткових ментальних перетворень між картографічним поданням і реальною сценою, що в умовах стресу збільшує ймовірність помилки. Доповнена реальність (AR) інтегрує навігаційні підказки безпосередньо у поле зору користувача, що підсилює ситуаційну обізнаність і зменшує когнітивне навантаження під час руху до цілі [1;3].

У роботі оцінюється вплив AR на ефективність пішохідного орієнтування у місті за показниками швидкості досягнення цілі, точності траєкторії (частота помилкових маневрів, надлишкова довжина шляху) та суб'єктивної зручності використання. Розглядаються методи візуалізації маршруту засобами AR у поєднанні з оглядовою міні-картою для збереження глобального контексту. Підхід ґрунтується на критичному аналізі наукових джерел, формуванні узгодженого набору метрик (зокрема, NASA-TLX для оцінювання ментального навантаження [2]) та проєктуванні концепції мобільного застосунку.

Запропонована концепція прототипу охоплює модулі локалізації (GPS/компас із можливістю візуальної прив'язки), прокладання маршруту вуличною мережею та просторове відображення підказок у точках прийняття рішень. Інтерфейс витримано в мінімалістичному стилі, аби не перевантажувати поле зору та знизити ментальні витрати на інтерпретацію [1].

Емпірична перевірка передбачає порівняння двох груп учасників у реальному міському кварталі. Одна рухається за AR-підказками, інша – з традиційною 2D-картою. Фіксуються час виконання завдання,

кількість навігаційних помилок, надлишкова відстань, а також суб'єктивні оцінки навантаження та зручності. Для аналізу різниць застосовуються стандартні статистичні тести (t-тест/ANOVA залежно від схеми).

Очікується статистично значуще скорочення часу досягнення цілі (орієнтовно на 10–25% залежно від маршруту) та зменшення кількості помилкових маневрів у групі з AR. Такі результати інтерпретуються як підвищення ситуаційної обізнаності та зменшення когнітивних витрат, що прямо відбивається на якості прийняття рішень на місцевості [1;3].

Практичне застосування передбачає інтеграцію AR-навігації до міських сервісів оповіщення населення та систем цивільного захисту для оперативного доступу до укриттів та інших критичних об'єктів. Серед обмежень: точність геопозиціювання, вплив умов освітлення на роботу камер і ризик візуального перевантаження. Ці чинники враховано у вимогах до інтерфейсу й плані подальших польових випробувань.

Список використаних джерел:

1. Augmented reality navigation systems / W. Narzt et al. *Universal Access in the Information Society*. 2005. Vol. 4, no. 3. P. 177–187. URL: https://doi.org/10.1007/s10209-005-0017-5 (дата звернення: 06.11.2025).

2. Hart S. G., Staveland L. E. Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. *Advances in Psychology*. 1988. P. 139–183. URL: https://doi.org/10.1016/s0166-4115(08)62386-9 (дата звернення: 06.11.2025).

3. Qiu Z., Mostafavi A., Kalantari S. Use of augmented reality in human wayfinding: a systematic review. *Virtual Reality*. 2025. Vol. 29, no. 4. URL: https://doi.org/10.1007/s10055-025-01226-w (дата звернення: 06.11.2025).

УДК 004.852

Марчук Г.В., ст. викладач
Любченко Д.В,. асистент
Державний університет «Житомирська політехніка»

ПІДВИЩЕННЯ ТОЧНОСТІ ASR ДЛЯ OOV-ЛЕКСИКИ

Розпізнавання мови (ASR) є ключовою технологією в сучасній людино-машинній взаємодії. Фреймворк Speech в iOS забезпечує доступ до потужних нейромережевих моделей, які ефективно працюють із загальновживаною лексикою, що тренована на великих мовних масивах [1]. Точність стандартних ASR-систем критично знижується при роботі з вузькоспеціалізованою лексикою, відомою як Out-of-Vocabulary (OOV) слова. Це стосується медичної термінології, назв фармацевтичних препаратів, технічного жаргону та унікальних власних назв. Недостатня точність у критично важливих галузях, як-от охорона здоров'я, може призвести до серйозних помилок, що обумовлює нагальну потребу в механізмах спеціалізації мовної моделі без повного перенавчання базового ASR-рушія.

Процес автоматичного розпізнавання мовлення (ASR) є, по суті, задачею максимізації ймовірності. Мета - знайти та вивести найбільш імовірну послідовність слів (W_{final}) за умови отриманого акустичного спостереження або звукового сигналу (O). Ця фундаментальна задача розв'язується за допомогою Теореми Баєса, яка дозволяє декомпозицію складної умовної ймовірності $P(W|O)$ на два основні, незалежно керовані, компоненти:

$$\hat{W} = \arg\max_{W} P(O|W) \cdot P(W), \qquad (1)$$

де $P(O|W)$ (Акустична модель) - оцінює ймовірність того, що саме послідовність слів W була вимовлена, призвівши до отриманого акустичного сигналу O; P(W) (Мовна модель, LM) - оцінює апріорну (попередню) ймовірність виникнення послідовності слів W у природній мові. Цей компонент відповідає за синтаксичну та семантичну коректність, виступаючи як потужний фільтр, що відсікає малоймовірні або безглузді послідовності.

Запропонований підхід інтеграції кастомних словників з явним прописом фонем є ефективним та необхідним механізмом спеціалізації ASR-систем в екосистемі Apple. Цей метод долає обмеження, притаманні базовим моделям, забезпечуючи клінічно або функціонально необхідний рівень точності розпізнавання OOV-слів. Це є критично важливим для створення надійних голосових інтерфейсів у

високоспеціалізованих галузях (охорона здоров'я, юридична сфера, технічні системи), де неточність розпізнавання є неприпустимою.

Базові мовні моделі ($P_{base}(W)$) тренуються на дуже великих масивах загальновживаного тексту. Якщо користувач вимовляє вузькоспеціалізований термін (наприклад, медичний діагноз, назва бренду, технічний термін), який не міститься у тренувальних даних базової моделі (так зване OOV – Out-Of-Vocabulary слово, W_{custom}), то ймовірність $P_{base}(W_{custom})$ буде надзвичайно низькою, часто близькою до нуля. Низька ймовірність переважає навіть сильний сигнал акустичної моделі, що призводить до помилки розпізнавання і заміни спеціалізованого слова на якесь фонетично схоже, але загальновживане слово.

Для вирішення цієї проблеми застосовується модель інтерполяції. Це процес злиття (fusion) двох мовних моделей - загальної та спеціалізованої - за допомогою зваженого середнього.

Інтерполяція коригує апріорну ймовірність P(W) саме для цільових спеціалізованих термінів. Кінцева (інтерпольована) ймовірність Pfinal(W) розраховується за формулою:

$$P_{final}(W) = (1-\lambda)P_{base}(W) + \lambda P_{custom}(W), \quad (2)$$

де $P_{base}(W)$ - ймовірність базової моделі отримана зі стандартної, великої, але неспеціалізованої мовної моделі. Для слів W_{custom} ця величина практично дорівнює 0. $P_{custom}(W)$ - ймовірність кастомної моделі, яка спеціально сконструйована і містить кастомний словник. Для цільових слів W_{custom} ця ймовірність штучно встановлюється як висока (наприклад, рівномірно розподілена для всіх слів словника). λ - коефіцієнт ваги інтерполяції, який є ключовим керуючим параметром, де $\lambda \in [0, 1]$. Якщо $\lambda = 0$, використовується лише базова модель, а якщо $\lambda = 1$, використовується лише кастомний словник. Оптимальне значення λ визначає ступінь довіри системи до спеціалізованого словника.

Завдяки інтерполяції, для спеціалізованих термінів W_{custom}, навіть невеликий, але ненульовий коефіцієнт λ призводить до значного збільшення кінцевої ймовірності $P_{final}(W_{custom})$.

Список використаних джерел:

1. Apple Developer Documentation. Speech Framework [Електронний ресурс]. 2025. URL: https://developer.apple.com/documentation/Speech (дата звернення: 30.10.2025).

УДК 004.4

Добрушин Ю.В., магістрант
Віктор А.С., PhD, доцент
Державний університет інформаційно-комунікаційних технологій

МЕТОДОЛОГІЧНІ ЗАСАДИ АВТОМАТИЗАЦІЇ ІНТЕГРАЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ СЕМАНТИЧНОГО АНАЛІЗУ

Постановка задачі. Сучасна IT-інфраструктура характеризується гетерогенністю та стрімким зростанням кількості програмних сервісів, що взаємодіють через API. Процес їх інтеграції залишається значною мірою ручним, трудомістким та схильним до помилок.

Ключовою проблемою є семантичний розрив, коли однакові за змістом сутності (наприклад, "ідентифікатор клієнта") мають різні синтаксичні назви в системах (customerId, client_id, user_number). Існуючі автоматизовані підходи, що базуються на синтаксичному порівнянні або простих онтологіях, демонструють недостатню точність та гнучкість. Це зумовлює необхідність розробки нового методу автоматизованого зіставлення (mapping) елементів API, який би спирався на глибоке розуміння їх семантичного значення.

Мета дослідження. Метою даної роботи є розробка та теоретичне обґрунтування методу автоматизованого семантичного зіставлення компонентів програмних інтерфейсів. Метод має базуватися на застосуванні сучасних моделей обробки природної мови (NLP), зокрема архітектури Transformer, для аналізу текстових описів API та створення їх векторних представлень (embeddings). Основна задача – довести, що запропонований підхід дозволяє досягти суттєво вищої точності зіставлення порівняно з існуючими аналогами.

Результати дослідження. В рамках дослідження запропоновано комплексний метод, що складається з трьох основних етапів.

Перший етап – збір та передобробка даних. Метод передбачає автоматичний парсинг стандартних специфікацій API, таких як OpenAPI (Swagger), для вилучення ключової інформації: назв кінцевих точок (endpoints), параметрів запитів, полів у тілі запиту/відповіді та їх текстових описів [1].

Другий етап – семантичне векторизування. На цьому етапі вилучені текстові описи кожного елемента API подаються на вхід попередньо навченої мовної моделі (наприклад, BERT або RoBERTa) [2]. Модель перетворює текст у багатовимірний числовий вектор (embedding), який кодує семантичне значення опису в контексті. Це є ключовим кроком,

що дозволяє перейти від синтаксичного порівняння рядків до порівняння змісту.

Третій етап – зіставлення на основі подібності. Для знаходження відповідностей між елементами двох різних API обчислюється метрика подібності між їх векторними представленнями, найчастіше – косинусна подібність [3]. Пари елементів з найвищим показником подібності вважаються семантичними відповідниками.

Згідно з аналізом сучасних досліджень, методи на основі Transformer-моделей демонструють точність (F1-score) у задачах семантичного зіставлення в діапазоні 85-94%. Це являє собою значне покращення порівняно з традиційними синтаксичними підходами (наприклад, на основі відстані Левенштейна або n-грам), ефективність яких зазвичай не перевищує 50-70% [4].

Таким чином, запропонований метод дозволяє не просто покращити, а кардинально підвищити якість автоматичної інтеграції, знижуючи кількість помилок, що виникають через семантичну неоднозначність.

Висновки та перспективи. Запропонований метод створює теоретичну основу для розробки нового покоління інтелектуальних систем інтеграції ПЗ. Його головна перевага полягає у здатності розуміти функціональне призначення елементів API, а не лише їх назви. Це дозволяє значно прискорити процес розробки, знизити кількість помилок та зменшити вимоги до кваліфікації інтеграторів.

Подальші дослідження можуть бути спрямовані на практичну реалізацію методу у вигляді програмного прототипу, його тестування на широкому наборі реальних API та розширення для аналізу не лише текстових описів, а й прикладів коду з документації для збільшення успішних варіантів зіставлення endpoints при інтеграції.

Список використаних джерел:

1. OpenAPI Initiative. (2021). OpenAPI Specification v3.0.3. Retrieved from: https://spec.openapis.org/oas/v3.0.3

2. Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, 1, 4171–4186.

3. Jurafsky, D., & Martin, J. H. (2023). Speech and Language Processing (3rd ed. draft). Prentice Hall.

4. Mudgal, S., et al. (2018). Deep learning for entity matching: A design space exploration. Proceedings of the 2018 International Conference on Management of Data (SIGMOD '18), 19–34.

УДК 004.4

Фоменко В А., здобувач
Савіцький Р.С., аспірант, ст. викладач
Державний університет «Житомирська політехніка»

АВТОМАТИЗОВАНИЙ ПОШУК ПОМИЛОК В УКРАЇНСЬКОМУ ТЕКСТІ З ВИКОРИСТАННЯМ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ

Якість текстового контенту українською мовою стає все важливішою в умовах цифровізації суспільства. Дослідження 2023 року показало, що близько 67% україномовного контенту в інтернеті містить орфографічні, пунктуаційні або граматичні помилки [1]. Українська мова зі своєю складною морфологією, системою відмінків та узгодження слів створює багато можливостей для виникнення помилок, які традиційні системи перевірки не можуть ефективно виявляти.

Словникові методи є найпростішим підходом до перевірки текстів. Вони порівнюють кожне слово зі списком правильних слів, але мають критичні обмеження для української мови.

Основна проблема використання словників у валідації тексту це те, що словники не розуміють контексту речення. Візьмемо для прикладу речення "Він одів пальто". Слово "одів" існує у словнику і є правильною формою дієслова "одіти". Словникова система визнає таке речення правильним. Але правила української мови вимагають тут використання "одягнув" (коли хтось одягає щось на себе), а не "одів" (коли хтось одягає когось іншого). Словник не може цього побачити, тому що аналізує слова окремо одне від одного [2].

Слова "адресат" і "адресант", "абонент" і "абонемент" всі є правильними. Словникова система не може визначити, яке з них підходить у конкретному контексті. Слово "замок" може означати споруду або пристрій для зачинення дверей, але словник не знає, який варіант потрібен у конкретному реченні.

Словоформи створюють додаткові труднощі десятки різних форм. Іменник змінюється за семи відмінками і числами, дієслово змінюється за особами, числами, часами та способами. Для української мови це означає мільйони словоформ, які практично неможливо підтримувати в актуальному стані.

Словникові методи можуть виявити тільки найпримітивніші помилки, коли слово взагалі не існує. Вони безсилі перед контекстними помилками, проблемами узгодження та паронімами, які становлять більшість помилок у реальних текстах.

У роботі використовується модель Pravopysnyk/best-unlp, яку розробили спеціально для української мови. Модель базується на архітектурі Transformers і її навчили на великих обсягах українських текстів. На відміну від словникових методів, модель аналізує весь контекст речення та розуміє зв'язки між словами.

Механізм уваги дозволяє моделі одночасно враховувати всі слова у реченні та їхні взаємозв'язки. Коли модель аналізує слово "одів" у реченні "Він одів пальто", вона бачить, що людина одягає щось на себе, а значить потрібне дієслово "одягнув [3].

Модель Pravopysnyk/best-unlp навчили розпізнавати типові помилки в українській мові. Це неправильне вживання дієслів одіти та одягнути, помилки в узгодженні прикметників з іменниками, неправильне відмінювання, порушення керування дієслів та пунктуаційні помилки. Модель не просто шукає слова у словнику, вона розуміє граматичну структуру та семантику тексту.

Система виявляє орфографічні помилки (друкарські помилки та порушення правил написання), граматичні помилки (неправильне узгодження слів за родом, числом і відмінком), пунктуаційні помилки (неправильне використання розділових знаків) та лексичні помилки (невідповідне використання слів і плутанина паронімів).

Ефективний пошук помилок в українському тексті неможливий без використання штучного інтелекту. Словникові методи застаріли і не відповідають вимогам сучасної обробки природної мови. Тільки моделі на основі Transformers можуть розуміти контекст та складні граматичні залежності української мови, що забезпечує якісне виявлення помилок у текстах.

Список використаних джерел:

1. Romanyshyn M., Chaplynskyi D. Ukrainian Language Corpus and Error Detection: Current State and Perspectives. Proceedings of the 4th Ukrainian NLP Workshop, 2023. DOI: 10.18653/v1/2023.unlp-1.12

2. Sang-Bum Kim, Hee-Soo Hahn, Changki Lee. Context-sensitive spelling correction using Google Web 1T 5-gram information. IEEE Transactions on Audio, Speech, and Language Processing, 2010. DOI: 10.1109/ICIG.2009.39

3. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I.. Attention is All you Need. Neural Information Processing Systems, 30, 5998–6008? 2017. URL: https://proceedings.neurips.cc/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf

УДК 004.7

Гольцев К.О., здобувач
Савіцький Р.С., аспірант, ст. викладач
Державний університет «Житомирська політехніка»

РОЗРОБКА ФІТНЕС-ПЛАТФОРМ НА ОСНОВІ NEXT.JS

Сучасні вебдодатки у сфері фітнесу вимагають поєднання високої швидкодії, інтерактивності та ефективної SEO-оптимізації. Ці характеристики особливо важливі для платформ, що поєднують публічні сторінки (маркетплейс тренерів, профілі, блог) та приватний функціонал такий як, особисті кабінети користувачів, тренувальні програми й чат у реальному часі.

Оптимальним інструментом для реалізації таких рішень є Next.js – фреймворк на основі React, який підтримує кілька стратегій рендерингу, зокрема Server-Side Rendering (SSR), Static Site Generation (SSG) та Client-Side Rendering (CSR) [1]. Next.js дозволяє об'єднати переваги серверних і клієнтських технологій у межах одного середовища. Статична генерація (SSG) застосовується для публічних сторінок, де критично важливими є швидкість завантаження та SEO. Процеси генерації сторінок різними методами представлені на рисунку 1.

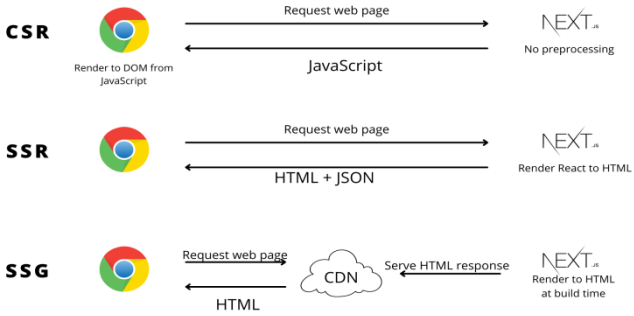


Рисунок 1 – Процеси генерації сторінок відповідними методами

Завдяки SSG контент генерується під час збірки, а користувач отримує HTML-сторінку, що суттєво зменшує час рендерингу. Серверний рендеринг використовується для сторінок із динамічними даними, SSR забезпечує актуальність інформації при кожному запиті, водночас підтримуючи високу індексацію пошуковими системами. CSR або SPA-підхід застосовується в особистому кабінеті користувача, де важлива плавність взаємодії без перезавантажень сторінок [2].

Фронтенд, побудований на Next.js, який легко інтегрується з бекендом, розробленим на ASP.NET Core Web API, через REST або GraphQL-запити [3]. Це дозволяє ефективно обмінюватися даними з базою PostgreSQL, що керується через ORM Entity Framework Core. Для підтримки функціоналу у реальному часі застосовується SignalR, який відповідає за миттєву передачу повідомлень між тренером і клієнтом. Середовище Next.js також підтримує інфраструктурну гнучкість, зокрема застосунок легко контейнеризується за допомогою Docker і розгортається на Vercel або Azure, забезпечуючи стабільність і масштабованість.

Використання Next.js як основи технологічного стеку для фітнес-додатків дозволяє поєднати швидкість статичних сайтів, динамічність сучасних SPA і SEO-оптимізацію серверного рендерингу. Такий підхід формує гнучку архітектуру, придатну для розширення функціональності, зокрема інтеграції платіжних систем, push-сповіщень або хмарних сховищ медіа.

Next.js демонстру ефективність у якості ядра комплексних платформ, орієнтованих на користувацький досвід та продуктивність.

Список використаних джерел:

1. Next.js Official Documentation. Rendering: Server Components and Client Components. URL: https://nextjs.org/docs/app/building-your-application/rendering/server-components.

2. Bhardwaj A. What the heck is SSG — Static site generation explained with Next.js URL: https://www.theanshuman.dev/articles/what-the-heck-is-ssg-static-site-generation-explained-with-nextjs-5cja.

3. Microsoft Documentation. Overview of ASP.NET Core. URL: https://learn.microsoft.com/en-us/aspnet/core/introduction-to-aspnet-core.

УДК 004.4: 004.94: 159.9

Кожухівський В.О., здобувач
Марчук Г.В., ст. викладач
Державний університет «Житомирська політехніка»

РОЗРОБКА КРОСПЛАТФОРМОВИХ СИСТЕМ ПОВЕДІНКОВОЇ КОРЕКЦІЇ З МОДУЛЕМ ГЕЙМІФІКАЦІЇ

В епоху інформаційного суспільства та поширення цифрової залежності (Digital Addiction) актуалізується задача розробки програмних інструментів, спрямованих на відновлення нейрохімічного гомеостазу користувачів, зокрема дофамінового балансу. Необхідність подолання цієї проблеми вимагає застосування не лише психологічних залучень, але й технологічно обґрунтованих рішень для стимулювання усвідомленої поведінки та закріплення адаптивних патернів [1, 2].

Метою роботи є розробка програмного комплексу, що функціонально поєднує трекінг звичок із модулем гейміфікації, спрямованим на перенаправлення системи винагороди мозку від миттєвої стимуляції до довгострокових позитивних дій.

Для реалізації бізнес-логіки обрано ASP.NET Core (C#). Вибір обґрунтований високою продуктивністю та підтримкою строго типізованої мови, що є критичним для забезпечення надійності та безпеки RESTful API при обробці конфіденційних даних користувачів та їхнього прогресу.

Ключовою архітектурною перевагою є колоборація між ASP.NET Core та клієнтським фреймворком Avalonia, що дозволяє повторне використання коду, створення спільних бібліотек для об'єктів передачі даних та оптимізація процесу розробки шляхом використання єдиної мови та екосистеми. Також обрано кросплатформовий UI-фреймворк Avalonia (з фокусом на Android). На відміну від .NET MAUI (що використовує нативні контролі), Avalonia застосовує власний механізм рендерингу (на базі Skia). Це гарантує 100% ідентичність UI на різних пристроях, що є важливим для забезпечення прогнозованого та контрольованого користувацького досвіду, необхідного для поведінкової корекції. Основною СУБД обрано PostgreSQL. Пріоритет надано об'єктно-реляційній моделі та повній ACID-відповідності, що є необхідною умовою для забезпечення цілісності даних прогресу користувача (стрики, досягнення). А використання розширеного типу даних JSONB у PostgreSQL дозволяє зберігати гнучкі структури (налаштування гейміфікації, кастомні поля звичок) в рамках реляційної моделі, поєднуючи надійність реляційного підходу з гнучкістю документо-орієнтованих систем. Для клієнтської частини обрано

патерн Model-View-ViewModel (MVVM), який є стандартом для Avalonia. MVVM забезпечує чітке розділення обов'язків (Separation of Concerns), що спрощує юніт-тестування логіки стану (ViewModel) та дозволяє незалежну роботу над дизайном (View).

У ядрі додатку реалізовано модель, спрямовану на посилення позитивного підкріплення корисних дій. Модель включає Streaks, це функція підрахунку $S(t)=S(t-1)+1$, якщо умова виконання звички виконана, інакше $S(t)=0$. Нарахування балів досвіду, де складність звички та послідовність виконання визначають швидкість прогресу користувача.

На сервері виділяється окремий «Gamification Service», що централізовано керує логікою досягнень (Achievements) та нарахуванням балів, що забезпечує атомарність та незмінність ключових ігрових механік.

Для підтримки високої продуктивності при масштабуванні та мінімізації навантаження на PostgreSQL вводиться рівень розподіленого кешування. Як зовнішній, розподілений кеш обрано Redis. На відміну від вбудованого кешу в пам'яті (In-Memory Cache), Redis гарантує узгодженість кешу при горизонтальному масштабуванні серверної частини (багаторазових екземплярах ASP.NET Core). Redis буде використовуватися не лише для кешування даних, що рідко змінюються (профілі, налаштування), але й для реалізації складних структур даних (наприклад, списків або множин) для динамічних лідербордів гейміфікації.

Запропонована архітектура застосунку базується на стратегічному виборі уніфікованого C#/.NET стеку, що забезпечує високу продуктивність, надійність та спрощення розробки. Комбінація ASP.NET Core для обробки бізнес-логіки, PostgreSQL для гарантії цілісності даних, Avalonia для контрольованого UI та інтеграція потужної гейміфікації Duolingo-типу створює необхідний технологічний фундамент для розробки ефективного інструменту, спрямованого на вирішення актуальної проблеми дофамінової дисрегуляції.

Список використаних джерел:

1. Lam, H., Harcourt, M. Digital Addiction in Organizations: Challenges and Policy Implications. *Employ Respons Rights.* 2024, Vol. 36, p.519–533. https://doi.org/10.1007/s10672-024-09493-6.

2. Prevalence and factors associated with digital addiction among students taking university entrance tests: a GIS-based study. /Al-Mamun, F. *et al. BMC Psychiatry.* 2024, Vol.24, p.322. https://doi.org/10.1186/s12888-024-05737-9.

УДК 004:339.9

Ячменьова С.О. студентка,
Коротун О.В., к.пед.н., доцент
Державний університет «Житомирська політехніка»

ВИЗНАЧЕННЯ КЛЮЧОВИХ IT-ПРОФЕСІЙ ЗА ДОПОМОГОЮ АНАЛІЗУ ДАНИХ

В останні роки швидкість технологічного прогресу та цифрова трансформація економік по всьому світу змінюють ринок праці, зокрема у секторі інформаційних технологій (IT). Зростаючий попит на кваліфікованих IT-фахівців вимагає від освітніх закладів, державних органів та самих працівників точного розуміння того, які саме професії є найбільш затребуваними та мають найбільший потенціал для зростання у найближчому майбутньому. Традиційні методи прогнозування ринку праці часто відстають від динаміки змін, що підкреслює необхідність використання сучасних підходів.

Набір даних для дослідження складається виключно з агрегованих даних про вакансії (проєкти) у сфері веб-розробки та IT, зібраних з міжнародної фриланс-платформи Upwork. Цей масив даних охоплює часовий проміжок за останні кілька місяців, відображаючи стан глобального ринку фрилансу. Кожен запис містить важливі неструктуровані та напівструктуровані атрибути, такі як точна назва проєкту/посади ("Senior Python Developer", "UX/UI Designer"), детальний опис проєкту (необхідні технічні та м'які навички), заявлений тип оплати (фіксована ціна чи погодинна ставка з діапазоном), а також географічне розташування клієнта та час публікації

Визначимо десять найбільш затребуваних професій на глобальному фриланс-ринку та зробимо візуалізацію за допомогою бібліотек Python (рис.1).

Абсолютними лідерами попиту є Front-End та Full-Stack програмісти, що підкреслює критичну потребу в фахівцях, здатних створювати клієнтську і серверну частини веб-застосувань. Значний сегмент - 514 вакансій, займають WordPress розробники, що відображає високу потребу у розробці та підтримці сайтів на цій популярній CMS. До переліку найбільш затребуваних увійшли UX/UI дизайнери, дата-аналітики, розробники мобільних застосунків, DevOps інженери та QA спеціалісти.

Визначено, що до топ-10 країн, які є основними джерелами попиту (замовників) на Web- та IT-послуги на платформі Upwork, увійшли Сполучені Штати Америки, Велика Британія, Канада, Австралія та інші економічно розвинені країни Західної Європи та Азії

(за кількістю опублікованих вакансій за останні кілька місяців).

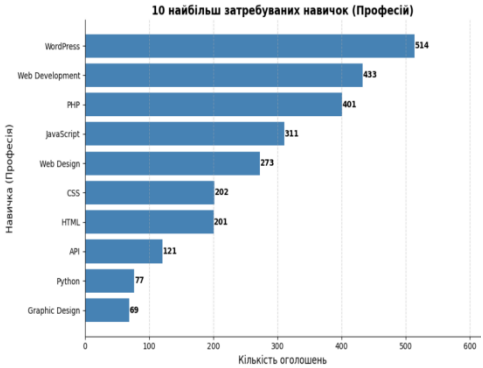


Рисунок 1 – Затребувані професії на глобальному фриланс-ринку

Це вказує на те, що попит на фриланс значною мірою корелює з обсягом та рівнем розвитку цифрової економіки у цих регіонах.

Що стосується вартості підписки на роботу, то для фрилансерів на Upwork застосовується система "Connects" - внутрішньої валюти, необхідної для подачі заявок на проекти. Реєстрація на платформі є безкоштовною, для активної роботи необхідне придбання Connects (базовий пакет коштує $0.15 за один Connect, подача заявки на одну вакансію вимагає від 2 до 6 Connects).

Отже, проведений аналіз даних з Upwork за останні кілька місяців підтверджує, що аналіз даних є ефективним інструментом для об'єктивного визначення затребуваних IT-професій у контексті світової гіг-економіки. Результати дослідження виявили домінування ролей, пов'язаних із Full-Stack та Front-End розробкою, високий і стабільний попит на WordPress Developers та UX/UI Designers, що підкреслює пріоритет клієнтів на створення якісних, функціональних та естетично привабливих веб-рішень. Ключовими центрами попиту є економічно розвинені країни, насамперед США, що корелює з їхньою лідируючою позицією у цифровій трансформації. Таким чином, успішна кар'єра в сучасному IT-секторі вимагає від фахівців не лише глибоких технічних знань, але й готовності до швидкої адаптації до трендів фрилансу та розуміння глобальної конкуренції за найбільш оплачувані проекти, що вимагають інвестицій у внутрішню валюту платформи.

Список використаної літератури:

1. World Economic Forum. The Future of Jobs Report. 2023. URL: https://www.weforum.org/publications/ (дата звернення: 11.11.2025).

УДК:004.67

Бичак К. А., магістрант
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ МЕТОДІВ І АЛГОРИТМІВ ДЛЯ СТВОРЕННЯ АВТОМАТИЗОВАНИХ РЕКОМЕНДАЦІЙНИХ СИСТЕМ

У сучасних інформаційних системах дедалі більшого значення набувають інтелектуальні технології, здатні адаптуватися до потреб користувача. Одним із рішень у цьому напрямі є автоматизовані рекомендаційні системи, які формують персоналізовані пропозиції на основі аналізу поведінкових даних. Проте постає проблема, яким способом формувати рекомендації, щоб забезпечити найбільшу ефективність взаємодії користувача з додатками.

Згідно з аналізом літературних джерел, існує три типи фільтрації рекомендаційних систем: контентна, колаборативна та гібридна [1].

При контентній фільтрації рекомендації формуються на основі раніше переглянутого користувачем контенту. Недоліком є те, що популярний чи якісний контент не рекомендується, оскільки вподобання інших користувачів не враховуються.

Колаборативна фільтрація, на відміну від контентної, формує рекомендації, засновані на моделі поведінки інших користувачів, що дозволяє усунути недоліки попереднього підходу. Але є проблема «холодного старту»: якщо користувачів дуже мало і вони ще не встигли надати достатньо інформації, рекомендації не є ефективними.

Гібридні методи фільтрації поєднують підходи та нейтралізують недоліки колаборативної та контентної фільтрацій. Єдиними проблемами можуть бути складність розробки та підтримки таких систем.

Крім проблем, які виникають в процесі формування автоматизованих рекомендацій, є ще проблеми збору і обробки даних. Згідно з одним із методів обробки даних, описаного в попередніх дослідженнях [2], для початку потрібно виокремити необхідні атрибути та значення об’єктів. Далі виконується процедура нормалізації даних і обчислення міри схожості між об’єктами, наприклад, за допомогою Евклідової відстані. Якщо міра схожості достатньо велика, то об’єкт рекомендується користувачу. Цей метод є найпростішим і достатньо ефективним для таких додатків, наприклад, як інтернет-магазини, де є не так багато різноманітних характеристик, які можуть вплинути на вибір користувача. Проте для складніших систем, де враховуються не

тільки характеристики об’єктів, а й складна поведінка користувача, цього недостатньо.

Для об’єктів, які складаються не тільки з текстової інформації, наприклад музика чи відео, доцільно використовувати технології штучного інтелекту (ШІ). У музичних додатках, наприклад Spotify чи YouTube Music, рекомендації формуються не лише на основі інформації про автора чи жанру, які вказані напряму, а й ритмічності, енергічності та інших характеристик самої пісні, яка записана у файлі [3]. Автори [4] вважають, що застосування ШІ може бути набагато ефективнішим за традиційні методи, оскільки може враховувати комплексні дані: поведінку користувача, динаміку вподобань, мультимедійні характеристики, поєднання метрик тощо.

У результаті проведеного аналізу встановлено, що ефективність автоматизованих рекомендаційних систем значною мірою залежить від правильного вибору методу фільтрації та алгоритмів обробки даних. Враховуючи переваги та недоліки різних методів фільтрації рекомендаційних систем, найбільш перспективним напрямом є застосування **гібридних підходів**, які забезпечують гнучкість і точність рекомендацій. Крім того, використання алгоритмів машинного навчання та штучного інтелекту дозволяє підвищити якість аналізу поведінкових даних, особливо у випадках із мультимедійним контентом. Отже, подальші дослідження доцільно спрямувати на розроблення **інтелектуальних гібридних моделей**, здатних адаптивно вдосконалювати свої рекомендації відповідно до змін у поведінці користувачів.

Список використаної літератури:

1. Парфененко Ю. В., Ковтун А. А., Вербицька А. А. Рекомендаційна інформаційна система для пошуку відеоматеріалів. Вісник КрНУ імені Михайла Остроградського. Випуск 5/2019 (118). URL: https://visnikkrnu.kdu.edu.ua/statti/2019_5_2019-5-97-102.pdf

2. Чередніченко О.Ю., Янголенко О.В., Іващенко О.В., Матвєєв О.М. Моделі формування рекомендацій у інтелектуальних системах електронної комерції. Системи обробки інформації. 2020. № 1(160). С. 32-39. https://doi.org/10.30748/soi.2020.160.04.

3. Косинський О. О. Програмна система рекомендацій музики на основі вподобань групи користувачів. / О. О. Косинський ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2024. – 64 с.

4. Zhang Q., Lu J., Jin Y. Artificial intelligence in recommender systems. *Complex & Intelligent Systems.* – 2021. – Vol. 7, No. 3. – P. 1479–1511. – DOI: 10.1007/s40747-020-00212-w

УДК 004.421

Яковенко Д.В., магістрант
Коротун О.В., к.пед.н., доцент
Державний університет «Житомирська політехніка»

ОПТИМІЗАЦІЯ ШВИДКОДІЇ ІНТЕРНЕТ-МАГАЗИНУ ЗАСОБАМИ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ТА СУЧАСНИХ ПІДХОДІВ ДО КЕШУВАННЯ

Швидкодія веб-ресурсів є одним із ключових факторів успішної роботи інтернет-магазинів у сучасних умовах високої конкуренції. Зростання кількості користувачів, збільшення асортименту товарів та ускладнення внутрішніх бізнес-процесів створюють значне навантаження на серверну інфраструктуру. Затримки в завантаженні сторінок, нестабільність роботи сервера та низька пропускна здатність можуть призвести до зменшення продажів і відтоку клієнтів, тому оптимізація продуктивності є одним із найважливіших технічних завдань для e-commerce платформ.

Одним із ефективних підходів до підвищення продуктивності є впровадження мікросервісної архітектури, яка передбачає поділ системи на окремі незалежні компоненти. Кожен мікросервіс відповідає за конкретний функціональний модуль: авторизацію, каталог товарів, обробку замовлень, роботу з кошиком тощо. Така архітектура дозволяє масштабувати частини системи, які зазнають найбільшого навантаження, замість дублювання всієї системи. Це забезпечує ефективне використання ресурсів, підвищує відмово стійкість та пришвидшує час реакції на користувацькі запити. Крім того, мікросервіси дають змогу застосовувати різні технологічні стеки для окремих модулів, що позитивно впливає на гнучкість системи та її здатність до розвитку.

Автори [1] зазначають, що правильне поєднання клієнтського та серверного кешування дозволяє досягти оптимального балансу між швидкістю завантаження, актуальністю контенту та навантаженням на інфраструктуру. Використання сучасних механізмів кешування є необхідною складовою розробки продуктивних і надійних прогресивних вебзастосунків. Тому другим важливим напрямом оптимізації є використання механізмів кешування, що дозволяє значно зменшити кількість звернень до бази даних та логічних обчислень. Залежно від структури інтернет-магазину можуть застосовуватися такі види кешування: *кешування статичних ресурсів через* C*ontent Delivery Network (CDN)* зберігає копії статичних файлів на географічно розподілених серверах, щоб швидше доставляти їх кінцевим користувачам; *кешування результатів запитів до бази даних* – це тимчасове зберігання результатів частих або складних SQL-запитів у

швидкій пам'яті, щоб уникнути повторного звернення до бази даних і зменшити її навантаження; *кешування результатів рендерингу сторінок* – готова HTML-структура або частини сторінки, які не часто змінюються, зберігаються у кеші, щоб не виконувати повний процес генерації сторінки при кожному запиті; *кешування проміжних обчислень* – результати тривалих або ресурсомістких обчислювальних операцій зберігаються у пам'яті для повторного використання, що значно прискорює загальну продуктивність програми.

Використання Redis або Memcached суттєво підвищує швидкість обробки даних, оскільки інформація зберігається в оперативній пам’яті й доступ до неї здійснюється значно швидше, ніж при роботі зі звичайною базою даних. Redis підтримує складні структури даних, тому підходить для кешування динамічних об’єктів, тоді як Memcached ефективний для простих ключ-значень. CDN додатково зменшує затримки, розміщуючи статичні ресурси на серверах, максимально наближених до користувача. Це розвантажує основну інфраструктуру й забезпечує стабільну роботу платформи за різких стрибків трафіку.

Поєднання мікросервісної архітектури з ефективним кешуванням дозволяє комплексно підвищити продуктивність всієї системи. Мікросервіси розподіляють навантаження між окремими модулями, усуваючи вузькі місця, а кешування зменшує кількість повторних звернень до бази даних. Це сприяє скороченню часу відповіді платформи на 30–70 % і забезпечує стабільність роботи під час пікових навантажень, а також робить систему більш передбачуваною, масштабованою, стійкою до перевантажень. Отже, таке поєднання створює надійну основу для побудови швидких і масштабованих інтернет-магазинів. Забезпечує високу продуктивність, стійкість до «стресу», здатність системи стабільно працювати в умовах зростання навантаження. У результаті інтернет-платформа швидше реагує на дії користувачів. підтримує комфортний рівень взаємодії, що є важливим для конкурентоспроможності сучасної електронної комерції.

Список використаних джерел:

1. Базиволяк М.І., Шмигер Г. П. Порівняльний аналіз механізмів кешування в прогресивних вебзастосунках. редакційний комітет. Сучасні цифрові технології та інноваційні методики навчання: досвід, тенденції, перспективи: матеріали XV Міжнародної науково-практичної інтернет-конференції, м. Тернопіль, 10 квітня, 2025 р. Тернопіль : ТНПУ ім. Володимира Гнатюка, 2025. С. 132-136.

УДК 004.738.5

Яковенко Д.В., магістрант
Коротун О.В., к.пед.н., доцент
Державний університет «Житомирська політехніка»

ПОВЕДІНКОВІ МЕТРИКИ ЯК ІНСТРУМЕНТ ОПТИМІЗАЦІЇ НАВІГАЦІЇ ТА СТРУКТУРИ ІНТЕРНЕТ-МАГАЗИНУ

Покращення взаємодії користувача з інтернет-магазином є ключовим чинником збільшення конверсії та утримання клієнтів. Ефективність навігації, логічна структура каталогу та зручність основних елементів інтерфейсу визначають, наскільки швидко та легко користувач може знайти потрібний товар і здійснити покупку. Аналіз поведінкових метрик дозволяє визначити «вузькі місця» у структурі сайту, які уповільнюють або ускладнюють процес взаємодії.

Детальний огляд сучасних моделей для оцінки і покращення інтерфейсів додатків для аналізу поведінкових даних користувачів наведено у статті [1]. До ключових поведінкових метрик належать: теплові карти активності, що демонструють області найбільшої концентрації натисків; показники тривалості перегляду сторінок; кліковіпатерни, які відображають пошукові наміри; дані систем веб-аналітики, що дозволяють оцінювати рівень взаємодії з елементами інтерфейсу. Використання інструментів Google Analytics, Hotjar, PiwikPRO, дає змогу побачити поведінку аудиторії, виявити приховані бар'єри у взаємодії, визначити фактори, що впливають на готовність користувачів продовжувати виконання дій на сайті. На основі зібраної інформації можна обґрунтовано приймати рішення щодо покращення структури інтернет-магазину. Наприклад, дані про маршрути руху користувачів, теплові карти кліків та рівень взаємодії з окремими елементами інтерфейсу дозволяють визначити ділянки, які користувачі сприймають як незрозумілі або перевантажені. Це дає змогу змінювати структуру каталогу, видимість та ієрархію товарних категорій, а також скорочувати кількість кроків між основними сторінками.

Отже, аналіз поведінкових метрик виступає одним із результативних методів оптимізації інтерфейсу інтернет-магазину, оскільки базується на реальних діях та потребах користувачів.

Список використаних джерел:

1. Новіков Ю.Л, Гамор І.М., Поперешняк С.В. Огляд моделей та алгоритмів оптимізації інтерфейсів додатків на основі поведінкових даних користувачів. Вісник Херсонського національного технічного університету, №3(90), 2024. С. 251-258.

УДК 004.7

Носов Є.Д., магістрант
Шушура О.М., д.т.н., професор
Соломаха С.А., к.е.н., доцент
Державний університет інформаційно-комунікаційних технологій

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ УПРАВЛІННЯ РЕСУРСАМИ ІНФОРМАЦІЙНИХ СИСТЕМ У ХМАРНИХ ТЕХНОЛОГІЯХ

Стрімкий розвиток цифровізації, зростання обсягів даних і масштабне впровадження хмарних сервісів призвели до того, що більшість сучасних інформаційних систем функціонують у гнучких, динамічних, розподілених середовищах. Хмарні технології дозволяють ефективно використовувати обчислювальні ресурси, забезпечувати масштабованість, високу доступність та економію витрат. Стандартні механізми масштабування часто виявляються недостатньо гнучкими, що призводить до надмірного споживання ресурсів або, навпаки, до нестачі продуктивності. У зв'язку з цим актуальним стає застосування інтелектуальних методів керування ресурсами, включаючи машинне навчання, предиктивну аналітику та адаптивні моделі, здатні оптимізувати роботу хмарних систем у режимі реального часу [1].

Постановка задачі. Основною проблемою є забезпечення ефективного управління обчислювальними, мережевими та сховищними ресурсами інформаційних систем, що працюють у динамічних хмарних середовищах. Нерівномірність навантаження, вимоги до продуктивності та інтеграція механізмів безпеки ускладнюють підтримання стабільної роботи систем. Тому необхідно дослідити й розробити інтелектуальні методи, здатні прогнозувати потребу в ресурсах та оптимізувати їх розподіл у режимі реального часу.

Мета дослідження. Метою дослідження є обґрунтування та розробка інтелектуальних підходів до управління ресурсами інформаційних систем у хмарних середовищах на основі предиктивних моделей і машинного навчання.

Для досягнення мети необхідно вирішити такі завдання:

- проаналізувати сучасні методи управління ресурсами в хмарних інформаційних системах та визначити їхні обмеження [2];
- дослідити можливості застосування машинного навчання та інтелектуальних алгоритмів для прогнозування навантаження й прийняття рішень щодо масштабування [3; 4];

– розробити узагальнену модель адаптивного управління ресурсами з урахуванням динамічних характеристик хмарного середовища;
– оцінити ефективність застосування інтелектуальних методів порівняно зі статичними та евристичними моделями.

Результати дослідження. Ефективне управління ресурсами у хмарних середовищах неможливе без комплексного моніторингу показників продуктивності - використання CPU, оперативної пам'яті, дискових операцій, мережевої активності та затримок. На основі результатів аналізу встановлено, що класичні методи масштабування, реалізовані у платформах на зразок Kubernetes, здебільшого орієнтуються на порогові значення та не враховують складних залежностей між навантаженням і споживанням ресурсів. У ході дослідження було розроблено узагальнену схему інтелектуальної системи управління ресурсами, що включає модулі моніторингу, аналітики, предиктивного моделювання та оптимізації.

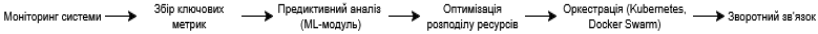


Рис. 1 – Схематична модель управління ресурсами

Запропонована модель дозволяє динамічно адаптуватися до змін навколишнього середовища та забезпечити підвищення ефективності роботи системи в цілому. Такі підходи суттєво покращують продуктивність інформаційних систем та забезпечують стабільність роботи у різноманітних умовах навантаження.

Висновки та перспективи. Таким чином, застосування інтелектуальних методів управління ресурсами у хмарних інформаційних системах є одним із найбільш перспективних напрямів розвитку сучасних інформаційних технологій. Предиктивні моделі, алгоритми машинного навчання та автоматизовані платформи оркестрації дозволяють значно підвищити ефективність, продуктивність і стабільність функціонування хмарних сервісів.

Список використаних джерел:

1. Mell P., Grance T. The NIST Definition of Cloud Computing. NIST Special Publication 800-145, 2011.
2. Kumar P., Singh S. Resource Management in Cloud Computing: Review and Future Directions. Journal of Cloud Computing, 2023.
3. Kubernetes Documentation. Kubernetes: Automated Container Orchestration. Режим доступу: https://kubernetes.io
4. Zhao Y. et al. Machine Learning-Based Resource Allocation in Cloud Environments. IEEE Access, 2022.

УДК 004.8

Лук'яненко А.А., здобувач
Українець М.О., асистент
Державний університет «Житомирська політехніка»

ДОЦІЛЬНІСТЬ ІНТЕГРАЦІЇ ШІ-АГЕНТА У ВЕБ-ПЛАТФОРМУ КУЛІНАРНИХ РЕЦЕПТІВ

Більшість українських кулінарних сайтів покладаються на класичні механізми взаємодії: статичні категорії, ручні фільтри та поверхневий пошук за ключовими словами. У таких системах користувач витрачає значні зусилля на відбір потрібного йому рецепта, його адаптацію під свої потреби (наприклад дієти чи алергії) та пошук відповідей на супутні питання. Протиріччя має місце між вимогами до адаптивності веб-платформ до потреб користувачів та наявними підходами до організації роботи веб-платформ кулінарних рецептів. Перспективним вирішенням є інтеграція штучного інтелекту (ШІ), а саме ШІ-агента для підвищення ефективності взаємодії з вмістом веб-платформи.

Метою дослідження є обґрунтування доцільності інтеграції ШІ-агента у веб-платформу кулінарних рецептів.

Інтеграція ШІ дає можливість суттєво змінити характер взаємодії, від роботи з користувацьким інтерфейсом до імітації спілкування з розумним помічником, що відповідає сучасним підходам до UX, які вже застосовуються в галузі програмування, наприклад, контекстний помічник у Cursor або GitHub Copilot змінюють сам спосіб роботи користувача з середовищем розробки [1].

Однак у противагу такому підходу, більшість сучасних кулінарних веб-платформ досі покладаються на традиційну модель взаємодії, де користувач має самостійно перетворити свій намір в послідовність взаємодій з користувацьким інтерфейсом. Через це, ускладняється передача контексту, в якому знаходиться користувач, до системи, що унеможливлює адаптацію до конкретних умов. Крім того, традиційні веб-платформи не дозволяють адаптувати наявні рецепти до специфічних потреб користувача, але це є важливим аспектом для забезпечення адаптивності, бо, наприклад, заміна одного з інгредієнтів через його відсутність або непереносимість користувачем може суттєво змінити процес приготування страви.

Інтеграція ШІ-агенту є перспективним рішенням цих проблем завдяки розумінню природної мови, контекстній персоналізації та здатності до створення адаптивних рекомендацій [2].

Для обґрунтування доцільності впровадження ШІ-агента було проведено порівняння роботи традиційної веб-платформи та з використанням ШІ і наведено очікуваний ефект від його інтеграції (таблиця 1).

Таблиця 1 – Порівняння підходів

UX-сценарій	**Традиційний підхід**	**Підхід із ШІ-агентом**	**Очікуваний ефект від інтеграції ШІ-агенту**
Пошук рецепта за інгредієнтами	Ручний підбір фільтрів, пошук комбінацій	Користувач вводить запит — агент генерує релевантну відповідь	Скорочення часу пошуку; покращення успішності пошуку
Адаптація рецепта під умови користувача	Користувач сам шукає заміни інгредієнтів і адаптує рецепт	Агент враховує умови та надає інструкції для адаптації рецепту	Зниження когнітивного навантаження
Отримання пояснень/порад	Потрібно шукати інструкції в інших статтях або відео	Агент надає всю необхідну інформацію за запитом без необхідності звертання до інших ресурсів	Користувачу зручно виконувати всі задачі в одному середовищі
Планування меню на тиждень	Ручне складання списків	Автоматична генерація меню	Економія часу, вища практична цінність

На відміну від традиційного підходу, підхід з інтеграцією ШІ дозволяє користувачу бути співрозмовником, який отримує адаптовані рекомендації, пояснення та допомогу в реальному часі. Це відповідає сучасним тенденціям UX, де інструменти стають чутливими до контексту і здатними підлаштовуватися під потреби користувача. Тому доцільність впровадження ШІ-агента полягає в суттєвому підвищенні зручності, швидкості та ефективності взаємодії з веб-платформою.

Список використаних джерел:

1. McTear M. Conversational AI: dialogue systems, conversational agents, and chatbots. *Synthesis lectures on human language technologies*. 2020. Vol. 13, no. 3. P. 1–251. URL: https://doi.org/10.2200/s01060ed1v01y202010hlt048 (date of access: 19.11.2025).

2. Teng C.-Y., Lin Y.-R., Adamic L. A. Recipe recommendation using ingredient networks. *The 3rd annual ACM web science conference*, Evanston, Illinois, 22–24 June 2012. New York, New York, USA, 2012. URL: https://doi.org/10.1145/2380718.2380757 (date of access: 19.11.2025).

УДК 343.21:004.4

Трибюк В.О., здобувач
Фант М.О., к.філол.н.
Державний університет «Житомирська політехніка»

ЮРИДИЧНІ ТА ЕТИЧНІ АСПЕКТИ ВЕБ-СКРАПІНГУ

На сьогоднішній день інформація – це один з головних ресурсів людства. Отримання та обробка цієї інформації вручну займає дуже багато часу, що для нас є проблемою у світі, який швидко розвивається і де кожна хвилина має значення. Саме тому зростає потреба в автоматизованих методах збору даних, одним із яких є веб-скрапінг. Веб-скрапінг – це автоматизована техніка, що дозволяє програмно витягувати дані із вебсайтів та формувати на їх основі власні інформаційні ресурси, каталоги або аналітичні вибірки [2].

Однак у процесі застосування, можуть виникнути низка проблем та обмежень, такі як етичність та легальне отримання інформації. Серед найбільш поширених труднощів варто виокремити – динамічні інтерфейси, захист від ботів, зміна структури сторінок, а також пов'язані з авторським правом, персональними даними та умовами користування веб ресурсами.

Тому перш ніж розпочинати веб-скрапінг певного контенту, доцільно перевірити, чи надає ресурс офіційні способи доступу до даних – зокрема:

- власний API;
- партнерські програми або комерційні ліцензії на контент.

За відсутності таких механізмів необхідно уважно ознайомитися з «Умовами надання послуг» та файлом robots.txt, який визначає дозволені або заборонені для автоматичного збору розділи сайту, а також може містити параметр Crawl-delay, який визначає мінімальний проміжок часу між запитами, що надсилаються до сайту.

Особливо важливим є врахування юридичних ризиків, які можуть призвести до штрафів та судових позовів. Основні проблемні зони:

1. Ігнорування умов надання послуг.

Багато веб-ресурсів забороняють автоматизований збір даних. Порушення цих умов вважається недотриманням контракту та злочином, що може призвести до блокування доступу або юридичних претензій з боку власника сайту.

2. Збір приватної або персональної інформації без правових підстав.

Збір персональних даних, таких як електронні адреси, номери телефонів, IP-адреси або інші ідентифікаційні відомості, регулюється спеціальними законодавчими актами. В Україні цей процес регламентується Законом України «Про захист персональних даних» [1]. На міжнародному рівні, застосовується Регламент ЄС про захист даних (GDPR) [4]. Несанкціоноване збирання або обробка персональних даних може кваліфікуватися як порушення правових норм та спричиняти юридичну відповідальність.

3. Створення надмірного навантаження на сервери через занадто часті запити.

Невеликий інтервал між HTTP-запитами може призвести до підвищеної завантаженості сервера та уповільнення роботи веб ресурсу, що розцінюється як неетична або навіть шкідлива поведінка. Таке порушення може призвести до блокування IP або судових позовів.

4. Копіювання захищеного авторським правом контенту без отримання дозволу.

Тексти, зображення, описи товарів, огляди та інші матеріали є інтелектуальною власністю. Масове копіювання контенту без ліцензійного дозволу або без посилань на власника може кваліфікуватися як порушення авторського права, навіть якщо сайт знаходиться у відкритому доступі [3].

Підводячи підсумки після проведеного дослідження можна виокремити, що в більшості випадків веб-скрапінг – це «сіра зона». Адже навіть, якщо інформація знаходиться у відкритому доступі, вона може захищатися різними юридичними законами, що ускладнює належне зібрання даних. Тому найбільш доцільним є використання офіційних джерел доступу до даних або укладання домовленостей із власниками веб ресурсів.

Список використаних джерел:

1. Про захист персональних даних. Офіційний вебпортал парламенту України [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

2. Introduction to Web Scraping - GeeksforGeeks. GeeksforGeeks [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/web-scraping/introduction-to-web-scraping/

3. Web scraping - legal or illegal? - geeksforgeeks. GeeksforGeeks [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/python/web-scrapping-legal-or-illegal/

4. What is GDPR, the eu's new data protection law? - gdpr.eu. GDPR.eu [Електронний ресурс] – Режим доступу до ресурсу: https://gdpr.eu/what-is-gdpr/

УДК 004.7

Сторчак Д.О., магістрант
Державний університет інформаційно-комунікаційних технологій

ІНСТРУМЕНТИ ДЛЯ ОПТИМІЗАЦІЇ HR-ПРОЦЕСІВ

Постановка задачі. Сучасні компанії стикаються з необхідністю швидко адаптувати свої кадрові процеси до цифрового середовища. Традиційні методи управління персоналом стають недостатньо ефективними в умовах зростання кількості даних, гібридного формату роботи та постійної зміни ринку праці. Саме тому актуальним є впровадження технологічних інструментів, які дозволяють автоматизувати рутинні завдання та підвищити ефективність роботи HR-відділів.

Мета дослідження. Метою роботи є аналіз сучасних цифрових інструментів, які використовуються для оптимізації HR-процесів, а також визначення їхнього впливу на ефективність управління персоналом в організаціях різного масштабу.

Результати дослідження. Цифрові технології відкрили нові можливості для HR-сфери. Найпоширенішими інструментами є системи управління персоналом (HRM-системи), такі як BambooHR, PeopleForce, Zoho People чи SAP SuccessFactors. Вони дозволяють вести електронний облік співробітників, формувати графіки, відстежувати відпустки, оцінювати продуктивність і спрощувати комунікацію між працівниками.

Іншим важливим напрямом є автоматизація рекрутингу. Сучасні сервіси, як-от Huntflow, Workable, Recruitee, допомагають створювати бази кандидатів, публікувати вакансії на різних платформах та навіть застосовувати штучний інтелект для попереднього відбору резюме. Це значно скорочує час на підбір персоналу й мінімізує людський фактор.

Окремо варто згадати аналітичні платформи, що працюють із великими даними. Вони допомагають HR-фахівцям прогнозувати плинність кадрів, визначати рівень задоволеності працівників і будувати ефективну систему мотивації. Використання таких інструментів дає можливість приймати рішення на основі фактів, а не лише інтуїції.

Крім того, велику популярність отримали чат-боти для HR-підтримки (наприклад, Leena AI чи Talla). Вони відповідають на типові

запитання співробітників, нагадують про дедлайни, допомагають проходити онбординг і підвищують зручність внутрішньої комунікації.

Висновки та перспективи.

Використання сучасних технологічних інструментів у сфері HR забезпечує економію часу, зменшення адміністративного навантаження та підвищення прозорості процесів. Проте для максимальної ефективності важливо не лише впровадити програмне забезпечення, а й навчити персонал працювати з ним, адаптувати систему під специфіку компанії та забезпечити захист персональних даних.

Подальші дослідження можуть бути спрямовані на вивчення впливу штучного інтелекту на процес прийняття управлінських рішень у HR та створення єдиних інтегрованих екосистем для управління людськими ресурсами.

Список використаних джерел:

1. Kavanagh M. J., Thite M., Johnson R. D. *Human Resource Information Systems: Basics, Applications, and Future Directions.* Thousand Oaks: SAGE Publications, 2021. 512 p.

2. Bissola R., Imperatori B. Digital transformation in HR management: Challenges and opportunities // *Journal of Human Resource Management.* – 2022. – Vol. 12, №3. – P. 45–57.

3. Коваленко Л. В. Інформаційні технології в управлінні персоналом // *Економіка та управління підприємствами.* – 2023. – №4. – С. 28–33.

4. Шевченко О. В. Автоматизація HR-процесів на основі сучасних цифрових платформ // *Інформаційні технології в економіці.* – 2024. – №2. – С. 60–65.

УДК 004.7: 004.93

Марчук Д.К., ст. викладач
Державний університет «Житомирська політехніка»

EDGE-ОРІЄНТОВАНИЙ ПІДХІД ДО МОНІТОРИНГУ ПАРКУВАЛЬНИХ ПРОСТОРІВ

Зростаюча кількість автомобілів у містах створює значні проблеми, зокрема, ускладнює пошук вільних паркувальних місць. Традиційні системи управління паркуванням, які покладаються на централізовану обробку даних, часто страждають від високих затримок і надмірного навантаження на мережу. Це робить їх недостатньо оперативними для водіїв, які шукають паркомісце в реальному часі.

Дане дослідження пропонує рішення, що ґрунтується на периферійному інтелекті (Edge Computing). Суть підходу полягає в тому, що значна частина обчислень відбувається безпосередньо на периферійних пристроях (Edge Devices), розташованих поблизу джерел даних. Джерелом даних виступають камери. Такий децентралізований підхід дозволяє істотно зменшити затримки, підвищити швидкість прийняття рішень та знизити вимоги до пропускної здатності мережі, що є критично важливим для створення інтелектуальної системи управління паркуванням.

Математична формалізація паркувального простору є фундаментальним кроком у системному підході, оскільки вона перетворює фізичні об'єкти на структуровані дані для подальшої обробки (рис.1).

Рисунок 1 – Математична формалізація паркувального простору

Кожне паркувальне місце Pi моделюється як унікальна геометрична область у R^2, визначена набором математичних функцій, що чітко задають її межі. Стан Pi у час t представляється булевою

змінною Si(t), де 1 означає, що паркомісце зайняте, а 0 — вільно. Це дозволяє описати загальний стан усього паркувального простору в будь-який момент часу t як вектор станів S(t), де кожен елемент вектора - це статус відповідного місця.

Ключовим елементом збору даних є розумна камера. На парковці може бути розгорнуто декілька камер, кожна з яких має свою унікальну зону покриття і генерує безперервний потік сирих зображень (кадрів). Сире зображення трансформується у структуровані дані. На відміну від традиційних систем, які надсилають весь відеопотік на центральний сервер, тут відбувається локальна обробка на Edge Devices. Процеси локальної обробки:

1. Калібрування та виділення області інтересу. На основі попереднього калібрування камери точно визначається і виділяється підобласть на зображенні, яка геометрично відповідає паркувальному місцю.
2. Вилучення ознак. До виділеної області застосовується функція (наприклад, шари згорткової нейронної мережі), що перетворює піксельні дані на вектор ознак, який містить суттєву інформацію (наявність автомобіля, його контури).
3. Локальна класифікація. Навчений класифікатор (вбудований в периферійний пристрій) приймає вектор ознак і видає локальну оцінку, яка є ймовірністю зайнятості місця.

Ця децентралізація обчислень забезпечує швидке прийняття рішень безпосередньо на периферії, зменшуючи обсяг даних, що передаються по мережі, лише до необхідних локальних оцінок, а не сирих відеопотоків.

Аналіз літературних джерел підтверджує актуальність та інноваційність запропонованого підходу, що вирішує критичні проблеми традиційних централізованих систем управління паркуванням, які страждають від високих затримок, навантаження на мережу та недостатньої оперативності через постійне зростання автомобільного парку в містах. Сучасні дослідження ([1], [2], [3], [4], [5], [6]) активно переходять від хмарних рішень до парадигми периферійних обчислень (Edge Computing), що є наріжним каменем даного дослідження. Зокрема, роботи [2], [3] та [6] демонструють, як інтеграція IoT, розумних камер (як ключових Edge Devices) та алгоритмів машинного зору/глибокого навчання забезпечує високоточне, індивідуалізоване та швидке виявлення статусу паркувальних місць, мінімізуючи обсяг переданих даних, що відповідає концепції локальної обробки та математичної формалізації паркувального простору (Pi як геометричної області в R^2).

Список використаних джерел:

1. X. Huang, P. Li, R. Yu, Y. Wu, K. Xie and S. Xie, "FedParking: A Federated Learning Based Parking Space Estimation With Parked Vehicle Assisted Edge Computing," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9355-9368, Sept. 2021, doi: 10.1109/TVT.2021.3098170.

2. C. Lee, S. Park, T. Yang and S. -H. Lee, "Smart Parking with Fine-Grained Localization and User Status Sensing Based on Edge Computing," *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, Honolulu, HI, USA, 2019, pp. 1-5, doi: 10.1109/VTCFall.2019.8891560.

3. W. Kim and I. Jung, "Smart Parking Lot Based on Edge Cluster Computing for Full Self-Driving Vehicles," in *IEEE Access*, vol. 10, pp. 115271-115281, 2022, doi: 10.1109/ACCESS.2022.3208356. keywords: {Sensors;Wireless sensor networks;Space vehicles;Aerospace electronics;Real-time systems;Image edge detection;Intelligent sensors;Edge computing;Smart devices;Edge computing;full self-driving;mobile edge;smart parking lot},

4. Sarker, V.K.; Gia, T.N.; Ben Dhaou, I.; Westerlund, T. Smart Parking System with Dynamic Pricing, Edge-Cloud Computing and LoRa. *Sensors* 2020, *20*, 4669. https://doi.org/10.3390/s20174669

5. A. F. Ala'anzy, M. A. Ala'anzy, U. A. Bukar, T. Zhukabayeva, D. Baumuratova and N. Karabayev, "Real-Time Oversight of Parking Space Management in IoT Edge Computing for Industry 4.0: A Case Study," *2024 IEEE 7th International Symposium on Telecommunication Technologies (ISTT)*, Langkawi Island, Malaysia, 2024, pp. 132-137, doi: 10.1109/ISTT63363.2024.10750756.

6. H. Bura, N. Lin, N. Kumar, S. Malekar, S. Nagaraj and K. Liu, "An Edge Based Smart Parking Solution Using Camera Networks and Deep Learning," *2018 IEEE International Conference on Cognitive Computing (ICCC)*, San Francisco, CA, USA, 2018, pp. 17-24, doi: 10.1109/ICCC.2018.00010.

УДК 004

Ковбасюк С.В., д.т.н., с.н.с.,
Українець М.О., аспірант
Державний університет «Житомирська політехніка»

ВИЗНАЧЕННЯ КООРДИНАТ МІСЦЕЗНАХОДЖЕННЯ БЕЗПІЛОТНОГО ПОВІТРЯНОГО СУДНА В УМОВАХ НЕДОСТУПНОСТІ ГЛОБАЛЬНИХ НАВІГАЦІЙНИХ СУПУТНИКОВИХ СИСТЕМ

Виконання навігації безпілотного повітряного судна (БПС) у складі безпілотного авіаційного комплексу (БпАК) включає в себе вирішення підзавдань з визначення та контролю дотримання маршруту. Для вирішення підзавдання контролю дотримання маршруту важливим аспектом є визначення координат поточного місцезнаходження (локалізації) БПС. Системи навігації сучасних БПС залежать від глобальних навігаційних супутникових систем (ГНСС) для отримання координат поточного місцезнаходження. Проте, точність позиціювання за допомогою ГНСС не дозволяє виконувати завдання покладені на БПС в несприятливих умовах [1] з необхідною ефективністю. Протиріччя має місце між вимогами до ефективності виконання завдань, покладених на БПС, та наявним методичним та алгоритмічним забезпеченням для визначення координат місцезнаходження БПС в умовах недоступності ГНСС.

Метою дослідження є визначення підходу до вирішення завдання локалізації БПС в умовах недоступності ГНСС.

Підхід до локалізації БПС залежить від даних, які БПС здатне отримувати за допомогою бортових датчиків під час польоту. Поширеним підходом до визначення місцезнаходження рухомих об’єктів на основі даних інерційного вимірювального пристрою (ІВП) є метод числення координат. Проте, використання даного підходу для локалізації БПС в умовах недоступності ГНСС не забезпечить достатньої точності через накопичення похибки з часом. Зображення з бортових камер є джерелом геопросторових даних, які використовуються для вирішення завдання локалізації. У роботах [2] та [3] дослідники реалізували системи візуальної навігації БПС. Система, описана в роботі [2], використовує геоприв’язані супутникові знімки, карти висот, зображення з бортової камери БПС та дозволяє визначати його координати незалежно від пори року, у яку здійснюється політ. Однак, запропонована система не працюватиме коректно, якщо висота польоту буде низькою або завдання виконуватиметься на місцевості без чітких візуальних орієнтирів чи перепадів висот. Система, описана в

роботі [3], працюватиме некоректно в складних погодних умовах та за наявності інших чинників погіршення видимості, наприклад, задимлення.

Враховуючи наявні недоліки систем візуальної навігації, для підвищення ефективності локалізації БПС в умовах недоступності ГНСС слід застосувати гібридний підхід, який поєднує в собі візуальну навігацію за допомогою геоприв'язаних супутникових знімків, метод числення координат на основі даних з ІВП та планування маршруту з руху з урахуванням особливостей місцевості.

Перед польотом на наземній станції БпАК слід виконати планування маршруту з урахуванням особливостей місцевості, щоб мінімізувати ризик прольоту над ділянками без візуальних орієнтирів. У разі неможливості скласти маршрут допустимої довжини без однотипних ділянок, слід використовувати метод числення координат на основі даних ІВП. Альтернативою цьому є набір висоти БПС для збільшення ймовірності визначення візуальних орієнтирів. При цьому слід запровадити механізм прийняття рішень з огляду на умови польоту, запас енергії, довжину маршруту тощо для визначення альтернативного способу отримання координат місцезнаходження БПС. Запропонований гібридний підхід до локалізації БПС дозволить покращити ефективність виконання завдань в умовах недоступності ГНСС.

Подальші дослідження будуть спрямовані на розробку методичного та алгоритмічного забезпечення гібридного підходу локалізації БПС на основі візуальної навігації, методу числення координат та планування маршруту руху.

Список використаних джерел:

1. Ковбасюк С. В., Українець М. О. Планування траєкторії польоту безпілотного повітряного судна в несприятливих умовах. Тези XV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології» : Тези міжнар. науково-техн. конф., м. Житомир, 28 берез. 2025 р. Житомир, 2025. С. 183–184. URL: https://conf.ztu.edu.ua/wp-content/uploads/2025/04/povnyj-tekst.pdf.

2. A seasonally invariant deep transform for visual terrain-relative navigation / A. T. Fragoso et al. Science robotics. 2021. Vol. 6, no. 55. P. eabf3320. URL: https://doi.org/10.1126/scirobotics.abf3320 (date of access: 20.11.2025).

3. Gurgu M.-M., Queralta J. P., Westerlund T. Vision-based GNSS-Free Localization for UAVs in the Wild. ICMERR 2022 conference proceedings : Conference Proceedings, Krakow, 9 December 2022. 2022. URL: https://arxiv.org/abs/2210.09727

УДК 004.4

Зулінський М.В., здобувач,
Марчук Д.К., ст. викладач
Державний університет «Житомирська політехніка»

ПІДХІД ДО ПОБУДОВИ МОДУЛЬНОЇ АРХІТЕКТУРИ ІГРОВОГО ПРОЦЕСУ НА РУШІЇ UNITY

Сучасні підходи до розробки ігор вимагають високий рівень структурованості коду. Через зростання складності в побудові ігор, за рахунок збільшення можливих механік призводить до неможливості покращувати код і змінювати його певні аспекти без шкоди. Тому, доцільно застосовувати підхід з розділенням більш складних задач на автономні частини – модулі [1]. Модуль виконує лише задані для нього функції та інтегрується як інтерфейс, що забезпечить легкість в адаптації та підтримці коду, а також у тестуванні. В Unity цей підхід дуже чудово вписується через принцип роботи рушія та його орієнтацію на об'єктно орієнтовану систему взаємодії та компоненти, що робить можливість інтеграції даного підходу дуже легким у використанні.

Метою дослідження являється доведення переваг модульної архітектури у складних проектах, та важливість її застосування на рушії Unity.

Unity через свою орієнтацію на об'єктно-компонентну систему надає нам вже готові засоби для інтеграції модульного підходу, що спирається на компонентні моделі. У такій моделі GameObject виступає контейнером для набору компонентів, які визначають окремі аспекти поведінки [2]. На практиці це відкриває шлях до використання різних підходів і інструментів, що допомагають будувати масштабовану та гнучку архітектуру. Серед найпоширеніших варто виділити такі:

1. *ScriptableObject* використовується для зберігання даних проєкту та окремої логіки, яку можна повторно застосовувати на різних сценах і об'єктах без дублювання чи перевизначення коду [3].
2. *Event-Drive Design* забезпечує взаємодію модулів через події, що мінімізує залежності між ними. Наприклад, система здоров'я може надіслати повідомлення про зміну стану, не знаючи нічого про інші модулі.
3. *Entity Component System* (ECS) використовується у великих проектах для розділення поведінки та даних для подальшого опрацювання великої кількості об'єктів, одночасно використовуючи вже створені модулі.
4. *Dependency Injection* (ID) відповідає за передачу залежностей між модулями без жорстокої прив'язки до конкретних компонентів та

класів, що в свою чергу підвищує можливість тестування та спрощує внесення змін до всього модуля.

На практиці модульний підхід у розробці ігрових процесів на Unity дозволяє створювати архітектуру, в якій окремі елементи гри можна легко змінювати та розширювати без втручання в основний або залежний код. Це спрощує адаптацію проєкту під різні платформи, зменшує дублювання логіки, покращує повторне використання компонентів та знижує ризик появи помилок у пов'язаних модулях.

До прикладу в іграх жанру RPG модулі можуть бути розділені та відповідати за керування інвентарем, бойовими системами, штучним інтелектом а також взаємодією з UI елементами. Завдяки такому поділу зміни в одному модулі не порушують роботу інших і не впливають на їхній функціонал. Таким чином алгоритми атаки для ворогів не мають впливу на UI та інвентар, а також не впливають на бойову систему.

Використання модульної архітектури являється ключовим підходом для побудови сучасних ігор. Вона впливає на гнучкість, масштабованість та подальшу підтримку проекту, що легко адаптується при потребі. Використання вже готових способів застосування компонентних моделей в Unity впливає на час розробки коду та його якість. Таким чином, модульна архітектура не лише впливає на покращення організації коду, а також збільшує ефективність команди при розділені задач між ними, що є критично важливим у сучасній ігровій індустрії.

Список використаних джерел:

1. Modular Software: Definition, Benefits, and Architecture Principles**.** *vFunction Blog*. 2023. URL: https://vfunction.com/blog/modular-software/ (дата звернення: 19.11.2025).

2. Nordon S. Unity Architecture: GameObject-Component Pattern. *Medium*. 2022. URL: https://medium.com/@simon.nordon/unity-architecture-gameobject-component-pattern-34a76a9eacfb (дата звернення: 20.11.2025).

3. Create Modular Game Architecture with ScriptableObjects in Unity 6. *Unity Resources*. 2024. URL: https://unity.com/resources/create-modular-game-architecture-scriptableobjects-unity-6 (дата звернення: 20.11.2025).

УДК 004.4

Левчук А. С., здобувач,
Марчук Д.К., ст. викладач
Державний університет «Житомирська політехніка»

ПРОЄКТУВАННЯ ІГРОВИХ МЕХАНІК У ПРОЄКТАХ ЖАНРУ ACTION RPG

Action RPG являє собою синтез екшн-ігор та рольових ігор, що акцентує увагу на динамічній бойовій системі в реальному часі з одночасним збереженням елементів розвитку персонажа. Проєктування збалансованих ігрових механік є критичним фактором успіху в цьому сегменті ринку, оскільки від якості механік залежить задоволення гравців та комерційний успіх проєкту.

Метою дослідження є аналіз принципів проєктування ключових ігрових механік у жанрі Action RPG.

Action RPG як жанр характеризується бойовою системою в реальному часі з акцентом на координацію та швидкість реакції гравця, збереженням RPG-елементів прокачки персонажа, системи навичок, інвентаря та спорядження.

Проєктування бойової системи базується на фундаментальних елементах, серед яких контроль ігрового простору відіграє важливішу роль, ніж просте завдання шкоди. Швидкість руху гравця повинна перевищувати швидкість ворогів для забезпечення можливості виходу з бою. Механіка відбиття (Knockback) після отримання пошкодження запобігає безкінечним циклам шкоди. Система атак включає період підготовки (Lead-in period), що має бути фіксованим та передбачуваним, та період після завдання шкоди (Lead-out period) до повернення в стан очікування [1].

Системи прогресії персонажа поділяються на вертикальну та горизонтальну [2]. Вертикальна прогресія передбачає поступове збільшення сили персонажа через підвищення характеристик HP, сили атаки та захисту, що забезпечує зрозумілу демонстрацію прогресу. Горизонтальна прогресія розширює можливості та варіанти гри без чистого збільшення сили, надаючи більшу різноманітність геймплею. Популярні моделі включають Activity-based progression, де навички покращуються через їх використання, Skill Tree Systems з масивним деревом пасивних навичок, що потребує стратегічного планування, та Job Systems з можливістю комбінування навичок різних професій.

Системи лута та предметів представлені двома основними підходами. Статичний лут характеризується тим, що кожен предмет жорстко закодований дизайнерами, що дозволяє точне балансування та

створення креативних унікальних предметів, проте обмежує реіграбельність. Процедурний лут генерується через алгоритми на основі префіксів та суфіксів, що забезпечує високу реіграбельність та постійний драйв пошуку кращого спорядження. Дизайн цікавих предметів має уникати простих статистичних бонусів та включати модифікатори, що змінюють геймплей та функціональність здібностей персонажа.

Баланс та складність систем в Action RPG знаходяться між повним контролем гравця, характерним для екшн-ігор, та абстрактними системами класичних RPG [3]. Успіх залежить від навичок гравця в реакції та таймінгу, а також від характеристик персонажа. Принципи балансування вимагають поєднання різноманітності з балансом, уникнення ситуацій домінування одного предмета або навички, надання гравцю значущих виборів з унікальними перевагами кожного варіанту. Психологічні аспекти прогресії створюють відчуття зростання сили.

Практичні рекомендації з проєктування включають визначення бажаного досвіду гравця з темпом та рівнем покарання за помилки, проєктування взаємодії гравця з вибором дій та витратою ресурсів, створення схеми бойового циклу, тестування концепції перед імплементацією коду та ітеративне налаштування балансу. Проєктування систем прогресії вимагає узгодження механік прогресії з наративом гри, забезпечення значущих виборів на кожному рівні, балансу між лінійною та вільною прогресією та створення синергії між різними системами навичок, спорядження та стилю гри.

Проєктування ігрових механік у жанрі Action RPG вимагає комплексного підходу до створення взаємопов'язаних систем бою, прогресії та лута з урахуванням балансу між навичками гравця та характеристиками персонажа.

Список використаних джерел:

1. Realtime Combat Design. How to Make an RPG. URL: https://howtomakeanrpg.com/r/a/realtime-combat-design.html (дата звернення: 22.11.2025).

2. Game Progression. Game Design Skills. URL: https://gamedesignskills.com/game-design/game-progression/ (дата звернення: 22.11.2025).

3. RPG Progression System Research. Adrian FR. URL: https://adrianfr99.github.io/RPG-progression-system/ (дата звернення: 22.11.2025).

УДК 004.9

Торба С.О., магістрант,
Сагайдак В.А., PhD
Державний університет інформаційно-комунікаційних технологій

ПЕРСОНАЛІЗОВАНИЙ ШІ-АСИСТЕНТ ДЛЯ ФІТНЕС-СТУДІЇ ЯК ЕЛЕМЕНТ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Інформаційні системи сучасності стрімко розвиваються під впливом новітніх технологій та розвитку штучного інтелекту. Системи для фітнес-студій та їм подібних закладів не є виключенням. Використання ШІ є невід`ємним фактором розвитку будь-якої системи у наш час, що для розглянутого прикладу є великою можливістю для розвитку - формування нових підходів до персоналізації управління тернувальним процесом, організації обробки даних, ведення обліку та підвищення загальної ефективності подібних систем. У цьому контексті персоналізований ШІ-асистент розглядається як важливий структурний елемент для цифрової екосистеми фітнес-студій чи спортзалів[1].

Основою для функціональності асистента будуть використані алгоритми машинного навчання, які забезпечуватимуть адаптацію рекомендацій відповідно заданих параметрів - різні поведінкові характеристики користувачів, історії відвідувань та проміжні результати тренувань. У сумі ці дані дають можливість формувати індивідуальні тренувальні плани, коригувати оптимальність навантажень та робити прогнози можливих змін фізичних показників. До того ж дослідження у сфері цифрових фітнес-платформ показують, що персоналізовані рекомендації позитивно впливають на мотивацію та загальну результативність процесу.

Однією з важливих складових ШІ-асистента є можливість обробляти дані у режимі реального часу та інтеграція у систему фітнес-студії. Це допомагає досягти узгодженості рекомендацій для тренувань із фактичним станом клієнта та його активністю.. Система може враховувати дані - типи тренувань, графік та його зміни, показники відновлення при інтеграції з фітнес-браслетами тощо. Та будь-які інші показники, які можуть підвищити точність запропонованих рішень

Застосування методів кластеризації [2] та прогнозування дозволятиме ідентифікувати типові профілі клієнтів, визначати типові шаблони поведінки та формувати рекомендації, спрямовані на довгостроковий результат, який у свою чергу може більш гнучко бути визначений самим користувачем. Поряд із цим використання методів

обробки природної мови[3] забезпечує цілком природну взаємодію між об'єктами система-користувач, що підвищує якість комунікації.

Встановлено, що впровадження персоналізованого AI-асистента у функціональну структуру фітнес-студії створює підґрунтя для комплексної цифрової підтримки користувача. Визначено, що асистент не лише оптимізує тренувальний процес, а й підвищує якість обслуговування за рахунок автоматизації рутинних операцій, генерації нагадувань, рекомендацій та прогнозів. Аргументовано, що поєднання алгоритмів штучного інтелекту з даними про активність користувача дозволяє формувати індивідуальні траєкторії фізичного розвитку. Класифіковано основні функції асистента: аналіз активності, формування рекомендацій, прогнозування динаміки показників та інтерактивну комунікацію..

Отже, персоналізований ШІ-асистент виступає важливою частиною сучасної інформаційної системи фітнес-студії, забезпечуючи підвищення ефективності тренувального процесу, покращення взаємодії з користувачем та формування адаптивного цифрового середовища. Масштабування таких систем визначає подальші перспективи розвитку індустрії фітнес-послуг у напрямі персоналізації та інтелектуальної підтримки.

Список використаних джерел:

1. Ahmed G., Khalif A. A., Doon M. A., Mohamed A. A., Ali I. A., Ahmed B. A. Personalized Gym Recommendation System Using Machine Learning. *International Journal of Engineering Trends and Technology*. 2025. Vol. 73, No. 4. P. 249-257. ISSN 2231-5381. DOI:10.14445/22315381/IJETT-V73I4P122. URL: https://ijettjournal.org/Volume-73/Issue-4/IJETT-V73I4P122.pdf (дата звернення: 20.11.2025).

2. Yin H., Aryani A., Petrie S., Nambissan A., Astudillo A., Cao S. A rapid review of clustering algorithms. *arXiv preprint*. 2024. arXiv:2401.07389. URL: https://arxiv.org/pdf/2401.07389 (дата звернення: 20.11.2025).

3. Wibawa A.P. Advancements in natural language processing: Implications, challenges, and future directions. *Telematics & Informatics Reports*. 2024. Vol. 16. Article 100173. DOI:10.1016/S2772-5030(24)00059-8. URL: https://www.sciencedirect.com/science/article/pii/S2772503024000598 (дата звернення: 20.11.2025).

УДК 004

Панібратець О.Д., здобувач,
Фуріхата Д.В., аспірант
Державний університет «Житомирська політехніка»

МЕТОДИ ПІДВИЩЕННЯ КОНВЕРСІЇ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ ЧЕРЕЗ ІНТЕРАКТИВНУ ВІЗУАЛІЗАЦІЮ ПЕРСОНАЛІЗОВАНИХ ТОВАРІВ

Електронна комерція активно розвивається, а персоналізація товарів стає одним із ключових чинників підвищення продажів. Для індивідуалізованої продукції характерна суттєва кількість відмов, що пов'язано з невизначеністю покупця щодо кінцевого вигляду виробу. Середній рівень конверсії в e-commerce становить 2-4 % [1], але для персоналізації цей показник зазвичай нижчий. Дослідження UX підтверджують, що інтерактивна взаємодія з товаром зменшує бар'єри прийняття рішення та підсилює довіру до бренду [4].

У межах роботи створено інструмент інтерактивної візуалізації, що дає змогу користувачеві завантажувати власні зображення, редагувати їх (масштаб, позиція, ротація) та переглядати результат у режимі реального часу. Алгоритми автоматичного позиціонування оптимізують розміщення зображення відповідно до пропорцій виробу. Система підтримує перегляд з різних кутів, що підвищує реалістичність моделі та наближає процес до огляду фізичного товару [2]. Завдяки адаптивному дизайну інструмент коректно працює на мобільних пристроях, які формують понад 60 % трафіку [1].

Для оцінки ефективності проведено A/B-тестування. Контрольна версія інтерфейсу показала конверсію 2,5 %, тоді як варіант із інтерактивною візуалізацією - 3,5-3,6 %, що становить зростання на близько 40 % [3]. Також зафіксовано зменшення показника відмов на 27 % та збільшення часу взаємодії з товаром на 32 %. Підвищення конверсії узгоджується з попередніми дослідженнями щодо впливу візуальних інструментів і рекомендованих систем на поведінку споживачів [4].

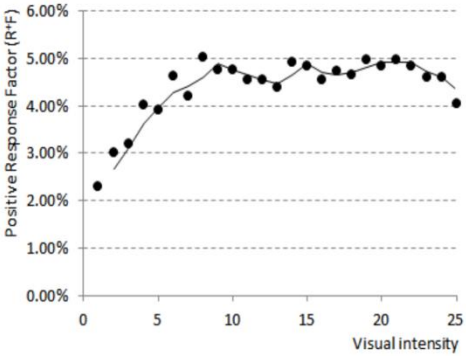


Рисунок 1 – Динаміка зміни коефіцієнта позитивної реакції (R^+F) зі зростанням рівня впливу [4]

Отримані результати свідчать, що інтерактивна візуалізація персоналізованої продукції є ефективним засобом збільшення продажів та покращення користувацького досвіду. Подальший розвиток системи може включати AR-функціонал, автоматичний аналіз якості зображень і розширення підтримки 3D-моделей.

Список використаних джерел:

1. Speed Commerce. 2025 eCommerce Benchmarks: Average Conversion Rates by Industry & By Year. URL: https://www.speedcommerce.com/insights/ecommerce-benchmarks-conversion-rates-by-industry-over-by-year/ (дата звернення: 17.11.2025).

2. Shankar D., Narumanchi S., Ananya H. A. та ін. Deep Learning Based Large Scale Visual Recommendation and Search for E-Commerce. arXiv preprint, 2017. URL: https://arxiv.org/abs/1703.02344 (дата звернення: 19.11.2025).

3.Red Stag Fulfillment. Average Ecommerce Conversion Rate: Industry Data for 2025. URL: https://redstagfulfillment.com/average-conversion-rate-for-ecommerce (дата звернення: 18.11.2025).

4. Jankowski J., Hamari J., Wątróbski J. A Gradual Approach for Maximising User Conversion without Compromising Experience with High Visual Intensity Website Elements. arXiv preprint, 2019. URL: https://arxiv.org/abs/1903.11997 (дата звернення: 19.11.2025).

УДК 004.7

Роман М. Р., здобувач
Державний університет
інформаційно-комунікаційних технологій

АРХІТЕКТУРА IoT-СИСТЕМИ ДЛЯ МОНІТОРИНГУ ЕКОЛОГІЧНИХ ПАРАМЕТРІВ

Постановка задачі

Дослідження архітектури IoT-системи для моніторингу параметрів навколишнього середовища та оцінка можливостей її застосування у міських, промислових та природоохоронних умовах.

Мета дослідження

Метою роботи є аналіз архітектури IoT-системи моніторингу довкілля, визначення її ключових компонентів: сенсорної мережі, протоколів зв'язку, хмарної платформи, аналітичних модулів та оцінка їх ролі у забезпеченні ефективного збору, обробки та використання екологічних даних у реальному часі.

Результати дослідження

Основою IoT-системи моніторингу є сенсорна мережа, що включає датчики температури, вологості, рівня шуму, вібрацій, концентрації газів або твердих частинок. Передавання даних здійснюється за допомогою енергоефективних протоколів LoRaWAN, ZigBee або NB-IoT, які забезпечують стабільну роботу на значних відстанях та при низькому енергоспоживанні. Зібрані дані надходять на шлюз IoT, де виконуються попередня фільтрація, агрегація та подальше передавання у хмарні сервіси.

Хмарна інфраструктура дає змогу обробляти великі обсяги даних, інтегрувати їх зі сторонніми сервісами та запускати алгоритми аналізу. Аналітичний модуль дозволяє будувати часові ряди, виявляти аномалії, прогнозувати зміни параметрів навколишнього середовища й формувати сигнали попередження про потенційні екологічні ризики.

Для користувачів створена веб-панель, що забезпечує візуалізацію інформації у вигляді графіків, картографічних шарів та інтерактивних віджетів. Використання GIS дозволяє визначати критичні зони та оцінювати просторовий розподіл забруднень. Система також підтримує push-сповіщення, що забезпечує оперативне інформування про перевищення контрольних норм.

До важливих аспектів архітектури належать питання безпеки: шифрування даних, автентифікація пристроїв, захист каналів передавання, резервування серверної інфраструктури та механізми автопоновлення роботи системи. Надійність сенсорної мережі забезпечується калібруванням датчиків, регулярною діагностикою та оптимізацією енергоспоживання.

Висновки та перспективи

Архітектура IoT-системи для моніторингу довкілля дозволяє ефективно збирати, передавати та аналізувати екологічні дані в режимі реального часу. Модульність, масштабованість та можливість інтеграції з інтелектуальними алгоритмами роблять такі системи придатними для використання в міських екосистемах, промислових зонах і природоохоронних територіях.

Подальші напрями розвитку передбачають використання штучного інтелекту, розширення аналітичних можливостей, створення точніших датчиків та впровадження сучасних комунікаційних технологій, зокрема 5G. Це дозволить підвищити точність моніторингу, забезпечити прогнозування екологічних загроз і підтримати сталий розвиток міст.

Список використаних джерел:

1. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for Smart Cities. IEEE Internet of Things Journal, 2014. Available at: https://dspace.networks.imdea.org/handle/20.500.12761/1295 (accessed 24 November 2025).

2. Gurbanova L., Abdullayev V. Application of IoT and Sensor Technologies in Environmental Monitoring. Environmental Research and Ecotoxicity, 2025. DOI: https://doi.org/10.56294/ere2025170 (accessed 24 November 2025).

УДК 004.7

Кучер В.О., магістрант
Єфремов Ю.М., к.т.н., доцент,
Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ АРХІТЕКТУР ГЛИБОКОГО НАВЧАННЯ ДЛЯ ПРОГНОЗУВАННЯ ФІНАНСОВИХ ЧАСОВИХ РЯДІВ

Глибоке навчання для прогнозування фінансових часових рядів стає пріоритетною технологією сучасної фінансової аналітики, оскільки забезпечує принципово новий рівень точності при моделюванні динаміки цін та побудові інвестиційних стратегій. На відміну від класичних статистичних підходів, таких як ARIMA чи GARCH, які здатні моделювати лише лінійні взаємозв'язки, нейронні мережі глибокого навчання дають змогу знаходити й ефективно використовувати складні нерівномірні та приховані патерни у великих обсягах ринкових даних. Завдяки потужним обчислювальним ресурсам та розвитку математичних основ, архітектури LSTM, GRU та Transformer стали золотим стандартом для фінансового прогнозування – як для короткострокового, так і для середньострокового горизонту аналізу.

Рекурентні моделі, зокрема LSTM та GRU, продемонстрували високу здатність до навчання на довгих часових послідовностях, що дозволяє вловлювати як основні ринкові тренди, так і короткотермінові коливання із збереженням залежностей на віддалених кроках. Модифікації на основі механізмів уваги, які активно використовуються у Transformer та Temporal Fusion Transformer, дають змогу підсилити роль контекстних ознак та враховувати вплив додаткових факторів, що особливо важливо у багатофакторному фінансовому прогнозуванні. Включення механізму уваги дозволяє виділяти найбільш значущі періоди або індикатори, що підвищує точність моделювання та спрощує інтерпретацію результатів навіть при суттєвій волатильності ринку.

У цьому дослідженні для прогнозування цін акцій Apple Inc. (AAPL) за серпень-вересень 2023 року були побудовані та оптимізовані моделі LSTM, GRU та Transformer з урахуванням актуальних гіперпараметрів. Моделі проходили навчання на історичних даних, а якість прогнозів оцінювалася за стандартними метриками MAE, RMSE та коефіцієнтом детермінації R^2. Було встановлено, що трансформерна архітектура досягла найкращих результатів (MAE = 0.80, RMSE = 0.94, R^2 = 0.88), що вказує на високу здатність цієї мережі правильно інтерпретувати динаміку акцій в умовах підвищеної невизначеності. LSTM показав також достатньо високу точність (MAE = 1.38, RMSE =

1.62, R^2 = 0.64), але поступився Transformer при роботі з короткими інтервалами прогнозу, що є типовим для ринків із швидкою зміною трендів. GRU забезпечив базову якість прогнозування (MAE = 2.27, RMSE = 2.54, R^2 = 0.12), що на практиці компенсується меншою складністю та швидкістю роботи з великим обсягом даних. Ансамблева модель, яка об'єднує результати декількох архітектур, у підсумку демонструє якість (MAE = 1.00, RMSE = 1.20, R^2 = 0.81), майже не поступаючись Transformer, що свідчить про ефективність гібридного підходу до розв'язання задач фінансового прогнозування.

Результати аналізу підтверджують, що сучасні методи глибокого навчання, зокрема архітектури з механізмом уваги, забезпечують суттєве зростання точності прогнозування у порівнянні з класичними нейромережами та статистичними моделями. Практична цінність підходу полягає в можливості динамічного вибору архітектури в залежності від горизонту прогнозу, ризиковості фінансового інструменту та наявності багатофакторних впливів, що особливо важливо для автоматизованих систем прийняття інвестиційних рішень. Подальші роботи у цій галузі мають бути спрямовані на вдосконалення інтеграції deep learning із класичними інструментами економічного аналізу, що дозволить підвищити стійкість систем до змін ринкової кон'юнктури та підвищити рівень автоматизації керування портфелями активів.

Список використаних джерел:

1. Zhang, Q., Yang, L., He, H. "Time series forecasting in financial markets using deep learning models: A comparative study." World Journal of Advanced Engineering and Technology Sciences, 2025, 13(3), 46–66. https://doi.org/10.56390/WJAETS.2025.0167

2. Wang, X., Zhu, Y., & Li, Z. "Enhancing financial time series forecasting with hybrid Deep Learning." Applied Soft Computing, 2025, 144, 110554. https://doi.org/10.1016/j.asoc.2025.110554

3. Thoque, H. "Decoding Stock Trends: A Comparative Study of GRU, LSTM, and Transformer Models." Transactions on Engineering and Computing Sciences, 2025, 13(3), 58–70. https://doi.org/10.34317/tecs.2025.13.3.58

УДК 004.7

Колесник О.А., здобувач,
Піонтківський В.І., асистент
Державний університет «Житомирська політехніка»

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ АВТОМАТИЗАЦІЇ БРОНЮВАННЯ УПРАВЛІННЯ ТА АНАЛІТИКИ У СФЕРІ ПОСЛУГ

У сучасних умовах високої конкуренції в сфері послуг веб-застосунки відіграють ключову роль у залученні нових клієнтів, підвищенні якості їх обслуговування, обробці даних для детальної аналітики бізнес-процесів та отриманні зворотного зв'язку. Такі системи дозволяють не лише оптимізувати й скоротити операційні процеси, пов'язані з ручною обробкою інформації, але й забезпечують бізнесу конкурентоспроможність на цифровому ринку, тобто досягнення лідерських позицій у пошуковій видачі за ключовими словами чи регіоном.

Аналіз даного сегменту дає змогу виокремити основні бізнес вимоги для такого застосунку:

1. Залучення клієнтів та користувацький досвід.

Висока позиція у пошуковій видачі забезпечує стабільний потік нових відвідувачів, однак наступним важливим етапом є перетворення цих відвідувачів на реальних клієнтів. Для досягнення високої конверсії необхідно впровадити спрощену систему реєстрації та бронювання, що мінімізує кількість кроків до оформлення послуги. Важливу роль відіграє також інтуїтивно зрозумілий, візуально привабливий та зручний інтерфейс, який формує довіру користувачів, покращує їх враження від взаємодії із системою та підштовхує до повторного використання сервісу.

2. Автоматизація бізнес процесів.

Максимальне скорочення ручної обробки інформації (наприклад, бронювання, оформлення замовлень, формування рахунків та управлінських звітів) підвищить ефективність та зменшить операційні витрати. Автоматичне формування детальних звітів дозволить керівництву оперативно реагувати на всі процеси та швидше приймати ключові рішення в розвитку власного бізнесу.

3. Гнучкість та розширення.

При проєктуванні таких систем необхідно заздалегідь закладати високу архітектурну гнучкість і масштабованість. Це вимагає врахування як потенційного якісного зростання бізнесу (впровадження

нових послуг та функціоналу) так і кількісного розширення (збільшення мережі закладів, кількості користувачів та обсягів даних). Також не варто забувати про такі технічні деталі, як можливість легкої інтеграції нових модулів, вони мають бути закладені ще на початковому етапі проєктування, не обмежуючись лише поточним списком бізнес-вимог.

Для задоволення цих ключових потреб системи важливо знайти ефективні архітектурні рішення, які в подальшому будуть сприяти тільки розширенню програмного продукту.

Бекенд системи пропоную реалізовувати на мовою програмування Java із застосуванням фреймворку Spring Boot, який забезпечить надійну побудову серверної логіки та масштабованої архітектури. Використання Spring Boot спрощує процес створення та підтримку основних операцій, налаштування взаємодії з базами даних, а також впровадження механізмів безпеки (аутентифікації та авторизації). Завдяки великому набору вбудованих модулів і автоматичній конфігурації, Spring Boot значно зменшує час на розгортання застосунку та підвищує стабільність роботи[2].

Фронтенд частину системи доцільно реалізувати з використанням JavaScript-фреймворку Next.js, який створений на базі бібліотеки React та забезпечує високу продуктивність, зручність розробки й SEO-оптимізацію завдяки можливості серверному рендерингу. Архітектура Next.js дозволяє ефективно поєднувати статичні та динамічні сторінки, що прискорює завантаження сторінки та забезпечить позитивний користувацький досвід. Завдяки вбудованій маршрутизації, системі кешування та підтримці API-роутів, фреймворк значно спрощує розробку в компонентно-орієнтованому стилі.

Додатково, використання React-компонентів дає змогу створювати модульний, легко масштабований користувацький інтерфейс, який можна швидко розширювати відповідно до нових функціональних вимог[1].

Також важливим елементом є вровадження на ранньому етапі CI/CD (Continuous Integration / Continuous Delivery), що є надзвичайно важливим для сучасних застосунків, оскільки дозволяє автоматизувати процеси збірки, тестування та розгортання нових версій системи. Такий підхід забезпечує безперервну інтеграцію змін у коді та їх поступову доставку на віддалені сервери, що мінімізує ризики виникнення помилок у продакшні, тому що від цього напряму залежить стабільний потік клієнтів.

Особливо важливо, підкреслити що маленькі, але регулярні оновлення виявляються набагато ефективнішими за великі релізи.

Кожна невелика зміна легше тестується, швидше впроваджується та простіше відкатується у разі виявлення проблем. Крім того, постійні оновлення дозволяють швидко отримувати зворотний зв'язок від користувачів і адаптувати функціонал під нагальні потреби[3].

Додатково система має включати модуль інтеграції з Telegram, у рамках якого спеціальний бот автоматично надсилатиме сповіщення як користувачам, так і працівникам. Такий бот оперативно інформуватиме про нові бронювання, зміни в графіку роботи, нагадування та інші важливі події. Використання Telegram- це ефективне інфраструктурне рішення, яке забезпечить швидку та зручну комунікацію без потреби розробляти окремі механізми для доставки повідомлень, що суттєво економить час і ресурси, підвищуючи загальний рівень сервісу та взаємодії між адміністраторами й клієнтами.

Також окремо слід виділити модуль генерації контенту, що використовує існуючі лінгвістичні моделі для створення та оптимізації тематичних статей. Такий підхід дозволяє автоматизувати контент-маркетинг, швидко формувати матеріали для сайту та покращувати SEO-показники без значних витрат часу копірайтерів.

Отже, впровадження сучасної інформаційної системи з автоматизацією бронювання, аналітики та AI-підтримкою дозволяє підвищити ефективність сервісу, оптимізувати бізнес-процеси та забезпечити високий рівень задоволеності користувачів.

Список використаних джерел:

1. Next.js:: documentation [Електронний ресурс]. – Режим доступу https://nextjs.org/docs (дата звернення 21.11.2025)

2. Spring Boot: documentation [Електронний ресурс]. – Режим доступу: https://spring.io/projects/spring-boot (дата звернення: 25.02.2025).

3. Towards cost-benefit evaluation for continuous software engineering activities [Електронний ресурс]. – Режим доступу: https://link.springer.com/article/10.1007/s10664-022-10191-w (дата звернення 20.11.2025)

УДК: 004.9

Біємська А.С., магістрант,
Свінцицька О.М., к.е.н., доцент
Державний університет «Житомирська політехніка»

МАТЕМАТИЧНА МОДЕЛЬ РОЗРАХУНКУ РОЗСІЮВАННЯ ПОСТРІЛУ В ЗАЛЕЖНОСТІ ВІД СТАНУ ПЕРСОНАЖА

Однією з ключових задач при розробці ігор жанру FPS (First Person Shooter) є створення реалістичної та збалансованої механіки стрільби. Статичні показники точності зброї ігнорують вплив фізичного стану стрільця на стабільність ведення вогню. Це призводить до так званої поведінки «run-and-gun», коли точність практично не погіршується під час руху, що суперечить як реальним фізичним законам, так і вимогам до збалансованості ігрового процесу [1].

Для подолання зазначених обмежень доцільним є застосування математичного моделювання динамічного розсіювання (spread), що змінюється в реальному часі. Розроблена модель описує залежність розсіювання від двох фундаментальних факторів — руху персонажа та використання режиму прицілювання ADS (Aim Down Sights). Поточне значення розсіювання визначається формулою:

$$Spread = BaseSpread \times (1 + \alpha \times M) \times (1 - \beta \times A)$$

де $BaseSpread$позначає базову характеристику точності конкретного виду зброї, M відображає наявність чи відсутність руху персонажа, α визначає ступінь зростання розсіювання внаслідок руху, A індикує стан прицілювання, а β встановлює величину стабілізаційного ефекту при використанні ADS. Так, підвищення коефіцієнта α робить стрільбу в русі суттєво менш ефективною, тоді як збільшення β стимулює використання прицілу, оскільки забезпечує підвищення точності.

Практична цінність запропонованої моделі полягає в її універсальності та здатності інтегруватися в широкий спектр ігрових сценаріїв. Наприклад, снайперські гвинтівки потребують вищої чутливості до руху, щоб уникнути нереалістичної високої точності під час переміщення, тоді як пістолети-кулемети, орієнтовані на ближній бій, можуть мати значно менший штраф за мобільність. Таким чином, параметри α та β можуть використовуватися як інструменти балансування між різними класами озброєння без потреби у створенні окремих, непов’язаних між собою моделей точності.

Реалізація моделі в ігровому рушії передбачає використання обчисленого значення Spread як парамерів конуса, в межах якого генерується випадкове відхилення напрямку польоту кулі від ідеальної

лінії прицілювання. Залежно від вимог реалізму та бажаного ігрового відчуття можуть застосовуватися різні методи стохастичного моделювання: рівномірний розподіл точок у площині перерізу конуса або гаусівський розподіл, що формує природніший розподіл влучань із більшою концентрацією поблизу центру [2]. Останній є більш обґрунтованим, оскільки він відповідає реальним закономірностям коливань ствола під час стрільби, спричиненим мікрорухами тіла та імпульсами віддачі.

Розширення моделі можливе за рахунок введення неперервних замість бінарних змінних. Зокрема, параметр M може визначатися не як факт руху, а як функція миттєвої швидкості персонажа, що дозволяє моделювати плавний перехід від стрільби стоячи до стрільби під час бігу. Аналогічно, індикатор A може бути поширений на багатоступеневу систему прицілювання, коли точність поступово зростає у процесі входження в режим ADS. Додатковими факторами для майбутніх модифікацій можуть стати поза персонажа (стоячи, присівши, лежачи), стабілізація зброї після серії пострілів, механіка віддачі та відновлення точності при автоматичній стрільбі, а також вплив параметрів втоми або навичок персонажа.

Таким чином, запропонована модель забезпечує реалістичнішу інтерпретацію механіки стрільби порівняно зі статичними підходами. Динамічне визначення точності створює багатий простір для тактичної взаємодії гравця з ігровим середовищем, сприяє підвищенню імерсивності та дозволяє гнучко налаштовувати характеристики різних класів зброї таким чином, щоб вони зберігали свою унікальність, але водночас залишалися збалансованими у межах загального геймплейного процесу. Модель є розширюваною, обчислювально недорогою та легко інтегрується в сучасні ігрові рушії, що робить її перспективною для широкого застосування у розробці комп’ютерних ігор.

Список використаних джерел:

1. Voorhees G. A., Call J., Whitlock K. *Guns, Grenades, and Grunts: First-Person Shooter Games*. Bloomsbury Academic & Professional. USA. 2012. URL: https://www.bloomsbury.com/us/guns-grenades-and-grunts-9781441193537/ (дата звернення: 22.11.2025).

2. Cricenti A. L., Branch P. A. *The Ex-Gaussian distribution as a model of first-person shooter game traffic*. Multimedia Systems, 2013. URL: https://link.springer.com/article/10.1007/s00530-012-0272-2 (дата звернення: 22.11.2025).

УДК: 004.9

Біємська А.С., магістрант,
Свінцицька О.М., к.е.н., доцент
Державний університет «Житомирська політехніка»

ЗВАЖЕНИЙ ВИПАДКОВИЙ ВИБІР У ПРОЦЕДУРНІЙ ГЕНЕРАЦІЇ ІГРОВИХ СУТНОСТЕЙ

Процедурна генерація контенту (Procedural Content Generation, PCG) у сучасній розробці програмного забезпечення розважального характеру є фундаментальним підходом, що дозволяє автоматизувати створення ігрових ресурсів за допомогою алгоритмічних засобів замість ручного моделювання кожного елемента [1]. Використання стохастичних алгоритмів дозволяє вирішити проблему обмеженості контенту, забезпечуючи високу варіативність ігрового процесу та реіграбельність.

Однак, застосування рівномірного розподілу ймовірностей (де всі події мають рівний шанс виникнення) часто є неприйнятним для задач ігрового балансу, оскільки це призводить до неконтрольованого хаосу та порушення кривої складності. Для забезпечення керованості генерації доцільним є використання методів, що дозволяють задавати ймовірність появи кожної сутності окремо. У даній роботі розглядається реалізація алгоритму зваженого випадкового вибору (Weighted Random Selection) як ефективного інструменту для динамічного спавну ігрових об'єктів.

Суть запропонованого підходу полягає у відмові від жорстко заданих послідовностей появи об'єктів на користь імовірнісної моделі, де кожному типу сутності (наприклад, класу ворога або типу ресурсу) присвоюється певний числовий коефіцієнт — вага (w). Вага є невід'ємним дійсним числом, що відображає відносну частоту появи даного елемента у загальній вибірці. Математично ймовірність $P(e_i)$ появи сутності e_i з множини доступних сутностей $E = \{e_1, e_2, \dots, e_n\}$ визначається як відношення ваги цієї сутності до суми ваг усіх елементів множини. Формула розрахунку виглядає наступним чином:

$$P(e_i) = \frac{w_i}{\sum_{j=1}^{n} w_j}$$

де w_i — вага i-го елемента, а знаменник дробу являє собою загальну вагу системи (W_{total}). Такий підхід дозволяє гнучко налаштовувати баланс: збільшення ваги одного елемента автоматично зменшує ймовірності появи інших, зберігаючи цілісність системи розподілу.

Алгоритмічна реалізація даного методу базується на концепції кумулятивного розподілу. Процес вибору можна представити як

розміщення відрізків довжиною w_i на одній числовій прямій загальною довжиною W_{total}. Випадкове число R, згенероване в діапазоні $[0, W_{total}]$ неминуче потрапить в один із цих відрізків, що і визначить обраний елемент.

Програмна логіка алгоритму може бути описана наступним псевдокодом:

```
Function GetWeightedRandomItem(ItemList):
    TotalWeight = 0
    For each Item in ItemList:
        TotalWeight += Item.Weight

    RandomValue = Random(0, TotalWeight)
    CumulativeWeight = 0

    For each Item in ItemList:
        CumulativeWeight += Item.Weight
        If RandomValue <= CumulativeWeight:
            Return Item

    Return Null (or DefaultItem)
```

Рис. 1 – Псевдокод процедурної генерації ігрових сутностей на основі методу зваженого випадкового вибору

У наведеному алгоритмі спочатку відбувається прохід по колекції для обчислення загальної суми ваг. На другому етапі генерується випадкове число. Третій етап — це лінійний пошук, де на кожній ітерації до акумулятора додається вага поточного елемента. Умова RandomValue <= CumulativeWeight спрацьовує саме тоді, коли кумулятивна сума "покриває" випадкове значення, що відповідає потраплянню у відповідний імовірнісний інтервал. Обчислювальна складність даного алгоритму становить $O(N)$, де N — кількість типів сутностей, що є прийнятним для систем реального часу з невеликою кількістю категорій об'єктів.

Таким чином, використання процедурної генерації на основі зваженого випадкового вибору забезпечує необхідний рівень абстракції між логікою прийняття рішень (яку складність встановити) та логікою виконання (якого саме ворога створити). Це дозволяє створювати гнучкі, масштабовані системи, де додавання нового контенту зводиться до розширення списку конфігурацій без втручання в ядро алгоритму, а варіативність ігрових ситуацій досягається шляхом маніпуляції числовими коефіцієнтами розподілу ймовірностей.

Список використаних джерел:

1. Shaker N., Togelius J., Nelson M. J. *Procedural Content Generation in Games*. Springer, 2016. URL: https://link.springer.com/book/10.1007/978-3-319-42716-4 (дата звернення: 22.11.2025).

УДК:004.67

Бродський Ю.Б., к.т.н., доцент
Пасічник В.О., магістрант
Державний університет «Житомирська політехніка»

РОЗРОБКА ВЕБ-ПЛАТФОРМИ ДЛЯ РОЗМІЩЕННЯ ТА ПОШУКУ ВОЛОНТЕРСЬКИХ ІНІЦІАТИВ

Волонтерський рух в Україні під час війни стрімко розвивається та є критично важливим (зокрема, дослідження показують значне збільшення кількості волонтерських ініціатив у 2022–2023 рр. [1]), проте, попри динамічний розвиток, він часто стикається з неефективним розподілом ресурсів та інформаційною роз'єднаністю. У багатьох випадках комунікація відбувається через соціальні мережі, месенджери або приватні канали, що ускладнює процес систематизації запитів, призводить до дублювання роботи та втрати часу. Відсутність структурованої бази волонтерських можливостей також створює бар'єри для нових учасників руху, які не завжди можуть швидко знайти спосіб долучитися. Це призводить до зниження ефективності координації та результату волонтерської діяльності.

У контексті сучасних викликів, особливого значення набуває цифровізація соціальних сервісів. Дослідження Ігнатенко К. та Садзаглішвілі Ш. показують, що цифровізація соціальних сервісів під час війни суттєво покращує координацію допомоги та взаємодію між громадським сектором і тими, хто потребує підтримки [2]. Дане дослідження зумовлене необхідністю забезпечити швидкий та зрозумілий процес підтримки суспільства за допомогою оптимізації волонтерських процесів. Створення спеціалізованої платформи дозволило відповідати темпам української цифровізації та оптимізувати використання людських ресурсів і часу. Теоретична значущість роботи полягає у формуванні підходів до створення ефективного цифрового інструменту для підтримки волонтерського руху, а практична у зміцненні стійкості громадських організацій, підвищенні координаційної ефективності та скороченні часу на організацію волонтерської діяльності.

Метою дослідження є обґрунтування доцільності та розробка веб-платформи, що забезпечує процеси організації та координації волонтерської діяльності в Україні під час війни.

У межах дослідження використано методи системного аналізу, порівняльного аналізу та інструменти інформаційного моделювання.

Особливу увагу було приділено вивченню користувацьких сценаріїв, типових процесів волонтерської взаємодії та способів пошуку волонтерських можливостей. Аналіз існуючих рішень дозволив визначити їхні сильні сторони та недоліки, що стало основою для формування оптимальної структури платформи та вибору найбільш ефективних функціональних модулів.

Платформа реалізована на основі монолітної архітектури з використанням PHP на базі фреймворку Laravel для бекенд-частини, HTML5, CSS3, JavaScript з використанням Vite для клієнської частини. Система включає покроковий модуль створення волонтерських ініціатив і алгоритм багатофакторного пошуку, який зіставляє навички та місцезнаходження волонтера з вимогами оголошення, забезпечуючи високу релевантність результатів. Додаткові фільтри дозволяють уточнювати вибірку оголошень за конкретними параметрами.

У результаті проведеного дослідження обґрунтовано доцільність та розроблено веб-платформу для розміщення та пошуку волонтерських ініціатив, спрямовану на підвищення ефективності організації та координації волонтерської діяльності в Україні в умовах воєнного часу.

Перспективним напрямом подальшого розвитку веб-платформи є її інтеграція з державними сервісами та інформаційними реєстрами, що сприятиме підвищенню прозорості та достовірності даних, розширить функціональні можливості системи, а також сприятиме поглибленню взаємодії між громадським сектором і державними структурами у сфері волонтерської діяльності.

Список використаних джерел:

1. Фонд «Демократичні ініціативи» імені Ілька Кучеріва. Скільки українців стали волонтерами після вторгнення РФ: результати соцопитування. УНІАН, 02.03.2023. (дата звернення: 13.10.2025). URL: https://www.unian.ua/society/skilki-ukrajinciv-stali-volonterami-pislya-vtorgnennya-rf-rezultati-socopituvannya-12735249.html

2. Катерина Ігнатенко, Шорена Садзаглішвілі. The digitalization of social services in response to the war in Ukraine. Social Work and Education. 2023 (дата звернення: 16.10.2025). URL: https://journals.uran.ua/swe/article/view/286626

УДК 004.7

Олійник А.В., магістрант,
Сагайдак В., доктор філософії
Державний університет інформаційно-комунікаційних технологій

АВТОМАТИЗОВАНА СИСТЕМА КОМПЛЕКСНОГО КОНТРОЛЮ ПЛОДОВИХ КУЛЬТУР ІЗ ЗАСТОСУВАННЯМ КОМП'ЮТЕРНОГО ЗОРУ ТА ІНТЕЛЕКТУАЛЬНИХ АЛГОРИТМІВ

Вступ. Фруктові сади та ягідні поля потребують регулярного догляду, включаючи боротьбу з бур'янами та шкідниками, своєчасний полив, спостереження за станом рослин та збір фруктів. Сучасні технології комп'ютерного зору та штучного інтелекту створюють автоматизовані системи для ефективного та послідовного виконання завдань. Ці системи зменшують необхідні витрати праці, можуть швидко реагувати на проблеми та покращувати якість продукції. У цьому звіті наведено приклади практичного застосування комп'ютерного зору та штучного інтелекту у вирощуванні фруктів та овочів.

Проблеми. Традиційний збір фруктів та управління садами значною мірою залежать від людської праці. Полуницю та яблука зазвичай збирають працівники вручну, що є трудомісткою та дорогою працею. Автоматизація цих завдань вимагає технологій, які можуть надійно ідентифікувати фрукти та рослини, орієнтуватися між рядами, оцінювати стиглість плодів та відрізняти корисні рослини від бур'янів. Також буде потрібен моніторинг стану ґрунту та рослин у режимі реального часу, включаючи вологість, поживні речовини та хвороби.

Опис системи та приклади застосування. Автоматизована система догляду за садом передбачає використання мобільного робота, оснащеного камерами та датчиками, комп'ютерної системи на основі штучного інтелекту та механізмів дії, таких як маніпулятори, форсунки, обприскувачі та системи зрошення. Комп'ютерний зір дозволяє камерам та датчикам виявляти плоди, оцінювати їх стиглість та ідентифікувати бур'яни або листя, що хворі. Алгоритми аналізують усі зображення та дані для прийняття рішень, таких як збирання фруктів чи активація зрошення, та керують роботизованим обладнанням.

Прикладами роботів для збору фруктів є американський робот Harvest CROO, який автоматично збирає полуницю. Він містить 3D-датчики сканування та камери, які знаходять точне місцезнаходження ягід та збирають стиглі. Цей робот використовує алгоритми штучного інтелекту для оцінки стиглості плодів та обережного відділення їх від

рослини. Іншим прикладом є FFRobotics з Ізраїлю, яка створила робота-збирача яблук, що складається з людської руки, що підвищує продуктивність у десять разів порівняно з ручним збиранням. У США Вашингтонський університет розробив мобільного робота, який збирає полуницю. Цей робот використовує камеру зі штучним інтелектом, м'які захоплювачі та вентилятор, щоб здувати листя, що дозволяє йому дістатися до ягід, прихованих під ними. Це дозволило йому успішно знаходити 80% ягід та покращувати ефективність збору врожаю за допомогою повітряних струменів. Літаючі роботи. Зараз проводяться випробування безпілотних літальних апаратів для збору фруктів. Прикладом є ізраїльський стартап Tevel та чилійська сільськогосподарська компанія Unifrutti, які розробляють літаючих роботів для збору яблук.

Літаючі роботи працюють цілодобово, оскільки отримують енергію від базової платформи. Контролер зі штучним інтелектом переглядає фотографії яблук і дає роботу команду збирати лише тоді, коли фрукти досягають потрібної стадії стиглості та не мають пошкоджень. Повітряні присоски збирають фрукти, щоб мінімізувати пошкодження. Інша роботизована установка Tevel, Darwin Harvesting, розміщує вісім автономних дронів на одній платформі на землі. Таким чином, можливий ретельний збір високоякісних фруктів, особливо у великих садах. Роботи Tevel використовують штучний інтелект, комп'ютерний зір та алгоритми машинного навчання, щоб залишатися гнучкими та продуктивними вдень і вночі. Багатофункціональні сільськогосподарські роботи.

Багатоцільові пристрої виконують такі завдання, як прополювання або обробіток ґрунту. Наприклад, італійська компанія Earth Automations розробила гусеничного робота Dood для виноградників та садів. Він може переміщатися між рядами, орієнтуватися та уникати перешкод за допомогою стереокамер та алгоритмів комп'ютерного зору. Робот здатний перевозити стандартне навісне обладнання, таке як обприскувачі або плуги, і працює або на електриці, або на дизельному паливі. Фермери в Європі та США вже можуть використовувати це рішення. Аналогічно, робот для видалення бур'янів від Carbon Robotics розпізнає бур'яни за допомогою камер та знищує їх лазером. Одна або кілька камер виявляють небажані рослини, а потужні лазери знищують бур'яни за дуже короткий час, до сотень тисяч з них на годину. Модулі комп'ютерного зору також були встановлені на культиватори для просапних культур для вибіркової обробки в рядках.

Сортування та пакування. Сортування та калібрування фруктів в основному виконується комп'ютерами з використанням системи зору. Наприклад, автоматизована сортувальна лінія використовує камери для

оцінки кольору, форми та розміру фруктів у русі, розділяючи їх на дефектні або нестандартні категорії. Розмір та форма фруктів у русі класифікуються на дефектні або нестандартні категорії. Українські виробники вже використовують оптичні сортувальники на основі штучного інтелекту для покращення якості продукції. Таким чином, ця система пришвидшує процес пакування та забезпечує однорідний розмір і колір продукції.

Переваги системи та перспективи впровадження. Комп'ютерний зір в автоматизованих системах пропонує численні переваги. По-перше, ця система значно знижує витрати на робочу силу. Роботи потребують менше робочої сили для збору врожаю та обробки і можуть бути дуже важливими під час сезонного дефіциту робочої сили. Наприклад, робот Harvest CROO допоміг фермеру з 850 акрами саду та зменшив його витрати на робочу силу, які перевищували 50 доларів на годину.

Система працює безперебійно, оскільки роботи ніколи не втомлюються і тому не потребують перерв. Вони демонструють однакову швидкість і точність у виконанні завдань, незалежно від умов роботи. По-третє, автоматизація підвищує якість продукції. Алгоритми штучного інтелекту можуть вибирати лише стиглі плоди для збору врожаю, не пошкоджуючи інші. Наприклад, дрони Tevel вибірково збирають яблука; отже, будуть зібрані лише стиглі та неушкоджені плоди. Важко підтримувати таку якість вручну на великих садах.

По-четверте, сенсори та системи зору дозволяють виявляти хвороби сільськогосподарських культур та дефіцит поживних речовин на ранній стадії. Швейцарська система PhytlSigns аналізує електричні імпульсні сигнали рослин за допомогою машинного навчання та швидко визначає стресові фактори, такі як посуха, зараження або дефіцит добрив, які неможливо побачити неозброєним оком. Таким чином, можна відповідно налаштувати зрошення та внесення добрив, уникаючи значних втрат.

Економічний вплив. У практичних випробуваннях автоматизовані системи продемонстрували економію ресурсів. Наприклад, комп'ютеризована система зрошення на основі штучного інтелекту, що використовується в проекті Vineland-LetsGrow, зменшила споживання води в теплицях на 15%, заощаджуючи приблизно 2800 доларів США на акр щорічно завдяки автоматизації рутинних завдань. Аналогічно, використання роботів для обприскування зменшує використання пестицидів, а роботи для прополювання скорочують використання гербіцидів. За словами експертів, впровадження робототехніки в садівництві може знизити ціни на фрукти на 20-30%, одночасно підвищуючи врожайність та якість. Перспективи в Україні Автоматизація в українському садівничому секторі все ще є дуже

новою. Незважаючи на це, попит на механізовані рішення зростає. Представники аграрної галузі виявляють великий інтерес до імпорту та тестування цих технологій. Обговорюються проекти інтеграції роботів на великих фермах та дослідження датчиків штучного зору місцевими науковими установами. Програми державної підтримки інновацій, такі як безповоротні гранти для сільськогосподарських стартапів, також можуть прискорити процес місцевого розвитку. Навчальні послуги з робототехніки для фермерів та місцевого виробництва (ремонт та обслуговування) є не менш важливими.

Висновки. Таким чином, автоматизована система догляду за плодовими культурами на основі комп'ютерного зору та штучного інтелекту допомагає фермерам підвищити ефективність та покращити якість вирощування фруктів. Ці системи ідентифікують фрукти та бур'яни, оцінюють стан рослин та приймають рішення щодо збору врожаю або переробки; відповідні дії здійснюють роботизовані модулі. Успіх таких рішень вже продемонстровано в США, Ізраїлі та Європі. Роботи фірм Harvest CROO та FFRobotics збирають ягоди та яблука відповідно. Дрони Tevel вибірково збирають фрукти в садах. Платформи виконують прополювання та культивацію садів за допомогою роботів, таких як Dood. Більше того, завдяки датчикам та системам на основі штучного інтелекту, стрес та хвороби можна виявити набагато раніше, що зменшує втрати врожаю. Впровадження цих технологій у місцеві сади дозволяє підвищити продуктивність та конкурентоспроможність вітчизняних виробників фруктів та овочів на світовому ринку.

Список використаних джерел:

1. Robotic harvester uses AI vision and soft grippers to pick hidden strawberries. Phys.org, 04.09.2025. Режим доступу: https://phys.org/news/2025-09-robotic-harvester-ai-vision-soft.html
2. Harvest CROO Robotics – Strawberry Harvesting Solutions. Офіційний сайт, 2024–2025. Режим доступу: https://www.harvestcroorobotics.com/
3. FFRobotics – The Future of Fresh Fruit Harvest. Офіційний сайт, 2020. Режим доступу: https://www.ffrobotics.com/
4. «Рій дронів з ШІ збирає стиглі яблука…». TONETO.net, 07.07.2023 (з посиланням на Tevel і Unifrutti). Режим доступу: https://toneto.net/news/tehnologii/...sobiraet-spelie-yabloki...
5. «Штучний інтелект допомагає збирати врожаї яблук». Останній Бастіон, 13.07.2023 (Tevel, Чилі). Режим доступу: https://bastion.tv/.../shtuchnij-intelekt...yabluk_n56089
6. «Теплиці почали поливати за допомогою штучного інтелекту». AgroTimes, 15.01.2020. Режим доступу: https://agrotimes.ua/tehnika/teplyczi-pochaly-polyvaty-za-dopomogoyu-shtuchnogo-intelektu/
7. «Автономний гусеничний робот Dood працює у садах». AgroTimes, 02.02.2023. Режим доступу: https://agrotimes.ua/tehnika/avtonomnyj-gusenychnyj-robot-dood-praczyuye-u-sadah/
8. PhytlSigns – Insights into Crop Stress. Vivent Biosignals, 2021. Режим доступу:

УДК 004

Грушевицький В.В., здобувач,
Українець М.О., асистент
Державний університет "Житомирська політехніка"

ПОРІВНЯННЯ ТЕХНОЛОГІЙ РЕАЛІЗАЦІЇ МУЛЬТИПЛЕЄРНОГО РЕЖИМУ ДЛЯ ГРИ ЖАНРУ REAL-TIME STRATEGY НА РУШІЮ UNITY

Наразі одним з найбільш поширених способів розваг серед людей різного віку є мультиплеєрні онлайн ігри, які залучають мільйонів гравців по всьому світу. Стратегічні ігри у реальному часі, як один із класичних жанрів, зберігають стабільний попит завдяки високій динаміці, необхідністю тактичного мислення та постійній взаємодії між гравцями. Упровадження мультиплеєрного режиму в іграх цього жанру дозволяє створити конкурентний і непередбачуваний ігровий процес, та розширити варіативність сценаріїв ігрових сесій. Актуальною проблемою є визначення оптимального підходу для реалізації багатокористувацького режиму з урахуванням особливостей жанру RTS.

Метою дослідження є порівняння технологій реалізації мультиплеєрного режиму для визначення найбільш оптимального рішення для гри жанру Real-time strategy (RTS) на рушію Unity.

В першу чергу слід визначити критерії порівняння, які є важливими для реалізації мультиплеєрного режиму в грі жанру RTS. Для порівняння технологій було обрано п'ять ключових параметрів: тип ліцензії визначає економічну доцільність, мережева модель впливає на безпеку та архітектуру, продуктивність оцінюється на основі здатності архітектури обробляти велику кількість об'єктів, хостинг визначає варіанти розгортання серверів, а основа синхронізації відповідає за технічний метод узгодження стану світу.

Розглянуто три популярні технології такі як: Photon Fusion, Mirror та Unity Netcode for GameObjects. Порівнюючи продуктивність було виявлено перевагу Photon Fusion над аналогами у контексті RTS завдяки tick-based архітектурі, яка значно ефективніше синхронізує сотні юнітів, ніж state-based підходи конкурентів [2]. Unity Netcode for GameObjects, хоча і перевершує Mirror за базовою швидкістю, все ж поступається Photon Fusion у стабільності при значному масштабуванні сцени [1]. У свою чергу, Mirror є найменш продуктивним, вимагаючи складної ручної оптимізації коду, для роботи у високонавантаженому середовищі [3].

Результати проведеного порівняння наведено в таблиці 1.

Таблиця 1. Порівняння технологій мультиплеєра для Unity

Критерій / Технологія	Photon Fusion	Mirror	Netcode for GameObjects
Тип ліцензії	Комерційна (наявний безкоштовний план з обмеженнями)	Open-source, безкоштовна	Безкоштовна
Мережева модель	Server Authoritative, Client Prediction, Shared Authority	Host-Client, Server Authoritative, Client Authoritative	Server Authoritative, Host-Client
Хостинг	Dedicated / Host / Shared	Dedicated / Host	Dedicated / Host
Основа синхронізації	Tick-based (пакети, прив'язані до симуляційних кроків)	State/Event-based (SyncVars, RPC)	State/Event-based (NetworkVariables, RPC)

Окрім показників швидкодії, кожна технологія має унікальний баланс функціональних можливостей та обмежень. Так, Mirror забезпечує повний контроль над архітектурою та нульову вартість ліцензії, проте вимагає трудомісткого ручного налаштування зовнішніх сервісів [3]. Unity Netcode for GameObjects має офіційну підтримку та інтеграцію з екосистемою Unity, однак залежність від сервісів UGS створює можливість додаткових витрат [1]. Натомість Photon Fusion пропонує найбільш досконалий технологічний стек (Prediction/ Rollback) для плавної симуляції RTS, але його головним недоліком є висока вартість при масштабуванні кількості гравців[1].

На основі проведеного порівняння було встановлено, що Photon Fusion є найбільш оптимальним рішенням для реалізації мультиплеєра в грі жанру RTS завдяки високій продуктивності, наявності технологій прогнозування та корекції стану, а також продуктивності при роботі з великими обсягами мережевих даних, характерних для RTS-проєктів.

Список використаних джерел:

1. Unity - Manual: Multiplayer. Unity - Manual: Multiplayer. URL: https://docs-multiplayer.unity3d.com/ (дата звернення: 20.11.2025).

2. Fusion | Photon Engine. Fusion 2 - Fusion 2 Introduction | Photon Engine. URL: https://doc.photonengine.com/fusion/current/fusion-2-intro (дата звернення: 20.11.2025).

3. Engelbrecht D. Building Multiplayer Games in Unity. Berkeley, CA : Apress, 2022. URL: https://doi.org/10.1007/978-1-4842-7474-3 (дата звернення: 20.11.2025).

УДК 004.94

Олексюк О.С., магістрант
Марчук Г.В., ст. викладач
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ГІБРИДНОГО АЛГОРИТМУ ПЛАНУВАННЯ ТРАЄКТОРІЇ ЛЕТАЛЬНОГО АПАРАТА

Планування траєкторії - ключове завдання автоматизованого керування літальними апаратами. Воно передбачає пошук оптимального маршруту, що забезпечує досягнення мети з урахуванням динамічних обмежень (швидкість, прискорення, кути крену). Актуальність проблеми полягає в необхідності створення ефективних алгоритмів, здатних будувати траєкторію в режимі реального часу, враховуючи як динаміку самого літального апарату, так і навколишнє середовище [1]. Дослідження зосереджено на аналізі та математичному обґрунтуванні гібридного алгоритму планування траєкторії, що поєднує кінодинамічний підхід з критеріями енергетичної ефективності та мінімізації стохастичного ризику.

Основна увага зосереджена на дослідженні гібридного алгоритму планування траєкторії, який поєднує кінодинамічний підхід із критеріями енергоефективності та мінімізації стохастичних ризиків. Метод об'єднує аналітичні моделі руху з евристичними алгоритмами для пошуку оптимальної траєкторії з урахуванням динаміки літака та зовнішньої невизначеності. Такий підхід забезпечує адаптивність системи до змінних умов середовища, зокрема поривів вітру, турбулентності, падіння уламків чи рухомих перешкод.

Керування рухом літального апарату формально описується диференціальним рівнянням:

$$\dot{x} = f(x, u, t), \qquad (1)$$

де x - вектор стану, що включає просторову позицію та кути орієнтації, а керуючі дії u, які формують траєкторію $x(t)$, визначаються тягою та аеродинамічними кутами.

Задача планування траєкторії полягає у визначенні оптимальної траєкторії $x(t)$ у тривимірному просторі, який проходить через область F (вільну від перешкод), тобто $x(t) \in F$, і з'єднує початковий x_0 та кінцевий x_f стани.

Оптимізація прогнозованої траєкторії здійснюється за кількома критеріями. Загальна цільова функція (J_{total}) мінімізує енергоспоживання (J_{energy}), мінімізує ризик зіткнення (J_{risk}) та враховує час польоту (J_{time}):

$$J_{total} = \lambda_1 J_{energy} + \lambda_2 J_{risk} + \lambda_3 J_{time}, \qquad (2)$$

де вагові коефіцієнти λ_i визначають пріоритет кожного критерію.

Алгоритми планування траєкторії поділяються на два класи. Перший - дискретні методи (алгоритми Дейкстри та A*), що будують шлях за графовими моделями та ефективні у статичних середовищах, але не враховують фізичні обмеження руху (наприклад, динаміку швидкості та прискорення). Другий клас - кінодинамічні алгоритми (RRT, RRT*), що забезпечують реалістичне моделювання, оскільки враховують динаміку об'єкта. В умовах невизначеності планування потребує мінімізації ризику, що гарантує стійкість шляху. Також важливо враховувати аеродинамічні характеристики летального апарату, що підвищить точність моделювання польоту [2].

В результаті аналізу встановлено, що поєднання евристичних методів із кінодинамічним плануванням дає змогу будувати траєкторії з урахуванням динаміки руху літального апарата. Ці алгоритми забезпечують мінімізацію енерговитрат та зменшення ризику зіткнення шляхом оптимізації траєкторії з урахуванням стохастичних відхилень і завдяки такому поєднанню формуються надійні та стабільні траєкторії, що знижують енергоспоживання та підвищують ефективність автономного керування літальними апаратами. Цей підхід також придатний для симуляції польотів у віртуальному середовищі, де важливими є фізична правдоподібність руху та обчислювальна ефективність алгоритму.

Теоретична та практична цінність роботи з погляду авторів полягає в сприянні розвитку напрямку кінодинамічного планування, що враховує невизначеність і аеродинамічні чинники. Крім того, результати дослідження можуть бути інтегровані в системи автономного пілотування та симуляційні платформи для підвищення фізичної достовірності моделювання руху літальних апаратів у складних умовах. Надалі передбачено удосконалити способи з метою інтеграції методів нейронних мереж для прогнозування траєкторії, що дозволить адаптувати алгоритм до різних типів літаків.

Список використаної літератури:

1. Poissant, D. A., Desbiens, A. L., Ferland, F., & Petit, L. (2025). ARENA: Adaptive Risk-aware and Energy-efficient NAvigation for Multi-Objective 3D Infrastructure Inspection with a UAV. *arXiv preprint arXiv:2502.19401*.

2. Airlangga, G., Bata, J., Adi Nugroho, O. I., Sugianto, L. F., Saputro, P. H., & Makin, S. J. (2025). Enhanced Advanced Multi-Objective Path Planning (EAMOPP) for UAV Navigation in Complex Dynamic 3D Environments. *International Journal of Robotics & Control Systems, 5*(2).

УДК 004.8

Дяченко Д.О., здобувач,
Державний університет
інформаційно-комунікаційних технологій

МЕТОДИ ПОБУДОВИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПЕРСОНАЛІЗОВАНОГО НАВЧАННЯ З ВИКОРИСТАННЯМ АЛГОРИТМІВ АДАПТАЦІЇ ТА ШТУЧНОГО ІНТЕЛЕКТУ

Перехід освіти у цифровий формат суттєво змінив вимоги до організації навчального процесу. Якщо раніше електронні курси слугували лише допоміжним інструментом, то сьогодні вони стають основним середовищем взаємодії студентів із навчальним матеріалом. У таких умовах постає потреба не лише у наданні доступу до навчальних ресурсів, а й у створенні систем, здатних адаптуватися під індивідуальні особливості кожного користувача. Різний рівень попередньої підготовки, різні стилі навчання, швидкість засвоєння інформації та навіть мотиваційні чинники роблять традиційний підхід «однаковий курс для всіх» малоефективним. Це особливо помітно в технічних дисциплінах, де складність матеріалу може змінюватися дуже нерівномірно, а помилки на ранніх етапах спричиняють труднощі в подальшому навчанні.

Проблема, яку необхідно вирішити, полягає у створенні інформаційної системи персоналізованого навчання, здатної автоматично визначати індивідуальні параметри користувача та будувати оптимальну освітню траєкторію. Така система має враховувати як явні дані (результати тестів, виконання завдань, час проходження модулів), так і приховані патерни поведінки, які складно оцінити без застосування методів штучного інтелекту.

Метою дослідження є розроблення та обґрунтування методів побудови адаптивної інформаційної системи навчання, що використовує алгоритми машинного навчання й моделі штучного інтелекту для персоналізації навчального процесу. До завдань дослідження входить аналіз існуючих підходів до адаптивного навчання, порівняння моделей оцінювання користувачів, визначення найбільш ефективних алгоритмів для побудови навчальних рекомендацій, а також розробка загальної структурної моделі системи.

У ході роботи, на основі аналізу було створено загальну архітектуру інформаційної системи персоналізованого навчання. Вона містить модуль збору даних, у якому фіксується поведінка користувача: правильність відповідей, час реагування, кількість повторів, активність у середовищі. Аналітичний модуль здійснює попередню обробку даних

і передає їх у блок адаптації, де відбувається побудова рекомендацій. Інтерфейс користувача надає навчальні матеріали відповідно до обраної моделі адаптації. Особливої уваги потребує модуль зворотного зв'язку, що дозволяє системі уточнювати свою модель користувача та покращувати рекомендації.

Під час створення прототипу було випробувано можливість адаптації навчання не лише на основі традиційних даних, а й на основі поведінкових індикаторів. Наприклад, швидкість гортання тексту, тривалість зупинок над складними фрагментами, час між неправильними відповідями, частота перемикання між типами контенту — усе це дозволяє визначити глибину розуміння матеріалу. Результати попереднього тестування продемонстрували, що система, яка враховує поведінкові параметри, значно точніше визначає рівень підготовки студентів і може пропонувати більш релевантні завдання.

У висновках варто зазначити, що використання алгоритмів адаптації та штучного інтелекту у побудові інформаційних систем навчання є перспективним напрямом, який дозволяє враховувати особливості кожного користувача, забезпечує гнучкість подачі матеріалу та створює комфортні умови для самостійного навчання.

Подальші напрями роботи пов’язані з удосконаленням моделей адаптації, зокрема інтеграцією нейромережевих підходів для глибшого аналізу навчальної поведінки, автоматичним визначенням стилю навчання нового користувача, а також врахуванням емоційних параметрів, отриманих на основі аналізу темпу роботи, пауз і патернів помилок. Додавання цих можливостей дозволить створити комплексну адаптивну систему, яка буде здатна не лише коригувати складність навчального контенту, а й підтримувати користувача в періоди високого навантаження та зниження мотивації.

Список використаних джерел:

1. Биков В. Ю., Спірін О. М., Пінчук О. П. Адаптивні інформаційні технології в освіті: стан і перспективи розвитку. Інформаційні технології і засоби навчання, 2019. С. 11-19. (дата звернення: 15.11.2025).

2. Кравчина О. Є. Персоналізація навчального процесу в електронному освітньому середовищі. *Інформаційні технології і засоби навчання*, 2017. С. 80-92 (дата звернення: 20.11.2025).

УДК 004.4

Субчак Ю.Ю. здобувач,
Марчук Г.В., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ ФУНКЦІОНАЛЬНИХ ВИМОГ ТА ІНСТРУМЕНТІВ РОЗРОБКИ МОБІЛЬНОГО ЗАСТОСУНКУ «ZHYTOMYR TRAVEL»

У сучасному туристичному середовищі мобільні застосунки відіграють ключову роль у взаємодії мешканців та гостей міста з його інфраструктурою. Для міст, що активно розвивають внутрішній туризм, створення інструментів цифрової навігації є не лише сервісною функцією, а й елементом брендування та ефективної популяризації локальних локацій. Саме тому розробка мобільного застосунку «Zhytomyr Travel», спрямованого на гейміфікацію туристичного досвіду, потребує глибокого аналізу функціональних вимог, обґрунтованого вибору технологій та побудови ефективних інтерактивних сценаріїв користувача [1].

Основою для формування детальних вимог до проєкту стали User Stories та Use Cases, які всебічно описують поведінку користувачів у різних сценаріях взаємодії: від першого запуску програми та ознайомлення з можливостями до виконання завдань, налаштування профілю та роботи з внутрішньою системою винагород - "житокоїнами". Система охоплює дві ключові групи користувачів: кінцевих користувачів, якими є відвідувачі та мешканці міста, та адміністраторів контенту, які забезпечують актуальність інформації. Для кінцевого користувача реалізується розгалужений функціонал, що включає онбординг, вибір стартового району міста або автоматичне визначення району за допомогою GPS, а також перегляд інтерактивної карти районів із чітким поділом на розблоковані та заблоковані з відповідними умовами доступу. Гейміфікація [2, 3, 4] досягається через виконання місій трьох рівнів складності, що можуть бути геолокаційними, заснованими на скануванні QR-кодів або потребувати надання текстових відповідей. Найважливішим мотиваційним елементом є система нагороди у вигляді "житокоїнів", які користувачі можуть витрачати на розблокування нових районів або отримання партнерських знижок. У цьому контексті критично важливим є не лише впровадження валюти, а й детальний аналіз її економічної моделі, що включає розрахунок адекватної винагороди за місії різної складності та встановлення збалансованих цін на витрати, задля підтримання довгострокової залученості та запобігання віртуальній інфляції.

Додатковий функціонал для користувача включає перегляд профілю, досягнень, виконаних завдань та можливість редагування персональної інформації.

Рисунок 1 деталізує архітектуру проєкту, розкриваючи ключові системні потоки: від взаємодії користувачів та функціонального наповнення карти, до циклу виконання місій і централізованого управління системою винагород через "житокоїни".

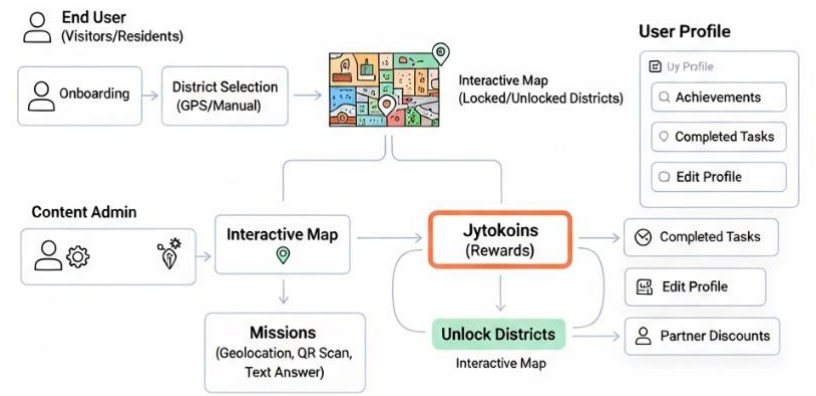


Рисунок 1 – Схема взаємодії ключових елементів проєкту

З боку управління контентом, адмін-панель забезпечує повний контроль над ключовим контентом: туристичними локаціями, подіями, завданнями, районами, партнерськими пропозиціями, досягненнями та преміям-підписками. Важливими також є модулі модерації користувацького контенту, який може генеруватися учасниками, та функція перегляду аналітики щодо активності користувачів, що дозволяє оптимізувати ігрові механіки.

З технічної точки зору, застосунок доцільно будувати на кросплатформенній технології, як-от Flutter або React Native [5, 6], що забезпечує одночасну підтримку мобільних операційних систем Android та iOS, скорочуючи терміни розробки та витрати. Для ефективної реалізації картографічних можливостей існують дві оптимальні опції: використання Google Maps API або OpenStreetMap. Вибір між ними повинен ґрунтуватися на порівняльному аналізі вартості ліцензування, точності локальних даних та простоти інтеграції функцій геозонування (Geofencing), необхідних для активації місій. Бекенд-частина може бути реалізована на Node.js із використанням Firebase або стандартного REST API, яке застосовується для авторизації

користувачів, збереження їхнього прогресу, обліку "житокоїнів", завдань та аналітики.

Особливе значення в архітектурі має забезпечення високих нефункціональних вимог. До них належить гарантування синхронізації прогресу між різними сесіями користувача та захист персональних даних, що вимагає уважного підходу до вибору структури бази даних та логіки взаємодії між клієнтською і серверною частинами. З огляду на природу геолокаційних місій, критичним аспектом є безпека: необхідний аналіз та впровадження механізмів запобігання фальсифікації GPS-координат (GPS spoofing) для забезпечення чесності отримання винагороди, а також коректна обробка QR-кодів.

Таким чином, комплексний аналіз інструментів і функціональних вимог дозволив сформувати цілісну, гнучку та надійну архітектуру мобільного застосунку «Zhytomyr Travel». Цей застосунок сприятиме цифровій трансформації туристичної інфраструктури Житомира та підвищенню залученості користувачів через інноваційні ігрові механіки, інтерактивні локації та мотивуючу систему винагород.

Список використаних джерел:

1. Vakaliuk, T. A., Marchuk, G. V., Levkivskyi, V. L., Morgun, A. M., & Kuznietsov, D. V. (2021, December). Development of AR Application to Promote the Historical Past of the Native Land. In *Digital Humanities Workshop* (pp. 125-131).

2. Янчук, Т., & Фурман, Т. (2024). Гейміфікація у електронній комерції: новий спосіб залучення клієнтів. *Економіка та суспільство*, (70). https://doi.org/10.32782/2524-0072/2024-70-56.

3. Romat, Y., & Biliavska, Y. (2020). Гейміфікація та її сприйняття поколінням «Z». *Scientific Notes of Ostroh Academy National University," Economics" Series*, (17 (45)), 23-28.

4. Деділова, Т., Юрченко, О., & Кононенко, Я. (2023). Гейміфікація як соціальний феномен і тренд сучасного маркетингу. *Проблеми і перспективи розвитку підприємництва*, (31), 54-63.

5. Gülcüoğlu, Ekrem & Ustun, Ahmet & Seyhan, Neşet. (2021). Comparison of Flutter and React Native Platforms. *Journal of Internet Applications and Management*. DOI:10.34231/iuyd.888243

6. Hossain, S., Rahman, M., & Rahman, M. (2023). The Evolution of Mobile Application Development Frameworks: A Comprehensive Study on React Native, Flutter, and Native. *IEEE Access*, 11, 105670-105682.

УДК 004.93:629.33

Панченко В.Ю., магістрант,
Ткаленко О.М., к.т.н, доцент
Державний університет
інформаційно-комунікаційних технологій

РОЛЬ ВЕЛИКИХ ДАНИХ (BIG DATA) У НАВЧАННІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ (LLM)

Стрімкий розвиток технологій штучного інтелекту в останні роки докорінно змінив ландшафт інформаційних систем, вивівши на передній план великі мовні моделі (LLM). Від автоматизації рутинних процесів до вирішення креативних задач — ці системи демонструють рівень компетенції, який раніше вважався доступним лише людині. Проте за лаштунками архітектурних проривів стоїть фундамент, без якого цей прогрес був би неможливим — дані. Саме симбіоз обчислювальних потужностей та безпрецедентних масивів інформації (Big Data) став каталізатором нової ери в машинному навчанні. У цьому контексті дослідження взаємозв'язку між характеристиками даних та можливостями моделей набуває особливої актуальності.

Постановка завдання

Великі мовні моделі (LLM), такі як GPT, Claude та LLaMA, демонструють безпрецедентні можливості у розумінні та генерації людської мови. Їхній успіх зумовлений не лише вдосконаленням архітектур (наприклад, Transformer), але й експоненційним зростанням обсягів навчальних даних. Розуміння того, як саме характеристики «великих даних» - обсяг, різноманітність та якість - впливають на кінцеві можливості моделей, є критичним завданням для подальшого розвитку галузі.

Мета дослідження

Аналіз кількісного та якісного впливу великих наборів даних (Big Data) на продуктивність, здатність до узагальнення, безпеку та появу «надзвичайних» (emergent) властивостей у сучасних великих мовних моделей.

Результат дослідження

Дослідження підтверджує, що парадигма «великих даних» є фундаментальною для сучасних LLM. Ключовим відкриттям є так звані «закони масштабування» (scaling laws), які демонструють чітку, прогнозовану залежність між збільшенням обсягу навчального корпусу (вимірюваного у трильйонах токенів) та покращенням продуктивності

моделі [1]. Справа не лише в запам'ятовуванні фактів; більші дані дозволяють моделям краще засвоювати складні синтаксичні конструкції, контекстуальні зв'язки та нюанси мови. Однак обсяг не єдиний фактор.

Критично важливою є різноманітність даних. Моделі, навчені на широкому спектрі джерел (книги, наукові статті, програмний код, діалоги, веб-сторінки), демонструють значно кращу здатність до узагальнення та виконання завдань "нульового пострілу" (zero-shot) у нових доменах [2]. Водночас якість даних напряму впливає на надійність та безпеку моделі.

Проблеми "сміття на вході - сміття на виході" (GIGO) є гострими: токсичний, упереджений або фактично неточний контент у навчальних даних неминуче відтворюється моделлю. Тому процеси курування та фільтрації даних, хоча й надзвичайно ресурсомісткі, стають не менш важливими, ніж сама архітектура моделі, для зменшення галюцинацій та небажаної поведінки [3].

Висновки та перспективи

Великі дані є «паливом» для великих мовних моделей. Їхня ефективність прямо залежить від обсягу, різноманітності та, що найважливіше, якості цього палива. Майбутні дослідження будуть зосереджені на розробці ефективніших методів курування даних, використанні синтетичних даних для заповнення прогалин у знаннях та вирішенні етичних проблем, пов'язаних із конфіденційністю та упередженістю даних, зібраних у веб-масштабі.

Список використаних джерел:

1. Scaling Laws for Neural Language Models [Електронний ресурс] – Режим доступу: https://medium.com/@aiml_58187/beyond-bigger-models-the-evolution-of-language-model-scaling-laws-d4bc974d3876

2. The Importance of Data Diversity and Quality in LLM Training [Електронний ресурс] – Режим доступу: https://arxiv.org/abs/2506.19262

3. Challenges in Web-Scale Data Curation for AI [Електронний ресурс] – Режим доступу: https://medium.com/@jasoncorso/data-curation-the-beast-behind-every-ai-model-d136eac4da6b

УДК 004.93:629.33

Бовкун О.С., магістрант,
Ткаленко О.М., к.т.н, доцент
Державний університет
інформаційно-комунікаційних технологій

РОЗРОБКА АВТОНОМНОГО МОДУЛЯ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ДЛЯ СИСТЕМИ ЗАПУСКУ АВТОМОБІЛЯ

Традиційні засоби захисту автомобіля (механічні замки, іммобілайзери) поступово втрачають ефективність через розповсюдження засобів електронного злому. Альтернативою є біометрична авторизація, яка прив'язує доступ не до фізичного ключа, а безпосередньо до особи власника. Однак більшість заводських рішень є дорогими та залежними від хмарних сервісів. Тому актуальною є розробка локальної системи розпізнавання обличчя, яку можна інтегрувати в наявний автотранспорт.

Постановка задачі.

Метою роботи є створення програмно-апаратного комплексу на базі мікрокомп'ютера Raspberry Pi, здатного виконувати ідентифікацію водія в реальному часі без підключення до мережі Інтернет. Система повинна керувати реле запалювання, блокуючи двигун у разі несанкціонованого доступу, та бути стійкою до спроб підробки зображення.

Методи та засоби реалізації.

Апаратною основою системи обрано одноплатний комп'ютер Raspberry Pi 4 Model B, який забезпечує достатню продуктивність для задач комп'ютерного зору. Захоплення відеопотоку здійснюється через CSI-інтерфейс камери, що мінімізує затримки передачі даних. Програмний алгоритм реалізовано мовою Python із використанням бібліотек OpenCV та face_recognition. Процес ідентифікації базується на побудові 128-вимірного вектора ознак обличчя (face embedding) та порівнянні його з еталоном за евклідовою відстанню. Для підвищення надійності впроваджено аналіз 68 антропометричних точок, що дозволяє відрізнити реальну людину від фотографії.

Результати дослідження.

Розроблено схему підключення, яка включає модуль гальванічної розв'язки на оптопарі TLP621 та драйвер ULN2803A для керування силовим реле. Це захищає логічні ланцюги мікрокомп'ютера від завад бортової мережі автомобіля. Програмна частина працює за

принципом "чорної скриньки": після подачі живлення система автоматично завантажує базу еталонів, ініціює камеру та переходить у режим сканування. При успішній авторизації (збіг > 75%) на GPIO-пін подається сигнал розблокування. У ході тестування досягнуто стабільної роботи алгоритму зі швидкістю обробки до 10 кадрів на секунду, що є достатнім для комфортної взаємодії з водієм.

Висновки та перспективи

Запропонована система дозволяє реалізувати бюджетний, але ефективний біометричний захист автомобіля. Головною перевагою розробки є повна автономність: обробка даних відбувається локально, що виключає ризик перехоплення інформації та залежність від мобільного покриття. Модульна архітектура дозволяє в майбутньому розширити функціонал, додавши, наприклад, GPS-трекінг або сповіщення власника через GSM-канал.

Список використаних джерел:

1. CMU School of Computer Science. URL: https://www.cs.cmu.edu/~efros/courses/LBMV07/Papers/viola-cvpr-01.pdf (дата звернення: 23.11.2025).
2. GitHub - ageitgey/face_recognition: The world's simplest facial recognition api for Python and the command line. GitHub. URL: https://github.com/ageitgey/face_recognition (дата звернення: 23.11.2025).
3. Raspberry Pi computer hardware. URL: https://www.raspberrypi.com/documentation/computers/raspberry-pi.html (дата звернення: 23.11.2025).

УДК 004.9

Даншина С. Ю., д.т.н., професор,
Проценко А. В. магістрант
Національний аерокосмічний університет
«Харківський авіаційний інститут»

БАГАТОВИМІРНА ГЕОВІЗУАЛЬНА АНАЛІТИКА ТРАНСПОРТНОЇ АВАРІЙНОСТІ З ВИКОРИСТАННЯМ ГІС

Проблема дорожньо-транспортної аварійності залишається однією з найгостріших у сфері громадської безпеки Україні. Так за даними ресурсу [1] у 2024 р. зафіксовано 25 781 випадків дорожньо-транспортних пригод (ДТП) з потерпілими, внаслідок яких загинуло 3 202 людини і травмовано 32 023 особи. Вже за перші сім місяців 2025 р. кількість ДТП з потерпілими сягнула 13 738, в яких загиблі 1 663 особи. При цьому рівень смертності на дорогах України у п'ять разів перевищує середньоєвропейський показники. Тому, у сучасному суспільстві питання безпеки дорожнього руху набувають все більшої актуальності.

Такі тривожні тенденції вказують на нагальну потребу впровадження сучасних аналітичних підходів до оцінки та зменшення аварійності. Зокрема, використання геоінформаційних систем (ГІС), тривимірної візуалізації та просторово-часового аналізу може суттєво підвищити ефективність виявлення «гарячих точок», розроблення заходів дорогоустрою та планування безпечної мережі.

Метою дослідження є підвищення ефективності заходів щодо забезпечення безпеки дорожнього руху, що ґрунтуються на ідентифікації сукупності причин транспортної аварійності шляхом геоінформаційного аналізу дорожньої мережі з використанням просторових і тривимірних моделей і виявлення небезпечних ділянок.

Для досягнення поставленої мети сформовано та вирішено такі задачі дослідження:

- збір та попередня обробка даних про ДТП за певний часовий період;
- геокодування та просторова інтеграція даних у середовищі ГІС;
- класифікація факторів та оцінювання причин аварійності за різними показниками (кількість подій, тяжкість наслідків, тип дорожніх сегментів);
- створення 2D і 3D-візуалізації інтенсивності ДТП з використанням інструментів ArcGIS Pro, зокрема Heat Map, 3D Scene і Space-Time Cube;
- аналіз просторово-часових кластерів аварійності, визначення найбільш небезпечних ділянок доріг;

- розроблення рекомендації щодо практичного застосування під час забезпечення безпеки дорожнього руху.

Узагальнюючи результати розв'язання наведених задач, запропановано метод формування переліку заходів щодо забезпечення безпеки дорожнього руху, що імплементує підходи геоаналітики для отримання ефективних рекомендацій.

Метод складається з двох основних етапів, зокрема:

Етап 1. Оброблення наявних даних транспортної аварійності з урахуванням геопросторовою складової. Цей етап поєднує такі кроки:

- вивчення просторово-часових закономірностей для первинного аналізу даних;
- ідентифікація «гарячих точок» – місць з найбільшою кількістю випадків ДТП для отримання картографічних 2D-моделей;
- аналіз часових даних по ДТП для визначення найнебезпечнішого часового періоду.

Етап 2. Геопросторовий 3D-аналіз транспортної аварійності у поєднанні з даними ДЗЗ. Цей етап поєднує наступні кроки:

- візуалізація даних у 3D-вигляді для визначення проблемних ділянок по роках у тривимірному просторі;
- аналіз проблемних ділянок за даними ДЗЗ на основі принципів дешифруваннння місцевості.
- формування висновків.

Таким чином, сформований метод аналізу транспортної аварійності дорожньої мережі та його реалізація засобами ГІС та 3D-візуалізації дає змогу більш наочно та комплексно оцінювати просторово-часові закономірності ДТП. Застосування сучасних інструментів ArcGIS Pro, таких як Heat Map, Space-Time Cube та 3D Scene, дозволяє не лише виявляти території з підвищеною концентрацією аварій, а й визначити динаміку їх змін у часі. Розроблений метод сприяє підвищенню ефективності прийняття управлінських рішень у сфері дорожньої безпеки, оскільки дозволяє інтегрувати дані про інтенсивність руху, типи доріг та соціально-економічні чинники під час формування заходів щодо забезпечення безпеки дорожнього руху.

Отримані результати можуть бути використані органами місцевого самоврядування, дорожніми службами та аналітичними центрами для моніторингу небезпечних ділянок і планування превентивних заходів з метою зменшення кількості ДТП та смертності на дорогах України.

Список використаних джерел:

1. Новини. *Міністерство внутрішніх справ України*. URL: https://mvs.gov.ua/press-center/news (дата звернення: 12.11.2025).

УДК 004.7

Лупашина А.А., здобувач,
Фант М.О., доцент,
Громський О.О., викл.-практ.,
Нерода С.І., викл.-практ.
Державний університет «Житомирська політехніка»

ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ ПРОЦЕСАМИ СТУДЕНТСЬКОГО ГУРТОЖИТКУ: АРХІТЕКТУРА, ФУНКЦІОНАЛЬНІ МОДУЛІ ТА ПРАКТИЧНІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ Й НАДІЙНОСТІ

Цифрові трансформації в освітніх установах вимагають не лише автоматизації операцій, але й проєктування системи, яка забезпечує високу доступність, зручність для користувачів та стійкість до помилок. Розроблювана інформаційна система для управління гуртожитками орієнтована на комплексне покриття життєвого циклу послуги: від подачі заявки на поселення до виписки та обробки технічних запитів. Основні функціональні модулі включають: реєстрацію та верифікацію студентів, керування житловим фондом (карта кімнат, плани поверхів), механізм бронювання і перенесення місць, обробку скарг і заявок, фінансові операції (оплата проживання, нарахування комунальних), інформування (push/email/SMS) та аналітику заповнюваності.

Архітектурно система побудована на принципах розділення відповідальностей: Presentation (React SPA / PWA), Application (API Gateway, NestJS), Data (PostgreSQL + кешування Redis) та інтеграційного рівня (модулі для зовнішніх сервісів). Для забезпечення швидкої відповіді при вибірках доступних місць і фільтрації використано двошарове збереження: основні транзакційні дані в PostgreSQL та кешування гарячих запитів у Redis. API реалізовано як REST із підтримкою часткового впровадження GraphQL для складних запитів аналітики та динамічних форм.

Окремий акцент зроблено на доступності та UX: інтерфейс спроектовано за принципами WCAG 2.1 (контраст, клавішна навігація, підписи до зображень), а мобільність користування досягається через PWA з можливістю офлайн-режиму для заповнення форм і перегляду раніше завантажених даних. Для інтерфейсних компонентів використано бібліотеки з підтримкою TypeScript, компонентну систему та lazy-loading модулів для пришвидшення початкового завантаження.

Надійність і відновлюваність системи забезпечуються через контейнери Docker, CI/CD пайплайни (GitHub Actions / GitLab CI), автоматизоване розгортання в кластері Kubernetes і політику бекапів

(щоденні дампи PostgreSQL + реплікація). Моніторинг і алертінг реалізовано за допомогою Prometheus + Grafana (метрики продуктивності), а централізоване логування — через ELK-стек (Elasticsearch, Logstash, Kibana). Такий підхід гарантує швидке виявлення деградацій продуктивності та автоматичне масштабування компонентів при зростанні навантаження.

Безпека і захист даних реалізовано комплексно: RBAC на рівні API, аутентифікація через OAuth2 / OpenID Connect або JWT для внутрішніх сервісів; шифрування конфіденційних полів у базі (PGP або поля з клієнтським шифруванням); захист від типових веб-загроз (OWASP Top 10) — CSP, валідація/санітизація введення, параметризовані запити для уникнення SQL-ін'єкцій. Для захисту персональних даних передбачено політику зберігання та видалення даних, журнал аудиту дій користувачів і механізм маскування чутливої інформації. Враховано вимоги конфіденційності та можливість адаптації політик під національне законодавство та європейські стандарти захисту даних.

Система підтримує збір телеметрії, що дозволяє створювати дашборди заповнюваності, швидкості обробки заявок і частоти звернень. Це допомагає прогнозувати потреби гуртожитку.

Реалізація проєкту передбачає застосування методологій тестування: юніт- та інтеграційні тести (Jest), e2e-тести (Cypress), а також перевірки безпеки (SAST/DAST інструменти). Такий комплекс заходів гарантує високу якість та надійність системи на всіх етапах життєвого циклу.

Отже, запропонована інформаційна система поєднує передові практики архітектури, інструменти забезпечення доступності, механізми високої доступності та безпеки, що робить її придатною для широкого впровадження в освітніх закладах та подальшого масштабування для кількох кампусів.

Список використаних джерел:

1. Web Content Accessibility Guidelines (WCAG) 2.1. W3C [Електронний ресурс] – Режим доступу до ресурсу: https://www.w3.org/TR/WCAG21/

2. Overview of entity framework core - EF core. Microsoft Learn: Build skills that open doors in your career [Електронний ресурс] – Режим доступу до ресурсу: https://learn.microsoft.com/en-us/ef/core/

3. Jest — Delightful JavaScript Testing. Facebook Open Source [Електронний ресурс] – Режим доступу до ресурсу: https://jestjs.io/docs/getting-started

УДК 004.7

Мандрик О.В., магістрант,
Бродський Ю.Б., к.т.н., доцент,
Державний університет «Житомирська політехніка»

АНАЛІЗ ПОТЕНЦІАЛУ ІГРОВИХ СИМУЛЯТОРІВ У РОЗВИТКУ МИСЛЕННЯ ТА ФОРМУВАННІ ПРАКТИЧНИХ НАВИЧОК У ГРАВЦІВ

Сьогодні бурхливий розвиток ігрової індустрії, експоненціальне покращення якості та складності ігрових додатків дозволяють ставити питання про розширення сфери застосування ігор, зокрема для навчання, тренування, вироблення корисних навичок тощо.

Вплив ігрових симуляторів на особливості мислення гравців сьогодні може вважатися беззаперечним, але ступінь такого впливу, як і стійкість відпрацьованих за допомогою такого впливу ментальних паттернів та практичних навичок потребує ретельного дослідження та оцінки. Також важливим лишається питання про негативні аспекти такого впливу – у чому вони полягають, наскільки сильними є, які сфери життя страждають від них найбільше, чи не нівелюють вони цілковито позитивний вплив від ігрових симуляторів тощо.

Підвищена актуальність теми вимагає зосередити увагу на вивченні впливу ігрових симуляторів на мислеві процеси гравців та оцінці перспектив їх використання як незадіяних високоефективних резервів для вироблення практичних навичок, отримання досвіду, максимально наближеного до реального, та вироблення необхідних паттернів.

В процесі проведення дослідження застосовувались методи опитування, проведені за допомогою мережі Internet, зокрема спеціально розроблених google-форм, опрацювання масиву відгуків на найбільш поширені та відомі ігрові симулятори, опубліковані результати наукових досліджень у англомовному сегменті мережі Internet тощо.

Аналіз останніх досліджень, зокрема в медичній сфері, було проведене кілька років тому під час якого учасники-студенти проходили чотирьох тижневе навчання за допомогою ігрових симуляторів, показало, що попри більшу зацікавленість у освітньо-ігровому процесі студенти не змогли виробити стійкі навички. Більше того, ігрова організація навчального процесу навіть істотно відволікала від самого навчання [1]. Водночас, опубліковано звіти і про інший експеримент, який досліджував вплив ігрового симулятору «Палата» на рефлексивне мислення студентів медсестринського фаху зі старших курсів. Кінцевий результат виявився помітним не тільки чисельно:

студенти порівнювали наявні знання в умовах командної роботи та співпраці, яких вимагала гра, і відзначали недоліки своєї роботи та помилки в опанованих знаннях. Подібний результат показало також дослідження із використанням ігрових симуляторів для пришвидшення мисленнєвих процесів та розвитку когнітивних здібностей у критичних ситуаціях [2]. Поєднання теорії та практики, яка концентрувалася навколо ігор, що імітували реальні критичні ситуації, призвело до значного пришвидшення мисленнєвих процесів та покращення результатів навчання в учасників експерименту. Про важливість ігрової симуляції у сучасному навчальному процесі свідчать і результати експерименту, проведеного на базі восьми загальних та спеціальних шкіл. Учні опановували основи точних наук, для прикладу, у дослідницькій ігровій симуляції вони власноруч проводили експерименти, змінювали вихідні умови їх проведення та робили висновки на основі отриманих даних, отримавши безпечне середовище для інтерактивного та цікавого навчального процесу [3].

В результаті проведеного аналізу дозволяють зробити висновок про значний потенціал ігрових симуляторів у сучасному навчальному процесі та професійному тренуванні – особливо за умови подальшого розвитку ігрових та віртуальних технологій. Звісно, для кожного окремого гравця результати будуть різнитися, але про вплив симуляційного процесу на мислення гравців можна говорити упевнено. Водночас нагальною лишається потреба вивчення кореляційного зв'язку між конкретними концепціями ігрових симуляторів, їх технічною реалізацією та ступенем позитивного вплив на мислення гравців. Існує потреба напрацювання та верифікації прийомів реалізації ігрових симуляторів, визначення мінімальних стандартів, які дозволять забезпечити бажаний вплив на мислення гравців та широке впровадження подібних додатків у навчальний процес та професійне тренування.

Список використаних джерел:

1. An experimental study on the effects of a simulation game on student's clinical cognitive skills and motivation.. URL: https://link.springer.com/article/10.1007/s10459-015-9641-x?utm_source.

2. Simulation game-based learning for cognitive apprenticeship development: a focus on processing speed.. URL: https://doaj.org/article/43ba7028e1d0415d8e62c12502b7ecbd.

3. Relative effectiveness of simulation games, blended learning, and interactive multimedia in basic science achievement of varying ability pupils.. URL: https://link.springer.com/article/10.1007/s10639-023-12414-z.

УДК 004

Татаренко Н. С, магістрант
Бродський Ю. Б, к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ФЕНОМЕНУ HOMELAB

Homelab все більше визнається не просто хобі для любителів, а відображає ширші зміни у ставленні людей до технологій та інфраструктури. Homelab (або домашня лабораторія) зазвичай означає приватне IT-середовище, яке людина створює у себе вдома і використовує для навчання, експериментів або самостійного хостингу серверів, мережевого обладнання, платформ віртуалізації та послуг. Замість того щоб працювати в корпоративних дата-центрах, користувачі домашніх лабораторій створюють у своїх домівках інфраструктуру, схожу на передову, що дає їм практичний доступ до сучасних систем без витрат і ризиків, пов'язаних із виробничими середовищами.[2]

З погляду ринку, домашні лабораторії не звужуються до нішевого сегмента: останні прогнози свідчать про те, що світовий Homelab ринок готується до значного зростання. Згідно з даними Market Research Future, у 2024 році ринок оцінювався приблизно в 6,37 млрд доларів США, а до 2035 року очікується майже його подвоєння[3], причому середньорічний темп зростання (CAGR) складе приблизно 7 відсотків. Фактори, що сприяють цьому зростанню, включають етос «зроби сам» (DIY), зростання попиту на інфраструктуру для віддаленої роботи та посилення інтересу до конфіденційності даних і самостійно розміщених сервісів.[3]

З технологічної думки, простір домашніх лабораторій зазнає значних змін. Однією з найпомітніших тенденцій є відхід від пропрієтарних платформ віртуалізації, таких як VMware, головним чином через підвищення вартості ліцензій.[1] Оператори домашніх лабораторій все частіше використовують гіпервізори з відкритим кодом, такі як Proxmox, XCP-ng або Nutanix Community Edition, цінуючи їх гнучкість і підтримку спільноти. Водночас багато користувачів об'єднують віртуальні машини в легкі контейнери, використовуючи Docker і Kubernetes. Цей перехід до контейнеризації підвищує ефективність, зменшуючи накладні витрати на ресурси та споживання енергії — обидві ці проблеми є критичними в домашніх умовах.[1] Деякі фахівці навіть досліджують можливість локального розгортання моделей штучного інтелекту, що відображає ріст амбіції

щодо використання передового штучного інтелекту в особистих середовищах.

На соціальному рівні домашні лабораторії функціонують як потужні навчальні платформи. Для IT-фахівців вони слугують для зміцнення практичних навичок: побудови, ремонту, налаштування та захисту інфраструктури без ризику для виробничої системи. Домашні лабораторії дозволяють користувачам «будувати реальні системи, усувати несправності та розвивати м'язову пам'ять... що безпосередньо перекладається на робочі завдання».[2]

Онлайн-спільноти, зокрема на Reddit, відіграють центральну роль у цьому явищі.[4] Люди діляться складними історіями про створення, просять поради або розмірковують про те, як розвивалася їхня лабораторія. Один користувач описав свою домашню лабораторію як «ніколи не закінчену... вона росте... і проникає в будинки моєї родини...» Інші цікавляться, де пролягає межа: коли «лабораторія» стає виробничим середовищем?.

В результаті проведеного аналізу визначено що внаслідок виникнення феномену, Homelab явище поступово виходить за межі звичайного технічного хобі та набуває значення важливого елемента цифрової культури що створює децентралізовані цифрові екосистеми та підсилює персональну технологічну автономію користувачів що в свою чергу покращує ефективність роботи серверного програмного забезпечення та підвищило рівень технічної грамотності у власників домашніх лабораторій.

Список використаних джерел:

1. Lee B. Top Home Lab Trends in 2024. Virtualizationhowto. 01.03.2024.URL: https://www.virtualizationhowto.com/2024/03/top-home-lab-trends-in-2024/ (дата звернення: 19.11.2025).

2. Stormagic. What Is a Homelab and Why Is It Important?. Stormagic.22.05.2025.URL: https://stormagic.com/company/blog/what-is-homelab/ (дата звернення: 19.11.2025).

3. Dhapte A. Homelab Market. *Market Research Future*. 01.10.2025. URL: https://www.marketresearchfuture.com/reports/homelab-market-21555 (дата звернення: 19.11.2025).

4. r/homelab URL: https://https://www.reddit.com/r/homelab/ (дата звернення: 19.11.2025).

УДК 004

Розбицький Р.Е., магістрант
Бродський Ю. Б, к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ ДЛЯ РОЗРОБКИ МАСШТАБОВАНИХ ВЕБ-СИСТЕМ

Мікросервісна архітектура (МСА) є підходом до побудови програмних систем, що грунтується на розподілі застосунку на невеликі, прямо не пов'язані сервіси, кожен із яких реалізує окрему бізнес-функцію. На відміну від монолітних систем, де всі модулі працюють у межах одного середовища, мікросервіси функціонують автономно та взаємодіють через легковагові мережеві протоколи. Цей підхід набув популярності стрімкому розширенню великих веб-застосунків, які зіштовхнулися з потребою відокремлення функціональності для підвищення ефективності розробки, стабільності системи та покращення масштабованості[1].

Однією з ключових особливостей МСА є незалежність сервісів. Кожен із них має власний життєвий цикл, кодову базу, середовище виконная та розгортання. Тобто кожен сервіс вважається окремим програмним додатком. Декомпозиція на дрібні компоненти дає змогу командам розробників працювати паралельно, не блокуючи одна одну, що пришвидшує створення функціоналу та зменшує ризик конфліктів під час інтеграції компонентів системи між собою[2]. Мікросервіси також часто характеризуються принципами polyglot persistence та polyglot programming: кожен сервіс може використовувати різні мови програмування та бази даних, відповідно до своїх потреб. Це підвищує оптимальність вибору технологій, але водночас ускладнює загальну інфраструктуру[3].

Важлвою технічною особливістю мікросервісної архітектури є розподілений характер системи. Мікросервіси взаємодіють через протоколи HTTP, REST, gRPC або черги повідомлень, що забезпечує гнучкість, але вводить додаткові мережеві ризики: затримки, втрату пакетів, непередбачувану поведінку. Унаслідок цього проєктування МСА невіддільне від практик DevOps, контейнеризації, оркестрації та автоматизованого моніторингу. Без інструментів на кшталт Docker, Kubernetes, систем логування й трасування, мікросервісна система швидко стає некерованою[4].

Серед основних переваг МСА виділяють високу масштабованість: кожен сервіс можна збільшувати або зменшувати незалежно від інших, що дає змогу ефективно розподіляти як людські, так і технічні ресурси. Ізоляція сервісів підвищує стійкість до помилок

— збій одного компоненту великої системи не призводить до її цілковитого падіння. Завдяки високій модульності спрощується підтримка, перероблення та впровадження нового функціоналу, а також створюються умови для впровадження гнучких методологій та постійного розгортання (CI/CD). Багато досліджень свідчать, що перехід до МСА покращує швидкість релізів та зменшує ризик системних збоїв, що особливо важливо для великих високонавантажених продуктів[5].

Разом із тим мікросервісна архітектура має певні недоліки. Найсуттєвішим є значне ускладнення інфраструктури: з'являється потреба в балансуванні навантаження, централізованому логуванні, тонкому налаштуванню API, підтримці стабільності даних та вирішенні проблем розподілених транзакцій в базах даних. Вартість розробки та підтримки системи може зрости, оскільки навіть прості операції потребують налагодженої взаємодії між сервісами. Наостанок, через більш високу абстрактність та загальну технічну складність, мікросервісна архітектура потребує зрілої команди розробників з високими технічними компетенціями.

Таким чином, мікросервісна архітектура є потужним підходом для великих, складних та швидко зростаючих програмних продуктів, для яких пріорітетом є гнучкість, масштабованість, простота підтримки та висока стійкість до помилок. В результаті аналізу визначено що мікросервісна архтектура дійсно є оптимальним архітектурним підходом до розробки великих масштабованих веб-систем, але підходить не для всіх систем меншого масштабу. Ми пропонуємо використовувати мікросервісну архітектуру за наявності досвідченої команди розробки та сучасної технічної бази.

Список використаних джерел:

1. Newman S. *Building Microservices.* 2nd ed. Sebastopol: O'Reilly Media, 2021. 352 c..

2. NGINX Inc**.** *Microservices Reference Architecture: NGINX Whitepaper* [Електронний ресурс]. 2021. Режим доступу: https://www.nginx.com

3. IBM Corporation. *Microservices Guide 2023: Principles, Patterns, and Deployment Models* [Електронний ресурс]. 2023. Режим доступу: https://www.ibm.com/cloud/architecture

4. Microsoft Azure Architecture Center. *Microservices Architecture Style – Updated Best Practices 2022* [Електронний ресурс]. 2022. Режим доступу: https://learn.microsoft.com/azure/architecture

5. Dragoni N., Giallorenzo S., Lafuente A. L., et al. *Microservices: Migration and Architectural Perspectives – 2020 Update.* ACM Digital Library, 2020. DOI: 10.1145/3380768.3380775.

UDC 004

Karyna Polishchuk, Master's Student,
Oleksii Chyzhmotria, Senior Lecturer.
Zhytomyr Polytechnic State University

ANALYSIS OF ATTACK VECTORS AGAINST MULTIFACTOR AUTHENTICATION SYSTEMS

The implementation of multifactor authentication (MFA) has become one of the most effective means of enhancing access control and protecting user accounts from unauthorized access. However, despite the significant improvement in security compared to single-factor systems, MFA mechanisms remain vulnerable to a variety of attack vectors that exploit human, technical, and organizational weaknesses. Analysing these attacks is critical to assessing how well MFA systems perform and identifying areas for improvement.

One of the most common threats is SIM swapping, which targets SMS-based authentication. In this attack, criminals trick mobile carriers into transferring a victim's phone number to a SIM card they control, enabling them to intercept one-time passwords and reset account credentials. This attack is especially dangerous because it circumvents digital security measures by exploiting vulnerabilities in telecom procedures. According to a 2023 FBI report, SIM swapping attacks have resulted in millions of dollars in cryptocurrency theft and identity fraud [1].

Phishing and man-in-the-middle (MITM) attacks represent another major category of MFA threats. Modern phishing tools have advanced beyond basic credential theft pages and now include real-time proxy features that can intercept authentication sessions between users and legitimate services. These sophisticated tools act as invisible intermediaries, capturing both passwords and second-factor codes during the authentication process. Browser-based reverse proxies such as Modlishka or Evilginx2 demonstrate how easily TOTP or push-based MFA can be bypassed when users are tricked into entering their data on a cloned website [2]. Session hijacking and replay attacks also remain relevant: adversaries can intercept valid authentication tokens or cookies and reuse them to impersonate users within active sessions.

A separate category of social engineering attacks exploits human behavior rather than technical flaws. The so-called MFA fatigue or "push bombing" attack overwhelms a user with repeated login prompts until they accidentally or intentionally approve one. According to Microsoft's Digital Defense Report, such attacks accounted for more than 20% of recorded MFA breaches in 2023 [3]. The success of these attacks highlights the need for

adaptive authentication policies that include number matching or contextual verification.

Comparative analysis of attack success rates across authentication methods reveals distinct vulnerability profiles. SMS-based MFA demonstrates the lowest resistance due to interception and SIM swapping, making it unsuitable for high-security environments. TOTP applications such as Google Authenticator provide stronger protection but remain susceptible to phishing-based code theft and replay within short time windows. Push notification systems offer convenience but face behavioral exploitation through fatigue or spoofed approval prompts. In contrast, hardware tokens and FIDO2 security keys provide the highest resistance because they use asymmetric cryptography and bind authentication to specific domains, preventing interception and replay [4].

Statistical data confirm that nearly 80% of successful MFA bypasses occur in systems using SMS or TOTP, while phishing-resistant methods such as FIDO2 account for less than 2% of incidents [5]. Nevertheless, widespread adoption of secure technologies remains limited due to cost, hardware availability, and user convenience factors. Therefore, the challenge lies in achieving a balance between usability and security.

In conclusion, the analysis of attack vectors against MFA systems demonstrates that no method is entirely immune to compromise. Effective protection requires a combination of phishing-resistant protocols, user education, and adaptive risk-based authentication. Future research should focus on developing hybrid mechanisms that integrate behavioral analytics, cryptographic verification, and contextual awareness to dynamically respond to evolving attack strategies.

References:

1. FBI; CISA. Public advisory on SIM-swapping attacks. FBI & CISA, 2023. 6 p.

2. Enisa. ENISA threat landscape 2023. European Union Agency for Cybersecurity, 2023. 144 p.

3. Microsoft. Digital defense report 2023. Microsoft Corporation, 2023. 131 p.

4. Cisco Talos. MFA bypass and exploitation report, Q1 2024. Cisco Systems, 2024. 18 p.

5. Verizon. Data breach investigations report 2024. Verizon Communications, 2024. 100 p.

UDC 004

Karyna Polishchuk, Master's Student,
Oleksii Chyzhmotria, Senior Lecturer
Zhytomyr Polytechnic State University

SYSTEMATIZATION AND CLASSIFICATION OF MULTIFACTOR AUTHENTICATION METHODS

The increasing number of cyber threats and the growing complexity of digital ecosystems have led to the widespread adoption of multifactor authentication (MFA) as a key mechanism for strengthening information security. However, the diversity of MFA implementations across platforms and technologies necessitates the development of a clear and unified classification system. The systematization of MFA methods enables a better understanding of their structure, security characteristics, and practical applicability within different organizational environments.

Traditionally, MFA mechanisms are categorized according to the authentication factors they employ: (1) knowledge factors – "something the user knows" (passwords, PINs, security questions); (2) possession factors – "something the user has" (hardware tokens, smart cards, mobile devices); and (3) inherence factors – "something the user is" (biometric identifiers such as fingerprints or facial recognition) [1]. While this tripartite model remains fundamental, modern digital ecosystems have extended it with contextual and behavioral factors – "something the user does" or "somewhere the user is" – enabling adaptive authentication based on device location, time, or usage patterns [2].

From a technological perspective, MFA systems can be classified into several distinct categories. TOTP systems generate temporary codes using cryptographic algorithms that are synchronised with server time, offering robust protection against brute-force attacks. SMS-based authentication relies on mobile networks to deliver one-time codes via text messages, offering high accessibility but limited resistance to SIM swapping and interception. Push notification-based authentication sends approval requests to trusted devices, allowing users to confirm login attempts through secure channels. Hardware tokens such as YubiKey and FIDO2 keys, use cryptographic challenge-response methods that offer the strongest protection against phishing and replay attacks [3].

Regarding system architecture, MFA can be implemented as centralised systems with all factors verified by one identity provider like Azure AD or Okta, or as federated systems, where authentication is shared across multiple trusted domains. A hybrid approach often combines both, allowing integration between corporate and cloud environments. Cloud-

based MFA services increasingly adopt standards such as FIDO2 and WebAuthn, which eliminate shared secrets and link authentication directly to the domain origin, thereby strengthening resistance to credential theft [4].

To enhance understanding and comparison, a structured taxonomy can be proposed that considers four core dimensions: (1) factor type, (2) delivery channel, (3) cryptographic model, and (4) user interaction. According to this extended classification, TOTP and SMS belong to symmetric key models relying on code transmission or generation, while push notifications and hardware tokens represent asymmetric or challenge-based mechanisms. Comparative evaluation demonstrates that hardware tokens and push-based systems achieve the best balance between security and usability, whereas SMS, despite being widespread, shows the highest exposure to social engineering and network attacks.

A summarized comparison of selected MFA technologies highlights the trade-off between usability and protection. TOTP offers offline functionality but requires synchronization; SMS provides convenience but low resilience; push notifications ensure a good user experience with moderate risk; and hardware tokens guarantee strong cryptographic security with limited accessibility due to cost and device dependency [5].

In conclusion, the proposed systematization and classification of MFA methods demonstrate that effective authentication strategies must combine multiple complementary factors while considering both technological capabilities and user behavior. Future research should focus on developing adaptive MFA architectures that dynamically adjust verification strength based on contextual risk, ensuring both robust protection and practical usability.

References:

1. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2023. 816 p.

2. ENISA. Guidelines on Modern Authentication and Authorization Protocols. European Union Agency for Cybersecurity, 2023. 80 p.

3. NIST. Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B). National Institute of Standards and Technology, 2022. 79 p.

4. FIDO Alliance. FIDO2: Moving the World Beyond Passwords, Technical Overview. FIDO Alliance, 2023. 75 p.

5. Microsoft. Multi-Factor Authentication Overview and Best Practices. Microsoft Corporation, 2024. 10 p.

УДК 004.7

Сичевський С.В, магістрант,
Свінцицька О.М., к.пед.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ЕФЕКТИВНОСТІ ТА РОЗРОБКА SERVERLESS-АРХІТЕКТУРИ НА ОСНОВІ GOOGLE CLOUD FUNCTIONS ДЛЯ АСИНХРОННОЇ ОБРОБКИ ПОДІЙ

В умовах експоненціального зростання обсягів даних (Big Data) та посилення вимог до гнучкості IT-інфраструктури, традиційні підходи до обробки подій стають економічно та ресурсно неефективними. Концепція Serverless Computing дозволяє вирішити ці проблеми, надаючи модель "плати-за-використання" та автоматичне масштабування. Метою дослідження є розробка та порівняльний аналіз ефективності Event-Driven архітектури на базі сервісів Google Cloud Platform (GCP). Для вирішення даної задачі необхідно спроектувати високонадійний та економічно ефективний механізм для асинхронної обробки непередбачуваних обсягів вхідних подій, мінімізуючи при цьому операційні витрати (OPEX).

Для реалізації цього підходу доцільно спроектувати Serverless-архітектуру, ключовим компонентом якої виступають GCP Cloud Functions. Для забезпечення асинхронної взаємодії передбачається використання сервісу Cloud Pub/Sub як високонадійної шини повідомлень, а також Cloud Storage як джерела тригерів для ініціації обробки завантажених файлів.

Обробка подій має відбуватися миттєво після їх надходження, викликаючи мікросервіси Cloud Functions, які виконуватимуть специфічну бізнес-логіку: від валідації та трансформації даних до їх запису у NoSQL-сховище.

Для підтвердження ефективності архітектури передбачається проведення порівняльного аналізу розробленої Serverless-моделі проти традиційної Container-based архітектури (наприклад, GCE/GKE) за ключовими метриками: латентність обробки, масштабованість та загальна вартість володіння (TCO). Очікується, що Serverless-модель на GCP продемонструє нульові витрати в стані простою та здатність до автоматичного горизонтального масштабування до понад 1000 інстансів за секунди, що забезпечить низьку середню латентність (≈ 50 мс) навіть при пікових навантаженнях.

Таким чином, запропонована Serverless-архітектура на базі GCP Cloud Functions є оптимальним рішенням для Event-Driven Architecture

(EDA), забезпечуючи значну економію ресурсів та високу відмовостійкість при обробці асинхронних подій. Цей підхід є переважаючим для сучасних хмарних рішень з нерівномірним навантаженням. Перспективи подальшого дослідження включають інтеграцію Google Cloud Workflows для надійної оркестрації та управління багатоетапними, складними процесами обробки.

Список використаних джерел:

1. Hasselbring, W., & Steinacker, T. The architecture of event-driven software systems. In Proceedings of the 2018 IEEE 25th International Conference on Software Analysis, Evolution and Reengineering (SANER). 2018. P. 1–10.

2. Eismann, S., Hirt, G., Tretter, O., Dreibich, O., Mitsch, K. Comparative performance analysis of serverless function platforms. *Proceedings of the 1st Workshop on Distributed Infrastructures for Deep Learning (DIDL'18)*. 2018. P. 1–6.

3. Hellerstein, J., Kulkarni, A., Sreekanti, V. Serverless Computing: Design, Implementation, and Performance. Foundations and Trends in Databases. 2019. Vol. 10, No 4. P. 251–388.

4. Google Cloud Documentation. Overview of Cloud Workflows. URL: https://cloud.google.com/workflows/docs/overview

УДК 004.75

Ясен А. Є., магістрант
Годлевський Ю. О., викладач-практик
Державний університет «Житомирська політехніка»

ІНТЕГРАЦІЯ ХМАРНИХ РІШЕНЬ У СУЧАСНУ РОЗРОБКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У сучасному світі розробки програмного забезпечення складно уявити створення продукту без використання в ньому хмарних технологій. Але для продуктивного результату спочатку потрібно дізнатися що хмарні технології являють із себе. Хмарні технології – це набір технологій, що дозволяють зберігати, обробляти дані і що не менш важливо використовувати різноманітні технології, таких як віртуальні машини, процесорна потужність, оперативна пам'ять, дискове сховище, тощо через інтернет, що дає можливість відмовитись від певного обладнання у локальному обладнанні [1].

Перша дія яку виконує будь-яка компанія яка має в перспективу інтегрування хмарних технологій у свій проект, є визначення потреб та очікування. На цьому етапі компанії потрібно чітко вирішити які цілі або задачі вони хочуть досягти за рахунок хмарних технологій. Це може бути як покращення продуктивності співробітників, оптимізація витрат на проект або просто створення набагато більшої IT інфраструктури [2]. Компанії потрібно з'ясувати, які програми, технології або сервіси потрібні працівникам для ефективної роботи. Це допоможе створити розширення можливостей працівників, дасть можливість доступу програм на віддалених машинах та покращення безпеки даних.

Після проведення аналізу наявних технологій, організація має визначити процеси в які вона хоче інтегрувати хмарні технології. Такий підхід допоможе спланувати майбутню архітектуру проекту та уникнути можливих труднощів у подальшому. Визначивши потрібні процеси, наступним кроком буде зробити вибір потрібної хмарної технології для інтеграції її у проект, що залежить виключно від потреб компанії та задач які вона виконує. Існують наступні варіанти:

Публічна хмара – тип хмарної технології, в якій ресурси надаються провайдером. До даних ресурсів мають доступ багато користувачів, але не дивлячись на це постачальник послуги гарантує безпеку даних. Дане рішення підходить для впровадження однієї або декілька систем компанії

Приватна хмара – технологія, що використовується лише одним клієнтом. Дане рішення чудове підійде компаніям, які працюють з

приватними даними, наприклад з даними у фінансовій системі, системі охорони здоров'я або в урядових установах.

Гібридна хмара – технологія, що використовується у поєднанні власної інфраструктури компанії з хмарною інфраструктурою. Завдяки користуванню такої моделі можна досягти максимальну відмовостійкість системи. Також можна поділити роботу по-типу у хмарних середовищах можна розмістити нові або невеликі проекти, а у власній інфраструктурі важливі дані.

Мультиклауд – технологія, в якій використовується одразу декілька хмарних сервісів від різних провайдерів для вирішення задач. Це може бути використання як публічної хмари так і приватної, головне отримувати найкращі постачання технології для рішення задач від різних провайдерів.

Проте серед великої кількості позитивних моментів при використанні технології, також є і недоліки та певні ризики під час інтеграції. Головною проблемою є сумісність систем під час інтеграції хмарного рішення. Але даний ризик можна максимально знизити за рахунок поетапного переносу даних у хмарні рішення. Потрібно спочатку переносити не критично важливі дані і поступово переходити на критичні [3]. Тим не менш під час роботи потрібно детально перевіряти перенесені дані аби переконатися в їх точності та повноті інформації, провести ретельне тестування аби виявити та одразу вирішити будь-які проблеми, що виникли. Також під час інтеграції, потрібно особливо звертати увагу на забезпечення потрібного захисту та конфіденційності даних. Чудовим вирішенням буде шифрування даних та впровадження жорсткого контролю даних, для обмеження небажаного отримання даних від небажаних для цього осіб.

Список використаних джерел:

1. Mell, P., & Grance, T. The NIST Definition of Cloud Computing. National Institute of Standards and Technology. 2011. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf (дата звернення: 24.11.2025).

2. AWS Cloud Adoption Framework: Business Perspective. URL: https://docs.aws.amazon.com/whitepapers/latest/aws-caf-business-perspective/aws-caf-business-perspective.html (дата звернення: 24.11.2025).

3. Common cloud migration challenges and how to manage them. URL: https://www.ibm.com/think/insights/cloud-migration-challenges (дата звернення: 24.11.2025).

УДК 004.925.3

Горшенін М.О., магістрант,
Горшенін О.Є., к.т.н., доцент
Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ CPU- ТА GPU-ОРІЄНТОВАНИХ ПІДХОДІВ ДО ВІДСІКАННЯ ОБ'ЄКТІВ У РЕНДЕРИНГУ РЕАЛЬНОГО ЧАСУ

Зі зростанням складності тривимірних сцен, та збільшенням кількості сцен з великою кількістю дрібних або повністю прихованих об'єктів питання ефективного відсікання невидимих об'єктів набуває критичного значення для рендерингу в реальному часі. Існують два фундаментальні підходи: відсікання на основі CPU, що використовує центральний процесор, і відсікання на основі GPU, де відсікання інтегрується у графічний конвеєр та виконується паралельно на тисячах потоків.

Незважаючи на велику кількість окремих досліджень щодо відсікання, застосування ієрархічних структур та GPU-паралелізму, у відкритій літературі відсутній системний порівняльний аналіз однотипних стратегій, реалізованих на CPU і GPU, із фіксацією їх реальних переваг, обмежень та сценаріїв доцільності застосування. Для проведення порівняння створено уніфіковане тестове середовище, що забезпечує повторювані експериментальні умови та ідентичні вхідні дані для всіх алгоритмів. Інструментальною основою обрано Unity Scriptable Render Pipeline . На базі SRP реалізовано набір алгоритмів відсікання, які повністю дублюють один одного на CPU та GPU.

Окрім цього, створено набір стандартизованих сцен-шаблонів зі змінною щільністю розташування об'єктів, їх розмірами та рівнем оклюзії. Це дозволяє перевірити алгоритми в умовах різного просторового розподілу геометрії та різної структури видимості.

Для кожного алгоритму проведено серію вимірювань, що дозволяють визначити: обчислювальну вартість: час виконання; ефективність відсікання: частку відкинутих об'єктів; поведінку у граничних випадках: сцени без оклюзії, повну оклюзію, надзвичайно велику кількість дрібних об'єктів; залежність продуктивності від кількості інстанцій об'єктів; взаємодію технік: які стратегії підсилюють одна одну, а які дублюють функціональність.

Алгоритми на CPU реалізовано як в однопотоковому режимі, так і з використанням багатопотокового паралелізму на основі Jobs/Burst. Методи на GPU реалізовано за допомогою обчислювальних шейдерів.

Особливу увагу приділено структурі HZB як універсальному ресурсу, здатному бути повторно використаним, що знижує загальну обчислювальну вартість рендерингу.

Також у роботі досліджено недоцільність обходу BVH-структур на GPU, зумовлену розбіжністю потоків. На основі попередніх вимірювань та даних із останніх досліджень очікується встановлення таких закономірностей: GPU-підходи забезпечують найменший час відсікання, особливо в поєднанні відсікання за пірамідою видимості та HZB-відсікання, завдяки паралельному виконанню та відсутності синхронізацій між CPU і GPU; CPU з BVH перевищує GPU за ефективністю у сценах із низьким рівнем оклюзії та упорядкованим розташуванням об'єктів, де деревоподібна структура прискорює відсікання цілих піддерев; обхід BVH на GPU є недоцільним для сцен із великою кількістю дрібних об'єктів через значні гілкування потоків виконання та втрату ефективності паралелізму; існують випадки, де відсікання взагалі не дає виграшу в продуктивності; комбіновані стратегії забезпечують найкращий баланс між точністю відсікання та швидкістю виконання. Прогнозується, що повністю GPU-орієнтований конвеєр має забезпечити найбільший приріст продуктивності на великих сценах (>50 тис. об'єктів), тоді як CPU+BVH залишатиметься конкурентоспроможним до 10 тис. об'єктів.

Подальші дослідження спрямовано на узагальнення отриманих даних для масштабних сцен, а також на вивчення адаптивних комбінованих стратегій, де вибір CPU- чи GPU-методу здійснюється автоматично на основі характеристик сцени.

Список використаних джерел:

1. Lee G. B., Lee S. Iterative GPU Occlusion Culling with BVH. Proceedings of High-Performance Graphics (HPG '20). Washington, D.C., USA, 2020. P. 1–2. DOI: 10.2312/hpg.20201194. URL: https://www.highperformancegraphics.org/posters20/04_lee_iterative_occlusion_culling_abstract.pdf (дата звернення: 24.11.2025).

2. Schütz M., Kerbl B., Wimmer M. Software Rasterization of 2 Billion Points in Real Time. 2022. Vol. 5, No. 3. P. 1–16. DOI: 10.1145/3543863. URL: https://www.cg.tuwien.ac.at/research/publications/2022/SCHUETZ-2022-PCC/ (дата звернення: 24.11.2025).

УДК 004.8

Воробйов А.П., здобувач
Державний університет «Житомирська політехніка»

ГІБРИДНИЙ МЕТОД ПРОГНОЗУВАННЯ ВАРТОСТІ НЕРУХОМОСТІ ЗА СТРУКТУРОВАНИМИ ДАНИМИ ТА ВІЗУАЛЬНИМ АНАЛІЗОМ ЗОБРАЖЕНЬ

Автоматизована оцінка вартості нерухомості є актуальною задачею, в основному, для ринку нерухомості, але також банківського сектору, або інвестиційних компаній. Класичні методи оцінки базуються переважно на табличних характеристиках об'єктів – площі, кількості кімнат, поверху, року введення в експлуатацію, місцезнаходження тощо. Однак такі підходи не враховують візуальну складову, яка суттєво впливає на сприйняття вартості покупцями: якість ремонту, стан оздоблення, естетику інтер'єру.

Експерименти з регресійними моделями на українських даних показують, що максимальна точність прогнозування ціни за табличними ознаками становить близько 65%. Це обумовлено тим, що значна частина цінової варіативності пов'язана з факторами, які складно формалізувати числово: стан ремонту, якість матеріалів, загальне враження від об'єкта.

У роботі пропонується гібридний метод прогнозування вартості нерухомості, який поєднує регресійний аналіз табличних даних із візуальною класифікацією якості об'єкта на основі фотографій. Ключова ідея полягає у використанні порядкової (ordinal) класифікації для оцінки візуальної якості, що дозволяє врахувати ієрархію вартості ремонту об’єкта (без оздоблення/ремонту - 0, чорновий - 1, совітський - 2 і далі за шкалою).

Архітектура системи складається з двох основних компонентів. Перший – регресійна модель для прогнозування базової ціни за табличними характеристиками: площа, кількість кімнат, поверх, тип будинку, район, відстань до лінії бойового зіткнення, тощо. Другий – згорткова нейронна мережа для класифікації візуальної якості об'єкта.

Для навчання візуального класифікатора використовується спеціалізована функція втрат CORN (Conditional Ordinal Regression Network), яка враховує порядок класів. Альтернативою до CORN є крос-ентропія, але на відміну від крос-ентропії, CORN забезпечує сильнішу функцію штрафу за помилки між віддаленими класами, що відповідає реальній різниці у вартості об'єктів. Тобто, якщо за результатом класифікації, в об’єкта виявлено найкращу якість інтер’єру, але ціна відповідає класу “без оздоблення” - штраф буде більший ніж звичайний.

Об'єднання результатів двох моделей реалізується через stacked generalization. На першому рівні базові моделі генерують прогнози: регресійна модель – ціну та інтервал невизначеності, візуальна модель – ймовірності належності до кожного класу якості. На другому рівні мета-модель навчається оптимально комбінувати ці прогнози.

Важливою особливістю підходу є використання механізму для агрегації інформації з кількох фотографій одного об'єкта. Це дозволяє моделі автоматично визначати найбільш інформативні зображення та зменшувати вплив неякісних або нерелевантних фото.

Альтернативним підходом може бути end-to-end мультимодальна нейронна мережа з двома гілками: також табличною MLP та візуальною CNN. Об'єднання модальностей здійснюється через cross-attention або біллінійний пулінг на рівні латентних представлень.

Попередні експерименти та навіть роботи з іншими методами [3], показують, що додавання візуальної компоненти дозволяє підвищити точність прогнозування щонайменше на 10–15% порівняно з моделями, які використовують лише табличні дані. Найбільший ефект спостерігається для нерухомості з нестандартними характеристиками, де візуальна інформація є найважливішою.

Запропонований гібридний метод відкриває можливості для створення більш точних автоматизованих систем оцінки нерухомості, які враховують як об'єктивні характеристики, так і суб'єктивне сприйняття об'єкта. Подальші дослідження спрямовані на розширення набору даних та інтеграцію додаткових джерел інформації.

Список використаних джерел:

1. SciKit Learn. URL: https://scikit-learn.org.

2. LearnOpenCV. Convolutional Neural Network (CNN). URL: https://learnopencv.com/.

3. Poursaeed O., Matera T., Belongie S. Vision-based Real Estate Price Estimation. Machine Vision and Applications. 2018. Vol. 29 : Computer Vision and Pattern Recognition. URL: https://doi.org/10.48550/arXiv.1707.05489.

УДК 004

Столярчук Д.В., здобувач
Варганова Д.О., ст. викладач
Державний університет «Житомирська політехніка»

РОЗРОБКА ФІНАНСОВОГО СИМУЛЯТОРА З ЕЛЕМЕНТАМИ ГЕЙМІФІКАЦІЇ ЯК ІНСТРУМЕНТУ НАВЧАННЯ ФІНАНСОВОЇ ГРАМОТНОСТІ

У сучасних умовах фінансова грамотність набуває особливої важливості, адже економічні процеси стають дедалі складнішими, а недостатній рівень фінансових знань часто спричиняє зростання заборгованості, поширення шахрайських схем та зниження фінансової стійкості громадян. Особливо проблема проявляється у випадках, коли люди несподівано отримують значні грошові суми — спадщину, страхові виплати чи інші одноразові надходження. Нерідко такі кошти витрачаються імпульсивно та без стратегічного планування: люди купують непотрібні речі, здійснюють ризикові інвестиції. Відсутність базових знань з управління бюджетом та довгострокового планування стає причиною того, що навіть значні суми зникають дуже швидко. Одним із ефективних способів подолання цієї проблеми є інтерактивні цифрові інструменти, зокрема фінансові симулятори, які поєднують навчальний контент та елементи гейміфікації [1].

Фінансовий симулятор являє собою програмний продукт, що моделює реальні економічні ситуації: бюджетування, інвестування, управління витратами, накопичення, роботу з депозитами, кредитами та оцінювання фінансових ризиків. Важливою особливістю такого інструменту є наявність інтерактивного «ігрового простору», у якому користувач може експериментувати з власними рішеннями без реальних фінансових втрат.

У симуляторі застосовуються різні елементи гейміфікації, такі як внутрішні нагороди, бали досвіду, а також система особистого прогресу. Користувач може змагатися з іншими учасниками у рейтингах, виконувати щоденні завдання та проходити різноманітні сценарії («сімейний бюджет», «фонд накопичень», «ризикові інвестиції») [2]. Також, симулятор може надсилати корисні нагадування: повідомлення на смартфон або електронні листи з мотиваційними фразами, підказками чи нагадуваннями про необхідність виконати сьогоднішнє завдання. Система дозволяє користувачеві працювати зі змінними параметрами: доходи, видатки, інфляція, зміни депозитних ставок, раптові фінансові події (штрафи, ремонти, підвищення цін). Це формує реалістичний досвід та допомагає

засвоїти практичні навички фінансового планування [1]. Вбудований модуль аналітики дозволяє відстежувати помилки та успіхи користувача, формує індивідуальні підказки, поради щодо оптимізації витрат, створення резервного фонду та покращення фінансової поведінки [3].

Для розробки кросплатформенного інтерфейсу можна використовувати такі середовища, як .NET MAUI або Unity, які забезпечують можливість запуску симулятора на Android, Windows, iOS та веб-платформах. Додатковим сучасним підходом є використання технології PWA (Progressive Web App), що дозволяє запускати застосунок без встановлення, працювати офлайн, отримувати push-сповіщення та зберігати дані локально. Завдяки цьому симулятор може функціонувати прямо у браузері. Крім того, використання PWA значно спрощує процес оновлення, адже нові функції стають доступними користувачам автоматично, без необхідності повторного встановлення застосунку. Також, використання Service Worker, який відповідає за кешування статичних ресурсів, фонову синхронізацію та обробку push-повідомлень. Для збереження даних локально можуть застосовуватися IndexedDB або LocalStorage, що дозволяє забезпечити стабільну роботу навіть за відсутності інтернету. Використання Web App Manifest дає змогу додати застосунок на домашній екран пристрою. У симулятор інтегруються навчальні модулі з поясненнями ключових понять: що таке бюджет, як працює відсоток, ризики інвестицій, чому важливо мати подушку безпеки [3].

Розробка фінансового симулятора з елементами гейміфікації є ефективним та інноваційним підходом до навчання фінансової грамотності. Поєднання реалістичних економічних сценаріїв, ігрових механік, аналітики та навчальних модулів дозволяє створити універсальний інструмент, який може використовуватись у навчальних закладах та для самостійного навчання.

Список використаних джерел:

1. OECD. Financial Literacy and Financial Education. [Електронний ресурс] – Режим доступу до ресурсу: https://www.oecd.org.

2. DUOLINGO Research. Motivation and gamified learning. [Електронний ресурс] – Режим доступу до ресурсу: https://research.duolingo.com.

3. Google Developers. Progressive Web Apps Documentation. [Електронний ресурс] – Режим доступу до ресурсу: https://web.dev/pwa.

УДК 004.413

Буджак Д.В., здобувач
Науковий керівник: Данильченко В.М., доцент
Державний університет інформаційно-комунікаційних технологій

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ ФІЛЬТРАЦІЇ ДАНИХ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Постановка задачі. Зростання обсягів інформації, швидкості її генерації та різноманіття форматів створює суттєві труднощі для ефективного відбору релевантних даних. Сучасні інформаційні системи опрацьовують терабайти структурованої та неструктурованої інформації, що ускладнює ручне або традиційне алгоритмічне фільтрування. Користувачі все частіше стикаються з перевантаженням інформацією, а системи — з необхідністю аналізувати великі масиви даних у реальному часі.

Традиційні фільтри, що ґрунтуються на простих ключових параметрах (категорія, дата, рейтинг), не завжди враховують контекст, смислове навантаження та приховані зв'язки в даних. Це створює потребу у впровадженні інтелектуальних алгоритмів, здатних аналізувати дані за змістом, а не лише за поверхневими характеристиками.

Мета дослідження. Мета роботи полягає у вивченні можливостей застосування штучного інтелекту для покращення процесів фільтрації даних. Особлива увага приділяється методам обробки природної мови, машинного навчання та семантичного аналізу, що дозволяють:

- коректно інтерпретувати запити користувача;
- автоматизувати відбір даних за змістовими ознаками;
- формувати персоналізований набір релевантної інформації;
- зменшити час пошуку потрібних даних у великих масивах.

Метою також є визначення переваг та обмежень інтелектуальних підходів порівняно з традиційними методами.

Результати дослідження. У процесі дослідження встановлено, що інтелектуальні методи фільтрації даних здатні значно підвищити точність та релевантність результатів у різних типах інформаційних систем. Основні можливості ШІ у цьому контексті включають:

1. Семантичний аналіз даних.

Алгоритми ШІ розпізнають значення, контекст і смислові зв'язки, що недоступно для класичних фільтрів. Це дозволяє розуміти не тільки "що шукає користувач", а й "чому саме це".

2. Обробка природної мови (NLP).

Система може працювати з описовими або неточними запитами, наприклад: «знайти тихе місце для роботи», «підібрати подію для вихідних».

3. Навчання на даних.

ШІ здатен адаптуватись до користувача, запам'ятовувати вподобання та змінювати логіку відбору.

4. Контекстне ранжування результатів.

Розумні алгоритми враховують не лише ключові слова, а й актуальність, популярність, поведінкові фактори та схожі патерни.

5. Обробка великих даних у реальному часі.

Інтелектуальні методи дозволяють масштабувати фільтрацію без втрати швидкості.

Застосування таких технологій дає змогу створити більш точні, адаптивні та персоналізовані інформаційні системи.

Висновки та перспективи. Застосування штучного інтелекту у процесах фільтрації даних дозволяє подолати ключові проблеми, пов'язані з великими обсягами інформації, низькою релевантністю результатів і високим навантаженням на користувача. Інтелектуальні методи забезпечують більш точне розуміння запитів, враховують контекст та адаптуються до змін у поведінці користувачів.

Перспективними напрямами подальших досліджень є:

– розробка універсальних моделей контекстної фільтрації;
– використання гібридних моделей, що поєднують статистичні й семантичні методи;
– підвищення точності семантичного аналізу за умов нечітких або суперечливих даних;
– оптимізація обчислювальних витрат і енергоспоживання для роботи на мобільних пристроях.

Список використаних джерел:

1.Google AI. Machine Learning & AI Guides [Електронний ресурс]. – Режим доступу: https://ai.google – Дата звернення: 25.11.2025.

2. Microsoft Azure AI Platform [Електронний ресурс]. – Режим доступу: https://azure.microsoft.com/en-us/products/ai-services – Дата звернення: 25.11.2025.

3. NVIDIA. AI & Deep Learning Technologies [Електронний ресурс]. – Режим доступу: https://www.nvidia.com/en-us/deep-learning-ai – Дата звернення: 25.11.2025.

4. OpenAI. Artificial Intelligence Research [Електронний ресурс]. – Режим доступу: https://openai.com – Дата звернення: 25.11.2025.

УДК 004

Хоменко Д.П., студент
Петросян А.Р., аспірант
Державний університет «Житомирська політехніка»

МЕТОДИКА ПОБУДОВИ ОПТИМІЗОВАНОЇ 3D-МОДЕЛІ БЕЗПІЛОТНОГО ПОВІТРЯНОГО СУДНА ДЛЯ СИСТЕМ ФІЗИЧНОГО МОДЕЛЮВАННЯ ПОЛЬОТУ

Система фізичного моделювання польоту (симулятор) безпілотного повітряного судна (БПС) необхідна для безпечного та ефективного тестування бортового програмного забезпечення (ПЗ) автопілота без ризику пошкодження апарату. Як зазначається в статті [1], помилки в алгоритмах ПЗ можуть призвести до аварій та створення загрози для оточуючих, а традиційне відлагодження неможливе через безперервність роботи польотного контролера і руху БПС в просторі. Симулятор дозволяє відтворювати повний набір сигналів датчиків і поведінку БПС в 3D-середовищі, моделювати аварійні ситуації, проводити відлагодження та оптимізацію алгоритмів, не ускладнюючи архітектуру ПЗ, що прискорює розробку, знижує витрати і підвищує надійність кінцевого продукту.

Існуючі 3D-моделі БПС поділяються на два типи: орієнтовані на художню візуалізацію та на інженерне проєктування. Художні моделі часто не відповідають вимогам метричної точності (габарити, центри мас), тоді як технічні моделі мають надлишкову кількість полігонів і не підтримують формати для інтеграції у фізичні рушії. Це створює розрив між наявними ресурсами та потребами розробників симуляторів.

Метою роботи є розробка та апробація методики створення 3D-моделей, що поєднує оперативність побудови, метричну точність та оптимізацію для фізичних рушіїв реального часу.

Для реалізації завдання було проведено порівняльний аналіз ПЗ: 3ds Max, Blender 3D та Autodesk Fusion 360. Критеріями відбору стали: коректність експорту у формат .fbx, ергономіка інтерфейсу та функціональні можливості. За сукупністю факторів інструментом розробки обрано Blender 3D [2].

Ключовим етапом проєктування є перенесення точних розмірів численних дрібних компонентів. Традиційні ручні заміри займають багато часу, тому для оптимізації запропоновано метод 2D-сканування деталей планшетним сканером. Це дає змогу отримати ортогональні проєкції з реальним масштабом 1:1, які можна використовувати як точні кресленики безпосередньо у 3D-редакторі.

Сучасні БПС мають складну геометрію та щільну компоновку компонентів (електроніка, карбонові рами, кріплення). Відтворення

таких об'єктів методом класичного полігонального моделювання вимагає значного часу та високої кваліфікації.

З метою оптимізації часових витрат на етапі формоутворення було застосовано метод конструктивної суцільної геометрії – Boolean operations. Специфіка деталей БПС – чіткі грані, техногенні форми тощо, дозволяє відмовитися від класичної побудови сітки підрозділення геометрії (Sub-D) на користь процедурного об'єднання геометричних примітивів.

Такий підхід (Hard Surface Boolean Workflow) значно пришвидшує створення складної форми, проте генерує топологію з наявністю багатокутників (N-gons). Для вирішення цієї проблеми та підготовки моделі до ігрового рушія застосовано алгоритм автоматичної тріангуляції на етапі експорту. Оскільки модель є статичним твердотільним об'єктом (Rigid Body) і не підлягає скелетній деформації, нерегулярність початкової топології не впливає на візуальну якість шейдингу (при правильному налаштуванні нормалей/Auto Smooth) та фізику колізій, забезпечуючи при цьому суттєву економію часу.

В результаті апробації методики було створено конструкцію БПС (FPV-квадрокоптера), що складається з 9 унікальних конструктивних елементів. Загальний час розробки склав орієнтовно 4 години, чим було підтверджено високу ефективність запропонованого підходу для швидкого наповнення фізичних симуляторів точними моделями.

Висновки. Запропонований підхід продемонстрував високу ефективність: час розробки повноцінної конструкції FPV-квадрокоптера було скорочено до 4 годин без втрати візуальної достовірності та функціональної сумісності з фізичними рушіями. Це дозволяє рекомендувати дану методику для прискореного наповнення бібліотек асетів навчальних симуляторів, що є критично важливим в умовах зростаючої потреби при розробці нового ПЗ автопілота та підготовці операторів БПС.

Список використаних джерел:

1. Arsen Petrosian, Ruslan Petrosian, Oleksandra Svintsytska. Test platform for Simulation-In-Hardware of unmanned aerial vehicle on-board computer. Proceedings of the 4rd Edge Computing Workshop. 2024. Vol.3666 . pp. 76-84.

2. Blender Foundation. Modeling and Geometry Nodes. Blender 4.0 Manual. URL: https://docs.blender.org/manual/en/latest/modeling/index.html (date of access: 24.11.2025).

3. Unity Technologies. Mesh geometry and topology. Unity Documentation. URL: https://docs.unity3d.com/Manual/AnatomyofaMesh.html (date of access: 24.11.2025).

УДК 004.7

Туровець А.В., магістрант,
Вакалюк Т.А., д.пед.н., професор
Державний університет «Житомирська політехніка»

РОЗРОБКА ВЕБОРІЄНТОВАНОЇ РЕКОМЕНДАЦІЙНОЇ СИСТЕМИ З ПОЯСНЮВАЛЬНИМИ ТА ЕМОЦІЙНИМИ МЕХАНІЗМАМИ НА ОСНОВІ ГІБРИДНИХ МЕТОДІВ ФІЛЬТРАЦІЇ

Зростаючий обсяг аудіовізуального контенту створює проблему вибору для користувачів. Існуючі рекомендаційні системи, що базуються на жанровій або колаборативній фільтрації, не враховують емоційні аспекти сприйняття контенту та не надають прозорих пояснень. Існує потреба в новій системі, що враховуватиме як жанрові уподобання, так і емоційний фон фільмів, забезпечуючи при цьому пояснення до кожної рекомендації.

Рекомендаційні системи вже тривалий час є об'єктом дослідження багатьох науковців. У роботах Ricci F., Rokach L. та Shapira B. [1] розглядаються основні підходи до побудови таких систем, зокрема методи контентної та колаборативної фільтрації, їхні можливості та обмеження. Питання обробки текстових даних, зокрема визначення емоційного забарвлення описів, детально подано в дослідженнях Jurafsky D. і Martin J.H. [2], де показано, як методи обробки природної мови можуть підсилювати якість моделювання користувацьких уподобань. Окремий напрям пов'язаний з інтерпретованістю алгоритмів: Molnar C. [3] наголошує, що зрозумілі пояснення роботи моделі є важливим чинником для підвищення довіри до рекомендаційних систем.

Метою є створення веб орієнтованої рекомендаційної системи для підбору фільмів, у якій поєднуються різні підходи до фільтрації даних, аналіз емоційної складової контенту та механізми пояснення отриманих рекомендацій. Така система має забезпечити індивідуальний підбір фільмів і при цьому дозволити користувачу розуміти, на яких підставах сформовано конкретну рекомендацію.

Розроблювана система містить кілька функціональних модулів: блок реєстрації та авторизації користувачів, базу даних фільмів, рекомендаційне ядро, модуль обробки текстових описів і компонент, що формує пояснення. У рекомендаційному ядрі поєднуються елементи контентної та колаборативної фільтрації, що дає змогу враховувати як характеристики самих фільмів, так і подібність у поведінці користувачів. Для роботи з текстами описів застосовуються методи

аналізу природної мови, що дозволяють визначити загальний емоційний настрій фільму. Пояснювальний модуль узагальнює отримані дані та формує аргументацію щодо того, чому саме цей фільм пропонується користувачу. На рисунку 1 відображено приклад архітектури рекомендаційної системи для фільмів.

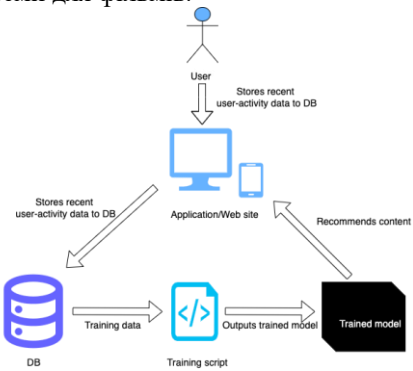


Рисунок 1 – Приклад архітектури рекомендаційної системи для фільмів

У процесі роботи були виокремлені переваги та недоліки різних видів фільтрації, що зазначені у таблиці 1.

Таблиця 1 – Порівняння методів фільтрації

Метод	Переваги	Недоліки
Контентна фільтрація	Враховує характеристики фільмів	Погано працює для нових користувачів
Колаборативна фільтрація	Враховує схожість користувачів	Вимагає великої кількості даних
Гібридна модель	Поєднує обидва підходи	Більш складна у реалізації

Розроблена концепція веб орієнтованої рекомендаційної системи дозволяє підвищити точність підбору фільмів та зробити процес рекомендацій більш зрозумілим для користувачів. Подальші дослідження передбачають практичну реалізацію прототипу системи, інтеграцію алгоритмів машинного навчання та оцінку ефективності рекомендацій.

Список використаних джерел:

1. Ricci F., Rokach L., Shapira B. Recommender Systems Handbook. Springer, 2022. https://link.springer.com/book/10.1007/978-1-0716-2197-4.

2. Jurafsky D., Martin J.H. Speech and Language Processing. 3rd ed. Stanford University, 2023. https://web.stanford.edu/~jurafsky/slp3/.

3. Molnar C. Interpretable Machine Learning. 2nd ed., 2022. https://christophm.github.io/interpretable-ml-book/.

УДК 004.7

Туровець А.В., магістрант,
Вакалюк Т.А., д.пед.н., професор
Державний університет «Житомирська політехніка»

РОЗРОБКА МОДУЛЯ ЕМОЦІЙНОГО АНАЛІЗУ ОПИСІВ ФІЛЬМІВ У СИСТЕМІ РЕКОМЕНДАЦІЙ НА ОСНОВІ NLP ТА ГІБРИДНОЇ ФІЛЬТРАЦІЇ

Сучасні онлайн-платформи пропонують користувачам величезну кількість фільмів, і саме тому системи рекомендацій відіграють важливу роль у виборі контенту. Аналіз наявних підходів дозволив помітити, що більшість із них зосереджені на жанрах, оцінках та порівнянні вподобань користувачів. Проте опис фільму часто містить певний емоційний настрій, який впливає на очікування і вибір. Брак урахування цих емоційних особливостей призводить до того, що рекомендації інколи здаються недоречними або випадковими. Тому постає потреба у модулі, який би міг визначати настрій текстового опису і використовувати цю інформацію під час формування рекомендацій.

Дослідження у сфері аналізу текстів свідчать, що завдяки сучасним методам обробки мови можна визначати емоції та загальний тон коротких текстів. У працях Jurafsky та Martin [1] розглянуті основи таких методів і способи роботи з текстовими даними. Водночас Mohammad і Turney [2] описують можливості використання емоційних словників, що дозволяють визначати зв’язок між словами та певними емоційними станами. Крім того, у роботах Li та співавторів [3] показано, що моделі глибинного навчання можуть досить точно класифікувати емоційний настрій коротких описів, до яких належать і анотації до фільмів.

Метою є створення і дослідження модуля, який визначає емоційний настрій опису фільму та використовує цю інформацію для покращення рекомендацій.

Робота модуля емоційного аналізу починається з обробки тексту: очищення від зайвих символів, нормалізації та виділення ключових слів. Далі текст подається у вигляді числового представлення, після чого визначається емоційний тон. Це може бути, наприклад, спокійний, напружений, позитивний чи сумний настрій. Результат аналізу подається у вигляді набору ознак, які далі використовуються рекомендаційним механізмом. Якщо користувач частіше обирає фільми з певним емоційним забарвленням, система зможе точніше підібрати нові варіанти, що відповідають його очікуванням. У такий спосіб емоційна характеристика доповнює звичайні параметри -жанр, рік

випуску, рейтинг. На рисунку 1 відображено приклад архітектури моделі визначення емоцій.

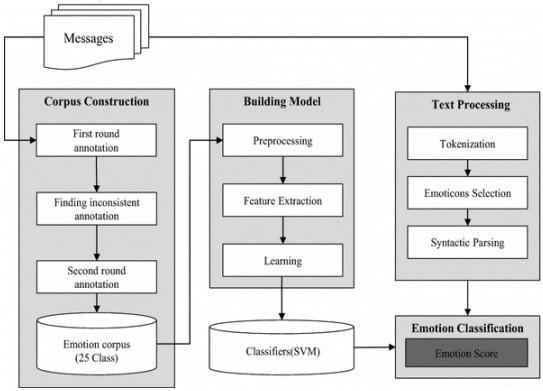


Рисунок 1 – Приклад архітектури рекомендаційної системи для фільмів

У процесі роботи були дослідження підходів до аналізу емоцій у текстах, що зазначені у таблиці 1.

Таблиця 1 – Порівняння методів фільтрації

Підхід	**Переваги**	**Недоліки**
Емоційні словники	Простий у використанні, зрозумілий	Не враховує контекст
Класичні моделі	Дають стабільні результати на простих текстах	Потребують попередньої векторизації
Глибинні моделі	Найкраща точність	Потребують більше ресурсів

Використання емоційного аналізу текстових описів дозволяє розширити можливості рекомендаційних систем і зробити їх поведінку ближчою до реальних очікувань користувачів. Такий підхід допомагає краще зрозуміти, який саме фільм людина хоче переглянути в певний момент, а не лише те, що їй подобалося раніше. Перспективним напрямом є розширення набору емоційних категорій та випробування модуля на різних жанрових групах.

Список використаних джерел:

1. Jurafsky D., Martin J.H. Speech and Language Processing. Stanford University, 2023.

2. Mohammad S., Turney P. NRC Emotion Lexicon, 2013.

3. Li S., Gao R., Huang X. Deep Learning Approaches for Emotion Classification, ACL, 2021.

УДК 004.7

Войтюк О.В., аспірант,
Державний університет «Житомирська політехніка»

ГЛИБОКО ВКЛАДЕНІ СТРУКТУРИ ДАНИХ ІЗ БАГАТОЗАЛЕЖНИМИ ЗВ'ЯЗКАМИ: ПРОДУКТИВНІСТЬ ТА ОНОВЛЕННЯ СТАНУ ПРИ РЕНДЕРИНГУ

Сучасні веб-застосунки дедалі частіше працюють із великими обсягами складних ієрархічних даних, що містять багаторівневі залежності між компонентами. Основним викликом у таких системах є забезпечення високої продуктивності рендерингу та ефективного оновлення стану. Глибока вкладеність DOM-структур призводить до значного збільшення кількості повторних рендерів, що знижує швидкодію, збільшує затримки та погіршує досвід користувача. Проблема торкається всіх сучасних веб-фреймворків, включно з React, Angular та Svelte [3, 5].

Різні архітектурні моделі фреймворків по-різному обробляють глибоко вкладені структури. Жоден фреймворк не є універсальним рішенням: вибір залежить від моделі використання та вимог до продуктивності. Велика кількість зв'язків між компонентами ускладнює відстеження змін стану та призводить до надмірних оновлень [4].

Серед інноваційних напрямків варто виділити сучасні підходи до вирішення окреслених завдань [1, 2, 6].

Алгоритмічне сплющення та автоматичне усунення глибини вкладеності: сучасні дослідження пропонують підходи, які автоматично перетворюють глибокі дерева даних на плоскі, індексовані структури з мінімізованою кількістю залежностей. Це зменшує каскадні оновлення та скорочує кількість операцій diff-аналізу під час рендерингу.

Локалізовані зони реактивності у вкладених структурах: інноваційні підходи передбачають автоматичне розбиття складного дерева компонентів на незалежні реактивні сегменти. Завдяки цьому будь-яка зміна в окремому піддереві не впливає на рендеринг усього застосунку, що суттєво підвищує продуктивність.

Адаптивна ізоляція стану: методологія, за якої фреймворк динамічно вирішує, які частини стану мають бути ізольовані (наприклад, за схемою «state islands»), а які — синхронізовані. Такий підхід зменшує когнітивні й обчислювальні витрати при роботі з багатозалежними даними.

Автоматичне виявлення та скорочення надлишкових залежностей: за допомогою статичного та напівдинамічного аналізу визначаються

залежності між компонентами, які не впливають на кінцевий рендер. Їх відсікання дає змогу зменшити кількість непотрібних оновлень та скоротити час реконсиляції.

Пріоритезовані черги оновлення: інноваційні scheduling-моделі дозволяють ранжувати оновлення залежно від рівня вкладеності, критичності компонентів та змін у потоках даних. Це створює «розумну» чергу рендерингу, що покращує реактивність інтерфейсу при великих навантаженнях.

Контекстне кешування глибоких структур: новий підхід передбачає зберігання проміжних результатів обчислення вкладених структур з урахуванням контексту використання. Це запобігає повторному проходженню дерева та скорочує витрати на обробку глибоких об'єктів.

Отже, ефективність рендерингу визначається комбінацією вибору фреймворка, моделі управління станом, алгоритмів оптимізації та використання GPU-спеціалізованих технологій. Вибір оптимальної архітектури залежить від масштабу застосунку, структури даних та вимог користувача, а подальші дослідження спрямовані на інтеграцію методів штучного інтелекту та апаратного прискорення у веб-середовище.

Список використаних джерел:

1. Curtis, S., & Fischer, B. Gavial: Programming the Web with Multi-tier Functional Reactive Programming. 2020. URL: https://arxiv.org/abs/2002.06188 (дата звернення: 10.07.2025).

2. Harper, L., Kim, D., & Müller, R. Signal-First Architectures: Rethinking Front-End Reactivity 2025. URL: https://arxiv.org/abs/2506.13815 (дата звернення: 05.10.2025).

3. Ollila, R., Mäkitalo, N., & Mikkonen, T. Modern Web Frameworks: A Comparison of Rendering Performance. J. Web Eng. 2022. URL: https://doi.org/10.13052/jwe1540-9589.21311 (дата звернення: 10.09.2025).

4. Sharma, N., Charan, S., , S., & , S. Performance and Developer Experience Comparison of Redux, Zustand, and Context API in React Applications. International Journal on Science and Technology. 2025. URL: https://doi.org/10.71097/ijsat.v16.i2.5026 (дата звернення: 07.09.2025).

5. Yerokhin, A., & Kameniev, D. Optimizing re-rendering in web applications: problem analysis and a React-based solution. Management Information System and Devises. 2025. URL: https://doi.org/10.30837/0135-1710.2025.184.090 (дата звернення: 07.09.2025).

6. Zhang, Y., Oliveira, M., & Bennett, C. Improving Front-end Performance through Modular Rendering and Adaptive Hydration (MRAH). 2025. URL: https://arxiv.org/abs/2504.03884 (дата звернення: 10.09.2025).

УДК 004:621.31

Петросян Р.В., старший викладач
Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ БАЗ ДАНИХ ЧАСОВИХ РЯДІВ ДЛЯ МОНІТОРИНГУ ЯКОСТІ ЕЛЕКТРОЕНЕРГІЇ

Підвищення вимог до надійності та ефективності енергопостачання, активна інтеграція розподілених енергоресурсів (таких як відновлювані джерела енергії, системи накопичення енергії та активні споживачі) і розвиток цифрових підстанцій кардинально ускладнюють режимні умови роботи сучасних енергетичних систем. У цьому контексті завдання моніторингу та аналізу якості електроенергії (ЯЕ) переходять з розряду допоміжних до категорії критично важливих для забезпечення стійкості та безпеки енергосистеми.

Сучасні комп'ютеризовані системи здатні генерувати великі масиви високочастотних даних, що містять детальну інформацію про параметри напруги і струму, частоти та гармонічні спотворення напруги, а також про швидкоплинні події – провали напруги, флікер тощо [1-3].

Проте традиційні підходи до зберігання та обробки інформації, засновані на реляційних системах керування базами даних, вже не здатні гарантувати потрібну продуктивність і гнучкість, оскільки їхня архітектура, орієнтована на транзакційність та цілісність даних, створює значні накладні витрати при операціях масового запису та часових запитах. Саме тому постає необхідність у використанні спеціалізованих систем зберігання – баз даних часових рядів (БДЧР). БДЧР – це база даних, оптимізована для зберігання та обробки часових рядів, яка представляє собою вимірювання з прив'язкою до часу [4]. Їхня ключова перевага полягає в тому, що час є основним виміром, а не просто атрибутом даних. Завдяки даній особливості система підтримує високошвидкісне додавання даних, ефективне їх стискання на рівні ядра підсистеми зберігання, а також застосування вбудованих інструментів часового аналізу.

При роботі з часовими рядами необхідно враховувати ряд особливостей, які роблять цей тип даних одночасно унікальним і складним для обробки:

1. Існують два основних підходи до організації зберігання даних.

Перший ґрунтується на моделі «ключ-значення», в якій кожна метрика зберігається в окремому часовому ряді і має власну послідовність міток часу.

Другий використовує мультиметричний формат: в рамках однієї часової мітки можуть зберігатися кілька значень, що відносяться до різних метрик.

Такий підхід забезпечує більш гнучку і багату структуру даних, що особливо важливо для комплексних систем вимірювань.

2. Часові ряди, як правило, характеризуються значними обсягами даних. По мірі зростання обсягу даних виникає необхідність у масштабуванні системи зберігання. тому БДЧР повинна забезпечувати: високу швидкість запису та вилучення даних; стабільну продуктивність при зростанні навантаження.

3. Обробка часових рядів вимагає наявності спеціалізованих обчислювальних механізмів, орієнтованих на виконання часових перетворень, агрегування, ресемплінгу та аналізу періодичності. Наявність таких операцій дозволяє ефективно виконувати розрахунок трендів, виявлення аномалій і аналіз кореляцій, виключаючи потребу в етапі складної попередньої підготовки даних.

Однак не всі системи БДЧР підходять для вирішення поставленого завдання, оскільки період дискретизації сигналів може досягати сотень мікросекунд. У контексті моніторингу ЯЕ найбільше практичне значення набувають високопродуктивні БДЧР. До таких систем належать, InfluxDB, що відрізняється високою пропускною здатністю при записі; TimescaleDB, що надає розвинені аналітичні можливості на основі SQL; а також високопродуктивні рішення – QuestDB.

Prometheus, незважаючи на широке поширення, в чистому вигляді менш придатний для даного сценарію внаслідок обмеженої роздільної здатності часових міток і моделі зберігання, орієнтованої переважно на моніторинг низькочастотних метрик.

Список використаних джерел:

1. ДСТУ EN 50160:2023. Характеристики напруги електропостачання в електричних мережах загальної призначеності. БУДСТАНДАРТ Online – нормативні документи будівельної галузі України. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=106226 (дата звернення: 24.11.2025).

2. Петросян Р.В. Алгоритм обчислення частоти напруги в електромережі з використанням квадратурних складових. Проблеми інформатизації та управління. 2024. №2(78). С. 69-76. URL: https://doi.org/10.18372/2073-4751.78.18963.

3. Петросян Р. В. Вимірювач частоти електричної мережі на базі цифрових фільтрів. Вісник ЖІТІ. 2002. №3(22). С. 78–80.

4. InfluxDB. InfluxData Documentation. URL: https://docs.influxdata.com/ (date of access: 24.11.2025).

Секція 4
ЕЛЕКТРОНІКА, ЕЛЕКТРОННІ КОМУНІКАЦІЇ, ПРИЛАДОБУДУВАННЯ ТА РАДІОТЕХНІКА

УДК 621.383

Махиборода А.І., *здобувач*
Національний технічний університет «Київський політехнічний інститут імені Ігоря Сікорського»

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОГО MPPT-АЛГОРИТМУ НА ОСНОВІ ANFIS ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФОТОЕЛЕКТРИЧНИХ СИСТЕМ

В умовах стрімкого розвитку відновлюваної енергетики сонячні фотоелектричні системи (ФЕС) посідають провідне місце серед джерел генерації електроенергії. Однак ефективність їх функціонування значною мірою залежить від здатності автоматичних систем адаптуватися до постійно змінюваних кліматичних умов, таких як освітленість, температура навколишнього середовища, часткове затінення та інші нестабільності. Відтак, проблема забезпечення максимальної енергетичної продуктивності ФЕС набуває особливої актуальності як наукового, так і прикладного рівня. У сучасних умовах інтенсивного впровадження сонячної енергетики зростає потреба у високоточних та адаптивних алгоритмах, що здатні забезпечувати стабільну роботу енергетичних систем у широкому діапазоні зовнішніх змін.

У цьому контексті методи стеження за точкою максимальної потужності MPPT (Maximum Power Point Tracking) відіграють ключову роль, оскільки дозволяють максимально ефективно відстежувати точку максимальної потужності (MPP) на вольт-амперній характеристиці сонячної батареї. Класичні алгоритми, попри їх простоту та реалізаційну зручність, показують недостатню точність у складних умовах роботи, зокрема при частковому затіненні. Це обумовлює необхідність застосування інтелектуальних підходів до оптимізації роботи ФЕС, серед яких значне місце посідають гібридні та штучно-інтелектуальні системи [1].

У роботі представлено інтелектуальний MPPT-алгоритм на основі ANFIS (Adaptive neuro fuzzy inference system) – адаптивної нечіткої системи виведення, що об’єднує нечітку логіку з нейронними мережами. Такий підхід дозволяє створити самонавчальний регулятор, який здатен адаптувати свою поведінку до зовнішніх змін в режимі

реального часу без необхідності створення жорстко заданої математичної моделі. ANFIS поєднує гнучкість лінгвістичних правил з потужністю навчання нейронної мережі, забезпечуючи точне відстеження MPP навіть у складних погодних умовах. Це особливо важливо для систем з нестабільним освітленням, де класичні методи демонструють значні втрати енергії [2].

Реалізована симуляційна модель у MATLAB/Simulink, що дозволяє змоделювати варіативні сценарії зміни освітленості, температури, PSC (Partial Shading Conditions), а також протестувати запропонований підхід у порівнянні з класичними методами P&O (Perturb and Observe) та InC (Incremental Conductance). Алгоритм впроваджено у мікроконтролерну систему на базі STM32 з інтеграцією DC-DC перетворювача, сенсорів струму та напруги, що дозволяє перевірити ефективність методу в реальних умовах [3].

Очікуваними результатами роботи є підвищення коефіцієнта корисної дії ФЕС на 7–12% у порівнянні з базовими методами MPPT, скорочення часу досягнення оптимального режиму, зменшення коливань навколо точки максимальної потужності та забезпечення стабільної роботи навіть у складних кліматичних умовах. Розроблене рішення має перспективу використання у складі автономних систем енергопостачання, зокрема для об’єктів критичної інфраструктури, мобільних енергетичних комплексів та інтелектуальних електромереж.

Список використаних джерел:

1. Podder, A., Roy, N., Samanta, S., & Mandal, K. (2019). MPPT methods for solar PV systems: A critical review based on tracking nature. IET Renewable Power Generation, 13(10), 1615–1632. https://doi.org/10.1049/iet-rpg.2018.5684

2. Mehmood, A., Mian, S. A., Mahmood, A., & Awan, S. M. (2025). A Robust MPPT Controller Design Using Artificial Neural Network Based Perturb and Observe Method for PV Systems. Applied Sciences, 15(3), 1031. https://doi.org/10.3390/app15031031

3. Volodymyr Chernenko, Petro Yahanov, Demyd Pekur, Roman Korkishko, Vasyl Kornaga, Viktor Sorokin, Analytical model of light current-voltage characteristics of a solar cell based on experimental data, Solar Energy Advances, Volume 4, 2024,100073, ISSN 2667-1131. https://doi.org/10.1016/j.seja.2024.100073

УДК 621.38

Качура О.В., к.т.н., доцент
С'янов О.Є., здобувач
Дніпровський державний технічний університет

МАТЕМАТИЧНА МОДЕЛЬ НАПІВПРОВІДНИКОВОЇ СТРУКТУРИ НА ОСНОВІ ДІОКСИДУ ВАНАДІЮ

Виникнення значних пускових струмів при ввімкненні електронних пристроїв до мережі живлення може призводити до переходу останніх у критичний режим з подальшим виходом з ладу. З метою запобігання даним процесам вдаються до застосування засобів захисту, що дозволяє знизити пікові значення струмів та подовжити терміни експлуатації електронного обладнання. Серед різноманітних засобів захисту знаходять застосування структури на основі діоксиду ванадію VO_2, які вмикаються послідовно з навантаженням. Для даних цілей ефективними є критичні терморезистори (критезистори) [1].

У роботі розроблено чисельну математичну модель терморезистора на основі методу кінцевих елементів для дослідження провідних властивостей у статичних та динамічних режимах.

Для математичного опису процесів, що протікають у структурі VO_2, скористаємося відомими математичними перетвореннями [1]:

$$\frac{\partial}{\partial x}\left(\varepsilon_a \frac{\partial \varphi}{\partial x}\right)+\frac{\partial}{\partial y}\left(\varepsilon_a \frac{\partial \varphi}{\partial y}\right)+\frac{\partial}{\partial z}\left(\varepsilon_a \frac{\partial \varphi}{\partial z}\right)=-\rho, \qquad (1)$$

де ε_a – абсолютна діелектрична проникність матеріалу; φ - електричний потенціал; ρ - об'ємна щільність заряду; x, y, z - вісі координат.

Рівняння (1) має бути доповнене рівнянням Лапласа для повітряного проміжку, яким оточено терморезистор:

$$\frac{\partial}{\partial x}\left(\varepsilon_a \frac{\partial \varphi}{\partial x}\right)+\frac{\partial}{\partial y}\left(\varepsilon_a \frac{\partial \varphi}{\partial y}\right)+\frac{\partial}{\partial z}\left(\varepsilon_a \frac{\partial \varphi}{\partial z}\right)=0. \qquad (2)$$

Вирішення системи (1)-(2) пов'язане з дослідженням мультифізичної тривимірної польової задачі. Коефіцієнти ε_a, ρ, C_p є нелінійними, залежать від величини і частоти струму, що протікає в об'ємі структури терморезистора. Для вирішення (1), (2) скористаємося методом кінцевих елементів. На рис. 1, а показано граничні умови досліджуваної моделі, її дискретна частина представлена на рис. 1, б.

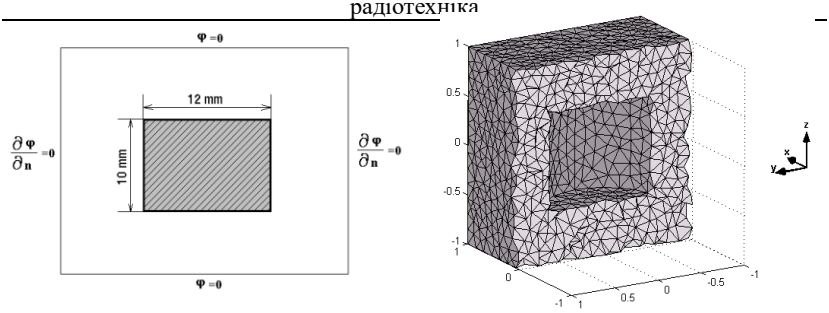


Рисунок 1 – Граничні умови та дискретна модель досліджуваного зразка

У результаті розрахунку отримано графіки напруженості електричного поля у поперечному перерізі зразка VO_2 (рис. 2).

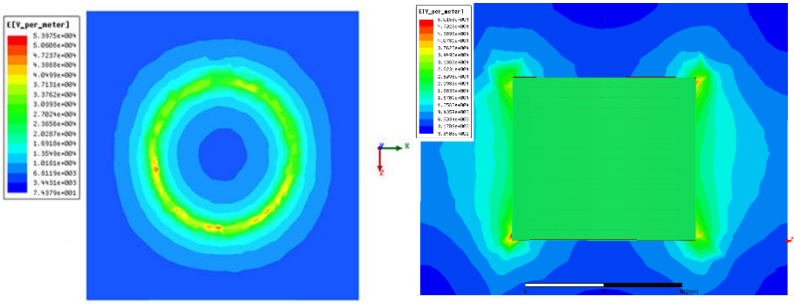


Рисунок 2 – Графіки напруженості електричного поля структури

У роботі створено тривимірну математичну модель терморезистора, яка дозволяє досліджувати електричні параметри структури на основі VO_2. Розроблена модель є універсальною і дозволяє враховувати як фізичні властивості терморезисторів, та і їх геометричні особливості.

Список використаних джерел:

1. O. Kachura, V. Kuznetsov, M. Tryputen, V. Kuznetsov, S. Kolychev. Artur Rojek. P. Hubskyi. Mathematical Model of a Semiconductor Structure Based on Vanadium Dioxide for the Mode of a Conductive Phase. Electronics 2025, 14(14), 2884; https://doi.org/10.3390/electronics14142884

2. Rini M., Hao Z., Schoenlein R.W. [et all]. Optical switching in VO2 films by below-gap excitation // Applied Phys. Letters. 2008. V. 92. P. 181-904.

УДК 621.317.373

Коренівська О.Л., к.т.н., доцент,
Бенедицький В.Б., ст. викладач
Державний університет «Житомирська політехніка»

ВИМІРЮВАННЯ РІЗНИЦІ ФАЗ ПРИ ВИКОРИСТАННІ ПРОГРАМНОГО СЕРЕДОВИЩА LTSPICE

Вивчення нормативної дисципліни «Теорія кіл і сигналів» у ЗВО ефективне лише тоді, коли поряд із засвоєнням основ теорії студенти в умовах лабораторного експерименту ознайомлюються на практиці з роботою електричних схем, джерелами живлення, осцилографом та вимірювальними приладами. Основним завданням лабораторного практикуму є засвоєння студентами практичних навичок підготовки та випробування електричних схем і пристроїв, зокрема набуття навичок вимірювання електричних величин, обробки експериментальних даних, побудова часових і векторних діаграм електричних величин і характеристики приладів, а також отримання експериментального підтвердження (з прийнятною точністю) теоретичних положень, викладених на лекціях.

Поряд з натурними експериментами в даний час широке поширення отримали комп'ютерне моделювання та аналіз схем електронних пристроїв в таких програмних середовищах, як PSpice, TINA-TI, KICad EDA, LabVIEW, NI Multisim та ін.

Одне з найпоширеніших завдань при аналізі ланцюгів змінного струму – це вимірювання різниці фаз. При використанні в роботі програмного середовища LTSpice (Linear Technology), в порівнянні з NI Multisim, відсутня наявність контрольно-вимірювальних приладів, які за зовнішнім виглядом і характеристиками наближені до їх промислових аналогів.

В LTspice вимірювання різниці фаз можна реалізувати кількома способами:

Спосіб 1: Пряме вимірювання за графіками (осцилографічний). Це найпростіший і наочний спосіб, який ідеально підходить для разових вимірювань. Недолік даного методу: вимагає ручного розрахунку, невисока точність.

Спосіб 2: Використання вбудованих математичних функцій. Цей спосіб є більш точним і автоматизованим. LTspice дозволяє будувати графіки не тільки сигналів, але і математичних виразів на їх основі.

Недолік даного методу: вимагає знання частотних і часових параметрів, менш точний, ніж AC Analysis.

Спосіб 3: Аналіз у частотній області (AC Analysis) – спосіб для вимірювання АЧХ і ФЧХ (амплітудно-частотної та фазо-частотної характеристик). Він показує різницю фаз безпосередньо. Недолік даного методу: вимагає налаштування, не показує перехідні процеси.

Для прискорення вимірювання різниці фаз при виконанні лабораторних робіт нормативної дисципліни «Теорія кіл і сигналів» пропонується апаратно-програмний спосіб реалізації фазометра, заснований на перетворенні різниці фаз у напругу (рис. 1).

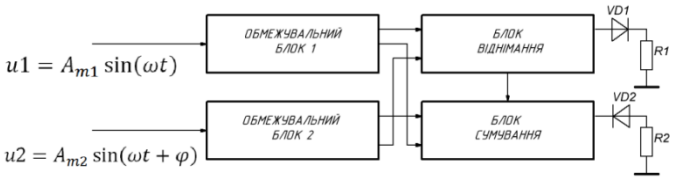


Рисунок 1

З використанням штатних функціональних блоків LTSpice вхідні синусоїдальні напруги u_1 і u_2 однакової частоти ω, що мають різницю фаз φ, перетворюють в напруги прямокутної форми, що мають однакові амплітуди. Отримані напруги подаємо на входи функціональних блоків, що реалізують сумування і віднімання, виходи яких під'єднанні послідовно до ідеальних діодів з навантаженням, в вигляді опорів.

Використовуючи вбудовані математичні функції, обчислюємо різницю фаз за формулою:

$$\varphi = \left(\frac{I_{\text{ср}}}{I_0} + 0.5\right) \cdot 180^{\circ},$$

де I_0 – амплітуди імпульсів струмів на виходах блоків сумування і віднімання; $I_{\text{ср}}$ − середнє значення різниці струмів, що викликаються напругами на виходах блоків сумування і віднімання.

Залежність φ від $I_{\text{ср}}$ не є однозначною в межах періоду. Виникаючу двозначність усувають реєструючи збіг позитивних фронтів напруги і струму. Якщо $0 < \varphi < \pi$ – фронти збігаються, при $\pi < \varphi < 2\pi$ фронти не збігаються.

Представлений спосіб, використовує можливості програмного середовища LTSpice, реалізовано у вигляді функціонального блока, вимірювання різниці фаз.

Список використаних джерел:

1. The LTspice Help Manual. Analog Devices. Режим доступу: https://ltspice.analog.com/help/LTspiceHelp.chm (дата звернення: 25.11.2025).

УДК 621.396.6

Коник С.В., магістрант,
Гнатюк М.О., к.ф.-м.н., доцент,
Дніпровський державний технічний університет

СИНТЕЗ СМУГОВИХ ФІЛЬТРІВ ДЛЯ SDR-РАДІОПРИЙМАЧІВ

Сучасні швидкодіючі аналогово-цифрові перетворювачі (АЦП) та засоби цифрової обробки сигналів дозволяють реалізовувати програмно-визначеного радіо, або software defined radio (SDR), які можуть бути оперативно переконфігуровані за допомогою програмних засобів відповідно до характеристик їх робочих сигналів.

Використання SDR технології дозволило значно підвищити ефективність засобів телекомунікації і впровадити нові цифрові види зв'язку. Зокрема, в останні роки підвищився інтерес дослідників до цифрового радіозв'язку у діапазоні коротких (3–30 МГц) та ультракоротких (30–300 МГц) хвиль. Особливості умов радіозв'язку у цьому діапазоні частот накладають достатньо суворі вимоги до динамічного діапазону тракту радіоприймачів. Полегшити умови роботи трактів радіоприймальних пристроїв можна за допомогою вхідних фільтрів на зосереджених елементах [2].

Для визначення величин параметрів елементів найбільш ефективно використовувати стандартизовані таблиці нормалізованих коефіцієнтів [1]. Однак, пряме використання таких таблиць для розрахунків смугових фільтрів найчастіше призводить до отримання нереалізованих значень параметрів окремих елементів. Найбільш ефективний підхід до проєктування смугових фільтрів у діапазоні коротких хвиль полягає у створенні фільтра-прототипа низької частоти із заданою частотою зрізу з подальшим його перерахунком у смуговий фільтр. Використання інверторів імпедансів при проєктуванні схем фільтрів дозволяє досягти бажаної ефективності схеми фільтру відносно як величин параметрів реактивних елементів, так і загальної топології схеми.

В роботі показано поетапну процедуру проєктуванняя смугового фільтру для радіоприймального пристрою короткохвильового діапазону частот у смузі частот 14 – 14.35 МГц, частотна характеристика фільтру буде відповідати характеристиці Чебишева з нерівномірністю 3 дБ та порядку 3. Першим етапом є розрахунок на основі нормалізованих коефіцієнтів з [1] фільтру прототипу нижніх частот (ФНЧ) із частотою зрізу, що дорівнює смузі пропускання цільового фільтру. Далі, до кожного з елементів розрахованого ФНЧ

додаються відповідні додаткові елементи із протилежним значенням комплексного імпедансу, таким чином отримуючи смуговий фільтр. Значення цих додаткових компонентів розраховуються за відомою формулою Томсона для коливального контуру, при цьому, резонансна частота ω_0 всіх контурів розраховується як середнє геометричне значення від нижньої та верхньої частоти смуги пропускання цільового фільтру.

Наступним кроком є використання інверторів імпедансів в загальній схемі фільтру для перетворення послідовного коливального контуру на паралельний із оптимальними значеннями ємності та індуктивності. Останнім етапом є використання схеми узгодження високого вхідного імпедансу фільтру із стандартизованим імпедансом 50 Ом. В якості узгодження використовується Г-подібна схема с послідовною ємністю. Остаточно, на рис. 1(а) показано топологію отриманого фільтру третього порядку, а його змодельована АЧХ показана на рис. 1(б).

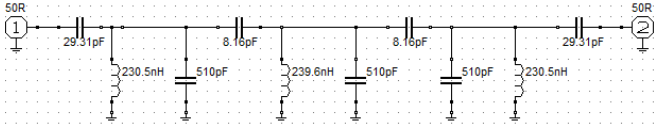


Рисунок 1 – Схема смугового фільтру

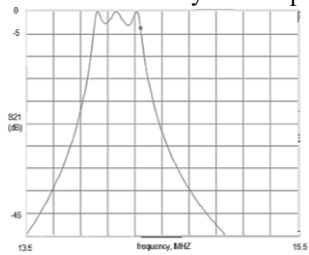


Рисунок 2 – Змодельована АЧХ отриманого фільтру

Таким чином, запропонована методика розрахунку елементів фільтру дозволяє отримати коректні результати.

Список використаних джерел:

1. Taylor, F. J. & Williams, A. Electronic Filter Design Handbook. 4th ed. McGraw-Hill Pub. 2006. 775 p.

2. Syed, L., Hasan, S. H., Rashid, H., & Gulistan, W. Designing Band Pass Filter for HF Radio's Front End. *2019 International Conference on Communication Technologies (ComTech)*, Rawalpindi, Pakistan, 2019, pp. 60-64, doi: 10.1109/COMTECH.2019.8737794.

УДК 621.3:004.9

Соболенко С.О., к.т.н., доц., начальник кафедри
Дубина О.Ф., к.т.н., доцент
Авсієвич Р.О., доктор філософії, доцент
Заєць Ю.О., заст. нач. факультету
Житомирський військовий інститут імені С.П. Корольова

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ІНТЕГРОВАНОЇ СИСТЕМИ ОХОРОНИ

У відповідності до [1], враховуючи мультиплікативний підхід до об'єднання узагальнюючих показників, показник ефективності та надійності інтегрованої системи охорони (ІСО) можна записати в аналітичному вигляді як

$$W_{\text{е}} = P_0, P_{\text{кл}}, P_{\text{св}}, P_{\text{н}}^{\text{сер}}, P_{\text{св}}^{\text{кз}}$$

де ймовірність виявлення об’єкта P_0 визначається датчиками руху і частково відеокамерами, ймовірність правильної класифікації $P_{кл}$ – відеокамерами, оператором і можливостями спеціального програмного забезпечення, ймовірність, що характеризує своєчасність обробки інформації в тракті сигнального розпізнавання $P_{\text{св}}$ - оператором і можливостями спеціального програмного забезпечення, ймовірність виконання, що характеризує своєчасність видачі інформації по каналу зв'язку $P_{\text{св}}^{\text{кз}}$ - станом і кількістю каналів зв’язку. Крім того, кожен елемент характеризується ймовірністю відмов, яка приблизно = $P_{\text{н}}^{\text{сер}}$.

Для дослідження ефективності запропонованого підходу і математичної моделі скористуємося сучасним обладнанням охоронної системи “Ajax”. Основними складовими комплекту є централь, та бездротові датчики. На основі даного набору шляхом додавання необхідних елементів у залежності від складності об’єкта охорони можна сформувати необхідну інтегровану систему охорони. Дані комплекти відрізняються різними параметрами і характеристиками пристроїв, що входять у склад.

Приблизні імовірнісні значення відповідних параметрів представлені в таблиці 2.

Для отримання реальних значень необхідно проводити дослідження кожного конкретного приладу (що частково робиться на виробництві) і застосовувати експертні групи. Ціна кожного комплекту представлена в умовних одиницях.

Таблиця 2

Склад системи охорони	P_o	$P_{кл}$	$P_{св}$	$P_{н}^{сер}$	$P_{св}^{кз}$	W_e	C
Ajax StarterKit. Video camera (2 MP)	0.8	0.7	0.9	0.9	0.7	0.32	282
Ajax StarterKit Cam (2 MP)	0.9	0.8	0.9	0.9	0.8	0.47	386
Ajax StarterKit Cam Plus (2 MP)	0.9	0.8	0.9	0.9	0.99	0.58	494
Ajax StarterKit Cam Plus (4 MP)	0.99	0.99	0.9	0.9	0.99	0.79	520
Ajax StarterKit Cam Plus (8 MP)	0.99	0.999	0.9	0.9	0.99	0.793	545

Графік залежності допустимих витрат на захист С від показника ефективності даної ІСО представлено на рис.1.

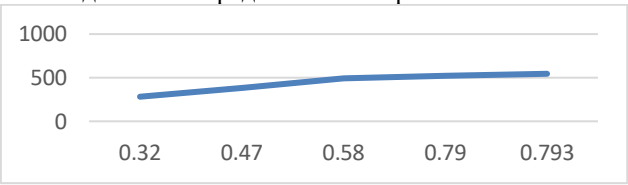


Рисунок 1 – Графік залежності допустимих витрат на захист С від показника ефективності даної ІСО

Аналіз даних таблиці 2 та графіку на рис.1 показує значення і характер зміни складових системи охорони у залежності від імовірнісних показників і, відповідно, витрат. Так, при застосуванні датчика руху без фотоверифікації значення $P_o, P_{кл}$ будуть найменшими, а при тільки двох каналах зв'язку в централі – значення $P_{св}^{кз}$ також буде мінімальним, що визначає найнижчий показник ефективності але, відповідно, найменші витрати. Застосування елементів системи охорони з кращими показниками приводить до збільшення витрат, але і покращення показника ефективності. Разом з цим, запропонована математична модель надає можливість визначати вагу покращення показника ефективності при виборі необхідних елементів.

Список використаних джерел:

1. Vakaliuk T., Dubyna O., Nikitchuk T., Andreiev O. Evaluation of the Effectiveness of the Integrated Security System as an Information System. Proceedings of the 11-th International Conference "Information Control Systems & Technologies", September 21–23, 2023. Odesa, Ukraine. CEUR Workshop Proceedings. 2023. Vol. 3513. pp. 16-26.

2. MIST Aerospace-IV 2021 IOP Conf. Series: Materials Science and Engineering 1227 (2022) 012008 IOP Publishing doi:10.1088/1757-899X/1227/1/012008.

УДК 621.396

Залевський В.Й., ст.наук.співробітник НЦ
Сидорчук О.Л., к.т.н., доцент, ст. викладач
Житомирський військовий інститут імені С.П. Корольова

ДОСЛІДЖЕННЯ ЕЛЕКТРОМАГНІТНОГО ПОЛЯ, ЩО ЗБУДЖУЄТЬСЯ АНТЕННОЮ СИСТЕМОЮ РЛС

Аналіз досліджень щодо перспектив розвитку радіоелектронних засобів озброєння та військової техніки доводить, що їх удосконалення ведеться з використанням новітніх технологій і передбачає збільшення функціональності окремих модулів, антенних систем тощо [1].

Удосконалення антенних систем здійснюється головним чином не шляхом створення принципово нових, а шляхом покращення характеристик і параметрів існуючих [2]**.** У якості опромінювачів таких систем досить часто виступають рупорні антени. В умовах сьогодення постійно виникає потреба у поліпшенні їх характеристик.

Наприклад, переносна РЛС наземної розвідки з індексом 1РЛ133 «Кредо» та більш ранні її модифікації є удосконаленими зразками озброєння. Усі зразки мають схожу антенну систему, яка складається з дзеркального параболоїда та рупорного опромінювача з прямокутною формою розкриву. Антена приймає електромагнітну хвилю лише лінійної поляризації у двосантиметровому діапазоні. Станція «Кредо-М1», у порівнянні з попередніми зразками, має у 1,5-2 рази більшу дальність дії. Основною функціональною особливістю радара є здатність виділяти інформацію про рухомі цілі на фоні різноманітних ландшафтів (кущі, трав'яне покриття, місцеві предмети), удень і вночі, у складних метеорологічних умовах (дощ, сніг, туман, задимлення, запилення атмосфери). Тобто станція має достатньо високі показники розрізнювальної здатності [2]. Такі показники у першу чергу залежать від поляризаційних характеристик антенної системи. Їх подальше покращення потребує більш детальних досліджень щодо визначення амплітуд електромагнітного поля, які збуджуються на розкриві опромінювача за різних поляризаційних властивостей хвилі, що випромінюється через антенну систему, та повертається назад від об'єкта зондування [2]. Це обумовлює необхідність з'ясування розсіювальних властивостей таких системи шляхом дослідження дифракції електромагнітного поля на її опромінювачі.

При побудові антенної системи станції «Кредо-М1» та більш ранніх подібних зразків приймально-передавальну антенну систему було спроектовано за умови, що площина поляризації хвилі, яка падає, і

площина її падіння співпадають. Інший випадок [1], а саме якщо хвиля є нормально (перпендикулярно) поляризованою до площин свого падіння не враховувався. Суперпозиція обох варіантів і є випадком довільного падіння. Таке поєднання у подальшому дозволить зробити висновки щодо можливості покращення поляризаційних характеристик антенних системам РЛС.

У доповіді надаються результати дослідження амплітуди електромагнітного поля, що збуджуються рупорним опромінювачем антенної системи. Розглянуто нестандартний випадок падіння хвилі, а саме за умови, що хвиля, яка повертається від об'єкта зондування, є нормально поляризованою до площини свого падіння. Визначення амплітуд поля та їх моделювання здійснено методами Гюйгенса-Кірхгофа та із застосуванням леми Лоренца.

Моделювання здійснено для двох типів (Е- і Н- площинних) рупорів, один з яких має параметри опромінювача антенної системи РЛС. Результати моделювання доводять, що на відміну від діаграм, отриманих за виразом із застосуванням методу Гюйгенса-Кірхгофа, подальше збільшення або зменшення довжини падаючої хвилі призведе до зменшення амплітуди. Таким чином вираз, отриманий із застосуванням леми Лоренца, є точнішим. Діаграми амплітуд поля не мають задніх та бокових пелюсток. Це свідчить про те, що врахування коефіцієнта відбиття у виразі дозволить провести більш якісніше моделювання у порівнянні із відомими (2).

Виведені на надані у доповіді вирази мають не тільки розрахунково-практичне, але й методичне значення. Їх використання сприятиме подальшим дослідженням розсіяного поля не тільки від поодинокого опромінювача, але й від системи «дзеркало + опромінювач», антенних решіток та інших подібних систем, що мають у якості опромінювачів рупори пірамідальної форми.

Список використаних джерел:

1. Сидорчук О. Л. Математичний апарат дослідження амплітуд поля, збудженого антенною системою радіолокаційної станції 1РЛ133 «Кредо» / О. Л. Сидорчук // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць. – Житомир : ЖВІ, 2016. – Вип. 13. – С. 62–72.

2. Sidorchuk O., Tofanchuk O., Methodology improvment of the electromagnetic field amplitude study related to the antenna system risk radio-solid station of land-development "Credo-M1" // Scientific works of Kharkiv National Air Force University. 2017. № 5 (54). С.102–109.

УДК 621.382.004.31

Клочко К.А., к.т.н., доцент
Пупков С.С., здобувач
Дніпровський державний технічний університет

РОЗПОДІЛЕНА СИСТЕМА КЕРУВАННЯ ТРАФІКОМ В «РОЗУМНОМУ» МІСТІ

Виробництво, транспорт, логістика та ланцюги постачання на сьогодні переживають період швидких та безпрецедентних перевтілень. Тому впровадження розумних технологій у вже сформовані міські системи набуває все більшої актуальності. Концепції Сталого розвитку адаптують місто до сучасного комфортного проживання в ньому.

Елементи «розумного» міста все частіше зустрічаються в організації роботи транспорту, вивезення сміття, облаштування паркінгів, зупинок та вуличного освітлення. А залучення інвестицій дозволяють розробити нові сервіси, які автоматизують процеси збору та аналізу інформації з датчиків, які були з ручним управлінням [1, 2].

Під розподіленою системою керування трафіком руху в «розумному» місті розуміємо таку систему керування, яка включає в себе систему розумного освітлення, що дозволяє налагодити міське освітлення, знизити витрати й зробити простір більш безпечним, систему управління світлофорами, яка дозволяє організувати безпечний та зручний рух автотранспорту містом, особлива увага приділяється перехрестям проїзних частин та V2X (Vehicle-to-Everything) – це технологія, що дозволяє транспортним засобам обмінюватися даними в режимі реального часу з усім, що їх оточує [3].

Для скорочення витрат на оплату рахунків за спожиту електроенергію вуличні ліхтарі оснащуються лампочками із датчиками руху, які за відсутності перехожих світять на 10-15% від номінальної потужності, а коли вони з’являється – лампочка включається на всю потужність. Датчики регулюють рівень освітленості: влітку зовнішнє освітлення включається пізніше, а взимку – раніше. Слід зазначити, що стабільне освітлення дає містянам більший комфорт та відчуття безпеки.

Керування світлофорами – це можливість організувати безпечний та зручний рух транспортних засобів та пішоходів в місті. Пропускна здатність доріг збільшується, що дозволяє швидше прибути в пункт призначення, а користуватися громадським транспортом стає більш комфортним. Світлофорні системи оснащуються датчиками, системами відеоспостереження та контролерами, які збирають та

аналізують дані в автоматичному режимі, що дозволить регулювати пропускну здатність доріг в залежності від щільності потоку машин [2].

Впровадження V2X-технології дозволить екосистемі автомобілів обмінюватись інформацією між собою та з інфраструктурою (світлофори, знаки дорожнього руху, пішоходи, місця для паркінгу), з використанням мобільних додатків або вбудованих в автомобіль систем з штучним інтелектом, та центрів обробки даних через стільникові мережі. Виділяють кілька компонентів V2X: зв'язок «транспортний засіб – транспортний засіб» (V2V), зв'язок «транспортний засіб – інфраструктура» (V2I), зв'язок «транспортний засіб – пішохід» (V2P) і зв'язок «транспортний засіб – мережа» (V2N). Різні варіанти використання даної технології матимуть різні набори вимог, які система зв'язку повинна обробляти ефективно, швидко і з мінімальними витратами [4].

Таким чином, розподілена система керування трафіком в «розумному» місті має охоплювати сучасні тенденції та можливості на ринку інтелектуального управління дорожнім рухом, включаючи використання штучного інтелекту та автоматизації в інтелектуальних рішеннях для його управління. Зростаюче впровадження технологій «від транспортного засобу до всього» (V2X) дозволить керувати дорожнім рухом у режимі реального часу шляхом підключення транспортних засобів до навколишнього середовища (світлофори, знаки дорожнього руху, пішоходи, місця для паркінгу) за умов встановлення даної технологій на кожному транспортному засобі.

Список використаних джерел:

1. Smart city: розумні технології сучасного міста. Огляди рішень. Режим доступу: https://hub.kyivstar.ua/articles/smart-city-rozumni-tehnologiyi-suchasnogo-mista (дата звернення: 20.10.2025).

2. Мішель Джойнсон «Зростання ринку розумного управління дорожнім рухом, що стимулюється сталим розвитком та урбанізацією, досягне 20 мільярдів доларів до 2027 року». Режим доступу: https://www.juniperresearch.com/research/sustainability-smart-cities/smart-cities/smart-traffic-management-research-report/ (дата звернення: 20.10.2025).

3. Спосіб розподіленої аеродинамічної компенсації дії вітрових збурень на траєкторію польоту повітряного судна: пат. 102654 Україна: B64C 13/00, B64C 13/16. № a 2012 09351 ; заявл. 31.07.2012 ; опубл. 25.07.2013, Бюл. № 14. 4 с.

4. What Is Vehicle To Vehicle OR V2V Communication Technology? Режим доступу: https://carbiketech.com/vehicle-to-vehicle-v2v-communication/ (дата звернення: 20.10.2025).

УДК 621.396.01

Колос Ю.О., к.т.н., доцент
Маслов О.А., викладач
Житомирський військовий інститут імені С. П. Корольова

МЕТОДИКИ І РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ВІДБИВНИХ ВЛАСТИВОСТЕЙ БПЛА З РІЗНИМИ ПОКРИТТЯМИ

Відомо, що ефективність застосування БПЛА в значній мірі залежить від здатності подолання ППО противника. Тому, одним з напрямків удосконалення БПЛА є зменшення його ефективної поверхні розсіювання (ЕПР). Важливим етапом виробництва і впровадження таких БПЛА є розробка та дослідження матеріалів, що дозволяють зменшити відбиття радіохвиль, а також дослідження ЕПР фюзеляжу БПЛА з використанням таких матеріалів.

В доповіді запропоновано використання різних методик і представлено результати досліджень відбивних властивостей як матеріалів, так і фюзеляжів БПЛА в лабораторних умовах.

З урахуванням наявних пристроїв та їх можливостей вибрані параметри, які дозволяють порівнювати ЕПР (відбивні властивості) об'єктів дослідження:

1. Коефіцієнт стоячої хвилі у фідері, в якому поширюються радіохвиля, що випромінюється і прийнята від об'єкту дослідження хвиля;
2. Коефіцієнт затухання радіохвилі, що відбивається від об'єкту дослідження;
3. Рівень сигналу, відбитого від об'єкту дослідження.

Отримано аналітичні вирази для оцінки зміни ЕПР за зміною вибраних вимірюваних параметрів. Приводяться результати досліджень 11 видів матеріалів та 5 фюзеляжів з різними покриттями в діапазоні частот 2,4…9 ГГц.

Дослідження проводилось шляхом порівняння існуючих та розроблених матеріалів, частин фюзеляжів і фюзеляжів в цілому.

Отримані експериментальні дані щодо впливу на ЕПР спеціального покриття, кількості шарів покриття, технології виконання матеріалів, кута спостереження об'єкту, наявності в конструкції БПЛА металевих елементів (кріплення двигуна та катапульти запуску, бойова частина). Встановлені елементи і деталі конструкції, що формують локальні піки відбиття. Основне відбиття спостерігалось від вогнутих і пласких частин.

В результаті лабораторних досліджень встановлено, що ряд матеріалів навпаки призводять до посилення відбиття до 20-25%. Тому їх використання недоцільно.

Ряд матеріалів також є не ефективними тому, що зменшують відбиття лише в межах 5%.

Разом з тим були відібрані ефективні матеріали, які були застосовані для виготовлення фюзеляжів. Ці матеріали знижували потужність відбитого сигналу від 3 до 7 дБ в залежності від ракурсу та частоти.

Крім того, встановлено частоти на яких обрані матеріали дозволяють найкраще зменшити відбиття, а на яких менш ефективні.

При зміні частоти в діапазоні 3…5 ГГц рівень відбитого сигналу може змінюватись на 4,7 дБ для одного і того ж об'єкту чи матеріалу.

Дослідження багатошарового покриття фюзеляжу показало, що покриття 2 шарами приводить до зменшення потужності відбиття в 3 і більше разів, коли немає масо габаритного макету бойової частини, і більше ніж у 4 рази, коли фюзеляж споряджений в порівнянні з фюзеляжем без покриття.

Потужність відбиття від фюзеляжу з покриттям в 3 шари на 40 – 60 % більше за потужність відбиття від фюзеляжу з покриттям у 2 шари. Тобто покриття у 2 шари краще ніж у 3 шари.

Спостерігається менше відбиття від фюзеляжу з 2 шарами покриття в порівнянні з відбиттям з трьома шарами, як і в Х-діапазоні. Тобто ефективність двошарового покриття вище.

Результати досліджень ЕПР шляхом обльоту БПЛА різними покриттями з використанням радару в реальних умовах збігаються з результатами лабораторних досліджень.

Тому одним з висновків роботи є доцільність відбору матеріалів на першому етапі в лабораторних умовах, а на другому етапі випробування їх в реальних умовах шляхом обльоту радару.

Список використаних джерел:

1. Knott, E. F., Schaeffer, J. F., Tuley, M. T. Radar Cross Section. 2nd ed. Raleigh: SciTech Publishing, 2004. 611 p.

2. Сухаревський О. І., Василець В. О., Нечитайло С. В. Довідник характеристик розсіювання повітряних та наземних радіолокаційних об'єктів. Харків : ХНУПС, 2019. 304 с.

УДК 629.783

Рихальський О.Р., к.т.н., доц., ст. викладач,
Каращук Н.М., к.т.н., доцент, ст. викладач
Петраш С.В., к.т.н., доц., доцент
Житомирський військовий інститут імені С.П. Корольова

МОДЕЛЮВАННЯ АНТЕННИХ СИСТЕМ З ВИСОКОВОЛЬТНИХ ЛІНІЙ ЕЛЕКТРОПЕРЕДАЧ ПРИ ДОСЛІДЖЕННІ ВПЛИВУ ЇХ ВИПРОМІНЮВАННЯ НА ФОРМУВАННЯ PLHR ВИПРОМІНЮВАННЯ В ІОНОСФЕРІ

За допомогою супутникових досліджень у 80-х роках минулого століття був відкритий ефект – відображення в іоносфері, і навіть у магнітосфері, гармонічного випромінювання електромереж – (power line harmonic radiation, PLHR). Встановлено, що потужні споживачі електроенергії формують на частотах, пов'язаних із частотою електромереж і її численними гармоніками, техногенні сигнали, які викликають зміни параметрів плазми та електромагнітного поля в іоносфері. І цей вплив стає останнім часом все помітнішим із-за зростаючого рівня виробництва та використання електричної енергії.

На сьогодні накопичено великий обсяг експериментальних даних супутникових досліджень, які переконливо свідчать про існування в іоносфері кластерів (мультиплетів) спектральних ліній гармонік 50 (60) Гц (аж до 10-15 ліній), центрованих біля середньої частоти, яка може змінюватися в досить широкому діапазоні - від 1 до 15 кГц. Дані отримано в експерименті на штучному супутнику Землі (ШСЗ) "Деметер"(2004- 2010 рр.), "Січ-1М"(2005 р.). Крім того, отриманий результат з борту ШСЗ "Чібіс-М" (запущеного 25.01.2012 р.) – вимірювання електричного поля при пролітанні ШСЗ над територією Бразилії. Орбіта "Чібіс-М" була майже колова на висоті 520 км, 08.08.2013 р., 03:47:34 - 03:53:34. Було чітко встановлено проникнення сигналу 60 Гц на висоти іоносфери. Електромережі протяжністю у сотні і тисячі кілометрів є антенами великої потужності. Явище випромінювання мультиплетів лініями електромереж реєструють над усією поверхнею Землі, але найчастіше у поясі геомагнітних широт (20 − 60)^{o}, тобто над економічно розвинутими районами. У відкритій лінії передачі електромагнітної енергії, якими є повітряні лінії електропередачі (ЛЕП) змінного струму, поле спрямованої хвилі не екрановане й існує у просторі, що оточує лінію.

При дослідженнях повітряна ЛЕП змінного струму розглянута як антенна система відповідної структури, яка складається з елементарних

електричних горизонтальних вібраторів, які підняти за допомогою опор над поверхнею Землі. В першому наближенні Земля та атмосфера розглядається як сферично шарувате середовище, електричні параметри якого залежать тільки від висоти до гладкої сферичної поверхні Землі. Конструкція і розміри опор ЛЕП визначаються її робочою напругою. Із зростанням робочої напруги збільшуються розміри і складність конструкцій ЛЕП.

За допомогою програми MMANA здійснено моделювання повітряних ЛЕП різних класів та конфігурацій, як антенних систем. Зокрема досліджено зміну коефіцієнта підсилення антенних систем відповідних моделей повітряних ЛЕП в смузі частот гармонічного випромінювання електромереж PLHR від 1 кГц до 5 кГц з кроком 50 Гц. Це частково якісно пояснює вплив зміни об'ємної густини енергії поля електромереж на інтенсивність ліній PLHR.

Список використаних джерел:

1. Ваврух М. Механізм формування ліній гармонічного випромінювання в іоносфері / М. Ваврух, В. Корепанов // Вісник Львівського ун-ту. Серія фізична. 2013. Вип. 48. С. 180–197. ISSN 1024-588X.

2. Дудкін Д. Ф. Випромінювання ліній електропередач у навколоземному просторі / Д. Ф. Дудкін, В. О. Проненко, В. Є. Корепанов, С. І. Клімов //. Космічна наука і технологія. 2014. Т. 20, № 5. С. 27–34. ISSN 1561-8889.

3. Nemec F., Parrot M., Santolik O. Influence of power line harmonic radiation on the VLF wave activity in the upper ionosphere: Is it capable to trigger new emissions. // J. Geophys. Res. 2010. 115. P. A11301. doi:10.1029/2010JA015718

4. Zelenyj L. M., Gurevich A. V., Klimov S. I. Academic microsatellite CHIBIS-M. // Space research. 2014. Vol. 1, Iss. 1. P. 52.

5. Рихальський О. Р. Аналітичне дослідження впливу випромінювання високовольтних ліній електропередач на формування гармонічного випромінювання в іоносфері. / О. Р. Рихальський, Н. М. Каращук, Р. В. Нетребко //Збірник наукових праць. – Житомир: ЖВІ, 2024. – Вип. 26. – С.81–92. https://doi.org/10.46972/2076-1546.2024.26.

УДК 621.37

Полегешко Д.В., здобувач
Водько А.М., здобувач
Івасишин Ю.І., здобувач
Сотник О.А., асистент
Дніпровський державний технічний університет

ОРГАНІЗАЦІЯ ВІДДАЛЕНОГО ДОСТУПУ ДО АПАРАТНИХ ЛАБОРАТОРНИХ СТЕНДІВ НА ОСНОВІ RED PITAYA ТА СИСТЕМИ LIBREBOOKING

Анотація. У роботі описано принципи організації віддаленого доступу до лабораторного стенду Red Pitaya RP-122-16, інтегрованого з системою бронювання LibreBooking та VPN WireGuard. Реалізовано ізоляцію сесій через overlay-root та механізм автоматичного очищення середовища. Наведено ключові архітектурні елементи, результати первинних експериментів та типовий зміст лабораторних завдань.

Сучасна інженерна освіта потребує доступу до реального апаратного обладнання поза межами фізичної лабораторії. Red Pitaya RP-122-16 [1] завдяки своїм вимірювальним можливостям є придатною платформою для побудови віддалених лабораторій. Основним викликом є організація безпечного, ізольованого та масштабованого доступу для здобувачів освіти. Розроблена система вирішує питання маршрутизації, аутентифікації, бронювання часу роботи та гарантує, що кожен користувач працює у незалежному середовищі, яке не впливає на інших.

Архітектура системи. Архітектура включає такі компоненти: сервер LibreBooking, що керує часовими слотами доступу й аутентифікацією; VPN-сервер WireGuard [2], який генерує користувацькі ключі та встановлює захищений канал; Nginx reverse-proxy для маршрутизації HTTP/SSH/WebSocket-запитів; набір субдоменів виду *lb.domain.ua, rp1.domain.ua*; а також Red Pitaya RP-122-16, що працює під керуванням операційної системи на базі ядра Linux.

Механізм ізоляції сесій. Для забезпечення чистого та незалежного середовища використано overlay-root [3]. Основна файлова система Red Pitaya монтується у режимі read-only, тоді як усі зміни під час сесії зберігаються у tmpfs. Після завершення бронювання тимчасові дані видаляються автоматично, що унеможливлює стороннє втручання та гарантує повторюваність лабораторних умов.

Реалізація інтеграції з LibreBooking. Система LibreBooking [4] використовується як центральний механізм керування доступом. Для кожного стенду Red Pitaya створюється окремий ресурс. Після

підтвердження бронювання виконується генерація ключа WireGuard, активується доступ до відповідного субдомену, запускається лічильник часу сесії, а завершення роботи відбувається після неактивності або закінчення зарезервованого інтервалу. Реалізовано REST-сповіщення, які інформують стенд про початок і завершення користувацької сесії.

Результати вимірювань. Проведено первинні експерименти із використанням мобільного клієнта через тунель WireGuard. Затримка ping через VPN становила 79–113 мс, середнє значення — 92–98 мс, що відповідає типовим характеристикам LTE-мереж. Затримка доступу до веб-інтерфейсу Red Pitaya (TCP-handshake) перебувала в діапазоні 88–110 мс, а час до отримання першого HTTP-байта (TTFB) – 95–120 мс. Отримані значення підтверджують стабільність роботи тунелю WireGuard і можливість повноцінного віддаленого керування лабораторним стендом у режимі реального часу.

Типовий зміст лабораторних завдань. Лабораторні завдання охоплюють базові та прикладні операції з використанням Red Pitaya, зокрема генерацію тестових сигналів, проведення осцилографічних вимірювань, аналіз частотної структури сигналів та роботу з інтерактивними веб-інтерфейсами пристрою у режимі реального часу.

Висновки. Запропонована система забезпечує масштабований, безпечний та ізольований віддалений доступ до апаратних лабораторних стендів. Комбінація LibreBooking, WireGuard, reverse-proxy та overlay-root формує основу для організації дистанційних лабораторних робіт з інженерних дисциплін. Подальший розвиток системи передбачає розширення набору лабораторних завдань, впровадження журналювання дій користувачів, інтеграцію додаткових стендів (STM32, ESP32, SDR), а також аналіз продуктивності reverse-proxy та overlay-root у масштабованих конфігураціях.

Список використаних джерел

1. Red Pitaya. Documentation and API Reference [Електронний ресурс].– Режим доступу: https://redpitaya.readthedocs.io/en/latest/ (дата звернення: 01.11.2025).

2. WireGuard Whitepaper [Електронний ресурс]. – Режим доступу: https://www.wireguard.com/papers/wireguard.pdf (дата звернення: 01.11.2025).

3. OverlayFS: Linux Kernel Documentation [Електронний ресурс]. – Режим доступу: https://docs.kernel.org/filesystems/overlayfs.html (дата звернення: 01.11.2025).

4. LibreBooking – Open-source booking platform [Електронний ресурс].– Режим доступу: https://github.com/LibreBooking (дата звернення: 01.11.2025).

УДК 321.396

Скрипніченко В.О., магістрант,
Морозов Д.С., ст. викладач,
Чухов В.В., к.т.н., доцент,
Фещенко С.О., аспірант
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ ДІЕЛЕКТРИЧНИХ ЛІНЗ З ПЕРІОДИЧНОЮ ПЕРФОРАЦІЄЮ ДЛЯ ЗМЕНШЕННЯ РІВНЯ БІЧНИХ ПЕЛЮСТОК РУПОРНИХ АНТЕН

Застосування діелектричних лінз на рупорних антенах дозволяє змінювати форму фазового фронту рупорного випромінювача, без зміни основної геометрії антени [1]. Завдяки керованій зміні швидкості поширення хвилі всередині діелектричного матеріалу лінза забезпечує зменшення розходження променю, покращують рівень бічних пелюсток і дозволяє сформувати рівномірніший фазовий розподіл на апертурі [2].

Одним із перспективних напрямів удосконалення діелектричних лінз є застосування періодичних структур, сформованих шляхом локального зменшення ефективної діелектричної проникності. До таких рішень належать лінзи з прямокутними вирізами, рівномірно розміщеними по всій робочій площині [3]. Завдяки використанню 3D-друку, стає можливо точніше формувати внутрішню геометрію діелектрика без істотного збільшення його маси або складності конструкції (рис.1).

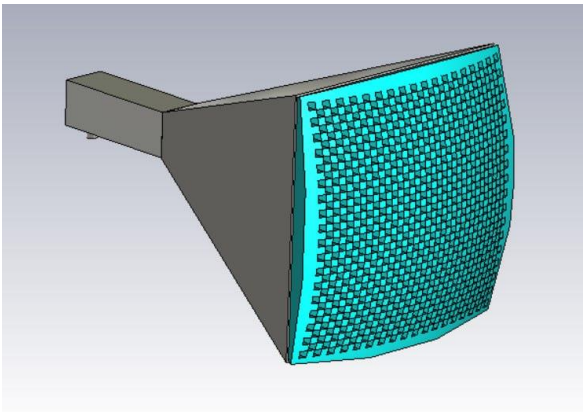


Рисунок 1 – Ескіз рупорної антени з діелектричною лінзою

У дослідженні використано діелектричний матеріал з ε_r=2,5, що відповідає легким та технологічно зручним для друку пластикам PETG. Прямокутні вирізи в лінзі мають форму регулярної квадратної решітки з геометричними розмірами 3,47 мм на 3,47 мм.

Таке компонування забезпечує контрольоване зниження ефективної діелектричної проникності та дозволяє формувати необхідний градієнт показника заломлення по площині лінзи.

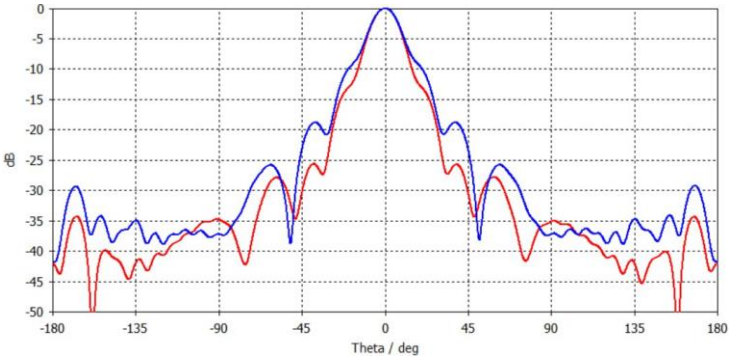


Рисунок 2 – Діаграма спрямованості рупорної антени з діелектричною лінзою (червона лінія) і без діелектричної лінзи (синя лінія)

Використання діелектричної лінзи дозволило знизити рівень бічних пелюсток з -18 дБ до -25 дБ (рис. 2), що свідчить про покращення просторової селективності рупорних антен.

Діелектричні лінзи з періодичною перформацією є простим і недорогим у виготовленні способом побудови і модернізації антенних систем на основі рупорних антен.

Список використаних джерел:

1. Carvalho S., Reis J., Mateus A., Caldeirinha R. Exploring design approaches for 3D printed antennas. *IEEE Access*. 2024. Vol. 12. P. 10718–10735. DOI: 10.1109/ACCESS.2024.3354372.

2. Whittaker T., Zhang S., Powell A., Stevens C. J., Vardaxoglou J. Y. C., Whittow W. 3D printing materials and techniques for antennas and metamaterials: a survey of the latest advances. University of Exeter. 2022. URL: https://hdl.handle.net/10871/132352

3. Baharom B. et al. Reduction of surface reflection on dielectric lens antenna by matching periodic square-pillars in 300-GHz band. *IEEE Access*. 2023. Vol. 11. P. 8481–8491. DOI: 10.1109/ACCESS.2023.3239397.

УДК 621.396.73

Фриз С.П.,
заслужений працівник освіти України, д.т.н, проф., професор,
Авсієвич Р.О., доктор філософії, доцент
Житомирський військовий інститут ім. С.П. Корольова

ВДОСКОНАЛЕННЯ МЕТОДІВ РАДІОМОНІТОРИНГУ НИЗЬКООРБІТАЛЬНИХ КОСМІЧНИХ СИСТЕМ

Станом на травень 2025 року на навколоземній орбіті експлуатувалося більше 12000 космічних апаратів, з яких більше 90 % були виведені на низьку навколоземну орбіту. В перспективі до 2030 року прогнозується збільшення кількості космічних апаратів саме на низькій навколоземній орбіті [1]. За вказаних умов виникає потреба у застосуванні методів радіомоніторингу для покращення космічної ситуаційної обізнаності та уникнення колізій космічних апаратів під час їх руху по земній орбіті.

Однак, радіомоніторинг низькоорбітальних космічних апаратів ведеться за наявності впливу ряду факторів, що знижують його ефективність: часові та енергетичні обмеження, обумовлені параметрами орбіти космічних апаратів, похибки синхронізації радіоприймального тракту з вхідним сигналом, обумовлені апріорною невизначеністю щодо параметрів радіосигналів та впливом ефекту Доплера, необхідність використання спеціалізованих антенних систем та систем синхронізації тощо. Зазначене вимагає впровадження на наземних приймальних станціях радіомоніторингу універсальних методів виявлення та виміру параметрів радіосигналів низькоорбітальних космічних апаратів, в тому числі тих, які придатні для застосування в умовах часткової апріорної параметричної невизначеності щодо радіосигналів, які випромінюються космічними апаратами [2].

В роботі розглянуто можливість вдосконалення пошукового методу виявлення радіосигналів, що базується на застосуванні критерію Неймана-Пірсона та періодограмного методу Уелча для виявлення радіосигналів низькоорбітальних космічних апаратів та оцінки їх спектральної щільності. В подальшому для уточнення параметрів виявленого радіосигналу пропонується застосовувати метод кореляційної обробки радіосигналів, заснований на розрахунку коефіцієнту кореляції Пірсона, який дозволяє уточнити частотні параметри радіосигналу через дискретний підбір тривалості символу.

Реалізація вдосконаленого пошукового методу можлива шляхом застосування програмних засобів, в основі яких лежать методи цифрової обробки радіосигналів. Зазначене дозволяє проводити виявлення та вимірювання параметрів радіосигналів в автоматичному режимі, що покращує ефективність ведення радіомоніторингу.

Застосування вказаного методу можливе спільно з радіоприймальними пристроями, побудованими за технологією програмно визначеного радіо.

Перевагою застосування запропонованого методу є можливість його використання в умовах впливу ефекту Доплера для більш точного визначення таких параметрів радіосигналів, як: центральна несуча радіочастота, ширина спектру радіосигналу та тривалість символу.

Практична цінність запропонованого методу полягає в тому, що він дозволяє зняти обмеження щодо ширини спектру сигналів під час вирішення завдань радіомоніторингу низькоорбітальних космічних систем із застосуванням програмно-визначених радіоприймальних пристроїв [3].

Зазначене реалізується завдяки застосуванню розробленого математичного апарату для розрахунку кроку зміни частоти гетеродину у блоці формування проміжних частот приймальних пристроїв, що в свою чергу впливає на визначення розміру частотних сегментів, що беруть участь в оцінці потужності спектральної щільності спектру сигналу, а також завдяки реалізації перекриття частотних смуг у суміжних частотних сегментах з подальшим їх згладженям.

Список використаних джерел:

1. База даних CelesTrak. Режим доступу: https://celestrak.org/satcat/search.php (дата звернення 20.11.2025).

2. ITU Publication Handbook Spectrum Monitoring. Режим доступу: https://www.itu.int/pub/R-HDB-23-2011 (дата звернення 20.11.2025).

3. Utilizing SDR for increased bandwidth in satellite communications. Режим доступу: https://apps.dtic.mil/sti/trecms/pdf/AD1136078.pdf (дата звернення 24.11.2025).

УДК 621.37

Антонюк С.С., бакалавр
Ципоренко В.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

СИСТЕМА СИГНАЛІЗАЦІЇ НА ОСНОВІ ДАТЧИКА РУХУ З АВТОМАТИЧНИМ ПЕРЕДАВАННЯМ ФОТОГРАФІЇ ТА ВКЛЮЧЕННЯМ ЗВУКОВОЇ СИГНАЛІЗАЦІЇ ПО КОМАНДІ З ВИКОРИСТАННЯМ МОБІЛЬНОГО ДОДАТКУ TELEGRAM

Метою роботи було розробити та експериментально перевірити систему сигналізації, здатну автоматично виявляти рух за допомогою PIR-датчика, здійснювати фотофіксацію за допомогою камери та передавати знімки разом із сповіщенням користувачеві через мобільний додаток Telegram. Додатковою функцією є дистанційна активація звукової сигналізації по команді з Telegram. Дослідження передбачало аналіз існуючих рішень, вибір оптимальних компонентів, розробку електричних схем та програмного забезпечення. Результати цієї розробки можуть знайти застосування у сфері домашньої безпеки, для захисту невеликих комерційних об'єктів.

Об'єктом вивчення є процес побудови та програмно-апаратної реалізації системи моніторингу на основі мікроконтролера ESP32-CAM. Для виявлення руху використовується інфрачервоний PIR-датчик HC-SR501, а для звукового сповіщення – активний бюзер. Для забезпечення надійності система включає модуль аварійного живлення.

В ході розробки було створено функціональну схему, рис. 1, яка реалізує взаємодію всіх компонентів. Програмний код для мікроконтролера було розроблено в середовищі Arduino IDE з використанням бібліотек для роботи з камерою, Wi-Fi та Telegram API. Алгоритм роботи системи, рис. 2, передбачає ініціалізацію, підключення до мережі, очікування сигналу від датчика руху, захоплення та відправку фотографії в Telegram-бот, а також обробку команд користувача для активації звукової сигналізації.

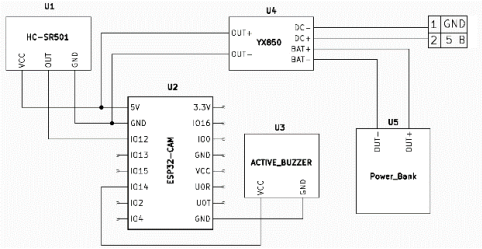


Рисунок 1 – Схема електрична функціональна системи сигналізації

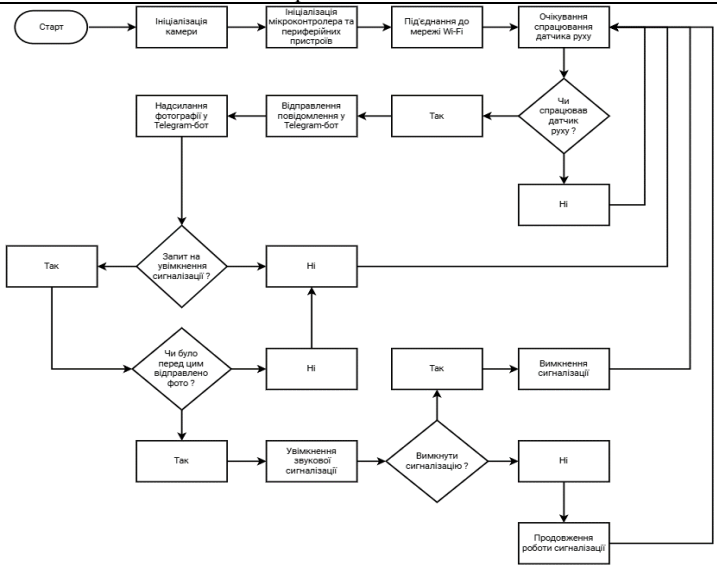


Рисунок 2 – Алгоритм виконання програми

Для перевірки роботи системи було зібрано діючий макет та проведено його всебічне тестування. Результати експерименту показали, що система стабільно виявляє рух, коректно захоплює зображення з роздільною здатністю 800x600 (SVGA) та миттєво передає його у заданий чат Telegram. Час між виявленням руху та отриманням повідомлення користувачем не перевищує 3 секунди. Команди керування базером (/buzzer) та світлодіодом спалаху (/flash), виконуються коректно. Система стабільно працює та відповідає ТЗ.

Результати тестування підтвердили правильність обраної архітектури та доцільність використання вибраних компонентів. Завдяки простоті, низькій собівартості та універсальності пристрій може бути інтегрований у системи безпеки різного рівня складності, забезпечуючи надійний та сучасний спосіб моніторингу об'єктів.

Список використаних джерел:

1. Бездротова камера з Wi-Fi – Ajax IndoorCam. Ajax Systems [Електронний ресурс]. – 2025. – Режим доступу: https://ajax.systems/ua/products/indoorcam.

2. Telegram Group: Control ESP32/ESP8266 Outputs (Arduino IDE) | Random Nerd Tutorials. Random Nerd Tutorials [Електронний ресурс]. – 2025. – Режим доступу: https://randomnerdtutorials.com/telegram-group-esp32-esp8266.

УДК 621.391

Воробкало Т.В., к.т.н., доцент
Воробкало О.К., студент
Черкаський державний технологічний університет

ОЦІНЮВАННЯ ІНФОРМАТИВНИХ ПАРАМЕТРІВ РАДІОСИГНАЛУ У БАГАТОКАНАЛЬНИХ СИСТЕМАХ ЗА УМОВ НЕГАУСІВСЬКИХ ЗАВАД

В радіотехнічних системах інформація передається за допомогою фізичних параметрів радіосигналів. Параметри, які змінюються відповідно до переданої інформації, називаються інформативними параметрами. Вибір параметра визначає тип модуляції, можливу завадостійкість, смугу частот, енергетичну ефективність та складність приймально-передавальної апаратури. Одними з основних інформативних параметрів радіосигналів є частота, фаза та часові характеристики. Ці параметри зазвичай використовуються для визначення параметрів джерела сигналу та каналу передачі [1].

Оскільки радіосигнали надходять до приймача на фоні завад, процес визначення інформативних параметрів передбачає виконання процедур оцінювання цих параметрів. Одним з ефективних методів оцінювання параметрів випадкових величин є метод максимізації полінома [2], який дозволяє оптимально враховувати статистичні властивості негауссівських завад. Підвищити точність оцінювання інформативних параметрів радіосигналів, а отже – збільшити завадостійкість приймальної системи та покращити надійність її роботи, можна також шляхом використання багатоканальної обробки. Тому метою роботи є розроблення алгоритмів оцінювання інформативних параметрів радіосигналу в умовах негауссівських завад із використанням методу максимізації полінома та багатоканальної обробки, а також дослідження асимптотичних властивостей отриманих оцінок.

У роботі побудовано модель випадкової величини, що приймається багатоканальною системою і являє собою адитивну суміш радіосигналу та негауссівської завади. Для опису завади використано моментно-кумулянтний підхід. Невідомими інформаційними параметрами, що підлягають оцінюванню, є частота сигналу та час запізнення, які, відповідно, несуть інформацію про радіальну швидкість та просторове положення джерела випромінювання. Усі інші параметри радіосигналу та завади вважаються апріорно відомими.

Відповідно до методу максимізації полінома у роботі розроблено алгоритми для знаходження оцінок частоти та часу запізнення радіосигналу при багатоканальному прийомі на фоні негауссівських завад при 1-му, 2-му та 3-му степенях поліному. Якщо невідомий лише один з параметрів, його оцінка визначається з розв'язку відповідного рівняння; якщо невідомі обидва параметри – виконується їх сумісне оцінювання шляхом розв'язку системи двох рівнянь.

Також у роботі досліджено точність алгоритмів оцінювання. При першому степені полінома отримується лінійна оцінка, яка не залежить від кумулянтних коефіцієнтів негаусівської завади. Дисперсії таких оцінок стандартно залежать від відношення сигнал/шум, кількості вибіркових значень та числа приймальних пристроїв і не демонструють покращення точності, слугуючи базою для порівняння з нелінійною обробкою при використанні поліномів вищих степенів.

При другому та третьому степені стохастичного полінома отримано дисперсії оцінок частоти та часу запізнення радіосигналу, які при порівнянні з лінійною обробкою демонструють зменшення дисперсії оцінок завдяки врахуванню коефіцієнтів асиметрії та ексцесу завади. Введено коефіцієнт ефективності, який показує ступінь покращення точності порівняно з лінійною обробкою. Показано, що при ненульових значеннях асиметрії та ексцесу дисперсія оцінок із ростом степеня полінома зменшується та прямує до нуля при наближенні параметрів розподілу завади до граничних значень.

Для сумісного оцінювання двох інформаційних параметрів побудовано варіаційні матриці, з яких видно, що спільне оцінювання параметрів приводить до збільшення їх дисперсій порівняно з окремим оцінюванням але при цьому зберігається покрашення точності завдяки врахуванню характеристик негауссівської завади.

Отже, використання методу максимізації полінома дозволяє отримати більш точні оцінки інформативних параметрів радіосигналу при багатоканальному прийомі в умовах негауссівських завад порівняно з традиційними методами, що ґрунтуються на припущенні гауссівського характеру завад. Розроблені алгоритми можуть бути покладені в основу високоточних пристроїв радіолокаційного визначення параметрів джерела сигналу у реальних завадових умовах.

Список використаних джерел:

1. Васильєв В. М. Радіонавігаційні системи: підручник / В. М. Васильєв. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2023. – 338 с.

2. Kunchenko Y.P. Polynomial parameter estimation of close to Gaussian random variables. – Aachen: Shaker Verlag, 2002. – 396 p.

УДК 621.396.67:004.77

Денисюк М.С., бакалавр,
Ципоренко В.Г., к.т.н., доцент
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ АНТЕН ДЛЯ БЕЗДРОТОВИХ МЕРЕЖ ІОТ В ПОБУТОВИХ УМОВАХ

У сучасних умовах швидкого розвитку інформаційно-комунікаційних технологій, бездротові мережі Інтернету речей (IoT) стали невід'ємною частиною повсякденного життя, забезпечуючи автоматизацію побутових процесів, моніторинг навколишнього середовища та інтеграцію розумних пристроїв у домогосподарствах. Антени, як ключові елементи цих мереж, відіграють вирішальну роль у забезпеченні стабільного зв'язку, мінімізації втрат сигналу та оптимізації енергоспоживання. У побутових умовах, де перешкоди у вигляді стін, меблів та електромагнітних завад є типовими, ефективність антен безпосередньо впливає на надійність систем, таких як розумні будинки, wearable-пристрої та сенсорні мережі. Дана робота присвячена аналізу ефективності антен для бездротових мереж IoT саме в таких умовах, з акцентом на теоретичні аспекти, порівняльний огляд існуючих рішень та практичні рекомендації. Це дозволить оптимізувати конструкції антен для повсякденного використання, враховуючи обмежені ресурси та вимоги до компактності, без необхідності в складних експериментальних установках.

Метою досліджень є комплексне дослідження ефективності антен для IoT-мереж у побутових умовах з метою розробки рекомендацій щодо їх вибору та застосування. У процесі досліджень планується провести аналіз ключових параметрів, таких як коефіцієнт підсилення (gain), ефективність випромінювання, ширина смуги пропускання та вплив мультишляхового поширення сигналу. Для досягнення мети виконано розрахунки втрат сигналу в типових indoor-середовищах (наприклад, за моделлю Rayleighfading), порівняльний аналіз типів антен (дипольні, патч, MIMO). Отримані результати дозволяють досягти високих кількісних показників системи, наприклад, покриття сигналу на відстанях 10-30 м з урахуванням завад, та сформулювати рекомендації щодо оптимізації для низькоенергетичних протоколів (Bluetooth LE, Zigbee). Очікуваний результат — набір практичних рекомендацій для інтеграції антен у побутові IoT-системи, що підвищить їх ефективність на 20-30% без додаткових витрат.

Об'єктом дослідження є антени для бездротових мереж IoT, зокрема їх характеристики та функціонування в реальних умовах. Це включає

омнідирекційні дипольні антени (з типовим gain 2.1 dBi та ефективністю 70-80%), компактні патч-антени (gain 6-7 dBi, ефективність 80-90%) та реконфігуровані системи на базі метаматеріалів. У фокусі – indoor-середовища, де фактори, такі як матеріали стін (бетон, дерево), вертикальні зміщення пристроїв та електромагнітні шуми від побутової техніки, призводять до втрат сигналу до 14 dB.

Проведено аналіз особливостей побудови антен для IoT, включаючи класифікацію типів антен, принципи роботи в діапазонах 2.4/5.8 GHz та mmWave (28 GHz), а також моделі поширення сигналу всередині приміщень (наприклад, мультишляховість та fading). Визначені перспективні варіанти побудови, такі як віртуальні антени для low-power пристроїв [1, 2].

Виконані дослідження факторів впливу на ефективність роботи антен (зменшення на 20% через стіни), позиціонування антен (точність 1-3 м для assettracking) та енергозберігання для подовження життя батарей [3, 4]. Проведено розрахунки gain та bandwidth для різних сценаріїв та сформовані відповідні рекомендації для їх покращення.

Проаналізована ефективность перспективних антен, таких як: дипольні vs, патч для wearable (gain -16 dBi для finger-ring) та MIMO для щільних мереж (gain до 12 dBi). Запропоновано застосування для підвищення їх ефективності amplify-and-forward для 3D-покриття, що покращує сигнал на 50%.

Список використаних джерел:

1. Antenna systems for IoT applications: a review. [Електронний ресурс]. – 2024. – Режим доступу: https://link.springer.com/article/10.1007/s43621-024-00638-z

2. A wearable finger-ringantenna forsmart-home Internet of Things. [Електронний ресурс]. – 2024. – Режим доступу: https://archiwum.pe.org.pl/articles/2024/7/50.pdf

3. Can IoT Devices be Powered up by Future Indoor Wireless Networks? [Електронний ресурс]. – 2024. – Режим доступу: https://dl.acm.org/doi/10.1145/3638550.3641134

4. Fine-Grained 3D Indoor Wireless Coverage for Small IoT Devices. [Електронний ресурс]. – 2021. – Режим доступу: https://conferences.sigcomm.org/sigcomm/2021/files/papers/3452296.3472890.pdf

УДК 621.314

Захожий О.Ю., аспірант
Ципоренко В.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЕНЕРГОКЕРОВАНИЙ БУСТЕРНИЙ МОДУЛЬ 5→6/9/12 В ДЛЯ IOT-ВУЗЛІВ, DVS-КЕРУВАННЯ ТА ЕНЕРГОЕФЕКТИВНІСТЬ

Автономні IoT-вузли потребують гібридного підходу до живлення. Типові DC-DC перетворювачі зазвичай оптимізовуються під фіксовану напругу, ігноруючи різні стани споживання. Сучасні MCU (наприклад STM32L476) дозволяють керувати живленням на периферії. Мета роботи: розробка моделі Boost-модуля зі змінною напругою (6/9/12 В) для зменшення енергії на цикл передачі повідомлення.

Розроблено схему на базі контролера LT3757 (рис. 1). Ключова особливість цієї моделі, це керування зворотним зв'язком через цифровий потенціометр або комутований дільник, який в свою чергу підключений до GPIO мікроконтролера.

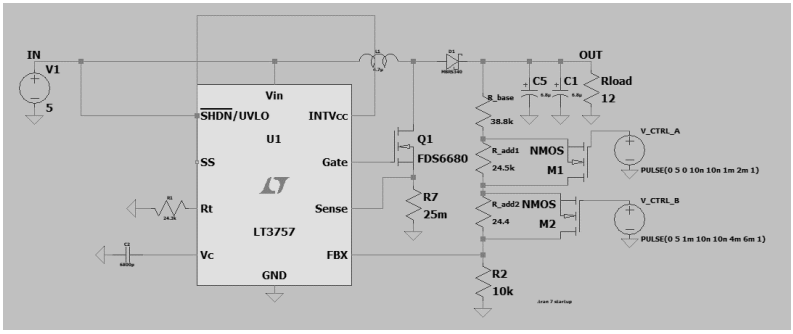


Рисунок 1 – Схема Boost-перетворювача з DVS-керуванням

Система має три статуси:

1. Sleep (6 В): мінімальна напруга для LDO сенсорів, MCU в режимі Stop (300 нА).

2. Radio (9 В): живлення трансивера (LoRa/RF) під час TX/RX.

3. Actuation (12 В): короткочасне живлення виконавчих механізмів.

Логіка базується на перериваннях. Перед активністю MCU змінює стан ключів у дільнику напруги і чекає завершення перехідного процесу t_{settle}, і потім виконує дію.

Індуктивність дроселя L розрахована для $\Delta I_L \approx 30\%$: $L \geq \frac{V_{in} \cdot D}{\Delta I_L \cdot f}$.

Для режиму 12 В обрано $L = 47$ мкГн.

Оцінка ефективності проводиться за метрикою енергії на повідомлення: $E_{msg} = \int P(t)\, dt$.

Моделювання в LTspice (рис. 2) підтвердило стабільність перемикання. Час встановлення при стрибку $6 \rightarrow 12$ В становить ≤ 3 мс, перерегулювання $< 3\%$.

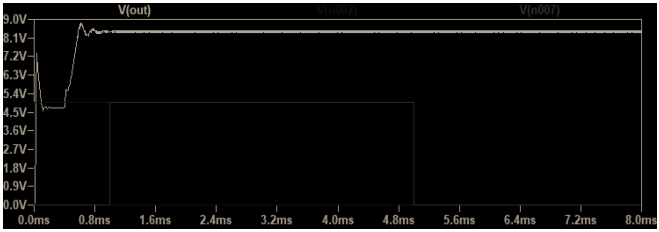


Рисунок 2 – Перехідний процес запуску та стабілізації вихідної напруги

Графік підтверджує відсутність значних перерегулювань (< 5%) та стабільність вихідної напруги при комутації керуючих сигналів (синій/червоний графіки). Це свідчить про стійкість зворотного зв'язку. Розрахунковий аналіз показує, що використання адаптивного режиму (DVS) дозволяє знизити споживання енергії на цикл повідомлення з 87 мДж (при постійних 12 В) до 48 мДж, забезпечуючи економію енергії на рівні 45%.

Список використаних джерел:

1. Analog Devices. LT3757 Datasheet: Boost, Flyback, SEPIC and Inverting Controller. 2025. Режим доступу: https://www.analog.com/media/en/technical-documentation/data-sheets/lt3757-3757a.pdf.

2. B. Torchani, Adaptive sliding mode control based on maximum power point tracking for boost converter of photovoltaic system under reference voltage optimizer. 2024. Режим доступу: https://www.frontiersin.org/journals/energy-research/articles/10.3389/fenrg.2024.1485470/full.

УДК 621.37

Рашко О.С., магістрант,
Ципоренко В.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

ВПЛИВ ПАРАМЕТРІВ ПІДКЛАДКИ НА ХАРАКТЕРИСТИКИ МІКРОСМУЖКОВОЇ АНТЕНИ

Мікрополоскові антени широко використовуються у сучасних бездротових системах зв'язку завдяки їхній компактності, низькому профілю та простоті інтеграції з друкованими платами. Одним із ключових чинників, що визначає їх ефективність, є властивості діелектричної підкладки. Параметри матеріалу підкладки – діелектрична проникність, тангенс кута діелектричних втрат та товщина – визначають резонансну частоту, ширину смуги пропускання, коефіцієнт підсилення та ефективність випромінювання антени.

Метою роботи є дослідження залежності основних характеристик мікрополоскової антени від параметрів діелектричної підкладки та формування рекомендацій для вибору матеріалу відповідно до вимог бездротових систем.

У роботі проведено аналітичний розрахунок прямокутної мікрополоскової антени для частоти 2,4 ГГц, розроблено чисельну модель у MATLAB та досліджено вплив підкладок FR4, Rogers RT/duroid та керамічних матеріалів. Аналітичні методи базуються на моделі лінії передачі та моделі резонаторної порожнини, що дозволило визначити геометричні параметри та вхідний опір антени. Чисельні методи (MoM, FEM, FDTD, FIT) використані для порівняльного аналізу точності моделювання та характеристик електромагнітних полів.

Досліджено частотні залежності активної та реактивної складових вхідного опору. На резонансній частоті 2,42 ГГц активна частина опору становила 52,3 Ом, що забезпечує узгодження з лінією живлення. Поза резонансом опір зменшується, що пов'язано зі зниженням ефективності випромінювання. Реактивна складова змінюється від ємнісної до індуктивної, перетинаючи нуль у точці резонансу, що характеризує добротність антени.

Проведено аналіз залежності резонансної частоти та КСВ від діелектричної проникності підкладки. Зі збільшенням εr резонансна частота зміщується вниз, а ширина смуги пропускання зменшується. Підкладка FR4 ($\varepsilon r = 4.4$, $\tan\delta = 0.009$) демонструє більші втрати та нижчу ефективність порівняно з Rogers RT/duroid, проте залишається популярною завдяки низькій вартості.

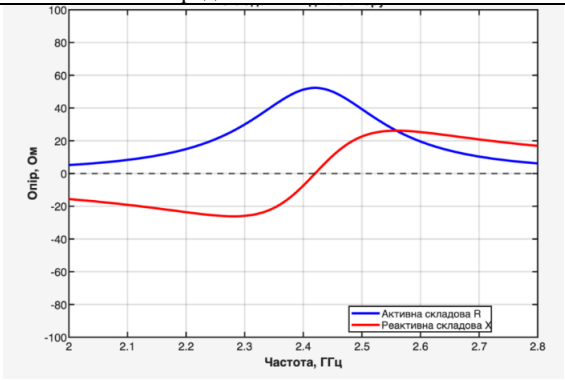


Рисунок 1 – Частотні залежності активної та реактивної складових вхідного опору

Окрему увагу приділено впливу товщини підкладки. Збільшення товщини покращує коефіцієнт підсилення, проте спричиняє зростання поверхневих хвиль, що негативно впливає на діаграму спрямованості.

Розглянуто застосування сучасних структур: фотонічних кристалів, метаматеріалів та штучних магнітних провідників (AMC), які дозволяють зменшити втрати, підвищити спрямованість та розширити смугу пропускання.

Узагальнюючи проведене дослідження, встановлено, що вибір підкладки є критичним етапом проєктування мікрополоскової антени. Для високоефективних систем доцільно використовувати матеріали з низькими втратами (Rogers), тоді як FR4 підходить для бюджетних рішень. Отримані результати можуть бути застосовані у системах Wi-Fi, IoT, 5G Sub-6 ГГц та іншій бездротовій техніці.

Список використаних джерел:

1. Chen M., Ouyang J., Jian A., Liu J., Li P., Hao Y., Gong Y., Hu J., Zhou J., Wang R., Wang J., Hu L., Wang Y., Ouyang J., Zhang J., Hou C., Wei L., Zhou H., Zhang D., Tao G. Imperceptible, designable, and scalable braided electronic cord. Nature Communications. 2022. Vol. 13, No. 1. Article 7097. DOI: https://doi.org/10.1038/s41467-022-34918-x

2. Gezahegn Y. A., Tang J., Sablani S. S., Pedrow P. D., Hong Y.-K., Lin H., Tang Z. Dielectric properties of water relevant to microwave assisted thermal pasteurization and sterilization of packaged foods. Innovative Food Science & Emerging Technologies. 2021. Vol. 74. Article 102837. DOI: https://doi.org/10.1016/j.ifset.2021.102837

УДК 621.37

Собецький В.М., магістрант
Ципоренко В.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ТОЧНОСТІ ПОЗИЦІОНУВАННЯ GNSS-ПРИЙМАЧІВ З ВИКОРИСТАННЯМ RTK-КОРЕКЦІЙ

Сучасні супутникові навігаційні системи (GPS, Galileo, BeiDou, ГЛОНАСС) забезпечують визначення координат у глобальних системах відліку з точністю від кількох метрів до кількох сантиметрів залежно від режиму роботи приймача. Одним із найбільш ефективних методів підвищення точності є застосування диференціальних корекцій у режимі RTK (Real-Time Kinematic), що дозволяє отримувати сантиметрову точність у реальному часі.

Метою даної роботи є аналіз принципів функціонування супутникових навігаційних систем та проведення експериментального дослідження точності приймача NEO-F9P у режимі RTK Fixed.

Об’єктом дослідження є процес визначення координат за сигналами GNSS. Предметом дослідження – похибки супутникового позиціонування та підходи до їхнього зменшення.

У роботі розглянуті базові принципи радіонавігації, структуру сигналів GPS, особливості PRN-кодів, модуляції DSSS/BPSK та побудови навігаційного повідомлення. Також описано процедури вимірювання кодової фази, фази несучої та формування координатно-часової інформації.

Значною частиною дослідження стала розроблена апаратна плата RockRTK, що виконує функції GNSS-модуля з підтримкою RTK-корекцій на основі приймача u-blox NEO-F9P. Плата містить інтерфейси для підключення антени, живлення та комунікації. RockRTK інтегрована з вбудованою Linux-системою, зібраною за допомогою Buildroot, що забезпечує обмін RTCM-повідомленнями та логування GNSS-даних. Використання власної апаратної платформи дало можливість оптимізувати структуру стенду та забезпечити стабільну роботу під час експериментів.

Для експериментальної частини було створено стенд з регулярною сіткою контрольних точок та колом радіусом 40 см. Приймач NEO-F9P на основі плати RockRTK працював у режимі RTK із локальною базовою станцією.

Рисунок 1 – Експериментальний стенд для вимірювання точності GNSS у режимі RTK

Результати досліджень показали, що у режимі RTK Fixed середньоквадратичне відхилення координат становить декілька сантиметрів, при цьому вертикальна складова має більшу похибку. Розроблена плата RockRTK, вимірювальний стенд та методика збору даних можуть бути використані для тестування GNSS-обладнання, дослідження RTK-приймачів та навчальних робіт у сфері супутникової навігації.

Список використаних джерел:

1. Kaplan E., Hegarty C. Understanding GPS/GNSS. Principles and Applications. Artech House Publishers. 2017. 1016 p.

2. Misra P., Enge P. Global Positioning System: Signals, Measurements, and Performance. Ganga-Jamuna Press. 2006. 569 p.

УДК 621.37

Тирчик В.В., бакалавр,
Ципоренко В.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

СИСТЕМА СИГНАЛІЗАЦІЇ З ВИКОРИСТАННЯМ ДАТЧИКА HC-SR04 ІЗ СПОВІЩЕННЯМ ПРО ЧАС ПРОНИКНЕННЯ ДО МОБІЛЬНОГО ДОДАТКУ TELEGRAM

У сучасному світі питання безпеки житлових, офісних та промислових приміщень набувають особливої актуальності. Традиційні системи сигналізації зазвичай вимагають значних фінансових витрат і професійного монтажу. Натомість розвиток мікроконтролерних технологій, зокрема платформи ESP32, дає змогу створювати прості, надійні та доступні системи безпеки із можливістю дистанційного керування та моніторингу через інтернет.

Метою даної роботи є розробка системи сигналізації, що базується на ультразвуковому датчику HC-SR04, мікроконтролері ESP32, та забезпечує автоматичне сповіщення користувача у мобільний додаток Telegram про факт проникнення у контрольовану зону. Додатково передбачена функція активації звукової сигналізації за командою користувача через Telegram-бот.

Об’єктом дослідження є процес вимірювання відстані до об’єкта та передача сигналів тривоги за допомогою бездротових технологій. Предметом дослідження є методи побудови автоматизованих охоронних систем на базі мікроконтролерів із Wi-Fi підключенням.

Основними компонентами системи є: – ультразвуковий датчик HC-SR04, який визначає відстань до об’єкта; – мікроконтролер ESP32, що виконує обробку отриманих даних і забезпечує зв’язок із Telegram; – п’єзоелектричний бузер, який виконує роль звукової сигналізації; – Telegram-бот, створений через API, для віддаленого сповіщення та керування системою.

Принцип роботи системи полягає в безперервному контролі відстані в межах контрольованої зони. Якщо об’єкт наближається ближче до заданого порогу (наприклад, 50 см), система фіксує це як спробу проникнення. ESP32 обчислює час події, формує повідомлення та надсилає його користувачу в Telegram. Для цього застосовується бібліотека WiFiClientSecure і протокол HTTPS, що гарантує безпечну передачу даних через мережу.

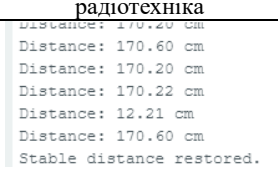


Рисунок 1 – Встановлення сталої відстані

Реалізація проєкту здійснена у середовищі Arduino IDE. Програмна частина включає модулі ініціалізації датчика HC-SR04, Wi-Fi підключення, функції відправлення повідомлень та активації бузера. Для підключення до Wi-Fi використовується стандартна бібліотека WiFi.h, а для зв'язку з Telegram — HTTPClient.h.

В процесі тестування встановлено, що система стабільно реагує на об'єкти, що з'являються на відстані менше 50 см. Затримка між моментом спрацювання датчика і надсиланням повідомлення у Telegram становить 1,5–2 с, що є прийнятним для систем реального часу. Дальність дії датчика — до 4 м, з точністю вимірювання ±3%.

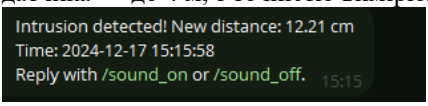


Рисунок 2 – Повідомлення про проникнення

Результати тестування підтвердили працездатність і надійність створеної системи. Виявлено, що Telegram-бот стабільно приймає команди /sound_on та /sound_off, що дозволяє користувачу дистанційно вмикати або вимикати звукову сигналізацію. Система демонструє високу точність спрацювання, а її реакція на подію є швидкою.

Розроблений проєкт є прикладом поєднання технологій інтернету речей (IoT) та цифрової обробки сигналів у побутових системах безпеки. Отримані результати засвідчують, що запропонована система може ефективно застосовуватися для охорони невеликих приміщень, квартир, гаражів або офісів. Її перевагами є низька собівартість, простота реалізації, зручність керування через Telegram та можливість автономної роботи.

Список використаних джерел:

1. Espressif Systems. *ESP32 Technical Reference Manual* [Електронний ресурс]. 2023. Режим доступу: https://www.espressif.com.

2. ElecFreaks. *HC-SR04 Ultrasonic Sensor Datasheet* [Електронний ресурс]. 2022. Режим доступу: https://www.elecfreaks.com.

УДК 621.37

Хімчик Н.С., бакалавр,
Ципоренко В.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

РОЗРОБКА РОЗУМНОГО ДОЗИМЕТРА НА ОСНОВІ МІКРОКОНТРОЛЕРІВ ATMEGA328P ТА ESP32

У сучасних умовах забезпечення радіаційної безпеки набуває особливої актуальності як у побутовому, так і в професійному секторах. Зростання потреби в доступних, надійних та інтелектуальних засобах контролю радіаційного фону спонукає до розробки нових технічних рішень на основі сучасної елементної бази. У цьому контексті розробка розумного дозиметра, що поєднує функціональність мікроконтролера ATmega328p для точного вимірювання іонізаційних подій та ESP32 для бездротової передачі даних, є логічним кроком у напрямку інтеграції IoT-технологій у радіаційний моніторинг.

Метою даної роботи є розробка та апаратно-програмна реалізація пристрою, здатного вимірювати рівень гамма- та бета-випромінювання за допомогою газонаповненого лічильника СБМ-20, обробляти отримані сигнали мікроконтролером ATmega328p та передавати результати в реальному часі через Wi-Fi або Bluetooth за допомогою модуля ESP32.

Об’єктом дослідження є процеси детектування іонізуючого випромінювання, обробки імпульсів та бездротової передачі виміряних значень. Предметом роботи виступає архітектура розумного дозиметра, що базується на подвійному мікроконтролерному управлінні та використанні сучасних засобів зв’язку.

Для живлення лічильника СБМ-20, який вимагає напруги 350–400В, було розроблено високовольтний перетворювач на основі таймера NE555 та MOSFET-транзисторів. Пульсації напруги стабілізовано за допомогою зворотного зв’язку на базі мікросхеми TL431. Сигнал, що формується при іонізаційному пробої у трубці, підсилюється за допомогою операційного підсилювача NE5532, що забезпечує надійну реєстрацію подій мікроконтролером ATmega328p через апаратні переривання. Цикл вимірювання триває 36 секунд – такий самий, як у класичних радянських дозиметрах, що дозволяє отримувати стабільні та порівнянні результати.

Експериментальна частина роботи включала збірку макету на макетній платі, налагодження програмного коду та порівняння отриманих даних з показниками еталонного дозиметра «БЕЛЛА», оснащеного ідентичним лічильником СБМ-20.

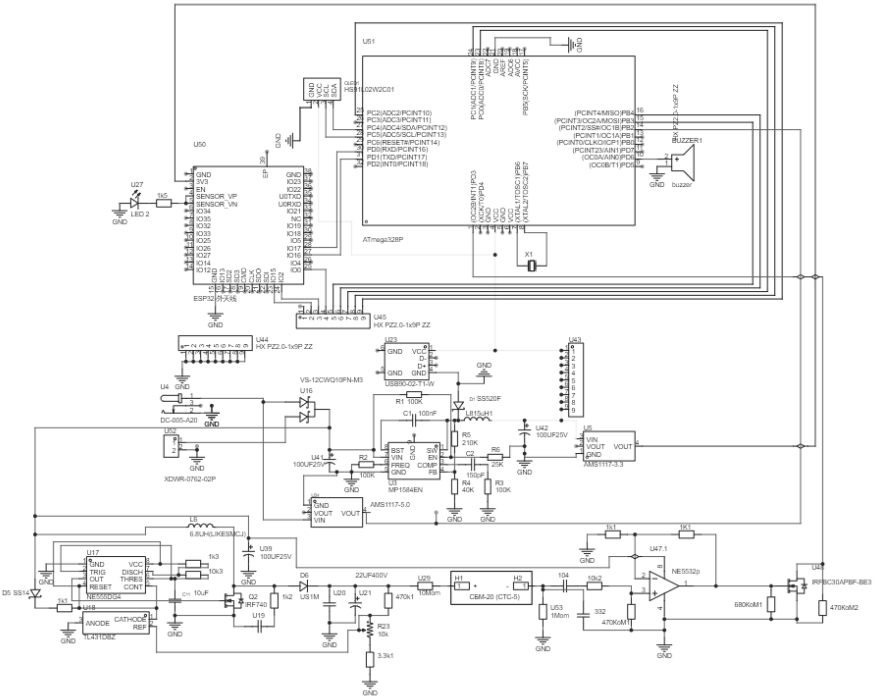


Рисунок 1 – Схема електрична принципова

Результати вимірювань показали, що розбіжність між пристроями не перевищує 4 одиниць при середньому фоні 0,12 мкЗв/год, що є допустимим для побутових пристроїв. Повне відображення даних на OLED-дисплеї, безперебійна робота через Telegram-бот і Bluetooth підтвердили функціональність пристрою.

Список використаних джерел:

1. Monk S. Programming Arduino: Getting Started with Sketches. New York: McGraw-Hill Education, 2016. 176 p.

2. ESP32-WROOM-32D-N16 Datasheet. Shanghai: Espressif Systems, 2022. 42 p.

3. ATmega328P Datasheet. Chandler: Microchip Technology Inc., 2023. 664 p.

УДК: 621.311.243

Ткачов А.К., аспірант,
Яганов П.О., к.т.н., доцент
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського

СИСТЕМА СЛІДКУВАННЯ ЗА ТОЧКОЮ МАКСИМАЛЬНОЇ ПОТУЖНОСТІ ДЛЯ АКУМУЛЯТОРНИХ БАТАРЕЙ

Сучасний перехід до відновлюваних джерел енергії зумовив підвищений інтерес до сонячної енергетики та фотоелектричних систем (ФЕС), що безпосередньо перетворюють енергію сонячного випромінювання на електричну. Постійне вдосконалення технологій експлуатації СЕ спрямоване на підвищення їх ефективності. Оскільки сонячний елемент, як фізичний компонент, має виражену нелінійну вольт-амперну характеристику (ВАХ), а залежність потужності від напруги характеризується наявністю єдиного максимуму – точки максимальної потужності (ТМП), визначення параметрів цієї точки є складним завданням. Це пояснюється тим, що її положення не є сталим і змінюється під впливом зовнішніх факторів.

Відсутність сталих параметрів ТМП зумовлює ще один важливий аспект – зміну ефективного опору навантаження, який також не є постійним у процесі роботи сонячного елемента. Визначення та підтримання оптимальних параметрів цих двох аспектів покладається на спеціальний пристрій – систему слідкування за точкою максимальної потужності (ССТМП).

Алгоритми функціонування ССТМП засновані на визначенні ТМП та підтриманні режиму роботи в околі цієї точки в залежності. Найпоширеніші алгоритми базуються на двох основних підходах – схемотехнічних та аналітичних. Схемотехнічні підходи передбачають постійне коригування параметрів ТМП (струму I_m та напруги V_m) які змінюються в залежності від зовнішніх умов. Підвищене енергоспоживання схемотехнічних методів зумовлене необхідністю безперервного моніторингу та регулювання робочих параметрів. Натомість аналітичні методи спираються на математичні співвідношення, що випливають із рівняння Шоклі (1), яке описує залежність струму від напруги в сонячному елементі.

$$I = I_{\text{кз}} - I_0\left(e^{\left(\frac{(U+IR_S)}{n\phi_t}\right)} - 1\right) \qquad (1)$$

Метою цієї роботи є проектування ССТМП для акумуляторних батарей, що буде включати оптимізацію двох основних підходів: використання аналітичного підходу до визначення координат ТМП та регулювання ефективного опору навантаження відповідно до необхідних значень акумуляторних батарей.

Відомо, що максимум функції визначається з умови рівності її похідної до нуля. Відповідно, координати точки максимальної потужності (ТМП) можна знайти, обчисливши похідну функції потужності, сформованої на основі рівняння (1) одноекспоненційної моделі сонячного елемента. Одне з таких аналітичних рішень подано у дослідженні [1], однак воно передбачає спрощення рівняння Шоклі шляхом нехтування шунтовим опором. Напруга в ТМП може бути визначена за формулою (1), де W_0 – функція Ламберта.

$$I_{mpp} = \left(1 - \frac{1}{W_0\left(\frac{I_f}{I_0} e^{\left(1-\frac{2I_f R_s}{nV_t}\right)}\right)}\right) I_f \qquad (2)$$

Іншим важливим аспектом є узгодження опорів навантаження та ефективного вихідного опору сонячного елемента (СЕ). Існує широкий спектр методів визначення ефективного опору – від найпростіших наближених[2] до більш точних методів, що базуються на аналізі параметрів у ТМП. Проте для акумуляторних батарей основним критерієм є не стільки узгодження опорів, скільки дотримання режиму постійного вихідного струму, оскільки саме в цьому режимі відбувається основне накопичення заряду. Таким чином, використання аналітичних методів розрахунку і забезпечення додатковим компонентом підтримання режиму постійного струму дозволяє побудувати ефективну ССТМП для акумуляторних батарей.

Список використаних джерел:

1. J.G. Tirado-Serrato, A. S. Garcia, and S. Maximov, “Analytical Computation of the Maximum Power Point of Solar Cells Using Perturbation Theory,” Energies, vol. 17, no. 23, Art. 6035, Nov. 2024, doi: 10.3390/en17236035.

2. Ткачов, А. К. Узгодження оптимального опору навантаження сонячної батареї зі споживачами електроенергії / А. К. Ткачов, П.О. Яганов, В. В. Черненко // XXIV Міжнародна науково-технічна конференція "Приладобудування: стан і перспективи", 13–14 травня 2025 р., Київ, Україна : збірник матеріалів конференції. – Київ : КПІ ім. Ігоря Сікорського, 2025. – С.353-357.

УДК: 621.311.243

Ткачов А.К., аспірант
Черненко В.В., к.ф.-м.н., с.н.с
Інститут фізики напівпровідників імені В.Є. Лашкарьова НАН України

ПОРІВНЯННЯ МЕТОДІВ ВИЗНАЧЕННЯ ТОЧКИ МАКСИМАЛЬНОЇ ПОТУЖНОСТІ СОНЯЧНОГО ЕЛЕМЕНТА ІЗ ВИКОРИСТАННЯМ ФУНКЦІЇ ЛАМБЕРТА ТА СПРОЩЕНИХ АНАЛІТИЧНИХ МОДЕЛЕЙ

Підвищення інтересу до використання сонячної енергетики у фотоелектричних системах (ФЕС) зумовлює не лише розширення масштабів їх застосування, а й активізацію досліджень, спрямованих на підвищення їх коефіцієнта корисноїдії (ККД). Це, своєю чергою, зумовлює необхідність поглибленого вивчення характеристик сонячних елементів та пошуку більш точних і енергоефективних аналітичних методів визначення точки максимальної потужності (ТМП), на відміну від традиційних ітераційних підходів.

Більшість відомих аналітичних методів ґрунтуються на аналізі похідної рівняння Шоклі, яке описує залежність струму від напруги сонячного елемента. Оскільки це рівняння містить експоненційний член, що зумовлює його нелінійність, найефективнішим способом спрощення похідної є використання функції Ламберта. Її застосування дозволяє подати рівняння у зручнішій аналітичній формі, придатній для прямого розв'язання рівнянь типу (1).

$$y = xe^x \tag{1}$$

Проте, оскільки функція Ламберта не виражається через елементарні функції, тому її аналітичне застосування обмежується спеціалізованими бібліотеками та математичними пакетами. Це, в свою чергу, зумовлює значне підвищення вимог до обчислювальних ресурсів, що пред'являються до систем слідкування за точкою максимальної потужності(ССТМП) сонячного елемента(СЕ).

Цей суттєвий недолік спонукає до пошуку спрощених аналітичних підходів – наприклад, апроксимації функції Ламберта або застосування альтернативних математичних методів, які дозволяють зменшити обчислювальну складність без суттєвої втрати точності.

Серед відомих апроксимацій можна виділити два основних методи – апроксимація розкладом в ряд Тейлора або використання асимптотичних апроксимацій. Проте, в свою чергу кожен із цих методів також має суттєві недоліки. Розклад в ряд Тейлора може

використовуватись лише в малому діапазоні значень близько нуля, а асимптотичні апроксимації мають значну похибку в деяких діапазонах.

Поєднання двох методів дозволяє отримати іншу формулу (2) апроксимації [1], що має дуже малу похибку на всьому діапазоні вимірювань, проте використання її в такому вигляді також призводить до великого обчислювального навантаження.

$$W(x) = P * \left(1 - \frac{3+3P+2Q}{4P+1} + \sqrt{\left(\left(\frac{3+3P+2Q}{4P+1}\right)^2 - \frac{6Q}{4P+1}\right)}\right) \quad (2),$$

де P = ln(x), Q=ln(P)=ln(ln(x)).

Альтернативою методам визначення ТМП на основі функції Ламберта є спрощені аналітичні підходи, що не потребують складних розрахунків. Якщо один із параметрів у точці максимальної потужності (напруга або струм) апроксимується аналітично (рис. 1), тоді обчислення іншого параметра зводиться до розв'язання простого трансцендентного рівняння [2].

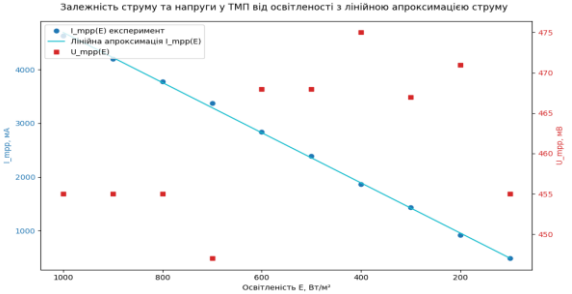


Рисунок 1 – Апроксимація напруги і струму в ТМП

Таким чином, використання цього альтернативного методу є перспективним для впровадження у ССТМП, оскільки він дозволяє істотно скоротити час розрахунку ТМП та знизити вимоги до обчислювальних ресурсів.

Список використаних джерел:

1. Ольшанський В. П. Про апроксимацію функції Ламберта / В. П. Ольшанський // Наукові записки. 2020. Вип. 1. С. 9. DOI: 10.20998/2222-0631.2020.1.09. УДК 517.5.

2. Volodymyr Chernenko, Petro Yahanov, Demyd Pekur, Roman Korkishko, Vasyl Kornaga, Viktor Sorokin, Analytical model of light current-voltage characteristics of a solar cell based on experimental data, Solar Energy Advances, Vol. 4. 2024. https://doi.org/10.1016/j.seja.2024.100073

УДК 621.391:621.37

Петраш С.В., к.т.н., доц., доцент
Рихальський О.Р., к.т.н., доц., ст. викладач
Зелінський О.В., викладач
Житомирський військовий інститут імені С.П.Корольова

МЕТОДИКА ВИЗНАЧЕННЯ ВИДУ МОДУЛЯЦІЇ РАДІОТЕХНІЧНИХ ВИПРОМІНЮВАЛЬНИХ ОБ'ЄКТІВ

Одним з ключових завдань кожної держави є контроль за випромінюванням радіотехнічних засобів з метою забезпечення національної безпеки і оборони, виявлення несанкціонованого випромінювання та визначення тих, що працюють в аварійному режимі.

Засоби радіотехнічного контролю (ЗРТК) в процесі роботи здійснюють розпізнавання активних радіовипромінювальних засобів (РВЗ). Важливу роль серед них відіграють засоби добування інформації, серед яких виділяється радіолокаційні станції та системи.

В ході обробки та аналізу інформації від таких РВЗ здійснюється їх розпізнавання, яке здійснюється в умовах апріорної невизначеності. В процесі розпізнавання здійснюється віднесення даних, отриманих на етапі вимірювання до визначеного типу. Отримані дані є параметрами сигналів і вважаються ознаками, на основі яких приймаються рішення. Вибір системи ознак базується на врахуванні їх інформативності, яка оцінюється за ймовірністю розпізнавання. В свою чергу інформативність залежить від ступеня невизначеності вихідних даних про РВЗ, точності виміру та числа параметрів, алгоритму розпізнавання, що застосовується.

Під час роботи ЗРТК змінюються умови радіоелектронної обстановки, що призводить до зміни інформативності ознак. Такі міркування примушують застосовувати в процесі розпізнавання надлишок ознак для забезпечення заданої ймовірності розпізнавання.

Найбільш поширенішими ознаками розпізнавання виступають параметри сигналів, до яких відносять несучу частоту, тривалість та період слідування імпульсів. Аналіз існуючих ЗРТК показав, що одночасного використання під час розпізнавання цих трьох параметрів в залежності від точності виміру змінює ймовірність розпізнавання у межах від 0,71 до 0,92. Додатковою ознакою розпізнавання, яку можна використати виступає вид модуляції прийнятих сигналів.

На даний момент існують методи визначення виду модуляції. Одні із таких методів (імітація поведінки рою медоносних бджіл) за результатами моделювання забезпечують високі значення ймовірності

розпізнавання (0,9 і вище). Недоліком таких методів є вимоги щодо додаткового часу для навчання алгоритму розпізнавання в реальному масштабі часу, що часто є неможливим. Інші із запропонованих методів не враховують зміну інформативності параметрів та їх кількість складає десятки.

Пропонується використовувати кореляційні методи, які можливо автоматизувати після перетворення сигналів до цифрового вигляду.

За автокореляційного метода вхідний сигнал подається на перший вхід перемножувала корелятора, а на другий вхід – через лінію затримки. На виході фільтра корелятора спостерігається сигнал, спектр якого визначається функцією модуляції вхідного сигналу.

За кореляційного прийому проводиться аналіз відгуків сигналів на виходах каналів двох кореляторів. Один канал – автокорелятор з диференціюючим колом після перемножувача та вихідним амплітудним детектором. У другому каналі вхідний сигнал переноситься у змішувачі на проміжну частоту і подається на вхід другого перемножувала, чим формується кореляційна функція. На другий вхід перемножувача подається вхідний затриманий сигнал. Після диференціюючого кола та амплітудного детектування отримується відгук. Аналіз відгуків у двох каналах дозволяє визначити вид модуляції сигналів.

Третій метод ґрунтується на порівнянні спектрів сигналів на вхідній та подвоєній частоті. Подвоєння досягається використанням аналізу спектра сигналу на другій гармоніці із застосуванням змішувача.

Застосування даних методів можливе як окремо, так і в сукупності, що залежить від конструктивних особливостей та призначення ЗРТК.

Проведене модулювання підтвердило правильність запропонованих рішень. Ймовірність розпізнавання залежить від виду модуляції сигналів та відношення сигнал/шум на вході і для, наприклад, періодичної послідовності прямокутних радіоімпульсів складає 0,97.

Список використаних джерел:

1. Liu L., Zhang Y., Qin X. Radar Waveform Recognition Based on Time-Frequency Features / L. Liu, Y. Zhang, X. Qin та ін. Electronics. 2018, Vol. 7, № 5, с. 59. MDPI. URL: https://doi.org/10.3390/electronics7050059.

2. Бондаренко В. О. Методичний підхід до визначення доцільної кількості ознак моніторингу для ідентифікації стану об’єктів розвідки. / Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.-К.: НУОУ, 2021. Вип. 3(73). С. 97-101. doi: https://doi.org/10.33099/2304-2745/2021-3-73/97-101.

УДК 621.37

Біденко К.А., бакалавр,
Ципоренко В.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

РОЗРОБКА СИСТЕМИ ЕКСТРЕНОГО ОПОВІЩЕННЯ В УМОВАХ БЛЕКАУТУ

У сучасних умовах, коли інфраструктура електроенергетики може зазнавати значних пошкоджень, особливо важливо створити системи екстреного оповіщення, які можуть працювати під час тривалих відключень електроенергії. Блекаути створюють ризик для життя та безпеки населення через повну втрату зв'язку, відсутність доступу до Інтернету та традиційні канали сповіщень. Тому, для підвищення стійкості громад і окремих об'єктів важливим завданням є створення автономної, незалежної системи оповіщення.

Метою дослідження є створення системи екстреного оповіщення, здатної працювати в автономному режимі, забезпечувати передачу критичних повідомлень без доступу до електромережі та централізованих каналів зв'язку, а також гарантувати максимальну надійність і простоту використання. Основними завданнями є вибір енергоефективних модулів зв'язку, розробка автономної системи живлення, формування алгоритмів оповіщення та забезпечення захищеної передачі даних. Одним з ключових моментів є вибір технології зв'язку, яка зможе працювати без Інтернету та мобільної мережі. Для цього можуть бути використані такі протоколи зв'язку, як LoRa, яка забезпечить далекобійний радіозв'язок із низьким електроспоживанням, або ж ESP-NOW, яка дозволить створити локальні автономні мережі між мікроконтролерами ESP32/ESP8266. Ці рішення гарантуватимуть передачу оповіщень за відсутності зовнішньої інфраструктури у радіусі від кількохсот метрів до кількох кілометрів.

Ще одним критичним аспектом системи є автономне живлення. Для забезпечення довготривалої роботи застосовуватимуться акумулятори великої ємності із можливим залученням сонячних панелей або суперконденсаторів. Енергозберігаючий режим мікроконтролерів дозволить суттєво збільшити час автономності без додаткового заряджання, що робить систему ефективною в умовах блекаутів. При цьому потрібно передбачити захист акумуляторів, оптимізацію енергоспоживання та балансування заряду.

Для передачі екстрених повідомлень можуть використовуватися звукові сирени, світлові індикатори, а також невеликі локальні дисплеї або мобільні пристрої, підключені до автономної мережі.

Загальна структура зображена на рисунку 1.

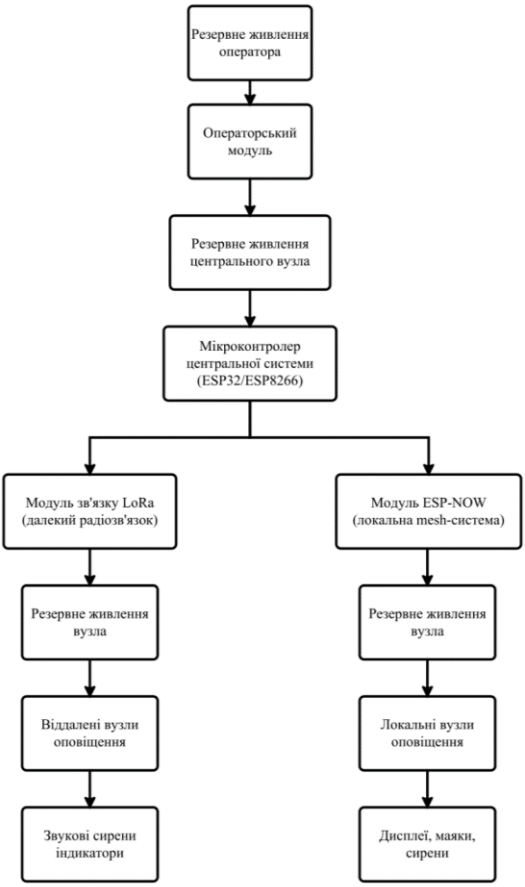


Рисунок 1 – Структурна схема системи екстреного оповіщення

Важливим є створення простого та інтуїтивного інтерфейсу для оператора, який дозволить швидко розсилати сигнали тривоги, повідомлення про небезпеку або інструкції щодо дій населення. У разі потреби система може бути інтегрована з Telegram-ботом чи SMS-шлюзом, коли зв’язок з’являється, для дублювання повідомлень.

Особливо важливо забезпечити стійкість системи до зовнішніх впливів. Необхідно враховувати низьку температуру, механічні навантаження, високий рівень вологості та електромагнітні перешкоди. Корпус пристрою має бути виконаний із захищених матеріалів, а антени

– оптимізовані для стабільного прийому навіть в умовах зниженої потужності передавача.

Важливою частиною побудови такої системи є правильне розміщення звукових джерел оповіщення. Від цього залежить, чи буде сигнал добре чути на всій території. Для цього використовують спеціальні алгоритми, які враховують рельєф, щільність забудови та можливі перешкоди. Такі розрахунки дозволяють визначити оптимальні точки встановлення сирен, уникнути «мертвих зон» та забезпечити рівномірне покриття звуку. Завдяки цьому можна зменшити кількість обладнання та енергоспоживання, що є особливо важливим під час блекаутів.

Крім того, оптимізоване розташування звукових модулів спрощує планування маршрутів евакуації та дій рятувальних служб. Чітке охоплення території забезпечить одночасне отримання повідомлень, із мінімальними затримками та достатнім рівнем гучності, що дозволить уникнути паніки та підвищує ефективність реагування на надзвичайні ситуації.

Також слід приділити увагу організації маршрутизації повідомлень між вузлами. Важливо забезпечити автоматичний пошук альтернативного шляху передачі сигналу в разі збою одного з вузлів або пошкодження частини мережі. У цьому випадку доцільно використовувати топологію мережі, властиву протоколам ESP-NOW або LoRa Mesh, оскільки це дозволяє вузлам працювати як ретранслятори. Такий принцип підвищує відмовостійкість системи та дозволяє надсилати важливі сповіщення навіть у інфраструктурах, які частково зруйновані.

Ще одним важливим аспектом є шифрування та автентифікація переданих сигналів. Під час надзвичайних ситуацій існує ризик перехоплення або навмисного блокування каналу зв’язку. Унеможливлення несанкціонованого втручання в роботу системи забезпечується за допомогою алгоритмів симетричного шифрування (AES-128/256), а також окремих ключів для кожного вузла. Це особливо важливо в ситуаціях, коли система оповіщення використовується в місцях масового скупчення людей, на об’єктах критичної інфраструктури або на стратегічних територіях.

Також важливо врахувати необхідність зворотнього зв’язку для діагностики та контролю працездатності вузлів. Автономні модулі надсилатимуть службові пакети контролеру, це дозволить відстежити якість сигналу, рівень заряду акумуляторів, стан датчиків і працездатність сирен. Такі регулярні перевірки дозволять системі швидко повідомити оператора про проблеми та автоматично перейти в

режим економії енергії, якщо вузол не використовується протягом тривалого часу.

Для підвищення ефективності використання енергії важливо оптимізувати режими роботи вузлів. Система може працювати в режимі «сну» під час неактивності, включаючись лише для перевірки каналу або при отриманні сигналу. Такий метод значно збільшує термін служби батареї, що дуже важливо у разі тривалих блекаутів, коли підзарядка батареї обмежена або взагалі відсутня.

Окремим напрямом удосконалення системи є інтеграція датчиків навколишнього середовища, зокрема температури, диму, газу або вібрацій. Такі датчики перетворять систему оповіщення на багатофункціональний комплекс. Вони зможуть автоматично визначати потенційно небезпечні ситуації й генерувати сигнал тривоги без участі оператора. Наприклад, виявлення диму або підвищеної температури може викликати сценарій «пожежної тривоги», а датчики вибухових газів можуть повідомити про потенційну аварію на промислових об'єктах.

Результатом роботи є автономна система екстреного оповіщення, здатна працювати в умовах повного знеструмлення, забезпечувати передачу важливої інформації на значні відстані та підтримувати зв'язок між декількома вузлами. Така система може застосовуватися для цивільної безпеки, інформування населення, роботи критичної інфраструктури та забезпечення стійкого функціонування місцевих громад під час надзвичайних ситуацій.

Список використаних джерел:

1. Пасічник А. М., Ріпа М. Ю. Алгоритм побудови та оптимізації територіального розміщення звукових джерел системи екстреного оповіщення населення. Systems and Technologies. 2024. Т. 67, № 1. С. 25–29. – Режим доступу: https://doi.org/10.32782/2521-6643-2024-1-67.4

2. Технології бездротового зв'язку ESP-NOW. [Електронний ресурс]. – Режим доступу: https://randomnerdtutorials.com

3. LoRa й LoRaWAN: як навчити пристрої спілкуватися з людиною. – Режим доступу: https://jooby.eu/uk/blog/radiotekhnolohiya-lora

4. Sistem Enkripsi Dokumen Digital Melalui Kombinasi AES-128 dan Hashing SHA-256 Berbasis Salt / F. M. Kaaffah та ін. Jurnal Ilmiah FIFO. 2025. Т. 17, № 1. С. 78. URL: https://doi.org/10.22441/fifo.2025.v17i1.009.

УДК 004.942

Богодвид О.В., магістрант
Сугоняк І.І., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ТОЧНОСТІ ВИМІРЮВАННЯ БІОМЕТРИЧНИХ ПОКАЗНИКІВ ЗА ДОПОМОГОЮ СТАНДАРТНИХ ДАТЧИКІВ СМАРТФОНУ

Сучасні смартфони оснащені широким спектром датчиків, що відкриває можливості для створення мобільних застосунків персонального моніторингу здоров'я. Використання вбудованих сенсорів для вимірювання біометричних показників є актуальним напрямком розвитку мобільної медицини, оскільки дозволяє здійснювати неперервний контроль стану здоров'я без потреби в дорогому спеціалізованому обладнанні [1]. Проте виникає важливе питання щодо точності та надійності таких вимірювань порівняно з професійними медичними приладами.

Метою дослідження є аналіз точності вимірювання основних біометричних показників - частоти серцевих скорочень, кількості кроків та тривалості сну - за допомогою стандартних датчиків смартфону та оцінка придатності цих вимірювань для систем персонального моніторингу здоров'я [2].

Одним з ключових біометричних показників є частота серцевих скорочень, яку можна визначити методом фотоплетизмографії (PPG) з використанням камери та спалаху смартфону. Принцип роботи полягає у реєстрації змін інтенсивності світла, що проходить через тканини пальця, які відповідають пульсовим хвилям. Для досягнення високої точності необхідно застосовувати алгоритми цифрової обробки сигналу, що включають видалення лінійного тренду, адаптивну фільтрацію шумів та нормалізацію даних. Виклики при реалізації методу PPG включають вплив зовнішнього освітлення, рухи користувача та індивідуальні особливості шкірного покриву.

Важливим етапом обробки PPG-сигналу є виявлення піків, що відповідають серцевим скороченням. Використання адаптивного порогу на основі статистичного аналізу сигналу дозволяє ефективно виявляти піки навіть за наявності шумів. Мінімальна відстань між піками визначається виходячи з фізіологічних обмежень максимальної частоти серцевих скорочень [3]. Валідація якості сигналу здійснюється шляхом аналізу стандартного відхилення, діапазону значень та

періодичності коливань, що дозволяє відсіювати невалідні вимірювання.

Підрахунок кроків реалізується на основі даних з акселерометра смартфону, який реєструє прискорення пристрою у трьох просторових вимірах. Алгоритм виявлення кроків базується на детекції характерних паттернів прискорення, що виникають під час ходьби чи бігу [4]. Для підвищення точності застосовується фільтрація низьких частот для усунення високочастотних шумів та встановлення динамічного порогу, що адаптується до темпу руху користувача. Точність підрахунку кроків залежить від розташування смартфону та характеру фізичної активності.

Моніторинг сну здійснюється шляхом аналізу рухової активності користувача протягом ночі з використанням акселерометра та гіроскопа. Періоди тривалої нерухомості інтерпретуються як фази сну, тоді як короткочасні рухи можуть вказувати на пробудження або неспокійний сон. Комбінування даних з різних датчиків підвищує надійність визначення тривалості та якості сну [5].

Застосування сучасних алгоритмів обробки сигналів дозволяє досягти достатнього рівня точності вимірювання біометричних показників через стандартні датчики смартфону для використання в системах персонального моніторингу здоров'я. Проте необхідно враховувати обмеження методів та забезпечувати валідацію якості вимірювань для підвищення надійності отриманих даних.

Список використаних джерел:

1. Google Android Developers. *Build with Android*. 2024. Режим доступу: https://developer.android.com/ (дата звернення: 01.11.2025).

2. Google Android Developers. *Sensors and location.* 2024. Режим доступу: https://developer.android.com/develop/sensors-and-location (дата звернення: 02.11.2025).

3. Google Android Developers. *Best practices for sensor usage.* 2024. Режим доступу: https://developer.android.com/guide/topics/sensors (дата звернення: 03.11.2025).

4. Google Developers. *Activity Recognition API.* 2024. Режим доступу: https://developers.google.com/location-context/activity-recognition (дата звернення: 04.11.2025).

5. Fino E., Mazzetti M. *Monitoring healthy and disturbed sleep through smartphone applications: A review of experimental evidence. Sleep and Breathing*. 2019. Vol. 23(1). P. 13-24. Режим доступу: https://link.springer.com/ article/10.1007/s11325-018-1661-3 (дата звернення: 04.11.2025).

УДК 628.971:681.5

Герасименко В.А., к.т.н., доцент
Денисенко Д.С., здобувач
Романов В.О., здобувач
Харківський національний університет міського господарства імені О.М. Бекетова

ПРОЄКТУВАННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ОСВІТЛЕННЯ ДЛЯ ГРОМАДСЬКИХ ПРОСТОРІВ

Інтенсивна урбанізація, зростання тривалості активного часу перебування людей у містах та посилення вимог до енергоефективності та безпеки громадських просторів зумовлюють перехід від традиційних систем освітлення до інтелектуальних рішень, інтегрованих у концепцію «розумного міста». Сучасні LED-технології в поєднанні з датчиками, мережами Інтернету речей (IoT) та хмарною аналітикою дозволяють створювати системи освітлення, що адаптуються до реального використання простору, змін погоди, часу доби й потреб користувачів, істотно знижуючи енергоспоживання без погіршення візуального комфорту. Дослідження останніх років [1] демонструють, що впровадження інтелектуальних систем у внутрішніх та зовнішніх громадських просторах дає змогу скорочувати споживання електроенергії на десятки відсотків за рахунок поєднання димування, зонального керування та адаптивних сценаріїв роботи освітлювальних приладів.

Ключовою відмінністю інтелектуальної системи освітлення від традиційної є її здатність до контекстно-залежного керування освітлювальними приладами на основі даних від різних сенсорів, прогнозних моделей та політик керування, закладених у програмне забезпечення. Типова архітектура такої системи має кілька рівнів: апаратний рівень (LED-світильники зі вбудованими драйверами, датчики присутності, освітленості, камери), рівень зв’язку (DALI-2, ZigBee, Bluetooth Mesh, NB-IoT, LoRaWAN), рівень керування (локальні контролери, шлюзи) та верхній рівень платформи, де здійснюються аналітика, формування сценаріїв, інтеграція з іншими сервісами «розумного міста». Наукові роботи з інтелектуального освітлення [2] показують, що переважна більшість сучасних рішень базується на IoT-підході. На рисунку 1 наведено структуру інтелектуальної системи освітлення та її складових.

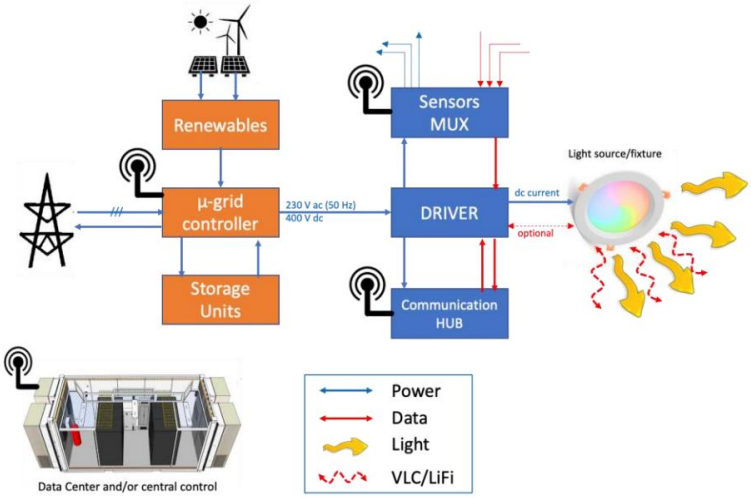


Рисунок 1 – Структура інтелектуальної системи освітлення

При проєктуванні інтелектуальної системи освітлення для громадських просторів важливо враховувати специфіку таких середовищ. Громадські простори мають багатофункціональний характер: тут можуть одночасно співіснувати потоки пішоходів, велосипедистів, зони відпочинку, дитячі майданчики, малі архітектурні форми, елементи озеленення тощо. Це вимагає розділення території на функціональні підзони з різними світлотехнічними вимогами – від базового рівня освітленості для безпечного пересування до акцентного підсвічування об'єктів та динамічного сценарного освітлення під час заходів. Додатковим обмеженням є необхідність зниження світлового забруднення, дотримання вимог до обмеження сліпучої дії, коректного вибору колірної температури та узгодження з місцевими нормативами й політиками.

Структуру процесу проєктування інтелектуальної системи освітлення доцільно будувати як послідовність етапів. На аналітичному етапі виконується збір та обробка вихідних даних: геометрія простору, характеристики покриттів, наявні елементи благоустрою, існуючі системи освітлення, статистика відвідуваності, вимоги нормативних документів щодо мінімальної освітленості, рівномірності та сліпучої дії. Наступним етапом формується набір цілей: мінімізація енергоспоживання, підвищення безпеки пересування, створення комфортної атмосфери, можливість організовувати події без додаткових тимчасових інсталяцій, інтеграція з системами

відеоспостереження, Wi-Fi-інфраструктурою тощо. На етапі концептуального проєктування визначається структура мережі освітлення, принципи зонування, вибір типів світильників, датчиків та протоколів зв'язку, а також загальна логіка керування (централізована, децентралізована або гібридна). Завершальний інженерний етап включає детальні світлотехнічні розрахунки, моделювання сценаріїв роботи, оцінку енергоефективності та окупності, розробку вимог до кібербезпеки й захисту даних користувачів.

Не менш важливою складовою проєктування є людиноцентричний підхід (HCL), який передбачає орієнтацію не лише на формальні нормативні показники, а й на суб'єктивне сприйняття світла користувачами: відчуття безпеки, атмосфери простору, візуальний комфорт. Сучасні дослідження [3] показують, що грамотно спроєктоване освітлення може істотно підвищувати привабливість громадських просторів, подовжувати час їх активного використання і сприяти соціальній взаємодії, водночас знижуючи рівень злочинності та кількість нещасних випадків у темну пору доби.

Проєктування інтелектуальної системи освітлення для громадських просторів є комплексним завданням, що поєднує світлотехнічні розрахунки, цифрові технології, урбаністичні підходи та соціально-психологічні аспекти сприйняття середовища. Подальший розвиток цього напрямку досліджень пов'язаний із глибшою інтеграцією методів штучного інтелекту, цифрових двійників міських просторів, а також із формуванням прозорих стандартів і рекомендацій, які дозволять масштабувати успішні пілотні рішення до рівня міських і регіональних систем освітлення.

Список використаних джерел:

1. González-Amarillo, C.-A.; Cárdenas-García, C.-L.; Caicedo-Muñoz, J.-A.; Mendoza-Moreno, M.-A. Smart Lumini: A Smart Lighting System for Academic Environments Using IoT-Based Open-Source Hardware. Revista Facultad de Ingeniería, Vol. 29, No. 54 (2020), e11060. DOI: 10.19053/01211129.v29.n54.2020.11060

2. Khemakhem S., Krichen L. A comprehensive survey on an IoT-based smart public street lighting system application for smart cities // Franklin Open. 2024. Vol. 8, Art. 100142. DOI: 10.1016/j.fraope.2024.100142

3. Bachanek, K.H.; Tundys, B.; Wiśniewski, T.; Puzio, E.; Marouškovά, A. Intelligent Street Lighting in a Smart City Concepts – A Direction to Energy Saving in Cities: An Overview and Case Study. Energies 2021, 14, 3018. https://doi.org/10.3390/en14113018

УДК 621.37

Дармограй Я.М., магістрант
Ципоренко В.Г., к.т.н., доцент
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ДИНАМІЧНО КЕРОВАНИХ ПРОТОКОЛІВ МОБІЛЬНИХ МЕРЕЖ

У сучасному світі мобільні комунікації відіграють ключову роль у забезпеченні зв'язку в умовах відсутності стаціонарної інфраструктури. Мобільні adhoc мережі (MANET) дозволяють пристроям самоорганізовуватися та обмінюватися даними без централізованого управління. Такі мережі застосовують для військових операцій, екстрених служб до систем розумного транспорту та інтернету речей.

Проведений аналіз показав, що існуючі протоколи маршрутизації для мобільних мереж мають ряд суттєвих недоліків. Проактивні протоколи (DSDV, OLSR) підтримують постійну інформацію про маршрути, що призводить до високого споживання мережевих ресурсів та енергії, особливо у великих мережах з мінливою топологією. Реактивні протоколи (AODV, DSR) створюють значні затримки при встановленні з'єднання через необхідність пошуку маршруту за запитом. Традиційні одношляхові підходи не використовують потенціал багатоінтерфейсних мобільних пристроїв для агрегації пропускної здатності [1].

В роботі виконано дослідження швидкодіючих методів керування передачею даних, які поєднують алгоритми контролю перевантажень мережі та динамічне керування протоколами передачі, що мінімізує затримки в чергах і підвищує пропускну здатность мобільних мереж. В результаті система забезпечує динамічне виявлення множинних шляхів між вузлами, оптимальне балансування навантаження між ними з урахуванням поточних умов мережі, безперервність з'єднання при мобільності вузлів та оптимізацію використання енергетичних ресурсів мобільних пристроїв.

Виконано дослідження методів інтеграції технології Multipath TCP (MPTCP) та реактивних протоколів маршрутизації для підвищення ефективності передачі даних у мобільних мережах. Показано, що для моніторингу роботи мобільних мереж доцільно контролювати швидкість передачі даних, затримки, надійність з'єднання, енергоефективність та масштабованість. В результаті за допомогою технології MPTCP отримуємо можливість одночасного використання кількох мережевих інтерфейсів (LTE, 5G) із вбудованими механізмами контролю перевантаження та відновлення після помилок, рис.1.

Технологія MPTCP передбачає створення множинних підпотоків TCP, які працюють незалежно, забезпечуючи безперервність з'єднання при переміщенні між точками доступу. Тому доцільно в MPTCP використовувати алгоритми планування пакетів (Default Scheduler, BLEST, Redundant Scheduler), які дозволяють оптимально розподіляти трафік між доступними шляхами з урахуванням їх характеристик (RTT, пропускна здатність, завантаженість). Приймачі MPTCP завдяки методам контролю перевантаження LIA та OLIA забезпечать коректність та ефективне балансування навантаження [2].

В результаті показано, що інтеграція протоколів MPTCP з AODV дозволяє швидко знаходити альтернативні шляхи при зміні топології, а використання множинних маршрутів підвищує загальну пропускну здатність з'єднання. Таким чином, забезпечуються динамічні з'єднання з підвищеною стійкістю до відмов окремих каналів та підвищення загальної ефективності роботи мережі.

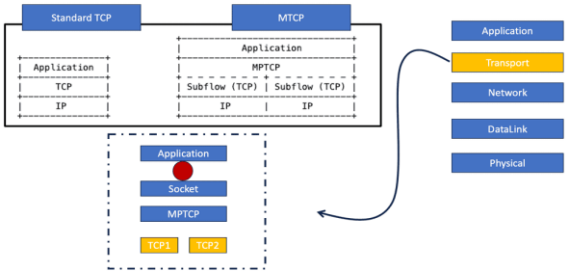


Рисунок 1 – Архітектура MTCP-з'єднання

Виконано моделювання, тестування та дослідження ефективності мереж мобільного з'вязку з динамічним керуванням протоколів на основі використання емуляторів мереж (ns-3, Mininet, OMNeT++). Результати досліджень підтвердили ефективність запропонованих методів.

Список використаних джерел:

1. Ford, A.; Raiciu, C.; Handley, M.; Barre, S.; Iyengar, J. Architectural Guidelines for Multipath TCP Development. 2070-1721. 2011. Режим доступу: https://www.rfc-editor.org/rfc/rfc6182

2. Wu, H.; Ferlin, S.; Caso, G.; Alay, Ц.; Brunstrom, A. A. Survey on Multipath Transport Protocols Towards 5G Access Traffic Steering, Switching and Splitting. IEEE Access 2021, 9, 164417–164439. Режим доступу:: https://ieeexplore.ieee.org/document/9645537

УДК 621.396

Морозов Д.С., ст. викладач,
Журавський Ю.В., д.т.н., професор,
Чухов В.В., к.т.н., доцент,
Коломієць Р.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

УДОСКОНАЛЕНИЙ МЕТОД СИНТЕЗУ БАГАТОШАРОВИХ АНТЕННИХ РЕШІТОК НА ОСНОВІ ПАТЧ-АНТЕН ІЗ КРУГОВОЮ ПОЛЯРИЗАЦІЄЮ

Використання багатошарових антенних решіток із діелектричних матеріалів різної товщини та діелектричної проникності, що чергуються з шарами металізації, дають змогу ефективно розділити площину антенних елементів та мережу живлення [1]. Зв'язок між мережею живлення і антенними елементами у такому випадку забезпечується шляхом використання щілин різної форми в шарах металізації. Використання мікросмужкових подільників мережі живлення разом із контролюванням ступеня зв'язку між антенним елементом і лінією живлення дає змогу синтезувати антенні решітки з амплітудним розподілом Тейлора або Дольфа-Чебишева для зниження рівня бічних пелюсток [2].

З метою збільшення кількості антених елементів синфазних антенних решіток застосовуються схеми з послідовним чи послідовно-паралельним живленням антенних елементів [3]. Антенні решітки з патч-антен із круговою поляризацією на основі багатошарових метало-діелектричних пластин для зв'язку між шарами використовують випромінючі щілини різної форми [4]. Хрестоподібні щілини забезпечують низький рівень Axial Ratio (AR, величина оберенена до коефіцієнту еліптичності) для прямокутних патчів решітки, однак вимагають високої точності виготовлення. Для додаткового узгодження щілини і мікросмужки живлення може використовуватись шлейф як продовження мікросмужки [5]. Недоліком такого підходу є неможливість використання послідовних схем живлення антенних елементів із подібним вертикальним шлейфом. Тобто більше одного антенного елемента на одній лінії живлення розмістити неможливо. Відповідно, для усунення зазначених недоліків та обмежень було вдосконалено метод синтезу багатошарових антенних решіток на основі патч-антен із круговою поляризацією з послідовним живленням елементів. Метод відрізняється тим, що на першому етапі забезпечується низький рівень AR шляхом визначення оптимальних

співвідношень довжини і ширини плечей хрестоподібної щілини збудження та розмірів прямокутного патча антенного елементу.

Для покращення AR оптимізується кут повороту прямокутної патч-антени. Удосконалення методу також включає посилення зв'язку між прямокутним патчем, щілиною збудження і мікросмужковою лінією живлення шляхом ітераційного визначення параметрів ємнісних шлейфів на лінії живлення. Додатковим елементом узгодження в удосконаленому методі є зрізання кутів прямокутного антенного патч-елемента для покращення його узгодження. Використання шлейфів і зрізаних кутів патч- елементів дають змогу контролювати амплітудний розподіл у межах плеча живлення решітки для зниження рівня бічних пелюсток антенної решітки.

Науковою новизною результатів дослідження є удосконалення методу синтезу багатошарових антенних решіток на основі патч-антен із круговою поляризацією, який відрізняється визначенням оптимальних співвідношень довжини і ширини плечей хрестоподібної щілини збудження за критерієм AR<3 dB за S_{11}< 20 dB, зрізанням кутів патч-антен та розрахунком їх розмірів і кутів повороту, ітераційним доузгодженням вхідного опору патч-антен ємнісними шлейфами на лінії живлення, що дозволяє мінімізувати рівень S_{11} при забезпеченні заданого рівня Axial Ratio у смузі робочих частот антени.

Список використаних джерел:

1. Liang C.-F., Yuan F., Lyu Y.-P., Liu B.-G. A wideband circularly polarized 2×2 patch antenna array. *Microwave and Optical Technology Letters.* 2025. Vol. 67. e70315. DOI: 10.1002/mop.70315.

2. Salim M., Najm T., Sultan Q., Saleh A. A new approach of applying Chebyshev distribution of series fed microstrip antenna array for radar applications. *The Applied Computational Electromagnetics Society Journal (ACES).* 2023. DOI: 10.13052/2022.ACES.J.370902.

3. Tan Q., Fan K., Yang W., Luo G. Low sidelobe series-fed patch planar array with AMC structure to suppress parasitic radiation. *Remote Sensing.* 2022. Vol. 14. Art. no. 3597. DOI: 10.3390/rs14153597.

4. Mohammadi Shirkolaei M. High efficiency X-band series-fed microstrip array antenna. *Progress In Electromagnetics Research C*. 2020. Vol. 105. P. 35–45. DOI: 10.2528/PIERC20061003.

5. Duarte M., Varum T., Matos J., Pinho P. In-house development of 17 GHz antennas: Potentials and difficulties. *URSI Radio Science Bulletin*. 2018. No. 364. P. 45–54. DOI: 10.23919/URSIRSB.2018.8486767.

Дзюба М.В., аспірант
Нікітчук С.М., ст.викладач
Гераймович О.М., ст.викладач
Державний університет «Житомирська політехніка»

АРХІТЕКТУРНІ ОСОБЛИВОСТІ ТА ВИБІР КОМУНІКАЦІЙНИХ ПРОТОКОЛІВ У СИСТЕМАХ «SMART HOME»

Сучасний етап розвитку інформаційного суспільства характеризується стрімким впровадженням концепції «Інтернету речей» (IoT) у повсякденне життя, що знайшло своє відображення у створенні інтелектуальних систем «розумного будинку» («Smart Home»). Одним із найбільш критичних та динамічних сегментів цього ринку є системи безпеки, що базуються на поєднанні відеомоніторингу та контролю доступу.

Традиційні системи контролю доступу (СКД), що використовують лише механічні ключі або прості RFID-ідентифікатори, вже не відповідають сучасним вимогам безпеки через вразливість до копіювання та відсутність можливості дистанційної верифікації особи в реальному часі. Актуальність даної роботи зумовлена необхідністю переходу від пасивного спостереження до інтелектуальних систем, здатних самостійно приймати рішення на основі аналізу відеоданих.

З точки зору радіотехніки та електронних комунікацій, особливу гостроту набуває проблема ефективної передачі широкосмугового відеосигналу через бездротові канали зв'язку в умовах обмеженого спектра та високого рівня завад у житлових масивах. Впровадження нових стандартів, таких як Wi-Fi 6 (802.11ax) та протоколу Matter, відкриває нові можливості для побудови стабільних, енергоефективних та мультибрендових мереж безпеки.

Окрім того, сучасним трендом є розвиток Edge Computing – перенесення обчислювальних потужностей безпосередньо на кінцеві пристрої (IP-камери, контролери). Це дозволяє мінімізувати затримки в передачі сигналу та підвищити рівень конфіденційності даних, що є вкрай важливим для приватного сектору.

Метою дослідження є розробка архітектури та технічних рішень для інтелектуальної системи відеомоніторингу та контролю доступу, яка забезпечує високу точність верифікації об'єктів у реальному часі та безперебійну взаємодію компонентів у межах єдиної екосистеми Smart Home.

У роботі обґрунтовано доцільність використання гібридної комунікаційної моделі для розділення потоків даних.

– відеоканал: обрано стандарт Wi-Fi 6 (802.11ax), який завдяки технології OFDMA забезпечує високу пропускну здатність для 4K-відео в умовах зашумленого середовища.

– канал керування: для виконавчих механізмів (замків) та датчиків визначено пріоритетність протоколів ZigBee або Thread (база для Matter), що забезпечують високу автономність пристроїв.

– енергетичне моделювання: розрахунок енергетичного бюджету радіолінії (Link Budget) показав, що при проходженні через дві стіни втрати на частоті 5 ГГц становлять 76.4 дБ, що на 6.4 дБ більше, ніж на частоті 2.4 ГГц.

– надійність: запас потужності для каналу 2.4 ГГц (ZigBee) становить 25 дБ, що гарантує стабільне керування доступом навіть крізь капітальні стіни.

– інтеграція: впровадження стандарту Matter дозволяє об'єднати різнорідні пристрої в єдину екосистему на рівні IP-пакетів без складних шлюзів.

Гібридна архітектура, що поєднує Wi-Fi 6 для відеомоніторингу та Thread/ZigBee для контролю доступу, дозволяє досягти оптимального балансу між швидкістю передачі медіаданих та надійністю керування замками. Використання стандарту Matter забезпечує високу сумісність пристроїв та наскрізне шифрування даних.

Список використаних джерел:

1. Сучасні засоби обмеження доступу та система керування відвідувачами – Режим доступу: https://www.bezpeka-shop.com/ua/blog/poleznye-sovety/suchasni-zasoby-obmezennia-dostupu-ta-systema-keruvannia-vidviduvachamy/?srsltid=AfmBOoreRae8sbnD7Yrm2W5LEUT8s1N21eh3WqIVJYSF8oATJzzICy4P

2. Архітектура кібербезпеки. Як побудувати надійний та сучасний захист [Електронний ресурс] // Avolutech. – Режим доступу: https://avolutech.com/blog/arxitektura-kiberbezpeky

3. Новий стандарт «Matter» та його використання у системах управління освітленням [Електронний ресурс]. – 2023. – Режим доступу: https://5watt.ua/uk/blog/statti/novij-standart-matter-ta-jogo-vikoristannya-u-sistemakh-upravlinnya-osvitlennyam.

Секція 5
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

УДК 004.4

Кольцова Н.О., здобувач,
Савіцький Р.С., ст. викладач
Державний університет «Житомирська політехніка»

ПІДТРИМКА ІНКЛЮЗИВНОСТІ: КУРС ДЛЯ РЕІНТЕГРАЦІЇ ВПО/ВЕТЕРАНІВ

У сучасному українському суспільстві важливим завданням є інтеграція внутрішньо переміщених осіб (ВПО) та ветеранів до соціального середовища через впровадження інклюзивних курсів. Соціальна та професійна реінтеграція цих груп населення є критично важливим завданням для забезпечення стійкості економіки та суспільної злагоди. Розвиток таких ініціатив сприяє не лише соціальній адаптації, а й покращенню психосоціального стану представників цих категорій населення. Освітні платформи відіграють ключову роль у забезпеченні доступності та гнучкості навчання, що є особливо важливим для людей з обмеженими можливостями пересування або специфічними потребами, спричиненими бойовими діями чи переміщенням. Актуальність теми підкреслюється також наявністю державних програм підтримки, які потребують якісних та інклюзивних освітніх продуктів для їх ефективної реалізації [1, 2].

Інклюзивність у контексті реінтеграції ВПО та ветеранів включає в себе створення сприятливих умов для їхнього навчання, працевлаштування та соціалізації. Важливою частиною таких курсів є використання інклюзивних педагогічних підходів, які дозволяють забезпечити рівні можливості для всіх учасників незалежно від їхнього соціального статусу чи фізичних можливостей. Програми повинні враховувати специфічні потреби учасників, зокрема ветеранів, у процесі реінтеграції в суспільство після служби [3].

Багато ветеранів та ВПО потребують швидкого освоєння нових професій, оскільки їхні попередні місця роботи можуть бути втрачені або професійні навички вимагають оновлення. Онлайн-курс має бути сфокусований на навичках, що користуються попитом, включаючи цифрову грамотність, навички самопрезентації та основи підприємництва [2].

Використання технологій, таких як онлайн-платформи та мобільні додатки, значно полегшує доступ до навчальних ресурсів для людей з

обмеженими можливостями або тих, хто змушений проживати у віддалених районах. Технології забезпечують не лише доступ до навчання, але й дозволяють інтегрувати адаптивні методики, що враховують особливості кожного учасника. Цифрові платформи можуть використовуватись для забезпечення доступу до психологічної підтримки, що є критично важливим для категорій населення, які зазнали посттравматичного стресового розладу чи депресії.

Курси для ветеранів повинні включати психоосвітні програми, що допомагають адаптуватися до цивільного життя, а також тренінги, спрямовані на розвиток професійних навичок. Важливим є врахування психологічних аспектів, таких як стрес, посттравматичний синдром та інші розлади, що можуть виникати у ветеранів після служби. Для цього необхідно впроваджувати курси з основ психосоціальної адаптації, що включають не лише теоретичні знання, але й практичні заняття.

Для ефективної реінтеграції ВПО та ветеранів важливо створити мережу соціальних партнерств, яка об’єднує державні органи, неурядові організації, бізнес та навчальні заклади. Спільна робота забезпечує комплексну підтримку соціальної адаптації, зокрема через посередництво неурядових організацій між державою та цільовими групами. Партнерства з бізнесом сприяють професійній орієнтації та працевлаштуванню ветеранів і ВПО, що є важливою частиною їх адаптації [4].

Аналіз успішних прикладів показує, що реінтеграція через навчання та курси дозволяє зменшити рівень соціальної ізоляції та стресу серед ВПО і ветеранів, що, у свою чергу, позитивно впливає на їх здатність знайти роботу, інтегруватися в нове середовище та зберігати психічне здоров'я. Такі програми допомагають не лише вирішити проблеми соціальної адаптації, а й зміцнюють соціальну згуртованість, забезпечуючи підтримку з боку громади та держави.

Список використаних джерел:

1. Кабінет Міністрів України. Реформа підтримки ветеранів. (н.д.). URL: https://www.kmu.gov.ua/reformi/bezpeka-ta-oborona/reforma-pidtrimki-veteraniv (дата звернення: 29.10.2025).
2. Закон України «Про соціальний і правовий захист військовослужбовців та членів їх сімей». Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2011-12
3. Захаріна Т. І. Теоретико-методичні засади соціальної реінтеграції ветеранів російсько-української війни у закладах вищої освіти: дис. докт. пед. наук : 13.00.05. Київ, 2024. С. 672.
4. Галина Гандзілевська, Олена Ратінська. Адаптація і реабілітація учасників бойових дій. Вісник Львівського університету. Серія психологічні науки. 2025. Випуск 23 С. 112–125

УДК 004.7

Рубай А.В., здобувач
Назар Ю.С., Ph.D
Львівський державний університет безпеки життєдіяльності

ТЕХНІЧНІ АСПЕКТИ МОДУЛЬНОЇ ІНТЕГРАЦІЇ ГОЛОСОВОГО ЗВ'ЯЗКУ В ОСВІТНІ ПЛАТФОРМИ

Виклики останніх років, зокрема пандемія COVID-19 та повномасштабна війна в Україні, актуалізували потребу в надійних інструментах дистанційної освіти. У цих умовах інтеграція голосового зв'язку в навчальні платформи набуває стратегічного значення для забезпечення безперервності навчального процесу.

Метою роботи є дослідження технічних аспектів модульної інтеграції голосового зв'язку в освітні платформи з подальшим впровадженням розроблених рішень у віртуальне навчальне середовище «Віртуальний університет» на базі moodle.

Голосова взаємодія робить дистанційне навчання більш природним, адже викладач і студенти можуть спілкуватися у режимі реального часу. Водночас інтеграція голосового зв'язку — це не просто додавання мікрофона чи кнопки «дзвінок». Це складний процес, що потребує продуманої архітектури та сучасних рішень. Модульність у цьому випадку є критично важливою, адже вона дозволяє розширювати або змінювати функціонал без повного перепроєктування системи, що особливо актуально для освітніх платформ, які постійно оновлюють та покращують своє середовище.

Основою голосових технологій у браузері виступає WebRTC — стандарт, що забезпечує низьку затримку передачі аудіо, прямі з'єднання між користувачами та адаптацію до змін якості інтернету. Саме він став базовим рішенням для масових онлайн-занять у період пандемії. Додатково застосовуються протоколи SIP для встановлення з'єднань, RTP для передачі аудіопотоків у реальному часі та кодек Opus, який гарантує високу якість звуку навіть за нестабільного інтернету.

Щоб голосовий модуль працював стабільно, платформа має спиратися на надійну інфраструктуру: STUN- і TURN-сервери для обходу мережевих обмежень, сервери сигналізації для встановлення з'єднань та механізми контролю якості зв'язку. В умовах війни в Україні такі рішення набули особливого значення, адже під час повітряних тривог, відключень електроенергії чи нестабільного мобільного інтернету система повинна залишатися працездатною.

Модульна інтеграція дає змогу освітнім системам обирати між власними медіасерверами (Janus, Kurento, Jitsi) та готовими хмарними

рішеннями (Twilio, Agora, Vonage, Microsoft Azure Communication Services). Такий підхід дозволяє оптимізувати витрати, швидко додавати нові функції та масштабувати систему зі зростанням кількості користувачів. Для наочної ілюстрації взаємодії описаних технологій та компонентів розроблено відповідну структурну схему.

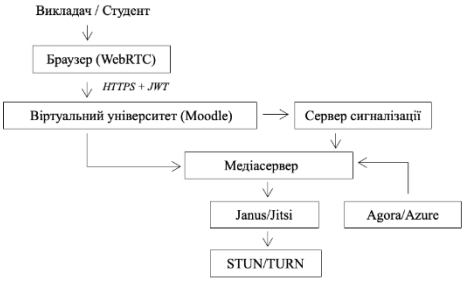


Рисунок 1 – Структурна схема модульної інтеграції голосового зв'язку

Запропонована на рисунку 1 архітектура реалізує взаємодію користувача з платформою через HTTPS із використанням JWT-аутентифікації. Обробка аудіопотоків делегується модульному медіасерверу, що дозволяє гнучко обирати між власними рішеннями (Janus, Jitsi) та хмарними сервісами (Agora, Azure) залежно від навантаження. Стабільність з'єднання та обхід NAT забезпечують інтегровані STUN/TURN-сервери, що є критично важливим під час роботи через мобільний інтернет або в умовах мережевих обмежень. Такий підхід дозволяє масштабувати систему без повного перепроєктування та оптимізувати витрати

Отже, модульна інтеграція голосового зв'язку є одним із ключових напрямів розвитку сучасних освітніх платформ. Вона перетворює освітню платформу на стійку комунікаційну систему, здатну адаптуватися до технічних обмежень та кризових умов, забезпечуючи якісну взаємодію учасників навчання.

Список використаних джерел:

1. RFC 8825. Overview: Real Time Protocols for Browser-based Applications / H. Alvestrand. Internet Engineering Task Force, 2021.

2. Newman S. Building Microservices: Designing Fine-Grained Systems. 2nd Edition. O'Reilly Media, 2021. 614 p.

3. Кузьмінська О. Г. та ін. Цифрова трансформація освітнього процесу в умовах воєнного стану // Інформаційні технології і засоби навчання. – 2022. – Т. 88, № 2. – С. 1–18.

УДК 378.147:004

Корнєва В.Р., викладач,
Терницький С.В., викладач
Прилуцький технічний фаховий коледж

ЦИФРОВА ТРАНСФОРМАЦІЯ ОСВІТНЬОГО ПРОЦЕСУ В УМОВАХ ЗМІШАНОГО НАВЧАННЯ

Цифрова трансформація освіти стала одним із ключових напрямів розвитку сучасних освітніх систем. Поширення інформаційно-комунікаційних технологій, активізація дистанційної взаємодії та потреба у гнучких моделях навчання сприяли переходу закладів освіти до змішаних форм організації освітнього середовища. Такий формат поєднує традиційну аудиторну роботу та онлайн-компоненти, що дозволяє оптимізувати навчальний процес, забезпечити індивідуальну траєкторію для кожного здобувача освіти та створити умови для ефективного поєднання теоретичної та практичної діяльності. Змішане навчання значно розширює можливості для самостійної, дослідницької та проєктної роботи, сприяючи розвитку навичок XXI століття.

Процес цифрової трансформації охоплює кілька структурних компонентів: оновлення педагогічних технологій, розвиток цифрової інфраструктури, формування цифрових компетентностей учасників освітнього процесу та запровадження нових моделей взаємодії між викладачем і студентом. Одним із ключових аспектів є використання хмарних сервісів, інтерактивних платформ та систем управління навчанням (LMS).

У межах змішаного навчання викладач отримує значно ширші можливості для адаптації навчальних матеріалів до потреб конкретних студентів. Інструменти штучного інтелекту дозволяють аналізувати результати діяльності здобувачів, прогнозувати рівень засвоєння, визначати прогалини в знаннях і пропонувати індивідуальні завдання для їх усунення. Широке застосування інтерактивних ресурсів — відеолекцій, анімацій, симуляторів, віртуальних лабораторій, сервісів спільної роботи та електронних бібліотек — сприяє активізації пізнавальної діяльності, розвитку критичного мислення та підвищенню навчальної мотивації. Такі ресурси роблять процес навчання більш візуальним, наочним і доступним навіть для студентів із різними стилями сприйняття інформації.

Важливим компонентом цифрової трансформації є формування цифрової грамотності та відповідальної поведінки здобувачів освіти. Сучасні студенти мають вміти ефективно працювати з великими масивами інформації, застосовувати різні цифрові інструменти,

критично оцінювати достовірність даних, керувати власною цифровою безпекою та приватністю. У змішаному навчанні ці навички набувають особливої ваги, оскільки якість виконання завдань та успішність навчання часто залежить від здатності студента працювати самостійно, користуючись наданими цифровими ресурсами.

Викладач у цифровому середовищі також виконує нові ролі: тьютора, фасилітатора, модератора командної роботи та консультанта. Замість традиційної ролі «джерела інформації» він стає організатором освітнього простору, спрямованого на осмислення, дослідження й самостійний пошук рішень. Змішане навчання дозволяє поєднувати синхронні зустрічі (онлайн або офлайн) та асинхронні активності, що створює гнучкі умови для навчання за індивідуальним темпом. Такий підхід сприяє розвитку самодисципліни, відповідальності, вмінь планування та самооцінювання.

Отже, цифрова трансформація освітнього процесу в умовах змішаного навчання є невід'ємним елементом модернізації сучасної освіти. Упровадження цифрових технологій потребує системного підходу, методичної підтримки, професійного розвитку педагогічних кадрів і створення єдиної цифрової екосистеми закладу освіти. Успішна цифрова трансформація відкриває нові перспективи для розвитку інноваційного навчального середовища, у якому здобувач освіти стає активним учасником, творцем знань і співорганізатором власної освітньої траєкторії.

Список використаних джерел:

1. ДСТУ 8302:2015. Бібліографічні посилання. Загальні положення та правила складання.
2. Anderson T. The Theory and Practice of Online Learning. AU Press, 2020.
3. Graham C. R. Blended Learning Systems: Definition, Models, and Future Directions. Wiley, 2019.
4. Redecker C. European Framework for the Digital Competence of Educators. Publications Office of the EU, 2017.
5. Horn M., Staker H. Blended: Using Disruptive Innovation to Improve Schools. Wiley, 2014.

УДК 378.147:004

Корнєва В.Р., викладач,
Корнєва С.П., викладач
Прилуцький технічний фаховий коледж

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЖИТТІ ВИКЛАДАЧІВ ФАХОВОЇ ПЕРЕДВИЩОЇ ОСВІТИ

Сучасний світ стрімко цифровізується, і ця тенденція впливає на всі сфери суспільного життя, зокрема й на освіту. Фахова передвища освіта, яка відіграє ключову роль у підготовці кваліфікованих робітників та молодших спеціалістів, сьогодні переживає активну трансформацію, спричинену розвитком інформаційних технологій. Викладач уже не є лише носієм знань — він перетворюється на фасилітатора навчання, організатора цифрового освітнього середовища, модератора комунікації та консультанта, здатного адаптуватися до швидких змін. Інформаційні технології стають не просто інструментом, а основою нової педагогічної взаємодії.

У житті сучасного викладача фахового коледжу інформаційні технології присутні щодня: від підготовки навчальних матеріалів до оцінювання студентів та організації освітнього процесу. Вони дозволяють по-новому побудувати комунікацію, розширюють можливості для візуалізації, моделювання, дистанційного навчання та перевірки знань. З появою нових цифрових сервісів, платформ і програм змінюється сам зміст професійної діяльності викладача, а також вимоги до його компетентностей. Сучасний педагог повинен володіти широким спектром цифрових навичок: від базового використання офісних програм до роботи зі складними освітніми платформами, віртуальними лабораторіями, системами автоматизації навчального процесу та інструментами штучного інтелекту.

Цифрова компетентність викладача стає основною умовою якісної освіти. Вона включає вміння створювати електронні освітні матеріали, організовувати онлайн-навчання, використовувати інтерактивні технології, забезпечувати інформаційну безпеку та дотримання академічної доброчесності. Викладач, який володіє цифровими інструментами, здатний швидко адаптувати навчальний процес до потреб студентів, забезпечити гнучкість і доступність навчання навіть у нестабільних умовах. Пандемія COVID-19 стала переломним моментом, коли освітня галузь була змушена перейти на дистанційний формат, і саме тоді цифрові навички стали життєво необхідними. Досвід, здобутий у цей період, продовжує впливати на сучасні практики навчання.

Викладачі активно використовують електронні освітні платформи, які стали ядром інтерактивного цифрового середовища. Google Classroom, Moodle, Microsoft Teams, Zoom та інші сервіси дозволяють формувати курси, завантажувати навчальні матеріали, організовувати онлайн-заняття, створювати тести, оцінювати роботи та підтримувати постійний зворотний зв'язок. Такі платформи забезпечують прозорість, контроль, системність навчального процесу та зручність зберігання електронних портфоліо студентів. Вони стали універсальним інструментом для асинхронної та синхронної взаємодії зі студентами.

Широке застосування набули хмарні технології. Google Drive, OneDrive та інші сервіси дозволяють зберігати документи, створювати спільні файли, організовувати колективну роботу над проєктами. Це особливо важливо для студентів технічних спеціальностей, які мають працювати з великою кількістю графічних матеріалів, звітів, креслень і схем. Хмара забезпечує зручний доступ із будь-якого пристрою, а викладач може легко перевіряти роботи та надавати коментарі.

Окреме місце в освітній діяльності викладача займає використання штучного інтелекту. Цей інструмент допомагає автоматизувати значну частину рутинної роботи: генерувати тести й завдання, перевіряти граматику та стилістику текстів, створювати методичні матеріали, адаптувати контент під різні рівні підготовки студентів. ШІ може аналізувати успішність студентів та прогнозувати, які теми викликають найбільші труднощі. Викладач отримує можливість оперативно виявляти проблеми та коригувати навчальну траєкторію кожного студента. Водночас використання штучного інтелекту вимагає від педагога високого рівня цифрової етики, адже виникають питання відповідальності, авторства та дотримання академічної доброчесності.

Список використаних джерел:

1. Національна рамка кваліфікацій: постанова Кабінету Міністрів України від 23.11.2011 № 1341.

2. Концепція розвитку освіти на 2015–2025 роки. Київ: МОН України, 2015.

3. Лук'янова Л. Б., Сисоєва С. О. Неперервна професійна освіта: теорія і практика. Київ: Освіта України, 2018.

4. Паламарчук О. М. Цифровізація освіти: проблеми та перспективи розвитку. Інформаційні технології в освіті. 2020. № 2. С. 34–42.

Секція 6
ЦИФРОВА ОБРОБКА СИГНАЛІВ ТА ЗОБРАЖЕНЬ В АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ

УДК 621.317

Горобець О.С., аспірант
Подчашинський Ю.О., д.т.н., професор
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

ПЕРСПЕКТИВНІ МЕТОДИ ЦИФРОВОЇ ОБРОБКИ ЗОБРАЖЕНЬ

В наш час цифрова обробка зображень знаходить широке застосування в різних сферах життя – в медицині (для підвищення якості МРТ, КТ та ультразвукових знімків, а також для комп'ютерної діагностики); в промисловості (автоматизований візуальний огляд та контроль якості продукції); у сфері безпеки та криміналістики (розпізнавати різноманітні об'єкти); у дистанційному зондуванні Землі (аналіз супутникових знімків); у наукових дослідженнях (для підвищення точності вимірювань і структурного аналізу).

Не зважаючи на стрімкий розвиток технологій, цифрова обробка зображень досі стикається з певними проблемами, які впливають на якість результатів та складність подальшого аналізу. Шуми, що виникають під час збирання або передавання даних, призводять до спотворення важливих деталей. Часто виникають труднощі з нечіткістю та низькою роздільною здатністю, що ускладнює коректне виділення об'єктів або меж. Неоднорідність освітлення спричиняє втрату контрасту та появу тіней, що можуть бути помилково інтерпретовані як об'єкти. Також ускладнює розпізнавання та класифікацію об'єктів варіативність сцен (зміни масштабу, ракурсу, повороту, деформацій об'єктів тощо). Значні труднощі виникають при обробці складних текстур або коли об'єкти частково приховані. Суттєве значення має збереження інформації під час стиснення, оскільки надмірні втрати можуть зробити подальший аналіз неможливим [1]. Усі ці фактори вимагають ретельного вибору відповідних алгоритмів і методів.

Найбільш перспективні методів цифрової обробки зображень – глибокі згорткові нейронні мережі, трансформерні архітектури,

дифузійні моделі, малопотужні моделі для обробки на периферійних пристроях та методи самонавчання [2, 3]. Глибокі згорткові мережі зберігають високу ефективність у задачах класифікації, сегментації та детектування об'єктів, оскільки добре виявляють локальні структури та інваріантні просторові ознаки. Їхня перевага полягає у високій точності та стійкості, однак недоліком лишається значна потреба у великих обсягах даних і обчислювальних ресурсів, що ускладнює використання в реальному часі на обмежених платформах.

Трансформерні моделі поступово стають універсальним інструментом у комп'ютерному зорі завдяки здатності враховувати глобальні залежності між частинами зображення. Це робить їх придатними для задач високого рівня, включно з генерацією описів, складною сегментацією та мультизадачними системами. Водночас їхні переваги пов'язані з масштабованістю та гнучкістю. Недоліки: висока вартість тренування та схильності до погіршення продуктивності при обмежених обсягах даних [2].

Дифузійні моделі мають значний потенціал у генерації, відновленні та суперрезолюції зображень завдяки здатності реконструювати структури з великою деталізацією. Їхні переваги – висока варіативність та контрольованість процесу генерації, недоліки – обчислювальна складність і повільність

Методи, орієнтовані на малопотужні пристрої, стають перспективними у сфері мобільних застосунків, розумних камер та IoT. Вони забезпечують прийнятний баланс між точністю та швидкодією, але часто втрачають частину якості через зменшення розміру моделі, що є критичним для високоточних або медичних систем [3].

Список використаних джерел:

1. Кобилін О.А., Творошенко І.С. Методи цифрової обробки зображень: навч. посіб. Харків: ХНУРЕ, 2021. 124 с.

2. Lepcha D., Goyal B., Dogra A. Image super-resolution: A comprehensive review, recent trends, challenges and applications. URL: https://doi.org/10.1016/j.inffus.2022.10.007 (дата звернення: 10.11.2025).

3. Shu L., Zhu Q., He Y., Chen W. A survey of super-resolution image quality assessment. URL: https://doi.org/10.1016/j.neucom.2024.129279 (дата звернення: 10.11.2025).

УДК 621.37

Горшенін О.Є., к.т.н., доцент,
Горшенін М.О., магістрант
Державний університет «Житомирська політехніка»

МЕТОД РАДІОНАВІГАЦІЇ БПЛА ЗА ПОЛЕМ РАДІОВИПРОМІНЮВАНЬ В УМОВАХ СКЛАДНОГО ЕЛЕКТРОМАГНІТНОГО ОТОЧЕННЯ

В останні десятиріччя кількість джерел радіовипромінювань у всіх діапазонах збільшилась на кілька ступенів. Це спричиняє значне зростання рівня перешкод традиційним радіонавігаційним системам (РНС) у тому числі і супутниковим. В сучасних умовах воєнного радіоелектронного придушення робота класичних глобальних РНС стає зовсім не можливою.

Сучасна концепція навігації базується на використанні різних штучних радіовипромінювань як навігаційних орієнтирів. Першим напрямком наукових робіт є методи навігації за штучними полями радіовипромінювань спеціально створених додатковими радіомаяками. На практиці не завжди є можливість розгортання мережі додаткових радіомаяків, тому активно досліджувався і напрямок навігаційного використання вже наявних джерел різноманітних радіовипромінювань.

Практично усі активні радіовипромінювання певного діапазону від стабільних джерел з відомими координатами за належний підхід можна використати за опорні дані локальної навігації. В [1] розглянуто загальну концепцію «сигналів можливості» (Signals of Opportunity, SoOP), коли існуючі комунікаційні або радіотрансляційні системи в той чи інший спосіб використовуються як орієнтири для навігації. Більшість робіт розглядає використання методів SoOP на основі частотно-часового аналізу сигналів джерел наземних та супутникових радіовипромінювань у різних діапазонах. В роботі [2] розглянута система, яка використовує пеленги від наземних базових станцій GSM та методом тріангуляції визначає поточне положення БПЛА.

У доповіді пропонується метод радіонавігації рухомого об’єкта (БПЛА), що також використовує за опорну інформацію попередньо сформовані базові карти радіосигналів стабільних та нерухомих джерел радіовипромінювань у певному діапазоні. На відміну від широко використовуваних наразі базових даних частотно-часового аналізу радіовипромінювань, пропонується формування базових двовимірних карт радіовипромінювань в координатах «пеленг-частота». Такий підхід дозволяє уникнути недоліку методів, які

базуються на вимірюванні часових параметрів, що пов'язаний з втратою надійності вимірювань з причини спуфінгу або низької стабільності опорних генераторів в пристрої обробки сигналів.

Карти формуються, оновлюються та закладаються в пам'ять бортового засобу навігації під час підготовки виходу на маршрут. Бортовий засіб пеленгації та спектроаналізу під час руху періодично формує оціночні дані поточного рівня випромінювань в координатах «пеленг-частота». Ці дані порівнюються кореляційними методами з зазначеними вище картами для оцінювання поточного положення носія. Метод має дати стійку оцінку поточного положення об'єкта навігації у найскладніших умовах радіоелектронного оточення за рахунок узагальнення даних від великої кількості зареєстрованих джерел випромінювань. За такий підхід джерелами випромінювань, що заважають поточному місцевизначенню вважаються усі джерела радіовипромінювань, що не зареєстровані на карті або змінили своє просторове положення. При цьому очікується, що вплив таких джерел перешкоджаючих радіовипромінювань вибраного діапазону буде мінімізуватися за рахунок кореляційного аналізу поточної картини радіоелектронної обстановки в площині «пеленг-частота» та опорної карти радіовипромінювань в діапазоні.

Розглянуті основні вимоги до карти поля опорних радіовипромінювань, що забезпечують стійкість і безперервність процесу місцевизначення. Сформовані пропозиції щодо вибору робочого діапазону засобу навігації, який працює за запропонованим методом, його функціональної схеми та його структури. Проаналізовані обмеження, що накладаються на бортовий засіб пеленгування та спектроаналізу та сформовані практичні рішення щодо реалізації елементів такого бортового радіопеленгатора та обчислювальних засобів обробки сигналів.

Список використаних джерел:

1. Wilfred E. Noel. Signals of Opportunity Navigation Using Wi-Fi Signal. Thesis. USAF Department of the air force. Air university. Air force institute of technology. Wright-Patterson Air Force Base, Ohio, 2011. URL: https://apps.dtic.mil/sti/tr/pdf/ADA540162.pdf (дата звернення: 24.11.2025).

2. Masud Al Aziz. Navigation for UAVs Using Signals of Opportunity. Submitted to the graduate degree program in partial fulfillment of the requirements for the PhD degree. Department of Electrical Engineering and Computer Science and the Graduate Faculty of the University of Kansas, 2015. URL: https://kuscholarworks.ku.edu/bitstreams/d88f1138-02d6-4616-99d9-b21284ccc8f4/download (дата звернення: 24.11.2025).

УДК 621.317

Іщенко О.С., аспірант
Подчашинський Ю.О., д.т.н., професор
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

КОМП'ЮТЕРИЗОВАНА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНА СИСТЕМА КОНТРОЛЮ РІВНЯ НАФТОПРОДУКТІВ У ЗАЛІЗНИЧНИХ ЦИСТЕРНАХ

Комп'ютеризована інформаційно-вимірювальна система (КІВС)) контролю рівня нафтопродуктів у залізничних цистернах застосовується за необхідності вимірювань великої кількості залізничних цистерн і дає можливість оперативного обліку маси нафтопродуктів у цистернах залізничного складу на будь-якій ділянці колії, у тому числі під контактною електромережею, контроль типу та якості нафтопродуктів без розкриття цистерн, без проведення аналізу в лабораторії. На рис. 1 наведена структурна схема системи [1].

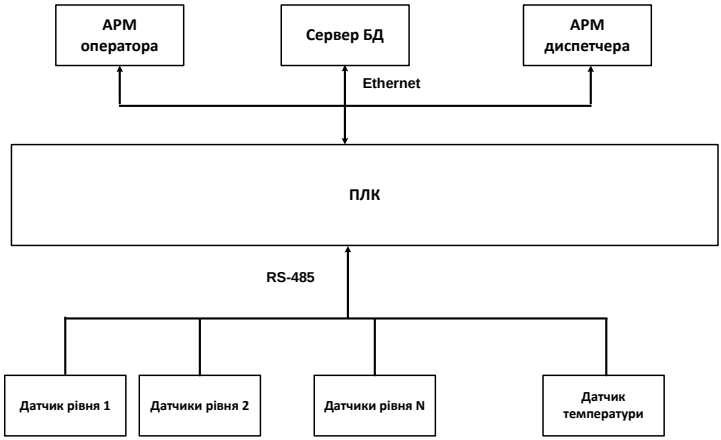


Рисунок 1 – Структурна схема КІВС контролю рівня нафтопродуктів у залізничних цистернах

Для контролю та обліку нафтопродуктів, що перевозяться, формування звіту у відповідності з товарно-транспортною накладною, розроблено програмне забезпечення, яке інсталюється в середовищі ОС Windows комп'ютера.

Перед початком вимірювань у рівнемір Analiq-M від комп'ютера з програми ANALIQ передається список номерів та типів цистерн, які слід виміряти відповідно до накладної (рис. 2).

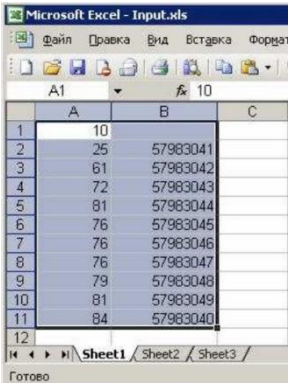


Рисунок 2 – Приклад списку номерів та типів цистерн

В енергонезалежній пам'яті рівнеміра-аналізатора записано понад 100 калібрувальних таблиць залізничних та стаціонарних резервуарів.

Незалежно від версії ПЗ, рівнемір-аналізатор дозволяє проводити групове запам'ятовування всіх даних вимірювань та обчислень з подальшою видачею їх у комп'ютер через RS485/USB.

У звіті відображаються: номер та тип цистерни згідно з накладною, рівень (мм), температура (град С), щільність (г/см^3, 4 знаки після коми), щільність наведена, об'єм (м^3), маса (Т, з точністю до кг.), тип продукту, визначений приладом (А76 Кременчук, Д9ч). підтоварної води (мм). Для суміші пропан-бутану відображається відсоток пропану. Прийняті від рівнеміра-аналізатора ANALIQ-M дані відображаються у форматі Excell.

Список використаних джерел:

1. Безвесільна О.М., Подчашинський Ю.О., Чепюк Л.О., Іщенко О.С. Комп'ютеризована система для вимірювання та контролю якості нафтопродуктів. Збірник матеріалів XXIII Міжнародної науково-технічної конференції «Приладобудування: стан і перспективи», 14 – 15 травня 2024 р., К : ПБФ, НТУУ КПІ ім. Ігоря Сікорського, 2024. 366 с. С. 114-116.

УДК 621.317

Левицький А.В., аспірант
Подчашинський Ю.О., д.т.н., професор
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

МЕТОДИ ТА ЗАСОБИ ВИЗНАЧЕННЯ ТА КОНТРОЛЮ ГЕОМЕТРИЧНИХ ПАРАМЕТРІВ ТРИВИМІРНИХ ОБ'ЄКТІВ ЗА СТЕРЕОЗОБРАЖЕННЯМ

Сучасні інформаційні технології активно використовують тривимірні моделі об’єктів у задачах комп’ютерної графіки, робототехніки, цифрової реконструкції, контролю якості та віртуальної реальності. Визначення геометричних параметрів 3D-об’єктів є ключовою задачею, що дозволяє відтворити форму, розміри та просторове положення предметів за доступними даними. Одним із найбільш доступних та універсальних підходів є методи відновлення тривимірної геометрії за фотографічними проекціями [1,2].

Подібні системи вимагають розробки алгоритмів автоматизованого визначення координат точок, що визначають поверхні об'єктів. Точність визначення координат залежить від характеру завдань, які вирішуватимуться з використанням подібних об'єктів.

Завдання вирішується використанням фотографічних проекцій. Цей спосіб має своєю перевагою практично необмежену роздільну здатність і простоту отримання та введення фотозображень у комп'ютер. Крім цього, в літературі є інформація про оцифровування голографічних зображень, використання лазерних далекомірів.

Завдання полягає в тому, щоб, використовуючи одну або декілька фотографічних проекцій, зроблених під різними кутами або з різних відстаней до об'єкта, визначити просторові координати точок об'єкта. Завдання полягає в тому, щоб, використовуючи одну або декілька фотографічних проекцій, зроблених під різними кутами або з різних відстаней до об'єкта, визначити просторові координати точок об'єкта.

На рис. 1 наведена схема визначення параметрів тривимірного зображення за проекціями.

Одним із найпоширеніших методів ідентифікації є кореляційний.. Кореляційний метод показує хороші результати під час зйомки гладких зображень під малими кутами. Однак, у зв'язку з тим, що даний метод має на увазі велику кількість обчислень, він досить ресурсномісткий.

Метод "квадрат різниці точок" дає гарні результати у задачі поєднання точок на рельєфному зображенні і також дозволяє

здійснювати пошук точок на зображеннях, знятих під досить великими кутами.

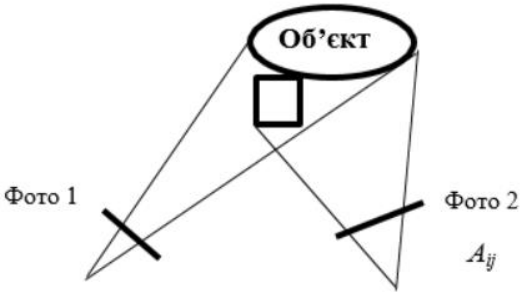


Рисунок 1 – Визначення параметрів тривимірного зображення за проекціями

Метод DCT (використання разом з дискретним косинусним перетворенням) набув поширення в алгоритмах стиснення з втратами, таких як JPEG та MPEG-4. Використання DCT у задачах пошуку точок покращило якість сполучення точок але і збільшило час поєднання точок на порядок

Метод "квадрат різниці матриць" аналізує зображення в розрізі трьох кольорів (R, G, B) (з або без використання DCT), є досить ефективним.

Таким чином, методи визначення геометричних параметрів тривимірних об'єктів на основі фотографічних проекцій залишаються актуальними, оскільки поєднують високу точність, універсальність та доступність обладнання. Подальший розвиток таких систем пов'язаний із покращенням алгоритмів розпізнавання, автоматизацією калібрування та інтеграцією сучасних методів комп'ютерного зору.

Список використаних джерел:

1. Rogers D. F. Procedural Elements for Computer Graphics. — New York: McGraw-Hill, 1997, 711 p.

2. Fundamentals of Computer Graphics by Peter Shirley and Steve Marschner - A + K Peter's, The Limited, Reading, Massachusetts, 2021, 752 p.

УДК 621.317

Лугових О.О., ст. викладач
Державний університет «Житомирська політехніка»

ВИБІР ОПТИМАЛЬНОГО ЗНАЧЕННЯ КОЕФІЦІЄНТА ЕКСПОНЕНЦІАЛЬНОГО ЗГЛАДЖУВАННЯ ДЛЯ ПАРАМЕТРІВ РУХУ ТЕХНОЛОГІЧНОГО ОБЛАДНАННЯ

Для зменшення похибки вимірювань доцільно застосувати метод експоненціального згладжування до виміряних значень координат.

З врахуванням дискретного характеру відеопослідовності маємо послідовність дискретних відліків координати $\{x_i^*\}$, $i=\overline{1,N}$. В цьому випадку найпростішою згладженою оцінкою для математичної моделі є:

$$\hat{x}_i = (1-\xi)x_i^* + \xi f_e(\hat{x}_{i-1}, \hat{x}_{i-2}, \ldots, \hat{x}_{i-s}), \quad (1)$$

де ξ – безрозмірна постійна величина, що є коефіцієнтом експоненційного згладжування, s – глибина пам'яті фільтра згладжування; f_e (.) – функція екстраполяції; x_i*– виміряне поточне значення координати.

В оцінці (1) розраховано екстрапольовано оцінку координати для апріорних моделей руху об'єктів:

– нерухомий стан: $\hat{x}_{ie} = f_e(\hat{x}_{i-1}) = \hat{x}_{i-1}$;

– рівномірний рух; $\hat{x}_{ie} = f_e(\hat{x}_{i-1}, \hat{x}_{i-2}) = 2\hat{x}_{i-1} - \hat{x}_{i-2}$;

– рівноприскорений рух: $\hat{x}_{ie} = f_e(\hat{x}_{i-1}, \hat{x}_{i-2}, \hat{x}_{i-3}) = 3\hat{x}_{i-1} - 3\hat{x}_{i-2} + \hat{x}_{i-3}$.

Важливим питанням є вибір значення коефіцієнта експоненціального згладжування ξ. Згідно формули (1), якщо $\xi \to 0$, то основний вклад в оцінку параметрів руху має поточне вимірювання координати, якщо $\xi \to 1$, то при оцінці враховуються всі попередні вимірювання. В першому випадку експоненціальне згладжування малоефективне, так як дисперсія похибки, тобто похибка оцінки поточних координат не зменшується. В другому випадку при змінах параметрів руху технологічного обладнання виникає динамічна похибка.

Рішення щодо вибору значення ξ може бути знайдено як рішення оптимізаційної задачі та чисельного моделювання оцінок, тобто

$$\sigma_{\sum}^2 \approx \sigma_{ст}^2 + \sigma_{дин}^2 = f(\xi, \sigma_x^2, v) \to \min. \quad (2)$$

Для двох типів обладнання були чисельно прораховані наступні похибки: середньоквадратичне значення похибки визначення поточної

координати у каналі з цифровою відеокамерою; до і після експоненціального згладжування. Результати прорахунків на рис.1.

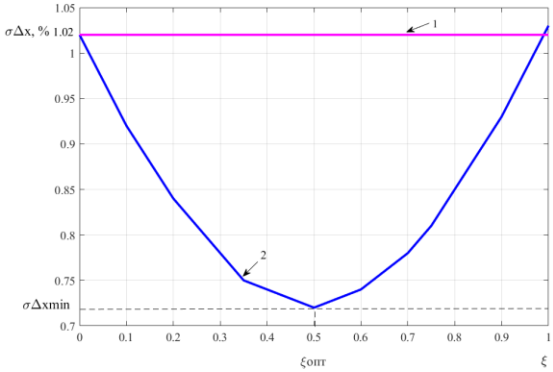


Рисунок 1 – Відносна середньоквадратична похибка визначення поточної координати: 1 – до експоненціального згладжування; 2 – після експоненціального згладжування

Чисельним моделюванням згідно (2) встановлено, що оптимальне значення коефіцієнту згладжування ξ = 0,5. При цьому точність визначення координат за цифровими відеозображеннями підвищено у 1,39 рази.

Цей метод має мінімальну можливу кількість обчислювальних операцій та використовує обмежену фіксовану кількість попередніх результатів вимірювань, що забезпечує підвищення точності визначення параметрів руху в реальному часі.

Список використаних джерел:

1.Турбал Ю. В., Кінда В. В. Аналіз пірамідального методу екстраполяції та моделей експоненційного згладжування для короткострокового прогнозу. Вісник Національного університету водного господарства та природокористування 2020.Вип. 4 (92). С. 165-171.URL: http://nbuv.gov.ua/UJRN/Vnuvgp_tekhn_2020_4_16.

2.Синтез алгоритмів фільтрації результатів вимірювань в системах навігації безпілотних літальних апаратів Зімчук І. В., Шапар Т. М., Ковба М. В. Житомирський військовий інститут імені С.П. Корольова, м. Житомир, Україна. Visnyk NTUU KPI Seriia – Radiotekhnika Radioaparatobuduvannia, 2024, Iss. 96, pp. 21–27.

3.Системологія на транспорті: підручник: у 5 кн./ За заг.ред. М.Ф. Дмитриченка. К.: Знання України, 2005. Кн. ІІ: Технологія наукових досліджень і технічної творчості / Е.В. Гаврилов, М.Ф. Дмитриченко, В.К. Доля та ін.. 318с.

УДК 621.317

Магалецький Я.В., аспірант
Подчашинський Ю.О., д.т.н., професор
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

КОМП'ЮТЕРИЗОВАНА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНА СИСТЕМА КОНТРОЛЮ ПАРАМЕТРІВ ДВИГУНІВ ВІДЦЕНТРОВИХ НАСОСІВ СИСТЕМ ВОДОПОСТАЧАННЯ

При експлуатації насосного обладнання дуже важливо мати оцінку механічних характеристик асинхронних двигунів відцентрових насосів в процесі ремонту або при заміні двигуна. Знання поточних механічних характеристик двигуна електроприводу насосу і відміна їх від його нормативних характеристик надає можливість покращення показників роботи обладнання і отримати економію спожитої електроенергії. На рис. 1 наведена структурна схема комп'ютеризованої інформаційно-вимірювальної системи (КІВС) контролю параметрів двигунів відцентрових насосів систем водопостачання.

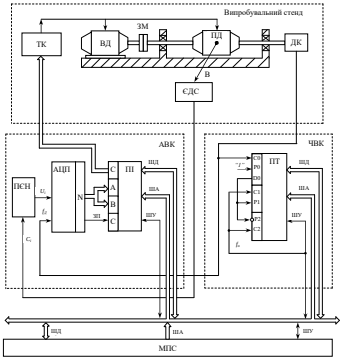


Рисунок 1 – Структурна схема КІВС контролю параметрів двигунів відцентрових насосів систем водопостачання

Вона містить випробувальний стенд (ВС), аналоговий вимірювальний канал (АВК), частотний вимірювальний канал (ЧВК) і мікропроцесорну систему (МПС). ВС складається з двигуна, що випробується (ВД), закріпленого на основі і приводного двигуна (ПД). Датчик кута (ДК) підключений до валу ПД. Вихід ДК підключений до

входу частотно-вимірювального каналу (ЧВК). Через тиристорний комутатор (ТК) виконується управління ПД і ВД.

Блок-схема алгоритму вимірювання пускового моменту асинхронних двигунів наведена на рис. 2, де ΔQ_{ci} – сила опору; α – кут повороту ротора приводного двигуна; k – кількість вимірювань; Q_{ui} – сила, пропорційна пусковому моменту; ΔQ_{ci} і Q_{ui} – середньоарифметичні значення.

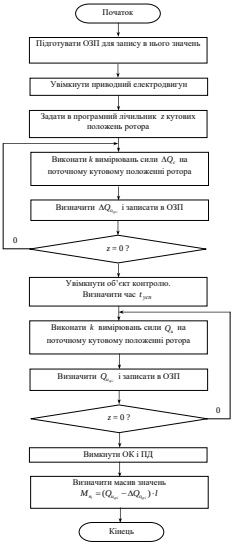


Рисунок 2 – Блок-схема алгоритму вимірювання пускового моменту асинхронних двигунів

Список використаних джерел:

1. Подчашинський , Ю. О., & Магалецький, Я. В. (2024). Аналіз проблематики та розробка структури комп'ютеризованої інформаційно-вимірювальної системи механічних характеристик асинхронного електропривода в насосному обладнанні. Технічна інженерія, (1(93), 295–300.

2. Подчашинський Ю.О., Магалецький Я.В., Чепюк Л.О. Мікропроцесорна система вимірювання пускового моменту електродвигунів відцентрових насосів. Тези XVII МНПК «Інтегровані інтелектуальні робототехнічні комплекси», 21–22 травня 2024 р. Київ: НАУ, 2024. С. 242-244.

УДК 621.317

Свістельник О.С., аспірант
Подчашинський Ю.О., д.т.н., професор
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНА СИСТЕМА КОНТРОЛЮ ПАРАМЕТРІВ МІКРОКЛІМАТУ НА ПОЛІГРАФІЧНОМУ ВИРОБНИЦТВІ

Інформаційно-вимірювальна система (ІВС) контролю параметрів мікроклімату на поліграфічному виробництві виконує роль фундаментального операційного інструменту, що підтримує стабільність технологічних процесів і знижує ризики відхилень, здатних впливати на якість друкованої продукції. Виробниче середовище поліграфії традиційно вважається надзвичайно чутливим до мікроклімату, оскільки властивості паперу, поліграфічних фарб, лаків, клейових композицій та полімерних матеріалів змінюються залежно від температури, вологості та наявності завислих частинок у повітрі. Саме тому надійне, стабільне й методологічно коректне вимірювання цих параметрів завжди було класичним орієнтиром для підприємств, які прагнуть утримувати операційну дисципліну та відповідати закладеним стандартам якості. Система працює на основі послідовного збору первинних сигналів від датчиків різних типів: сенсори температури реєструють тепловий стан повітря, датчики вологості визначають відносний вміст водяної пари, а оптичні або лазерні лічильники частинок пилу фіксують концентрацію мікроскопічних забруднювачів, здатних потрапляти на друкарські форми, папір або елементи машин. Усі ці вхідні параметри формують комплексну телеметрію, яка надходить у блок обробки сигналів, де за проходить через фільтрацію, математичне згладжування, компенсацію похибок та приведення до стандартизованих одиниць, що дозволяє уникнути спотворення результатів і гарантує відповідність класичним методам метрологічної практики [1].

Сенсорний рівень системи працює безперервно, забезпечуючи реальний час роботи та постійний моніторинг навіть за умов динамічних змін технологічного процесу. Датчики вологості, зазвичай побудовані на базі ємнісних або резистивних методів, передають показники з високою стабільністю, дозволяючи виявляти навіть незначні коливання, що можуть вплинути на стан кінцевого виробу. Датчики температури, що використовують платинові терморезистори

типу Pt100 або Pt1000, перетворюють тепловий стан виробничого приміщення на цифрові значення з високою точністю та низькою похибкою. Лазерні сенсори пилу вимірюють концентрацію частинок, що розсіюють світло лазерного променя, таким чином забезпечуючи можливість відстежувати рівень забруднення та контролювати ризики появи точкових дефектів у друкованому шарі. Сигнали з сенсорів надходять у блок обробки, де реалізовано алгоритм фільтрації – рухоме середнє, що забезпечує стабільність даних, виключаючи випадкові піки або шум вимірювань. На цьому ж етапі виконується масштабування та приведення даних до нормативних діапазонів, що дозволяє зіставити фактичні значення з корпоративними або галузевими стандартами, усталеними в поліграфічній сфері.

Синхронізована робота сенсорного рівня і рівня обробки дозволяє підтримувати оптимальний мікроклімат, що є критично важливим для забезпечення стабільної поведінки поліграфічних матеріалів. Папір залишатиметься рівним, не втратить своїх геометричних параметрів і не набуде хвилястості; фарби зберігатимуть свою в'язкість і прогнозований час висихання; обладнання працюватиме у стабільному режимі без зайвого зношування.

На рис. 1 наведена структурна схема ІВС контролю параметрів мікроклімату на поліграфічному виробництві.

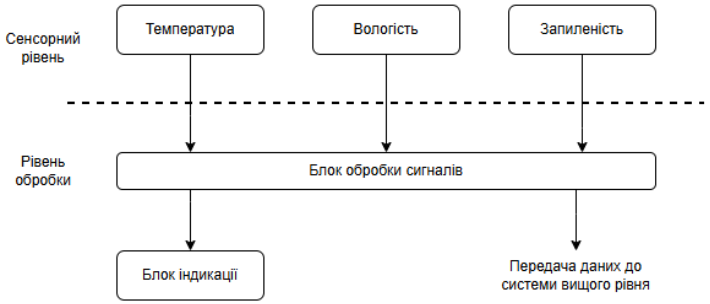


Рисунок 1 – Структурна схема ІВС контролю параметрів мікроклімату на поліграфічному виробництві

Список використаних джерел:

1. Högberg O., Talaskivi M., Ström G. Humidity Effects on Plain Paper in Inkjet Printing // Proc. IS&T Int'l Conf. on Digital Printing Technologies (NIP 17), 2001. P. 874–877. DOI: 10.2352/ISSN.2169-4451.2001.17.1.art00099_2.

УДК 621.317

Ступак А.Г., аспірант
Подчашинський Ю.О., д.т.н., професор
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

ВЕЙВЛЕТ-СТИСНЕННЯ ЗОБРАЖЕНЬ В ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ МЕДИЧНОГО ЗАСТОСУВАННЯ

Застосування вейвлет-перетворення у процедурах стиснення зображень медичного застосування відбувається з деякою втратою частки інформації. Керуючи процедурою стиснення та обираючи її параметри, можливо забезпечити прийнятну похибку відновлення зображень.

Можна розповсюдити вейвлет-перетворення на послідовності більшого розміру. Спочатку перетворюються рядки зображення, а потім – стовпці разом з перетвореними рядками. Програмно розраховується одне і те ж одномірне перетворення, яке також застосовується для перетворення і рядків, і стовпців зображення [1].

Початкове зображення 4×4 (1)

$$\begin{bmatrix} x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \\ x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} \\ x_{4,1} & x_{4,2} & x_{4,3} & x_{4,4} \end{bmatrix} \qquad ((1)$$

яке можна представити як функцію, що задана в одиничному квадраті $\lfloor 0,1 \rfloor \times \lfloor 0,1 \rfloor$:

$$f(x,y) = \sum_{i=1}^{4} \sum_{j=1}^{4} x_{i,j} X_{I_i \times I_j}(x,y) \qquad ((2)$$

Після перетворень, отримуємо

$$f(x,y) = \sum_{i=1}^{4} \sum_{j=1}^{4} x_{i,j} \phi_{2,j-1}(x) \phi_{2,j-1}(y) =$$

$$= \sum_{i=1}^{4} \left\{ \sum_{j=1}^{4} x_{i,j} \phi_{2,j-1}(y) \right\} \phi_{2,j-1}(x) = \sum_{i=1}^{4} \tilde{x}_i(y) \phi_{2,i-1}(x) \qquad 9(3)$$

де

$$\tilde{x}_i(y) = \sum_{j=1}^{4} x_{i,j}\phi_{2,j-1}(y) \qquad ((4)$$

Застосуємо одномірне вейвлет-перетворення для кожного i=1,...,4 у (4). Отримаємо новий набір рівнянь для $\tilde{x}_i(y)$ i=1,...,4, з коефіцієнтами, що є результатом вейвлет-перетворення послідовності $\{x_{i,1},..., x_{i,4}\}$

$$\tilde{x}_i(y) = a^i_{0,0}\phi_{0,0}(y) + d^i_{0,0}\psi_{0,0}(y) + d^i_{1,0}\psi_{1,0}(y) + d^i_{1,1}\psi_{1,1}(y) \qquad ((5)$$

для кожного I=1,...,4. Це еквівалентно застосуванню одномірного вейвлет-перетворення до кожного рядка вихідного зображення (1). Після підстановки (5) назад у (3) і пере упорядкування членів отримаємо

$$f(x,y) = \left\{\sum_{i=1}^{4} a^i_{0,0}\phi_{2,i-1}(x)\right\}\phi_{0,0}(y) + \left\{\sum_{i=1}^{4} d^i_{0,0}\phi_{2,i-1}(x)\right\}\psi_{0,0}(y) + \qquad ((6)$$
$$+ \left\{\sum_{i=1}^{4} d^i_{1,0}\phi_{2,i-1}(x)\right\}\psi_{1,0}(y) + \left\{\sum_{i=1}^{4} d^i_{1,1}\phi_{2,i-1}(x)\right\}\psi_{1,1}(y)$$

Кожна із сум в дужках в (6) знову подібна рівнянню $f(t) = x_1\phi_{2,0}(t) + x_2\phi_{2,1}(t) + x_3\phi_{2,2}(t) + x_4\phi_{2,3}(t)$, і тому одномірне вейвлет-перетворення може бути застосоване до кожного з цих виразі, що еквівалентно застосуванню одномірного вейвлет-перетворення до кожного стовпця вихідного зображення (1).

Таким чином можна обчислювати двомірне вейвлет-перетворення зображення розміром $2^n \times 2^n$, шляхом застосування одномірного вейвлет-перетворення до кожного із 2^n рядків, а потім застосувати одномірне вейвлет-перетворення до кожного із 2^n стовпців. Такий спосіб має перевагу у реалізації, оскільки не потрібно дороблятиі існуюче одномірне перетворення і є ефективним для цілей стиснення відеозображень.

Список використаних джерел:

1. Gonzalez R., Woods R. Digital Image Processing. 4th Edition. Pearson, 2017. – 1192 p.

2. Ступак А.Г., Подчашинський Ю.О., Чепюк Л.О., Левківський О.А. Застосування вейвлет-перетворення до стиснення зображень в інформаційно-вимірювальних системах медичного застосування. Технічна інженерія. 2025. Вип. 1(95). С. 304-311.

УДК 621.317

Товстік С.О., аспірант

Подчашинський Ю.О., д.т.н., професор
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ СЕНСОРІВ ПРОСТОРОВОГО ПОЛОЖЕННЯ ПАНЕЛЕЙ СОНЯЧНОЇ ЕЛЕКТРОСТАНЦІЇ

Сонячна енергетика стрімко розвивається, стаючи дедалі важливішим джерелом відновлюваної енергії. Для максимальної ефективності сонячних електростанцій, як великих промислових, так і невеликих домашніх, потрібні точні та надійні сенсори [1]. Сенсори для сонячних батарей відіграють ключову роль у моніторингу, керуванні та оптимізації роботи цих систем, дозволяючи отримувати максимум енергії від сонячного світла. Розглянемо докладніше типи сенсорів, їх функції, переваги використання та розвитку.

Існує кілька типів сенсорів, які застосовуються у сонячних електростанціях, кожен із яких призначено вимірювання певних параметрів. Вибір конкретного типу сенсора залежить від вимог системи та умов експлуатації.

Піранометри – прилади для виміру сумарної сонячної радіації, тобто енергії сонячного світла, що падає на горизонтальну поверхню і використовуються для визначення загальної кількості сонячної енергії, доступної для перетворення на електрику. Піранометр складається з чорної поверхні, яка поглинає сонячне випромінювання, та термопари, яка вимірює температуру цієї поверхні. Чим більше сонячної енергії поглинається, тим вище температура поверхні і тим більше напруга, що генерується термопарою. Ця напруга пропорційна інтенсивності сонячної радіації.

Піргеометри – прилади для вимірювання довгохвильової (інфрачервоної) радіації, що випускається атмосферою і земною поверхнею і використовуються для визначення теплового балансу системи та оцінки втрат енергії. Піргеометр аналогічний піранометру, але має спеціальний фільтр, який пропускає тільки інфрачервоне випромінювання. Він вимірює температуру поверхні, що поглинає інфрачервоне випромінювання, і генерує напругу, пропорційну інтенсивності випромінювання.

Піргеліометри – прилади для вимірювання прямої сонячної радіації, тобто енергії сонячного світла, що падає поверхню під прямим кутом і використовуються для визначення ефективності фокусуючих сонячних колекторів. Піргеліометр складається з труби з вузьким отвором, через який сонячне світло потрапляє на датчик, який вимірює інтенсивність

прямого сонячного світла, виключаючи розсіяне випромінювання. Піргеліометри зазвичай встановлюються на трекерах, які автоматично відстежують положення Сонця.

Датчики температури використовуються для вимірювання температури сонячних панелей, навколишнього середовища та інших компонентів системи і необхідні для контролю теплового режиму роботи та запобігання перегріву. Існує кілька типів датчиків температури, що використовуються у сонячних електростанціях: термопари (прості та надійні датчики, засновані на ефекті Зеєбека); термістори (напівпровідникові датчики, що змінюють опір в залежності від температури); резистивні термометри опору (RTD, засновані на зміні опору металу в залежності від температури); інтегральні датчики температури (мікросхеми, що містять усі необхідні компоненти для вимірювання та перетворення температури на електричний сигнал).

Розвиток сенсорів для сонячної енергетики йде за кількома напрямками:

– для підвищення точності вимірювань розробляють нові сенсори з більш високою точністю вимірювань, що дозволяє більш ефективно оптимізувати роботу системи.

– зменшення розмірів та вартості: розробляються компактні та недорогі сенсори, які можна використовувати у невеликих сонячних електростанціях.

– інтеграція з бездротовими технологіями: розробляються бездротові сенсори, які спрощують встановлення та підключення до системи керування.

– розробка багатофункціональних сенсорів: розробляються сенсори, які можуть вимірювати кілька параметрів одночасно, що знижує кількість необхідних сенсорів та вартість системи.

– використання штучного інтелекту: розробляються системи управління на основі штучного інтелекту, які можуть аналізувати дані від сенсорів та приймати рішення щодо оптимізації роботи системи в режимі реального часу.

Список використаних джерел:

1. Sri Niwas Singh,Prabhakar Tiwari,Sumit Tiwari Fundamentals and Innovations in Solar Energy **:** Springer **:** 2021, Pages**:** 497, DOI: 10.1007/978-981-33-6456-1/

УДК 621.391

Фабрикатор М.О., *здобувач,*

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Телекомунікаційна система класифікації звукових сигналів для моніторингу та оперативного інформування

Забезпечення оперативного інформування населення у надзвичайних ситуаціях є критично важливим завданням сучасних телекомунікаційних систем. Вимоги до швидкодії, достовірності й персоналізації сповіщень постійно зростають, а традиційні канали, як мобільні сповіщення чи централізовані системи оповіщення, не завжди забезпечують достатній рівень адаптивності. Наприклад, міжнародна система екстрених повідомлень NOAA Weather Radio (США) передає сповіщення широкому загалу, але не враховує індивідуальні характеристики споживачів, чи локальні акустичні події [1]. У ЄС та США активно застосовуються мобільні інфраструктури Cell Broadcast та WEA (Wireless Emergency Alerts), однак їх використання залежить від стану мобільної мережі та роботи зовнішніх серверів [2].

З іншого боку, сучасні дослідження демонструють ефективність штучного інтелекту у виявленні небезпек, аналізі потокових даних та класифікації складних сигналів у системах моніторингу середовища [3; 4]. Окремий напрям становлять акустичні системи ідентифікації - від виявлення пострілів (ShotSpotter), до аналізу шумового фону міст та виявлення дронів [5; 6]. Експерти зазначають, що поєднання телекомунікаційних технологій та алгоритмів глибинного навчання відкриває можливість створення персональних систем раннього оповіщення нового покоління [7].

У дослідженні створено телекомунікаційну систему персонального моніторингу, яка інтегрує дві підсистеми: апаратно-програмний модуль отримання даних з інформаційного простору та нейромережну підсистему ідентифікації звукових сигналів локального середовища. Підхід відповідає сучасним рекомендаціям оптимізації IoT-систем моніторингу, де частина обчислень переноситься на сервер для зменшення навантаження на крайові пристрої [8].

Аналіз звуку виконується в частотній області шляхом побудови Mel-спектрограм, які є одним з найбільш інформативних форматів для задач аудіокласифікації. Кожен аудіосигнал перетворюється у матрицю 128×128, нормалізується та подається на вхід згорткової нейронної мережі. Додатково обчислюється спектральний центроїд, який слугує компактною характеристикою розподілу енергії по частотах та

використовується для підвищення роздільної здатності моделі, що узгоджується з сучасними методами аудіорозпізнавання [9].

Розроблена мережа містить три згорткові шари (32, 64 та 128 фільтрів), два шари максимального пулінгу та повнозв'язний шар з 128 нейронами. Навчання моделі відбувалося у TensorFlow з оптимізатором Adam протягом 20 епох на розмічених даних кількох класів звуків. Для формування вибірки використано стандартний підхід із розбиттям на тренувальний та тестовий набори у пропорції 4:1. У результаті отримано точність ~70% на тестовій вибірці. При аналізі Grad-CAM виявлено, що мережа коректно виділяє ділянки спектрограми, які містять найбільш інформативні частотні компоненти, що свідчить про правильність навчання.

Інтеграція акустичної підсистеми з телекомунікаційним модулем забезпечила можливість комплексного реагування: система визначає зміни у зовнішніх джерелах інформації та появу потенційно небезпечних звукових подій. Тестування підтвердило, що пристрій здатен працювати у режимі безперервного моніторингу, оновлення, ідентифікування, персонального оповіщення користувача.

Отримані результати демонструють перспективність поєднання методів цифрової обробки аудіо сигналів та глибинного навчання у сфері систем безпеки. Запропонований підхід можна масштабувати за рахунок розширення набору класів звуків, інтеграції сенсорних модулів, використання захищених протоколів обміну та підключення до розподілених систем обробки подій.

Список використаних джерел:

1. NOAA Weather Radio. URL: https://www.weather.gov/nwr/
2. European Commission. Public Warning Systems in the EU.
3. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.
4. Abdel-Hamid O. et al. Convolutional Neural Networks for Speech Recognition. IEEE/ACM TASLP, 2014.
5. Meier P. Digital Humanitarians: How Big Data Is Changing Disaster Response. CRC Press, 2015.
6. Shin S. et al. Acoustic-based drone detection. Sensors, 2021.
7. Singh A., Sharma M. AI-based Early Warning Systems. Journal of Safety Science, 2022.
8. Duffy M. Edge–Cloud Architectures for IoT Monitoring. IEEE IoT Journal, 2020.
9. Tzanetakis G., Cook P. Musical genre classification using audio features. IEEE TASLP, 2002.

Секція 7
КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ ТА РОБОТОТЕХНІКА

УДК 004.7

Браташов І. В., магістрант
Ткаленко О.М., к.т.н., доцент
Державний університет інформаційно-комунікаційних технологій

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ IoT НА ПРОМИСЛОВОМУ ПІДПРИЄМСТВІ

Технології Інтернету речей (IoT) стають одним із ключових напрямів розвитку сучасного промислового виробництва. Вони забезпечують взаємодію між обладнанням, сенсорами, комп'ютерними системами та людиною через мережеві інтерфейси. Завдяки цьому з'являється можливість створення єдиного інформаційного простору підприємства, у якому здійснюється автоматичний збір, передавання, аналіз та обробка даних у режимі реального часу. У даній роботі розглянуто практичний приклад впровадження IoT-рішення на базі мікроконтролера Arduino Nano для моніторингу роботи промислових машин. Такий підхід дозволяє організувати централізований контроль обладнання з мінімальними фінансовими витратами, що особливо актуально для малих і середніх підприємств.

Більшість підприємств використовують ручні або частково автоматизовані методи обліку роботи машин, що не забезпечує своєчасного отримання інформації про стан обладнання та ефективність його використання. Це ускладнює планування ремонтів, контроль навантаження та аналіз продуктивності. Постає завдання розробити систему, яка дозволяє відстежувати активність промислових машин у реальному часі, фіксувати періоди роботи та простої, автоматично формувати звіти і зберігати дані для подальшої аналітики. Важливо, щоб така система була доступною, простою у впровадженні, не вимагала значних витрат та могла інтегруватися у вже існуючі виробничі процеси.

Метою дослідження є створення комп'ютерно-інтегрованої IoT-системи для моніторингу роботи промислового обладнання. Основне завдання полягає у розробленні апаратно-програмного комплексу, що забезпечує збір, передавання і збереження даних про роботу машин. Очікуваним результатом є підвищення ефективності виробництва,

мінімізація людських помилок і створення передумов для подальшої автоматизації процесів обліку та управління.

У межах дослідження створено експериментальний зразок системи, яка включає мікроконтролер Arduino Nano, чотири реле для фіксації сигналів від виробничих машин та персональний комп’ютер для збереження й обробки даних.

Обмін інформацією між мікроконтролером і ПК здійснюється через COM-порт, що забезпечує стабільну передачу даних без додаткового мережевого обладнання. Програмне забезпечення розроблено мовою C# у середовищі .NET Framework 4.7.2. Воно автоматично формує щоденні текстові звіти, що містять інформацію про час роботи кожної машини, і дозволяє експортувати дані у формат Excel для подальшого аналізу.

Під час тестування система продемонструвала стабільну роботу, точність фіксації часу та зручність у використанні. Її структура дозволяє легко масштабувати рішення — підключати додаткові датчики, реле або інші пристрої для розширення функціональності.

Запропонована система підтвердила ефективність застосування технологій IoT у виробничому середовищі. Вона дозволяє автоматизувати процес збору даних без значних фінансових вкладень і складної технічної інфраструктури.

Перспективним напрямом подальших досліджень є інтеграція бездротових модулів зв’язку (Wi-Fi, LoRa, Ethernet) для віддаленої передачі даних, створення хмарного сховища, розробка веб-інтерфейсу для відображення стану обладнання в реальному часі та використання алгоритмів машинного навчання для прогнозування поломок і оптимізації графіків технічного обслуговування.

Список використаних джерел:

1. Барановський О. В., Гаврилюк І. С. Інтернет речей у промислових системах: принципи побудови та сфери застосування // Наукові праці ОНАХТ. – 2021. – №1(85). – С. 45–52.

2. Khanna, A., & Kaur, S. (2020). Internet of Things (IoT) in Industrial Automation: A Review. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 9(3), 2278–1323.

3. Arduino Documentation. Arduino Nano Technical Reference. URL: https://docs.arduino.cc/

4. Єрмоленко С. В. Розвиток промислового інтернету речей (IIoT) у контексті автоматизації виробництва // Вісник НТУ 'ХПІ'. – 2022. – №3. – С. 89–94.

УДК: 004.94:621.039.7-026.5

Андрєєв К.В., магістрант
Хом'як Е.А., PhD, ст. викладач
Національний авіакосмічний університет ім. М.Є. Жуковскького «Харківський авіаційний інститут»
Гусєв О.В., здобувач
Таразанов Ю.А., здобувач
Григор'єва Є.С., к.т.н., ст.викладач
Український державний університет залізничного транспорту

МОДЕЛЮВАННЯ СТАНУ ЗАХОРОНЕНИХ ВІТРИФІКОВАНИХ РАДІОАКТИВНИХ ВІДХОДІВ

Захоронення радіоактивних відходів (РАВ) є складним і міждисциплінарним процесом, що охоплює геологію, геохімію, геомеханіку, матеріалознавство та інші особливості. Необхідно охарактеризувати коротко- та довгострокові реакції пов'язаних із означеним процесом труднощів [1].

Критичним питанням є характеристика спричинених пошкоджень або зон з тріщинами на різних етапах захоронення. Моделювання зародження та поширення тріщини за допомогою мультифізичних процесів все ще є актуальною проблемою. Було розроблено різні типи чисельних методів для опису розриву зміщення, пов'язаного з виникненням тріщини [2]. Одним із основних механізмів руйнування є пошкодження, викликане виникненням і поширенням мікротріщин. Макроскопічне руйнування структур найчастіше викликано появою локальних тріщин чи розломів.

Для опису стану захоронених вітрифікованих РАВ було проведено фізико-математичне моделювання процесів, що прогнозуються чи передбачаються у вітрифікованих РАВ. За основу було взято модель, що ґрунтується на законі радіоактивного розпаду [3] і дозволяє прогнозувати зміни в активності радіонуклідів, тому є основою для модуля довгострокового прогнозування:

$$A(t) = A_0 \cdot e^{-\lambda t},$$

де: A(t) – активність у момент часу t, Бк; A_0 – початкова активність, Бк; λ – стала розпаду, $с^{-1}$.

Означена модель дозволяє розрахувати зміни радіаційного навантаження протягом усього періоду зберігання відходів. Для оцінки радіаційної обстановки використовується формула потужності дози:

$$Ḣ = A \cdot Г / r^2,$$

де: Ḣ – потужність еквівалентної дози, Зв/год; А – активність джерела, Бк; Г – гамма-стала радіонукліда, Звм²/(Бкгод); r – відстань від джерела до точки вимірювання, м.

Наведена формула застосовується в алгоритмах автоматичного радіаційного контролю для визначення безпечних відстаней і часу роботи для обслуговуючого персоналу в зоні зберігання вітрифікованих радіоактивних відходів [4]. Тепловиділення було розраховано через загальну потужність:

$$P = \sum A_i \cdot E_{\text{ср}\,i},$$

де: Р – теплова потужність, Вт; Аі – активність і-го радіонукліда, Бк; Еср і – середня енергія розпаду, що перетворюється у теплову, для і-го радіонукліда, Дж/розпад. Для бета й гамма-випромінювачів практично вся енергія перетворюється у теплову. Таким чином забезпечується робота з термомоніторингу, що дозволить прогнозувати різні температурні режими і запобігати термічному пошкодженню скляної матриці. Було розроблено програмне забезпечення для автоматизованого моніторингу стану захоронених вітрифікованих радіоактивних відходів. Статистична обробка даних вимірювань здійснювалась з використанням стандартного відхилення і визначенням похибки середнього значення:

$$\sigma = \sqrt{\Sigma\,(x_i - \mu)^2/N - 1}\,, \Delta\mu = \sigma/\sqrt{N}$$

де: μ – вибіркове середнє значення; хі – і-те вимірювання; N – кількість вимірювань; σ – стандартне відхилення; Δμ – стандартна похибка середнього значення.

Дані статистичні формули складають основу модуля обробки експериментальних даних, оскільки дозволяють забезпечити достовірність результатів вимірювань і подальше автоматичне виявлення аномалій.

Список використаних джерел:

1. Shao J., Yu Zh., Vu M.-N. Multiscale modeling of thermo-hydromechanical behavior of clayey rocks and application to geological disposal of radioactive waste. Journal of Rock Mechanics and Geotechnical Engineering, 2025. Vol. 17, Iss 1. Pp. 1–19. https://doi.org/10.1016/j.jrmge.2024.11.008

2. Morita N. Chapter 2 – Finite element methods. Finite Element Programming in Nonlinear Geomechanics and Transient Flow, 2021. https://doi.org/10.1016/B978-0-323-91112-2.00004-5

3. «Слідами CHORNOBYL»: навч. посіб. до циклу уроків освітнього проекту «Слідами Chornobyl» / Мінакова К.О., Петров С.О., Радогуз С.А., Сокол Є.І., Томашевський Р.С., Лазуренко О.П., Сінческул О.Л., Лаврова І.О., Шестопалов О.В., Ільїнська О.І., Зайцев Р.В. – Харків: НТУ «ХПІ», 2019. 112 с.

УДК 621.311:621.316.9

Раданович В. Я., здобувач
Добржанський О.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

ПРОБЛЕМНІ ПИТАННЯ ВИКОНАННЯ РЕЛЕЙНОГО ЗАХИСТУ НА ВИСОКІЙ ТА НИЗЬКІЙ НАПРУЗІ

Проблема забезпечення надійної та селективної роботи релейного захисту є однією з ключових у сучасній електроенергетиці, оскільки від неї безпосередньо залежить стабільність енергосистем, безпека експлуатації та збереження обладнання на різних рівнях напруги. Попри активний розвиток мікропроцесорних технологій, релейний захист і надалі стикається з низкою технічних та експлуатаційних викликів.

У мережах високої напруги (110 кВ і вище) основними проблемами залишаються забезпечення швидкодії, селективності та стійкої роботи захисту в умовах складних аварійних процесів. Під час коротких замикань у таких системах виникають аперіодичні складові струму, зміна опору дуги та взаємний вплив паралельних ліній, що ускладнює визначення місця пошкодження, особливо для дистанційних захистів. Для забезпечення точності та стабільності спрацювання необхідне вдосконалення алгоритмів цифрової фільтрації й вимірювання імпедансу, які здатні функціонувати в динамічних режимах енергосистеми. Додатковою складністю є зростання частки розподіленої генерації, що змінює напрямки та рівні струмів короткого замикання, порушуючи узгодженість традиційних схем. Одним із практичних шляхів вирішення цієї проблеми є впровадження адаптивних систем релейного захисту, які автоматично коригують уставки та режими роботи залежно від поточного стану мережі. Такі системи здатні забезпечити ефективну дію автоматики повторного включення, що мінімізує ризик розвитку каскадних аварій і підвищує загальну стійкість енергосистеми.

У мережах низької напруги проблематика має інший характер і пов'язана передусім із низькими струмами коротких замикань, перевантаженнями та виникненням дугових процесів. Значний опір петлі «фаза–нуль» часто призводить до того, що струм замикання не перевищує уставки автоматичних вимикачів, через що вони не спрацьовують своєчасно. Це створює небезпеку займання, пошкодження ізоляції та ураження людей електричним струмом. Для підвищення ефективності в таких мережах широко застосовуються пристрої захисного відключення (ПЗВ), диференційні системи та дугові детектори, які реагують на відхилення форми струму та швидкість зміни

параметрів. Однак поширення систем дугового захисту обмежується високою вартістю, складністю налаштування та ймовірністю хибних спрацювань, зумовлених імпульсними перешкодами.

Для систем високої напруги найбільш перспективним напрямом є впровадження адаптивних та інтелектуальних релейних пристроїв, які функціонують на основі цифрових протоколів (зокрема IEC 61850) і використовують аналітичні алгоритми для визначення місця пошкодження. Для мереж низької напруги важливим напрямом розвитку є підвищення чутливості та завадостійкості пристроїв, розширення функцій ПЗВ і дугового захисту, що дає змогу запобігати аваріям і підвищити рівень електробезпеки.

Реалізація комплексної, ієрархічно узгодженої системи релейного захисту, що охоплює як високовольтні, так і низьковольтні рівні, є ключовим чинником підвищення ефективності та стабільності електроенергетичних мереж. Її практична реалізація ґрунтується на впровадженні цифрових технологій, адаптивних алгоритмів і сучасних комунікаційних протоколів, які забезпечують узгоджену взаємодію між усіма рівнями захисту. Інтелектуальні системи релейного захисту, здатні до самоналаштування та аналізу поточного стану мережі в реальному часі. Використання сучасних ПЗВ, диференційного та дугового захисту з розширеними функціональними можливостями дозволяє забезпечити ефективне виявлення небезпечних струмів, уникнути перегрівів і попередити виникнення пожеж. Упровадження таких рішень сприяє формуванню гнучких, технологічно розвинених електроенергетичних систем, здатних забезпечити безперервну селективність, високу швидкодію та надійність роботи захисту.

Список використаних джерел:

1. Voltage Protection Relay: Working Principle and Functions [Електронний ресурс]. - Режим доступу: https://www.iqytechnicalcollege.com/Scada_%20Supervisory%20Control%20And%20Data%20Acquisition.pdfhttps://www.chintglobal.com/global/en/about-us/news-center/blog/voltage-protection-relay.html

2. Д.П. Козярський, Е.В. Майструк, І.П. Козярський // Посібник – «Основи релейного захисту та автоматизації енергосистем», 2019.

УДК 004.45

Шельпяков В.Ю., спеціаліст вищої категорії, викладач
ВСП «Глухівський агротехнічний фаховий коледж Сумського НАУ»

ЗАСОБИ OPEN HARDWARE ТА OPEN SOURCE В НАУКОВІЙ ДІЯЛЬНОСТІ

Активний розвиток науки відбувається завдяки впровадженню інформаційно-комунікаційних технологій (ІКТ), які забезпечують ефективну роботу з інформацією, автоматизацію етапів наукових досліджень, створення інноваційних моделей та продуктів.

Під поняттям «інформаційні технології» зібрано сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів. Застарілі методи та засоби навчання не відповідають нинішнім вимогам і не підлягають тенденціям стрімкого розвитку науково-технічного прогресу, що спонукає до впровадження інноваційних методів, з їх подальшим використанням та адаптуванням в навчальний процес.

Важливим напрямком цифровізації наукової діяльності є використання апаратно-програмних платформ відкритого коду (АППВК), за допомогою яких можна створювати експериментальні прилади, здійснювати моніторинг параметрів технологічних процесів та навколишнього середовища, проводити моделювання та тестування інноваційних розробок. Як науковий інструмент АППВК охоплює технічні засоби та програмне забезпечення, вихідні схеми та коди яких є відкритими для науковців та здобувачів освіти і сприяють вільному доступу до розробок, обміну досвідом за принципами Open Source і Open Hardware.

Апаратно-програмні платформи надають можливості створювати низьковартісні лабораторні установки для вимірювання фізичних, хімічних або біологічних параметрів, здійснювати автоматизований збір і обробку експериментальних даних, розробляти інтерактивні системи управління та контролю, реалізовувати інноваційні освітні проєкти. Відкриті платформи – такі як Arduino, Raspberry Pi та Fritzing – поєднують електронні системи, комунікативні технології та програмування в єдине інтегроване середовище завдяки своїй доступності та гнучкості.

Апаратна платформа Arduino, яка складається з мікроконтролера та середовища програмування, є універсальним інструментом для реалізації освітніх інновацій, оскільки надає змогу реалізовувати

наукові ідеї через прототипи нових пристроїв з можливістю автоматизації процесів керування.

Міні-комп'ютер Raspberry Pi вважається більш продуктивною апаратною платформою, коли обробка та комплексний аналіз даних здійснюється у реальному часі. Він має вищу обчислювальну потужність та повноцінне програмне забезпечення. Raspberry Pi володіє вбудованою підтримкою технологій машинного навчання та штучного інтелекту, що дозволяє реалізовувати складні аналітичні завдання без використання зовнішніх ресурсів. Платформа сумісна з потужними мовами програмування, такими як Java, C++, Python, а також інтегрується з новітніми версіями пакету прикладних програм Matlab, забезпечуючи гнучкість у розробці алгоритмів і візуалізації результатів.

Для моделювання електронних схем та ефективної візуалізації проєктів на базі платформ Arduino та Raspberry Pi рекомендовано до використання спеціалізоване програмне середовище Fritzing. Такий інструмент надає можливість здійснювати попередню перевірку ідей технічної направленості ще до створення пристроїв, мінімізуючи як ризики, так і витрати. Fritzing значно спрощує процес документування результатів експериментів та розробок, дозволяє створювати професійні схеми та макети PCB-плат.

Використання апаратно-програмних платформ відкритого коду – один із чинників формування сучасної культури відкритої науки. Завдяки принципам Open Source та Open Hardware, АППВК створюють умови для вільного обміну досвідом, науковими ідеями та результатами досліджень між інженерами, науковцями, студентами в усьому світі.

Описані платформи є інструментами для практичного навчання і дослідницької діяльності в багатьох технічних галузях: електроніці, робототехніці та мехатроніці – для вивчення принципів роботи з мікроконтролерами, сенсорами, системами керування рухами та навігацією; у телекомунікаціях – для реалізації безпровідної передачі даних; в системному і прикладному програмуванні – при написанні та тестуванні коду для взаємодії з мікроархітектурою електронних систем.

Список використаних джерел:

1. Інформаційно-комунікаційні технології в освіті: словник. Київ : ТОВ «ЦП «КОМПРИНТ», 2019. 134 с.

2. Могильний С.Б. Мікрокомп'ютер Raspberry Pi – інструмент дослідника: посібник. Київ : «Талком», 2014. 340 с.

3. Сучасні інформаційно-комунікаційні технології: Навчальний посібник / Швачич Г.Г. та ін. Дніпро : НМетАУ, 2017. 230 с.

УДК 681.5

Раданович В. Я., здобувач
Добржанський О.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЕНЕРГОЕФЕКТИВНІ СИСТЕМИ КЕРУВАННЯ МІКРОРОБОТАМИ НА ОСНОВІ НЕЙРОМОРФНИХ ТЕХНОЛОГІЙ

Нейроморфні обчислення є перспективним напрямом для підвищення енергоефективності керування автономними мікророботами. Їхня ключова ідея полягає у використанні спайкових нейронних мереж, що працюють за принципом мозку та активуються лише за наявності події. Це дозволяє суттєво зменшити споживання енергії та забезпечити швидку реакцію системи навіть за обмежених ресурсів живлення. Нейроморфні чіпи, такі як Intel Loihi, IBM TrueNorth і SpiNNaker, демонструють значно менші затрати енергії порівняно з традиційними процесорами, що робить їх придатними для задач реального часу – навігації, аналізу сенсорних даних та уникнення перешкод.

Подійно-орієнтований принцип роботи також дозволяє більш ефективно обробляти інформацію від сенсорів, особливо якщо дані надходять нерівномірно або в умовах шумів. Разом з тим існують певні труднощі впровадження таких систем — зокрема, нестандартні інструменти розробки, складність навчання спайкових мереж та обмежений вибір апаратних платформ.

Незважаючи на ці виклики, нейроморфні технології мають значний потенціал для створення більш автономних, легких і енергоощадних мікророботів. Подальші дослідження у напрямі апаратно-програмної інтеграції та вдосконалення алгоритмів навчання можуть зробити такі системи стандартом у майбутніх робототехнічних застосуваннях.

Список використаних джерел:

1. Energy-Efficient Neuromorphic Chips for Real-Time Robotic Control: A Review[Електронний ресурс]. - Режим доступу: https://www.researchgate.net/publication/395248441_EnergyEfficient_Neuromorphic_Chips_for_eal-Time_Robotic_Control_A_Review

2. Reinforcement co-Learning of Deep and Spiking Neural Networks for Energy-Efficient Mapless Navigation with Neuromorphic Hardware[Електронний ресурс].- Режим доступу: https://arxiv.org/abs/2003.01157

УДК 621.313.333

Безвесільна О.М., д.т.н., професор
Ткачук А.Г., к.т.н, доцент
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Державний університет «Житомирська політехніка»

МОДЕЛЮВАННЯ ЦИФРОВОГО ДВІЙНИКА ЕЛЕКТРОПРИВОДА СТАБІЛІЗАТОРА ОЗБРОЄННЯ ДЛЯ АНАЛІЗУ ЕНЕРГОСПОЖИВАННЯ ТА ДІАГНОСТИКИ НЕСПРАВНОСТЕЙ

Сучасні системи стабілізації озброєння вимагають високої точності та швидкодії електроприводів, адже саме вони відповідають за стабільне наведення гармати або оптико-прицільного блока під час руху бойової техніки. Робота таких систем відбувається у складних умовах під впливом вібрацій, механічних ударів, температурних коливань і сильних електромагнітних полів. Унаслідок цього електромеханічні вузли піддаються комплексним динамічним навантаженням, що поступово спричиняє деградацію характеристик, зниження енергоефективності та підвищення ймовірності відмови у критичних ситуаціях [1-2].

Традиційні методи технічного контролю не забезпечують своєчасного виявлення прихованих дефектів, адже базуються переважно на планових оглядах або реагуванні після появи несправності. На відміну від цього, концепція цифрового двійника передбачає створення математичної моделі електропривода, яка відтворює його фізичну поведінку у режимі реального часу та дозволяє аналізувати внутрішні процеси без втручання у роботу реального пристрою.

Таке моделювання відкриває можливості для оцінювання енергоспоживання, прогнозування зносу та розроблення систем технічного обслуговування за станом. Крім того, цифрові двійники сприяють перевірці нових алгоритмів керування і зменшують ризики під час експериментів із бойовими системами.

Розвиток цієї технології особливо важливий для оборонної мехатроніки, де поєднуються електромеханіка, автоматизація, аналітика великих даних та елементи штучного інтелекту. Створення цифрового двійника електропривода стабілізатора озброєння дозволяє підвищити надійність, передбачуваність і довговічність системи загалом, забезпечуючи при цьому ефективніше використання

енергоресурсів і скорочення часу простоїв під час експлуатації військової техніки [1-3].

У середовищі MATLAB/Simulink реалізовано модель електропривода з урахуванням нелінійностей двигуна постійного струму, інерційних характеристик механізму наведення та ПІД-регулятора, налаштованого на оптимальні перехідні процеси. Для забезпечення зворотного зв'язку між цифровим двійником і фізичним об'єктом використано сенсорні дані струму, напруги та температури, що надходять від контролера типу STM32 через інтерфейс IoT-модуля MQTT. Система підтримує обмін даними у реальному часі та дозволяє створювати базу сценаріїв для аналізу різних режимів роботи.

Розроблений цифровий двійник дозволяє аналізувати миттєве енергоспоживання та визначати оптимальні режими живлення, виявляти відхилення у характеристиках струму й моменту, прогнозувати стан електропривода за допомогою алгоритмів машинного навчання, а також формувати рекомендації для технічного обслуговування за станом (Condition-Based Maintenance). Застосування цифрового двійника дає змогу знизити ризики відмови системи стабілізації до 30 % та підвищити ефективність енергоспоживання до 12%.

Створення цифрових двійників електроприводів стабілізаторів озброєння є перспективним напрямом розвитку оборонної галузі. Такі системи підвищують надійність та передбачуваність роботи складних електромеханічних комплексів. Подальші дослідження спрямовано на інтеграцію нейронних мереж для автоматичного виявлення відмов і розширення моделі до рівня цифрового двійника всього стабілізатора.

Список використаних джерел:

1. Бойова машина піхоти БМП-2. Загальна будова: навчальний посібник / В.В. Близнюк, В.Б. Добровольський, Д.В. Зайцев – К.: ВД «СКІФ». 2022. – 212 с.

2. Дії механізованого відділення при озброєнні бойової машини піхоти БМП-2: навчальний посібник / Д.В. Зайцев, В.Б. Добровольський, О.С. Дем'янюк, А.П. Наконечний – К.: ВД «СКІФ». 2022. – 120 с.

3. Ткачук А.Г., Безвесільна О.М., Гуменюк А.А., Янчук В.М., Крижанівська І.В. «Дослідження основних напрямів розвитку сучасної системи стабілізації озброєння». Технічна інженерія, 2020, № 2 (86), с. 73-80. DOI: 10.26642/ten-2020-2(86)-73-80.

УДК 004.056.53

Марченко К.Л., здобувач
Ткачук Д.Ю., аспірантка
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ КАМЕР ДЛЯ КОНТРОЛЮ ЯКОСТІ ПРОДУКЦІЇ У ВИРОБНИЦТВІ

Використання промислових відеокамер у системах контролю якості продукції є одним із ключових напрямів цифрової трансформації сучасних виробництв. Камери виступають базовими сенсорами, що забезпечують безперервний збір візуальних даних про об'єкти, які рухаються конвеєрними лініями, тоді як алгоритми обробки зображень та методи машинного навчання виконують функції «аналітичного ядра», формуючи рішення щодо придатності виробу. На відміну від традиційного візуального контролю, що покладається на оператора, автоматизовані системи машинного зору забезпечують відтворюваність результатів, високу швидкість перевірки та мінімізацію впливу людського фактора, що є критично важливим для серійного та масового виробництва.

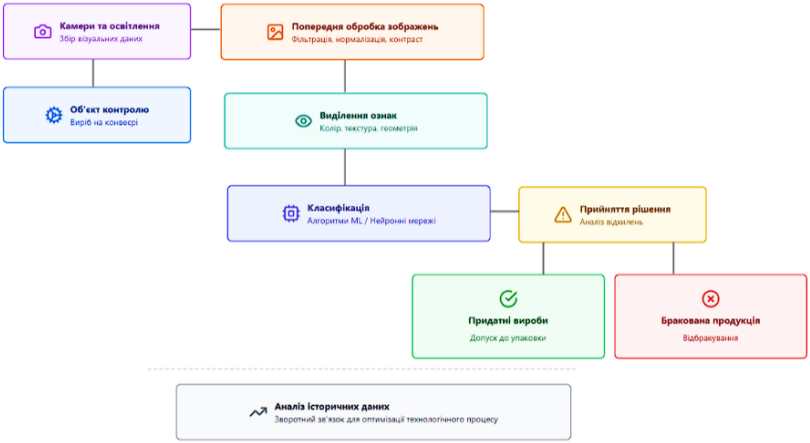


Рисунок 1 – Структурна схема системи контролю якості на основі машинного зору

У складних промислових процесах типові дефекти поверхні: отвори, тріщини, подряпини, відколи, порушення геометрії крайок, нерівномірність покриття безпосередньо впливають на надійність та довговічність виробів, а також призводять до зростання витрат на переробку й рекламації. Впровадження систем контролю на основі

камер дозволяє автоматизувати виявлення таких дефектів у режимі реального часу. Типова архітектура системи включає: підсистему освітлення та відеокамер, модуль попередньої обробки зображень (фільтрація шумів, нормалізація яскравості, підвищення контрасту), модуль сегментації та виділення ознак (колір, текстура, геометричні параметри), класифікатор (традиційні алгоритми або нейронні мережі) та модуль прийняття рішень, інтегрований із промисловим контролером. Завдяки такій структурі забезпечується можливість стабільного виявлення відхилень навіть за змінних умов освітлення, швидкості конвеєра чи варіацій сировини.

Після навчання алгоритмів машинного зору на еталонних зразках система порівнює поточні зображення виробів із допустимими шаблонами та в разі виявлення відхилень за кольором, формою, розмірами або текстурою формує сигнал на промисловий контролер для автоматичного відбракування продукції. Відбракування реалізується за допомогою пневматичних або роботизованих механізмів, потоків стисненого повітря чи інформування оператора, що забезпечує автоматизоване сортування за класами якості, контроль маркування, упаковування та повноти комплектації. Важливою складовою таких систем є накопичення й аналіз історичних даних про дефекти, що дає змогу виявляти технологічні тенденції, пов'язані з сировиною, режимами роботи обладнання або налаштуваннями лінії, та коригувати виробничі параметри. Таким чином, системи машинного зору виконують не лише функцію оперативного контролю якості, а й роль аналітичного інструменту для довгострокової оптимізації виробництва. Інтеграція відеосистем з промисловою автоматикою та аналітикою даних підвищує стабільність якості, знижує рівень браку й витрати на переробку та формує технічну основу для створення адаптивних «розумних» виробничих ліній.

Список використаних джерел:

1. Машинний зір – перехід від Індустрії 4.0 до Індустрії 5.0 URL: https://www.mdpi.com/2076-3417/14/4/1471#B13-applsci-14-01471

2. Використання машинного зору для виявлення та запобігання дефектам у виробництві URL: https://emergentvisiontec.com/applications/inspection-and-automation/defect-detection-and-prevention/

УДК 004.4:003.26:681.326.3

Омельчук І.А., викладач
Пількевич І.А., д-р.техн.наук, професор
Мірошніченко С.І., викладач
Житомирський військовий інститут ім. С.П. Корольова

МЕТОДИ МАТЕМАТИЧНОГО ПРОГНОЗУВАННЯ ДЛЯ ВИКОРИСТАННЯ В СИСТЕМАХ УПРАВЛІННЯ РОБОТИЗОВАНИМИ КОМПЛЕКСАМИ

Інтенсивний розвиток сучасних вимірювальних та інформаційних систем дозволяють автоматизувати і дистанціювати процеси управління різноманітними об'єктами. То ж XXI сторіччя принесло людству чергову технологічну революцію. Мікроконтролери, смартфони, системи передачі даних, стрімкий розвиток інформаційних мереж істотним чином змінив буття кожної країни та родини. За минулі 10-15 років в провідних країнах світу почали інтенсивно з'являтися різноманітні зразки роботизованих комплексів наземного базування або в обмеженому розумінні UGV (unmanned ground vehicles), що стало результатом розвитку сучасних інформаційно вимірювальних технологій. Роботизовані системи широко впроваджуються і в військовому напрямку. Значна потреба ширшого використання роботизованих систем присутня в сухопутних військах, які є найбільш «контактними» (перебувають у постійній бойовій взаємодії з військовими підрозділами супротивника) і при цьому зазнають найбільш відчутних втрат у військових діях. Розвиток сучасних військових технологій зумовлює стрімке впровадження в практику ведення бойових дій широкого спектру наземних дистанційно керованих систем різноманітного призначення, однак висвітлення проблеми автоматизації процесів керування цими комплексами шляхом функціонування мобільних роботів на рівнях управління оператором, та адаптації їх до умов бойового застосування безпосередньо в місцях виконання ними поставлених задач.

Останнім часом з'явилося кілька потужних світових шкіл та проектів щодо розробки та впровадження автоматичних систем та їх складових.

Також багато наукових закладів військового та цивільного спрямування працюють над розробкою та вдосконаленням наземних роботизованих комплексів [1], їх тягових і маневрових характеристик [2], розробці систем керування рухомими апаратами [3].

Метою даної роботи є розробка та впровадження алгоритму системи стабілізації курсової стійкості наземних роботизованих комплексів. В основу алгоритму покладено аналізування значення відцентрових сил та побудову лінії прогнозного тренду щодо їх поведінки. На основі цих даних проводиться програмний аналіз стабільності траєкторії, або обирається варіант реагування на поведінку колісного агрегату на зміну траєкторії, що були спричинені характеристиками дорожнього покриття чи рельєфу.

Також маючи результати замірів сил реакції рухомого агрегату на початку маневру є можливість побудувати лінію тренду для даного конкретного моменту руху з прогнозуванням розвитку подій. Отже маючи масив замірів на початку маневру можна математично зпрогнозувати розвиток події та поведінку рухомого апарата [4].

Математичний апарат та методика прогнозування розвитку сил реакції під час виконання маневру, що пропонується побудовано на основі статистичної обробки даних вимірювання відцентрових сил що діють на рухомий апарат.

На сьогоднішній день методи статистичного моделювання широко використовуються в економічних розрахунках та прогнозах [5]. Враховуючи, що використання вимірювань під час руху рухомого агрегату є циклічним, результати вимірювань отримані під час руху можуть бути розглянуті як дискретний стохастичний часовий ряд з певним кроком. Виміряні значення сил що діють на апарат який рухається постійно змінюються, відповідно часовий ряд в умовах конкретної дорожньої обстановки також є різним і визначає поведінку рухомого об'єкту в конкретний момент часу. Очевидно, що для кожного відрізку шляху, і маневру цей ряд є індивідуальним.

Як вказано в [5], експонентну середню S_t можна виразити через значення часового ряду x

$$S_t = \alpha x_t + \beta S_{t-1} = \alpha x_t + \alpha\beta x_{t-1} + \beta^2 S_{t-2} = \ldots =$$
$$= \alpha x_t + \alpha\beta x_{t-1} + \alpha\beta^2 x_{t-2} + \ldots + \alpha\beta^l x_{t-i} + \ldots + \beta^N S_0 = \alpha\sum_{i=0}^{N-l}\beta^l x_{t-i} + \beta^N S_0, \quad (1)$$

де $N-$ кількість членів ряду; S_0 – деяка величина, що характеризує початкові умови для першого застосування формули при $t = 1$; α – параметр згладжування, $\alpha = \text{const}, 0 \le \alpha \le 1; \beta = 1 - \alpha$.

Отже,

$$S_t = \alpha\sum_{i=0}^{\infty}\beta^i x_{i-t} \cdot \quad (2)$$

Таким чином, величина S_t є зваженою сумою всіх членів ряду. Причому вага падає експоненційно залежно від давнини (віку)

спостереження. Це й пояснює, чому величина S_t названа експонентною середньою.

Отже, використовуючи дану математичну модель можна з великим ступенем імовірності зпрогнозувати розвиток сил реакції що діятимуть на наземний комплекс при виконанні маневру в конкретних умовах, і застосувати завчасно дії, щодо коригування курсу рухомого агрегату.

Такими діями може бути або швидка коригуюча зміна положення керованих коліс, або коригуванням курсової стійкості динамічним способом [5].

Висновки. Використовуючи запропонований метод можна значно покращити тактико технічні характеристики наземних рухомих роботизованих комплексів.

Також, використовуючи математичне прогнозування, та застосування коригуючих керувальних дій завчасно, є можливість підвищити швидкість виконання маневрів, що значно ускладнить виявлення та ураження комплексу на полі бою, і дасть змогу підняти його показники живучості.

Список використаних джерел:

1. Перспективи використання мобільних роботизованих комплексів в широкому спектрі вирішення задач мілітарного спрямування / Зінько Р. В., Ванкевич П. І., Черненко А. Д. та ін. // Збірник наукових праць Військової академії. Одеса, 2018. Вип. № 1 (9). С. 17–27. URL:http://zbirnyk.vaodessa.org.ua/images/zbirnyk_9/03.pdf

2. Грубель М. Г., Крайник Л. В., Боднар М. Ф. Оцінка тягово-швидкісних характеристик військової автомобільної техніки за умов руху бездоріжжям методами імітаційного моделювання // Озброєння та військова техніка, 2019. № 3. С. 46–52. URL: http://nbuv.gov.ua/UJRN/ovt_2019_3_6 (дата звернення: 05.11.2024).

3. Папуша Д., Чепюк Л. Автоматизована система управління рухом робота для дослідження небезпечних приміщень // Комп'ютерні технології: інновації, проблеми, рішення – 2017 : тези доп. II Міжнар. наук.-техн. конф. URL: https://conf.ztu.edu.ua/wp-content/uploads/2017/11/154.pdf (дата звернення: 05.11.2025).

4. Бобошко О. А. Наукові основи підвищення показників маневреності автомобілів: дис. на здобуття ступеня доктора технічних наук за спец. 05.22.02 – Автомобілі і трактори / Харківський нац. автомобільно-дорожній університет. Харків, 2019. 332 с. URL:https://uacademic.info/ua/document/0519U001087

5. Бідюк П. І. Ймовірнісно-статистичні методи моделювання і прогнозування : [монографія] / П. І. Бідюк, О. П. Гожий. – Миколаїв : Чорноморський державний університет ім. Петра Могили, 2014. – 440 с. URL:https://dspace.chmnu.edu.ua/jspui/bitstream.pdf

УДК 621.311.22:621.316.925:681.5

Бєляк П.Л., здобувач
Ткачук А.Г., к.т.н, доцент
Янчук В.М., к.т.н, доцент
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ ГІБРИДНИХ НЕЙРОННО-ФІЗИЧНИХ МОДЕЛЕЙ ДЛЯ ОПТИМІЗАЦІЇ РЕГУЛЮВАННЯ НАПРУГИ В ЕНЕРГОСИСТЕМАХ

Стабільність напруги є одним із ключових чинників надійності функціонування сучасних енергосистем. Зростання частки відновлюваних джерел енергії (ВДЕ), розвиток мікромереж, а також поява децентралізованих систем генерації змінюють характер електричних мереж, роблячи їх більш динамічними та складними для традиційного керування. Коливання потужності вітрових і сонячних установок, а також нерівномірне навантаження у промислових і побутових споживачів призводять до нестабільності рівня напруги, збільшення втрат та зниження якості електроенергії. Класичні регулятори напруги (типу ПІ або ПІД) орієнтовані на лінійні або квазістатичні режими роботи, тому не завжди здатні адекватно реагувати на швидкі нелінійні зміни параметрів системи. Їхня ефективність знижується в умовах стохастичних флуктуацій напруги, гармонічних спотворень або раптових змін навантаження. Сучасні підходи до автоматизованого регулювання напруги потребують моделей, здатних одночасно враховувати фізичні закономірності електромагнітних процесів і адаптуватися до непередбачуваної поведінки елементів мережі.

У цьому контексті перспективними є гібридні нейронно-фізичні моделі (Physics-Informed Neural Networks, PINN), які поєднують аналітичні рівняння стану електричної мережі з нейронними мережами, що навчаються на емпіричних даних. Такі моделі дозволяють уникнути повної заміни фізичних законів статистичними підходами та зберегти інтерпретованість результатів. Їхнє застосування відкриває можливості для реалізації адаптивного регулювання напруги з урахуванням часових змін у споживанні, погодних факторів, топології мережі та динаміки генерації ВДЕ (рис. 1).

Додатковою перевагою є здатність PINN-моделей виконувати прогнозування короткочасних відхилень напруги, що створює підґрунтя для розроблення прогнозно-адаптивних систем керування (Predictive Control Systems). Це дозволяє зменшити кількість аварійних спрацювань, підвищити стабільність режимів роботи станцій і мінімізувати реактивні втрати.

Особливої актуальності ця тематика набуває в умовах цифрової трансформації енергетики України, коли електричні станції переходять до інтеграції в інтелектуальні мережі Smart Grid та використовують елементи цифрових двійників для моніторингу й керування. Гібридні нейронно-фізичні моделі можуть стати основою для побудови таких цифрових двійників енергетичних об'єктів, здатних забезпечити синхронізоване керування генерацією, накопичувачами енергії та споживачами [1-2].

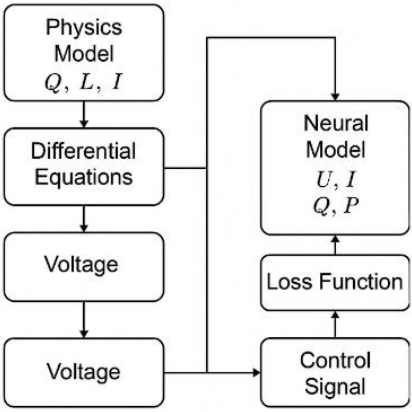


Рис. 1. Структурна схема зв'язку між фізичною та нейронною моделями регулювання напруги

Запропонована гібридна модель продемонструвала на 27 % менше відхилення напруги у перехідних процесах порівняно з класичним ПІ-регулятором. Час встановлення напруги скоротився на 15–20 %, а коефіцієнт стабільності системи зріс до 0,98.

Модель не лише стабілізує напругу, а й забезпечує прогнозне керування за рахунок передбачення змін у навантаженні та генерації. Це дозволяє мінімізувати кількість спрацьовувань регулятора та зменшити втрати енергії в лініях.

Список використаних джерел:

Misyris G. S., Venzke A., Chatzivasileiadis S. «Physics-Informed Neural Networks for Power Systems». arXiv preprint, 2019. Режим доступу: https://arxiv.org/pdf/1911.03737.pdf

Lal D. K. «Combined load-frequency and terminal voltage control of power system using FOPID controller». Journal of Electrical Systems and Information Technology, 2019. Режим доступу: https://jesit.springeropen.com/articles/10.1186/s43067-019-0010-3

УДК 004.932

Тарасюк Д.В., здобувач
Ткачук Д.Ю., аспірантка
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ КОМП’ЮТЕРНОГО ЗОРУ ДЛЯ МОНІТОРИНГУ СТАНУ СІЛЬСЬКОГОСПОДАРСЬКИХ ПОЛІВ ЗА ДОПОМОГОЮ БПЛА

Сучасний розвиток аграрної галузі визначається цифровізацією та впровадженням інтелектуальних систем підтримки прийняття рішень, зокрема інтеграцією комп’ютерного зору й безпілотних літальних апаратів у задачі моніторингу сільськогосподарських угідь. Використання БПЛА з RGB, мульти- та гіперспектральними камерами забезпечує збір аерофотоданих, які обробляються методами комп’ютерного зору та машинного навчання. Застосування згорткових нейронних мереж дає змогу автоматизувати оцінювання стану посівів, виявлення аномалій і прогнозування врожайності в межах концепції точного землеробства.

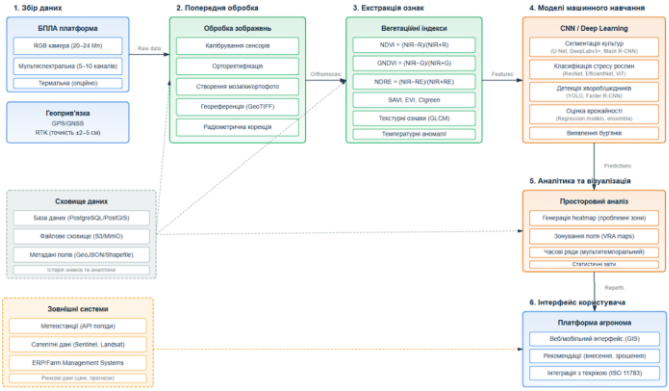


Рис. 1.1. Функціональна схема системи моніторингу полів з використанням БПЛА та модулів комп’ютерного зору

Система моніторингу ґрунтується на збиранні аерофотознімків з БПЛА, оснащених RGB, мультиспектральними та термальними камерами, з подальшою геоприв’язкою й орторектифікацією даних. Обробка зображень методами комп’ютерного зору та машинного навчання, зокрема із застосуванням згорткових нейронних мереж, забезпечує класифікацію стану посівів, виявлення зон стресу та прогнозування розвитку культур. Формування спектральних і теплових карт, розрахунок вегетаційних індексів і аналіз структурних змін рослин

дозволяють своєчасно ідентифікувати ознаки захворювань та оптимізувати локалізоване використання аграрних ресурсів із мінімальним впливом на довкілля. Вітчизняний досвід свідчить, що впровадження подібних систем на підприємствах аграрного сектору України дає змогу скоротити витрати на моніторинг у 3–5 разів та підвищити точність оцінки стану посівів на понад 90 %. Аналітичні модулі дозволяють порівнювати показники у різні періоди вегетації, формувати динамічні звіти та приймати обґрунтовані управлінські рішення.

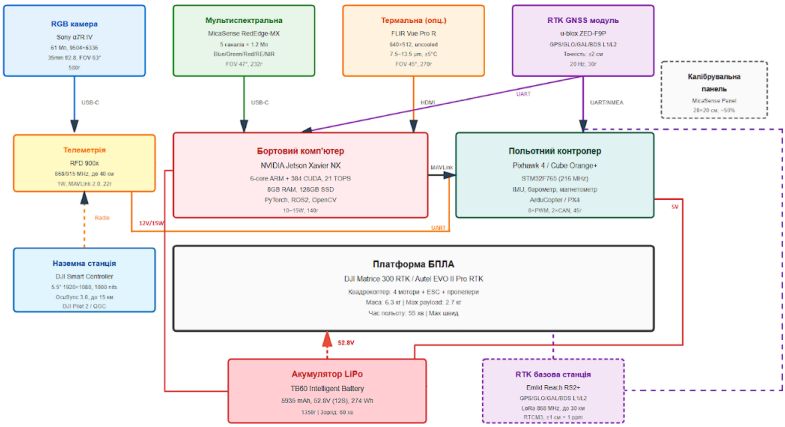


Рис. 1.2. – Компоновка апаратної частини комплексу БПЛА для агромоніторингу.

Використання БПЛА у поєднанні з технологіями комп’ютерного зору забезпечує високу точність і оперативність моніторингу стану посівів, суттєво скорочує часові та трудові витрати, а також дозволяє автоматизовано відстежувати динаміку розвитку культур. Це сприяє раціональному використанню води, добрив і засобів захисту рослин, підвищуючи екологічну ефективність виробництва. Подальший розвиток таких систем пов’язаний із інтеграцією з технологіями IoT, супутниковими даними та сенсорними мережами, а також нейромережевих моделей глибокого навчання для адаптивного аналізу польових даних.

Список використаних джерел:

1. A Review on UAV-Based Applications for Precision Agriculture. (MDPI) URL: https://www.mdpi.com/2078-2489/10/11/349

2. How Drones and Computer Vision are Used to Enhance Crop Yield. (Aya Data) URL: https://www.ayadata.ai/how-drones-and-computer-vision-are-used-to-enhance-crop-yield/

УДК 621.311.22:621.316.925:681.5

Линець А.Л., здобувач
Ткачук А.Г., к.т.н, доцент
Крижанівська І.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

ІНТЕГРАЦІЯ НАКОПИЧУВАЧІВ ЕНЕРГІЇ У СИСТЕМИ АВТОМАТИЗОВАНОГО РЕГУЛЮВАННЯ ЕЛЕКТРИЧНИХ СТАНЦІЙ

Сучасні електроенергетичні системи зазнають трансформацій, пов'язаних із зростанням частки відновлюваних джерел, нестабільністю генерації та підвищеними вимогами до балансування навантаження. В умовах частих коливань споживання та генерації традиційні системи регулювання частоти й потужності втрачають ефективність.

Інтеграція накопичувачів енергії (літій-іонних, гібридних, суперконденсаторних) у системи автоматизованого регулювання дозволяє підвищити гнучкість роботи станцій, забезпечити швидкодію реакції на зміни навантаження й стабілізувати параметри мережі у реальному часі.

Використання накопичувачів відкриває можливості для згладжування пікових режимів, зменшення втрат при пусках агрегатів, підтримання оптимального енергетичного балансу та переходу до адаптивних систем керування типу Smart Grid. Для українських електростанцій, які поступово переходять до децентралізованої генерації, ця технологія є ключовою для підвищення енергетичної безпеки та ефективності [1-2].

Метою досліджень є розроблення підходів до інтеграції систем накопичення енергії у контур автоматизованого регулювання електричних станцій з метою підвищення стабільності параметрів частоти, напруги та ефективності використання генераційних потужностей [3].

Дослідження виконано на основі створення комп'ютерної моделі енергетичного вузла, який містить три основні компоненти: синхронний генератор, що працює у складі електростанції; систему автоматизованого регулювання потужності (САРП), реалізовану на основі ПІ-контролера; блок накопичувача енергії (BESS), підключений через двонаправлений DC/DC-перетворювач до шини постійного струму. Моделювання здійснювалося у середовищі MATLAB/Simulink із використанням реальних електричних параметрів літій-іонних модулів типу LG Chem RESU10H (номінальна напруга – 300 В, ємність

– 100 А·год, максимальний струм заряду/розряду – 100 А). Для оцінювання динаміки частоти генератора застосовано модель синхронної машини типу Simscape Electrical Machines. Система керування формує сигнал керування потужністю накопичувача P_{BESS} залежно від миттєвого відхилення частоти Δf від номінального значення f_0. Алгоритм базується на виразі:

$$P_{BESS} = K_P \cdot \Delta f + K_I \int \Delta f dt,$$

де *Kp, Ki* – коефіцієнти ПІ-регулятора, що налаштовуються з урахуванням інерційності системи.

Для підвищення стабільності у непередбачуваних умовах застосовано адаптивну зміну коефіцієнтів регулятора залежно від швидкості зміни навантаження, яку оцінюють за допомогою предиктивної моделі на базі методу ковзного середнього. Передбачено двонаправлений обмін енергією: під час надлишку генерації накопичувач переходить у режим заряду, зменшуючи коливання частоти; у періоди пікових навантажень – віддає енергію у мережу, забезпечуючи стабільність напруги.

Моделювання показало, що використання накопичувачів енергії дозволяє зменшити амплітуду коливань частоти на 35–40 %, а відхилення напруги на 20–25 % у порівнянні з традиційним контуром регулювання. Крім того, інтеграція BESS дає змогу знизити тривалість перехідних процесів і підвищити коефіцієнт корисного використання генераторів.

У структурі Smart Grid такі накопичувачі можуть виконувати функції резервного живлення, пікового зрівнювання, підтримання реактивної потужності та швидкого реагування на аварійні зміни навантаження.

Список використаних джерел:

1. Wang Y., Saad W., Han Z., Poor H. V., Başar T. A Game-Theoretic Approach to Energy Trading in the Smart Grid. arXiv 2013. https://arxiv.org/abs/1310.1814

2. Alavi S. A., Mehran K., Hao Y., Mirsaeedi H., Vahidinasab V. A Distributed Event-Triggered Control Strategy for DC Microgrids Based on Publish-Subscribe Model Over Industrial Wireless Sensor Networks. arXiv 2019. https://arxiv.org/abs/1906.03623

3. Tkachuk A.H., Kryzhanivska I.V., Poklyachenko O.V., Tkachuk D.Yu. Development of intelligent electric power systems based on computer-integrated technologies for monitoring and management of energy flows. Журнал «Наука і техніка сьогодні». Серія: "Техніка". 2025. №6 (47). С. 945-955

УДК 004.932

Сардаківський А.В., здобувач
Ткачук Д.Ю., аспірантка
Державний університет «Житомирська політехніка»

ІНТЕГРАЦІЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ І МУЛЬТИСПЕКТРАЛЬНОГО АНАЛІЗУ В СИСТЕМАХ ТОЧНОГО ЗЕМЛЕРОБСТВА

У сучасному аграрному виробництві одним із ключових завдань є підвищення ефективності використання ресурсів, зменшення втрат урожаю та забезпечення своєчасного виявлення проблемних ділянок полів. Для вирішення цих завдань усе ширше застосовуються безпілотні літальні апарати (БПЛА), які завдяки високій мобільності та точності зйомки забезпечують оперативний моніторинг стану посівів і ґрунтового покриву.

У практичних умовах дрони обладнуються різними типами сенсорних систем: мультиспектральними, тепловізійними та RGB-камерами, що дає змогу проводити комплексний аналіз стану рослин і отримувати багатоканальні дані про параметри вегетації. Мультиспектральні сенсори дозволяють обчислювати індекси вегетації (NDVI, GNDVI, NDRE), які відображають рівень фотосинтетичної активності та фізіологічний стан культур. Тепловізійна зйомка використовується для оцінювання вологості ґрунту та виявлення зон водного стресу, тоді як RGB-зображення забезпечують візуальний огляд полів і фіксацію просторових неоднорідностей.

Важливу роль у процесі моніторингу відіграє обробка зображень, отриманих із БПЛА. Аналіз спектральних характеристик, кольорової гами та контрастності дає можливість визначати ступінь розвитку культур, наявність бур'янів, механічних пошкоджень або ознак захворювань рослин. Використання алгоритмів комп'ютерного зору та розпізнавання кольору дає змогу автоматично сегментувати зображення, виділяти зони зі зниженою інтенсивністю фотосинтезу, оцінювати рівень хлорофілу та визначати ослаблені ділянки. На основі цих даних формується цифрова карта поля, яка забезпечує аграрія актуальною інформацією для прийняття оперативних управлінських рішень.

Для збору, обробки та візуалізації даних широко застосовуються спеціалізовані програмні комплекси, такі як Pix4D, DroneDeploy, Agisoft Metashape і DJI Terra, які реалізують автоматичне створення ортофотопланів, тривимірних моделей рельєфу та індексних карт стану

рослин. Завдяки цим інструментам забезпечується інтеграція даних із польових місій у єдиний аналітичний простір управління господарством. Серед сучасних апаратно-програмних рішень для агромоніторингу важливе місце займає DJI Mavic 3M, який поєднує RGB-камеру з роздільною здатністю 20 Мп та мультиспектральний модуль із чотирма сенсорами у зеленому, червоному, крайово-червоному й ближньому інфрачервоному діапазонах. Вбудований RTK-модуль забезпечує геодезичну точність позиціонування до 1 см, а тривалість польоту досягає 43 хвилин, що дозволяє проводити детальний моніторинг значних площ із високою просторовою роздільністю [1].

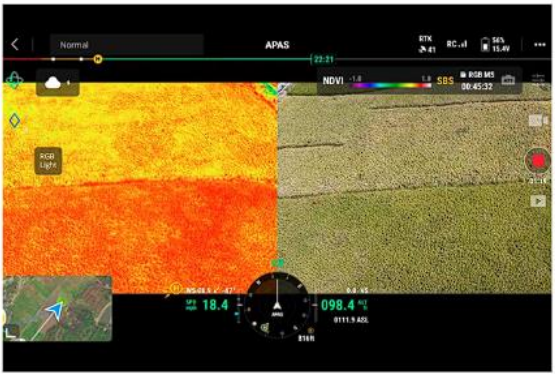


Рис.1.Візуалізація результатів мультиспектрального аналізу поля

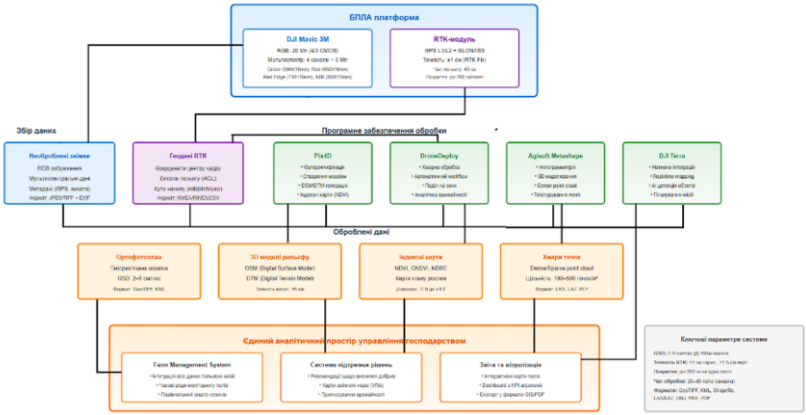


Рис.2. Схема технічної архітектури комплексу моніторингу поля з використанням БПЛА, сенсорів і програмного забезпечення для обробки зображень

Отримані в результаті аерофотозйомки індексні карти, сформовані на основі мультиспектральних та теплових даних, забезпечують кількісну й просторово деталізовану оцінку стану посівів протягом усього вегетаційного періоду. Аналіз динаміки вегетаційних індексів дає змогу об'єктивно оцінювати ефективність застосування агротехнічних заходів, таких як внесення мінеральних добрив, засобів захисту рослин, зрошення або регулювання густоти посівів, шляхом порівняння стану рослин до та після виконання відповідних операцій. Просторова локалізація відхилень від нормативних значень індексів дозволяє своєчасно ідентифікувати проблемні зони поля на ранніх етапах вегетації, зокрема ділянки з дефіцитом поживних речовин, водним або температурним стресом, розвитком хвороб чи нерівномірністю сходів, що є критично важливим для запобігання втратам урожаю. На основі цих даних формується науково обґрунтована стратегія диференційованого управління полем, яка передбачає локалізоване застосування ресурсів із урахуванням просторової неоднорідності агроценозу, що сприяє зниженню витрат, підвищенню економічної ефективності виробництва та мінімізації негативного впливу на довкілля. Подальша інтеграція результатів аерокосмічного моніторингу з цифровими платформами управління агропідприємством, геоінформаційними системами та базами агрономічних даних створює передумови для впровадження інтелектуальних систем підтримки прийняття рішень, автоматизованого планування агротехнічних операцій і переходу до комплексних, адаптивних технологій точного землеробства, здатних функціонувати в умовах змінних природно-кліматичних та виробничих факторів.

Список використаних джерел:

1. DJI Mavic 3M – DJI. URL: https://ag.dji.com/mavic-3-m (дата звернення: 07.11.2025)

2. Zhang, D. et al. Integration of UAV Multispectral Remote Sensing and Precision Agriculture Monitoring. MDPI, 2025.

3. Guebsi, R. et al. Drones in Precision Agriculture: A Comprehensive Review. MDPI, 2024.

4. Grbović, Ž. et al. Integrating UAV Multispectral Imaging and Proximal Sensing for High-Precision Crop Monitoring. PLOS One, 2025.

5. Samko, M. Monitoring using UAVs in Precision Farming Technologies. Earthdoc.org, 2025.

УДК 621.314.25:004.89

Богдановський М.В., ст. викладач
Корнійчук С.М., здобувач
Державний університет «Житомирська політехніка»

ІНВЕРСНА НЕЙРОНЕЧІТКА МОДЕЛЬ ОЦІНКИ ЗАЛИШКОВОГО РЕСУРСУ ВИСОКОВОЛЬТНИХ ТРАНСФОРМАТОРІВ НАПРУГИ

Сучасні трансформатори напруги (ТН) є складними пристроями енергетичного комплексу, надійність роботи яких залежить від багатьох факторів. Фактори можливо поділити на окремі групи: параметри ізоляції, параметри конденсаторного дільника, теплові параметри, параметри трансформаторної частини, механічні та конструктивні параметри. В роботі [1] визначено поняття залишкового ресурсу трансформаторів. На підставі проаналізованих методик оцінки залишкового ресурсу за станом оливи, що широко використовується у світовій практиці діагностування, була запропонована нелінійна модель, що включає в себе основні фактори:

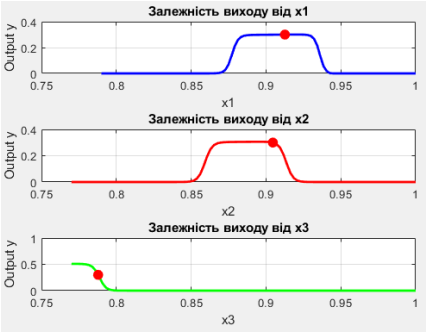
$$k_{\text{заг.рес}} = k_{\text{Кт}}^{p_{\text{Кт}}} \cdot k_{\text{Темб}}^{p_{\text{Темб}}} \cdot k_{\text{ебн}tg(\delta)}^{p_{\text{ебн}tg(\delta)}} \cdot k_{Rосн}^{p_{Rосн}} \cdot k_{1\text{Тнад}}^{p_{\text{Тнад}}} \cdot k_{2\text{Тнад}}^{p_{\text{Тнад}}} \cdot k_{3\text{Тнад}}^{p_{\text{Тнад}}} \cdot$$
$$\cdot k_{1\Delta C\text{x}}^{p_{\Delta C\text{x}}} \cdot k_{2\Delta C\text{x}}^{p_{\Delta C\text{x}}} \cdot k_{3\Delta C\text{x}}^{p_{\Delta C\text{x}}} \cdot k_{1C\text{tg}(\delta)}^{p_{C\text{tg}(\delta)}} \cdot k_{2C\text{tg}(\delta)}^{p_{C\text{tg}(\delta)}} \cdot k_{3C\text{tg}(\delta)}^{p_{C\text{tg}(\delta)}} \cdot k_{1Rел}^{p_{Rел}} \cdot k_{2Rел}^{p_{Rел}} \cdot$$
$$k_{3Rел}^{p_{Rел}} \cdot \cdot k_{\text{Тс}}^{p_{\text{Тс}}} \cdot k_{\text{Кон}}^{p_{\text{Кон}}} \cdot k_{\text{ХАРГ}}^{p_{\text{ХАРГ}}},$$

де *Темб* - температура верхньої частини баку, *Кт* - коефіцієнт трансформації між виводами елементів, Rосн - активний опір ізоляції ТН, *tg(δ)* - тангенс кута діелектричних втрат в паперово-масляній ізоляції в навантаженому режимі, *Кон* - кислотне число, *Тс* - температура займання оливи °С, *ХАРГ* - узагальнений імпакт-фактор розчинених в трансформаторному маслі газів, *Тнад* - надлишкова температура апаратного виводу дільника напруги, ΔСХ - дрейф ємності паперово-масляної ізоляції, *tg(δ)* тангенс кута діелектричних втрат в паперово-масляній ізоляції в розвантаженому режимі, *Rєл* - активний опір ізоляції ємнісного елементу. В результаті дослідження було запропоновано нейронечітку модель (ANFIS), яка після навчання на експериментальних даних роботи трансформаторів дозволяє прогнозувати вплив факторів на коефіцієнт залишкового ресурсу. Основну проблему являє широка варіативність комбінації факторів, що можуть давати однаковий коефіцієнт залишкового ресурсу, тому розв'язання оберненої задачі є важливим. Для вирішення даної задачі можливо використати функцію помилки, яка обчислює різницю між бажаним виходом і виходом моделі ANFIS для заданих входів та

оптимізаційні алгоритми (наприклад, fmincon, ga, particleswarm) для знаходження таких вхідних значень, які мінімізують цю помилку. Основна процедура розрахунку в середовищі MATLAB наступна:

```
% 2. Створення початкової FIS-структури
numMFs = 5;
mfType = 'gaussmf';
fis = genfis1(data, numMFs, mfType);
% 3. Навчання ANFIS-моделі
numEpochs = 100;
[trainedFIS, ~] = anfis(data, fis, numEpochs);
% 4. Оптимізація для заданого виходу
error_func = @(x) abs(evalfis(x(:)', trainedFIS) - desired_y);
x0 = [(min(x1)+max(x1))/2 (min(x2)+max(x2))/2 (min(x3)+max(x3))/2];
lb = [min(x1) min(x2) min(x3)];
ub = [max(x1) max(x2) max(x3)];
options = optimoptions('fmincon', 'Display', 'none', 'Algorithm', 'sqp');
[x_opt, ~] = fmincon(error_func, x0, [], [], [], [], lb, ub, [], options);
```

Результат роботи програми на обмеженій до 10 значень виборки даних та залежність залишкового ресурсу на рівні 30% по кожному з трьох факторів наведено на рисунку 1.



Designated epoch number reached --> ANFIS training completed at epoch 100.

Minimal training RMSE = 0.000000

? Оптимальні входи для y = 0.300:

x1 = 0.9126 x2 = 0.9046 x3 = 0.7878

? Отриманий вихід: 0.3000

Рис.1.Залежність залишкового ресурсу.

Список використаних джерел:

1. Богдановський М.В., Гуменюк А.А., Доброжанський О.О., Ткачук А.Г., Ковальчук І. В. Використання нечітких нейронних мереж для діагностування ємнісних високовольтних трансформаторів напруги // Наукові праці ДонНТУ. Серія: «Електротехніка і енергетика» №2 (33)'2025. – С. 73–81. Режим доступу: https://elen.donntu.edu.ua/2074-2630-2025-2-73-81.pdf

УДК 004.056.5

Раданович В. Я., здобувач
Ткачук Д. Ю., асистентка
Державний університет «Житомирська політехніка»

АВТОМАТИЗОВАНИЙ КОНТРОЛЬ ПРАВИЛЬНОСТІ СОРТУВАННЯ ПОСИЛОК У ЛОГІСТИЧНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНОГО ЗОРУ ТА НЕЙРОННОЇ МЕРЕЖІ YOLO

Інтенсивне зростання електронної комерції спричинило різке підвищення навантаження на логістичні комплекси, де традиційні методи автоматизації, зокрема класичні геометричні алгоритми на кшталт ICP вже не забезпечують необхідної ефективності. Вони потребують значної попередньої обробки даних, чутливі до шумів та оклюзій і потребують багато ресурсів, що робить їх непридатними для високошвидкісних конвеєрів. У результаті знижується робастність системи за умов зміни орієнтації, щільного розташування або взаємного перекриття посилок.

Сучасні підходи роблять акцент на глибоких нейронних мережах, які дозволяють передбачати оптимальну зону чи положення захоплення без складної проміжної обробки. Архітектури типу FCN і Mask R-CNN демонструють високу якість сегментації, але їх обчислювальна складність і зниження точності при великому перекритті об'єктів обмежують їх придатність у реальному часі.

Для вирішення цих проблем запропоновано інтегрований метод швидкого сортування посилок на основі багатозадачного глибокого навчання. У його основі оптимізована модель YOLOv8-S із зменшеною кількістю каналів та динамічним зважуванням функцій втрат (GradNorm/DWA), що дало змогу скоротити кількість параметрів на 35–40% без втрати точності. Досягнута продуктивність ≥ 80 FPS відповідає вимогам конвеєрів зі швидкістю 1.5–2 м/с, а середня точність детекції становить mAP = 0.94.

Додаткова реалізація багатозадачної моделі оцінки точки захоплення на основі прогнозування 5–7 ключових точок для визначення повної 6D-пози (x, y, z, α, β, γ) збільшує продуктивніть. Навчання проводилось із використанням гібридної функції втрат, що поєднує L1/Smooth L1 для координат і IoU-компоненту для якості області захоплення. Це забезпечило точність орієнтації до ±5° та позиційну похибку не більше ±2 мм, що суттєво підвищує стійкість системи до оклюзій і невпорядкованого розташування посилок.

Такий підхід перевершує сегментаційні FCN/Mask R-CNN-рішення за швидкодією, робастністю та адаптивністю.

Запропонована система дає змогу роботизованому маніпулятору точно визначати цільовий об'єкт, оцінювати його положення та виконувати автоматичне захоплення без участі оператора.

Оптимізовані моделі на основі YOLO формують перспективну платформу для високопродуктивної автоматизації логістичних процесів у сучасних умовах стрімкого розвитку електронної комерції.

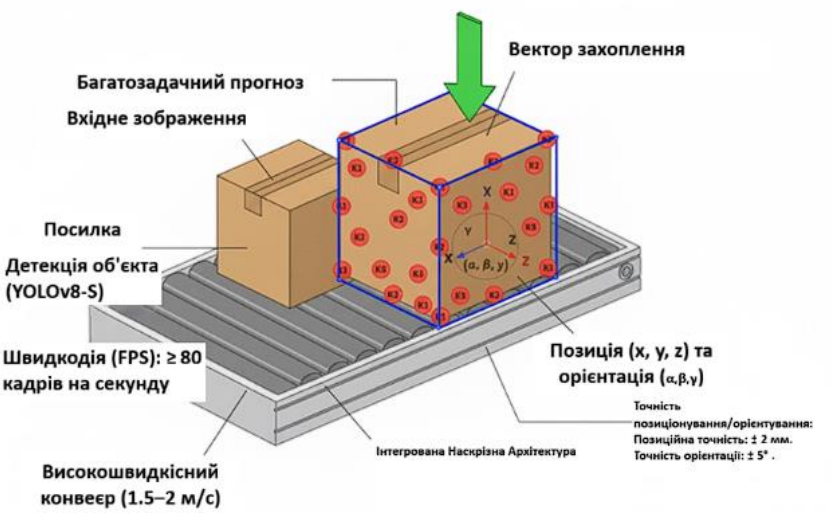


Рис. 1. Візуалізація роботи інтегрованої системи сортування посилок

Список використаних джерел:

1. Visual Sorting of Express Parcels Based on Multi-Task Deep Learning [Електронний ресурс].- Режим доступу:https://www.mdpi.com/1424-8220/20/23/6785

2.Ultralytics YOLO applications in logistics [Електронний ресурс].- Режим доступу:https://www.ultralytics.com/solutions/ai-in-logistics

УДК 621.9

Богдановський М.В., ст. викладач
Горбік Д.П., здобувач
Державний університет «Житомирська політехніка»

РОЗРОБКА СИМУЛЯТОРА ДЛЯ ДОСЛІДЖЕННЯ ЗАДАЧ ПРЯМОЇ І ЗВОРОТНОЇ КІНЕМАТИКИ МАНІПУЛЯТОРІВ

У роботі представлено програмний симулятор, призначений для вивчення кінематики маніпуляторів з трьома ступенями свободи.

Основна мета – створення навчального віртуального стенду, який дозволяє студентам на практиці опанувати основи прямої та зворотної кінематики, математичні методи обчислення положення виконавчого органу, а також моделювання руху у реальному часі.

Питання викладання робототехніки та мехатроніки у вищій школі передбачає не лише ознайомлення з фізичними платформами, але й детальне вивчення алгоритмів керування. Однією з базових задач є зворотна кінематика — знаходження необхідних кутів обертання приводів для досягнення заданого положення виконавчого органу.

Метою розробки є створення симулятора, який дозволяє вводити координати цільової точки, обчислювати кути за допомогою методів зворотної кінематики, моделювати рух у площині XY та забезпечувати візуальний супровід розрахунків. Маніпулятор моделюється як триланкова система у площині XY. Пряма кінематика визначається за допомогою тригонометричних рівнянь:

$$x = L_1 \cdot \cos(\theta_1) + L_2 \cdot \cos(\theta_1 + \theta_2) + L_3 \cdot \cos(\theta_1 + \theta_2 + \theta_3),$$
$$y = L_1 \cdot \sin(\theta_1) + L_2 \cdot \sin(\theta_1 + \theta_2) + L_3 \cdot \sin(\theta_1 + \theta_2 + \theta_3).$$

Для обчислення зворотної кінематики застосовано ітераційний метод Левенберга–Марквардта, що базується на апроксимації Якобіана та корекції похибки положення. Метод дозволяє ефективно знаходити розв'язки навіть у випадках, коли прямий аналітичний метод не застосовується. Використано формулу $\Delta\theta = (J^T \cdot J + \lambda \cdot I)^{-1} \cdot J^T \cdot e$, де J — Якобіан, e — вектор похибки, λ — параметр демпфування. Алгоритм перевіряє досяжність координати виконавчого органу; у разі її недосяжності виводиться повідомлення про помилку, що дозволяє користувачеві коригувати введені значення.

Програмну реалізацію виконано з використанням C++/CLI у середовищі Windows Forms. Графічний інтерфейс дозволяє у реальному часі вводити кути обертання або координати виконавчого органу,

перемикатися між режимами прямої та зворотної кінематики, переглядати математичні розрахунки у текстовому вікні, моделювати рух ланок. Система підтримує перевірку діапазонів обертання суглобів, побудову траєкторій та їх відтворення через анімацію. Вся візуалізація реалізована за допомогою векторної графіки у 2D. Структура коду модульна та гнучка для подальших розширень.

Створене програмне ядро симулятора має масштабовану та платформонезалежну архітектуру, що забезпечує можливість його перенесення у середовище Unity для побудови тривимірної інтерактивної моделі маніпулятора. Такий підхід передбачає чітке відокремлення обчислювального рівня, який реалізує алгоритми прямої та зворотної кінематики, обчислення Якобіана й перевірку обмежень суглобів, від рівня візуалізації та користувацької взаємодії, що дозволяє зберегти математичну коректність розрахунків. Перехід з C++/CLI на C# полягає у відтворенні структури класів кінематичного ланцюга та реалізації алгоритмів у вигляді незалежних модулів, придатних для роботи в реальному часі в ігровому циклі Unity.

Збереження методу Левенберга–Марквардта як базового інструменту зворотної кінематики забезпечує чисельну стійкість і контроль точності розв’язків, зокрема поблизу сингулярних конфігурацій. Використання Unity відкриває можливості інтеграції фізичного рушія, сучасної 3D-візуалізації та розширених сценаріїв взаємодії, а також створює передумови для зв’язку з реальними маніпуляторами і використання симулятора як цифрового двійника в навчальних і дослідницьких робототехнічних системах.

Список використаних джерел:

1.Craig J. J. Introduction to Robotics: Mechanics and Control. – 4th ed. – Pearson, 2018. – 448 p.

2.Levenberg K. A method for the solution of certain nonlinear problems in least squares // Quarterly of Applied Mathematics. – 1944. – Vol. 2, No. 2. – P. 164–168.

3.Marquardt D. An Algorithm for Least-Squares Estimation of Nonlinear Parameters // Journal of the Society for Industrial and Applied Mathematics. – 1963. – Vol. 11, No. 2. – P. 431–441.

УДК 004.7

Чайківський А.В., здобувач
Ткачук Д.Ю., аспірантка
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ ІНФРАЧЕРВОНОГО СПЕКТРА ДЛЯ ПІДВИЩЕННЯ ТОЧНОСТІ МАШИННОГО ЗОРУ В УМОВАХ НИЗЬКОЇ ОСВІТЛЕНОСТІ

Системам машинного зору важливо забезпечити стабільне розпізнавання об'єктів незалежно від умов освітлення. Проте в темряві або при слабкому освітленні традиційні оптичні сенсори, що працюють лише у видимому спектрі, демонструють значне зниження точності. Одним із ефективних шляхів розв'язання цієї проблеми є використання інфрачервоного (ІЧ) спектра, який дозволяє отримувати якісні зображення навіть за відсутності природного чи штучного освітлення.

Інфрачервоне випромінювання має більшу довжину хвилі, ніж видиме світло (понад 700 нм), що дозволяє сенсорам фіксувати сигнали, які не залежать від рівня освітлення. Камери, оптимізовані для ближнього інфрачервоного (NIR) діапазону, здатні «бачити» об'єкти, коли видиме світло відсутнє або його надто мало.

За даними компанії Basler AG, NIR-сенсори мають підвищену фоточутливість і здатні забезпечити більш високий контраст зображення без додаткового підсилення шумів [1]. Це робить їх ефективними для систем спостереження, робототехніки та контролю виробничих процесів.

Використання інфрачервоного спектра у системах машинного зору має суттєві переваги, особливо в умовах низької освітленості. Завдяки здатності ІЧ-випромінювання проникати крізь туман, пил або дим, зображення, отримане такими камерами, зберігає високу інформативність навіть у складних умовах навколишнього середовища. Це дозволяє значно покращити контраст і видимість деталей, які у звичайному видимому спектрі могли б бути повністю приховані. Однією з головних переваг є також менша залежність від зовнішнього освітлення – інфрачервоні камери можуть ефективно працювати навіть у повній темряві, використовуючи підсвітку у ближньому інфрачервоному діапазоні, що робить їх надзвичайно корисними для систем відеоспостереження, безпілотних апаратів і роботизованих комплексів, які діють у нічний час або при слабкому освітленні [2]. Використання ІЧ-зображень підвищує точність алгоритмів машинного навчання, що підтверджується дослідженням LLVIP (Low-Light Visible-Infrared Paired Dataset). Згідно з отриманими результатами, поєднання

видимого та інфрачервоного спектрів дозволяє алгоритмам розпізнавання краще ідентифікувати контури, форми та об'єкти навіть у темряві, де звичайна камера не може забезпечити достатню чіткість. Такий підхід значно розширює можливості систем штучного інтелекту, роблячи їх ефективнішими у складних умовах освітлення.

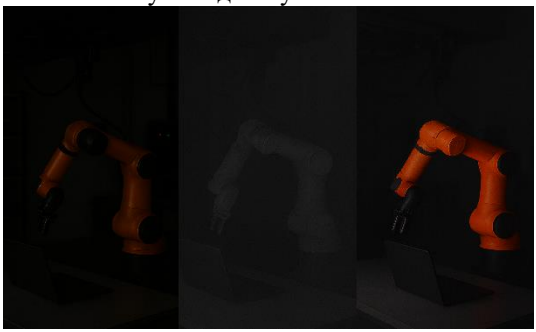


Рисунок 1 – Без інфрачервоного/ з інфрачервоним/ інфрачервоним + RGB

На практиці інфрачервоні камери знаходять широке застосування у різних сферах. У системах відеоспостереження вони дають змогу виявляти людей, транспортні засоби й інші об'єкти без потреби у видимому освітленні. В автономній навігації дронів і роботів ІЧ-зір допомагає розпізнавати перешкоди та орієнтуватися в просторі при недостатньому світлі, підвищуючи безпеку та надійність руху. У промисловості ж такі системи використовуються для контролю якості продукції, вони дають змогу виявляти дефекти поверхні, перевіряти герметичність упаковки або контролювати структуру матеріалів, що є невидимими для звичайних RGB-камер [2].

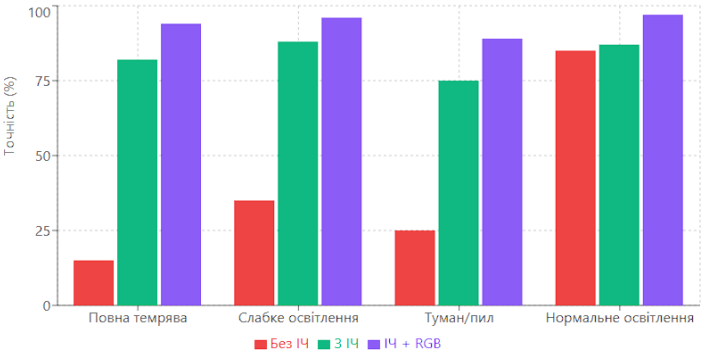


Рисунок 2 – Точність розпізнавання об'єктів в різних умовах освітленості (%)

Таблиця 1 – Порівняльні характеристики систем машинного зору

Параметр	**Без ІЧ**	**З ІЧ (NIR)**	**ІЧ + RGB**
Точність (темрява)	15%	82%	94%
Робочий діапазон	400-700 нм	700-940 нм	400-940 нм
Контрастність	Низька (30%)	Висока (90%)	Максимальна (98%)
Шум сигналу	45 дБ	28 дБ	22 дБ
Залежність від освітлення	Критична	Мінімальна	Відсутня
Проникнення крізь туман	Слабке	Хороше	Відмінне

Ефективність роботи інфрачервоних систем машинного зору визначається трьома головними складовими: сенсорною частиною, освітленням та програмною обробкою. Сенсорна частина зазвичай базується на камерах без IR-cut фільтра або спеціалізованих NIR-сенсорах, здатних уловлювати ближнє інфрачервоне випромінювання з високою квантовою ефективністю. ІЧ-освітлення, зазвичай у діапазоні 850–940 нм, є безпечним для людського ока та забезпечує рівномірне підсвічування сцени. Як зазначається у матеріалах компанії ProPhotonix, якість зображення значною мірою залежить від рівномірності освітлення та правильного вибору довжини хвилі для конкретних поверхонь чи матеріалів [2]. На завершальному етапі програмна обробка зображення включає алгоритми фільтрації шумів, нормалізації яскравості й поєднання ІЧ- та видимих каналів, що дозволяє отримати максимально точне та інформативне зображення. Інтеграція інфрачервоних технологій у машинний зір створює основу для розвитку нових інтелектуальних систем спостереження, керування й автоматизованого контролю якості, відкриваючи нові можливості для промисловості, безпеки та автономних систем у цілому.

Список використаних джерел:

1. Basler AG. Near-Infrared (NIR) Cameras. – Basler Official Website. URL: https://www.baslerweb.com/en/learning/near-infrared-nir-cameras/ (дата звернення: 12.11.2025).

2. ProPhotonix. IR Machine Vision Lighting. – ProPhotonix Application Notes. URL: https://www.prophotonix.com/applications/machine-vision-lighting/ir-machine-vision-lighting/(дата звернення: 12.11.2025).

УДК 378.147:004

Гальвіта А., здобувач
Корнєва В.Р., викладач
Прилуцький технічний фаховий коледж

СУЧАСНІ ПІДХОДИ ДО РОЗВИТКУ КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ У ВИРОБНИЧИХ СИСТЕМАХ

Цифрова трансформація освіти стала одним із ключових напрямів розвитку сучасних освітніх систем. Поширення інформаційно-комунікаційних технологій, активізація дистанційної взаємодії та потреба у гнучких моделях навчання сприяли переходу закладів освіти до змішаних форм організації освітнього середовища. Такий формат поєднує традиційну аудиторну роботу та онлайн-компоненти, що дозволяє оптимізувати навчальний процес, забезпечити індивідуальну траєкторію для кожного здобувача освіти та створити умови для ефективного поєднання теоретичної та практичної діяльності. Змішане навчання значно розширює можливості для самостійної, дослідницької та проєктної роботи, сприяючи розвитку навичок XXI століття.

Процес цифрової трансформації охоплює кілька структурних компонентів: оновлення педагогічних технологій, розвиток цифрової інфраструктури, формування цифрових компетентностей учасників освітнього процесу та запровадження нових моделей взаємодії між викладачем і студентом. Одним із ключових аспектів є використання хмарних сервісів, інтерактивних платформ та систем управління навчанням (LMS).

У межах змішаного навчання викладач отримує значно ширші можливості для адаптації навчальних матеріалів до потреб конкретних студентів. Інструменти штучного інтелекту дозволяють аналізувати результати діяльності здобувачів, прогнозувати рівень засвоєння, визначати прогалини в знаннях і пропонувати індивідуальні завдання для їх усунення. Широке застосування інтерактивних ресурсів — відеолекцій, анімацій, симуляторів, віртуальних лабораторій, сервісів спільної роботи та електронних бібліотек — сприяє активізації пізнавальної діяльності, розвитку критичного мислення та підвищенню навчальної мотивації. Такі ресурси роблять процес навчання більш візуальним, наочним і доступним навіть для студентів із різними стилями сприйняття інформації.

Важливим компонентом цифрової трансформації є формування цифрової грамотності та відповідальної поведінки здобувачів освіти. Сучасні студенти мають вміти ефективно працювати з великими

масивами інформації, застосовувати різні цифрові інструменти, критично оцінювати достовірність даних, керувати власною цифровою безпекою та приватністю. У змішаному навчанні ці навички набувають особливої ваги, оскільки якість виконання завдань та успішність навчання часто залежить від здатності студента працювати самостійно, користуючись наданими цифровими ресурсами.

Викладач у цифровому середовищі також виконує нові ролі: тьютора, фасилітатора, модератора командної роботи та консультанта. Замість традиційної ролі «джерела інформації» він стає організатором освітнього простору, спрямованого на осмислення, дослідження й самостійний пошук рішень. Змішане навчання дозволяє поєднувати синхронні зустрічі (онлайн або офлайн) та асинхронні активності, що створює гнучкі умови для навчання за індивідуальним темпом. Такий підхід сприяє розвитку самодисципліни, відповідальності, вмінь планування та самооцінювання.

Отже, цифрова трансформація освітнього процесу в умовах змішаного навчання є невід'ємним елементом модернізації сучасної освіти. Упровадження цифрових технологій потребує системного підходу, методичної підтримки, професійного розвитку педагогічних кадрів і створення єдиної цифрової екосистеми закладу освіти. Успішна цифрова трансформація відкриває нові перспективи для розвитку інноваційного навчального середовища, у якому здобувач освіти стає активним учасником, творцем знань і співорганізатором власної освітньої траєкторії.

Список використаних джерел:

1. Ковальов В.М. Комп'ютерно-інтегровані технології: основи та перспективи / В.М. Ковальов, Ю.А. Смирнов // Науковий вісник Миколаївського національного університету імені В. О. Сухомлинського. – 2018. №3. – С. 45-53.

2. Лещенко В.В. Сучасні комп'ютерні технології в автоматизації виробничих процесів / В.В. Лещенко, І.М. Гриньків // Автоматизація та інформаційні технології в промисловості. – 2021. – Вип. 12. – С. 112-120.

УДК 621.865

Ткачук А.Г., к.т.н, доцент
Черниш О.А., к.ф-л.н., доцент
Кравчук А.Р., PhD
Василевський Д.В., здобувач
Державний університет «Житомирська політехніка»

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ДЛЯ ЗБОРУ ТА АНАЛІЗУ СИТУАЦІЙНИХ ДАНИХ

Сучасні виклики у сфері національної безпеки та оборони потребують швидких, точних і масштабованих рішень для опрацювання великих масивів даних. Традиційні методи збору та аналізу розвідувальної інформації дедалі більше поступаються інтелектуальним системам, здатним працювати в режимі реального часу, забезпечуючи високу оперативність прийняття рішень. У роботі представлено підхід до побудови інтелектуальної системи збору, оброблення й аналізу ситуаційних даних на основі штучного інтелекту, машинного навчання та технологій обробки потоків даних [1-3].

Запропонована система має модульну структуру і складається з двох функціональних підсистем: модуля збору розвідувальної інформації та модуля її аналітичної обробки. Основою першого модуля є мобільна роботизована колісна платформа, обладнана тепловізором, камерою нічного бачення, сенсорами для виявлення вибухонебезпечних газів, системою контролю рівня радіаційного забруднення та комплексом дистанційного аудіоспостереження. Інтегроване спеціалізоване програмне забезпечення забезпечує попередню обробку відео- та аудіопотоків з метою виділення характерних ознак об'єктів спостереження. Керування платформою здійснюється дистанційно, у тому числі із застосуванням VR-технологій, що підвищує точність візуального сприйняття та ситуаційної оцінки оператором.

Другий модуль орієнтований на аналітичну інтерпретацію зібраних даних. Його основу становлять методи лінгвістичного аналізу, машинного навчання та нейронних мереж, які застосовуються для автоматизованої класифікації, профайлінгу і визначення поведінкових характеристик потенційного зловмисника [4]. Система забезпечує систематизацію інформації, виокремлення змістових маркерів, індикаторів ризику та формування оцінки вірогідності реалізації конкретних намірів. Такий підхід дозволяє створювати узгоджену інтелектуальну модель ситуації, що може бути використана для підтримки прийняття рішень у польових умовах.

Застосування саме колісного шасі зумовлене низкою технічних та експлуатаційних переваг. По-перше, це вища енергоефективність у порівнянні з гусеничними та крокуючими платформами. Колісний привід потребує значно менших витрат енергії на переміщення, що дозволяє збільшити тривалість автономної роботи та радіус дії. По-друге, підвищена прохідність та швидкість пересування. Колісні шасі забезпечують значно більшу швидкість на рівних і напіврівних поверхнях, що є критичним для оперативного збору даних під час розвідувальних місій. Також у платформи буде не 4 колеса, а 6. Шестиколісне шасі забезпечує суттєво кращу здатність долати нерівності місцевості завдяки: рівномірнішому розподілу маси по опорним точкам, зменшенню навантаження на кожне колесо, більшій кількості точок контакту з поверхнею. Це дозволяє платформі рухатися кам'янистим чи м'яким ґрунтом, сухими руслами, пересіченою місцевістю та у міській зоні з уламками будівельних конструкцій.

Завдяки зменшенню вібрацій і коливань сенсорні системи формують точніший зображувальний ряд, аудіосенсори отримують менш зашумлений сигнал, стабільність роботи датчиків радіаційного й газового моніторингу зростає. Це покращує точність даних, що надходять в аналітичний модуль.

Другий модуль системи забезпечує аналітичну інтерпретацію інформації: лінгвістичний аналіз аудіоданих, виявлення характерологічних маркерів, побудову профайлу потенційного зловмисника та оцінювання його поведінкових намірів.

Список використаних джерел:

1. Moczulski,W., Bulandra, K., & Adamczyk, M. (2017). Autonomous mobile robotic system for supporting counterterrorist and surveillance operations. In H. Bouma, F. Carlysle-Davies, R. J. Stokes, & Y. Yitzhaky (Eds.), Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies. SPIE. https://doi.org/10.1117/12.2278657

2. Kowalski, G., Glowka, J., Maciaś, M., & Puchalski, S. (2017). Modular robotic system for forensic investigation support. In H. Bouma, F. Carlysle-Davies, R. J. Stokes, & Y. Yitzhaky (Eds.), Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies. SPIE. https://doi.org/10.1117/12.2278735

3. Li J, Murong Li JX, Lai B, et al. Wireless sensor network for indoor air quality monitoring. 2014, 4:6. DOI: 10.1016/j.medengphy.2011.10.011.

4. Голобородько К. Лінгвістична експертиза тексту: юридичний та мовний аналіз. Збірник наукових праць "Український світ у наукових парадигмах". 2020. № 7. Режим доступу – https://cutt.ly/N1onZ7W

УДК 631.173; 004.896

Ткачук А.Г., к.т.н, доцент
Кравчук А.Р., PhD
Мельник О.Л., к.т.н., доцент
Козяр Я.А., аспірант
Державний університет «Житомирська політехніка»

РОЗРОБКА 3D-МОДЕЛІ КОРПУСУ МОБІЛЬНОЇ РОБОТИЗОВАНОЇ ПЛАТФОРМИ З ПІДВИЩЕНОЮ ПРОХІДНІСТЮ

Сучасні наземні роботизовані комплекси (НРК), інтелектальні мобільні роботи, мобільні роботизовані системи тощо, все частіше застосовуються для вирішення цивільних та мілітарних завдань. Особливість мобільних роботів є універсальність, гнучкість керування та можливість адаптації до різноманітних ситуацій, що робить їх високоефективними інтелектуальними пристроями. Одним із перспективних напрямків в сфері мобільної робототехніки є напрям моніторингу та спостереження, що є основною складовою розвідувальних операцій.

Метою даної роботи є представлення конструкції та 3D-моделі мобільної роботизованої платформи для розвідувальних операцій.

Конструкцію створеної роботизованої платформи представлено на рис. 1. В основу ідеї роботизованої інтелектуальної системи покладено проєкт всюдихідної платформи, розробленої за концепцією малогабаритного «марсохода» позашляхової мобільної платформи, що повторює принципи конструкцій реальних планетарних марсоходів [1]. Основною перевагою такої схеми є висока прохідність, забезпечена низкою технічних рішень.

За основу взято прямокутний каркас, в якому продумані елементи кріплення для батарей та системи керування. Виготовлення корпусу пропонується виконати із алюмінієвого верстатного профілю, який є стійким до корозії та має достатню міцність, також такий матеріал добре обробляється.

До корпусу кріпляться ходова система, яка виконана як «незалежна» підвіска, тобто кожне з шести колес є незалежним відносно інших у позиціонуванні. Ця схема реалізована за рахунок використання взаємозалежних підвісів, яка також дозволяє ефективно розподіляти навантаження між колесами.

Зазначений ефект досягається завдяки рухомим осям, що працюють незалежно одна від одної. Для цього використано спеціально

спроєктований підшипниковий вузол і механізм компенсації нерівностей під час подолання перешкод.

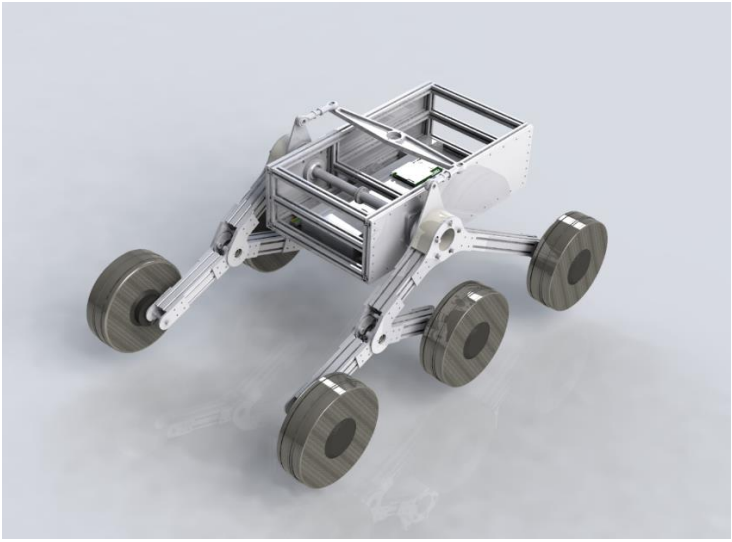


Рисунок 1 – Порівняння роботи методів виявлення об'єктів

Основним елементом є балансирна балка, з'єднана з колесами через шарнірні з'єднання з можливістю регулювання. Така схема забезпечує плавний рух навіть на складних ділянках рельєфу.

Колісні модулі та приводи базуються на електроприводах із мотор-колесами, подібними до тих, що використовуються в сучасних електросамокатах, електроскутерах та інших видах двоколісного електротранспорту. На відміну від типових рішень, у даному проєкті використано колеса зі спеціальною газонаповненою гумою, яка покращує амортизаційні характеристики та плавність руху по кам'янистих, піщаних та комбінованих поверхнях.

Прогнозується, що розроблена конструкція мобільної роботизованої платформи покаже високу ефективність переміщення на різних поверхнях та в різних умовах експлуатації при тестуванні.

Список використаних джерел:

1. Pico, N.; Park, S.-H.; Yi, J.-s.; Moon, H. Six-Wheel Robot Design Methodology and Emergency Control to Prevent the Robot from Falling down the Stairs. Appl. Sci. 2022, 12, 4403. https://doi.org/10.3390/app12094403

УДК 621.865

Ткачук А.Г., к.т.н, доцент
А.Р. Кравчук, PhD
Покляченко О.В., аспірант
Скударнов Б.С., здобувач
Державний університет «Житомирська політехніка»

ПРОЄКТУВАННЯ СИСТЕМИ ЕНЕРГОЗАБЕЗПЕЧЕННЯ ТА ТЕРМОРЕГУЛЯЦІЇ ДЛЯ РОБОТИЗОВАНОЇ ПЛАТФОРМИ

У роботі розглянуто підхід до проєктування інтегрованої системи енергозабезпечення та терморегуляції для мобільної роботизованої платформи, призначеної для роботи в умовах значних коливань температури та нерівномірного навантаження на силові й сенсорні модулі. Актуальність дослідження зумовлена стрімким розширенням сфер застосування наземних роботизованих систем, що виконують завдання підвищеної відповідальності у складних експлуатаційних умовах. У військовій сфері мобільні платформи застосовуються для розвідки, транспортування вантажів, підтримки автономних або дистанційно керованих операцій із підвищеним рівнем ризику для особового складу. В інспекційних роботизованих системах необхідність тривалої автономної роботи та стабільного температурного режиму визначає здатність виконувати моніторинг критичної інфраструктури, технічні огляди або діагностику небезпечних об'єктів. В аварійно-рятувальних сценаріях наявність ефективної енергосистеми є ключовою умовою для забезпечення роботи сенсорних модулів, тепловізорів, систем зв'язку та навігації, що дозволяє роботам виконувати завдання у зонах із обмеженим доступом, токсичним середовищем чи високою ймовірністю повторних руйнувань.

Система енергозабезпечення розглядається як комплекс, що включає акумуляторний блок, модуль керування живленням та силову електроніку. Однією з ключових задач є забезпечення оптимального балансу між енергомісткістю батарейного масиву, масо-габаритними характеристиками платформи та тривалістю автономної роботи. Окрему увагу приділено питанням стабілізації напруги для високочутливих сенсорних модулів, а також захисту силових ліній від перевантаження, коротких замикань і температурних аномалій. Застосування інтелектуальних алгоритмів керування дає змогу прогнозувати споживання енергії залежно від зміни рельєфу, швидкості руху та характеру активних підсистем [1-5].

Система терморегуляції передбачає підтримання робочого діапазону температур для акумуляторів, електроприводів і сенсорних елементів. До її складу входять пасивні та активні компоненти: тепловідвідні елементи, вентиляторні модулі, термоізоляційні матеріали та датчики температури з високою швидкодією. Описано методи оцінювання теплових потоків та моделювання процесів нагрівання під час інтенсивного навантаження. Розроблена концепція враховує можливість роботи в умовах низьких температур, де виникає потреба в попередньому підігріві акумуляторного блоку для запобігання втраті ємності та деградації елементів живлення.

Особлива увага приділяється живленню сенсорного комплексу, до якого входять тепловізор, камера нічного бачення, газоаналізатори, радіаційні датчики та модулі аудіоаналізу. Ці елементи мають низькі допустимі межі коливань напруги та чутливі до імпульсних перешкод.

Для забезпечення стабільності напруги застосовуються такі технічні рішення:

1. Використання багатоступеневих DC/DC-перетворювачів.
2. Ізоляція сенсорних контурів живлення.
3. Алгоритми динамічної компенсації напруги.
4. Терморегуляція в умовах динамічних навантажень.
5. Взаємодія енергетичної та термічної систем з обчислювальним модулем.

Запропонована система енергозабезпечення та терморегуляції забезпечує безперервне й стабільне функціонування роботизованої платформи у широкому діапазоні зовнішніх умов. Особливу увагу приділено стабілізації напруги для високоточних сенсорних модулів.

Список використаних джерел:

1. Chenrui Hu, Optimization Design and Energy Efficiency Management of Robot Power Systems. Academic Journal of Science and Technology, Vol.12, No.1, 2024.

2. Kowalski, G., Glowka, J., Maciaś, M., & Puchalski, S. (2017). Modular robotic system for forensic investigation support. In H. Bouma, F. Carlysle-Davies, R. J. Stokes, & Y. Yitzhaky (Eds.), Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies. SPIE. https://doi.org/10.1117/12.2278735

3. Li J, Murong Li JX, Lai B, et al. Wireless sensor network for indoor air quality monitoring. 2014, 4:6. DOI: 10.1016/j.medengphy.2011.10.011.

4. Lee, M.-F.R. & Nugroho, A., Intelligent Energy Management System for Mobile Robot. Sustainability, 2022.

5. R. Singh, Advanced Power Converters and Learning in Diverse Robotic Systems. Energies, 2023.

УДК 621:317

Перцов А.А., здобувач
Гуменюк А.А., к.т.н., доцент
Громовий О.А., к.т.н., доцент
Янчук В.М., к.т.н., доцент
Державний університет «Житомирська політехніка»

ПЕРЕВАГИ ОПТИМАЛЬНИХ АДАПТИВНИХ СИСТЕМ ПОРІВНЯНО З AI-РІШЕННЯМИ: ПРАКТИЧНИЙ АНАЛІЗ НА ПРИКЛАДІ ТЕХНОЛОГІЙ TIAMA

У сучасному виробництві склотари одна з найбільших проблем – стабільний контроль якості за умов постійної зміни продукції, складу, освітлення та особливостей лінії. На практиці не кожна система справляється з реальними, а не лабораторними умовами. Один із прикладів технології, яка працює стійко саме при таких змінних, – це модуль ATLAS компанії TIAMA. Він відноситься до класу оптимальних адаптивних систем, і саме завдяки цьому підходу поводиться набагато передбачуваніше, ніж більшість рішень, побудованих на нейромережах.

ATLAS – це багатокамерна інспекційна система, яка встановлюється на лінії для контролю пляшок або банок з усіх основних напрямків: горло, плече, корпус і дно. Камер може бути різна кількість, і в цьому одна з його сильних сторін – конфігурація підбирається під конкретну лінію, а не навпаки. Система працює чітко в ритмі конвеєра, зчитуючи зображення кожної пляшки і аналізуючи їх через алгоритми, які розраховані саме на скло: відбиття, нерівності, посічка. ATLAS не намагається "вгадати", що це – його логіка чітка: є відхилення від норми чи немає. Навчання ATLAS – це не той процес, що у нейромереж, де потрібно тисячі прикладів. Тут усе набагато практичніше.

Подається група еталонних виробів. Система сканує їх, аналізує форму, контури, відблиски, геометрію. Створює маски зон допуску – де можливі особливості виробу, і це не брак. Виставляє місцеві пороги чутливості. Система пропонує поправки, якщо бачить підозрілі ділянки. Більша частина роботи – автоматична, на все йде кілька хвилин. Оператор може домальовувати маски власноруч. Це критично важливо при блискучих переходах, декоративних елементах чи технологічних "нерівностях", які виглядають як дефект, але фактично ним не є. Наприклад: посічкоподібний блиск, який у даної моделі вважається нормою. У таких випадках просто замальовується ця зона, і ATLAS перестає сприймати її як небезпеку. Це те, чого AI часто не дозволяє без повного перенавчання.

ATLAS дає простір як для програмних, так і для фізичних

налаштувань.

Можна змінювати:

Технічно: чутливість, пороги, логіку перевірки, структуру масок;

Фізично: положення камер, їхній кут і відстань;

Оптично: напрям і режим підсвітки.

У реальності навіть зміна кольору скла або товщини стінки вже може створити відблиски, які "ламають" нейромережу. Для ATLAS – це просто питання корекції ракурсу чи маски.

Отже, нейромережі мають свою силу, але в контролі скла вони не завжди підходять.

- *Вимога величезних датасетів*

AI потрібно показати тисячі пляшок – нормальних і бракованих – з різними варіантами дефектів. На реальному заводі такої можливості немає. ATLAS працює на основі еталону, а не статистики.

- *Реакція на зміни форми або допустимих відхилень*

Якщо в AI ввести нову модель пляшки або навіть варіацію тієї ж моделі з трохи іншим радіусом плічка – система може почати видавати хибні спрацьовування.

В ATLAS це вирішується корекцією маски – хвилинна справа.

- *Рідкі дефекти*

Якщо дефект трапляється раз на 40 тисяч пляшок –AI просто не вчиться з таких прикладів. У ATLAS алгоритми працюють по фізичному відхиленню, а не по накопиченому досвіду.

- *Зміна освітлення, оптики або камери*

Для AI це зазвичай означає донавчання або повну перебудову моделі.

Для ATLAS – підкрутив кут підсвітки або камеру фізично – працює далі.

Додаткові особливості ATLAS, важливі в реальній роботі

- Підтримка різних профілів для всіх моделей, що працюють на лінії.
- Можливість розширення кількості камер без переписування системи.
- Віртуальна перевірка перед запуском партії, щоби уникнути помилок у налаштуванні.
- Гнучкі маски – система враховує, що скло ніколи не є ідеально однаковим.
- Стійкість до дрібних шумів і артефактів, характерних для гарячої лінії.

ATLAS від TIAMA демонструє, що оптимальні адаптивні системи у промисловій перевірці якості часто є більш практичними, ніж складні AI-рішення. Їхня сила не в "інтелекті", а в передбачуваності, стабільності та контролі. ATLAS забезпечує точність завдяки поєднанню алгоритмів, модульності, можливості ручного доопрацювання масок та гнучкому фізичному налаштуванню камер і освітлення. На відміну від ШІ, який потребує великих датасетів і чутливий до найменших змін у зовнішніх умовах, ATLAS дозволяє швидко адаптуватися до нових партій, форм і реальних виробничих ситуації без ризику втрати якості контролю.

У промисловій практиці найважливіше – не "розумність", а стабільність, повторюваність і можливість миттєво реагувати на реальні умови виробництва. І саме тут оптимальні адаптивні системи, такі як TIAMA ATLAS, мають відчутну і практично підтверджену перевагу.

Список використаних джерел:

1. TIAMA. ATLAS – smart camera check detection beyond expectations. Офіційна сторінка продукту.
URL: https://www.tiama.com/atlas-smart-camera-check-detection/
2. TIAMA. ATLAS System — "atlas" (English version). Інструкція / брошура (PDF) для системи ATLAS. youniverse.tiama.com
3. TIAMA / Glass-Container Industry Catalogue. Atlas: Check Detection by Cameras. PDF-каталог, де описана технологія візуального інспектування тари. glasstec-online.com

Секція 8
СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У БІОМЕДИЦИНІ

УДК 004.7

Ветров А.О., магістрант,
Нікітчук Т.М., к.т.н., доцент
Державний університет «Житомирська політехніка»

БІОМЕДИЧНИЙ МОНІТОРИНГ ГЕЙМЕРІВ: АРХІТЕКТУРА ЗБОРУ ДАНИХ З НОСИМИХ ПРИСТРОЇВ ТА АНАЛІЗ СТАНУ КОРИСТУВАЧА

Інтерактивні ігрові середовища, завдяки своїй здатності генерувати контрольовані багатокористувацькі стимули, все частіше використовуються не лише для розваг, а й для глибокого дослідження психологічних і фізіологічних реакцій користувачів. Використання біометричних сенсорів під час ігрової взаємодії – таких, як монітори варіабельності серцевого ритму (HRV), датчики шкірно-гальванічної реакції (GSR) для вимірювання емоційного збудження чи навіть портативні ЕЕГ-системи для оцінки когнітивного навантаження – дозволяє об'єктивно дослідити емоційний стан, рівень стресу та концентрацію уваги конкретної людини. Актуальність теми посилюється тим, що, не зважаючи на стрімке поширення носимих сенсорів (від фітнес-браслетів до спеціалізованих дослідницьких пристроїв), на сьогодні відсутня єдина гнучка система, здатна інтегрувати біометричні дані у реальному часі під час ігрових сесій. Ця проблема є особливо гострою через високу фрагментованість ринку: дані передаються через різні протоколи. Основною проблемою, що звідси випливає, є розрізненість даних, суттєва різниця у форматах та частоті дискретизації їх передавання, що унеможливлює їх сумісне використання, а також нагальна потреба в зручній, уніфікованій візуалізації для аналітики та прийняття рішень.

Метою даного дослідження є підвищення ефективності аналізу стану користувачів ігрових додатків шляхом розробки архітектури та програмних засобів системи, що вирішує ключову проблему технологічної та семантичної розрізненості даних. Досягнення мети передбачає створення уніфікованого програмного конвеєра, який дозволить системі підключатися до широкого спектру носимих пристроїв, використовуючи їх нативні протоколи. Така система має інтегрувати в реальному часі різнорідні потоки даних, уніфікувати їх

формати, приводячи все до єдиної, стандартизованої моделі даних та забезпечити синхронізовану візуалізацію цих показників для негайного аналізу дослідником або розробником.

Об’єктом дослідження є складний процес збору, потокової обробки та багатовимірного аналізу біометричних даних користувачів, що відбувається у реальному часі під час безпосередньої взаємодії гравця з ігровими додатками. Цей процес розглядається в контексті гетерогенного середовища, що включає різні пристрої, операційні системи та ігрові платформи.

Предметом дослідження виступають архітектурні моделі, методи та алгоритми уніфікації і синхронізації даних, а також конкретні програмні засоби, необхідні для неінвазивної інтеграції в ігровий процес та ефективної стандартизації фізіологічних й психоемоційних показників.

У результаті дослідження буде створено програмний модуль до кросплатформної системи, який забезпечить надійну та гнучку інтеграцію біомедичних даних користувачів безпосередньо в процес ігрової взаємодії. Отримана розробка зможе застосовуватися для фундаментального аналізу впливу ігрових середовищ та специфічних ігрових механік на фізіологічний та емоційний стан користувачів. Ключовою прикладною цінністю даного дослідження є можливість реалізації механізмів адаптивного керування ігровим процесом, таких, як динамічне регулювання складності гри на основі рівня стресу гравця або зміна наративу відповідно до його емоційної реакції. Це відкриває шлях для подальших досліджень у сфері біомедичної інженерії, психофізіології, людино-машинної взаємодії та розробки терапевтичних ігрових додатків із зворотним біологічним зв'язком.

Список використаних джерел:

1. Cheah, I., Shimul, A. S., & Phau, I. (2022). Motivations of playing digital games: A review and research agenda. Psychology & Marketing, 39(5), 937-950.

2. Koshy, A., & Koshy, G. M. (2020). "The potential of physiological monitoring technologies in esports." International Journal of Esports.

3. Sun, W., Guo, Z., Yang, Z., Wu, Y., Lan, W., Liao, Y., & Liu, Y. (2022). A review of recent advances in vital signals monitoring of sports and health via flexible wearable sensors. Sensors, 22(20), 7784.

4. Dave, D. M. K., & Mittapally, B. K. (2024). Data integration and interoperability in IoT: challenges, strategies and future direction. Int. J. Comput. Eng. Technol.(IJCET), 15, 45-60.

5. Nahavandi, D., Alizadehsani, R., Khosravi, A., & Acharya, U. R. (2022). Application of artificial intelligence in wearable devices: Opportunities and challenges. Computer Methods and Programs in Biomedicine, 213, 106541.

УДК 796: 617.572-053.8-085

Коренівська О.Л., к.т.н., доцент,
Бенедицький В.Б., ст. викладач,
Сергійчук М.В., здобувач,
Галанзовська В.О., здобувач
Державний університет «Житомирська політехніка»

СИСТЕМА ГІБРИДНОГО КЕРУВАННЯ ПРОТЕЗОМ ВЕРХНЬОЇ КІНЦІВКИ

Сучасні протези верхніх кінцівок дедалі більше наближаються за функціональністю до біологічної руки, проте одним з ключових обмежень залишається ефективність системи керування. Традиційні підходи, що реалізують біоелектричне або міотонічне керування протезом, залежать від якості залишкової м'язової активності та часто мають низьку точність через шум сигналів, втому м'язів, складність калібрування або фізіологічні обмеження користувача.

У зв'язку з цим спостерігається потреба в гібридних системах керування, які об'єднують кілька каналів взаємодії людини з протезом. Такий комплексний підхід дозволяє компенсувати недоліки окремих технологій та забезпечити більшу надійність та точність виконання рухів, кращу адаптацію до стану користувача (при м'язовій втомі можна переключитися на голосове або зорове керування) тощо.

У роботі [1] описано переваги та недоліки різних альтернативних способів керування протезами кінцівок. В даній публікації розглянемо подальшу розробку та синтез гібридної системи керування протезом (рис. 1), яка поєднує три незалежні канали керування: міотонічний, голосовий та комп'ютерний зір.

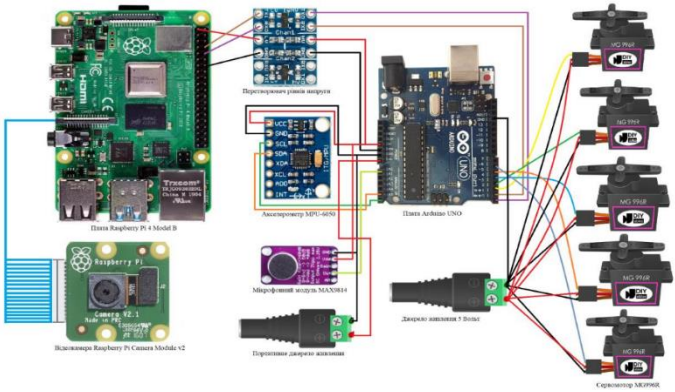


Рисунок 1 – Структура гібридної системи керування протезом

В основі системи взаємодія Raspberry Pi 4, Arduino UNO, набору сенсорних модулів та сервоприводів MG996R/MG958R.

Raspberry Pi виступає центральним модулем логіки та штучного інтелекту і забезпечує обробку даних: голосове розпізнавання, обробку зображення з камери та реалізацію алгоритмів комп'ютерного зору. Відеокамера Raspberry Pi Camera V2 використовується для аналізу жестів, позиції предметів та визначення цільових траєкторій.

Мікрофонний модуль MAX9814 сприймає голосове керування.

Акселерометр MPU-6050 забезпечує стабілізацію руху та аналіз мікроколивань для підвищення плавності керування.

Міотонічний модуль реєструє електроміотонічний сигнал м'язів для прямого керування захватом.

Arduino UNO виконує роль низькорівневого контролера, який отримує команди від Raspberry Pi та перетворює їх у сигнали керування сервоприводами кисті протеза. Приводи MG996R/MG958R реалізують рухи пальців, кисті та зап'ястя.

Залежно від режиму система розпізнає: об'єкти, жести, положення руки та орієнтацію предмета, траєкторію руху, відстань до цілі. Такий підхід дозволяє підвищити точність, зручність та адаптивність роботи протеза для користувача, а також забезпечує резервування в разі відмови одного з каналів керування.

Розроблена система забезпечує природніші рухи протеза, розширює функціональні можливості кінцівки та підвищує рівень автономності користувача. Гібридне керування створює основу для інтелектуальних протезів нового покоління з високим ступенем інтерактивності та адаптивності, у поєднанні з алгоритмами штучного інтелекту дозволяє не лише виконувати команди, а й аналізувати оточення, прогнозувати рухи та забезпечувати напівавтономні дії. Такі системи відкривають шлях до створення протезів, які не просто виконують команди, а здатні розуміти контекст, передбачати дії та взаємодіяти із навколишнім середовищем на рівні справжньої кінцівки.

Список використаних джерел:

1. Сергійчук М.В., Галанзовська В.О., Коренівська О.Л., Бенедицький В.Б. Способи керування протезом з використанням штучного інтелекту. Тези XV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології», 28 – 29 березня 2025 року. Житомир : «Житомирська політехніка», 2025. С. 252-253..

2. Сергійчук М.В. Розробка гібридної системи керування біонічним протезом руки. Кваліфікаційна робота. Житомир. 2025. – 64 с.

УДК 606:61

Korenivska O.L., Ph.D., Associate Professor,
Nikitchuk T.M., Ph.D., Associate Professor,
Bogoyavlenska Y.V., Ph.D., Associate Professor
Zhytomyr Polytechnic State University

INTRODUCTION OF MODERN MEDICAL MONITORING SYSTEMS INTO THE TRAINING OF BIOMEDICAL ENGINEERING SPECIALISTS

Current trends in the digitisation of medicine require higher education institutions to provide students with access to modern means of measuring human vital signs and skills in working with integrated telemedicine systems. High-quality practical training of specialists, especially in the G22 Biomedical Engineering programme, should include working with devices that measure blood pressure, heart rate, blood oxygen saturation, body temperature, respiratory rate, ECG and other parameters.

In order to improve the quality of practical training and strengthen research capacity, the medical devices and systems laboratory was modernised as part of the Horizon Europe 'WIDE AcrossEU' project. A key element of the modernisation was the addition of a modern medical vital signs monitor and the purchase of spirometry devices and telemedicine devices. This equipment opens up opportunities for the educational process and experimental research in the field of physiology and biomedical measurements.

The purchased laboratory base is a multifunctional tool that can be used to train students majoring in Biomedical Engineering in several key areas:

1. Practical and laboratory work

A medical monitor of vital signs, equipped with sensors for measuring blood pressure, heart rate, saturation and body temperature, allows students to acquire the necessary practical skills required by the updated educational programmes.

Students learn about the structure and principles of monitoring systems, as well as the basics of specific methods for measuring physiological parameters: pulse oximetry (determination of blood saturation SpO_2, heart rate), methods for measuring pressure and principles for measuring temperature, ECG, and respiratory parameters. Training in the practical aspects of creating and configuring a medical network in a medical facility with the connection of diagnostic equipment and data transfer to a central storage facility. Training in setting up patient records. Students record,

process and analyse human physiological parameters obtained from the monitor. Basics of medical data processing.

2. Research and experimental studies

The equipment opens up wide opportunities for conducting applied physiological and bioengineering research: this includes studying the body's adaptive responses to various factors, primarily increased physical and mental stress. Research into the influence of external factors, such as peripheral blood supply and movement, on the accuracy and occurrence of artefacts when measuring saturation (SpO_2) and heart rate (PPG measurement).

3. Development of telemedicine and IoT systems

As part of their work with the equipment, students can participate in the development of modern technological solutions that are particularly relevant to the field of telemedicine. Specifically, this involves developing the concept of IoT (Internet of Things) architecture for the secure transmission of biometric data from a monitoring device to a doctor or to medical data storage servers.

4. Verification of the performance and reliability of various diagnostic and therapeutic methods. Verification of the accuracy of physiological parameter measurements of proprietary devices.

Thus, the specified equipment has become an important element of the educational and scientific infrastructure, providing opportunities for laboratory work, experiments and research in the field of physiology, biomedical engineering and

List of sources used:

1. Korenivska O., Benedytskyi V., Denysiuk D. Biomedical engineering in sports medicine. XXXIII International scientific and practical conference «State of Scientific Research: Methods and Prospects for Development Across Different Fields», August 7-9, 2024. Graz, Austria. International Scientific Unity, 2024. p. 93 - 97.

The paper has been developed within the framework of the project "Widen performance in research and innovation capacity and competence Across EU" / "WIDE AcrossEU" 101 158 561 Horizon Europe program. Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

УДК 606:61

Фещенко С.В., аспірант,
Мацієвський В.А., аспірант,
Нікітчук Т.М., к.т.н., доцент,
Марцева Л.А., д.пед.н., професор
Державний університет «Житомирська політехніка»

РОЗРОБКА ТА АПРОБАЦІЯ АПАРАТНО-ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ МОНІТОРИНГУ ФУНКЦІОНАЛЬНОГО СТАНУ ОПЕРАТОРІВ ЕРГАТИЧНИХ СИСТЕМ

Надійність функціонування сучасних стратегічних об'єктів значною мірою залежить від психофізіологічного стану людини-оператора. Проблема полягає у виникненні «неврозу відкладеної дії» – стану, коли високе нервове напруження не супроводжується м’язовою розрядкою, що призводить до вегетативного дисбалансу.

Сучасні людино-машинні (ергатичні) системи (рис.1) характеризуються стрімким зростанням обсягів інформації та швидкості технологічних процесів. У таких умовах людина-оператор стає ключовою, але водночас найбільш вразливою ланкою управління. На відміну від технічних засобів, надійність яких визначається інженерними рішеннями, надійність людини лімітується її біологічними можливостями, які еволюційно не були пристосовані до специфіки сучасної операторської праці (рис. 1.2).

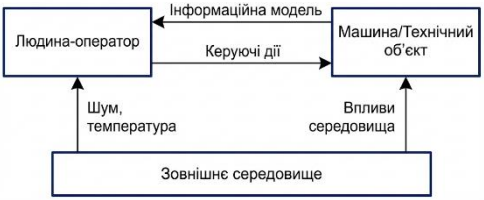


Рисунок 1 – Структурна схема ергатичної системи

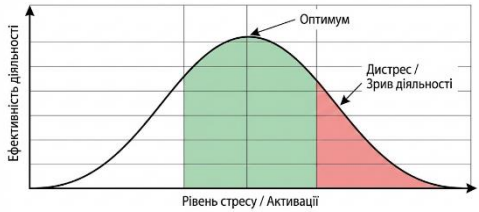


Рисунок 2 – Залежність ефективності діяльності оператора від рівня психоемоційного напруження (за законом Єркса-Додсона)

У роботі представлено результати розробки мобільної системи «HRV-Analysis System» для амбулаторного контролю серцевого ритму. Обґрунтовано архітектуру системи та алгоритми цифрової обробки сигналів для виявлення ознак професійної втоми операторів у режимі in situ.

Для вирішення задачі моніторингу було спроектовано апаратно-програмний комплекс (рис. 3), що складається з:

– мобільного модуля реєстрації, який забезпечує зняття ЕКГ-сигналу з частотою дискретизації 250 Гц та бездротову передачу даних через Bluetooth;

– програмного модуля аналізу, зокрема для детекції R-зубців за пороговим алгоритмом та розрахунку спектральних показників методом швидкого перетворення Фур'є (FFT).

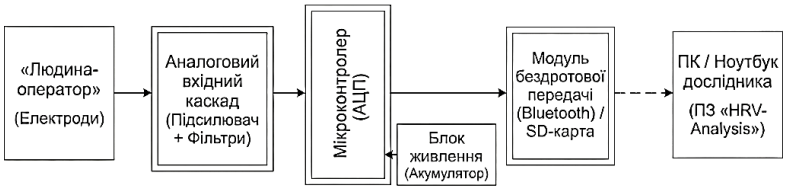


Рисунок 3 – Структурна схема апаратно-програмного комплексу «HRV-Analysis System»

Апробація комплексу на вибірці з 30 операторів підтвердила його стійкість до рухових артефактів та високу точність формування ритмограми (до 1 мс) у реальних виробничих умовах.

Запропонований комплекс дозволяє проводити доклінічну діагностику зриву адаптації без переривання технологічного процесу. Отримані дані є фундаментом для створення автоматизованих систем підтримки прийняття рішень щодо допуску персоналу до виконання критичних завдань.

Список використаних джерел:

1. Страхова О. П. Система автоматизованого контролю функціонального стану людини, що перебуває у ергатичній системі «особа – комп'ютер» : дис. канд. біол. наук : 14.03.11 / Страхова Оксана Петрівна. – Запоріжжя,2018. – 236с.

2. Heart Rate Variability. Standards of measurement, physiological interpretation, and clinical use / Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology // Circulation. – 1996. – Vol. 93, № 5. – P. 1043–1065.

3. Майданник В. Г. Оцінка варіабельності серцевого ритму та адаптаційних можливостей у дітей, хворих на цукровий діабет І типу / В. Г. Майданник [та ін.] // Вісник Вінницького національного медичного університету. – 2020. – Т. 24, № 3. – С. 403–409.

Богатов Д.В., магістрант,
Сімчук А.Р., аспірант,
Нікітчук В.С., студентка,
Корніюк А.В., ст. викладач
Державний університет «Житомирська політехніка»

МАРКЕРИ ВАРІАБЕЛЬНОСТІ СЕРЦЕВОГО РИТМУ В ОЦІНЦІ «ЦІНИ АДАПТАЦІЇ» ОПЕРАТОРІВ ПРИ ПСИХОЕМОЦІЙНОМУ НАВАНТАЖЕННІ

Діяльність операторів характеризується режимом «операційного спокою», який приховує стан гіпермобілізації регуляторних систем. Метою дослідження є визначення найбільш інформативних критеріїв втоми на основі теорії двоконтурної моделі регуляції Р. Баєвського.

Згідно з теорією функціональних систем та працями Р. Баєвського, варіабельність серцевого ритму (ВСР) відображає баланс між симпатичним та парасимпатичним відділами ВНС. Зниження параметрів ВСР свідчить про напруження регуляторних систем та зниження адаптаційних резервів організму, що характерно як для операторів, так і для осіб із хронічними захворюваннями, наприклад, діабетом, де також спостерігається вегетативна дисфункція.

Сутність методу полягає у вимірюванні часових інтервалів між послідовними R-зубцями електрокардіограми (R-R інтервали). У здорової людини в стані спокою ці інтервали неоднакові, що свідчить про домінування автономного (парасимпатичного) контуру регуляції та високі адаптаційні можливості. Зниження варіабельності, навпаки, є маркером посилення симпатичної активності та централізації управління

Для діагностики стресового стану операторів найбільш інформативними є наступні групи показників, які детально аналізуються у сучасних клінічних дослідженнях [1, 2].

Для моніторингу стану операторів доцільно використовувати комплекс показників, які дозволяють різнобічно оцінити роботу регуляторних систем:

1. Часові показники/показники часового ряду:

- SDNN (стандартне відхилення R-R інтервалів) – є мірою загальної варіабельності та відображає сумарний ефект вегетативної регуляції.

Його зниження є універсальним маркером виснаження адаптаційних резервів;

- RMSSD (квадратний корінь із середнього квадрата різниць послідовних інтервалів) – основний маркер активності парасимпатичної ланки. Падіння цього показника є першою ознакою втоми та зниження відновлювальних можливостей оператора.

2. Спектральні показники /показники спектрального аналізу:

- LF – хвилі низької частоти, пов'язані з активністю симпатичного відділу, барорефлекторною регуляцією та симпатичною регуляцією судинного тонусу;
- HF – високочастотні хвилі, що відображають дихальну аритмію та вагусний контроль – маркери дихальної аритмії та вагусного впливу;
- LF/HF – коефіцієнт вагосимпатичного балансу. Зростання цього співвідношення свідчить про переважання процесів збудження над процесами гальмування, що характерно для психоемоційного стресу.

3. Геометричні методи та Індекс Напруги:

- індекс напруги (SI) – розрахунковий показник, який характеризує ступінь жорсткості ритму. Високі значення SI вказують на виражену централізацію управління ритмом та стан дистресу, що характерно для психоемоційного стресу [2].

Рисунок 1 підтверджує твердження про «активацію симпато-адреналової системи» та «зміну структури ритму».

Використання цих показників дозволяє виявити доклінічні зміни функціонального стану оператора, прогнозувати зниження надійності його роботи та своєчасно вживати заходів для корекції (відпочинок, психологічне розвантаження), запобігаючи помилкам та аваріям.

Зростання Індексу напруги (SI) у 6,6 раза свідчить про жорстку централізацію управління ритмом та «вимкнення» автономного контуру регуляції. Кореляційний аналіз підтвердив сильний зворотний зв'язок між SI та загальною варіабельністю ($r = -0,82$), що робить ці параметри надійними предикторами функціонального стану.

Отже, критичним рівнем для операторів є значення $SI > 300$ у.о., що вимагає негайної технічної перерви. Використання геометричного аналізу (трансформація «Трикутника Баєвського» у вузьку «голку») дозволяє візуалізувати стресовий стан для оперативного контролю.

Список використаних джерел:

1. Майданник В. Г. Оцінка варіабельності серцевого ритму та адаптаційних можливостей у дітей, хворих на цукровий діабет I типу / В. Г. Майданник [та ін.] // Вісник Вінницького національного медичного університету. – 2020. – Т. 24, № 3. – С. 403–409.

2. Голдовський Б. М. Вплив стресу на показники варіабельності серцевого ритму в співробітників виїзного персоналу швидкої медичної допомоги / Б. М. Голдовський // Медицина невідкладних станів. – 2015. – № 8 (71). – С. 92–95.

Квітка Р.В., магістрант,
Мацієвський В.А., аспірант,
Нікітчук Т. М., к.т.н., доцент,
Державний університет «Житомирська політехніка»

РОЗРОБКА БІОТЕХНІЧНОЇ СИСТЕМИ МОНІТОРИНГУ СТАНУ СЕРЦЕВО-СУДИННОЇ СИСТЕМИ ДЛЯ РАННЬОЇ ДІАГНОСТИКИ ВІРУСНИХ ЗАХВОРЮВАНЬ

Гострі респіраторні вірусні інфекції (ГРВІ) та наслідки пандемії COVID-19 продемонстрували системний токсичний вплив вірусів на організм, що часто призводить до ускладнень з боку серцево-судинної системи1. Традиційні методи діагностики в амбулаторних умовах обмежені епізодичними вимірюваннями, що не дозволяє фіксувати ранні регуляторні зміни. Актуальність роботи полягає у створенні доступної неінвазивної системи для моніторингу стану пацієнта в режимі реального часу для зниження ризику важких кардіологічних ускладнень.

При проектуванні системи неінвазивного моніторингу стану серцево-судинної системи у хворих на ГРВІ необхідно дотримуватися принципів модульності, енергоефективності та ергономічності. Система розглядається як сукупність апаратних та програмних засобів, що забезпечують замкнений цикл обробки інформації: від реєстрації первинного фотоплетизмографічного сигналу до візуалізації діагностичних висновків.

На рис. 1 представлена узагальнена структурна схема розроблюваної системи.

Основними функціональними блоками системи є:

Для реалізації системи обрано метод фотоплетизмографії, що забезпечує мультифункціональність: одночасний контроль сатурації (SpO_2), частоти серцевих скорочень (ЧСС) та варіабельності пульсу. Апаратна частина базується на мікроконтролері ESP32 та інтегрованому сенсорі MAX30102 з 18-бітним АЦП, що дозволяє реєструвати сигнал навіть при низькій периферійній перфузії.

Зовнішній термінал (смартфон/ПК) виконує функцію розширеної аналітики. Оскільки розрахунок спектральних показників ВСР та індексу Баєвського потребує значних обчислювальних ресурсів та

накопичення масивів даних (гістограм), доцільно перенести ці операції на бік потужного процесора смартфона або хмарного сервера.

Розроблене алгоритмічне забезпечення включає:

– каскадну цифрову фільтрацію для мінімізації впливу артефактів руху;

– адаптивний пороговий алгоритм детекції піків пульсової хвилі;

– програмну логіку автоматичної генерації статусу STATUS_STRESS_WARNING при стабільному падінні показника RMSSD нижче 20 мс протягом 3 хвилин.

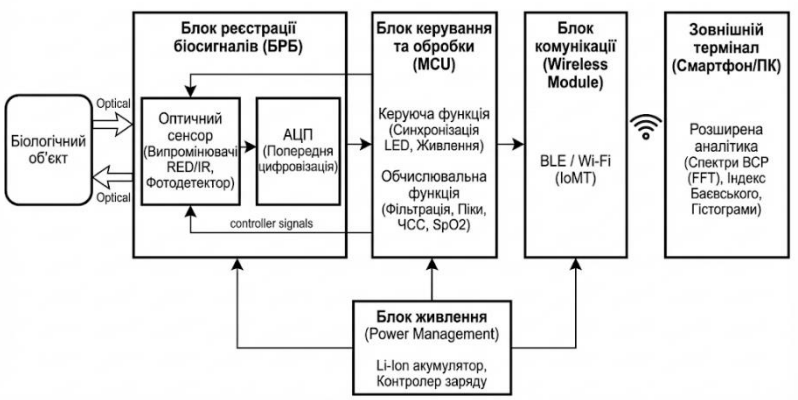


Рисунок 1 – Узагальнена структурна схема розроблюваної системи

Для інтеграції в екосистему IoMT організовано енергоефективний канал передачі даних за протоколом Bluetooth Low Energy.

Запропонована архітектура системи забезпечує високу точність вимірювань та надійність передачі даних. Використання сучасних алгоритмів обробки біосигналів дозволяє виявляти ознаки виснаження адаптаційних резервів організму ще до появи критичних клінічних симптомів.

Список використаних джерел:

[1] Ferrera, F., Ferrero, F., Blanco, C., Viera, J., Vega, M., Blanco, J. (2006).

Design of a low-cost instrument for pulse oximetry. Proceedings of the IEEE Instrumentation and Measurement Technology Conference, pp. 573-577.

[2] Hoff, D. Zhang, R. Stalter, T. and Carlson, M. (2003). Pulse Oximetry. Undergraduate Thesis. Electrical and Computer Engineering, North Carolina State University, USA.

[3] Deni, H. Muratore, D. M. Malkin, R A. (2005). Development of a Pulse Oximeter Analyzer for the Developing World. Proceedings of the IEEE 31st Annual Northeast Bio-engineering Conference. pp. 227-228.

УДК 004.8

Янчук Е.А., магістрант
Нікітчук Т.М., к.т.н., доцент
Коренівська О.Л., к.т.н., доцент
Державний університет «Житомирська політехніка»

ІНТЕРФЕЙСИ МОЗОК–КОМП'ЮТЕР: СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ

Інтерфейси мозок-комп'ютер (ІМК, англ. Brain-Computer Interface, BCI) є перспективним напрямом розвитку інформаційних технологій, що дозволяє створювати прямий канал взаємодії між мозком людини та зовнішніми комп'ютерними системами. Такі технології відкривають нові можливості у сфері медицини, реабілітації, нейрокібернетики та автоматизованих систем керування.

Згідно з дослідженням Elashmawi W.H. та ін. ІМК поділяються на інвазивні, напівінвазивні та неінвазивні (табл.1)**.** Найбільш поширеними є неінвазивні системи на основі електроенцефалографії (ЕЕГ), оскільки вони є безпечними, відносно недорогими та не потребують хірургічного втручання. Основними парадигмами роботи таких систем є моторне уявлення (MI), потенціали P300 та стимульовані зорові потенціали (SSVEP). Це означає, що в майбутньому можна створити системи, які зможуть розпізнавати думки та наміри людини, перетворюючи їх на команди для комп'ютерів або навіть роботизованих пристроїв. Наприклад, вже були успішно проведені експерименти, коли учасники могли керувати курсором на екрані лише за допомогою думок.

Таблиця 1

Технологія	Метод	Застосування	Стан
Neuralink	Імплантація електродів	Терапія нейрологічних розладів	Експериментальна фаза
EEG	Нонінвазивні датчики	Моніторинг активності мозку	Застосовується
ECoG	Часткова імплантація	Контроль протезів	Клінічне застосування
fMRI	Сканування мозку	Дослідження мозку	Наукові дослідження

Значного прогресу у розробці ІМК вдалося досягти завдяки застосуванню методів глибокого навчання. Як зазначають Hossain K.M. та ін., згорткові та рекурентні нейронні мережі дають змогу покращити точність розпізнавання мозкових сигналів і забезпечити адаптацію системи до індивідуальних особливостей користувача. Попри це, залишаються проблеми, пов'язані з нестачею якісних навчальних вибірок та високою варіативністю даних між різними користувачами.

Новітні дослідження демонструють перехід від теоретичних до практичних рішень. Так, у роботі Ding Y. та ін. представлено неінвазивну систему ІМК, яка забезпечує реальне керування рухами роботизованої руки на основі ЕЕГ-сигналів у режимі реального часу. Це доводить можливість створення ефективних допоміжних технологій для людей з порушеннями рухових функцій.

Отже, розвиток інтерфейсів мозок-комп'ютер демонструє стійку тенденцію інтеграції нейрофізіологічних методів із штучним інтелектом.

Мета роботи – проаналізувати сучасні підходи до побудови інтерфейсів мозок–комп'ютер, визначити їхні ключові переваги та обмеження, а також оцінити перспективи застосування таких технологій у біомедичній інженерії. У роботі використано методи оглядового аналізу наукових публікацій, порівняння існуючих технічних рішень та узагальнення результатів сучасних досліджень у сфері ІМК. Проблематика розвитку інтерфейсів мозок-комп'ютер пов'язана насамперед із низьким співвідношенням сигнал/шум у ЕЕГ-сигналах, значною індивідуальною варіативністю нейронної активності, складністю адаптації алгоритмів до конкретного користувача та обмеженнями неінвазивних підходів у порівнянні з інвазивними системами. Додатково актуальними залишаються питання стабільності роботи ІМК, підвищення швидкодії, зменшення затримок та забезпечення надійної класифікації мозкових сигналів у реальному часі. Саме ці аспекти істотно впливають на можливість практичного впровадження ІМК у медичну реабілітацію, системи керування протезами та асистивні технології.

Список використаних джерел:

1. Elashmawi W.H. et al. A Comprehensive Review on Brain–Computer Interface (BCI). Applied Sciences. 2024.

2. Hossain K.M. et al. Status of Deep Learning for EEG-based Brain–Computer Interfaces. Frontiers in Computational Neuroscience. 2023.

3. Ding Y. et al. EEG-based Brain–Computer Interface Enables Real-time Noninvasive Robotic Control. Nature Communications. 2025.

4. Інтерфейси "мозок-комп'ютер" та розвиток нейроінтернету. Веб-ресурс: https://maxnet.ua/blog/internet-tendenciyi-za-yakimi-varto-stezhiti-u-nastupni-5-rokiv/
5. Підключення мозку до інтернету. Веб-ресурс: https://proit.com.ua/news/pidklyuchennya-mozku-do-internetu-mozhlyvosti-ta-vyklyky/

УДК 004.9:61

Дудка В.Р., магістрант
Дніпровський державний технічний університет

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У БІОМЕДИЦИНІ

Біомедицина швидко змінюється під впливом інформаційних технологій, формуючи нову парадигму охорони здоров'я – точну, персоналізовану та доступну. Блокчейн-технології забезпечують захищений обмін медичними даними між лікарнями та пацієнтами, підвищуючи довіру до системи охорони здоров'я. Штучний інтелект допомагає лікарям у діагностиці: аналізує великі масиви даних, розпізнає патології на зображеннях, прогнозує ризики серцево-судинних та онкологічних хвороб, зменшуючи кількість помилок [1, 2].

У Житомирській політехніці в рамках програми «Біомедичний комп'ютинг» студенти вивчають методи обробки даних та моделювання біологічних процесів. Інтернет речей (IoT) у медицині створює мережу «розумних» пристроїв, що постійно відстежують стан здоров'я пацієнтів. Телемедицина й мобільні додатки забезпечують дистанційний моніторинг: контроль тиску, рівня глюкози чи серцевого ритму з автоматичною передачею даних лікарю. У межах дисципліни «Розробка додатків медичного спрямування» студенти створюють прототипи телемедичних систем, інтегрованих із електронною системою охорони здоров'я України [3].

3D-друк відкриває нові можливості для біоінженерії: індивідуальні протези та імпланти вже застосовуються, а біодрук тканин і органів дає перспективи регенеративної медицини [4]. Хмарні технології дозволяють зберігати та обробляти великі масиви медичних даних, забезпечуючи доступ лікарів до інформації у будь-який час. У наукових збірниках Житомирської політехніки представлені роботи з моделювання біологічних процесів та використання 3D-технологій.

Робототехніка забезпечує точність операцій та допомагає у реабілітації (екзоскелети). Нанотехнології роблять терапію ефективнішою: наночастинки доставляють ліки безпосередньо до уражених клітин, а «розумні» системи контролю вивільнення реагують на зміни мікросередовища пухлини.

Біоінформатика стала нервовою системою сучасної біомедицини. Вона аналізує дані від геномних секвенувань до електронних карток пацієнтів, відкриваючи нові закономірності розвитку хвороб і створюючи персоналізовані схеми лікування.

Разом із можливостями виникають виклики: захист персональних даних, висока вартість інновацій, потреба у цифрових навичках медиків та етичні аспекти використання штучного інтелекту.Великі дані (Big Data) у біомедицині допомагають виявляти приховані закономірності та прогнозувати розвиток захворювань на популяційному рівні [5].

Висновки. Інформаційні технології стали невід'ємною складовою біомедицини, забезпечуючи точність, персоналізацію та доступність медичних послуг. Їх інтеграція відкриває перспективи для розвитку регенеративної медицини, телемедицини та біоінженерії. Водночас важливо враховувати виклики – від захисту даних до етики застосування штучного інтелекту. Віртуальна та доповнена реальність застосовуються для навчання медиків, моделювання операцій та реабілітації пацієнтів. Українські університети, зокрема Житомирська політехніка, відіграють ключову роль у підготовці фахівців, здатних реалізувати ці можливості.

Список використаних джерел:

1. Гриценко, В. І., Котова, А. Б., Вовк, М. І., Кіфоренко, С. І., Бєлов, В. М. Інформаційні технології в біології та медицині. Київ: Наукова думка, 2007. 256 с.

2. Жолос, О. В. Сучасні інформаційні технології у біології. Київ: КНУ ім. Т. Шевченка, 2022. 312 с.

3. Житомирська політехніка. Наукові статті конференції «Сучасні інформаційні технології у медицині та біології». Житомир: ЖДТУ, 2021–2024. Електронний ресурс.

4. Житомирська політехніка. Освітня програма «Біомедична інженерія (Біомедичний комп'ютинг)». Житомир: Факультет ІКТ, 2023. 54 с.

5. Житомирська політехніка. Навчальна дисципліна «Розробка додатків медичного спрямування». Житомир: Факультет ІКТ, 2022.

Секція 1. МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Терещук В. О., Чижмотря О. В.	Технології оптичного розпізнавання символів та їх застосування	3
Mykola Turchyn, Olena Chyzhmotria, Iryna Dmytrenko	Seaborn as a tool for effective work with categorical data	5
Mykola Turchyn, Olena Chyzhmotria, Iryna Dmytrenko	Seaborn as a tool for effective work with numerical data	7
Roman Kormysh, Olena Chyzhmotria, Iryna Dmytrenko	The robustness of the naive bayes classifier to data imbalances in first aid datasets	9
Roman Kormysh, Olena Chyzhmotria, Iryna Dmytrenko	The role of symptom severity in improving naive bayes-based first aid diagnosis accuracy	11
Башманівський М. О., Чижмотря О. В., Дмитренко І. А.	Архітектура full-stack застосунку для інтелектуального аналізу reddit з використанням локальних великих мовних моделей	13
Башманівський М. О., Чижмотря О. В., Дмитренко І. А.	Гібридна методологія аналізу контенту Reddit: поєднання класичного NLP та генеративних моделей для узагальнення та виявлення тональності	15
Груницький Д. С., Чижмотря О. В., Дмитренко І. А.	Виділення і структуризація ключових понять у текстових навчальних матеріалах	17
Груницький Д. С., Чижмотря О. В., Дмитренко І. А.	Інтеграція чат-ботів	19
Груницький Д. С., Чижмотря О. В., Дмитренко І. А.	Система створення персоналізованих конспектів	21
Shostak Anatoliy	On modification of the algorithm for constructing an AVL tree	23

Кирилова Є. В., Шушура О. М., Соломаха С. А.	Аналітичний огляд сучасних архітектур DNN, CNN, RNN та Transformer у задачах регресії та класифікації	25
Рябко О. Д., Єфремов Ю. М.	Актуальність розробки системи управління закладами харчування	27
Рябко О. Д. Єфремов Ю. М.	Аналіз існуючих систем управління закладами харчування	29
Новічков Є. М., Чижмотря О. В.	Використання Bi-LSTM моделі з механізмом уваги для автоматичного тегування тексту	31
Трибюк В.О., Фант М.О.	Стек технологій для реалізації платформи для косметичних колекцій та блогу	33
Козлик С. О., Фант М. О.	Технологічний стек для системи керування процесами видавництва	35
Бойко О. Р., Хрущак С. В.	Vibe coding: сучасні інструменти та підходи до програмування на основі штучного інтелекту	37
Дрожак В. Т., Єфремов Ю. М.	Веб платформа для пошуку та організації студентських стажувань	39
Волинець А. Ю., Вакалюк Т. А.	Абстрактна математична модель для побудови реактивних систем	41
Єфремов Ю. М., Коломієць А. О.	Гібридні алгоритми у рекомендаційних системах: поєднання контентного та колаборативного підходів	43
Єфремов Ю. М., Коломієць А. О.	Оптимізація точності рекомендацій за допомогою методів глибинного навчання	45
Обміняний Д. С., Чижмотря О. В.	Дослідження моделей прогнозування ризиків у життєвому циклі IT-проєктів на основі інтелектуальних технологій	47
Обміняний Д. С., Чижмотря О. В.	Інтелектуальна система підтримки прийняття рішень для планування та оптимізації ресурсів IT-проєктів	49

Лупашина А. А., Фант М. О., Громський О. О., Нерода С. І.	Архітектура та технічна реалізація веб-системи управління студентським гуртожитком	51
Харченко Ю. В., Вакалюк Т. А.	Проблема холодного старту в рекомендаційних алгоритмах для книжкових веб-додатків	53
Харченко Ю. В., Вакалюк Т. А.	Гібридні рекомендаційні алгоритми для персоналізованого підбору книжок	55
Затилюк Д. О., Локтікова Т. М.	Особливості розробки онлайн-бібліотеки з персоналізованими функціями читання	57
Пилипенко Є. В., Локтікова Т. М., Кушнір Н. О.	Сучасний стан і тенденції розвитку сервісів для бронювання житла	59
Купрієнко М. С., Варганова Д. О.	Моделювання перетину двох прямих у просторі засобами програмування	61
Паламарчук І. С., Локтікова Т. М., Лисогор Ю. І.	Дослідження принципів побудови та проєктування системи управління виробництвом крафтових м’ясних виробів	63
Голенко М. Ю.	Аналіз методів формування теплових карт для адаптивного покращення зображень з БПЛА	65

Секція 2. КОМП’ЮТЕРНА ІНЖЕНЕРІЯ, КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Держанівська А. О., Покотило О. А., Щур Н. О.	Аналіз криптографічних завдань у CTF-змаганнях	67
Нарольський Т. М., Балацька В. С., Полотай О. І.	Математичне моделювання рівня довіри в децентралізованих інформаційних системах КСЗІ на основі блокчейн-технологій	69
Нарепеха Д. Ю., Полотай О. І., Балацька В. С.	Аналіз використання мітигації ризиків інформаційної безпеки локальних комп'ютерних мереж на підприємстві	71

Дорогий Я. Ю., Цуркан В. В., Дорога-Іванюк О.О.	Застосування ШІ при вивченні дисциплін з кібербезпеки	73
Боднарашик А. О., Покотило О. А.	Відмивання коштів у криптовалютних мережах та методи їх аналізу	75
Сарапин В. Є., Шабала Є. Є.	Гібридний підхід для діагностики мережевих аномалій через параметр Херста та QoS-метрики	77
Палагін В. В., Яковлєв Б. В., Гуржій І. В.	Інтеграція SIEM-системи Wazuh в державних фінансових установах	79
Шоломинський Ю.Р., Маслова Н. О., Балацька В. С.	Криптографічні аспекти генерації безпечних простих чисел	81
Нечипорук М. В., Саган Б. В., Скальська А. Р., Чешун В. М.	Система захисту інформаційних ресурсів інтернет-провайдера	83
Декалюк Б. О., Ханін Н. В., Чешун Д. В.	Застосування технологій виявлення вразливостей програмного забезпечення	85
Денега А. Р., Ящук В. І., Полотай О. І.	Комплексний підхід до виявлення та запобігання інсайдерським загрозам у комп'ютерних мережах	87
Дмитрук Б. О., Ящук В. І., Ткаченко А. М.	Комплексний аналіз векторів інфікування інформаційних систем шкідливим програмним кодом та розроблення багаторівневої стратегії кіберзахисту	89
Краєвський Ю. Р., Ящук В. І., Полотай О. І.	Методологія виявлення та нейтралізації фішингових атак із використанням системи захисту електронної пошти Microsoft Defender for Office 365	91

Черкас С. А., Ящук В. І., Пановик У. П.	Інтеграція технологій безпеки для підвищення захищеності IoT-систем у побутовому середовищі	93
Щерб'як М. Т., Ящук В. І., Шклярський Р. А.	Розроблення концептуальної моделі системи захисту корпоративної мережі ТОВ «Інфо Простір Плюс» від несанкціонуваного доступу на основі багаторівневої архітектури безпеки	95
Маруняк С. Т., Кирик М. І.	Інтерпретований аналіз ознак для підвищення точності класифікації аномалій BGP	97
Бень Д. Ю., Ткачук Р. Л., Ящук В. І.	Адміністративно-правові механізми забезпечення кібербезпеки держави	99
Зеленчук А. Р., Ткачук Р. Л., Федина Б. І.	Інформаційна безпека в системі національної безпеки держави	101
Кривий Р. А., Ткачук Р. Л., Балацька В. С.	Кібербезпека банківського сектору: сучасні загрози та роль ШІ у протидії	103
Панченко Н. А., Ткачук Р. Л., Полотай О. І.	Кібертероризм, дезінформація та інформаційні обмеження як загрози держбезпеці	105
Ціфринець В. М., Ткачук Р. Л., Івануса А. І.	Вплив дезінформації на національну безпеку України	107
Шелуха О. О., Овсянніков Д. В.	Методи та технології організації захищеного доступу корпоративної мереж	109
Ретивих К. О., Колощук М. С.	Моніторинг і візуалізація мережевого трафіку за допомогою Zenarmor Dashboard	111
Ференз А. Р., Фальковський І. Г.	Огляд мережевих протоколів, що використовуються для моніторингу	113

Хавер А. В.	Кольорові сітки Петрі як математичний засіб моделювання кібератак в технологічних системах промислових об'єктів критичної інфраструктури	115
Сарапин В. Є.	Виявлення мережевих аномалій засобами аналізу трафіку	117
Пирч О. В., Коробко Р. М., Панько Р. М.	Особливості виявлення аномалій у мережевому трафіку малої інтенсивності	119
Жеребцов Д. В., Кухар А. А., Сергійко В. М., Рудюк Б. М.	Міграція з IPv4 на IPv6: проблеми, ризики та перспективи реалізації	121
Гавриш О. С., Сімонов В. О.	Розробка та впровадження раціональних політик доступу для мережі приватної компанії	124
Жеребцов Д. В., Кухар А. А., Сергійко В. М., Рудюк Б. М.	Роль Firewall в сучасних мережах	126
Рій А. І., Заблоцький С. О., Кирик М. І.	Гібридна модель Isolation Forest-GAN-Transformer для аналізу мережевих аномалій	128
Yanchuk V., Humeniuk A.	Data and application security aspects for international e-commerce solutions in Europe and Ukraine	130
Гребенюк Д. М.	Honeypot-платформа для виявлення атак	133
Череватий Б. С., Шушура О. М., Соломаха С. А.	Система забезпечення моніторингу інформаційної безпеки корпоративних Telegram-чатів	136
Polishchuk K., Chyzhmotria O., Vakaliuk T.	Why Camellia failed to become a widespread cryptographic standard	138

Ліщинський В. В., Романець О. А., Марчук Я. В., Рудюк Б. М.	Роль DHCPv6 у автоматичній конфігурації IPv6-адрес у корпоративних мережах	140
Ліщинський В. В., Романець О. А., Марчук Я. В., Рудюк Б. М.	Безпека DHCPv6: методи захисту від атак та неправомірного розподілу адрес	142
Єфіменко А. А., Бродський Ю. Б., Єфіменко А. А.	Модель побудови SOC з використанням інтеграцій відкритих програмних рішень	144
Фальковський І. Г., Карп'юк І. В.	Модель оптимізація управління кінцевими точками на базі MECM у Windows-інфраструктурі	146
Слободянюк А. О., Бродський Ю. Б.	Аналіз та рекомендації щодо впровадження багаторівневого захисту локальної мережі	148
Томасов Р. О., Бродський Ю. Б.	Аналіз найпоширеніших типів вразливостей у WordPress	150
Качур В. В., Рудюк Б. М.	Порівняльний аналіз протоколів Telnet та SSH для забезпечення безпечного віддаленого адміністрування мережевого обладнання	152
Мосійчук Р. І., Рудюк Б. М.	Віддалений доступ у мережах IPv6	154
Лещенко Б. С., Єфіменко А. А.	Зменшення розміру контейнерних образів як стратегія зниження поверхні атаки	156
Омельчук І. А., Пількевич І. А., Мірошніченко С. І.	Методи математичного прогнозування для використання в системах управління роботизованими комплексами	158
Manko M., Tuz V.	Comparative analysis of classical, post-quantum, and quantum cryptographic methods for secure military communications	161

Коровайченко Ю.Ю., Нікітін А. М.	Модель багатошарового аналізу мережевого трафіку та роль алгоритму Random Forest у ієрархії методів інтелектуального виявлення аномалій	165
Цевчук В. С., Бродський Ю. Б.	Проєктування Honeypot-підсистеми для захисту публічних портів корпоративних мереж	167
Приходько Д. С., Петросян Р. В.	Порівняльний аналіз технологій MPLS та SD-WAN при побудові мережевої інфраструктури	169
Боцанюк І. М., Бродський Ю. Б.,	Адаптивна модель підвищення стійкості систем виявлення фішингу	171
Гаврилюк В. А., Бродський Ю. Б.	Аналіз та рекомендації забезпечення захищеності розподілених корпоративних мереж	173
Сердійчук І. С., Бродський Ю. Б.	Шляхи удосконалення захисту гетерогенної мережі підприємства з використанням комплексу VPN-технологій	175
Івченко О. В., Єфименко Д. В.	Розробка та впровадження комплексної системи захисту мережі на основі фаєрволів Cisco нового покоління (NGFW)	177
Івченко О. В., Бочаров П. І.	Аналіз та оптимізація алгоритмів динамічної маршрутизації в мережах з великою кількістю вузлів	179
Кожухівський А. Д., Ганусяк С. І.	Прогнозування ботнет-активності в інформаційній системі підприємства за допомогою регресійних моделей	181
Макаревич С. О., Дячук О. Ю., Колощук М. С.	Honeypot/Honeynet у корпоративному середовищі: стратегія збору емпіричних даних для прогнозної безпеки	185
Млинський Б. М., Дячук О. Ю.	Архітектура та відмовостійкість стеків Cisco Catalyst 2960-SF: аналіз FlexStack/FlexStack-Plus	187

Ожго Ю. А., Миколайчук В. В.	Дослідження популярних Container Runtime	189

Секція 3. ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Тетерук Д. О., Бродський Ю. Б.	Аналіз та оцінювання впливу використання доповненої реальності на ефективність орієнтування користувачів у міському середовищі	191
Марчук Г. В., Любченко Д. В.	Підвищення точності ASR для OOV-лексики	193
Добрушин Ю. В., Віктор А. С.	Методологічні засади автоматизації інтеграції програмного забезпечення на основі семантичного аналізу	195
Фоменко В. А., Савіцький Р. С.	Автоматизований пошук помилок в українському тексті з використанням моделей штучного інтелекту	197
Гольцев К. О., Савіцький Р. С.	Розробка фітнес-платформ на основі Next.js	199
Кожухівський В. О., Марчук Г. В.	Розробка кросплатформових систем поведінкової корекції з модулем гейміфікації	201
Ячменьова С. О., Коротун О. В.	Визначення ключових IT-професій за допомогою аналізу даних	203
Бичак К. А., Бродський Ю. Б.	Аналіз методів і алгоритмів для створення автоматизованих рекоменда-ційних систем	205
Яковенко Д. В., Коротун О. В.	Оптимізація швидкодії інтернет-магазину засобами мікросервісної архітектури та сучасних підходів до кешування	207
Яковенко Д. В., Коротун О. В.	Поведінкові метрики як інструмент оптимізації навігації та структури інтернет-магазину	209
Носов Є. Д., Шушура О. М. Соломаха С. А.	Інтелектуальні методи управління ресурсами інформаційних систем у хмарних технологіях	210

Лук'яненко А. А., Українець М. О.	Доцільність інтеграції ШІ-агента у веб-платформу кулінарних рецептів	212
Трибюк В. О., Фант М. О.	Юридичні та етичні аспекти веб-скрапінгу	214
Сторчак Д. О.	Інструменти для оптимізації HR-процесів	216
Марчук Д. К.	Edge-орієнтований підхід до моніторингу паркувальних просторів	218
Ковбасюк С. В., Українець М. О.	Визначення координат місцезнаходження безпілотного повітряного судна в умовах недоступності глобальних навігаційних супутникових систем	221
Зулінський М. В., Марчук Д. К.	Підхід до побудови модульної архітектури ігрового процесу на рушії Unity	223
Левчук А. С., Марчук Д. К.	Проєктування ігрових механік у проєктах жанру Action RPG	225
Торба С. О., Сагайдак В. А.	Персоналізований ШІ-асистент для фітнес-студії як елемент сучасної інформаційної системи	227
Панібратець О. Д., Фуріхата Д. В.	Методи підвищення конверсії в електронній комерції через інтерактивну візуалізацію персоналізованих товарів	229
Роман М. Р.	Архітектура IoT-системи для моніторингу екологічних параметрів	231
Кучер В. О., Єфремов Ю. М.	Порівняльний аналіз архітектур глибокого навчання для прогнозування фінансових часових рядів	233
Колесник О. А., Піонтківський В. І.	Розробка інформаційної системи для автоматизації бронювання управління та аналітики у сфері послуг	235
Біємська А. С., Свінцицька О. М.	Математична модель розрахунку розсіювання пострілу в залежності від стану персонажа	238

Біємська А. С., Свінцицька О. М.	Зважений випадковий вибір у процедурній генерації ігрових сутностей	240
Бродський Ю. Б., Пасічник В. О.	Розробка веб-платформи для розміщення та пошуку волонтерських ініціатив	242
Олійник А. В., Сагайдак В. А.	Автоматизована система комплексного контролю плодових культур із застосуванням комп'ютерного зору та інтелектуальних алгоритмів	244
Грушевицький В. В., Українець М. О.	Порівняння технологій реалізації мультиплеєрного режиму для гри жанру Real-time strategy на рушію Unity	248
Олексюк О. С., Марчук Г. В., Бродський Ю. Б.	Аналіз гібридного алгоритму планування траєкторії летального апарата	250
Дяченко Д. О.	Методи побудови інформаційної системи персоналізованого навчання з використанням алгоритмів адаптації та штучного інтелекту	252
Субчак Ю. Ю., Марчук Г. В.	Аналіз функціональних вимог та інструментів розробки мобільного застосунку «Zhytomyr Travel»	254
Панченко В. Ю., Ткаленко О. М.	Роль великих даних (Big Data) у навчанні великих мовних моделей (LLM)	257
Бовкун О. С., Ткаленко О. М.	Розробка автономного модуля біометричної ідентифікації для системи запуску автомобіля	259
Даншина С. Ю., Проценко А. В.	Багатовимірна геовізуальна аналітика транспортної аварійності з використанням ГІС	261
Лупашина А. А., Фант М. О., Громський О. О., Нерода С. І.	Інформаційна система управління процесами студентського гуртожитку: архітектура, функціональні модулі та практичні механізми забезпечення доступності й надійності	263

Мандрик О. В., Бродський Ю. Б.	Аналіз потенціалу ігрових симуляторів у розвитку мислення та формуванні практичних навичок у гравців	265
Татаренко Н. С., Бродський Ю. Б.	Аналіз феномену Homelab	267
Розбицький Р. Е., Бродський Ю. Б.	Аналіз мікросервісної архітектури для розробки масштабованих веб-систем	269
Karyna Polishchuk, Oleksii Chyzhmotria	Analysis of attack vectors against multifactor authentication systems	271
Karyna Polishchuk, Oleksii Chyzhmotria	Systematization and classification of multifactor authentication methods	273
Сичевський С. В., Свінцицька О. М.	Аналіз ефективності та розробка Serverless-архітектури на основі Google Cloud Functions для асинхронної обробки подій	275
Ясен А. Є., Годлевський Ю. О.	Інтеграція хмарних рішень у сучасну розробку програмного забезпечення	277
Горшенін М. О., Горшенін О. Є.	Порівняльний аналіз CPU- та GPU-орієнтованих підходів до відсікання об'єктів у рендерингу реального часу	279
Воробйов А. П.	Гібридний метод прогнозування вартості нерухомості за структурованими даними та візуальним аналізом зображень	281
Столярчук Д. В., Варганова Д. О.	Розробка фінансового симулятора з елементами гейміфікації як інструменту навчання фінансової грамотності	283
Буджак Д. В., Данильченко В. М.	Інтелектуальні методи фільтрації даних у сучасних інформаційних системах	285
Хоменко Д. П., Петросян А. Р.	Методика побудови оптимізованої 3D-моделі безпілотного повітряного судна для систем фізичного моделювання польоту	287

Туровець А. В., Вакалюк Т. А.	Розробка веборієнтованої рекомендаційної системи з пояснювальними та емоційними механізмами на основі гібридних методів фільтрації	289
Туровець А. В., Вакалюк Т. А.	Розробка модуля емоційного аналізу описів фільмів у системі рекомендацій на основі NLP та гібридної фільтрації	291
Войтюк О. В.	Глибоко вкладені структури даних із багатозалежними зв'язками: продуктивність та оновлення стану при рендерингу	293
Петросян Р. В.	Застосування баз даних часових рядів для моніторингу якості електроенергії	295

Секція 4. ЕЛЕКТРОНІКА, ЕЛЕКТРОННІ КОМУНІКАЦІЇ, ПРИЛАДОБУДУВАННЯ ТА РАДІОТЕХНІКА

Махиборода А. І.	Розробка інтелектуального MPPT-алгоритму на основі ANFIS для підвищення ефективності фотоелектричних систем	297
Качура О. В., С'янов О. Є.	Математична модель напівпровідникової структури на основі діоксиду ванадію	299
Коренівська О. Л., Бенедицький В. Б.	Вимірювання різниці фаз при використанні програмного середовища LTSPICE	301
Коник С. В., Гнатюк М. О.	Синтез смугових фільтрів для SDR-радіоприймачів	303
Соболенко С. О., Дубина О. Ф., Авсієвич Р. О., Заєць Ю. О.	Дослідження ефективності застосування інтегрованої системи охорони	305
Залевський В. Й., Сидорчук О. Л.	Дослідження електромагнітного поля, що збуджується антенною системою РЛС	307
Клочко К. А., Пупков С. С.	Розподілена система керування трафіком в «розумному» місті	309

Колос Ю. О., Маслов О. А.	Методики і результати дослідження відбивних властивостей БПЛА з різними покриттями	311
Рихальський О. Р., Каращук Н. М., Петраш С. В.	Моделювання антенних систем з високовольтних ліній електропередач при дослідженні впливу їх випромінювання на формування PLHR випромінювання в іоносфері	313
Полегешко Д. В., Водько А. М., Івасишин Ю. І., Сотник О. А.	Організація віддаленого доступу до апаратних лабораторних стендів на основі Red Pitaya та системи Librebooking	315
Скрипніченко В. О., Морозов Д. С., Чухов В. В., Фещенко С. О.	Використання діелектричних лінз з періодичною перфорацією для зменшення рівня бічних пелюсток рупорних антен	317
Фриз С.П., Авсієвич Р.О.	Вдосконалення методів радіомоніторин-гу низькоорбітальних космічних систем	319
Антонюк С. С., Ципоренко В. В.	Система сигналізації на основі датчика руху з автоматичним передаванням фотографії та включенням звукової сигналізації по команді з використанням мобільного додатку Telegram	321
Воробкало Т. В., Воробкало О. К.	Оцінювання інформативних параметрів радіосигналу у багатоканальних системах за умов негаусівських завад	323
Денисюк М. С., Ципоренко В. Г.	Дослідження ефективності антен для бездротових мереж IoT в побутових умовах	325
Захожий О. Ю., Ципоренко В. В.	Енергокерований бустерний модуль 5→6/9/12 в для IoT-вузлів, DVS-керування та енергоефективність	327
Рашко О. С., Ципоренко В. В.	Вплив параметрів підкладки на характеристики мікросмужкової антени	329

Собецький В. М., Ципоренко В. В.	Дослідження точності позиціонування GNSS-приймачів з використанням RTK-корекцій	331
Тирчик В. В., Ципоренко В. В.	Система сигналізації з використанням датчика HC-SR04 із сповіщенням про час проникнення до мобільного додатку Telegram	333
Хімчик Н. С., Ципоренко В. В.	Розробка розумного дозиметра на основі мікроконтролерів Atmega328p та ESP32	335
Ткачов А. К., Яганов П. О.	Система слідкування за точкою максимальної потужності для акумуляторних батарей	337
Ткачов А. К., Черненко В. В.	Порівняння методів визначення точки максимальної потужності сонячного елемента із використанням функції ламберта та спрощених аналітичних моделей	339
Петраш С. В., Рихальський О. Р., Зелінський О. В.	Методика визначення виду модуляції радіотехнічних випромінювальних об’єктів	341
Біденко К. А., Ципоренко В. В.	Розробка системи екстреного оповіщення в умовах блекауту	343
Богодвид О. В., Сугоняк І. І.	Аналіз точності вимірювання біометричних показників за допомогою стандартних датчиків смартфону	347
Герасименко В.А., Денисенко Д.С., Романов В.О.	Проєктування інтелектуальної системи освітлення для громадських просторів	349
Дармограй Я.М., Ципоренко В.Г.	Дослідження динамічно керованих протоколів мобільних мереж	352
Морозов Д.С., Журавський Ю.В., Чухов В.В., Коломієць Р.О.	Удосконалений метод синтезу багатошарових антенних решіток на основі патч-антен із круговою поляризацією	354

Секція 5. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

Кольцова Н. О., Савіцький Р. С.	Підтримка інклюзивності: курс для реінтеграції ВПО/ветеранів	358
Рубай А. В., Назар Ю. С.	Технічні аспекти модульної інтеграції голосового зв'язку в освітні платформи	360
Корнєва В. Р., Терницький С. В.	Цифрова трансформація освітнього процесу в умовах змішаного навчання	362
Корнєва В. Р., Корнєва С. П.	Сучасні інформаційні технології в житті викладачів фахової передвищої освіти	364

Секція 6. ЦИФРОВА ОБРОБКА СИГНАЛІВ ТА ЗОБРАЖЕНЬ В АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ

Горобець О. С., Подчашинський Ю.О., Чепюк Л. О.	Перспективні методи цифрової обробки зображень	366
Горшенін О. Є., Горшенін М. О.	Метод радіонавігації БПЛА за полем радіовипромінювань в умовах складного електромагнітного оточення	368
Іщенко О. С., Подчашинський Ю.О., Чепюк Л. О.	Комп’ютеризована інформаційно-вимірювальна система контролю рівня нафтопродуктів у залізничних цистернах	370
Левицький А. В., Подчашинський Ю.О., Чепюк Л. О.	Методи та засоби визначення та контролю геометричних параметрів тривимірних об’єктів за стереозображенням	372
Лугових О. О.	Вибір оптимального значення коефіцієнта експоненціального згладжування для параметрів руху технологічного обладнання	374
Магалецький Я. В., Подчашинський Ю.О., Чепюк Л. О.	Комп’ютеризована інформаційно-вимірювальна система контролю параметрів двигунів відцентрових насосів систем водопостачання	376

Свістельник О. С., Подчашинський Ю.О., Чепюк Л. О.	Інформаційно-вимірювальна система контролю параметрів мікроклімату на поліграфічному виробництві	378
Ступак А. Г., Подчашинський Ю.О., Чепюк Л. О.	Вейвлет-стиснення зображень в інформаційно-вимірювальних системах медичного застосування	380
Товстік С. О., Подчашинський Ю.О., Чепюк Л. О.	Аналіз сенсорів просторового положення панелей сонячної електростанції	382
Фабрикатор М. О.	Телекомунікаційна система класифікації звукових сигналів для моніторингу та оперативного інформування	384

Секція 7. КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ ТА РОБОТОТЕХНІКА

Браташов І. В., Ткаленко О. М.	Впровадження технологій IoT на промисловому підприємстві	386
Андрєєв К. В., Хом'як Е. А., Гусєв О. В., Таразанов Ю. А., Григор'єва Є. С.	Моделювання стану захоронених вітрифікованих радіоактивних відходів	388
Раданович В. Я., Доброжанський О. О.	Проблемні питання виконання релейного захисту на високій та низькій напрузі	390
Шельпяков В. Ю.	Засоби Open Hardware та Open Source в науковій діяльності	392
Раданович В. Я., Доброжанський О. О.,	Енергоефективні системи керування мікроботами на основі нейроморфних технологій	394
Безвесільна О. М., Ткачук А. Г.	Моделювання цифрового двійника електропривода стабілізатора озброєння для аналізу енергоспоживання та діагностики несправностей	395
Марченко К. Л., Ткачук Д. Ю.	Використання відеокамер для контролю якості продукції у виробництві	397

Омельчук І. А., Пількевич І. А., Мірошніченко С. І.	Методи математичного прогнозування для використання в системах управління роботизованими комплексами	399
Бєляк П. Л., Ткачук А. Г., Янчук В. М.	Використання гібридних нейронно-фізичних моделей для оптимізації регулювання напруги в енергосистемах	402
Тарасюк Д. В., Ткачук Д. Ю.	Використання комп'ютерного зору для моніторингу стану сільськогосподарських полів за допомогою БПЛА	404
Линець А. Л., Ткачук А. Г., Крижанівська І. В.	Інтеграція накопичувачів енергії у системи автоматизованого регулювання електричних станцій	406
Сардаківський А. В., Ткачук Д. Ю.	Інтеграція БПЛА і мультиспектрального аналізу в системах точного землеробства	408
Богдановський М. В., Корнійчук С. М.	Інверсна нейронечітка модель оцінки залишкового ресурсу високовольтних трансформаторів напруги	411
Раданович В. Я., Ткачук Д. Ю.	Автоматизований контроль правильності сортування посилок у логістичних системах з використанням комп'ютерного зору та нейронної мережі YOLO	413
Богдановський М. В., Горбік Д. П.	Розробка симулятора для дослідження задач прямої і зворотньої кінематики маніпуляторів	415
Чайківський А. В., Ткачук Д. Ю.	Використання інфрачервоного спектра для підвищення точності машинного зору в умовах низької освітленості	417
Гальвіта А., Корнєва В. Р.	Сучасні підходи до розвитку комп'ютерно-інтегрованих технологій у виробничих системах	420
Ткачук А. Г., Черниш О. А., Кравчук А.Р., Василевський Д.В.	Інтелектуальна система для збору та аналізу ситуаційних даних	422

Кравчук А. Р., Козяр Я. А., Ткачук А. Г., Мельник О. Л.	Розробка 3D-моделі корпусу мобільної роботизованої платформи з підвищеною прохідністю	424
Ткачук А. Г., Кравчук А. Р., Покляченко О. В., Скударнов Б. С.	Проєктування системи енергозабезпечення та терморегуляції для роботизованої платформи	426
Перцов А. А., Гуменюк А. А., Громовий О. А., Янчук В. М.	Переваги оптимальних адаптивних систем порівняно з AI-рішеннями: практичний аналіз на прикладі технологій TIAMA	428

Секція 8. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У БІОМЕДИЦИНІ

Ветров А. О., Нікітчук Т. М.	Біомедичний моніторинг геймерів: архітектура збору даних з носимих пристроїв та аналіз стану користувача	431
Коренівська О. Л., Бенедицький В. Б., Сергійчук М. В., Галанзовська В. О.	Система гібридного керування протезом верхньої кінцівки	433
Korenivska O. L., Nikitchuk T. M., Bogoavlenska Y. V.,	Introduction of modern medical monitoring systems into the training of biomedical engineering specialists	435
Фещенко С. В., Мацієвський В. А., Нікітчук Т. М., Марцева Л. А.	Розробка та апробація апаратно-програмного комплексу для моніторингу функціонального стану операторів ергатичних систем	437
Богатов Д. В., Сімчук А. Р., Нікітчук В. С., Корніюк А. В.	Маркери варіабельності серцевого ритму в оцінці «ціни адаптації» операторів при психоемоційному навантаженні	439
Квітка Р. В., Мацієвський В. А., Нікітчук Т. М.	Розробка біотехнічної системи моніторингу стану серцево-судинної системи для ранньої діагностики вірусних захворювань	441

Янчук Е. А., Нікітчук Т. М., Коренівська О. Л.	Інтерфейси мозок-комп’ютер: сучасні тенденції розвитку	443
Дудка В. Р.	Сучасні інформаційні технології у біомедицині	445

Наукове видання

Комп’ютерні технології: інновації, проблеми, рішення: тези доповідей VIII Всеукраїнської науково-технічної конференції

Житомир, 02-03 грудня 2025 р.

Відповідальний за випуск: Ю.В. Венгловська

Свідоцтво про внесення до Державного реєстру суб’єктів видавничої справи ДК № 7177 ВІД 04.11.2021 р.

Адреса редакції: Державний університет «Житомирська політехніка», вул. Чуднівська, 103, м.Житомир, 10005