Національний технічний університет
«Дніпровська політехніка»

INFORMATION TECHNOLOGY: COMPUTER SCIENCE, SOFTWARE ENGINEERING AND CYBER SECURITY

Випуск 3

Видавничий дім
«Гельветика»
2024

Журнал включений до Переліку наукових фахових видань України (категорія «Б») за спеціальностями 121 – Інженерія програмного забезпечення, 122 – Комп'ютерні науки, 123 – Комп'ютерна інженерія, 124 – Системний аналіз, 125 – Кібербезпека відповідно до наказів МОН України № 735 (додаток № 4) від 29.06.2021 р. та № 491 (додаток № 3) від 27.04.2023 р.

Реєстрація суб'єкта у сфері друкованих медіа: Рішення Національної ради України з питань телебачення і радіомовлення № 865 від 21.03.2024 року.

Мови видання: українська, англійська, німецька, польська, іспанська, французька, болгарська.

Офіційний сайт видання: www.journals.politehnica.dp.ua/index.php/it

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення StrikePlagiarism.com від польської компанії Plagiat.pl.

ISSN 2786-507X (Print)
ISSN 2786-5088 (Online)

UDC 004.932: 004.896
DOI https://doi.org/10.32782/IT/2024-3-1

Stanislav AVRAMENKO
Postgraduate Student at the System Analysis and Control Department, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave, Dnipro, Ukraine, 49005, avramenko.st.y@nmu.one
ORCID: *0009-0001-7182-7852*

Timur ZHELDAK
Candidate of Technical Sciences, Associate Professor, Head of the System Analysis and Control Department, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave, Dnipro, Ukraine, 49005, zheldak.t.a@nmu.one
ORCID:*0000-0002-4728-5889*
Scopus Author ID: *55602208300*

To cite this article: Avramenko, S., Zheldak, T. (2024). Vyiavlennia obiektiv na osnovi hlybokoho navchannia dlia avtonomnoho keruvannia: zastosuvannia ta vidkryti problemy [Deep-learning based object detection for autonomous driving: aplications and open challenges]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 3–13, doi: https://doi.org/10.32782/IT/2024-3-1

DEEP-LEARNING BASED OBJECT DETECTION FOR AUTONOMOUS DRIVING: APPLICATIONS AND OPEN CHALLENGES

Object detection is a critical component of autonomous driving systems, enabling accurate identification and localization of vehicles, pedestrians, cyclists, traffic signs, and other road objects. Deep learning techniques have revolutionized this field, propelling object detection capabilities to unprecedented levels. This paper presents a survey of state-of-the-art deep learning-based object detection methods tailored for autonomous driving applications using monocular camera input.

The purpose of this work is *to provide a unified perspective on modern deep learning approaches to object detection tailored for the unique requirements of autonomous driving. The monocular camera modality is chosen for its cost-effectiveness, widespread availability, and compatibility with existing automotive hardware. The focus is solely on deep learning techniques due to their ability to learn rich feature representations directly from data.*

The methodology *involves a systematic review of real-world applications and challenges, including pedestrian detection, traffic sign recognition, low-light conditions, and real-time performance requirements.*

The scientific novelty*. This survey consolidates the latest developments in camera-based object detection for autonomous driving, providing a comprehensive and up-to-date resource for researchers and practitioners. It offers insights into emerging techniques, such as attention mechanisms, multi-scale feature fusion, and model compression, which address critical challenges like occlusion handling, small object detection, and computational efficiency. Furthermore, the survey explores the potential of explainable AI and meta-learning techniques to enhance the transparency, interpretability, and generalization capabilities of object detectors in autonomous driving contexts.*

Conclusions*. Deep learning-based object detection has made significant strides in recent years, enabling robust and accurate perception for autonomous vehicles. However, challenges persist in real-world deployment, including handling diverse lighting conditions, adverse weather scenarios, and ensuring reliable performance under occlusions. This survey highlights promising research directions, such as incorporating attention mechanisms, temporal information, and multi-scale architectures, to address these challenges and pave the way for safer and more reliable autonomous driving systems.*

Key words: *object detection, autonomous driving, deep learning, transformers, attention mechanisms, occlusion handling, real-time performance.*

Станіслав АВРАМЕНКО
аспірант кафедри системного аналізу та управління, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
ORCID: *0009-0001-7182-7852*

Тімур ЖЕЛДАК
кандидат технічних наук, доцент, завідувач кафедри системного аналізу та управління, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
ORCID: *0000-0002-4728-5889*
Scopus Author ID: *55602208300*

Бібліографічний опис статті: Авраменко, С., Желдак, Т. (2024). Виявлення об'єктів на основі глибокого навчання для автономного керування: застосування та відкриті проблеми. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 3–13, doi: https://doi.org/10.32782/IT/2024-3-1

ВИЯВЛЕННЯ ОБ'ЄКТІВ НА ОСНОВІ ГЛИБОКОГО НАВЧАННЯ ДЛЯ АВТОНОМНОГО КЕРУВАННЯ: ЗАСТОСУВАННЯ ТА ВІДКРИТІ ПРОБЛЕМИ

Виявлення об'єктів є критично важливим компонентом систем автономного водіння, що дозволяє точно ідентифікувати та локалізувати транспортні засоби, пішоходів, велосипедистів, дорожні знаки та інші дорожні об'єкти. Технології глибокого навчання зробили революцію в цій галузі, піднявши можливості виявлення об'єктів до безпрецедентного рівня. Ця стаття представляє огляд найсучасніших методів виявлення об'єктів на основі глибокого навчання, розроблених для додатків автономного водіння з використанням монокулярної камери.

***Метою цієї роботи є** надання єдиного погляду на сучасні підходи глибокого навчання до виявлення об'єктів, спеціально розроблені для унікальних вимог автономного водіння. Модальність монокулярної камери обрано через її економічну ефективність, широку доступність і сумісність з існуючим автомобільним обладнанням. Основна увага зосереджена виключно на техніках глибокого навчання завдяки їхній здатності вивчати представлення багатьох властивостей безпосередньо з даних.*

***Методологія** передбачає систематичний огляд реального застосування та проблем, включаючи виявлення пішоходів, розпізнавання дорожніх знаків, умови слабкого освітлення та вимоги до продуктивності в реальному часі.*

***Наукова новизна**. Цей огляд об'єднує останні розробки в області виявлення об'єктів за допомогою камери для автономного водіння, надаючи всебічне і актуальне джерело для дослідників і практиків. Він пропонує розуміння нових методів, таких як механізми привернення уваги, багатомасштабне об'єднання властивостей і стиснення моделі, які вирішують критичні проблеми, такі як обробка загородження, виявлення малих об'єктів і ефективність обчислень. Крім того, огляд досліджує потенціал зрозумілого штучного інтелекту, і методів метанавчання для підвищення прозорості, інтерпретації та можливостей узагальнення детекторів об'єктів у контексті автономного водіння.*

***Висновки**. За останні роки виявлення об'єктів на основі глибокого навчання досягло значних успіхів, забезпечивши надійне та точне сприйняття для автономних транспортних засобів. Однак під час розгортання в реальному світі залишаються проблеми, включаючи роботу з різними умовами освітлення, несприятливими погодними сценаріями та забезпечення надійної роботи в умовах загородження. Цей огляд підкреслює багатообіцяючі напрямки досліджень, такі як включення механізмів уваги, тимчасової інформації та багатомасштабних архітектур, щоб вирішити ці проблеми та прокласти шлях для безпечніших і надійніших систем автономного водіння.*

***Ключові слова:** виявлення об'єктів, автономне водіння, глибоке навчання, трансформери, механізми уваги, загородження, продуктивність у реальному часі.*

Introduction. Autonomous driving systems (ADS) have garnered significant attention in recent years, driven by the promise of enhanced transportation safety, efficiency, and accessibility. At the core of these systems lies the critical task of object detection, which enables the accurate identification and localization of various elements in the surrounding environment, including vehicles, pedestrians, cyclists, traffic signs, and other road objects. Reliable object detection is paramount for safe navigation and decision-making in self-driving vehicles, as it provides the foundational awareness necessary to plan and execute appropriate actions.

The advent of deep learning has revolutionized the field of computer vision, propelling object detection capabilities to unprecedented levels. Modern deep learning-based object detectors have demonstrated remarkable accuracy and robustness, outperforming traditional computer vision techniques. However, the unique challenges posed by autonomous driving scenarios demand even higher standards of performance, reliability, and efficiency.

Autonomous vehicles must operate in dynamic and complex environments, where varying lighting conditions, adverse weather, occlusions, and diverse object appearances can significantly impact detection accuracy. Moreover, the real-time nature of autonomous driving necessitates object detectors capable of processing high-resolution video streams at high frame rates while maintaining low latency, ensuring timely decision-making and response.

By synthesizing the latest research efforts and insights, this paper aims to provide a comprehensive understanding of the state-of-the-art in deep learning-based object detection for autonomous driving and pave the way for future advancements in this critical domain.

Applications and Open Challenges.

Pedestrian detection. This component of autonomous driving systems is critical to ensure the safety of vulnerable road users. It enables self-driving vehicles to identify and track pedestrians in their surroundings, allowing them to make informed decisions and take appropriate actions to avoid collisions or other hazardous situations. Accurate pedestrian detection is essential for maintaining the trust and acceptance of autonomous vehicles by the public.

Despite significant advancements in computer vision and machine learning techniques, pedestrian detection for autonomous driving still faces several challenges. Occlusion, where pedestrians are partially obscured by other objects or vehicles, remains a significant hurdle. Varying lighting conditions, weather patterns, and diverse pedestrian appearances (clothing, posture, etc.) can also impact the reliability of detection algorithms. Additionally, distinguishing between static and moving pedestrians, predicting their intentions, and handling edge cases like crowded scenarios pose ongoing challenges.

(Lyssenko et al., 2024) address the safety-critical aspect of pedestrian detection in automated driving, where misdetections of critical pedestrians can endanger vulnerable road users. They introduce a safety-adapted loss function that leverages time-to-collision and distance information to quantify the criticality of pedestrians during training. Their approach aims to mitigate the misdetection of critical pedestrians without sacrificing overall performance.

Several papers discuss using the YOLO object detection algorithm for pedestrian detection in real-time scenarios. (Mishra & Jabin, 2023) and (Zuo et al., 2021) show that YOLO has proven effective at detecting and localizing objects in images with impressive speed. YOLO using transfer learning on pre-trained models is discussed by (Mishra & Jabin, 2023). (Zuo et al., 2021) evaluate different YOLO variants like YOLO-Tiny, YOLO, and YOLO-SPP, with YOLO and YOLO-SPP showing high average confidence, and YOLO-Tiny having fast detection speed suitable for real-time scenarios. The improved YOLO-R model proposed by (W. Lan et al., 2018) with added Passthrough layers can effectively improve pedestrian detection accuracy while reducing false and missed detections, achieving 25 FPS.

Other works focus on pedestrian detection using infrared images and multimodal data fusion techniques. (Wei et al., 2023) propose an approach using an improved UNet and YOLO network that shares visible light information from related datasets, achieving high detection accuracy on infrared pedestrian datasets, with a real-time speed of 25.6 FPS on edge devices. (Y. Zhang et al., 2022) introduce a lightweight vehicle-pedestrian detection algorithm based on YOLOv4 with a MobileNetv2 backbone, multi-scale feature fusion, and coordinate attention mechanism, improving accuracy and speed over the original YOLOv4. (Y. Chen et al., 2023) propose the TF-YOLO detector that uses a transformer-fusion module in a two-stream backbone to robustly integrate visible and infrared images, improving pedestrian detection performance under various illumination conditions compared to state-of-the-art approaches.

Pedestrian detection in crowded scenes poses challenges due to occlusion and scale variations. The recently proposed end-to-end detectors DETR and deformable DETR, based on transformer architectures, have shown promising results by avoiding hand-crafted components, but (Lin et al., 2021) found their performance surprisingly poor on crowd pedestrian detection compared to Faster-RCNN. Several works aim to address this issue. (Han et al., 2024) propose an improved deformable DETR (IDPD) with a dynamic neck and hybrid decoding loss to alleviate information loss and positive-negative imbalance. (Yuan et al., 2022) demonstrate the effectiveness of vision transformers for fast and accurate single-stage pedestrian detection by proposing a spatial and multi-scale feature enhancement module. (Deng & Li, 2024) introduce an efficient dense pedestrian detection algorithm using EfficientNet as the backbone, a cross-fertilization module for fusing multi-scale features, and noise removal training to improve detection of occluded and small-scale pedestrians while reducing model size and computation.

Moving object detection (MOD) is essential for identifying potential collision risks from dynamic objects in the environment. Several works have proposed deep learning approaches to tackle this problem by jointly modeling motion and appearance cues. (Siam et al., 2018) introduced MODNet, a two-stream architecture that combines object detection and motion segmentation for improved accuracy. (Yahiaoui et al., 2019) extended this idea to fisheye surround-view cameras with FisheyeMODNet. (Rashed, Essam, et al., 2021) explored end-to-end MOD in the bird's eye view (BEV) space using monocular images, demonstrating significant improvements over traditional inverse perspective mapping methods.

To further improve MOD performance, researchers have explored incorporating additional information into the models. VM-MODNet (Rashed, Sallab, et al., 2021) leverages vehicle motion

information to enable ego-motion compensation, leading to substantial gains in accuracy. (Hernandez et al., 2020) fused semantic information from a deep learning detector with occupancy grid estimations to recognize moving objects. RST-MODNet (Ramzy et al., 2019) developed a real-time spatio-temporal architecture that exploits temporal motion information from sequential images and optical flow for increased robustness.

In addition to deep learning approaches, researchers have also explored alternative strategies for real-time MOD in autonomous driving systems. (Jha et al., 2021) introduced a system that combines object detection and tracking algorithms, adaptively controlling their execution cycles to ensure real-time performance in various edge computing environments. (Z. Zhou et al., 2023) proposed RENet, a novel RGB-Event fusion network that jointly exploits complementary modalities from conventional cameras and event cameras for more robust MOD under challenging scenarios. (D. Liu et al., 2020) presented MFCN, an end-to-end deep learning framework that leverages temporal coherence and motion patterns in video features for improved object detection accuracy while maintaining efficiency.

Traffic sign detection task faces challenges such as multi-scale targets and real-time performance requirements. Several studies have aimed to improve the detection accuracy and speed for multi-scale traffic signs by enhancing the feature pyramid network of object detectors like YOLOv5. (J. Wang et al., 2021) proposed an adaptive attention module and feature enhancement module in the feature pyramid to reduce information loss and enhance representation ability. The ETSR-YOLO algorithm (H. Liu et al., 2023) generated an additional high-resolution feature layer and introduced improved C3 modules to suppress background noise and enhance feature extraction. (T. Chen & Ren, 2023) designed a cross-level loss function to enable each level of the MFL-YOLO model to learn diverse features and improve fine-grained details for detecting damaged traffic signs.

Other approaches have focused on improving the performance of object detectors like SSD for traffic sign detection. (You et al., 2020) proposed a lightweight SSD network with 1x1 convolution kernels and color-based filtering to improve detection speed while maintaining accuracy. (Wu & Liao, 2022) combined SSD with a receptive field module and path aggregation network to improve small traffic sign detection and integrate multi-scale features. (Greer, Gopalkrishnan, Deo, et al., 2023; Greer, Gopalkrishnan, Landgren, et al., 2023) defined the concept of «salient» traffic signs/lights that influence driver decisions and trained Deformable DETR models with a salience-sensitive loss function to emphasize performance on these salient objects.

Some studies have explored alternative architectures like transformers for traffic sign recognition. (Farzipour et al., 2023) proposed a hybrid model combining convolutional and transformer-based blocks with a locality module to capture local and global features, achieving high accuracy on traffic sign datasets. The DSRA-DETR algorithm (Xia et al., 2023) introduced dilated spatial pyramid pooling and multi-scale feature residual aggregation to improve multi-scale traffic sign detection with DETR. (S. Chen et al., 2024) presented a semi-supervised learning framework combining CNN and multi-scale transformer with hierarchical sampling and local/global information aggregation for accurate traffic sign detection and recognition from vehicle panoramic images.

Semi-supervised object detection methods leverage both labeled and unlabeled data to improve performance, and they are widely used in autonomous driving systems where only a fraction of objects are labeled (Hu et al., 2022). These methods generate pseudo-labels for unlabeled objects, which can significantly improve performance but also introduce noise and errors, especially for video data (W. Chen et al., 2024; Hu et al., 2022). Approaches have been proposed to generate more robust pseudo-labels by leveraging motion continuity in video frames (Hu et al., 2022) and using semi-supervised co-training with unsupervised data augmentation to improve generalization and robustness under adversarial attacks (W. Chen et al., 2024). Additionally, methods have been developed to correct and refine pseudo-labels to reduce classification and localization noise (He et al., 2023), as well as to enhance the quality of object queries and selectively filter high-quality pseudo-labels in transformer-based object detection models (Shehzadi et al., 2024). These advancements in semi-supervised object detection aim to improve accuracy, consistency, and robustness, particularly for challenging scenarios involving small or occluded objects in autonomous driving applications.

Real-time object detection. Recent advances in real-time object detection for autonomous driving have focused on developing efficient and accurate models. (Miraliev et al., 2024) propose a real-time memory-efficient multitask learning model for joint object detection, drivable area segmentation, and lane detection, achieving high accuracy and a processing speed of 112.29 fps. (Mahaur et al., 2023) introduce architectural modifications to the

YOLOv5 model, including group depthwise separable convolutions and attention-based dilated blocks, improving small object detection accuracy by 8.35% on the BDD100K dataset while increasing speed by 3.1%. The DPNet algorithm (Q. Zhou et al., 2022) presents a dual-path network with a lightweight attention scheme, enabling parallel extraction of high-level semantic features and low-level object details, achieving state-of-the-art trade-off between detection accuracy and efficiency. (A. Wang et al., 2024) introduce YOLOv10, a real-time end-to-end object detector with consistent dual assignments for NMS-free training and holistic efficiency-accuracy driven model design, significantly reducing computational overhead and enhancing capability compared to previous YOLOs. (Zhao et al., 2024) propose RT-DETR, the first real-time end-to-end object detector, featuring an efficient hybrid encoder and uncertainty-minimal query selection, outperforming advanced YOLOs in both speed and accuracy on the COCO dataset.

Low light condition. Operate seamlessly 24/7 without being limited by nighttime or poor visibility scenarios is crucial for enabling safe and reliable autonomous driving in all environments and conditions. (X. Wang et al., 2022) and Pham et al. (Pham et al., 2020) propose methods to enhance low-light images and improve object detection accuracy, which is crucial for applications like traffic monitoring and autonomous driving. (X. Wang et al., 2022) utilize dark channel prior and adaptive gamma transformation to restore scene radiance and develop the LL4PH-Net framework for low-light traffic object detection. (Pham et al., 2020) introduce DriveRetinex-Net, a deep retinex neural network trained on a low-light driving dataset (LOL-Drive), which decomposes images into reflectance and illumination maps, enhancing the latter for improved object detection.

Several other approaches tackle the challenge of object detection in adverse weather and low-light conditions for autonomous driving. The IDOD-YOLOV7 algorithm (Qiu et al., 2023) jointly optimizes image defogging (AOD) and enhancement (SAIP) modules with YOLOV7 detection, improving perception in low-light foggy environments. (W. Liu et al., 2022) propose Image-Adaptive YOLO (IA-YOLO), where a differentiable image processing module adaptively enhances images for better object detection. (Guo et al., 2024) introduce HawkDrive, a transformer-based visual perception system with stereo vision and edge computing for depth estimation and semantic segmentation in night scenes. (Ye et al., 2024) propose VELIE, a vehicle-based efficient low-light image enhancement method using Swin Vision Transformer and U-Net for real-time inference and edge deployment in intelligent vehicles.

Overview of Modern Techniques.

Modern deep learning-based object detection systems for autonomous driving must possess exceptional accuracy in detecting and precisely localizing a wide range of objects, including vehicles, pedestrians, cyclists, traffic signs, and other road elements. They should demonstrate this high level of accuracy under diverse lighting conditions, varying weather scenarios, and situations with partial occlusion. Additionally, these systems need to deliver real-time performance, capable of processing high-resolution video streams at high frame rates while maintaining low latency to enable timely decision-making and response. Furthermore, robustness and reliability are crucial, ensuring safe and consistent operation even in challenging scenarios. There are some approaches that may help to meet these requirements.

Incorporating attention mechanisms into object detectors can help them focus on relevant regions and better handle occlusions. (S. Zhang et al., 2021) propose an attention mechanism across CNN channels to represent various occlusion patterns for pedestrian detection and re-identification, employing attention guided self-paced learning to balance optimization across different occlusion levels. (Zou et al., 2020) proposed an attention guided neural network model (AGNN) that uses an attention mechanism to selectively weight and integrate features from sub-images representing body parts of occluded pedestrians for improved detection performance.

Leveraging temporal information from video sequences can help in tracking and predicting the movement of occluded objects. It was proposed a novel spatio-temporal fusion Transformer (STFT) (Qi et al., 2024) model that incorporates a dynamic template update strategy based on salient points feature representation, an IoU-Aware target state estimation head, and an IoU-Aware criterion for robust thermal infrared object tracking to address the limitations of existing approaches in handling scale variations, appearance changes, and occlusions.

Incorporating FPNs or similar multi-scale architectures can help object detectors capture both fine-grained and contextual information, improving small object detection. (Huang et al., 2023) propose the Multiple Link Feature Pyramid Networks (MLFPN) with novel information transfer pathways and Poly-Scale Convolution (PSconv) to reduce feature information loss and improve pedestrian detection. (Yahya et al., 2023)

introduce the Fast Region-Convolutional Neural Network (R-CNN) with the Attention-guided Context Feature Pyramid Network (ACFPN) for object detection in autonomous vehicles, achieving better mean Average Precision (mAP). (Dang et al., 2023) propose the hierarchical attention feature pyramid network (HA-FPN), comprising transformer feature pyramid networks (TFPNs) that apply self-attention across scales to capture contextual information, and channel attention modules (CAMs) that select channels with rich information to improve bounding box detection accuracy and object localization, while minimizing computational overhead. (Xie et al., 2022) proposed FocusTR (Focusing on the valuable features by multiple Transformers) architecture that presents novel self-attention mechanisms, including spatial-wise boxAlign attention, context-wise affinity attention, and level-wise attention, along with low and high-level fusion and Pre-Ln, to effectively fuse multi-level and multi-sensor feature pyramids for object detection in autonomous driving.

Model Compression and Quantization techniques like model pruning, quantization, and knowledge distillation can significantly reduce the computational complexity and memory footprint of object detectors. (H. Liu et al., 2021) and (Youn et al., 2023) explore knowledge distillation as a technique for compressing large neural networks like vision transformers and convolutional neural networks into smaller and more efficient models suitable for resource-constrained devices such as autonomous vehicles. The core idea involves training a smaller «student» model to mimic the behavior of a larger and more accurate «teacher» model, transferring knowledge from the teacher to the student. (Q. Lan & Tian, 2023) and (Agand, 2024) propose enhancing this process with techniques like model pruning, quantization, and adaptive instance/scale-wise distillation.

In autonomous driving contexts, Flexi-Compression (H. Liu et al., 2021), Quasar-ViT (Li et al., 2024), and the approach by (Youn et al., 2023) focus on compressing vision transformers and convolutional neural networks used for object detection, semantic segmentation, and navigation by employing architectural modifications, hardware-aware neural architecture search, and combining distillation with pruning and quantization. Additionally, (Q. Lan & Tian, 2023) introduce multi-teacher adaptive instance distillation, while (Agand, 2024) explores an end-to-end transformer-based sensor fusion method using knowledge distillation to improve performance and handle challenging scenarios in autonomous driving.

Incorporating meta-learning techniques, which learn to adapt to new domains quickly, can enhance the generalization capabilities of object detectors. (Sun et al., 2024) propose a transformer-based few-shot object detection approach for traffic scenarios. It employs class-agnostic training to extend the detector to novel classes and combines visual prompts with pseudo-class embeddings to improve query generation. This approach does not require retraining during inference and accurately localizes novel objects through an improved query generation mechanism.

Integrating explainable AI techniques can provide local explanations for individual predictions made by object detectors and improve transparency and interpretability. (Dong et al., 2023) propose a novel approach to enhance trustworthiness in autonomous driving systems through explainable deep learning models. Instead of treating decision-making as a classification task, it frames it as an image-based language generation (image captioning) task, where the model generates textual descriptions of driving scenarios to serve as explanations for its decisions. (Cultrera, Luca., 2023) presents an approach to autonomous driving based on imitation learning using visual attention mechanisms. By selectively weighting and prioritizing relevant regions in the image, this method aims to mimic the human approach to driving and enhance interpretability and explainability. (Adom & Mahmoud, 2024) introduce RB-XAI, a Relevance-Based Explainable AI algorithm that uses Concept Relevance Propagation (CRP) to provide transparent concept-level explanations for the behavior of object detection models used in autonomous vehicles. CRP generates explanations that automatically identify and visualize relevant concepts within the input space, shedding light on the crucial areas responsible for the models' decisions. (Kolekar et al., 2022) propose an explainable inception-based U-Net model with Grad-CAM visualization for semantic segmentation in unstructured traffic environments on Indian roads. The inception U-Net model combines an inception-based module as an encoder for automatic feature extraction and a decoder for reconstructing the segmentation feature map. Grad-CAM is used to interpret the deep learning model, increasing consumer trust by providing visual explanations.

Conclusions. The field of object detection for autonomous driving has seen remarkable progress, with innovative architectures demonstrating state-of-the-art performance. However, several challenges remain, including handling occlusions, varying lighting conditions, diverse

object appearances, and achieving real-time performance with high accuracy and robustness.

To tackle these challenges, future research should prioritize integrating attention mechanisms to focus on relevant regions, leveraging temporal information from video for tracking occluded objects, and incorporating multi-scale architectures like FPNs to capture fine-grained and contextual information. Additionally, model compression techniques like knowledge distillation, quantization, and pruning can reduce computational complexity for efficient inference. Incorporating meta-learning can enhance generalization to new domains, while explainable AI techniques can provide local explanations, improving transparency and interpretability. Other promising directions include multi-task learning for joint perception tasks, sensor fusion approaches leveraging complementary modalities, and semi-supervised methods to leverage unlabeled data. Ultimately, continued research efforts in these areas, coupled with hardware advancements, will pave the way for safe and reliable autonomous driving by enabling efficient, accurate, and robust object detection systems capable of operating in diverse real-world environment.

BIBLIOGRAPHY:

1. Lyssenko M. A safety-adapted loss for pedestrian detection in automated driving / M. Lyssenko, P. Pimplikar, M. Bieshaar, [et al.]. arXiv, 2024.

2. Mishra S. Real-time pedestrian detection using yolo / S. Mishra, S. Jabin. 2023.

3. Zuo X. Pedestrian detection based on one-stage yolo algorithm / X. Zuo, J. Li, J. Huang, [et al.]. *Journal of Physics: Conference Series.* 2021. Vol. 1871, No. 1. P. 012131.

4. Lan W. Pedestrian detection based on yolo network model. W. Lan, J. Dang, Y. Wang, S. Wang. 2018.

5. Wei J. Infrared pedestrian detection using improved unet and yolo through sharing visible light domain information. J. Wei, S. Su, Z. Zhao, [et al.]. Measurement. 2023. Vol. 221. P. 113442.

6. Zhang Y. A lightweight vehicle-pedestrian detection algorithm based on attention mechanism in traffic scenarios / Y. Zhang, A. Zhou, F. Zhao, H. Wu. Sensors (Basel, Switzerland). 2022. Vol. 22, No. 21. P. 8480.

7. Chen Y. TF-yolo: a transformer–fusion-based yolo detector for multimodal pedestrian detection in autonomous driving scenes / Y. Chen, J. Ye, X. Wan. World Electric Vehicle Journal. 2023. Vol. 14, No. 12. P. 352.

8. Lin M. DETR for crowd pedestrian detection / M. Lin, C. Li, X. Bu, [et al.]. arXiv, 2021.

9. Han W. IDPD: improved deformable-detr for crowd pedestrian detection / W. Han, N. He, X. Wang, [et al.]. Signal, Image and Video Processing. 2024. Vol. 18, No. 3. P. 2243–2253.

10. Yuan J. Effectiveness of vision transformer for fast and accurate single-stage pedestrian detection / J. Yuan, P. Barmpoutis, T. Stathaki. Advances in Neural Information Processing Systems. 2022. Vol. 35. P. 27427–27440.

11. Deng S. Efficient dense pedestrian detection based on transformer / S. Deng, J. Li. 2024.

12. Siam M. MODNet: motion and appearance based moving object detection network for autonomous driving / M. Siam, H. Mahgoub, M. Zahran, [et al.]. 2018.

13. Yahiaoui M. FisheyeMODNet: moving object detection on surround-view cameras for autonomous driving / M. Yahiaoui, H. Rashed, L. Mariotti, [et al.]. arXiv, 2019.

14. Rashed H. BEV-modnet: monocular camera based bird's eye view moving object detection for autonomous driving / H. Rashed, M. Essam, M. Mohamed, [et al.]. 2021.

15. Rashed H. VM-modnet: vehicle motion aware moving object detection for autonomous driving / H. Rashed, A. E. Sallab, S. Yogamani. 2021.

16. Hernandez A. E. G. Recognize moving objects around an autonomous vehicle considering a deep-learning detector model and dynamic bayesian occupancy / A. E. G. Hernandez, O. Erkent, C. Laugier. Shenzhen, China: IEEE, 2020.

17. Ramzy M. RST-modnet: real-time spatio-temporal moving object detection for autonomous driving / M. Ramzy, H. Rashed, A. El Sallab, S. Yogamani. 2019.

18. Jha S. Real time object detection and trackingsystem for video surveillance system. S. Jha, C. Seo, E. Yang, G. P. Joshi. Multimedia Tools and Applications. 2021. Vol. 80, No. 3. P. 3981–3996.

19. Zhou Z. RGB-event fusion for moving object detection in autonomous driving / Z. Zhou, Z. Wu, R. Boutteau, [et al.]. arXiv, 2023.

20. Liu D. Video object detection for autonomous driving: motion-aid feature calibration / D. Liu, Y. Cui, Y. Chen, [et al.]. Neurocomputing. 2020. Vol. 409. P. 1–11.

21. Wang J. Improved yolov5 network for real-time multi-scale traffic sign detection / J. Wang, Y. Chen, M. Gao, Z. Dong. arXiv, 2021.

22. Liu H. ETSR-yolo: an improved multi-scale traffic sign detection algorithm based on yolov5 / H. Liu, K. Zhou, Y. Zhang, Y. Zhang. PLOS ONE. 2023. Vol. 18, No. 12. P. e0295807.

23. Chen T. MFL-yolo: an object detection model for damaged traffic signs / T. Chen, J. Ren. arXiv, 2023.

24. You S. Traffic sign detection method based on improved ssd / S. You, Q. Bi, Y. Ji, [et al.]. Information. 2020. Vol. 11, No. 10. P. 475.

25. Wu J. Traffic sign detection based on ssd combined with receptive field module and path aggregation network / J. Wu, S. Liao. Computational Intelligence and Neuroscience. 2022. Vol. 2022. P. 4285436.

26. Greer R. Salient sign detection in safe autonomous driving: ai which reasons over full visual context / R. Greer, A. Gopalkrishnan, N. Deo, [et al.]. arXiv, 2023.

27. Greer R. Robust traffic light detection using salience-sensitive loss: computational framework and evaluations / R. Greer, A. Gopalkrishnan, J. Landgren, [et al.]. arXiv, 2023.

28. Farzipour A. Traffic sign recognition using local vision transformer / A. Farzipour, O. N. Manzari, S. B. Shokouhi. arXiv, 2023.

29. Xia J. DSRA-detr: an improved detr for multiscale traffic sign detection / J. Xia, M. Li, W. Liu, X. Chen. Sustainability. 2023. Vol. 15, No. 14. P. 10862.

30. Chen S. A semi-supervised learning framework combining cnn and multiscale transformer for traffic sign detection and recognition / S. Chen, Z. Zhang, L. Zhang, [et al.]. *IEEE Internet of Things Journal*. 2024. Vol. 11, No. 11. P. 19500–19519.

31. Hu S. PseudoProp: robust pseudo-label generation for semi-supervised object detection in autonomous driving systems / S. Hu, C.-H. Liu, J. Dutta, [et al.]. 2022.

32. Chen W. Robust object detection for autonomous driving based on semi-supervised learning / W. Chen, J. Yan, W. Huang, [et al.]. Security and Safety. 2024. Vol. 3. P. 2024002.

33. He Y. Pseudo-label correction and learning for semi-supervised object detection / Y. He, W. Chen, K. Liang, [et al.]. arXiv, 2023.

34. Shehzadi T. Sparse semi-detr: sparse learnable queries for semi-supervised object detection / T. Shehzadi, K. A. Hashmi, D. Stricker, M. Z. Afzal. arXiv, 2024.

35. Miraliev S. Real-time memory efficient multitask learning model for autonomous driving / S. Miraliev, S. Abdigapporov, V. Kakani, H. Kim. IEEE Transactions on Intelligent Vehicles. 2024. Vol. 9, No. 1. P. 247–258.

36. Mahaur B. An improved lightweight small object detection framework applied to real-time autonomous driving / B. Mahaur, K. K. Mishra, A. Kumar. Expert Systems with Applications. 2023. Vol. 234. P. 121036.

37. Zhou Q. DPNet: dual-path network for real-time object detection with lightweight attention / Q. Zhou, H. Shi, W. Xiang, [et al.]. arXiv, 2022.

38. Wang A. YOLOv10: real-time end-to-end object detection / A. Wang, H. Chen, L. Liu, [et al.]. arXiv, 2024.

39. Zhao Y. DETRs beat yolos on real-time object detection / Y. Zhao, W. Lv, S. Xu, [et al.]. arXiv, 2024.

40. Wang X. Low-light traffic objects detection for automated vehicles / X. Wang, D. Wang, S. Li, [et al.]. 2022.

41. Pham L. H. Low-light image enhancement for autonomous driving systems using driveretinex-net / L. H. Pham, D. N.-N. Tran, J. W. Jeon. 2020.

42. Qiu Y. IDOD-yolov7: image-dehazing yolov7 for object detection in low-light foggy traffic environments / Y. Qiu, Y. Lu, Y. Wang, H. Jiang. Sensors. 2023. Vol. 23, No. 3. P. 1347.

43. Liu W. Image-adaptive yolo for object detection in adverse weather conditions / W. Liu, G. Ren, R. Yu, [et al.]. arXiv, 2022.

44. Guo Z. HawkDrive: a transformer-driven visual perception system for autonomous driving in night scene / Z. Guo, S. Perminov, M. Konenkov, D. Tsetserukou. arXiv, 2024.

45. Ye L. VELIE: a vehicle-based efficient low-light image enhancement method for intelligent vehicles / L. Ye, D. Wang, D. Yang, [et al.]. Sensors. 2024. Vol. 24, No. 4. P. 1345.

46. Zhang S. Guided attention in cnns for occluded pedestrian detection and re-identification / S. Zhang, D. Chen, J. Yang, B. Schiele. *International Journal of Computer Vision.* 2021. Vol. 129, No. 6. P. 1875–1892.

47. Zou T. Attention guided neural network models for occluded pedestrian detection / T. Zou, S. Yang, Y. Zhang, M. Ye. Pattern Recognition Letters. 2020. Vol. 131. P. 91–97.

48. Qi M. Exploring reliable infrared object tracking with spatio-temporal fusion transformer / M. Qi, Q. Wang, S. Zhuang, [et al.]. Knowledge-Based Systems. 2024. Vol. 284. P. 111234.

49. Huang T. Dense pedestrian detection based on multiple link feature pyramid networks / T. Huang, S. Yang, T. Yu, X. Fu. Hangzhou, China: SPIE, 2023.

50. Yahya M. Object detection and recognition in autonomous vehicles using fast region-convolutional neural network / M. Yahya, R. A. Reddy, K. Al-Attabi, [et al.]. 2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS). 2023. P. 1–5.

51. Dang J. HA-fpn: hierarchical attention feature pyramid network for object detection / J. Dang, X. Tang, S. Li. Sensors. 2023. Vol. 23, No. 9. P. 4508.

52. Xie B. FocusTR: focusing on valuable feature by multiple transformers for fusing feature pyramid on object detection / B. Xie, L. Yang, Z. Yang, [et al.]. 2022 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). 2022. P. 518–525.

53. Liu H. Flexi-compression: a flexible model compression method for autonomous driving / H. Liu, Y. He, F. R. Yu, J. James. Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications. 2021. P. 19–26.

54. Youn E. Compressing vision transformers for low-resource visual learning / E. Youn, S. M. J, S. Prabhu, S. Chen. 2023.

55. Lan Q. Instance, scale, and teacher adaptive knowledge distillation for visual detection in autonomous driving / Q. Lan, Q. Tian. IEEE Transactions on Intelligent Vehicles. 2023. Vol. 8, No. 3. P. 2358–2370.

56. Agand P. Knowledge distillation from single-task teachers to multi-task student for end-to-end autonomous driving / P. Agand. Proceedings of the AAAI Conference on Artificial Intelligence. 2024. Vol. 38, No. 21. P. 23375–23376.

57. Li Z. Quasar-vit: hardware-oriented quantization-aware architecture search for vision transformers / Z. Li, A. Lu, Y. Xie, [et al.]. 2024.

58. Sun E. Transformer-based few-shot object detection in traffic scenarios / E. Sun, D. Zhou, Y. Tian, [et al.]. Applied Intelligence. 2024. Vol. 54, No. 1. P. 947–958.

59. Dong J. Why did the ai make that decision? towards an explainable artificial intelligence (xai) for autonomous driving systems / J. Dong, S. Chen, M. Miralinaghi, [et al.]. Transportation Research Part C: Emerging Technologies. 2023. Vol. 156. P. 104358.

60. Cultrera, Luca. Visual attention and explainability in end-to-end autonomous driving / Cultrera, Luca. 2023.

61. Adom I. RB-xai: relevance-based explainable ai for traffic detection in autonomous systems / I. Adom, M. N. Mahmoud. SoutheastCon 2024. P. 1358–1367.

62. Kolekar S. Explainable ai in scene understanding for autonomous vehicles in unstructured traffic environments on indian roads using the inception u-net model with grad-cam visualization / S. Kolekar, S. Gite, B. Pradhan, A. Alamri. Sensors. 2022. Vol. 22, No. 24. P. 9677.

REFERENCES:

1. Lyssenko, M. A. (2024). safety-adapted loss for pedestrian detection in automated driving / M. Lyssenko, P. Pimplikar, M. Bieshaar, [et al.]. arXiv

2. Mishra, S. (2023). Real-time pedestrian detection using yolo / S. Mishra, S. Jabin.

3. Zuo, X. (2021). Pedestrian detection based on one-stage yolo algorithm / X. Zuo, J. Li, J. Huang, [et al.]. *Journal of Physics: Conference Series*. Vol. 1871, No. 1. P. 012131.

4. Lan, W. (2018). Pedestrian detection based on yolo network model / W. Lan, J. Dang, Y. Wang, S. Wang.

5. Wei, J. (2023). Infrared pedestrian detection using improved unet and yolo through sharing visible light domain information / J. Wei, S. Su, Z. Zhao, [et al.]. Measurement. Vol. 221. P. 113442.

6. Zhang, Y. A. (2022). lightweight vehicle-pedestrian detection algorithm based on attention mechanism in traffic scenarios / Y. Zhang, A. Zhou, F. Zhao, H. Wu. Sensors (Basel, Switzerland). Vol. 22, No. 21. P. 8480.

7. Chen, Y. (2023). TF-yolo: a transformer–fusion-based yolo detector for multimodal pedestrian detection in autonomous driving scenes / Y. Chen, J. Ye, X. Wan. World Electric Vehicle Journal. Vol. 14, No. 12. P. 352.

8. Lin, M. (2021). DETR for crowd pedestrian detection / M. Lin, C. Li, X. Bu, [et al.]. arXiv,

9. Han, W. (2024). IDPD: improved deformable-detr for crowd pedestrian detection / W. Han, N. He, X. Wang, [et al.]. Signal, Image and Video Processing. Vol. 18, No. 3. P. 2243–2253.

10. Yuan, J. (2022). Effectiveness of vision transformer for fast and accurate single-stage pedestrian detection / J. Yuan, P. Barmpoutis, T. Stathaki. Advances in Neural Information Processing Systems. Vol. 35. P. 27427–27440.

11. Deng, S. (2024). Efficient dense pedestrian detection based on transformer / S. Deng, J. Li.

12. Siam, M. (2018). MODNet: motion and appearance based moving object detection network for autonomous driving / M. Siam, H. Mahgoub, M. Zahran, [et al.].

13. Yahiaoui, M. (2019). FisheyeMODNet: moving object detection on surround-view cameras for autonomous driving / M. Yahiaoui, H. Rashed, L. Mariotti, [et al.]. arXiv,

14. Rashed, H. (2021). BEV-modnet: monocular camera based bird's eye view moving object detection for autonomous driving / H. Rashed, M. Essam, M. Mohamed, [et al.].

15. Rashed, H. (2021). VM-modnet: vehicle motion aware moving object detection for autonomous driving / H. Rashed, A. E. Sallab, S. Yogamani.

16. Hernandez, A. E. G. (2020). Recognize moving objects around an autonomous vehicle considering a deep-learning detector model and dynamic bayesian occupancy / A. E. G. Hernandez, O. Erkent, C. Laugier. Shenzhen, China: IEEE.

17. Ramzy, M. (2019). RST-modnet: real-time spatio-temporal moving object detection for autonomous driving / M. Ramzy, H. Rashed, A. El Sallab, S. Yogamani.

18. Jha, S. (2021). Real time object detection and trackingsystem for video surveillance system / S. Jha, C. Seo, E. Yang, G. P. Joshi. Multimedia Tools and Applications. Vol. 80, No. 3. P. 3981–3996.

19. Zhou, Z. (2023). RGB-event fusion for moving object detection in autonomous driving / Z. Zhou, Z. Wu, R. Boutteau, [et al.]. arXiv,

20. Liu, D. (2020). Video object detection for autonomous driving: motion-aid feature calibration / D. Liu, Y. Cui, Y. Chen, [et al.]. Neurocomputing. Vol. 409. P. 1–11.

21. Wang, J. (2021). Improved yolov5 network for real-time multi-scale traffic sign detection / J. Wang, Y. Chen, M. Gao, Z. Dong. arXiv,

22. Liu, H. (2023). ETSR-yolo: an improved multi-scale traffic sign detection algorithm based on yolov5 / H. Liu, K. Zhou, Y. Zhang, Y. Zhang. PLOS ONE. Vol. 18, No. 12. P. e0295807.

23. Chen, T. (2023). MFL-yolo: an object detection model for damaged traffic signs / T. Chen, J. Ren. arXiv,

24. You, S. (2020). Traffic sign detection method based on improved ssd / S. You, Q. Bi, Y. Ji, [et al.]. Information. Vol. 11, No. 10. P. 475.

25. Wu, J. (2022). Traffic sign detection based on ssd combined with receptive field module and path aggregation network / J. Wu, S. Liao. Computational Intelligence and Neuroscience. Vol. 2022. P. 4285436.

26. Greer, R. (2023). Salient sign detection in safe autonomous driving: ai which reasons over full visual context. R. Greer, A. Gopalkrishnan, N. Deo, [et al.]. arXiv,

27. Greer, R. (2023). Robust traffic light detection using salience-sensitive loss: computational framework and evaluations. R. Greer, A. Gopalkrishnan, J. Landgren, [et al.]. arXiv,

28. Farzipour, A. (2023). Traffic sign recognition using local vision transformer / A. Farzipour, O. N. Manzari, S. B. Shokouhi. arXiv.

29. Xia, J. (2023). DSRA-detr: an improved detr for multiscale traffic sign detection / J. Xia, M. Li, W. Liu, X. Chen. Sustainability. Vol. 15, No. 14. P. 10862.

30. Chen, S. (2024). A semi-supervised learning framework combining cnn and multiscale transformer for traffic sign detection and recognition / S. Chen, Z. Zhang, L. Zhang, [et al.]. IEEE Internet of Things Journal. Vol. 11, No. 11. P. 19500–19519.

31. Hu, S. (2022). PseudoProp: robust pseudo-label generation for semi-supervised object detection in autonomous driving systems. S. Hu, C.-H. Liu, J. Dutta, [et al.].

32. Chen, W. (2024). Robust object detection for autonomous driving based on semi-supervised learning / W. Chen, J. Yan, W. Huang, [et al.]. Security and Safety. Vol. 3. P. 2024002.

33. He, Y. (2023). Pseudo-label correction and learning for semi-supervised object detection / Y. He, W. Chen, K. Liang, [et al.]. arXiv,

34. Shehzadi, T. (2024). Sparse semi-detr: sparse learnable queries for semi-supervised object detection / T. Shehzadi, K. A. Hashmi, D. Stricker, M. Z. Afzal. arXiv,

35. Miraliev, S. (2024). Real-time memory efficient multitask learning model for autonomous driving / S. Miraliev, S. Abdigapporov, V. Kakani, H. Kim. IEEE Transactions on Intelligent Vehicles. Vol. 9, No. 1. P. 247–258.

36. Mahaur, B. (2023). An improved lightweight small object detection framework applied to real-time autonomous driving / B. Mahaur, K. K. Mishra, A. Kumar. Expert Systems with Applications. Vol. 234. P. 121036.

37. Zhou, Q. (2022). DPNet: dual-path network for real-time object detection with lightweight attention / Q. Zhou, H. Shi, W. Xiang, [et al.]. arXiv,

38. Wang, A. (2024). YOLOv10: real-time end-to-end object detection / A. Wang, H. Chen, L. Liu, [et al.]. arXiv,

39. Zhao, Y. (2024). DETRs beat yolos on real-time object detection / Y. Zhao, W. Lv, S. Xu, [et al.]. arXiv,

40. Wang, X. (2022). Low-light traffic objects detection for automated vehicles / X. Wang, D. Wang, S. Li, [et al.].

41. Pham, L. H. (2020). Low-light image enhancement for autonomous driving systems using driveretinex-net / L. H. Pham, D. N.-N. Tran, J. W. Jeon.

42. Qiu, Y. (2023). IDOD-yolov7: image-dehazing yolov7 for object detection in low-light foggy traffic environments / Y. Qiu, Y. Lu, Y. Wang, H. Jiang. Sensors. Vol. 23, No. 3. P. 1347.

43. Liu, W. (2022). Image-adaptive yolo for object detection in adverse weather conditions / W. Liu, G. Ren, R. Yu, [et al.]. arXiv.

44. Guo, Z. (2024). HawkDrive: a transformer-driven visual perception system for autonomous driving in night scene / Z. Guo, S. Perminov, M. Konenkov, D. Tsetserukou. arXiv.

45. Ye, L. (2024). VELIE: a vehicle-based efficient low-light image enhancement method for intelligent vehicles / L. Ye, D. Wang, D. Yang, [et al.]. Sensors. Vol. 24, No. 4. P. 1345.

46. Zhang, S. (2021). Guided attention in cnns for occluded pedestrian detection and re-identification / S. Zhang, D. Chen, J. Yang, B. Schiele. *International Journal of Computer Vision*. Vol. 129, No. 6. P. 1875–1892.

47. Zou, T. (2020). Attention guided neural network models for occluded pedestrian detection / T. Zou, S. Yang, Y. Zhang, M. Ye. Pattern Recognition Letters. Vol. 131. P. 91–97.

48. Qi, M. (2024). Exploring reliable infrared object tracking with spatio-temporal fusion transformer / M. Qi, Q. Wang, S. Zhuang, [et al.]. Knowledge-Based Systems. Vol. 284. P. 111234.

49. Huang, T. (2023). Dense pedestrian detection based on multiple link feature pyramid networks / T. Huang, S. Yang, T. Yu, X. Fu. Hangzhou, China: SPIE.

50. Yahya, M. (2023). Object detection and recognition in autonomous vehicles using fast region-convolutional neural network / M. Yahya, R. A. Reddy, K. Al-Attabi, [et al.]. 2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS). P. 1–5.

51. Dang, J. (2023). HA-fpn: hierarchical attention feature pyramid network for object detection / J. Dang, X. Tang, S. Li. Sensors. Vol. 23, No. 9. P. 4508.

52. Xie, B. (2022). FocusTR: focusing on valuable feature by multiple transformers for fusing feature pyramid on object detection / B. Xie, L. Yang, Z. Yang, [et al.]. 2022 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). P. 518–525.

53. Liu, H. (2021). Flexi-compression: a flexible model compression method for autonomous driving / H. Liu, Y. He, F. R. Yu, J. James. Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications. P. 19–26.

54. Youn, E. (2023). Compressing vision transformers for low-resource visual learning / E. Youn, S. M. J, S. Prabhu, S. Chen.

55. Lan, Q. (2023). Instance, scale, and teacher adaptive knowledge distillation for visual detection in autonomous driving / Q. Lan, Q. Tian. IEEE Transactions on Intelligent Vehicles. Vol. 8, No. 3. P. 2358–2370.

56. Agand, P. (2024). Knowledge distillation from single-task teachers to multi-task student for end-to-end autonomous driving / P. Agand Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 38, No. 21. P. 23375–23376.

57. Li, Z. (2024). Quasar-vit: hardware-oriented quantization-aware architecture search for vision transformers / Z. Li, A. Lu, Y. Xie, [et al.].

58. Sun, E. (2024). Transformer-based few-shot object detection in traffic scenarios / E. Sun, D. Zhou, Y. Tian, [et al.]. Applied Intelligence. Vol. 54, No. 1. P. 947–958.

59. Dong, J. (2023). Why did the ai make that decision? towards an explainable artificial intelligence (xai) for autonomous driving systems / J. Dong, S. Chen, M. Miralinaghi, [et al.]. Transportation Research Part C: Emerging Technologies. Vol. 156. P. 104358.

60. Cultrera, Luca. (2023). Visual attention and explainability in end-to-end autonomous driving / Cultrera, Luca.

61. Adom, I. (2024). RB-xai: relevance-based explainable ai for traffic detection in autonomous systems / I. Adom, M. N. Mahmoud. SoutheastCon. P. 1358–1367.

62. Kolekar, S. (2022). Explainable ai in scene understanding for autonomous vehicles in unstructured traffic environments on indian roads using the inception u-net model with grad-cam visualization / S. Kolekar, S. Gite, B. Pradhan, A. Alamri. Sensors. Vol. 22, No. 24. P. 9677.

UDC 004.932.72
DOI https://doi.org/10.32782/IT/2024-3-2

Kyrylo ANTOSHYN
PhD Student at the Department of Computer Science, Zaporizhzhia National University, 66, Universytets'ka Str., Zaporizhzhia, Ukraine, 69600, kyrylo.antoshyn@gmail.com
***ORCID:** 0009-0001-4166-5418*

Yuliia LYMARENKO
Candidate of Technical Sciences, Associate Professor at the Department of Software Engineering, Zaporizhzhia National University, 66, Universytets'ka Str., Zaporizhzhia, Ukraine, 69600, yuliia.lymarenko@gmail.com
***ORCID:** 0000-0002-1643-6939*

To cite this article: Antoshyn, K., Lymarenko, Yu. (2024). Rozrobka metodu na osnovi rozpiznavannia obiektiv dlia vyznachennia polozhennia liudyny v obmezhenomu prostori u realnomu chasi [Development of a method based on object detection for real-time person location detection in a confined space]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 14–22, doi: https://doi.org/10.32782/IT/2024-3-2

DEVELOPMENT OF A METHOD BASED ON OBJECT DETECTION FOR REAL-TIME PERSON LOCATION DETECTION IN A CONFINED SPACE

Real-time person detection provides an opportunity to solve such a complex problem as person location detection in a confined space. The solution to this issue lies in the implementation of an effective method to localize a person inside a confined space (for example, inside the room) since outdoor positioning systems like GPS do not provide high accuracy indoors. Existing computer systems that solve this problem require specialized infrastructure: devices attached to the human body, sensors, etc. This approach is not cheap and does not provide a universal solution. A device that is present in almost every building is a camera. Many existing computer systems that analyze the video stream use Kinect depth cameras, which are outdated and require additional installation. There is a limited number of solutions that analyze video stream from an RGB camera in combination with computer vision methods for person localization. Therefore, research and development of a more effective method for the above-mentioned problem using computer vision is relevant.

***The aim** of the work is to develop a method of localizing a person in a confined space that is efficient in terms of speed and accuracy, which would use the video stream of the camera in combination with the computer vision method – object detection. The method should work on an NVIDIA Jetson Nano microcomputer (which is a relatively cheap and popular solution from NVIDIA) in real-time.*

***The methodology** for solving the problem is to leverage a deep neural network to detect the person in real-time and then use a perspective transformation algorithm to estimate the person's location. A person's location is the center point of the bottom edge of the bounding box transformed from the camera perspective in a way as if the camera was positioned directly above the floor. YOLOv4-tiny neural network model was trained on the COCO and Open Images datasets using the Darknet deep learning framework.*

***The scientific novelty** is that the method for person indoor localization was developed, which is based on the combination of a person detection method using a deep convolutional neural network and perspective transformation algorithm for further location estimation in a confined space. The proposed method is more versatile than known methods that use Kinect depth cameras. The proposed method can work on a microcomputer and estimate the location of several people in one pass with an average error of 23 cm and with a speed of 16 FPS, which is superior to the known alternative approaches.*

***Conclusions.** The problem of real-time person location detection in a confined space and means of solving it based on object detection using a deep convolutional neural network are studied. A neural network, based on the YOLOv4-tiny model, was trained using the COCO and Open Images datasets, and showed an accuracy of 55.1% and 71.4%, respectively. A method has been developed that uses a trained neural network to determine a bounding box around a person in the frame, and then determines its position using a perspective transformation algorithm: the method works on an NVIDIA Jetson Nano microcomputer with an average error of 23 cm and a speed of 16 FPS, processing a video stream from the RGB camera.*

***Key words:** person indoor localization, person detection, perspective transformation, deep learning, convolutional neural network, YOLO, NVIDIA Jetson Nano.*

Кирило АНТОШИН
аспірант кафедри комп'ютерних наук, Запорізький національний університет, вул. Університетська, 66, м. Запоріжжя, Україна, 69600
***ORCID:** 0009-0001-4166-5418*

Юлія ЛИМАРЕНКО
кандидат технічних наук, доцент кафедри програмної інженерії, Запорізький національний університет, вул. Університетська, 66, м. Запоріжжя, Україна, 69600
***ORCID:** 0000-0002-1643-6939*

Бібліографічний опис статті: Антошин, К., Лимаренко, Ю. (2024). Розробка методу на основі розпізнавання об'єктів для визначення положення людини в обмеженому просторі у реальному часі. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 14–22, doi: https://doi.org/10.32782/IT/2024-3-2

РОЗРОБКА МЕТОДУ НА ОСНОВІ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ ДЛЯ ВИЗНАЧЕННЯ ПОЛОЖЕННЯ ЛЮДИНИ В ОБМЕЖЕНОМУ ПРОСТОРІ У РЕАЛЬНОМУ ЧАСІ

Розпізнавання людини в режимі реального часу дає можливість вирішувати таку складну проблему як визначення положення людини в обмеженому просторі. Розв'язання даної задачі полягає в реалізації ефективного методу локалізації людини в замкнутому просторі (наприклад, всередині кімнати), оскільки системи позиціонування у відкритому просторі, такі як GPS, не забезпечують високої точності у приміщенні. Існуючі комп'ютерні системи, які вирішують дану проблему, потребують спеціалізованої інфраструктури: пристроїв, прикріплених до тіла людини, датчиків тощо. Такий підхід недешевий і не дає універсального рішення. Пристрій, який наявний практично в кожній будівлі – це камера. Переважна більшість існуючих комп'ютерних систем, які аналізують відеопотік, використовують камери глибини Kinect, які є застарілими та потребують додаткового встановлення. Існує обмежена кількість рішень, які аналізують відеопотік з RGB камери у поєднанні з методами комп'ютерного зору для локалізації людини. Отже, дослідження та розробка ефективнішого методу вирішення вищезазначеної проблеми з використанням комп'ютерного зору є актуальним.

***Метою роботи** є розробка ефективного за швидкістю та точністю методу локалізації людини в приміщенні, який би використовував відеопотік камери в поєднанні з методом комп'ютерного зору – розпізнавання об'єктів. Метод повинен працювати на мікрокомп'ютері NVIDIA Jetson Nano (який є відносно дешевим і популярним рішенням від NVIDIA) в режимі реального часу.*

***Методологія** вирішення проблеми полягає у використанні глибокої нейронної мережі для розпізнавання людини в режимі реального часу разом з алгоритмом перспективного перетворення для подальшої оцінки положення людини. Положення людини – це центральна точка нижньої сторони обмежувальної рамки, трансформована з перспективи камери таким чином, ніби камера розташована прямо над підлогою. Модель нейронної мережі YOLOv4-tiny була навчена на наборах даних COCO та Open Images за допомогою фреймворку глибокого навчання Darknet.*

***Наукова новизна** полягає в тому, що було розроблено метод локалізації людини в приміщенні, який базується на поєднанні методу виявлення людини за допомогою глибокої згорткової нейронної мережі та алгоритму перспективного перетворення для подальшого визначення положення в обмеженому просторі. Запропонований метод є більш універсальним за відомі методи, які використовують камери глибини Kinect. Запропонований метод може працювати на мікрокомп'ютері та визначати положення декількох людей за один прохід із середньою похибкою 23 см та швидкістю 16 FPS, що є кращим за відомі альтернативні підходи.*

***Висновки.** Досліджена проблема визначення положення людини в обмеженому просторі у реальному часі та засоби її вирішення на основі розпізнавання об'єктів з використанням глибокої згорткової нейронної мережі. Проведено навчання нейронної мережі на основі моделі YOLOv4-tiny з використанням датасетів COCO та Open Images, яке показало точність 55.1% та 71.4% відповідно. Розроблено метод, який використовує навчену нейронну мережу для визначення обмежувальної рамки навколо людини у кадрі, а після – визначає її положення з використанням алгоритму перспективного перетворення: метод працює на мікрокомп'ютері NVIDIA Jetson Nano із середньою похибкою 23 см та швидкістю 16 FPS, обробляючи відеопотік з RGB камери.*

***Ключові слова:** локалізація людини в приміщенні, розпізнавання людини, трансформація перспективи, глибоке навчання, згорткова нейронна мережа, YOLO, NVIDIA Jetson Nano.*

The urgency of the problem. The development of artificial intelligence makes our life more optimized. One of the tasks that we have successfully automated is real-time object detection. The possibility of person detection is the cornerstone for solving more complex problems, one of which is real-time person location detection in a confined space.

A computer system that effectively solves this problem can be implemented in various areas of our life. For example, we can create a notification system that will respond to the movement of people in locations that may be dangerous or prohibited: areas with harmful substances in enterprises, areas with confidential information in security agencies, spaces with valuable exhibits in museums, etc. Such notification systems can be extended to improve the quality of life of people with disabilities: the system will help people with visual impairments to successfully move around the house by providing voice prompts depending on their location. In addition, we can create recreation areas for children and adults of a completely new level: a system in a shopping and entertainment center will project images from a projector onto the floor and reproduce effects under people in the areas they walk.

To implement such systems, we need to develop a method for person indoor localization. Outdoor positioning technologies like GPS do not provide high accuracy indoors, because signals from satellites can be affected by surroundings like walls, roofs, tunnels etc. Many of the existing computer systems that solve this problem require specialized infrastructure for their work: devices attached to the human body, sensors, etc. This approach is not cheap and does not provide a universal solution. A device that is available in almost every modern building is a camera, the video stream from which we can leverage as input data.

Many existing computer systems that analyze the video stream use Kinect depth cameras, which are outdated and require additional installation. There is a limited number of solutions that analyze video stream from an RGB camera in combination with computer vision methods for person localization. Researchers in the field of artificial intelligence create not only accurate, but also fast and lightweight models of neural networks (for example, YOLOv4-tiny), which can be trained to detect objects on relatively inexpensive graphics processors (for example, NVIDIA GeForce GTX 1050) and used on microcomputers optimized for solving high-performance tasks (for example, NVIDIA Jetson Nano). This approach guarantees a much lower price for the hardware complex, as well as data security since all calculations take place locally.

Therefore, research and development of a more effective method for the above-mentioned problem using computer vision is relevant.

Analysis of recent research and publications.

An overview of real-time person location detection in a confined space problem.

Rainer Mautz conducts an overview of the problem of determining the location of objects, including people, in a confined space, and describes available technologies for its solution as well as shows areas in which the solution to the problem has practical value (Mautz, 2012). He states that the dominating technologies for positioning in outdoor environments, called Global Navigation Satellite Systems (GNSS), perform poorly within buildings. Researcher illustrates 13 technologies for indoor positioning: cameras, Wi-Fi, Bluetooth, and others. Based on his research, cameras provide high accuracy, but computer systems based on this technology can work at room level only.

Oussama Kerdjidj et al. provide a comprehensive overview of indoor localization problem with the focus on deep learning approaches (Kerdjidj, Himeur, Sohail et al., 2024). Researchers outline recent studies that use various architectures of deep neural networks to achieve robust indoor localization: convolutional neural networks (CNNs), recurrent neural networks (RNNs) or hybrid models. They state that deep learning-based methods are resilient against noise and missing data.

An overview of solutions to real-time person location detection in a confined space problem.

Adrian Cosma et al. provide an overview of solutions to the real-time person location detection in a confined space problem (Cosma, Radoi, Radu, 2018). They claim that all existing solutions can be divided into two groups: solutions that require a specialized infrastructure for their work and solutions that use the existing infrastructure such as wireless access points, surveillance cameras in buildings and inertial sensors in mobile devices. Researchers state that most of the recent solutions of the second group use smartphone sensors and Wi-Fi, however, systems that use video stream from cameras also exist. Camera-based systems use computer vision algorithms and do not require users to wear special sensors, which simplifies the use of such systems in cases where users are not well-versed in information technologies.

Many of the existing computer vision-based systems use depth cameras (RGB-D) to solve the problem. Huan Wang et al. developed a novel RGB-D camera-based indoor occupancy

positioning system called CIOPS-RGBD (Wang, Wang, Li, 2023). Researchers were using 4 Kinect cameras to take color and depth images simultaneously. The idea was to combine results taken from various cameras: data fusion and 3D reconstruction algorithm was designed and developed. They used OpenPose library to extract keypoints (shoulders and neck) that were aligned on the depth image. Their system achieves excellent accuracy within 20 cm in a scenario when people are sitting. However, it takes 5 seconds (0.2 FPS) to localize people (CPU: 9980, GPU: 2080TI), which is not enough for real-time. The main drawback of the system, according to its authors, is that the operation distance and perspective of the RGB-D sensor are limited: when used in larger spaces, more cameras are required.

Adrian Cosma et al. developed a computer system that uses a video stream from an RGB camera as input data and works on a device with limited resources (Cosma, Radoi, Radu, 2018). The system processes the video stream using a deep neural network to estimate a person's key points. The obtained data are used to determine the person's location in a confined space. The person's location is the midpoint between their legs, transformed from the camera's perspective relative to the floor. The average error of their system is 36 cm, and the speed is 6.25 FPS.

Ángel Carro-Lagoa et al. developed a computer system that consists of several microcomputers (edge devices) with connected cameras (Carro-Lagoa, Barral, González-López et al., 2023). Each microcomputer estimates a person's location using pose estimation and then sends this information to the Real-time Location System (RTLS) server. The server performs multicamera tracking of the detected person. The average error of their system is below 40 cm, and the speed is 2 FPS.

To estimate a person's location in a confined space using computer vision, it is required to solve two problems in succession. First, we need to detect the person in the frame. Then, we need to estimate the person's location from the perspective of the camera relative to the confined space (floor). To solve the first problem, it is effective to use a deep neural network. Since there are new versions of YOLO like YOLOv4, YOLOv4-tiny etc., we can leverage object detection method instead of keypoint detection. Keypoint detection method's disadvantage is the considerable number of frames in which the neural network cannot detect a person (Cosma, Radoi, Radu, 2018). To solve the second problem, we can leverage perspective transformation.

An overview of real-time person detection problem.

Object detection in the image is object localization with bounding box and object classification. Ross Girshick et al. in 2014 developed one of the first CNN-based methods for object detection – R-CNN (Girshick, Donahue, Darrell et al., 2014). The approach consists in generating approximately 2000 regions of interest in the image using a Selective Search algorithm. The warped regions are fed into a convolutional neural network (CNN) for features extraction. After that, Support Vector Machines (SVMs) are used for objects classification. The main drawback of their approach is that it takes 49 seconds to detect objects, because CNN needs to run for each region of interest. Two improvements of R-CNN were developed: Fast R-CNN (Girshick, 2015) and Faster R-CNN (Ren, He, Girshick et al., 2016). These methods detect objects in the image 2.3 seconds and 0.2 seconds (5 FPS) respectively, which is not enough for real-time. Accuracy of Faster R-CNN on the PASCAL VOC 2007 dataset is 73.2%.

Joseph Redmon et al. in 2016 developed a much faster, but less accurate detector called YOLO (You Only Look Once) (Redmon, Divvala, Girshick et al., 2016). YOLO uses a single neural network to predict bounding boxes and class probabilities in one evaluation. This eliminates the need for a detection pipeline that the R-CNN family methods use, and the system can be optimized end-to-end directly on detection performance. YOLO works at 45 FPS with 63.4% precision on the PASCAL VOC 2007 dataset, which is only 10% less than the Faster R-CNN method.

Alex Bochkovskiy et al. in 2020 presented YOLOv4 detector, which is the next generation of YOLOv3 (Bochkovskiy, Wang, Liao, 2020). The idea behind YOLOv4 is that researchers introduced new features to the YOLO model to improve accuracy like Weighted-Residual-Connections (WRC), Mish-activation and others. They achieved 43.5% precision on the COCO dataset at a speed of ~65 FPS on Tesla V100.

The logic behind selection of model, framework, datasets, and computer vision library for real-time person detection problem.

The aim of the work is that the developed method for indoor positioning should work on the NVIDIA Jetson Nano microcomputer in real-time. The YOLOv4-tiny model is a deep CNN, smaller version of YOLOv4, which can work on the microcomputer. The main advantage of YOLOv4-tiny is its speed: it works at a speed of 371 FPS on the NVIDIA GeForce GTX 1080 Ti GPU and achieves an accuracy of 40.2% on the COCO dataset.

YOLOv4-tiny outperforms other models that can work on microcomputers: MobileNetV3 (Howard, Sandler, Chu et al., 2019) and SqueezeNet (Iandola, Han, Moskewicz et al., 2016).

For model training we have chosen Darknet framework – an open-source deep learning framework written in C/C++ that is primarily leveraged to train and use YOLOv2, YOLOv3, YOLOv4 models, and their lightweight versions. Its initial developer was Joseph Redmon, the author of the original YOLO model. Alex Bochkovskiy, author of YOLOv4, continued his work by adding support for new layers, activation functions, ability to work on Windows and more (Bochkovskiy, 2020).

Common Objects in Context (COCO) dataset has been chosen for model training. COCO is a widely used large-scale dataset containing images of complex everyday scenes. It contains annotations for solving the following tasks: object detection, key points detection, pose estimation, object segmentation and generation of text descriptions for images. COCO includes 1.5 million objects of 80 classes (categories) and 200 thousand annotated images (Lin, Maire, Belongie et al., 2015).

Open Images (The Open Images Dataset V4, OID V4) dataset has been chosen for model training too. Open Images is a large-scale dataset containing about 9.2 million annotated images. It includes 19.8 thousand object classes for classification, 600 object classes for detection, and 57 object classes for visual relationship recognition. The images contain complex scenes with an average of 8 objects (Kuznetsova, Rom, Alldrin et al., 2020).

OpenCV library has been chosen to use trained YOLO model: Alex Bochkovskiy states that YOLOv4-tiny works at 773 FPS on the NVIDIA GeForce RTX 2080 Ti, if OpenCV is used, compared to 443 FPS if Darknet is used. OpenCV is an open-source computer vision library written in C++. OpenCV includes algorithms for image processing and transformation, functionality for working with video, as well as module for using deep neural networks (dnn module).

An overview of a person coordinate estimation in a confined space problem.

After the detector has detected a person in the frame, it is necessary to determine their coordinate (middle point of the bottom edge of the bounding box) relative to the confined space (floor) from the perspective of the camera. To solve the problem, we need to select 4 points on the floor from the camera perspective, 4 points of the destination image and calculate the matrix for perspective transformation. After that, we will be able to transform any point in the projection area from the perspective of the camera. Perspective transformation can be achieved using OpenCV (Shaikh, 2020).

The purpose of the article.

The purpose of the article is to present analysis of recent research regarding real-time person indoor localization problem as well as to demonstrate a developed method that effectively solves this problem in terms of speed and accuracy: the method works on the NVIDIA Jetson Nano microcomputer by processing RGB camera video stream in real-time and outperforms existing alternatives.

Presenting main material.

The developed method is based on solving two problems step-by-step: detect a person in real-time using deep convolutional neural network and then estimate person's location using perspective transformation algorithm. Below solutions to each problem are precisely described as well as comparison with similar methods is outlined.

Training YOLOv4-tiny models to detect people.

The training was conducted on a Windows laptop with Intel Core i7-8550U CPU and NVIDIA GeForce GTX 1050 GPU. To train the YOLOv4-tiny model, the Darknet framework and its dependencies (the CUDA Toolkit, the cuDNN and OpenCV libraries) were installed.

After setting up the training environment, images of people from COCO and Open Images datasets were prepared. The developer of the Darknet framework states that the size of the training set should be between 2000 and 10000 images. There is a general recommendation that the size of the validation set should be 20% of the training set. Therefore, 10000 training images and 2000 validation images were chosen from both datasets since the model's generalization capabilities improve as the as the size of the training set grows (when data is of high quality, obviously). The use of several datasets allowed us to compare the quality of trained models.

To prepare the COCO dataset, a Python script was developed: https://github.com/KyryloAntoshyn/person-location-detector/blob/master/training/download_coco_single_class_images.py. It uses JSON annotations and COCO API to download the required number of images of the Person class from the training and validation sets. An important part of the script is convert_and_write_annotations function that converts a COCO annotation to a YOLO format (all dimensions are relative to image width and height): <object-class> <x_center> <y_center> <width> <height> where <object-class> is the class identifier, <x_center> and <y_center> are the coordinates of the center of the bounding box, and <width> and <height> are its dimensions.

To prepare the Open Images dataset, Open Images Dataset v4 Toolkit was used. An important part of the toolkit is convert_annotations.py module that converts an Open Images annotation to a YOLO format.

To train the model, training files were prepared according to recommendations of YOLOv4-tiny author. It is worth noting that the transfer learning was carried out in our scenario: the weights of the convolutional layers of the previously trained network were used: yolov4-tiny.conv.29. This approach allows to speed up the learning process and increase the probability that the neural network will learn to effectively solve the given problem.

Optimal training parameters and model architecture were chosen based on the problem being solved: neural network should detect single class (Person) as well as work on the NVIDIA Jetson Nano microcomputer in real-time. A file with the training parameters and configuration of the neural network, a file with the names of the classes of objects on which we train the neural network, a file with the paths to the corresponding files and directories necessary for training can be found at (separate files were created for both COCO and Open Images datasets): https://github.com/KyryloAntoshyn/person-location-detector/tree/master/training.

Darknet framework requires files with relative paths to the training and validation images. To create these files automatically, a Python script was developed, placed in the scripts directory, and executed (the name of the dataset directory is given as an input): https://github.com/KyryloAntoshyn/person-location-detector/blob/master/training/generate_dataset_images_relative_paths.py.

Analyzing trained YOLOv4-tiny models that detect people.

Weights with which models demonstrated the highest accuracy on the validation dataset can be found at: https://github.com/KyryloAntoshyn/person-location-detector/tree/master/person_location_detector/detection_models. These weights are used in the developed method.

Figure 1 shows the graph of YOLOv4-tiny model training on the COCO dataset.

The graph shows that the final error (in blue) of the neural network is 1.07, and the accuracy (in red) is 55.1%. It is clearly visible that at 1000 iterations an accuracy of 41% was obtained, at 3500 iterations – 54%, then it dropped to 52% and only at the end of training we got 55.1%. When the accuracy of the model drops, an overfitting takes place, a process when the model detects objects well on the training set but begins to detect poorly on the validation set. It can be concluded that training for 3500 batches is optimal for this model and dataset.

Figure 2 shows the graph of YOLOv4-tiny model training on the Open Images dataset.

The graph shows that the final error of the neural network is 0.91, and the accuracy is 71.4%. It is

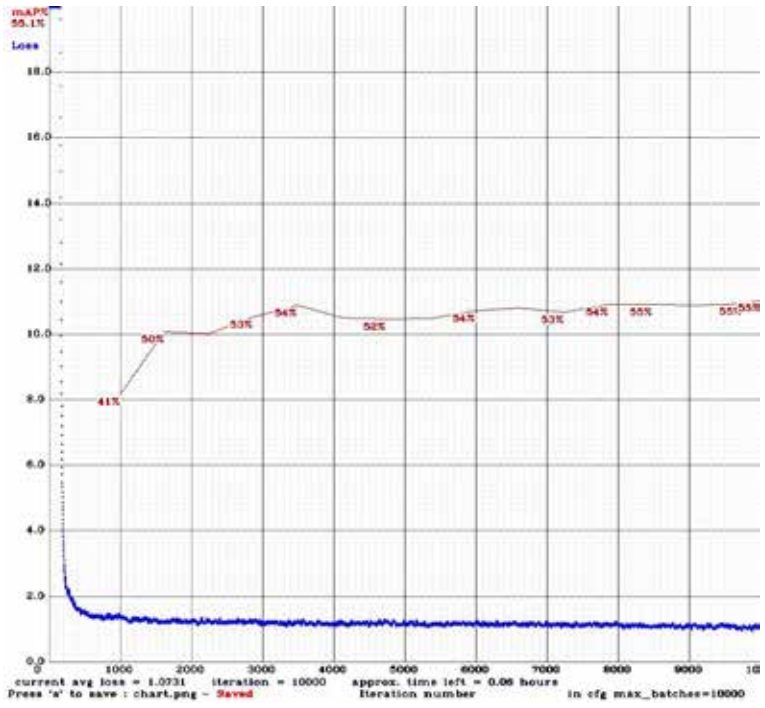


Fig. 1. The graph of YOLOv4-tiny model training on the COCO dataset

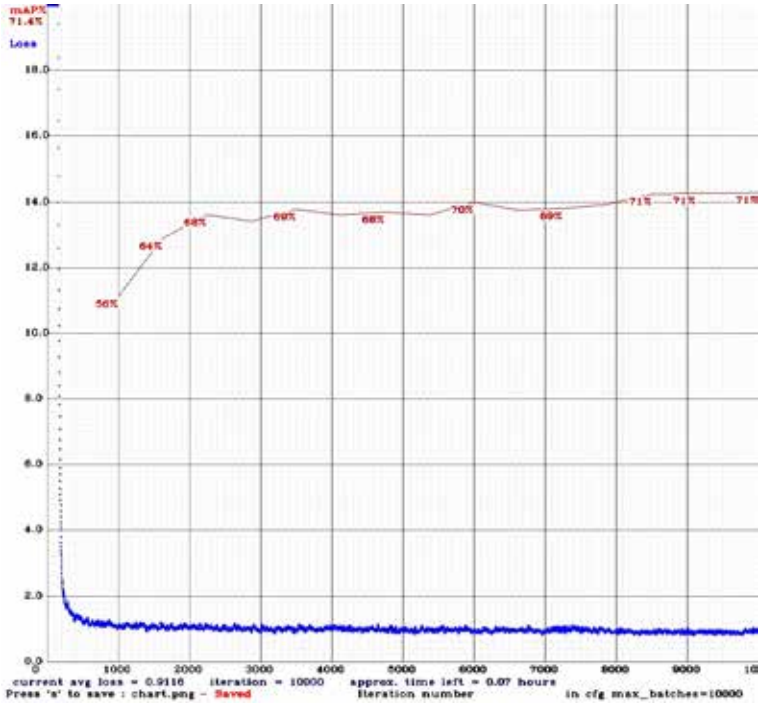


Fig. 2. The graph of YOLOv4-tiny model training on the Open Images dataset

clearly visible that at 1000 iterations an accuracy of 56% was obtained, at 3500 iterations – 69%, then it dropped to 68% and only at the end of training we got 71.4%. It can be concluded that training for 3500 batches is optimal for this model and dataset too.

At first glance, the model trained on the Open Images dataset should be more accurate due to higher precision obtained during training. However, after models' evaluation using the Oxford Town Center video, it was concluded that both models work with the same accuracy. One of the reasons is that the COCO dataset contains images with more complex scenarios, so it is more difficult for the neural network to perform generalization. Another reason is the presence of significant noise in the validation images since pre-processing of the datasets was not performed.

The training images of both datasets were checked using the LabelImg tool. The COCO dataset was found to contain annotations for a group of people, and Open Images for non-real people: mannequins, video game characters, toys, etc. To solve both problems it is required to manually remove such annotations and images. The best way, obviously, is to collect and annotate 2000-10000 images at the location where the system will be installed.

Any of the trained models can be used in the developed method, but it is required to evaluate which of them works better at the location where the system will be installed. To improve accuracy, we can try to experiment with some recommendations of YOLOv4-tiny author, some of which are: set random=1 in each yolo layer to change input image size during training randomly, increase the size of neural network to width=608 and height=608, validate quality of annotations etc.

Estimating the location of detected people.

The trained neural network model is used in the developed computer system that combines object detection approach with perspective transformation algorithm to estimate person location in the camera stream.

First, we initialize 3×3 perspective transformation matrix using OpenCV: https://github.com/KyryloAntoshyn/person-location-detector/blob/master/person_location_detector/services.py#L289. 4 pairs of points are used: coordinates of the projection area from the perspective of the camera and coordinates of the actual projection area on the floor.

Then, transformed coordinate $(\hat{x},\hat{y})$ is calculated using Expression 1, where $M_{11},M_{12},\ldots,M_{ij}$ are the elements of already initialized perspective transformation 3×3 matrix, (x,y) is the person coordinate from the camera point of view. Implementation can be found at: https://github.com/KyryloAntoshyn/person-location-detector/blob/master/person_location_detector/services.py#L327.

$$(\hat{x},\hat{y})=\left(\frac{M_{11}\times x+M_{12}\times y+M_{13}}{M_{31}\times x+M_{32}\times y+M_{33}},\frac{M_{21}\times x+M_{22}\times y+M_{23}}{M_{31}\times \boldsymbol{x}+M_{32}\times y+M_{33}}\right) \quad (1)$$

Accuracy and speed of the developed method.

Table 1

Comparison of speed of the developed method when using different devices

Device	Speed (FPS)
Training PC (NVIDIA GeForce GTX 1050)	83
NVIDIA Jetson Nano	16

The error is measured as the distance between the determined point (marked in green) and the actual point (marked in blue).

Table 2

Developed method error in various scenarios

Scenario	Error (cm)
A person is facing the camera	15
The person's back is turned to the camera	30
Part of the human body is covered by another object	25

Figure 3 shows the scenario when a person is facing the camera.

From the results obtained, for the given scenarios, the average error is 23 cm. The accuracy of the developed method primarily depends on the accuracy of trained neural network models that detect people.

The bounding box approach has two drawbacks. First, the frame does not always fit tightly to the human body, which gives an error when determining position. Then, a person can put one leg back and then its position will be determined relative to the front leg, which is also not completely accurate. These issues can be resolved using keypoints detection approach that was leveraged by Adrian Cosma et al., Ángel Carro-Lagoa et al. and Huan Wang et al. However, keypoints detection approach requires more computing resources and often does not detect a person in the frame, therefore, can be a bottleneck if the method should work on microcomputer.

To increase accuracy, we can try to combine several methods for person detection: object detection with pose estimation, combine results from several cameras set at different angles, create

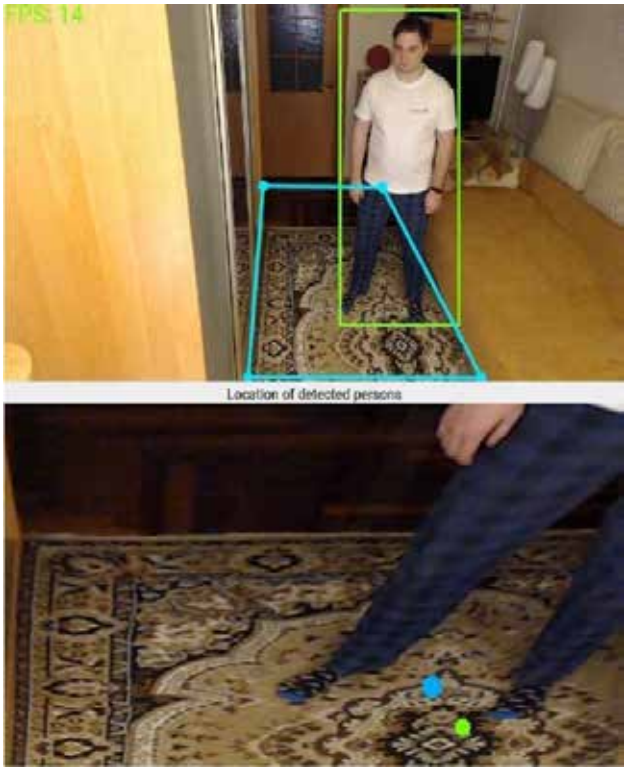


Fig. 3. Scenario when a person is facing the camera

our own dataset at the location where the system will be installed, consider using wide-angle camera viewing directly onto the floor. In fact, most of the areas of application of the developed method described in this work do not require determination of a person's location with perfect accuracy and, therefore, the approach with the bounding box is more optimal.

Conclusions. Indoor localization problem has been investigated: advantages and disadvantages of existing technologies as well as modern computer vision approaches to its solution. An effective method in terms of speed and accuracy that uses a camera video stream in combination with object detection and perspective transformation approaches has been developed. The method works on the NVIDIA Jetson Nano microcomputer in real-time with a speed of 16 FPS and accuracy of 23 cm. Therefore, it outperforms existing alternatives in terms of speed and accuracy.

BIBLIOGRAPHY:

1. Mautz R. Indoor Positioning Technologies. Zurich:Institute of Geodesy and Photogrammetry, 2012.

2. Kerdjidj O., Himeur Y., Sohail S. S., Amira A., Fadli F., Atalla S., Mansoor W., Copiaco A., Gawanmeh A., Miniaoui S., Dawoud D. W. Uncovering the Potential of Indoor Localization: Role of Deep and Transfer Learning. *IEEE Access*. 2024. Вип. 12. С. 73980–74010.

3. Cosma A., Radoi I. E., Radu V. CamLoc: Pedestrian Location Detection from Pose Estimation on Resource-constrained Smart-cameras. 2018.

4. Wang H., Wang G., Li X. An RGB-D camera-based indoor occupancy positioning system for complex and densely populated scenarios. *Indoor and Built Environment*. 2023. Вип. 32, № 6. С. 1198–1212.

5. Carro-Lagoa Á., Barral V., González-López M., Escudero C. J., Castedo L. Multicamera edge-computing system for persons indoor location and tracking. *Internet of Things*. 2023. Вип. 24.

6. Girshick R., Donahue J., Darrell T., Malik J. Rich feature hierarchies for accurate object detection and semantic segmentation. 2014.

7. Girshick R. Fast R-CNN. 2015.

8. Ren S., He K., Girshick R., Sun J. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks. 2016.

9. Redmon J., Divvala S., Girshick R., Farhadi A. You Only Look Once: Unified, Real-Time Object Detection. 2016.

10. Bochkovskiy A., Wang C.-Y., Liao H.-Y. M. YOLOv4: Optimal Speed and Accuracy of Object Detection. 2020.

11. Howard A., Sandler M., Chu G., Chen L.-C., Chen B., Tan M., Wang W., Zhu Y., Pang R., Vasudevan V., Le Q. V., Hartwig A. Searching for MobileNetV3. 2019.

12. Iandola F. N., Han S., Moskewicz M. W., Ashraf K., Dally W. J., Keutzer K. SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size. 2016.

13. Yolo v4, v3 and v2 for Windows and Linux. URL: https://github.com/AlexeyAB/darknet (дата звернення: 23.08.2024).

14. Lin T.-Y., Maire M., Belongie S., Bourdev L., Girshick R., Hays J., Perona P., Ramanan D., Zitnick C. L., Dollár P. Microsoft COCO: Common Objects in Context. 2015.

15. Kuznetsova A., Rom H., Alldrin N., Uijlings J., Krasin I., Pont-Tuset J., Kamali S., Popov S., Malloci M., Kolesnikov A., Duerig T., Ferrari V. The Open Images Dataset V4: Unified image classification, object detection, and visual relationship detection at scale. 2020.

16. OpenCV Perspective Transformation. URL: https://medium.com/analytics-vidhya/opencv-perspective-transformation-9edffefb2143 (дата звернення: 23.08.2024).

REFERENCES:

1. Mautz, R. (2012). Indoor Positioning Technologies. Zurich:Institute of Geodesy and Photogrammetry,

2. Kerdjidj, O., Himeur, Y., Sohail, S. S., Amira, A., Fadli, F., Atalla, S., Mansoor, W., Copiaco, A., Gawanmeh, A., Miniaoui, S., Dawoud, D. W. (2024). Uncovering the Potential of Indoor Localization: Role of Deep and Transfer Learning. IEEE Access. Vol. 12. C. 73980–74010.

3. Cosma, A., Radoi, I. E., Radu, V. (2018). CamLoc: Pedestrian Location Detection from Pose Estimation on Resource-constrained Smart-cameras.

4. Wang, H., Wang, G., Li, X. (2023). An RGB-D camera-based indoor occupancy positioning system for complex and densely populated scenarios. Indoor and Built Environment. Vol. 32, № 6. С. 1198–1212.

5. Carro-Lagoa, Á., Barral, V., González-López, M., Escudero, C. J., Castedo, L. (2023). Multicamera edge-computing system for persons indoor location and tracking. Internet of Things. Vol. 24.

6. Girshick, R., Donahue, J., Darrell, T., Malik, J. (2014). Rich feature hierarchies for accurate object detection and semantic segmentation.

7. Girshick, R. (2015). Fast R-CNN.

8. Ren, S., He, K., Girshick, R., Sun, J. (2016). Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks.

9. Redmon, J., Divvala, S., Girshick, R., Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection.

10. Bochkovskiy, A., Wang, C.-Y., Liao, H.-Y. M. (2020). YOLOv4: Optimal Speed and Accuracy of Object Detection.

11. Howard, A., Sandler, M., Chu, G., Chen, L.-C., Chen, B., Tan, M., Wang, W., Zhu, Y., Pang, R., Vasudevan, V., Le, Q. V., Hartwig, A. (2019). Searching for MobileNetV3.

12. Iandola, F. N., Han, S., Moskewicz, M. W., Ashraf, K., Dally, W. J., Keutzer, K. (2016). SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size.

13. Yolo v4, v3 and v2 for Windows and Linux. Retrieved from: https://github.com/AlexeyAB/darknet (дата звернення: 23.08.2024).

14. Lin, T.-Y., Maire, M., Belongie, S., Bourdev, L., Girshick, R., Hays, J., Perona, P., Ramanan, D., Zitnick, C. L., Dollár, P. (2015). Microsoft COCO: Common Objects in Context.

15. Kuznetsova, A., Rom, H., Alldrin, N., Uijlings, J., Krasin, I., Pont-Tuset, J., Kamali, S., Popov, S., Malloci, M., Kolesnikov, A., Duerig, T., Ferrari, V. (2020). The Open Images Dataset V4: Unified image classification, object detection, and visual relationship detection at scale.

16. OpenCV Perspective Transformation. Retrieved from: https://medium.com/analytics-vidhya/opencv-perspective-transformation-9edffefb2143 (дата звернення: 23.08.2024).

УДК 004.422
DOI https://doi.org/10.32782/IT/2024-3-3

Катерина ГОРІШНЯ
студентка кафедри програмної інженерії, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0009-0001-9032-4249*

Ірина АФАНАСЬЄВА
кандидат технічних наук, доцент кафедри програмної інженерії, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0000-0003-4061-0332*

Костянтин ОНИЩЕНКО
старший викладач кафедри програмної інженерії, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0000-0002-7746-4570*

Наталія ГОЛЯН
кандидат технічних наук, доцент кафедри програмної інженерії, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0000-0002-1390-3116*

Віра ГОЛЯН
кандидат технічних наук, доцент кафедри програмної інженерії, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0000-0002-7196-5286*

Бібліографічний опис статті: Горішня, К., Афанасьєва, І., Онищенко, К., Голян, Н., Голян, В. (2024). Проектування програмної системи для бронювання квитків. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 23–32, doi: https://doi.org/10.32782/IT/2024-3-3

ПРОЕКТУВАННЯ ПРОГРАМНОЇ СИСТЕМИ ДЛЯ БРОНЮВАННЯ КВИТКІВ

Дана робота присвячена розробці та впровадженню платформи для бронювання квитків, яка відповідає сучасним вимогам користувачів та організаторів заходів.

***Мета роботи.** Метою даної роботи є проектування та розробка програмної системи для бронювання та покупки квитків на заходи «Ticketer». Основним завданням є створення зручного та ефективного інструменту, який забезпечить користувачам швидкий доступ до інформації про події, а також надасть організаторам заходів сучасні інструменти для управління продажами.*

***Методологія.** У процесі проектування платформи було використано поетапний підхід, який включав аналіз ринку, прототипування, визначення бізнес-правил та проектування архітектури системи. Основні елементи інтерфейсу та функціональні можливості були спочатку розроблені у вигляді прототипу за допомогою інструменту Figma, що дозволило оптимізувати користувацький досвід. Крім того, були створені діаграми сценаріїв використання, CRC-карти, об'єктні діаграми та діаграми класів, що допомогли структуровано визначити архітектуру системи та забезпечити узгодженість її компонентів. Особлива увага приділялася забезпеченню надійності та масштабованості платформи, що дозволить її подальший розвиток та інтеграцію з іншими сервісами.*

***Наукова новизна.** Наукова новизна проекту полягає в інтеграції сучасних функцій, таких як реальні оновлення доступності квитків, персоналізовані рекомендації та багатоплатформена доступність. Це дозволяє підвищити ефективність роботи платформи та задовольнити змінювані потреби сучасних користувачів. Використання прототипування на ранніх стадіях розробки та поетапного підходу до проектування архітектури забезпечує високий рівень гнучкості та адаптивності системи.*

***Висновки.** В результаті дослідження було створено повнофункціональну платформу для бронювання квитків «Ticketer», яка забезпечує зручний, безпечний і персоналізований досвід для користувачів, а також надає організаторам заходів ефективні інструменти для управління продажами. Платформа відповідає сучасним вимогам ринку і має високий потенціал для подальшого розвитку та масштабування.*

***Ключові слова:** бронювання квитків, інтерфейс користувача, платформа, архітектура системи, масштабованість.*

Kateryna GORISHNIA
Student at the Department of Software Engineering, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, kateryna.horishnia@nure.ua
***ORCID:** 0009-0001-9032-4249*

Iryna AFANASIEVA
Ph.D., Associate Professor at the Department of Software Engineering, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, iryna.afanasieva@nure.ua
***ORCID:** 0000-0003-4061-0332*

Kostiantyn ONYSHCHENKO
Senior Lecturer at the Department of Software Engineering, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, kostiantyn.onyshchenko@nure.ua
***ORCID:** 0000-0002-7746-4570*

Natalia GOLIAN
Ph.D., Associate Professor at the Department of Software Engineering, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, nataliia.golian@nure.ua
***ORCID:** 0000-0002-1390-3116*

Vira GOLAN
Ph.D., Associate Professor at the Department of Software Engineering, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, vira.golan@nure.ua
***ORCID:** 0000-0002-7196-5286*

To cite this article: Gorishnia, K., Afanasieva, I., Onyshchenko, K., Golian, N., Golan, V. (2024). Proektuvannia prohramnoi systemy dlia broniuvannia kvytkiv [Design of a software system for ticket booking]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 23–32, doi: https://doi.org/10.32782/IT/2024-3-3

DESIGN OF A SOFTWARE SYSTEM FOR TICKET BOOKING

This paper is dedicated to the development and implementation of a ticket booking platform that meets the modern requirements of users and event organizers.

***Aim of the study.** The aim of this research is the design and development of a software system for booking and purchasing tickets for events, called «Ticketer». The primary objective is to create a convenient and efficient tool that provides users with quick access to event information while offering event organizers modern tools for sales.*

***Methodology.** The process of designing the platform followed a phased approach, including market analysis, prototyping, defining business rules, and system architecture design. The main interface elements and functionalities were initially developed as a prototype using the Figma tool, which allowed for the optimization of the user experience. In addition, use case diagrams, CRC cards, object diagrams, and class diagrams were created to structurally define the system architecture and ensure the consistency of its components. Special attention was given to ensuring the platform's reliability and scalability, allowing for further development and integration with other services.*

***Scientific novelty.** The scientific novelty of the project lies in the integration of modern features such as real-time ticket availability updates, personalized recommendations, and multi-platform accessibility. This enhances the platform's efficiency and meets the changing needs of modern users. The use of prototyping in the early stages of development and a phased approach to architecture design ensure a high level of system flexibility and adaptability.*

***Conclusions.** As a result of the research, a fully functional ticket booking platform «Ticketer» was created, providing a convenient, secure, and personalized experience for users while offering event organizers effective tools for sales management. The platform meets modern market demands and has high potential for further development and scaling.*

***Key words:** ticket booking, user interface, platform, system architecture, scalability.*

Актуальність проблеми. У сучасному світі проведення різноманітних заходів, таких як концерти, театральні вистави, спортивні події, стає все більш популярним. Однак, процес купівлі квитків на ці заходи часто супроводжується численними труднощами, такими як довгі черги, обмежена доступність квитків та фрагментована інформація. Це призводить до незадовільного користувацького досвіду та втрати можливостей для організаторів заходів максимізувати

продаж квитків. У зв'язку з цими викликами, нова платформа для продажу квитків на заходи має на меті революціонізувати індустрію квитків, забезпечуючи безперебійний та ефективний процес бронювання як для користувачів, так і для організаторів.

Аналіз останніх досліджень і публікацій. Існуючі платформи для продажу квитків, такі як Ticketsbox та Karabas, надають користувачам базові можливості для бронювання та купівлі квитків. Однак, вони часто не задовольняють змінювані потреби користувачів та організаторів. Дослідження показують, що сучасні користувачі потребують реальних оновлень доступності квитків, персоналізованих рекомендацій та мобільної доступності (Smith, Jones, 2020). Крім того, організатори заходів потребують інструментів для аналізу переваг клієнтів, що дозволяє оптимізувати стратегії продажу та маркетингу (Lee, 2019).

Мета дослідження. Метою даного дослідження проектування, розробка та впровадження нової платформи для бронювання та купівлі квитків «Ticketer», яка надасть користувачам зручний та швидкий доступ до інформації про заходи, а також забезпечить організаторів заходів ефективними інструментами для управління продажами та маркетингом. Платформа буде оснащена сучасними функціями, такими як реальні оновлення доступності, персоналізовані рекомендації та багатоплатформена доступність, що дозволить підвищити задоволеність користувачів та збільшити продажі квитків.

Виклад основного матеріалу дослідження. Проєкт «Ticketer» було розроблено на основі детально визначеного документа «Vision & Scope», який окреслює головну мету та стратегію розвитку платформи (Wiegers, Beatty, 2013, International Organization for Standardization, 2008). Відповідно до документа, основною метою платформи є надання користувачам зручного та сучасного інструменту для бронювання та покупки квитків на різні події, включаючи театральні вистави, кіносеанси та спортивні заходи. Проєкт орієнтований на покращення користувацького досвіду через персоналізовані рекомендації, які надаються на основі вподобань користувача, та забезпечення безпеки даних за допомогою двофакторної аутентифікації.

Наступнм етапом було створено прототип системи «Ticketer» у Figma (Vilppu, 2019), який став ключовим етапом у процесі розробки. Цей прототип дозволив візуалізувати та тестувати користувацький інтерфейс на ранніх стадіях проекту, що забезпечило ефективну оцінку зручності використання та ідентифікацію потенційних проблем до етапу повної реалізації.

Головна сторінка застосунку для бронювання квитків Ticketer містить стратегічно розміщені елементи навігації та переліку доступних подій, що дозволяє користувачеві оперативно знаходити необхідну інформацію. Для підвищення ефективності пошуку подій, на сторінці «Каталог» реалізовано інтегрований фільтр та сортування, що дозволяє користувачам швидко знаходити події відповідно до їхніх уподобань, зокрема за датою, місцем проведення та типом заходу (рис. 1).

На сторінці «Подія» (рис. 2) користувач може отримати доступ до детальної інформації про конкретну подію, включаючи її опис, дату, місце проведення та інші важливі деталі, що забезпечує інформованість і сприяє прийняттю обґрунтованого рішення щодо бронювання квитка. Окрім того, користувач має змогу додати подію до списку бажань, що підвищує персоналізованість та адаптивність сервісу (Kotler, Keller, 2016).

Насупним етапом в проектуванні програмної системи для забезпечення повноцінної взаємодії користувачів із системою «Ticketer», важливе значення має діаграма сценаріїв використання, відома як Smart Use Case Diagram (Max Zosim, 2024). Ця діаграма (рис. 3) ілюструє основні процеси взаємодії користувачів із системою, включаючи такі ключові функції, як реєстрація, пошук подій, бронювання квитків та керування обліковим записом.

Система «Ticketer» побудована на основі кількох класів, які були визначені за допомогою CRC-карт (Class-Responsibility-Collaborator). Ці карти дають можливість чітко визначити відповідальність кожного класу, а також їхню співпрацю з іншими класами (Ambler, 2019). За результатами виконаного аналізу, **д**ля забезпечення відповідності системи вимогам користувачів та бізнес-цілям проекту також була ророблена діаграма класів (Class Diagram), яка відображає структуру системи на рівні класів та їх взаємозв'язки (Max Zosim, 2024).

На діаграмі класів (рис. 4) можна побачити взаємозв'язки між основними компонентами системи «Ticketer». Зокрема, класи User, Ticket, Payment та інші пов'язані між собою через асоціації, що відображає їх взаємодію в рамках системи. Клас User містить атрибути, такі як id, email, password, що визначають основні характеристики користувача. Клас Ticket включає атрибути id, paymentId, startTime, endTime, що

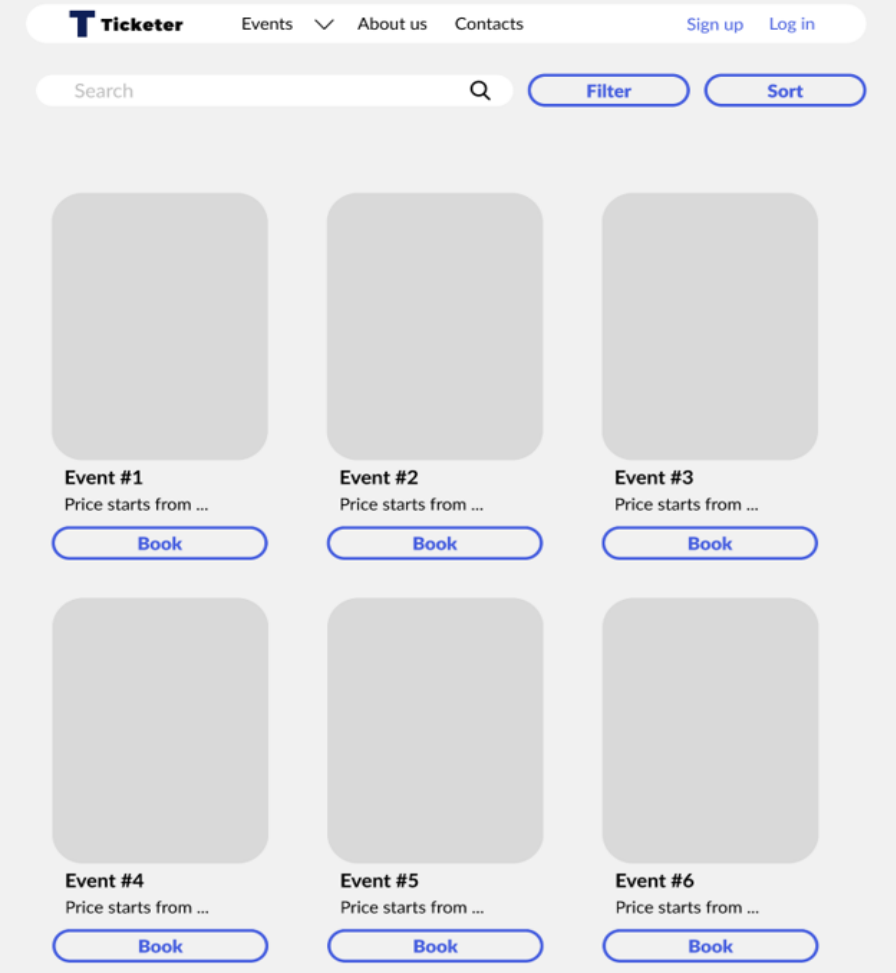


Рис. 1. Фрагменти сторінки «Каталог» з переліком подій

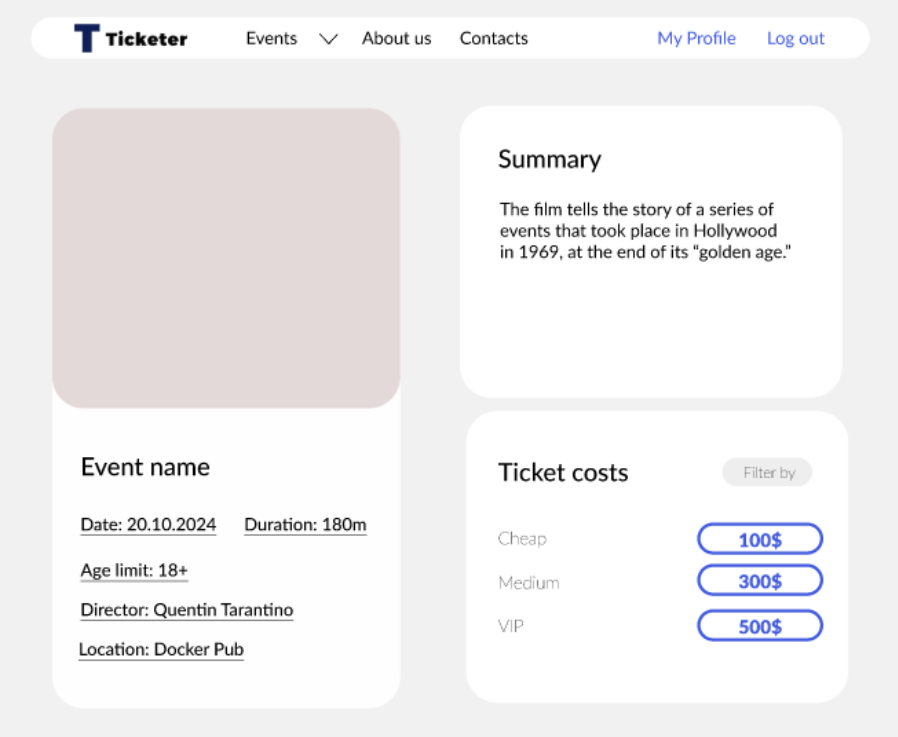


Рис. 2. Фрагменти сторінки «Подія»

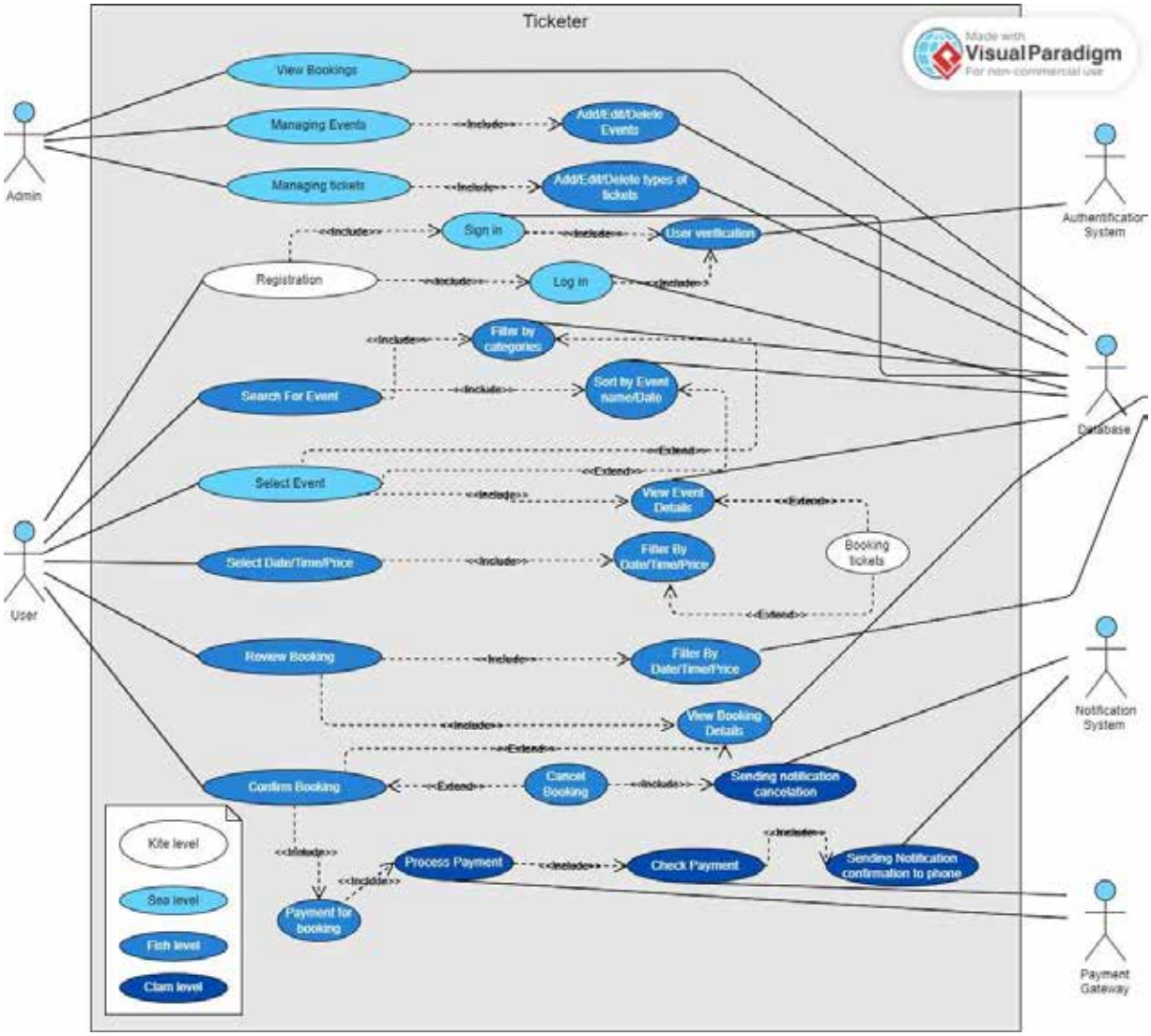


Рис. 3. Smart Use Case diagram проекту «Ticketer»

описують інформацію про квиток, який може бути придбаний користувачем.

Важливим елементом є клас Payment, який містить атрибути moneyPaid, date, userId, eventId, що забезпечують управління процесом оплати квитків. Взаємодія між класами реалізується через методи, такі як buyTicket, refundTicket, createEvent, createPayment, які відповідають за виконання основних функцій системи. Це забезпечує узгоджену роботу різних компонентів системи, що є ключовим для її стабільного функціонування.

Наступним етапом в проектуванні програмної системи було розроблено діаграма об'єктів (Object Diagram), що надає більш детальне уявлення про те, як класи інстанціюються під час виконання програми. Ця діаграма (рис. 5) ілюструє конкретні приклади взаємодії об'єктів класів у реальному часі, що дозволяє краще зрозуміти динаміку роботи системи і виявити проблеми ще на етапі проектування, що, в свою чергу, допомагає уникнути помилок у процесі розробки (Max Zosim, 2024).

Щоб ефективно відслідковувати стан системи в різних сценаріях, було реалізовано діаграма станів (StateChart). Вона відображає, як система переходить з одного стану в інший залежно від дій користувачів або інших подій (Max Zosim, 2024).

На діаграмі станів (рис. 6) можна побачити послідовність станів, через які проходить система під час виконання різних процесів. Наприклад, процес вибору події починається зі стану «Start», після чого користувач може переглядати каталог подій, вибирати конкретну подію та отримувати детальну інформацію про неї. Далі система переходить до авторизації користувача, де він може увійти до свого облікового запису або зареєструвати новий, якщо ще не має облікового запису.

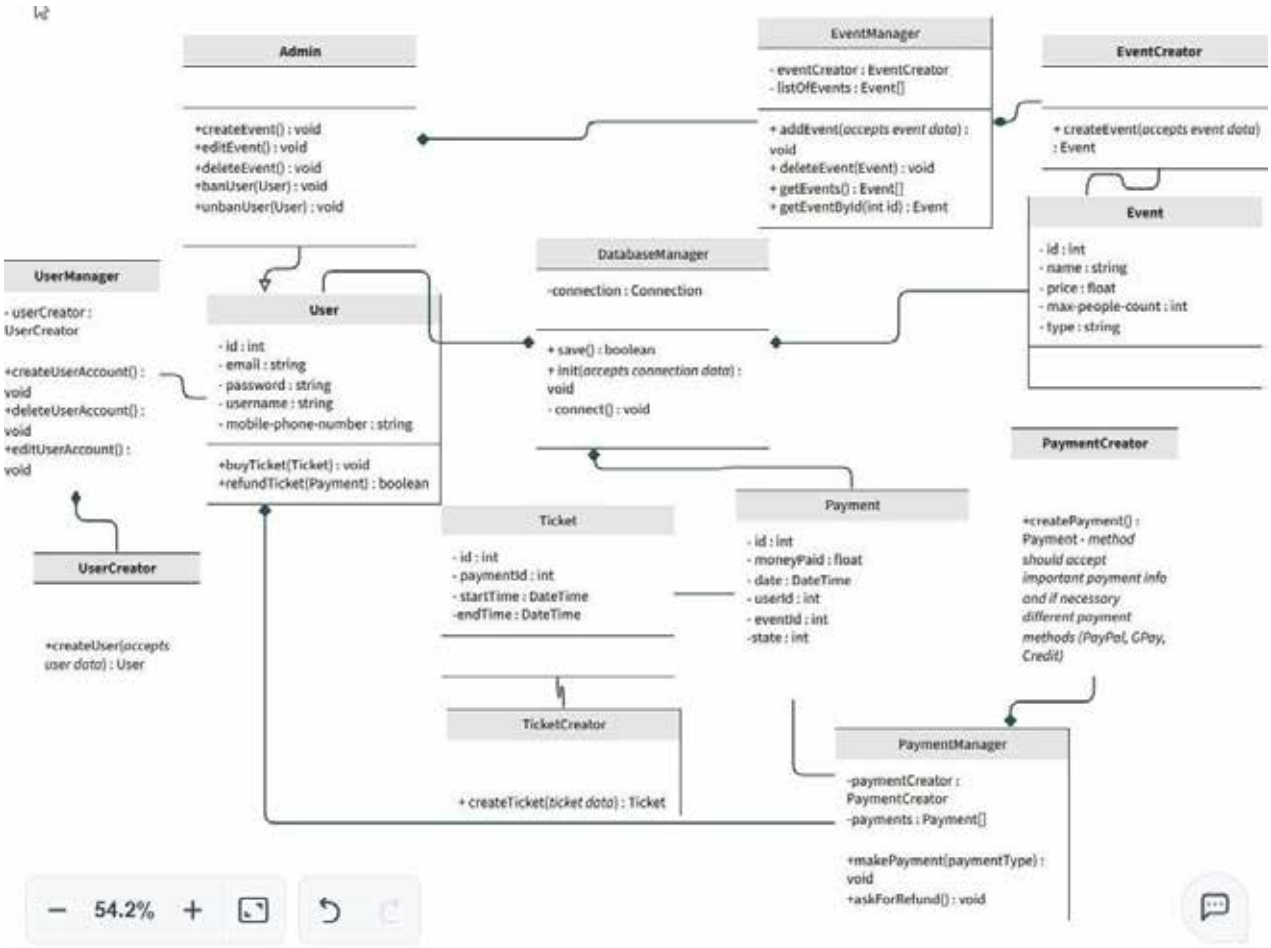


Рис. 4. Class diagram проекту «Ticketer»

Після авторизації користувач може оформити замовлення, яке включає створення замовлення, підтвердження та процес оплати. Система забезпечує перевірку валідності платежу, після чого квиток надсилається користувачу. Ця діаграма дозволяє розробникам краще зрозуміти, як система реагує на дії користувача в різних сценаріях, що допомагає забезпечити її надійність та стабільність в умовах реального використання.

Для відображення розгортання системи у виробничому середовищі було розроблено діаграму розгортання (Deployment Diagram). Вона демонструє, як різні компоненти системи розподілені на серверах та інших апаратних засобах, що забезпечує їхню доступність і масштабованість (Agile Modeling, 2024).

На цій діаграмі (рис. 7) можна побачити розподіл різних компонентів системи «Ticketer» на декілька серверів, таких як Backend Server, Frontend Server, Database Server, та інші. Компоненти, такі як Backend application, Frontend application, Database, Redis, Nginx, і Storage, розгорнуті на відповідних серверах, що забезпечує оптимальну взаємодію між ними.

Наприклад, Backend Server обробляє бізнес-логіку і взаємодіє з Database Server для зберігання даних, тоді як Frontend Server відповідає за рендеринг інтерфейсу для кінцевих користувачів. Використання серверів, таких як Nginx для управління HTTP-запитами та Redis для кешування даних, допомагає підвищити продуктивність та масштабованість системи (NGINX, 2024).

Остаточним результатом проекту «Ticketer» є повнофункціональний продукт, який включає всі перераховані вище елементи і забезпечує користувачам зручний та безпечний спосіб бронювання квитків на різні події (рис. 8-9). Завдяки ретельному плануванню і тестуванню на всіх етапах розробки, платформа «Ticketer» здатна задовольнити потреби користувачів і відповідає сучасним вимогам ринку, що робить її конкурентоспроможною та ефективною на ринку подібних послуг.

Висновки. Підсумовуючи, проект «Ticketer» пройшов через ретельний і поетапний процес проектування, за життєвим циклом розробки програмної системи, який охопив всі ключові аспекти від початкового планування до

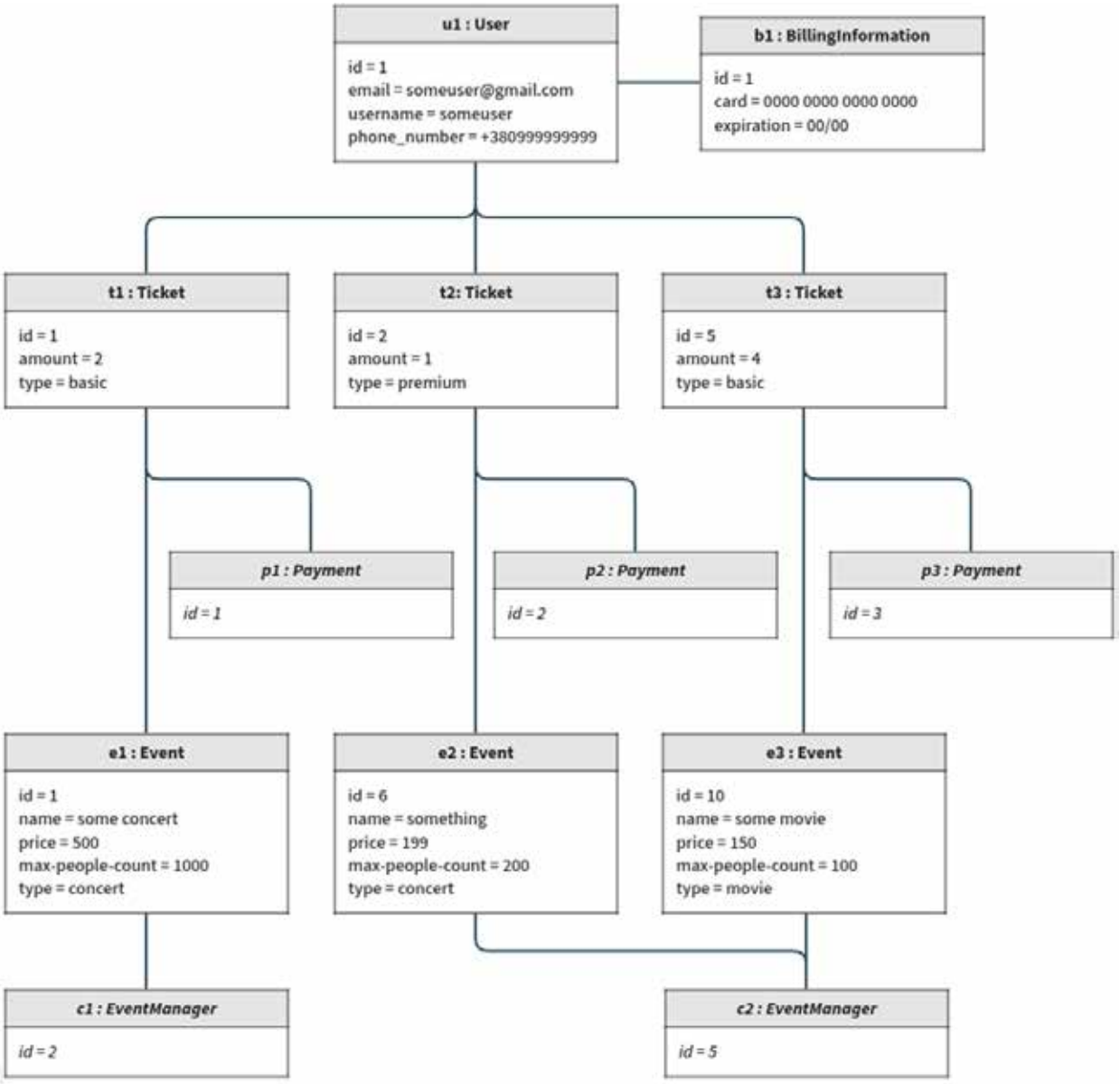


Рис. 5. Object diagram проекту «Ticketer»

остаточного розгортання платформи. Завдяки використанню сучасних інструментів прототипування, чіткому визначенню бізнес-правил і детальному проектуванню архітектури, вдалося створити платформу, яка не тільки задовольняє потреби користувачів, але й відповідає сучасним вимогам ринку.

Платформа «Ticketer» забезпечує зручний і безпечний спосіб бронювання квитків на різні події, що робить її конкурентоспроможною і здатною зайняти провідну позицію на ринку подібних послуг. Всі виклики, з якими ми стикалися під час розробки, були успішно подолані завдяки комплексному підходу до планування і реалізації проекту. Цей досвід наочно демонструє, що при правильній організації процесу розробки і уважному ставленні до деталей можна створити високоякісний продукт, який буде затребуваним і успішним на ринку.

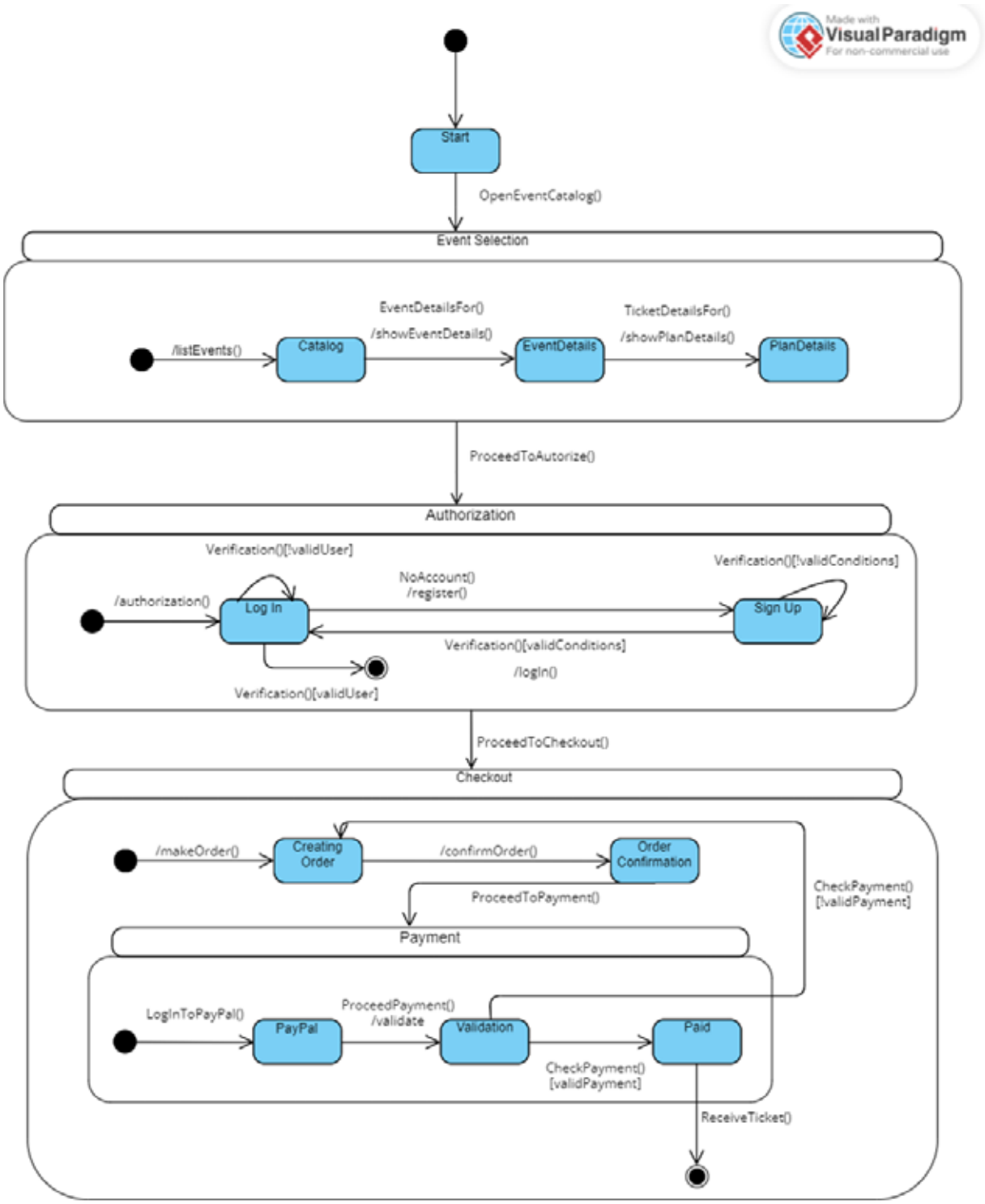


Рис. 6. State Chart проекту «Ticketer»

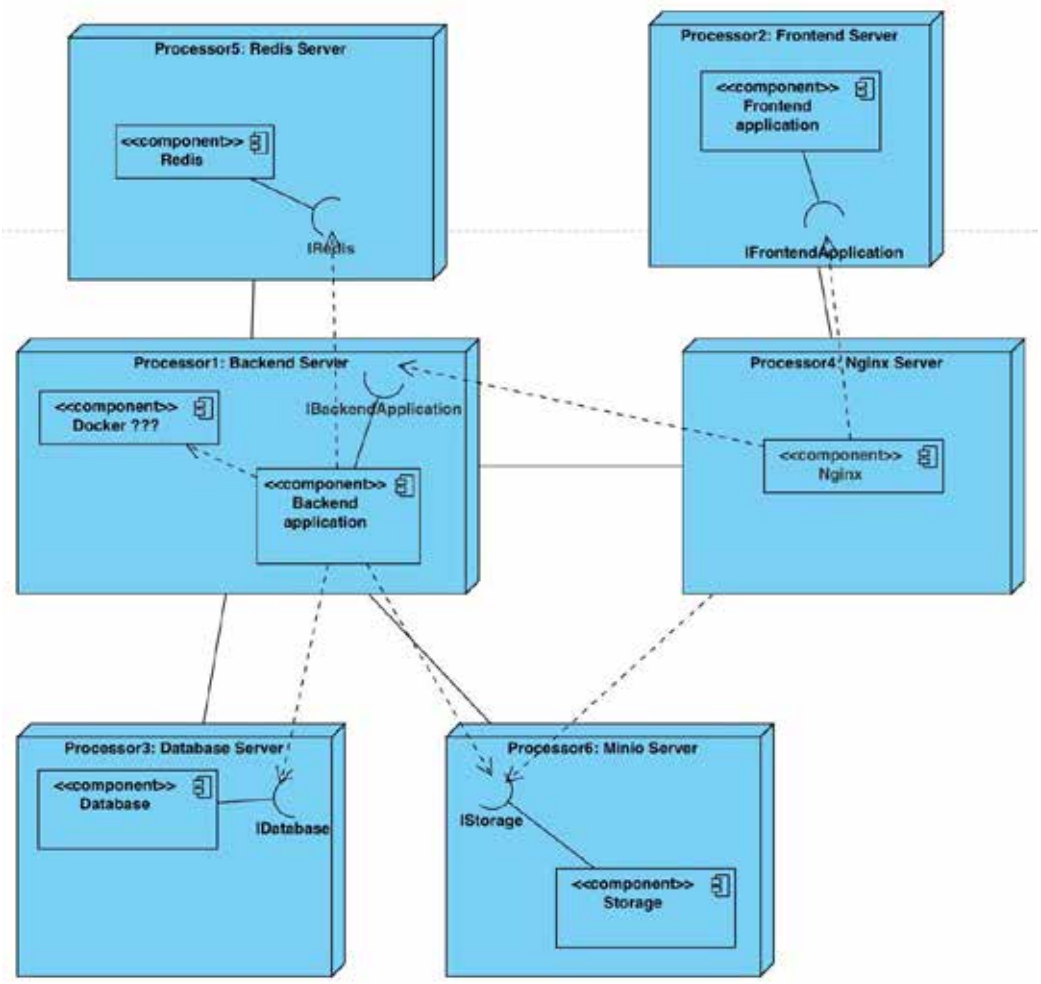


Рис. 7. Deployment Diagram проекту «Ticketer»

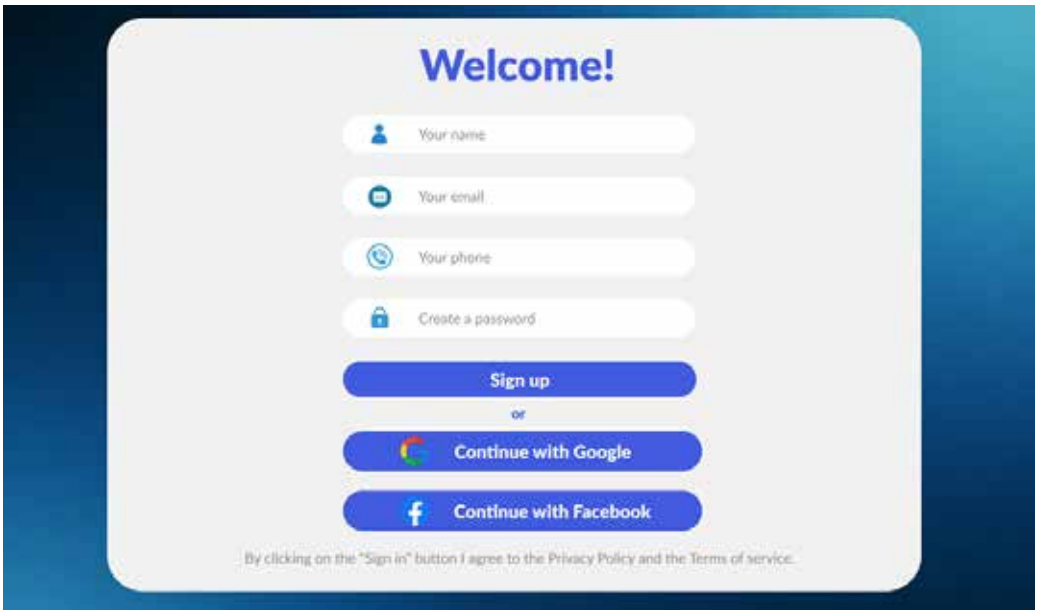


Рис. 8. Сторінка реєстрації (або входу) на платрофму «Ticketer»

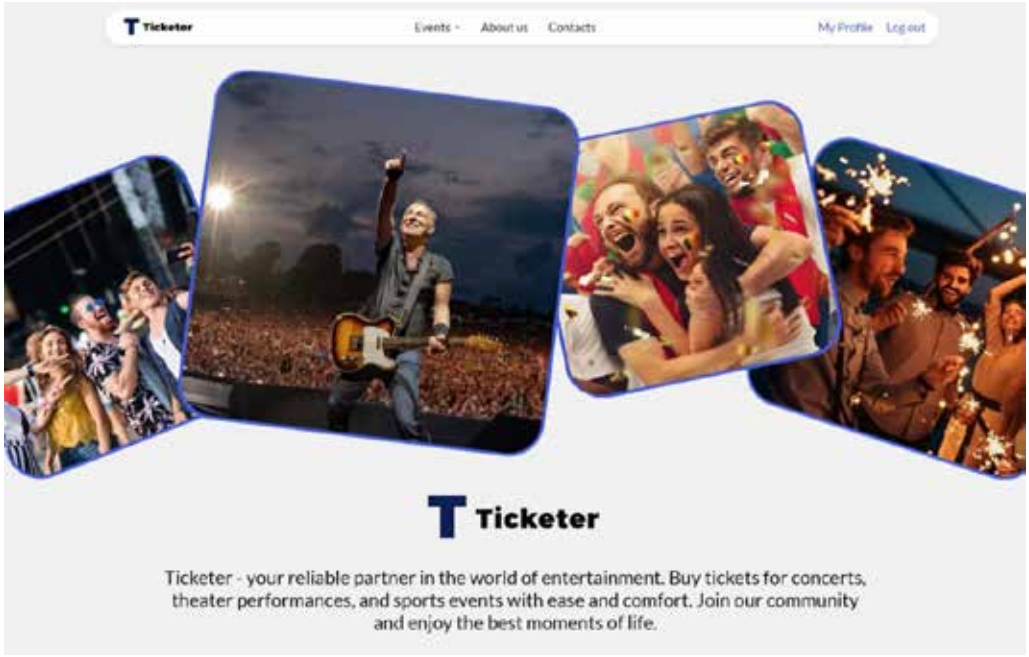


Рис. 9. Головна сторінка платформи «Ticketer»

ЛІТЕРАТУРА:

1. Smith A., Jones B. Digital Transformation in Business: Strategy and Practice. Routledge, 2020. 320 p.
2. Lee J. Digital Business and E-commerce Management. Pearson, 2019. 450 p.
3. Wiegers K., Beatty J. Software Requirements. 3rd ed. Microsoft Press, 2013. 590 p.
4. Systems and software engineering – Software Life Cycle Processes. ISO 12207:2008. [Чинний від 2008-02-01]. 122 с. (Міжнародний стандарт).
5. Vilppu H. Prototyping for Designers: Developing the Best Digital and Physical Products. O'Reilly Media, 2019. 290 p.
6. Kotler P., Keller K. L. Marketing Management. 15th ed. Pearson, 2016. 812 p.
7. Unified Modeling Language. URL: https://www.maxzosim.com/unifikovana-mova-modeluvannia/ (дата звернення: 30.08.2024).
8. Ambler S. W. The Object Primer: Agile Model-Driven Development with UML 2.5. Cambridge University Press, 2019. 400 p.
9. Agile Modeling Artifacts. URL: https://agilemodeling.com/artifacts/crcmodel.htm (дата звернення: 30.08.2024).
10. NGINX. NGINX Web Server Guide. URL: https://docs.nginx.com/nginx/admin-guide/web-server/ (дата звернення: 30.08.2024).

REFERENCES:

1. Smith, A., & Jones, B. (2020). Digital transformation in business: Strategy and practice. Routledge.
2. Lee, J. (2019). Digital business and e-commerce management. Pearson.
3. Wiegers, K., & Beatty, J. (2013). Software requirements (3rd ed.). Microsoft Press.
4. International Organization for Standardization. (2008). ISO/IEC 12207:2008 Systems and software engineering – Software life cycle processes. Retrieved from: https://www.iso.org/standard/43447.html
5. Vilppu, H. (2019). Prototyping for designers: Developing the best digital and physical products. O'Reilly Media.
6. Kotler, P., & Keller, K. L. (2016). Marketing management (15th ed.). Pearson.
7. Max Zosim. (2024). Unified modeling language. Retrieved from: https://www.maxzosim.com/unifikovana-mova-modeluvannia/
8. Ambler, S. W. (2019). The object primer: Agile model-driven development with UML 2.5. Cambridge University Press.
9. Agile Modeling. (2024). Agile modeling artifacts. Retrieved from: https://agilemodeling.com/artifacts/crcmodel.htm
10. NGINX. (2024). NGINX web server guide. Retrieved from: https://docs.nginx.com/nginx/admin-guide/web-server/

UDC 004.5:004.93, 004.42, 004.92
DOI https://doi.org/10.32782/IT/2024-3-4

Serhii ZELINSKYI
PhD Student at the Department of Computer Engineering, Faculty of Radiophysics, Electronics and Computer Systems, Taras Shevchenko National University of Kyiv, 60, Volodymyrska Str., Kyiv, Ukraine, 01033
***ORCID:** 0009-0003-6271-2601*

Yuriy BOYKO
Candidate of Physical and Mathematical Sciences, Associate Professor, Head of the Department of Computer Engineering, Faculty of Radiophysics, Electronics, and Computer Systems, Taras Shevchenko National University of Kyiv, 60, Volodymyrska Str., Kyiv, Ukraine, 01033
***ORCID:** 0000-0003-1417-7424*
***Scopus Author ID:** 24722552300*

To cite this article: Zelinskyi, S., Boyko, Yu. (2024). Doslidzhennia vzaiemodii na osnovi pohliadu ta zhestiv u veb-seredovyshchi: porivniannia z vzaiemodiieiu kompiuternoiu mysheiu dlia manipuliuvannia obiektamy [Exploring gaze-gesture interaction on the web: a comparison with mouse input for object manipulation]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 33–42, doi: https://doi.org/10.32782/IT/2024-3-4

EXPLORING GAZE-GESTURE INTERACTION ON THE WEB: A COMPARISON WITH MOUSE INPUT FOR OBJECT MANIPULATION

***The purpose** of this study is to implement and evaluate a web-based gaze-gesture interaction method for object manipulation using a standard web camera. This method combines gaze tracking for object selection with hand gestures for natural manipulation tasks like rotating, scaling, and dragging. Unlike other implementations of such interaction that require specialized hardware, this method uses widely available technology, making advanced interaction techniques more accessible.*

***The scientific novelty** lies in developing a gaze-gesture interaction system that operates entirely on a web platform using standard hardware, removing the need for expensive, specialized equipment and enabling broader adoption.*

***The methodology** involved creating a web-based system using computer vision algorithms for real-time gaze tracking and gesture recognition. A user study was conducted where participants completed object manipulation tasks using both the gaze-gesture input and traditional mouse input, with task completion times recorded and analyzed.*

***Conclusion.** The study shows that gaze-gesture interaction is particularly effective for tasks requiring simultaneous actions, such as rotating and scaling objects, outperforming mouse input in these scenarios. While mouse input remains more efficient for simpler tasks, gaze-gesture interaction offers strong potential for enhancing complex task interactions on web platforms, contributing to the development of more accessible and intuitive input methods.*

***Key words:** gaze-gesture interaction, mouse interaction, web-based interaction, object manipulation, human-computer interaction, gaze tracking, accessible technology, hand gesture recognition.*

Сергій ЗЕЛІНСЬКИЙ
аспірант кафедри комп'ютерної інженерії, факультет радіофізики, електроніки та комп'ютерних систем, Київський національний університет імені Тараса Шевченка, вул. Володимирська, 60, м. Київ, Україна, 01033
***ORCID:** 0009-0003-6271-2601*

Юрій БОЙКО
кандидат фізико-математичних наук, доцент, завідувач кафедри комп'ютерної інженерії факультету радіофізики, електроніки та комп'ютерних, Київський національний університет імені Тараса Шевченка, вул. Володимирська, 60, м. Київ, Україна, 01033
***ORCID:** 0000-0003-1417-7424*
***Scopus Author ID:** 24722552300*

Бібліографічний опис статті: Зелінський, С., Бойко, Ю. (2024). Дослідження взаємодії на основі погляду та жестів у веб-середовищі: порівняння з взаємодією комп'ютерною мишею для маніпулювання об'єктами. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 33–42, doi: https://doi.org/10.32782/IT/2024-3-4

ДОСЛІДЖЕННЯ ВЗАЄМОДІЇ НА ОСНОВІ ПОГЛЯДУ ТА ЖЕСТІВ У ВЕБ-СЕРЕДОВИЩІ: ПОРІВНЯННЯ З ВЗАЄМОДІЄЮ КОМП'ЮТЕРНОЮ МИШЕЮ ДЛЯ МАНІПУЛЮВАННЯ ОБ'ЄКТАМИ

Метою *цього дослідження є реалізація та оцінка веб-орієнтованого методу взаємодії на основі погляду та жестів для маніпулювання об'єктами, використовуючи стандартну веб-камеру. Цей метод поєднує відстеження погляду для вибору об'єктів з жестами рук для природних маніпуляцій, таких як обертання, масштабування та перетягування. На відміну від інших реалізацій цієї взаємодії, що вимагають спеціалізованого обладнання, цей метод використовує широко доступні технології, роблячи передові техніки взаємодії більш доступними.*

Наукова новизна *полягає в розробці системи взаємодії на основі погляду та жестів, яка працює повністю на веб-платформі з використанням стандартного обладнання, що усуває потребу в дорогому спеціалізованому обладнанні та дозволяє ширше впровадження.*

Методологія *включає створення веб-системи з використанням алгоритмів комп'ютерного зору для відстеження погляду в реальному часі та розпізнавання жестів. Було проведено дослідження за участю користувачів, які виконували завдання з маніпулювання об'єктами, використовуючи як метод введення на основі погляду та жестів, так і традиційне введення комп'ютерною мишею, з подальшим записом та аналізом часу виконання завдань.*

Висновок. *Дослідження показує, що взаємодія на основі погляду та жестів є особливо ефективною для завдань, що вимагають одночасних дій, таких як обертання та масштабування об'єктів, перевершуючи введення комп'ютерною мишею у таких сценаріях. Хоча введення комп'ютерною мишею залишається більш ефективним для простіших завдань, взаємодія на основі погляду та жестів має великий потенціал для підвищення ефективності користувачів при виконанні складних завдань на веб-платформах, сприяючи розвитку більш доступних та інтуїтивно зрозумілих методів введення.*

Ключові слова: *взаємодія на основі погляду та жестів, взаємодія комп'ютерною мишею, веб-орієнтована взаємодія, маніпулювання об'єктами, взаємодія людина-комп'ютер, відстеження погляду, доступні технології, розпізнавання жестів рук.*

Introduction. The interaction between users and computer systems has greatly evolved, expanding from traditional input devices like the mouse and keyboard to more natural methods, including eye-tracking, hand gestures, facial expressions, or their combinations. These advancements are designed to create more engaging and efficient user experiences, especially in complex digital environments.

Motivation. Pointing to graphical elements is one of the fundamental tasks in human-computer interaction (HCI) (Argelaguet & Andujar, 2013). Eye-tracking stands out compared to traditional mouse input due to its speed (Ware & Mikaelian, 1986). This allows users to quickly select objects simply by looking at them. On the other hand, hand gestures allow for more natural and intuitive manipulation of objects, enabling users to rotate, scale, and move items as they would in the physical world. The combination of gaze tracking and hand gestures has gained considerable attention, especially in virtual reality (VR) (Pfeuffer et al., 2017), where it enhances user experience by creating seamless and immersive interactions. However, the adoption of this interaction method outside of VR, particularly on the web, has been limited due to hardware requirements.

Objective. The primary objective of this study is to implement and evaluate a gaze and hand gesture-based interaction (gaze-gesture interaction) technique on the web using only a standard computer web camera. By removing the need for specialized hardware, the study aims to make this advanced interaction method more accessible and practical for a broader range of users.

Approach. To achieve this objective, the study involves the development of a web-based platform that leverages a standard web camera for gaze tracking and gesture recognition. The effectiveness of the gaze-gesture interaction method is evaluated by comparing it to the traditional mouse input method in scenarios where users are required to manipulate objects, such as rotating, scaling, and dragging. The comparison is based on task completion time.

Related Work. In recent years, new types of input methods have appeared in the field of human-computer interaction. Traditional devices like the mouse and keyboard have been supplemented by more advanced techniques, including gaze tracking, hand gestures, and facial expressions. For instance, (Rozado et al., 2017) describe the FaceSwitch, which supports

motor-impaired users to interact with a computer hands-free by using gaze pointing for target selection and facial gestures for target-specific action commands. (Wachs et al., 2011) examines various applications of vision-based hand-gesture interfaces across different fields, such as medical systems, assistive technologies, entertainment, crisis management, disaster relief, and human-robot interaction.

Gaze and Hand Gesture Interaction

Gaze tracking is recognized for its speed, allowing users to quickly select and focus on objects simply by looking at them. This makes gaze interaction faster than other input modalities (Ware & Mikaelian, 1986), particularly in scenarios where quick selections are necessary. Hand gestures complement gaze tracking by providing a more natural way to manipulate objects, enabling actions like rotating, scaling, and dragging with intuitive hand movements. (Slambekova et al., 2012) presented a framework for enabling the use of both gaze and hand gestures for interaction within a 3D virtual world.

A set of interaction techniques combining gaze and free-space hand gestures has been presented in (Chatterjee et al., 2015). Results showed that the combination of gaze and gesture can outperform systems using gaze or gesture alone. Another study showed the gaze-assisted techniques to outperform hands-only input and gives insight into trade-offs in combining gaze with direct or indirect, and spatial or semantic freehand gestures (Lystbæk et al., 2022).

(Ryu et al., 2019) proposed a spatial interaction technique called gaze-grasp pose interaction (GG Interaction) that can be used in 3D virtual spaces for object manipulation.

Another research introduced a novel virtual mouse system that enables users to control an on-screen pointer using hand and eye gestures, providing a contactless input method (Reddy et al., 2023).

The combination of gaze tracking and hand gestures has been studied in the context of virtual reality (VR). In VR environments, this interaction method allows users to look at objects and manipulate them with their hands, creating a highly immersive experience (Pfeuffer et al., 2017).

Despite the advantages of the interaction method based on the combination of gaze and hand gestures, this approach has its own challenges. In (Pfeuffer, 2024), the author discusses design principles and issues, focusing on interfaces that use gaze and pinch interaction.

Limitations of Current Implementations. Most implementations from the presented research rely on sophisticated equipment like eye-trackers, cameras with infrared (IR) sensors, or devices such as Microsoft Kinect. Some studies have even developed custom-made eye-tracking devices to enable this interaction method (Hales, 2013). The need for specialized hardware creates a barrier to the broad adoption of such an interaction method, particularly on more accessible platforms like the web.

Web-Based Interaction and Accessibility. With the increasing popularity of web applications, there is a growing interest in implementing advanced interaction techniques using widely available hardware. Recent advancements in computer vision and machine learning have made it possible to track gaze and recognize gestures directly in the browser using standard web cameras. This, in turn, allows us to bring gaze and gesture-based interaction methods to the web. However, the effectiveness and practicality of these web-based implementations in real-world scenarios remain underexplored.

Summary. Existing research highlights the advantages of combining gaze tracking and hand gestures, particularly in VR environments, where they enhance user experience and interaction efficiency. However, the reliance on specialized hardware limits the broader adoption of this method, especially on the web. This study aims to address this gap by implementing and evaluating a web-based gaze-gesture interaction method that utilizes a standard web camera. Through this research, we want to make this advanced interaction technique more accessible and practical for everyday use.

Methods

System Overview

The developed system integrates eye-tracking and hand gesture recognition technologies to enable intuitive interaction with on-screen objects. Fig. 1 illustrates the system architecture diagram. The system is composed of four primary modules:

1. **Eye-Tracking Module.** Responsible for detecting the user's gaze and identifying the on-screen object they are focusing on.

2. **Hand Detection Module.** Detects and tracks the user's hands, providing real-time positional data of key hand landmarks.

3. **Gesture Recognition Module.** Interprets the hand landmarks to recognize specific gestures, such as pinch gestures, and sends this information to the Object Manipulation module.

4. **Object Manipulation Module.** Receives data from the Eye-Tracking and Gesture Recognition modules and determines the appropriate transformation (e.g., selection, dragging, scaling,

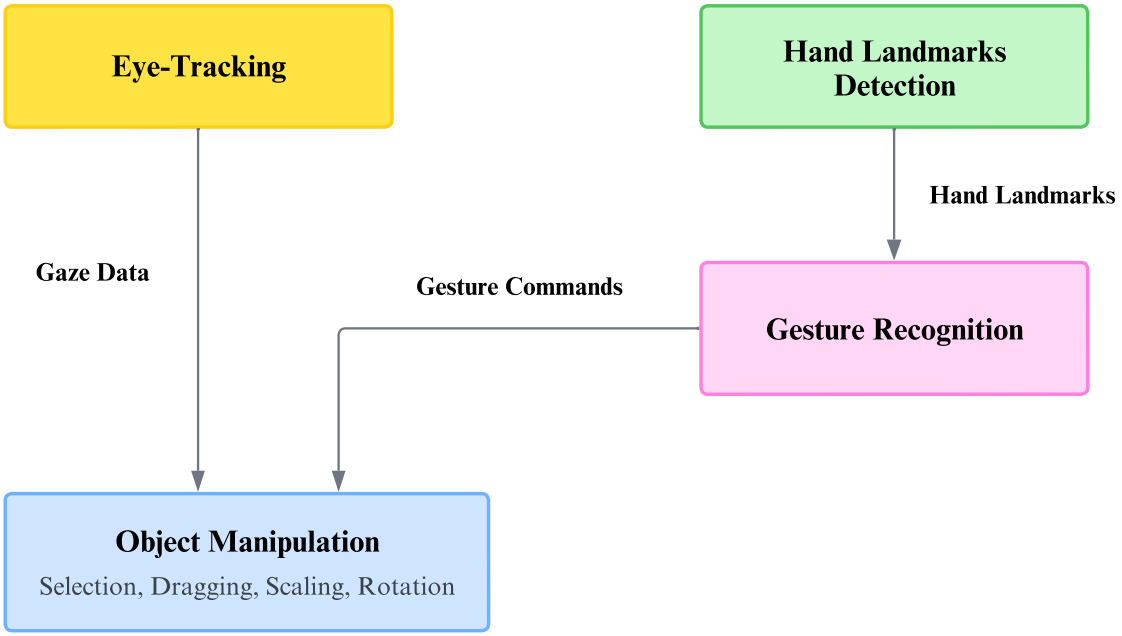


Fig. 1. System architecture overview

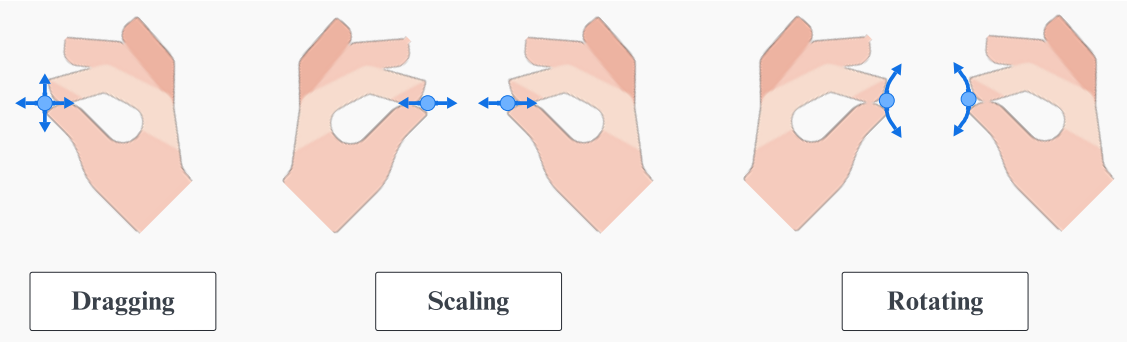


Fig. 2. Illustration of the hand gestures recognized by the system for dragging, scaling, and rotating objects

rotation) to be applied to the selected object based on the user's input.

Eye-Tracking Module. The Eye-Tracking Module, which was implemented using WebGazer.js (Papoutsaki et al., 2016), continuously monitors the user's gaze direction to determine the point of regard on the screen. This information is used to identify which object the user intends to interact with. The gaze data is crucial for initiating the selection process, allowing for hands-free interaction.

Hand Detection Module. The Hand Detection Module utilizes the MediaPipe Hand Landmarker (Google, n.d.) to accurately identify and track the positions of key landmarks on the user's hands. This module is responsible for providing the positional data necessary for gesture recognition. The detected hand landmarks are continuously updated to reflect the user's hand movements in real time.

Gesture Recognition Module. The Gesture Recognition Module processes the hand landmark data provided by the Hand Detection Module to identify specific gestures. For instance, the system recognizes pinch gestures by calculating the Euclidean distance between the thumb and index fingertip landmarks. When this distance falls below a specified threshold, the gesture is classified as a pinch. The recognized gestures are then passed on to the Object Manipulation Module, which uses the input to perform actions such as dragging, scaling, and rotating the selected object.

Fig. 2 illustrates gestures the system can detect and respond to. They include:

- **Dragging.** A single-hand pinch gesture is used to drag objects across the screen.
- **Scaling.** A two-hand pinch gesture, where the distance between the hands increases or decreases, is used to scale the object.
- **Rotating.** A two-hand pinch gesture, where the hands rotate relative to each other, is used to rotate the object.

Object Manipulation Module. The Object Manipulation Module is responsible for applying the appropriate transformation to the selected object based on the combined input from the Eye-Tracking and Gesture Recognition modules. This module determines whether to select, drag, scale, or rotate the object depending on the user's gaze position and the recognized gestures. For instance, if the system detects a gaze fixated on an object and a pinch gesture, it triggers the selection and dragging of that object. If pinch gestures are detected on both hands, the system initiates scaling and/or rotation actions depending on the movement direction.

Interaction Workflow

The interaction process in the developed system is designed to provide an intuitive and seamless user experience by integrating gaze-based object selection with hand gesture-driven manipulation. The interaction flowchart is displayed in Fig. 3. The interaction workflow is as follows:

1. **Gaze at Object.** The user initiates the interaction by gazing at the desired object on the screen. The eye-tracking module detects the gaze point and selects the object for potential manipulation.
2. **Hand Gesture Detection.** The system continuously monitors the user's hands to detect any gestures. The hand detection module identifies the positions of key hand landmarks and sends this data to the gesture recognition module.
3. **Gesture Recognition.** Once a gesture is detected, the system interprets the specific type of gesture being performed. The recognition module identifies single-hand pinch gestures for dragging and two-hand pinch gestures for scaling and rotating.
4. **Object Manipulation.** Based on the recognized gestures and gaze data, the system performs the corresponding action – whether it be dragging, scaling, rotating, or a combination of scaling and rotating – on the selected object.

The system supports simultaneous scaling and rotation of the selected object. When a two-hand pinch gesture is detected, the system analyzes both the distance between the hands (for scaling) and the rotational movement (for rotation). If both actions are detected simultaneously, the system applies both transformations concurrently to the selected object.

System Interface Overview

The interface used during the evaluation sessions is illustrated in Fig. 4. This screenshot captures the key elements of the system that were critical for conducting the experiments:

1. **Video Feed and Hand Landmark Overlay.** The interface features a live video feed with hand landmarks overlayed to provide real-time feedback on recognized gestures.

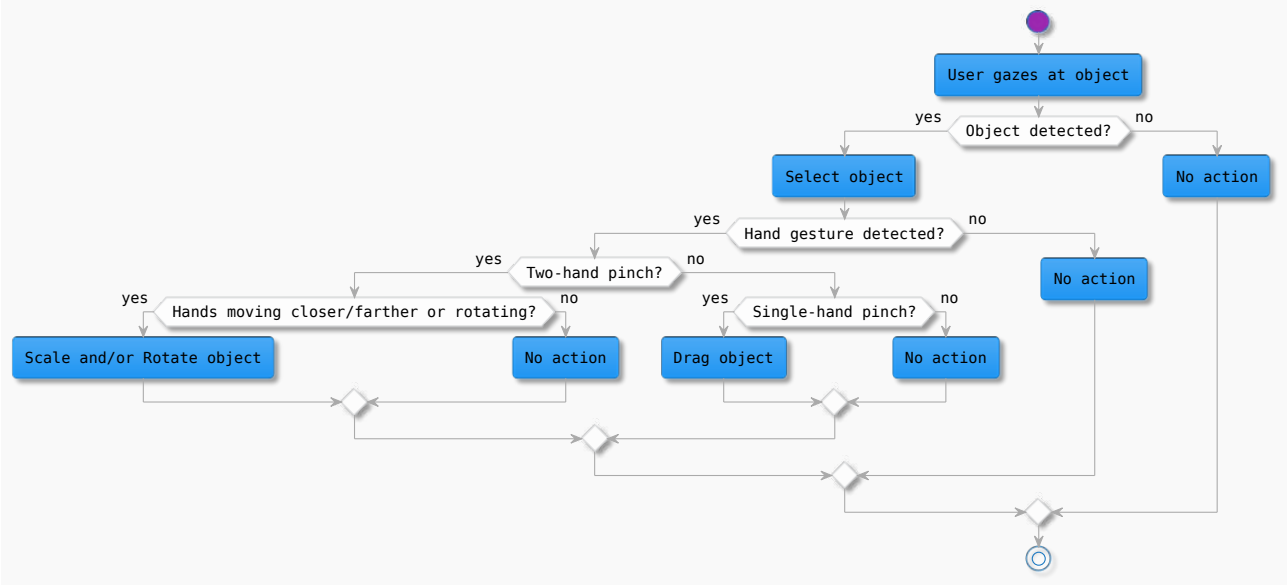


Fig. 3. Interaction workflow

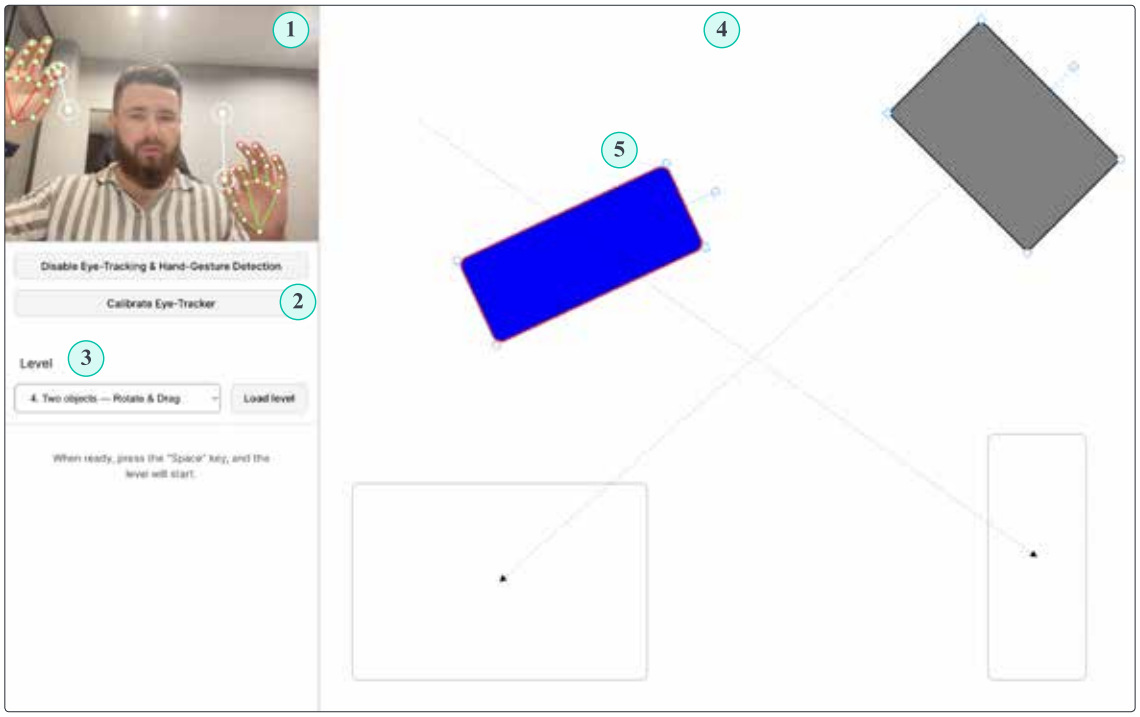


Fig. 4. Screenshot of the developed system interface – manipulating selected object

2. **Eye-Tracker Calibration Button.** A calibration tool is provided to ensure the accuracy of the eye-tracking system before each session starts.

3. **Level Picker.** A tool for selecting different levels, varying in difficulty.

4. **Object Manipulation Stage.** This area displays the objects participants need to manipulate and position within their respective designated areas.

5. **Selected Object.** The object the current transformation is applied to.

The tasks for participants were structured into 5 different levels, with increasing complexity from Level 1 to Level 5. Each level can be completed using either mouse input or gaze-gesture Input.

To complete a level, users must position objects in the designated areas (the system displays a designated area for each object using hint arrows). After completing a level, the system displays the time taken by a user to complete it. The complexity of the levels is based on the number of objects and transformations users need to apply to the objects in order to complete the level:

- **Level 1.** Drag one object to the designated area.
- **Level 2.** Drag two objects to their respective designated areas.
- **Level 3.** Scale and drag two objects to the designated areas.
- **Level 4.** Rotate and drag two objects to the designated areas.
- **Level 5.** Rotate, scale, and drag two objects to their designated areas.

Fig. 5 contains an overview of all evaluation levels.

The user interface of the completed level is illustrated in Fig. 6. The following key elements, except those already mentioned, are numerically highlighted:

1. **Time Display.** After the current level is completed, the system displays the time taken by the user to complete it.

2. **Gaze Indicator.** Displays the user's gaze point.

3. **Matched Object.** The object is successfully positioned within the designated area.

Evaluation and Results

Evaluation Approach

To evaluate the effectiveness of the gaze-gesture interaction method in comparison to the traditional mouse input method, a user study was conducted involving 10 participants. Each participant completed 5 levels, designed to progressively increase in complexity, using both interaction methods. Each participant completed each level 5 times (5 trials) for each method.

The levels were structured as follows:

- **Level 1.** Simple object dragging: participants had to **drag one object** to a designated area.
- **Level 2.** Dragging multiple objects: participants had to **drag two objects** to their respective designated areas.

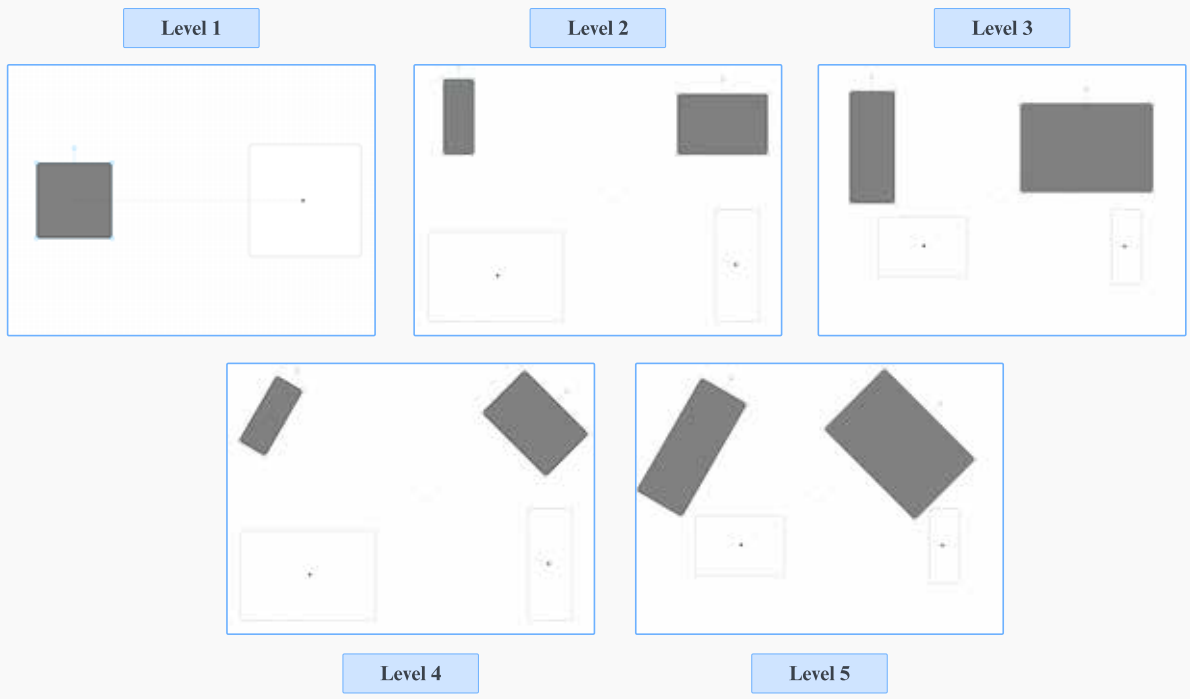


Fig. 5. Overview of all evaluation levels

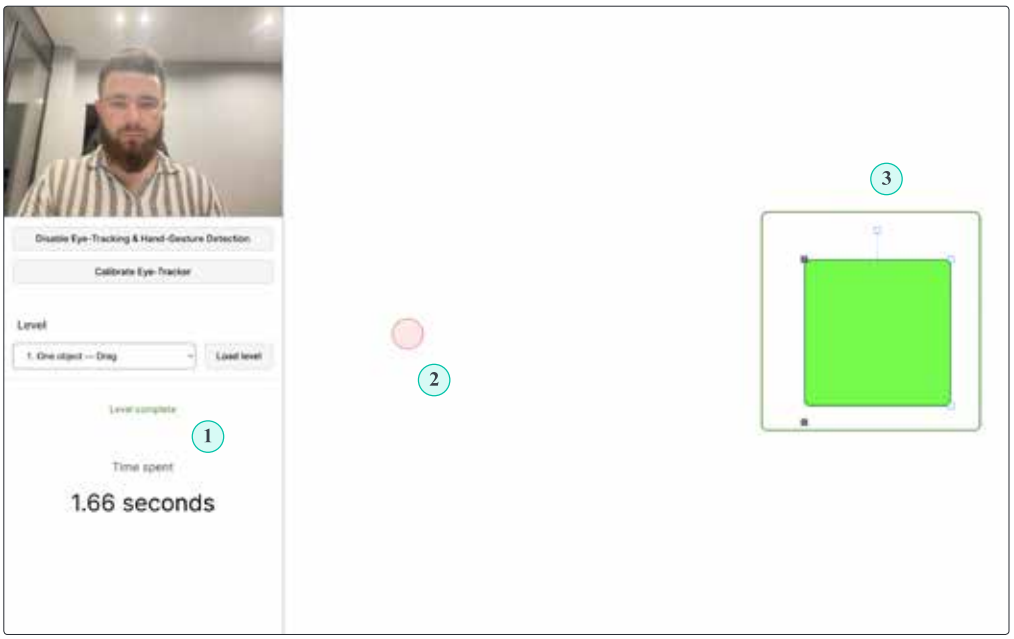


Fig. 6. Screenshot of the developed system interface – completed level

- **Level 3.** Scaling and dragging objects: participants had to **scale and drag two objects** to their respective designated areas.
- **Level 4.** Rotating and dragging objects: participants had to **rotate and drag two objects** to their respective designated areas.
- **Level 5.** A combination of rotating, scaling, and dragging objects: participants had to **rotate, scale, and drag two objects** to their respective designated areas.

The primary metric used for evaluation was the time taken to complete each level, recorded in seconds.

Results. The average task completion time for each level, aggregated across all participants, is shown in Fig. 7. The chart compares the performance of the mouse input method with the gaze-gesture interaction method.

As shown in the chart, the mouse input method generally resulted in faster task completion times

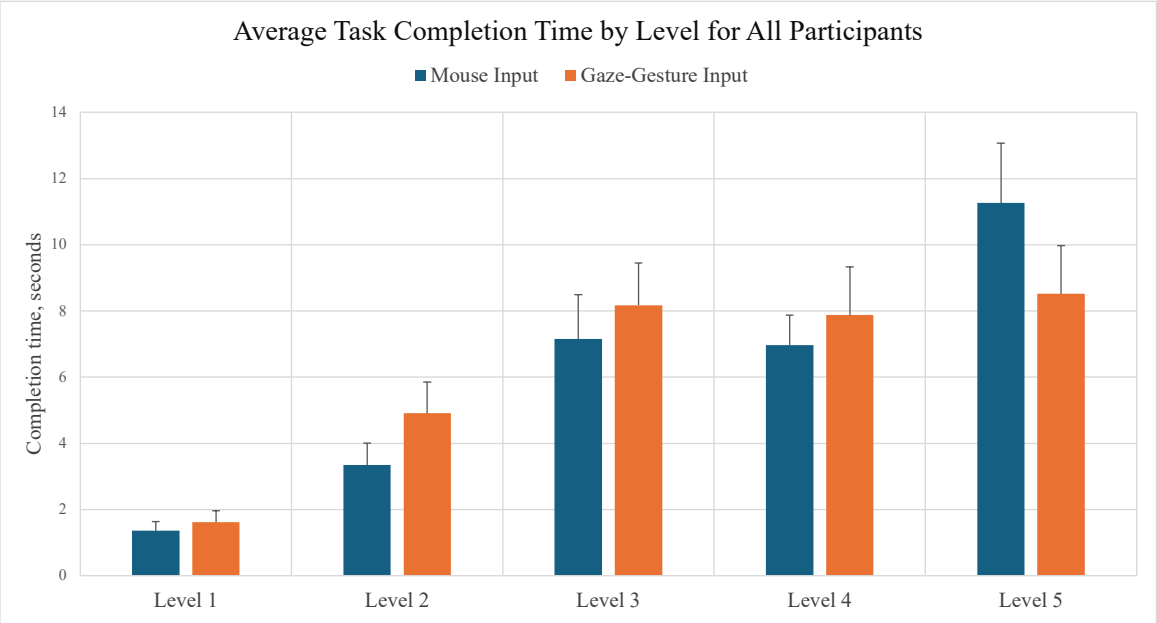


Fig. 7. Average task completion time by level across all participants

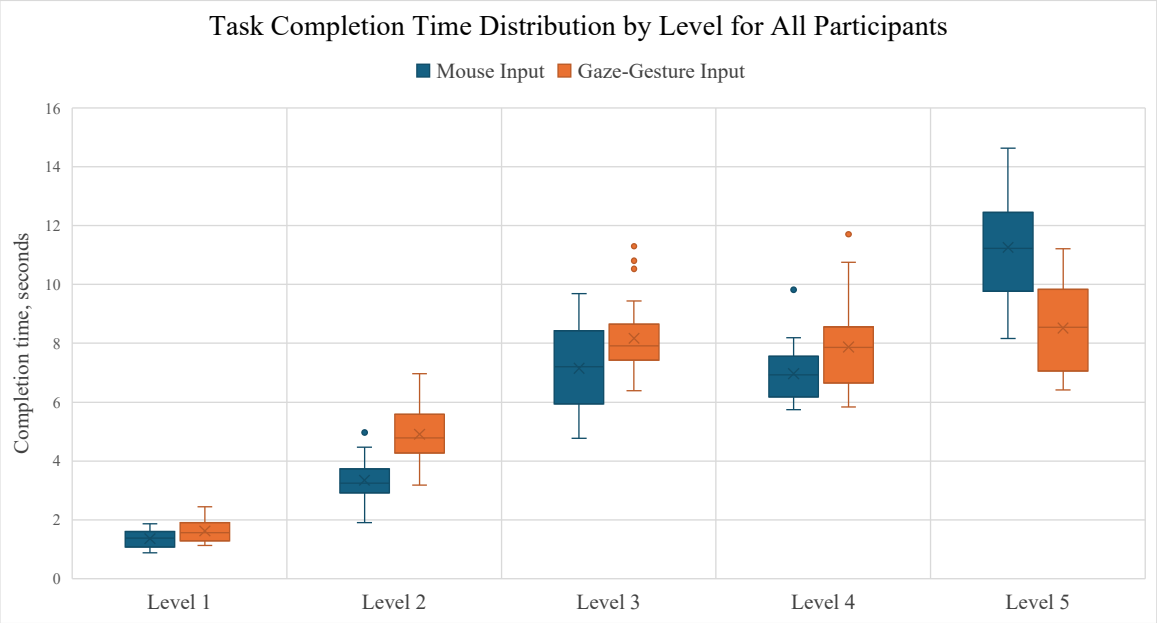


Fig. 8. Task completion time distributed by level for all participants

across most levels, particularly for simpler tasks. However, in Level 5, where participants were required to rotate, scale, and drag objects, the gaze-gesture interaction method outperformed the mouse interaction method. This suggests that the gaze-gesture interaction method is particularly well-suited for complex tasks that involve multiple simultaneous actions.

The box plots of the task completion times for each level are shown in Fig. 8. It illustrates variability in participants' performance for both interaction methods. The mouse input method generally has lower variability, particularly in the earlier levels. In contrast, the gaze-gesture interaction method showed higher variability, which is expected given the novelty of the interaction technique. However, in Level 5, the gaze-gesture interaction method not only matched but exceeded the mouse method in efficiency, as indicated by the lower median completion time. This supports the observation that participants were able to leverage the simultaneous nature of gaze and hand gestures to perform complex actions more efficiently than when using a mouse, which required separate, sequential actions.

Discussion. While the mouse interaction method remains more efficient for simpler tasks, its sequential nature limits its effectiveness in complex scenarios. This study highlights the potential of the gaze-gesture interaction method, particularly in complex tasks that involve simultaneous actions like rotating, scaling, and dragging objects. Implemented and evaluated on a web-based platform using a standard web camera, this method requires no additional hardware, making it accessible and practical for a wide range of users. Additionally, with the gaze-gesture interaction method, it is possible to simultaneously manipulate multiple objects – users can capture and control two objects independently with each hand, which is not possible with traditional mouse input.

Potential Applications

Given its web-based implementation and reliance on standard technology, the gaze-gesture interaction method has several potential applications:

- **Web-Based Interactive Applications.** This method could be used in web applications that require complex object manipulations, such as online design tools, interactive maps, interactive educational platforms, and virtual reality environments accessed through a browser.
- **Remote Collaboration Tools.** It could enhance web-based collaboration platforms by allowing users to interact more naturally with shared content, such as rotating and scaling 3D models in real time.
- **Accessibility Tools.** The gaze-gesture method could provide an alternative input mechanism for users with limited mobility, offering more intuitive control over web interfaces with no need for traditional input devices.

Future Directions

Future research could explore hybrid approaches that combine the gaze-gesture interaction method with traditional input devices, as this may be useful in specific use cases. Additionally, further investigation into a wider range of applications for the gaze-gesture interaction method could help assess and expand its utility across various digital environments.

Conclusions. This study evaluated the gaze-gesture interaction method, implemented and tested on a web-based platform using a standard web camera with no additional hardware requirements. The results demonstrate that while the traditional mouse input method is more efficient for simpler tasks, the gaze-gesture method shows better results in scenarios that require simultaneous actions, like rotating, scaling, and dragging objects.

The ability to perform multiple actions concurrently is a significant advantage of the gaze-gesture method, making it particularly suitable for complex, multitasking environments. The implementation on the web using a standard camera demonstrates the accessibility and practicality of this approach, eliminating the need for specialized hardware.

Future work should focus on exploring hybrid approaches that combine the gaze-gesture interaction method with traditional input devices, as this may offer benefits in certain scenarios. Additionally, further research could investigate broader applications of the gaze-gesture interaction method across various digital environments to assess its potential to enhance interaction efficiency and user experience.

BIBLIOGRAPHY:

1. Argelaguet F., Andujar C. A survey of 3D object selection techniques for virtual environments. *Computers & Graphics*, 2013. 37(3), 121–136. https://doi.org/10.1016/j.cag.2012.12.003

2. Chatterjee I., Xiao R., Harrison C. Gaze+gesture: Expressive, precise and targeted free-space interactions. *Proceedings of the 2015 ACM on International Conference on Multimodal Interaction*, 2015. 131–138. https://doi.org/10.1145/2818346.2820752

3. Google. (n.d.). MediaPipe hand landmarker. URL: fhttps://ai.google.dev/edge/mediapipe/solutions/vision/hand_landmarker June 26, 2024

4. Hales J. Interacting with objects in the environment by gaze and hand gestures. 2013. URL:https://api.semanticscholar.org/CorpusID:52206471

5. Lystbæk M. N., Rosenberg P., Pfeuffer K., Grønbæk J. E., Gellersen H. Gaze-hand alignment: Combining eye gaze and mid-air pointing for interacting with menus in augmented reality. *Proceedings of the ACM on Human-Computer Interaction*, *6*(ETRA), 2022. 1–18. https://doi.org/10.1145/3530886

6. Papoutsaki A., Sangkloy P., Laskey J., Daskalova N., Huang J., Hays J. WebGazer: Scalable webcam eye tracking using user interactions. *Proceedings of the 25th International Joint Conference on Artificial Intelligence (IJCAI)*, 2016. 3839–3845.

7. Pfeuffer K. Design principles & issues for gaze and pinch interaction. *ArXiv*, abs/2401.10948. 2024. URL: https://api.semanticscholar.org/CorpusID:267069101

8. Pfeuffer K., Mayer B., Mardanbegi D., Gellersen H. Gaze + pinch interaction in virtual reality. *Proceedings of the 5th Symposium on Spatial User Interaction*, 2017. 99–108. https://doi.org/10.1145/3131277.3132180

9. Reddy N. L., Murugeswari R., Imran Md., Subhash N., Reddy N. V. K., Adarsh N. B. Virtual mouse using hand and eye gestures. *2023 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, 2023. 1–5. https://doi.org/10.1109/ICDSAAI59313.2023.10452550

10. Rozado D., Niu J., Lochner M. Fast human-computer interaction by combining gaze pointing and face gestures. *ACM Transactions on Accessible Computing*, 2017. 10(3), 1–18. https://doi.org/10.1145/3075301

11. Ryu K., Lee J.-J., Park J.-M. GG interaction: A gaze–grasp pose interaction for 3D virtual object selection. *Journal on Multimodal User Interfaces*, 2019. 13(4), 383–393. https://doi.org/10.1007/s12193-019-00305-y

12. Slambekova D., Bailey R., Geigel J. Gaze and gesture based object manipulation in virtual worlds. *Proceedings of the 18th ACM Symposium on Virtual Reality Software and Technology*, 2012. 203–204. https://doi.org/10.1145/2407336.2407380

13. Wachs J. P., Kölsch M., Stern H., Edan Y. Vision-based hand-gesture applications. *Communications of the ACM*, 2011. *54*(2), 60–71. https://doi.org/10.1145/1897816.1897838

14. Ware C., Mikaelian H. H. An evaluation of an eye tracker as a device for computer input2. *Proceedings of the SIGCHI/GI Conference on Human Factors in Computing Systems and Graphics Interface*, 1986. 183–188. https://doi.org/10.1145/29933.275627

REFERENCES:

1. Argelaguet, F., & Andujar, C. (2013). A survey of 3D object selection techniques for virtual environments. *Computers & Graphics*, *37*(3), 121–136. https://doi.org/10.1016/j.cag.2012.12.003

2. Chatterjee, I., Xiao, R., & Harrison, C. (2015). Gaze+gesture: Expressive, precise and targeted free-space interactions. *Proceedings of the 2015 ACM on International Conference on Multimodal Interaction*, 131–138. https://doi.org/10.1145/2818346.2820752

3. Google. (n.d.). MediaPipe hand landmarker. Retrieved June 26, 2024, from https://ai.google.dev/edge/mediapipe/solutions/vision/hand_landmarker

4. Hales, J. (2013). Interacting with objects in the environment by gaze and hand gestures. https://api.semanticscholar.org/CorpusID:52206471

5. Lystbæk, M. N., Rosenberg, P., Pfeuffer, K., Grønbæk, J. E., & Gellersen, H. (2022). Gaze-hand alignment: Combining eye gaze and mid-air pointing for interacting with menus in augmented reality. *Proceedings of the ACM on Human-Computer Interaction*, *6*(ETRA), 1–18. https://doi.org/10.1145/3530886

6. Papoutsaki, A., Sangkloy, P., Laskey, J., Daskalova, N., Huang, J., & Hays, J. (2016). WebGazer: Scalable webcam eye tracking using user interactions. *Proceedings of the 25th International Joint Conference on Artificial Intelligence (IJCAI)*, 3839–3845.

7. Pfeuffer, K. (2024). Design principles & issues for gaze and pinch interaction. *ArXiv*, abs/2401.10948. https://api.semanticscholar.org/CorpusID:267069101

8. Pfeuffer, K., Mayer, B., Mardanbegi, D., & Gellersen, H. (2017). Gaze + pinch interaction in virtual reality. *Proceedings of the 5th Symposium on Spatial User Interaction*, 99–108. https://doi.org/10.1145/3131277.3132180

9. Reddy, N. L., Murugeswari, R., Imran, Md., Subhash, N., Reddy, N. V. K., & Adarsh, N. B. (2023). Virtual mouse using hand and eye gestures. *2023 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, 1–5. https://doi.org/10.1109/ICDSAAI59313.2023.10452550

10. Rozado, D., Niu, J., & Lochner, M. (2017). Fast human-computer interaction by combining gaze pointing and face gestures. *ACM Transactions on Accessible Computing*, *10*(3), 1–18. https://doi.org/10.1145/3075301

11. Ryu, K., Lee, J.-J., & Park, J.-M. (2019). GG interaction: A gaze–grasp pose interaction for 3D virtual object selection. *Journal on Multimodal User Interfaces*, *13*(4), 383–393. https://doi.org/10.1007/s12193-019-00305-y

12. Slambekova, D., Bailey, R., & Geigel, J. (2012). Gaze and gesture based object manipulation in virtual worlds. *Proceedings of the 18th ACM Symposium on Virtual Reality Software and Technology*, 203–204. https://doi.org/10.1145/2407336.2407380

13. Wachs, J. P., Kölsch, M., Stern, H., & Edan, Y. (2011). Vision-based hand-gesture applications. *Communications of the ACM*, *54*(2), 60–71. https://doi.org/10.1145/1897816.1897838

14. Ware, C., & Mikaelian, H. H. (1986). An evaluation of an eye tracker as a device for computer input2. *Proceedings of the SIGCHI/GI Conference on Human Factors in Computing Systems and Graphics Interface*, 183–188. https://doi.org/10.1145/29933.275627

UDC 004.056.5
DOI https://doi.org/10.32782/IT/2024-3-5

Vadym KAIDALOV
Postgraduate Student at the Department of Software Engineering, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, vadym.kaidalov@gmail.com
ORCID: *0009-0007-0027-9207*

Vira GOLIAN
Candidate of Technical Sciences, Associate Professor, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, vira.golan@nure.ua
ORCID: *0000-0002-7196-5286*
Scopus Author ID: *56008181700*

To cite this article: Kaidalov, V., Golian, V. (2024). Pokrashchennia avtentyfikatsii na osnovi dynamiky natyskannia klavish: balansuvannia tochnosti ta zruchnosti korysuvannia cherez efektyvne navchannia [Improving Keystroke Dynamics Authentication: Balancing Accuracy and User Experience Through Efficient Training]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 43–50, doi: https://doi.org/10.32782/IT/2024-3-5

IMPROVING KEYSTROKE DYNAMICS AUTHENTICATION: BALANCING ACCURACY AND USER EXPERIENCE THROUGH EFFICIENT TRAINING

The aim of this study *is to enhance the security and user experience of two-factor authentication systems through the application of keystroke dynamics, a form of behavioral biometrics. Keystroke dynamics analyze the unique typing patterns of users to offer a biometric factor for authentication, which complements the traditional knowledge-based method (username and password). This study specifically seeks to evaluate different anomaly detection algorithms to determine the minimum number of password repetitions required for effective training, optimizing both system security and user convenience.*

Methodology. *The study replicates and extends the evaluation procedure of Killourhy and Maxion, who provided a public dataset and a detailed protocol for analyzing keystroke dynamics. The algorithms are evaluated by varying the number of password repetitions used for training, with the aim of determining the optimal training size that balances security (lower EER) and efficiency (reduced user effort).*

Scientific Novelty. *The scientific novelty of this research lies in its investigation of the trade-off between security and user convenience in keystroke dynamics-based authentication systems. While many studies have focused on improving the accuracy of anomaly detection, this research emphasizes the importance of minimizing the training burden on users by determining the minimum number of password repetitions required for stable performance. By focusing on training efficiency and computational resource optimization, this research advances the field of behavioral biometrics and contributes to the practical deployment of keystroke dynamics in real-world authentication systems.*

Conclusion. *The study demonstrates that keystroke dynamics can significantly improve the security of two-factor authentication systems without imposing excessive burdens on users. The findings confirm that the Manhattan (scaled) and Outlier Count (z-score) algorithms perform relatively well, particularly when the training set size is small, which is critical for practical use in authentication systems where users may be unwilling to provide numerous password repetitions. This study not only replicates the results of prior research but also contributes new insights into optimizing the training process for keystroke dynamics-based anomaly detection. Future work may explore integrating keystroke dynamics with other biometric factors, such as mouse dynamics, to develop even more secure and user-friendly multimodal authentication systems. Furthermore, continuous authentication mechanisms represent an exciting direction for future research, providing ongoing verification of user identity throughout a session rather than solely at login.*

Key words: *keystroke dynamics, two-factor authentication, anomaly detection, behavioral biometrics, user authentication, security, continuous authentication.*

Вадим КАЙДАЛОВ
аспірант кафедри Програмної Інженерії, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
ORCID: *0009-0007-0027-9207*

Віра ГОЛЯН
кандидат технічних наук, доцент кафедри Програмної Інженерії, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0000-0002-7196-5286*
***Scopus Author ID:** 56008181700*

Бібліографічний опис статті: Кайдалов, В., Голян, В. (2024). Покращення автентифікації на основі динаміки натискання клавіш: балансування точності та зручності користування через ефективне навчання. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 43–50, doi: https://doi.org/10.32782/IT/2024-3-5

ПОКРАЩЕННЯ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ДИНАМІКИ НАТИСКАННЯ КЛАВІШ: БАЛАНСУВАННЯ ТОЧНОСТІ ТА ЗРУЧНОСТІ КОРИСТУВАННЯ ЧЕРЕЗ ЕФЕКТИВНЕ НАВЧАННЯ

***Мета цього дослідження** – покращити безпеку та досвід користувачів систем двофакторної аутентифікації шляхом застосування динаміки натискання клавіш, форми поведінкової біометрії. Динаміка натискання клавіш аналізує унікальні шаблони набору тексту користувачів для створення біометричного фактору автентифікації, який доповнює традиційний метод, що базується на знаннях (ім'я користувача та пароль). Це дослідження спрямоване на оцінку різних алгоритмів виявлення аномалій, щоб визначити мінімальну кількість повторень пароля, необхідну для ефективного навчання, оптимізуючи як безпеку системи, так і зручність для користувача.*

***Методологія.** Дослідження повторює і розширює процедуру оцінки Killourhy та Maxion, які надали публічний набір даних і детальний протокол для аналізу динаміки натискання клавіш. Алгоритми оцінюються шляхом варіювання кількості повторень пароля, використаних для навчання, з метою визначення оптимального розміру навчання, що збалансовує безпеку (менший EER) та ефективність (зменшене навантаження на користувача).*

***Наукова новизна.** Наукова новизна цього дослідження полягає в дослідженні компромісу між безпекою і зручністю для користувача в системах автентифікації на основі динаміки натискання клавіш. Хоча багато досліджень зосереджені на поліпшенні точності виявлення аномалій, це дослідження підкреслює важливість мінімізації навантаження на користувачів шляхом визначення мінімальної кількості повторень пароля, необхідної для стабільної роботи. Зосереджуючи увагу на ефективності навчання та оптимізації обчислювальних ресурсів, це дослідження просуває галузь поведінкової біометрії і сприяє практичному впровадженню динаміки натискання клавіш у реальних системах автентифікації.*

***Висновок.** Дослідження демонструє, що динаміка натискання клавіш може суттєво покращити безпеку систем двофакторної автентифікації без накладення надмірного навантаження на користувачів. Результати підтверджують, що алгоритми Manhattan (scaled) і Outlier Count (z-score) працюють відносно добре, особливо коли розмір навчального набору малий, що критично для практичного використання в системах аутентифікації, де користувачі можуть бути не готові надати численні повторення пароля. Це дослідження не лише повторює результати попередніх досліджень, але й вносить нові ідеї для оптимізації процесу навчання для виявлення аномалій на основі динаміки натискання клавіш. Майбутні роботи можуть досліджувати інтеграцію динаміки натискання клавіш з іншими біометричними факторами, такими як динаміка миші, щоб розробити ще більш безпечні та зручні багатомодальні системи автентифікації. Крім того, механізми безперервної автентифікації є захоплюючим напрямком для майбутніх досліджень, забезпечуючи постійну перевірку ідентичності користувача протягом сесії, а не тільки при вході.*

***Ключові слова:** динаміка натискання клавіш, двофакторна автентифікація, виявлення аномалій, поведінкова біометрія, автентифікація користувачів, безпека, безперервна автентифікація.*

Introduction. User authentication is the process of verifying a user's identity widely used in computer systems to protect data from unauthorized access. Typically, a username and password pair is used as a piece of the knowledge that only the genuine user should know to confirm their identity. However, such an approach is often not secure enough, leading to the introduction of the so-called «second factor» in the authentication process. Generally, there are three types of the factors: knowledge-based (something a user knows, e.g., the username and password values), possession-based (something a user has, e.g., their personal smartphone), and biometric-based (something a user is, e.g., their iris scan). The introduction of the second factor makes it harder for impostors to deceive the authentication system. However, the possession-based factors usually require additional effort from the genuine user, such as unlocking their smartphone and entering a PIN code or responding to a notification, thus worsening the user experience. Biometric authentication uses unique biometric traits of individuals to verify their identity. These traits can be broadly

divided into physiological (e.g., iris scan, fingerprint, voice) and behavioural (e.g., typing rhythms, mouse or touchscreen navigation patterns). In particular, keystroke dynamics is the process of identifying individual users on the basis of their typing rhythms, which are in turn derived from the timestamps of key-press and key-release events on the keyboard (Maxion & Killourhy, 2010, p. 201-210). This form of authentication uses behavioural biometric traits of users. If the authentication process is performed once when the user enters the system, it is called «static» authentication. If the biometric authentication is performed continuously during the user's session, it is called the «continuous» authentication (Ryu et al., 2021, p. 34541-34557). The current study examines a two-factor authentication system that verifies a user's identity by confirming their password as something that only the genuine user knows and applying keystroke dynamics on the timestamps of the keyboard events produced during the password entry. Such a system does not require any additional effort from users while being more secure due to the use of a second factor for authentication.

Related works. Killourhy and Maxion enabled the comparison of different anomaly detectors' performance across studies in the keystroke dynamics literature. They publicly shared a data set, developed an evaluation procedure, and measured the performance of various anomaly-detection algorithms on an equal basis (Maxion & Killourhy, 2010, p. 201-210). Typing data was collected from 51 subjects, each typing the same password 400 times. The researchers extracted various timing features from the raw data, such as keydown-keydown times and hold times. Fourteen anomaly detectors from the literature were reimplemented and evaluated according to a well-defined procedure. Another study by the same authors analysed factors influencing the accuracy of anomaly-detection algorithms: the algorithm itself, amount of training, choice of features, use of updating, impostor practice, and typist-to-typist variation (Killourhy & Maxion, 2010, p. 256-276). Their results indicated that the algorithm, amount of training, and use of updating were highly influential while impostor practice and feature set had minor effect. Some typists were significantly easier to distinguish than others. The researchers considered training amounts of 5, 50, 100, and 200 password repetitions done by the genuine user during the model training stage. While their study aimed to determine whether the amount of training could significantly influence the results in general, the problem of achieving stable accuracy rates with minimal training was not covered. Comparing the number of password repetitions required from users to train different anomaly-detection models can help select better models in terms of user experience, which is covered in this study. Additionally, determining the minimum number of repetitions needed to train an anomaly-detection model can help choose a reasonable size for the sliding window used in updating typing profiles, thus optimizing the use of computational resources.

Purpose. The purpose of this study is to reproduce the evaluation procedure described by Killourhy and Maxion, develop a method for comparing the minimum number of password repetitions needed to achieve stable accuracy rates for the best-performing anomaly detectors identified by the researchers, and share the Python source code with the research community to facilitate reproducibility. By determining the minimum number of repetitions required for training, the study aims to optimize the size of the sliding window used in updating typing profiles, thereby conserving computational resources.

Methodology. The data set shared by Killourhy and Maxion consists of keystroke-timing data collected from 51 subjects over 8 sessions. Each subject was asked to type the same password, «.tie5Roanl», 50 times during each session, providing timing information for a total of 400 password entries. The rationale for the choice of the password and other aspects of the data collection were described in detail by the researchers (Killourhy & Maxion, 2009, p. 125-134).

The raw typing data, such as key events and timestamps, cannot be used directly by an anomaly detector. Instead, sets of timing features are extracted from this raw data and organized into a vector of times, known as a timing vector. These features are used to train and test the detectors. The time between the key presses of consecutive keys (Keydown-Keydown), the time between the release of one key and the press of the next (Keyup-Keydown), and the time between the press and release of each key (Hold) are all available as features in the timing vectors provided by the mentioned data set. However, a study has shown there is no difference in anomaly detection accuracy among feature sets that include the Hold features and at least either Keydown-Keydown or Keyup-Keydown features (Killourhy & Maxion, 2010, p. 256-276). Therefore, only the Hold and Keyup-Keydown features are used from the data set for the evaluation procedure of the current study to conserve computational resources. The Enter key is also considered part of the password, so its Keyup-Keydown and Hold features are included as well. Given the aforementioned

password and the Enter key inclusion, each timing vector consists of 21 features: 11 Hold features and 10 Keyup-Keydown features.

Killourhy and Maxion implemented and evaluated 14 anomaly detectors from the keystroke-dynamics and pattern-recognition literature (Killourhy & Maxion, 2009, p. 125-134). They observed a clear division between seven detectors that were competitive in their evaluation and seven that were not. In the current study, the 5 best-ranked anomaly detectors have been reproduced according to the descriptions provided by the researchers: «Manhattan (scaled)», «Nearest Neighbour (Mahalanobis)», «Outlier Count (z-score)», one-class SVM and «Mahalanobis».

Typing data produced by an impostor should be detected as anomalous by an anomaly detector. In this context, the presence of an anomaly is referred to as a positive outcome, while its absence is called a negative outcome. When an anomaly detector incorrectly identifies a timing vector produced by the genuine user as anomalous, this mistake is termed a «false positive». All possible outcomes are shown in Table 1.

An anomaly detector produces a numeric value as a score assigned to the input timing vector. A threshold value must be chosen so that the detector marks the timing vector as anomalous if the score exceeds the threshold. The choice of a threshold value greatly influences the performance rates of detectors, so a range of threshold values should be used for performance measurements.

Given a certain threshold value, the True Positive Rate (TPR) and the False Positive Rate (FPR) are defined as follows:

$$TPR = \frac{TP}{TP + FN}$$

$$FPR = \frac{FP}{FP + TN}$$

In the keystroke-dynamics authentication literature, the True Positive Rate (TPR), also known as the «Hit Rate», indicates the frequency with which a detector correctly identifies an impostor. The «Miss Rate», defined as (1 – TPR), reflects the rate at which an impostor is mistakenly identified as a genuine user. The False Positive Rate (FPR), or «False-Alarm Rate» (FAR), denotes the frequency with which a genuine user is incorrectly rejected.

Given a constant set of the Hold and Keyup-Keydown features selected, the evaluation procedure described by Killourhy and Maxion (Killourhy & Maxion, 2010, p. 256-276) uses the first T training repetitions produced by a genuine-user subject S to train an anomaly-detection algorithm A. Here T can be 5, 50, 100 or 200 repetitions, S can be any of the subject identifiers specified in the data set, and A can be one of the mentioned algorithms. At the scoring stage, the genuine-user test data is composed of the subsequent 200 repetitions from (T + 1) to (T + 200). The «practiced» impostor test data consists of the last 5 password repetitions from each of the remaining 50 users, resulting in a total of 250 impostor timing vectors. As shown by the researchers, impostor practice represents a minor threat to the accuracy of keystroke-dynamics detectors but is still included in the current evaluation procedure to ensure realism.

The evaluation procedure for the sliding-window updating case is more complex. The concept involves sliding a window of size T over the genuine user's typing data, advancing the window in increments of 5 repetitions for computational efficiency. For each window, the detector is trained on the repetitions within that window and then tested using the next five repetitions. This process is repeated as the window is incremented. Since there are 200 repetitions of genuine-user test data, this results in 40 cycles of training and testing (200/5). The evaluation procedure is well-defined by the researchers (Killourhy & Maxion, 2010, p. 256-276) and is accurately reproduced in the current study, as shown in the following sections. According to their results, the use of updating is a highly influential factor.

Across the keystroke-dynamics authentication literature, such anomaly detectors performance measures as the Equal Error Rate (EER) and the Zero-Miss False Alarm Rate (ZMFAR) have been used. They both give an understanding of a detector's performance over a range of different treshold values. The EER is defined as the point at which the Miss Rate and the False-Alarm Rate are equal. At this point, the system's rate of incorrectly rejecting genuine users is equal to the rate

Table 1

Table of possible outcomes of an anomaly detector's work

Anomaly detection result	Anomaly is actually present (Impostor)	No anomaly is actually present (Genuine user)
Anomaly is detected	True Positive (TP)	False Positive (FP)
No anomaly is detected	False Negative (FN)	True Negative (TN)

of incorrectly accepting impostors. The EER provides a single value that reflects the overall accuracy of the system, with a lower EER indicating better performance. The ZMFAR is defined as the minimum False-Alarm Rate when the threshold is set to ensure the Miss Rate is zero. This metric reflects a detector's performance under the condition of zero tolerance for impostors involved in the performance evaluation.

A Receiver Operating Characteristic (ROC) curve is used to visualize a detector's performance across various threshold values. Figure 1 illustrates an example of a ROC curve for the «Outlier Count (z-score)» algorithm, trained on data from the subject «s010» (excluding Keydown-Keydown features, with a sliding window enabled, and a training set size of 15).

Intuitively, a larger area under the ROC curve indicates higher overall performance of an anomaly detector. While minor variations in the ratio of outcomes can significantly affect the ZMFAR value, EER is a more robust and balanced performance measure that represents the trade-off between false alarms and misses. Consequently, EER has been selected to compare the performance of detectors, as demonstrated in the following sections.

The anomaly-detection algorithms and the described evaluation procedure have been implemented using Python, NumPy, Pandas, and scikit-learn. These implementations have been shared on GitHub to support further research (Kaidalov, 2024).

Findings. Firstly, it was crucial to replicate the EER and ZMFAR values reported by Killourhy and Maxion from their initial comparison of anomaly detectors (Killourhy & Maxion, 2009, p. 125-134). The values reported by the researchers and those reproduced in the current study are presented in Table 2.

While most of the rates match with insignificant differences, there is an almost 2% difference in the

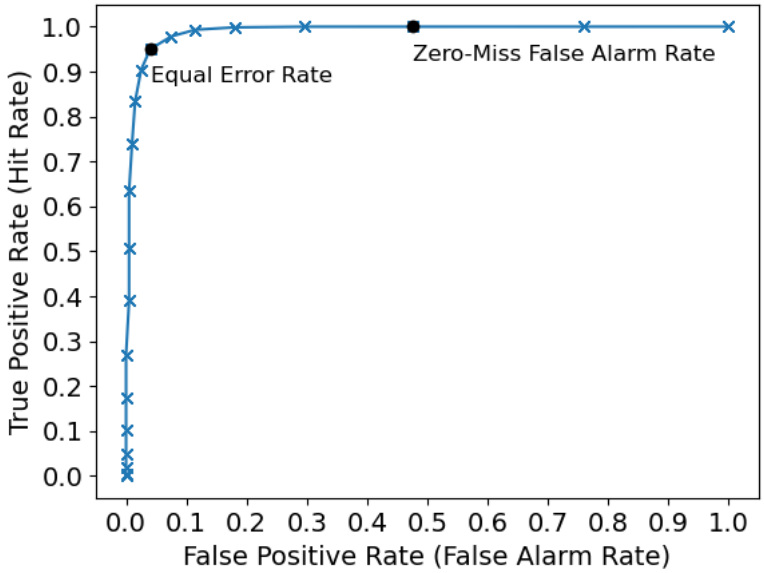


Fig. 1. An example ROC curve for the «Outlier Count (z-score)» algorithm

Table 2

Table of the EER and ZMFAR values reported in (Killourhy & Maxion, 2009, p. 125-134) and reproduced in the current study

Anomaly-detection algorithm	Average EER in (Killourhy & Maxion, 2009, p. 125-134)	Reproduced average EER	Average ZMFAR in (Killourhy & Maxion, 2009, p. 125-134)	Reproduced average ZMFAR
Manhattan (scaled)	0.096 (0.069)	0.098 (0.068)	0.601 (0.337)	0.610 (0.333)
Nearest Neighbour (Mahalanobis)	0.100 (0.064)	0.100 (0.063)	0.468 (0.272)	0.468 (0.270)
Outlier Count (z-score)	0.102 (0.077)	0.101 (0.076)	0.782 (0.306)	0.782 (0.303)
One-class SVM	0.102 (0.065)	0.119 (0.059)	0.504 (0.316)	0.500 (0.282)
Mahalanobis	0.110 (0.065)	0.110 (0.064)	0.482 (0.273)	0.482 (0.270)

EER for the one-class SVM algorithm. This discrepancy can be attributed to differences in implementations. Although the researchers specified the v parameter as 0.5, they did not indicate which kernel was used. In the current study, the default values of the scikit-learn package were used for the remaining parameters of OneClassSVM during evaluation.

The extended evaluation procedure published by Killorhy and Maxion (Killourhy & Maxion, 2010, p. 256-276) had introduced such parameters as sliding windows updates, training amount, impostors practice, and a feature set. The exact EER values for the 'Manhattan (scaled)' algorithm were reported as 7.1% for unpracticed impostors and 9.7% for practiced impostors. Sliding window updates were used, Keydown-Keyup features and Enter features were excluded, and the training amount was set to 100. The evaluation procedure reproduced in this study successfully replicates the EER values reported by the researchers.

The implemented anomaly detectors were evaluated with training set sizes ranging from 5 to 100, increasing by increments of 5 password repetitions. Given its significant impact, updating was enabled. The feature set included Hold and Keyup-Keydown features, as well as Enter key features. To ensure realism, impostor practice was enabled. The obtained EER values are presented in Table 3, and a visual comparison of EER values at different training set sizes is shown in Figure 2.

Figure 2 presents a line plot illustrating the Equal Error Rate (EER) of various anomaly detection algorithms as a function of training set size. The x-axis represents the training set size, ranging from 5 to 100, while the y-axis indicates the EER, ranging from 0 to 0.35.

The «Manhattan (scaled)» algorithm shows a gradual decline in EER as the training set size increases, indicating improved performance with more training data. In contrast, the «Outlier count (z-score)» algorithm initially decreases but then shows an increase in EER, suggesting possible overtraining as the model becomes too specialized to the training data and loses generalization capability.

The «Nearest Neighbour (Mahalanobis)» algorithm demonstrates only minor improvements over the Mahalanobis algorithm, despite requiring significantly higher computational resources. This suggests that the algorithm's additional complexity may not be justified given the marginal performance gains. The one-class SVM algorithm maintains a relatively constant high EER across all training set sizes.

Notably, the EER values for the «Manhattan (scaled)» and «Outlier count (z-score)» algorithms are relatively lower at smaller training set sizes,

Table 3

Table of EER values for each reproduced anomaly detector at training set sizes ranging from 5 to 100

Training set size	Manhattan (scaled)	Nearest Neighbour (Mahalanobis)	Outlier Count (z-score)	One-class SVM	Mahalanobis
5	0.135	0.302	0.100	0.282	0.287
10	0.117	0.267	0.093	0.269	0.263
15	0.110	0.228	0.092	0.262	0.227
20	0.109	0.237	0.095	0.257	0.236
25	0.106	0.209	0.099	0.254	0.210
30	0.105	0.173	0.100	0.251	0.173
35	0.104	0.160	0.101	0.248	0.159
40	0.102	0.152	0.101	0.242	0.152
45	0.099	0.143	0.100	0.236	0.143
50	0.097	0.136	0.100	0.232	0.136
55	0.095	0.130	0.099	0.229	0.131
60	0.094	0.125	0.101	0.229	0.128
65	0.093	0.123	0.102	0.223	0.125
70	0.093	0.123	0.102	0.222	0.126
75	0.093	0.122	0.103	0.222	0.126
80	0.093	0.120	0.103	0.220	0.125
85	0.093	0.118	0.103	0.217	0.124
90	0.093	0.118	0.104	0.215	0.123
95	0.092	0.115	0.102	0.212	0.121
100	0.091	0.114	0.103	0.209	0.119

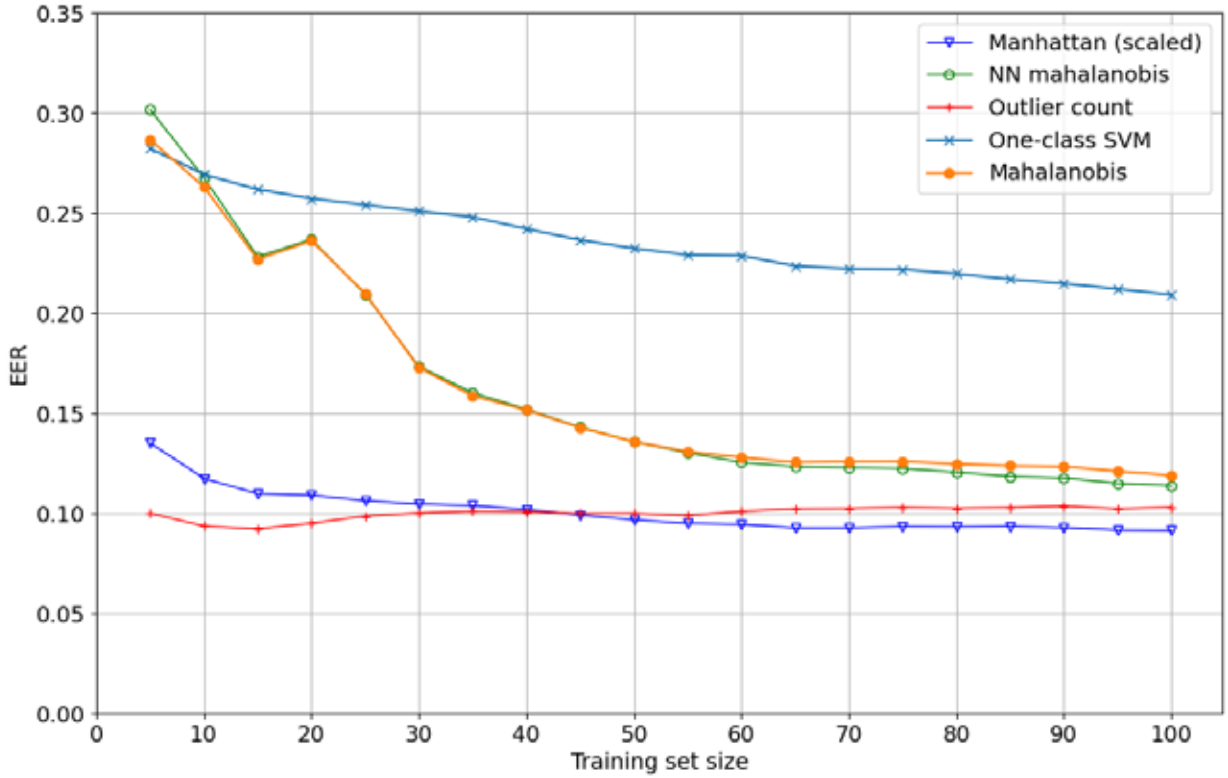


Fig. 2. The graph of the EER values for each reproduced anomaly detector at training set sizes ranging from 5 to 100

suggesting higher practical value when limited data is available.

Conclusion. This study has successfully replicated and extended the evaluation of anomaly detection algorithms applied to keystroke dynamics for two-factor authentication systems. By reproducing the performance metrics (EER and ZMFAR) for various algorithms as initially reported by Killourhy and Maxion, we have confirmed the reliability of their findings. Among the algorithms tested, the «Manhattan (scaled)» and «Outlier Count (z-score)» showed promising results, especially when using smaller training sets, which is critical for practical deployment.

One significant outcome of this research is the determination of the minimum number of password repetitions needed to achieve stable accuracy rates. This result is particularly valuable for reducing user effort in the training phase and optimizing computational resources during real-time authentication processes. The methodology and Python code made available further contribute to reproducibility, a key aspect of advancing research in keystroke dynamics.

Looking forward, several promising areas for future exploration have emerged. First, while the current study focused on a single password input, expanding the analysis to include more diverse passwords could improve the robustness of anomaly detection models. Second, exploring the integration of keystroke dynamics with other biometric factors, such as mouse dynamics or touchscreen patterns, could lead to the development of multimodal biometric systems, offering enhanced security and user experience. Additionally, improving the performance of machine learning algorithms, particularly through the use of deep learning models, might yield better generalization capabilities for unseen data.

Another avenue for future work includes investigating the potential for continuous authentication mechanisms. Rather than only verifying users at login, continuous authentication can monitor user behaviour throughout their session, providing an added layer of security. Lastly, optimizing the computational efficiency of the system remains a critical challenge, especially for real-time applications. Exploring lightweight models or optimizing feature extraction processes could help deploy keystroke-based authentication systems in resource-constrained environments.

In conclusion, the findings of this study contribute to the ongoing development of secure and user-friendly authentication systems. Future research should focus on extending the methods presented here and addressing the emerging challenges in keystroke dynamics and behavioural biometrics.

BIBLIOGRAPHY:

1. R. A. Maxion, K. S. Killourhy. Keystroke biometrics with number-pad input. 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN). 2010. P. 201–210. URL: https://doi.org/10.1109/DSN.2010.5544311 (date of access 19.09.2024)

2. R. Ryu, S. Yeom, S.-H. Kim, D. Herbert. Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. IEEE Access. Vol. 9. P. 34541–34557. 2021. URL: https://doi.org/10.1109/ACCESS.2021.3061589 (date of access 19.09.2024).

3. K. S. Killourhy, R. A. Maxion. Why Did My Detector Do *That*?! Recent Advances in Intrusion Detection. RAID 2010. Lecture Notes in Computer Science. 2010. Vol 6307. P. 256–276. URL: https://doi.org/10.1007/978-3-642-15512-3_14 (date of access 19.09.2024).

4. K. S. Killourhy, R. A. Maxion. Comparing anomaly-detection algorithms for keystroke dynamics. 2009 IEEE/IFIP International Conference on Dependable Systems & Networks. P. 125–134. URL: https://doi.org/10.1109/DSN.2009.5270346 (date of access 19.09.2024).

5. V. D. Kaidalov. GitHub – vkaidalov/keystroke-dynamics-authentication. GitHub. 2024. URL: https://github.com/vkaidalov/keystroke-dynamics-authentication (date of access: 19.09.2024).

REFERENCES:

1. Maxion, R. A., Killourhy, K. S. (2010). Keystroke biometrics with number-pad input. 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN). P. 201–210. Retrieved from: https://doi.org/10.1109/DSN.2010.5544311 (date of access 19.09.2024)

2. Ryu, R., Yeom, S., Kim, S. -H., Herbert, D. (2021). Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. IEEE Access. Vol. 9. P. 34541–34557. Retrieved from: https://doi.org/10.1109/ACCESS.2021.3061589 (date of access 19.09.2024).

3. Killourhy, K. S., Maxion, R. A. (2010). Why Did My Detector Do *That*?! Recent Advances in Intrusion Detection. RAID 2010. Lecture Notes in Computer Science. Vol 6307. P. 256–276. Retrieved from: https://doi.org/10.1007/978-3-642-15512-3_14 (date of access 19.09.2024).

4. Killourhy, K. S., Maxion, R. A. (2009). Comparing anomaly-detection algorithms for keystroke dynamics. 2009 IEEE/IFIP International Conference on Dependable Systems & Networks. P. 125–134. Retrieved from: https://doi.org/10.1109/DSN.2009.5270346 (date of access 19.09.2024).

5. Kaidalov, V. D. (2024) GitHub – vkaidalov/keystroke-dynamics-authentication. *GitHub*. Retrieved from: https://github.com/vkaidalov/keystroke-dynamics-authentication (date of access: 19.09.2024).

УДК 004.9
DOI https://doi.org/10.32782/IT/2024-3-6

Віта КАШТАН
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та комп'ютерної інженерії, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького 19, Дніпро, Україна, 49005
***ORCID:** 0000–0002–0395–5895*
***Scopus-AuthorID:** 57201902879*

Володимир ГНАТУШЕНКО
доктор технічних наук, професор, завідувач кафедри інформаційних технологій та комп'ютерної інженерії, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0003-3140-3788*
***Scopus Author ID:** 6505609275*

Іван ЛАКТІОНОВ
доктор технічних наук, доцент, професор кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0001-7857-6382*
***Scopus Author ID:** 57194557735*

Григорій ДЯЧЕНКО
кандидат технічних наук, доцент кафедри електропривода, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0001-9105-1951*
***Scopus Author ID:** 57201252081*

Бібліографічний опис статті: Каштан, В., Гнатушенко, В., Лактіонов, І., Дяченко, Г. (2024). Геоінформаційна технологія нейромережевої сегментації для картографування земного покриву. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 51–62, doi: https://doi.org/10.32782/IT/2024-3-6

ГЕОІНФОРМАЦІЙНА ТЕХНОЛОГІЯ НЕЙРОМЕРЕЖЕВОЇ СЕГМЕНТАЦІЇ ДЛЯ КАРТОГРАФУВАННЯ ЗЕМНОГО ПОКРИВУ

Актуальність розвитку сучасних технологій для сегментації земельного покриву зростає у зв'язку з підвищеними вимогами до точного моніторингу та управління земельними ресурсами, в тому числі, сільськогосподарського призначення. Традиційні методи сегментації часто не забезпечують достатню точність у класифікації складних класів, таких як сільськогосподарські культури, дерева, будівлі та дороги. ***Мета роботи*** *полягає в розробці геоінформаційної технології для виділення множинних ознак із супутникових знімків Sentinel-2 та їх використання для сегментації земного покриття за допомогою нейронної мережі ResNet.*

Методологія. *У цьому дослідженні використовуються знімки Sentinel-2 для аналізу земного покриття. Спочатку зображення проходять попередню обробку, яка включає атмосферну корекцію, геометричне та радіометричне калібрування. Потім дані нормалізуються для підвищення стабільності навчання нейронної мережі. На наступному етапі зображення обробляються для виділення спектральних, морфологічних і текстурних ознак, які є вхідними даними для моделі ResNet. Модель застосовує конволюційні шари і функцію активації ReLU для автоматичного виділення ознак. Для класифікації використовується повнозв'язний шар з функціями Softmax та Cross-Entropy. Після навчання модель класифікує кожен піксель, створюючи сегментоване зображення, яке відображає різні класи земного покриття, зокрема сільськогосподарські угіддя, будівлі, дерева та дороги.*

Наукова новизна *дослідження полягає в розробці новітньої методології обробки супутникових зображень Sentinel-2, що включає інтеграцію комплексної попередньої обробки, нормалізацію даних, мультимодальне виділення ознак та використання глибоких нейронних мереж для автоматичного виділення*

та класифікації ознак. Впровадження нових підходів до атмосферної, геометричної та радіометричної корекції, а також застосування ResNet з функціями активації ReLU та повнозв'язних шарів з функціями Softmax і Cross-Entropy, забезпечує підвищення точності класифікації та деталізації сегментації земного покриття.

Висновки. *Дослідження показало, що запропонована технологія забезпечує суттєве покращення точності і якості класифікації в порівнянні з традиційними методами, такими як IsoData, K-means, SVM, Minimum Distance, Maximum Likelihood та Parallelepiped. Результати демонструють, що технологія на основі ResNet досягає високої точності в сегментації основних класів земного покриву: сільськогосподарські культури, дерева, будівлі та дороги, що є важливим для ефективного моніторингу та управління земельними ресурсами.*

Ключові слова: *нейромережева сегментація, глибоке навчання, матриця неточностей, матриця помилок, оптичні супутникові знімки, модель ResNet.*

Vita KASHTAN
Candidate of Technical Science, Associate Professor, Associate Professor at the Information Technology and Computer Engineering Department, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, kashtan.v.yu@nmu.one
ORCID: *0000–0002–0395–5895*
Scopus-AuthorID: *57201902879*

Volodymyr HNATUSHENKO
Doctor of Technical Science, Professor, Head of the Information Technology and Computer Engineering Department, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, hnatushenko.v.v@nmu.one
ORCID: *0000-0003-3140-3788*
Scopus Author ID: *6505609275*

Ivan LAKTIONOV
Doctor of Technical Science, Associate Professor, Professor at the Department of Software Engineering, Dnipro University of Technology, 19, Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, laktionov.i.s@nmu.one
ORCID: *0000-0001-7857-6382*
Scopus Author ID: *57194557735*

Grygorii DIACHENKO
Ph.D, Associate Professor at the Department of Electric Drive, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, diachenko.g@nmu.one
ORCID: *0000-0001-9105-1951*
Scopus Author ID: *57201252081*

To cite this article: Kashtan, V., Hnatushenko, V., Laktionov, I., Diachenko, G. (2024). Heoinformatsiina tekhnolohiia neiromerezhevoi sehmentatsii dlia kartohrafuvannia zemnoho pokryvu [Geoinformation technology neural network segmentation for land cover mapping]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 51–62, doi: https://doi.org/10.32782/IT/2024-3-6

GEOINFORMATION TECHNOLOGY NEURAL NETWORK SEGMENTATION FOR LAND COVER MAPPING

The relevance of developing modern technologies for land cover segmentation is growing due to increased requirements for accurate monitoring and management of land resources including for agricultural purposes. Traditional segmentation methods often lack accuracy in classifying complex classes such as crops, trees, buildings, and roads. ***The work aims*** *to develop geographic information technology for extracting multiple features from Sentinel-2 satellite images and using them to segment the land cover using the ResNet neural network.*

Methodology. *This study uses Sentinel-2 images for land cover analysis. First, the images undergo pre-processing, which includes atmospheric correction and geometric and radiometric calibration. Then, data is normalized to improve the stability of the neural network training. At the next stage, the images are processed to extract spectral, morphological, and textural features, which are the input to the ResNet model. The model uses convolutional layers and the ReLU activation function to extract features automatically. A fully connected layer with Softmax and Cross-Entropy functions is used for classification. After training, the model classifies each pixel, creating a segmented image that shows different classes of land cover, including farmland, buildings, trees, and roads.*

The scientific novelty *of the research is the development of the latest methodology for processing Sentinel-2 satellite images, including integration of complex pre-processing, data normalization, multimodal feature extraction, and the use of deep neural networks for automatic feature extraction and classification. The new approaches to atmospheric, geometric, and radiometric correction, as well as the use of ResNet with ReLU activation and fully connected layers with Softmax and Cross-Entropy functions, improve the accuracy of classification and detail of land cover segmentation.*

Conclusions. *The study showed that the proposed technology provides a significant improvement in classification accuracy and quality compared to traditional methods such as IsoData, K-means, SVM, Minimum Distance, Maximum Likelihood, and Parallelepiped. The results demonstrate that the ResNet-based technology demonstrates high precision in segmenting the main land cover classes–crops, trees, buildings, and roads–which is crucial for effective land monitoring and management.*

Key words: *network segmentation, deep learning, confusion matrix, error matrix, optical satellite images, ResNet model.*

Вступ. Точне та своєчасне володіння інформацією про сільськогосподарські землі, зокрема за допомогою створення карт земного покриву, є надзвичайно важливим для розвитку сучасного сільського господарства. Визначення площі та територіальне розміщення посівів є важливим для отримання необхідної аграрної інформації (Solórzano J.V., 2021). Традиційні методи сегментації земного покриву за допомогою польових вимірювань, досліджень та статистичних аналізів потребують значних людських та фінансових ресурсів (Zhang H., 2021). Завдяки стрімкому розвитку технологій дистанційного зондування Землі (ДЗЗ), зокрема підвищенню просторової та часової роздільної здатності зображень, багатоспектральні дані дистанційного зондування стали широко застосовуватися в аграрних дослідженнях (Peng X., 2021). Багатоспектральні дані відіграють важливу роль у моніторингу стану посівів, оцінці врожайності сільськогосподарських культур та моніторингу шкідників (Lianze T., Vincent G.). Однак, незважаючи на значний прогрес у космічних технологіях та збільшення кількості датчиків супутників спостереження Землі, створення детальних карт ґрунтового покриву залишається складним, трудомістким та тривалим процесом (Rakhlin A., 2018). Карти земного покриву зазвичай мають обмежену часову роздільну здатність, що ускладнює постійний моніторинг змін. Наприклад, продукти наземного покриву EU Corine (Bossard M., 2000) доступні лише для певних років, а останні продукти Європейського космічного агентства (ESA) WorldCover (Zanaga D., 2021) охоплюють лише 2020 та 2021 роки. Отже, існує необхідність у створенні машинних моделей, які можуть точно створювати карти земного покриву на основі супутникових даних, що дозволить покращити моніторинг змін та управління сільськогосподарськими ресурсами.

Літературний огляд. Традиційні методи сегментації поділяються на два основні типи: некерована та керована класифікація (Makantasis K., 2015). Прикладом некерованої класифікації є методи, такі як K-середнє (K-means) та максимізація очікуваного значення (Expectation Maximization), які дозволяють створювати категорії для обробки даних, однак атрибути результатів класифікації залишаються невизначеними. Алгоритм IsoData, який є вдосконаленою версією K-means, дозволяє адаптивно змінювати кількість кластерів під час ітераційного процесу класифікації.

До методів керованої класифікації відносяться метод опорних векторів (SVM), дерева рішень, класифікація за максимальною правдоподібністю (MaximumLikelihood), метод мінімальної відстані (MinimumDistance) і паралелепіпедний метод (Parallelepiped). У цих методах параметри дискримінантної функції визначаються на основі відомих даних про елементи зображення. Після цього дискримінантна функція застосовується для класифікації невідомих елементів зображення, що забезпечує точність класифікації на основі навчальних даних.

Традиційні методи сегментації відзначаються високою повторюваністю та оперативністю порівняно з візуальною інтерпретацією даних. Але їх точність значно знижується при зміні даних або області дослідження (Xie C., 2022).

На відміну від класичних алгоритмів машинного навчання, глибинне навчання (ГН) демонструє унікальні переваги в класифікації зображень. Тоді як традиційні алгоритми машинного навчання вимагають ручної розробки ознак для завдань класифікації, глибинне навчання усуває необхідність у цьому; алгоритми на основі ГН автоматично навчаються і вилучають ознаки, що мають відношення до цільового завдання. Ця властивість автоматичного вилучення ознак забезпечує високу надійність моделей глибинного навчання та спрощує їх адаптацію до різних наборів даних (Kamilaris A., 2018). Крім того, алгоритми глибинного навчання можуть обробляти великі масиви даних, виявляючи

потенційні шаблони та закономірності, що сприяє підвищенню точності та ефективності класифікації земного покриву. Але незважаючи на переваги, які надає глибинне навчання, класифікація зображень у галузі дистанційного зондування часто обмежується через відсутність надійно маркованих наборів даних.

Один з найбільш досліджених і широко використовуваних наборів даних для класифікації зображень дистанційного зондування – це набір землекористування UC Merced (UCM), представлений в роботі (Yang Y., 2010). Набір даних містить 21 клас землекористування та земного покриву, з 100 зображеннями для кожного класу розміром 256x256 пікселів і з просторовою роздільною здатністю близько 30 см на піксель. Всі зображення мають колірний простір RGB і були отримані з колекції знімків міських територій Національної карти США, отриманих з літальних апаратів. Але, невелика кількість зображень на клас є значним обмеженням для використання цього набору даних у задачах класифікації.

Для покращення ситуації з набором даних, різні дослідження використовували комерційні зображення Google Earth для створення нових наборів даних (Zhao L., 2016). Наприклад, набори даних PatternNet (Zhou W., 2018) і NWPU-RESISC45 (Cheng G, 2017) базуються на зображеннях з дуже високою роздільною здатністю до 30 см на піксель. Однак, через складність і трудомісткість процесу створення маркованих наборів даних, ці набори даних також мають обмежену кількість зображень на клас, що варіюється від кількох сотень до кількох тисяч.

Одним з найбільших доступних наборів даних є набір аерофотознімків (Aerial Image Dataset, AID), який включає 30 класів, кожен з яких містить від 200 до 400 зображень розміром 600x600 пікселів, отриманих з Google Earth. Незважаючи на розширене покриття класів, використання комерційних і попередньо оброблених зображень обмежує їхню придатність для реальних програм спостереження Землі, таких як Sentinel-2.

Також, набір даних SAT-6, представлений в (Basu S., 2015) базується на аерофотознімках з просторовою роздільною здатністю 1 метр на піксель. Набір даних SAT-6 отримано з зображень Національної програми сільськогосподарських знімків (NAIP) і включає 6 класів: неродючі землі, дерева, луки, дороги, будівлі та водні об'єкти. Патчі зображень мають розмір 28x28 пікселів і представлені в червоному, зеленому, синьому та ближньому інфрачервоному діапазонах.

Порівняно з наборами даних, згаданими вище, розроблено новий набір даних, який використовує супутникові зображення з роздільною здатністю 10 метрів на піксель, що робить його більш відповідним для реальних програм спостереження Землі. Наш набір даних базується на знімках супутника Sentinel-2, що дозволяє включати значно більшу площу покриття.

Мета дослідження: розробка геоінформаційної технології для виділення множинних ознак із супутникових знімків Sentinel-2 та їх використання для сегментації земного покриття за допомогою нейронної мережі ResNet. Це дозволить підвищити точність та деталізацію класифікації різних типів земного покриття, таких як сільськогосподарські культури, дерева, об'єкти забудови та дороги, що в свою чергу сприяє поліпшенню моніторингу та управління земельними ресурсами.

Виклад основного матеріалу. У рамках дослідження було виконано наступні кроки: попередня обробка даних, вилучення спектральних, морфологічних і текстурних ознак з супутникових знімків, навчання глибокої нейронної мережі ResNet і сегментація зображень земного покриття. Алгоритм, що ілюструє роботу геоінформаційної технології, представлено на рисунку 1.

Знімки Sentinel-2 з 12 каналами після завантаження проходять етап попередньої обробки, який включає атмосферну корекцію, геометричне та радіометричне калібрування (Каштан В.Ю., 2024). Після цього дані приводяться до однакового масштабу для підвищення стабільності навчання нейронної мережі.

Наступним етапом є виділення множинних ознак: спектральних (містять інформацію про різні типи земного покриття), морфологічних (дозволяють виділяти структури та форми об'єктів на зображенні) та текстурних ознак (дозволяють визначати характеристики поверхні земного покриття), які служать вхідними даними для подальшої обробки в нейронній мережі. Це дозволяє моделі навчатися різноманітним зразкам, характерним для різних типів земного покриття. Ці етапи обробки виконуються як для попередньо оброблених, так і для первинних даних Sentinel-2.

Для навчання моделі підготовлено навчальні вибірки первинних даних супутника Sentinel-2 Дніпропетровщини до та після попередньої обробки. Вибірка містила класи: AnnualCrop (сільськогосподарські угіддя), Trees (дерева), Buildings (об'єкти забудови) та Roads (дороги). Кожне зображення мало розмір 64x64 пікселів,

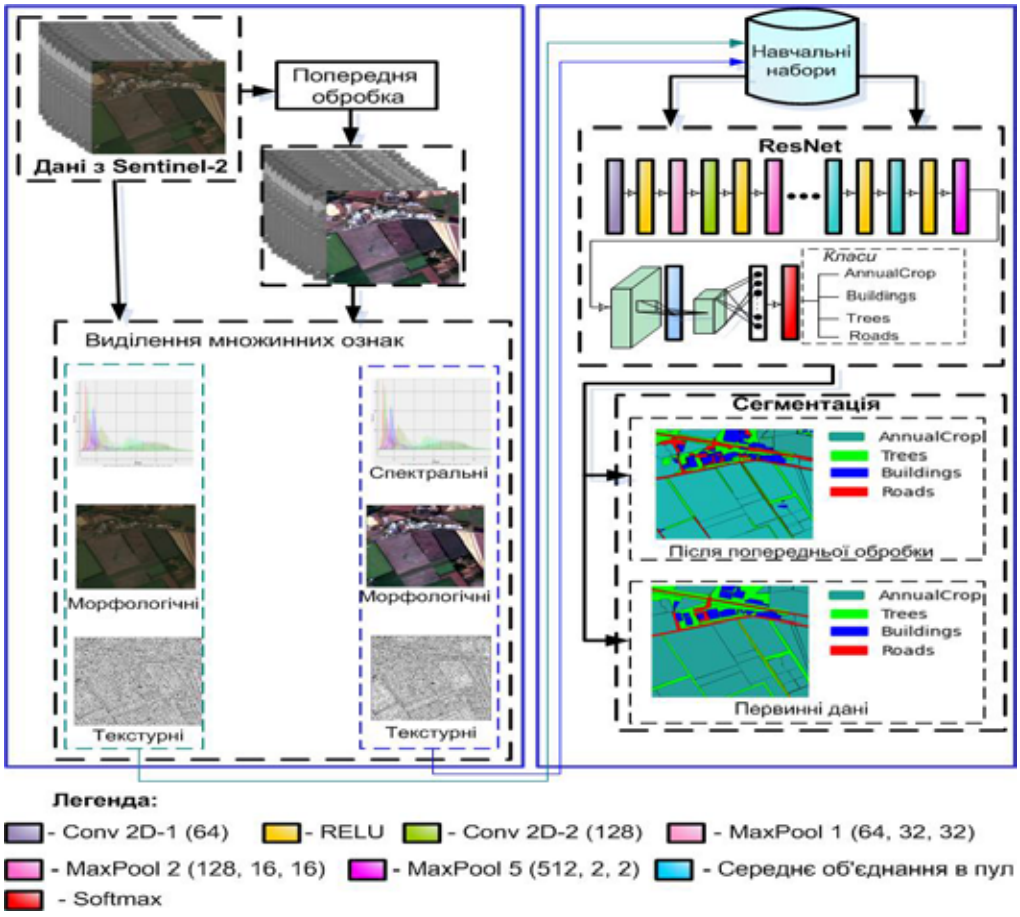


Рис. 1. Схема запропонованої геінформаційної технології

що дозволило забезпечити високу деталізацію та точність моделі.

Під час навчання виділені спектральні, морфологічні та текстурні ознаки подаються на вхід ResNet. Ця глибока нейронна мережа використовує послідовність конволюційних шарів для автоматичного виділення високорівневих ознак із вхідних зображень (Selmi L., 2022)

$$Y_{i,j} = \sum_{m-1}^{M} \sum_{n=1}^{N} x_{i+m-1,j+n-1} \cdot k_{m,n} \,, \qquad (1)$$

де *x* – вхідне зображення, *k* – ядро конволюції, *y* – вихідне зображення.

Функція активації ReLU:

$$f(x)=max(0,x) \qquad (2)$$

На етапі класифікації виділені ознаки подаються на вхід повнозв'язного шару нейронної мережі. Повнозв'язний шар, або fully connected layer, здійснює кінцеву класифікацію на основі отриманих ознак, що дозволяє визначити належність кожного пікселя до одного з чотирьох класів: сільськогосподарські угіддя (AnnualCrop), будівлі (Buildings), дерева (Trees) та дороги (Roads). Функція втрат для класифікації (Softmax та Cross-Entropy) (Selmi L., 2022):

$$Soft\max(z_i) = \frac{e^{zi}}{\sum_j e^{zi}} \qquad (3)$$

$$Cross - EntropyLoss = -\sum_{i \in C} y_i \log(\hat{y}_i) \,, \qquad (4)$$

де y_i – істинна ймовірність класу, $\hat{y}_i$ – передбачена ймовірність класу; *C* – множина всіх класів.

Адаптивне середнє пудлінгування (Selmi L., 2022):

$$y_{i,j} = \frac{1}{|R|} \sum_{(m,n) \in P} x_{m,n} \,, \qquad (5)$$

де $y_{i,j}$ – значення пікселя у вихідному зображенні після пулінгування; *R* – область усереднення, тобто область вхідного зображення, значення пікселів якої усереднюються; $|R|$ – кількість елементів (пікселів) в області *R*; $x_{m,n}$ – значення пікселя у вхідному зображенні.

Модель навчається на підготовлених вибірках, оптимізуючи параметри за допомогою зворотного поширення помилки. Це дозволяє моделі адаптуватися до різноманітних варіацій

у даних та забезпечувати точну класифікацію типів земного покриття.

На основі результатів класифікації створюється сегментоване зображення, де кожному пікселю присвоюється клас. Це дозволяє візуально відобразити результати аналізу супутникових даних та забезпечити точну сегментацію земного покриття.

Експерименти. В роботі використано супутникові знімки Sentinel-2 Дніпропетровщини (рис. 2). На рисунку 3 наведено результати сегментації земного покриву, отримані за допомогою розробленої технології.

За результатами візуального аналізу можна зробити висновок, що класифікація земного покриву після попередньої обробки знімка та застосування нейронної мережі ResNet є значно чіткішою та точнішою у порівнянні з класифікацією на первинних даних супутникових знімків Sentinel-2.

У цьому дослідженні проведено порівняння різних методів сегментації, включаючи IsoData, K-means, SVM, Minimum Distance, Maximum Likelihood, Parallelepiped і запропонований метод на основі нейронної мережі. На рисунку 4 наведено результат сегментації класичними методами (IsoData, K-means, SVM, Minimum Distance, Maximum Likelihood, Parallelepiped) та запропонований метод (рис. 3 г) на основі нейронної мережі ResNet.

Результати. За результатами візуального аналізу, метод IsoData (рис. 4а) показує здатність розпізнавати основні ділянки з культурами та деревами. Але, значні труднощі виникають при сегментації будівель та доріг, що призводить до змішування класів та знижує загальну точність методу. Метод K-means (рис. 4б) демонструє дещо вищу точність порівняно з IsoData. Культури та дерева класифікуються успішніше, але проблеми з розрізненням будівель та доріг все ще залишаються. Деякі області будівель і доріг змішані з іншими класами, що впливає на точність сегментації. Метод SVM (рис. 4в) демонструє вищу точність сегментації культур та дерев в порівнянні з IsoData та K-means. Метод Minimum-Distance (рис. 4г) демонструє нижчу точність порівняно з методами IsoData, K-means та SVM. Великі області пікселів були помилково класифіковані, особливо у класі доріг, що робить цей метод менш ефективним для задач сегментації. Метод Maximum-Likelihood (рис. 4ґ) показує кращі результати, ніж Minimum Distance, але все ще виникають значні проблеми з сегментацією доріг. Культури та дерева класифікуються успішно, а будівлі – з певними труднощами. Метод Parallelepiped (рис. 4д) стикається з значними труднощами при класифікації всіх класів. Велика частина пікселів була помилково класифікована, що знижує загальну ефективність методу. Запропонована технологія (рис. 3г) демонструє значно кращі результати порівняно з класичними підходами. Класи такі, як дерева, дороги, будівлі та культури, були чітко ідентифіковані, що свідчить про ефективність методів сегментації для супутникових знімків Sentinel-2.

а) б)

Рис. 2. Супутникові знімки космічного апарату Sentinel-2 синтезовані у R-G-B канали: а) первинний; б) після попередньої обробки

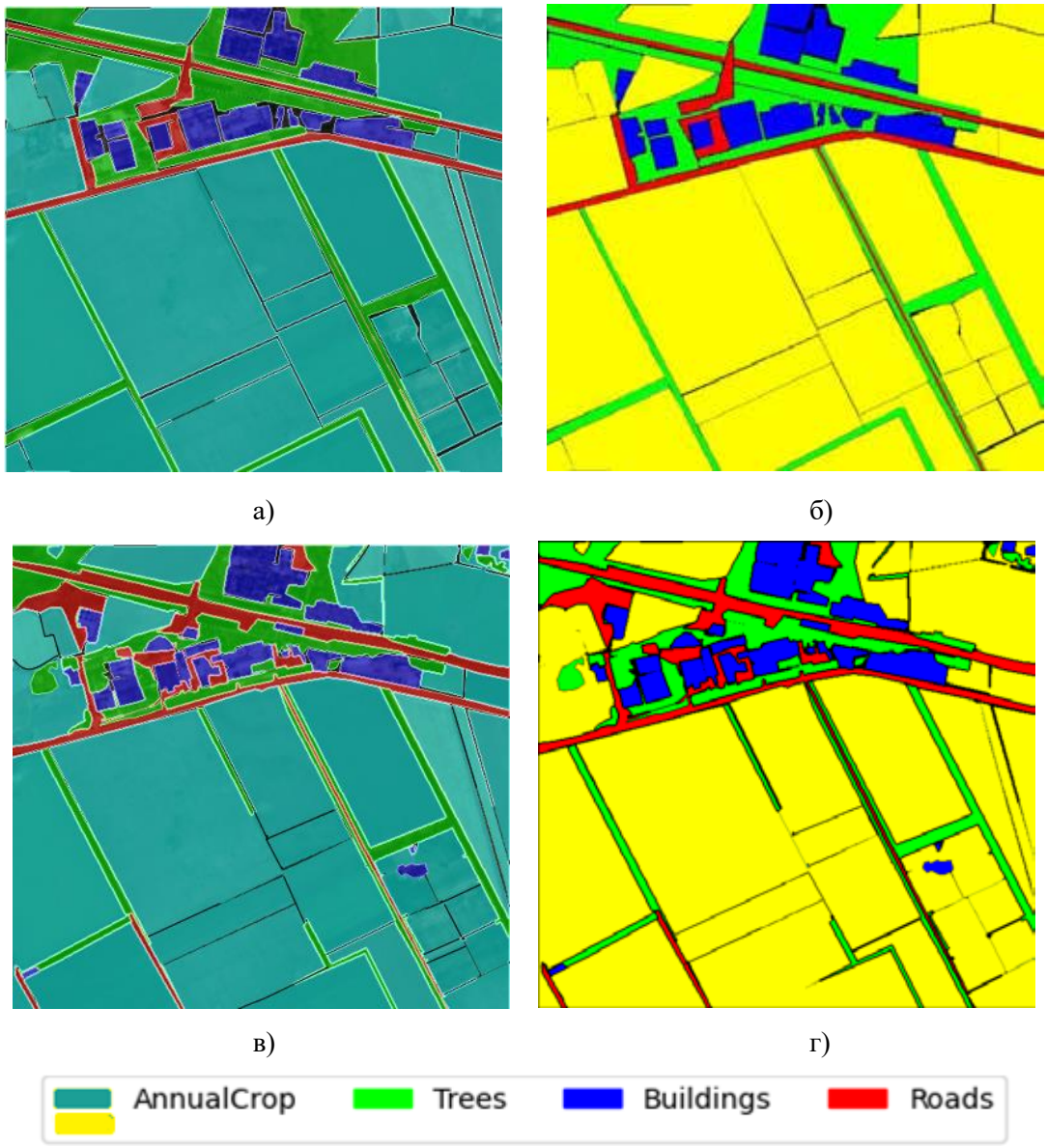


Рис. 3. Результати сегментації земного покриву за даними Sentinel-2: а) первинний знімок; б) тематична карта для первинного знімку; в) знімок після обробки; г) тематична карта для знімку після застосування запропонованої технології

На рисунку 5 представлено графіки динаміки зміни втрат (Loss) та точності (Accuracy) для тренувального і тестового наборів даних протягом 30 епох навчання нейронної мережі. Значне зниження втрат під час навчання (рис. 5а) спостерігається вже на перших епохах. З 0.5 на початку, втрати швидко зменшуються до приблизно 0.15 вже на 5-й епосі. Потім зниження продовжується повільнішими темпами, досягаючи 0.008 до кінця 30 епохи. Це свідчить про те, що модель добре навчається на навчальних даних. Точність під час навчання (рис. 5б) значно збільшується з 88% до приблизно 94% вже на перших епохах. Потім зростання продовжується більш поступово, досягаючи близько 99.9% до кінця 30-ї епохи. Це демонструє, що модель успішно навчається на навчальних даних і здатна досягти високої точності.

Для кількісного аналізу побудовано матрицю невідповідностей (confusion matrix) (Rakhlin A., 2018), яка дозволила оцінити точність класифікації пікселів за чотирма класами: AnnualCrop, Trees, Buildings, і Roads (рис. 6). Матриця невідповідностей дозволяють детально оцінити точність сегментації різними методами. Для методу IsoData (рис. 6а) спостерігаються значні помилки при класифікації доріг (Roads), де більшість пікселів (74223) були неправильно класифіковані як AnnualCrop. Це свідчить про низьку точність для класу доріг (Roads). Метод K-means (рис. 6б) також показав помилки при класифікації доріг, але краща

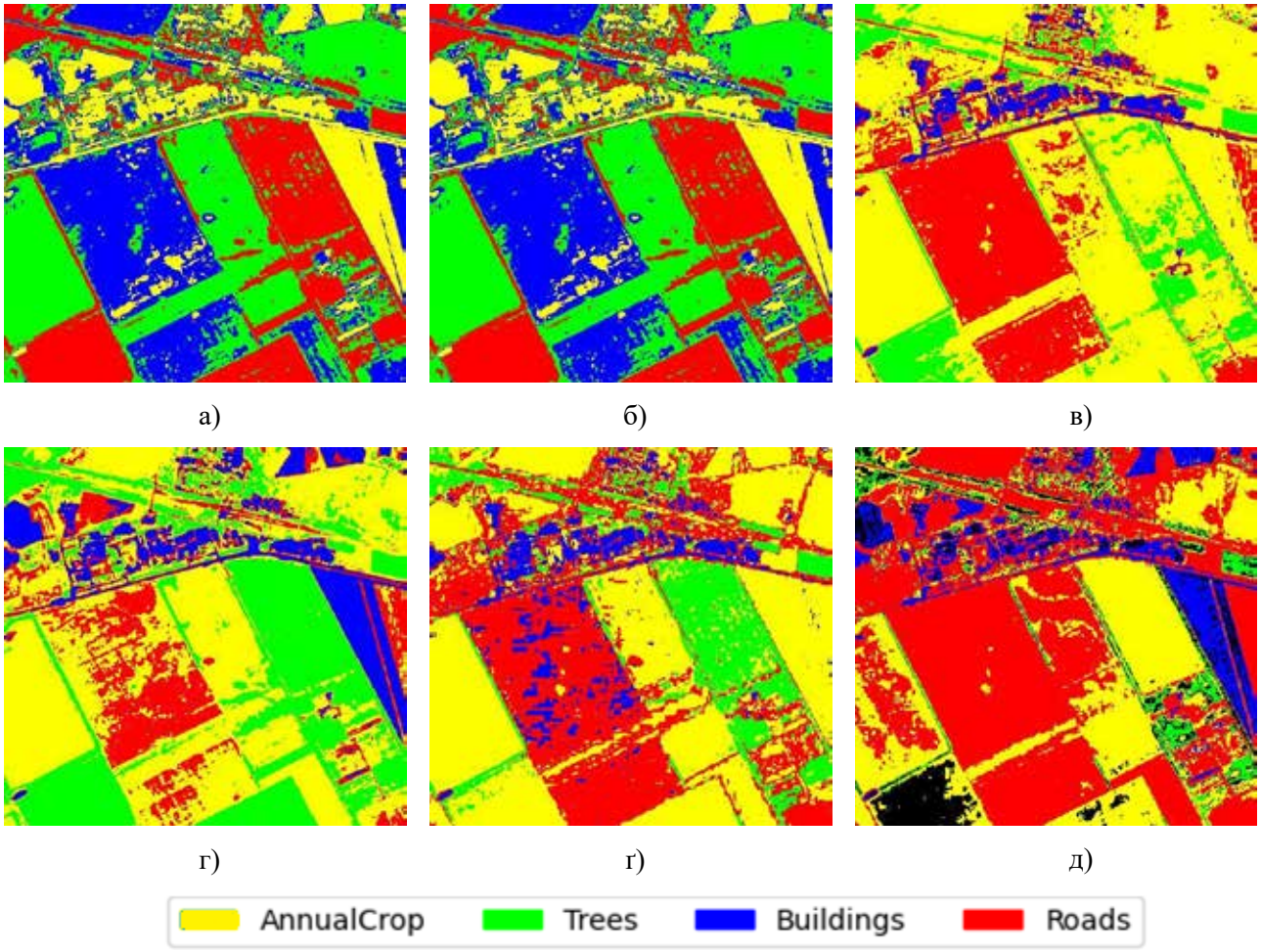


Рис. 4. Сегментація земного покриву для Sentinel-2: а) IsoData; б) K-means; в) SVM; г) Minimum Distance; ґ) Maximum Likelihod; д) Parallelepiped

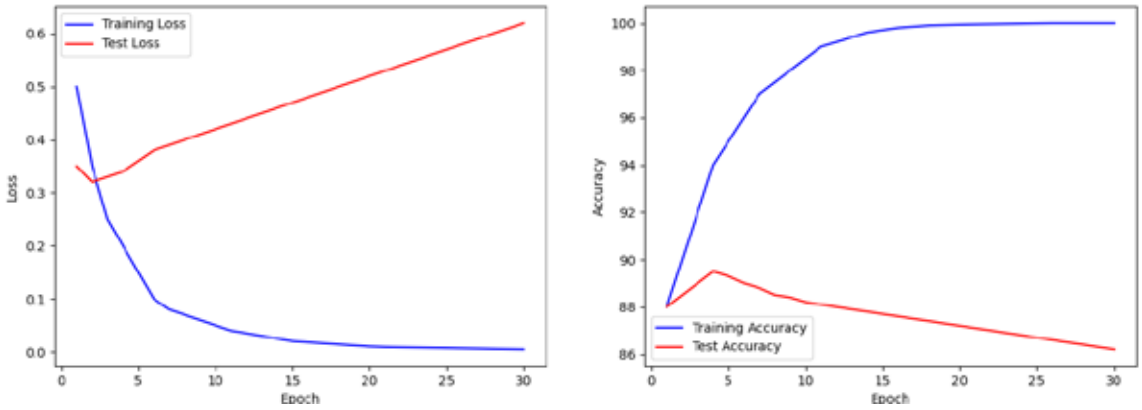
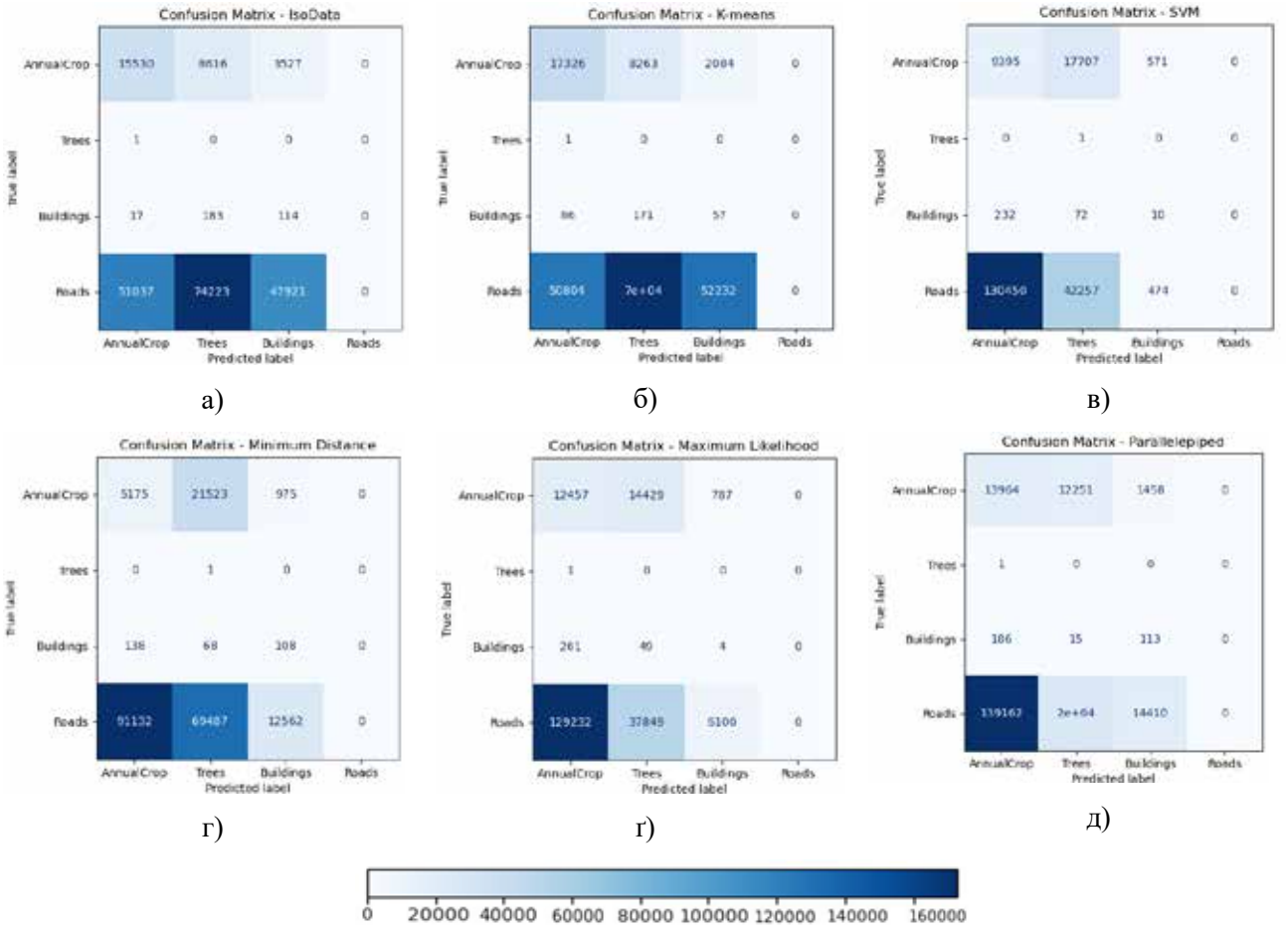


Рис. 5. Графік динаміки зміни втрат та точності: а) тренувального набору; б) тестового набору

точність у порівнянні з методом IsoData. SVM (рис. 6в) має найбільше помилок при класифікації доріг, але суттєво менше помилок для інших класів в порівнянні з методами K-means та IsoData. Метод Minimum Distance (рис. 6г) показав вищу точність при класифікації будівель (Buildings) і дерев (Trees), але все ще мав значні помилки при класифікації доріг (69487 пікселів).

Для методу Maximum Likelihood (рис. 6ґ) спостерігається вища точність при класифікації доріг (37849 пікселів) у порівнянні з методами IsoData, K-means, SVM та Minimum Distance, але все ще залишається значна кількість



а) б) в)

г) ґ) д)

Рис. 6. Матриця невідповідностей для: а) IsoData; б) K-means; в) SVM; г) Minimum Distance; ґ) Maximum Likelihod; д) Parallelepiped

помилок при класифікації інших класів. Метод Parallelepiped (рис. 6д) показує найгірші результати серед класичних методів, з найбільшими помилками для всіх класів, зокрема для доріг (19609 пікселів). Запропонована технологія на основі нейронної мережі (рис. 7а) продемонструвала найкращі результати з мінімальними помилками для всіх класів. Всі пікселі були правильно класифіковані (AnnualCrop: 25831, Trees: 1, Buildings: 314, Roads: 172964), що вказує на високу точність технології.

Аналіз матриць помилок дозволяє виявити, які класи були неправильно класифіковані і в які інші класи вони були помилково віднесені (рис. 8). Метод IsoData (рис. 8а) показав значні помилки, зокрема для класу доріг (74223 пікселів), які були неправильно класифіковані як AnnualCrop. Метод K-means (рис. 8б) демонструє помилки, схожі на ті, що спостерігаються у методі IsoData, але з дещо покращеною точністю; кількість помилок для класифікації доріг становила 70145 пікселів. Метод SVM (рис. 8в) має найбільші помилки для класу доріг (130450 пікселів), але значно покращив точність для інших класів.

Minimum Distance (рис. 8г) демонструє кращі результати для класифікації будівель (68 пікселів) і дерев (0 пікселів), але зберігаються значні помилки для класу доріг (69487 пікселів). Метод Maximum Likelihood (рис. 8ґ) має кращі результати для класифікації доріг порівняно з іншими методами, але все ще спостерігається значна кількість помилок, зокрема для класу дерев (Trees). Метод Parallelepiped (рис. 8д) відзначився найбільшими помилками серед усіх методів, зокрема для класифікації доріг, де було виявлено 19609 помилкових пікселів. Запропонована технологія на основі нейронної мережі (рис. 7б) продемонструвала найкращі результати з мінімальними помилками для всіх класів. Це вказує на високу точність і ефективність у порівнянні з класичними методами.

Висновки. Розроблено геоінформаційну технологію нейромережевої сегментації для картографування земного покриву. В роботі досліджено класи земного покриву, зокрема сільськогосподарські культури (AnnualCrop), дерева (Trees), будівлі (Buildings) та дороги (Roads). Для реалізації технології було

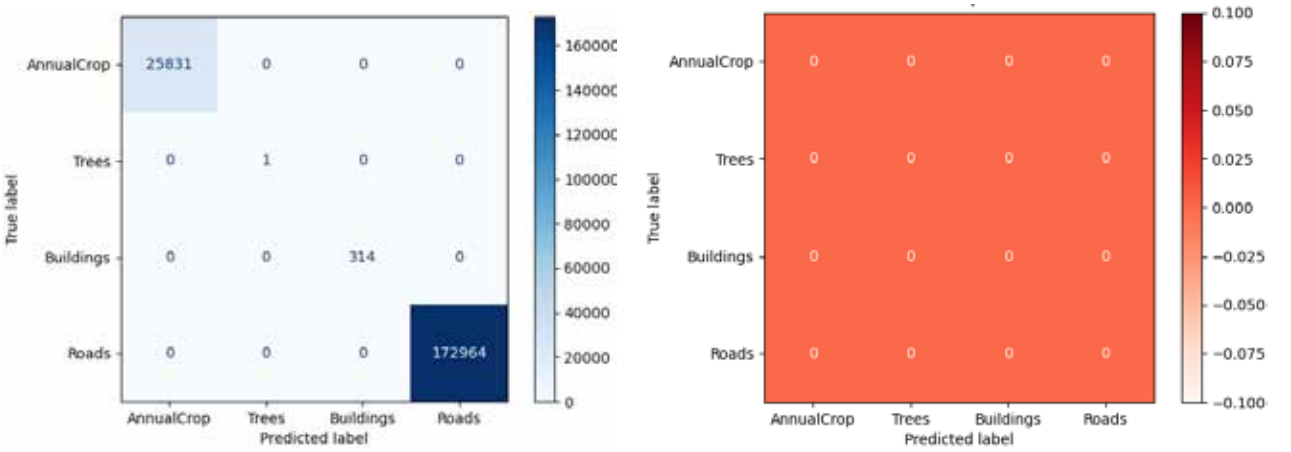
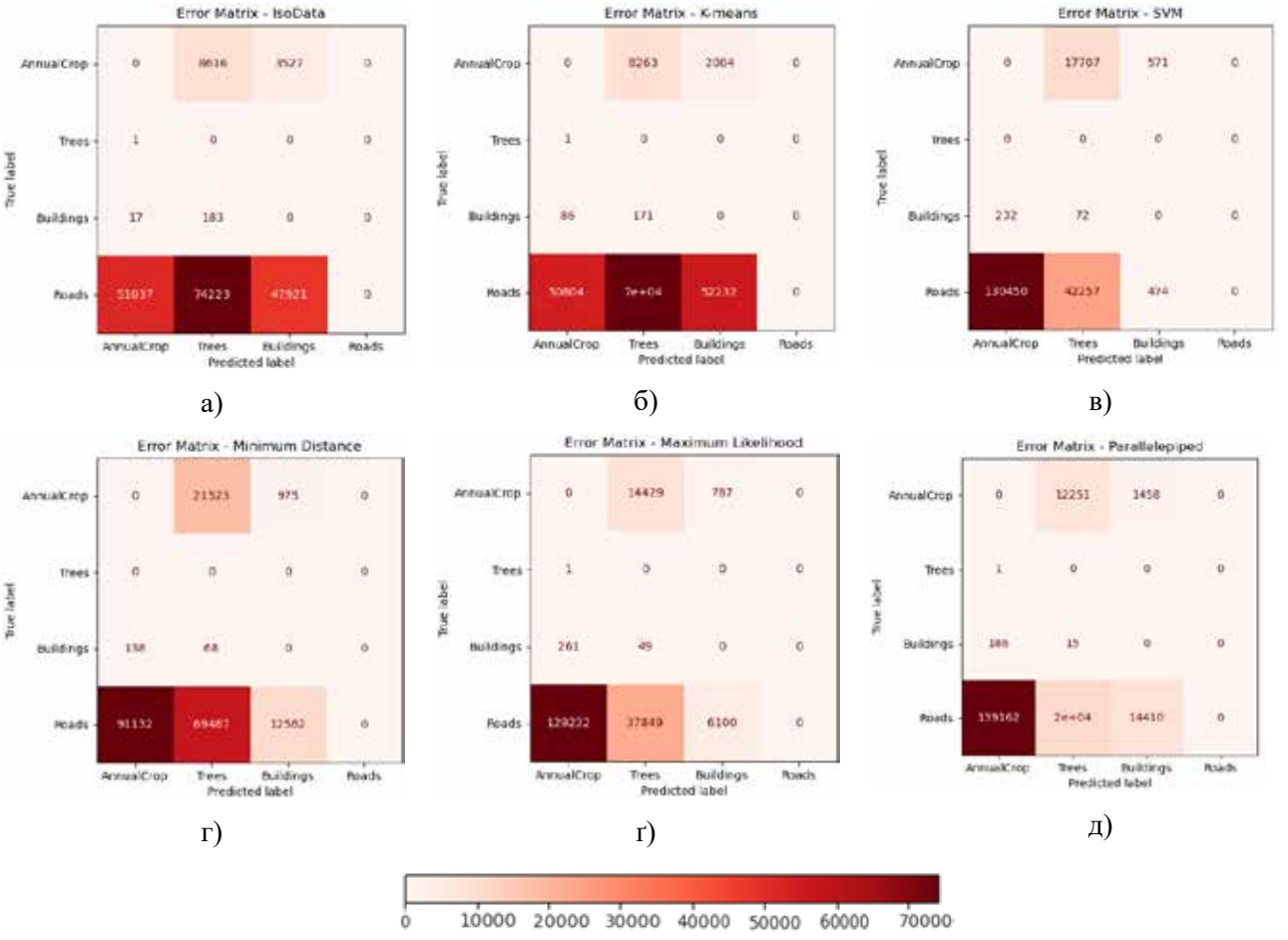


Рис. 7. Кількісні показники запропонованої технології: а) матриця невідповідностей; б) матриця помилок



а) б) в) г) ґ) д)

Рис. 8. Матриця помилок для: а) IsoData; б) K-means; в) SVM; г) Minimum Distance; ґ) Maximum Likelihod; д) Parallelepiped

використано модель ResNet, яка була навчена на даних супутника Sentinel-2 для Дніпропетровщини, що включають ці класи, з метою забезпечення точності їх класифікації.

Дослідження показало, що технологія на основі нейронної мережі ResNet значно перевищує традиційні методи сегментації за точністю та якістю класифікації. Традиційні методи, такі як IsoData, K-means, SVM, Minimum Distance, Maximum Likelihood та Parallelepiped мають суттєві обмеження, зокрема при сегментації доріг,

сільськогосподарських культур, що підтверджено аналізом матриць невідповідностей і помилок.

Якість та точність сегментації значно залежать як від первинних даних, так і від їх попередньої обробки. Попередня обробка даних, включаючи атмосферну корекцію, геометричне та радіометричне калібрування, а також нормалізація масштабів, має важливе значення для досягнення високої точності сегментації. Запропонована технологія демонструє високий рівень точності та ефективності у сегментації всіх класів земного покриву: сільськогосподарські культури (25831 піксель), дерева (1 піксель), будівлі (314 пікселів), дороги (172964 пікселі). Це свідчить про високу точність і ефективність сегментації.

Таким чином, використання моделі ResNet в поєднанні з виконаною попередньою обробкою первинних даних оптичного супутника Sentinel-2 демонструє суттєве покращення результатів сегментації зображень, підтверджуючи переваги сучасних нейронних мереж у порівнянні з традиційними методами.

Дослідження статті виконані в рамках науково-дослідної теми «Розвиток програмно-апаратного забезпечення інтелектуальних технологій для сталого вирощування сільськогосподарських культур у воєнний та повоєнний час» (номер держреєстрації 0124U000289).

ЛІТЕРАТУРА:

1. Solórzano J. V., Mas J. F., Gao Y., Gallardo-Cruz J. A. Land Use Land Cover Classification with U-Net: Advantages of Combining Sentinel-1 and Sentinel-2 Imagery. Remote Sens. 2021, 13, 3600

2. Zhang H., Wang L., Tian T., Yin J. A Review of Unmanned Aerial Vehicle Low-Altitude Remote Sensing (UAV-LARS) Use in Agricultural Monitoring in China. Remote Sens. 2021, 13, 1221.

3. Peng X., Han W., Ao J., Wang Y. Assimilation of LAI Derived from UAV Multispectral Data into the SAFY Model to Estimate Maize Yield. Remote Sens. 2021, 13, 1094.

4. Lianze T., Yong L., Hongji Z., Sijia L. Summary of UAV Remote Sensing Application Research in Agricultural Monitoring. Sci. Technol. Inf. 2018, 16, 122–124.

5. Vincent G., Antin C., Laurans M., Heurtebize J., Durrieu S., Lavalley C., Dauzat J. Mapping plant area index of tropical evergreen forest by airborne laser scanning. A cross-validation study using LAI2200 optical sensor. Remote. Sens. Environ. 2017, 198, 254–266.

6. Rakhlin A., Davydow A., Nikolenko S. Land cover classification from satellite imagery with u-net and lovász-softmax loss. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, Salt Lake City, UT, USA, 18–22 June 2018, 262–266.

7. Bossard M., Feranec J., Otahel J. CORINE Land Cover Technical Guide: Addendum; European Environment Agency: Copenhagen, Denmark, 2000; Volume 40.

8. Zanaga D., Van De Kerchove R., De Keersmaecker W., Souverijns N., Brockmann C., Quast R., Wevers J., Grosu A., Paccini A., Vergnaud S., et al. ESA WorldCover 10 m 2020 v100; OpenAIRE: Los Angeles, CA, USA, 2021.

9. Makantasis K., Karantzalos K., Doulamis A., Doulamis N. Deep supervised learning for hyperspectral data classification through convolutional neural networks. In Proceedings of the 2015 IEEE International Geoscience and Remote Sensing Symposium (IGARSS), Milan, Italy, 2015, 4959–4962

10. Xie C., Zhu H., Fei Y. Deep coordinate attention network for single image super-resolution. IET Image Process. 2022, 16, 273–284.

11. Kamilaris A., Prenafeta-Boldú F.X. Deep learning in agriculture: A survey. Comput. Electron. Agric. 2018, 147, 70–90.

12. Yang Y., Newsam S. Bag-of-visual-words and spatial extensions for land-use classification. In Proceedings of the 18th SIGSPATIAL international conference on advances in geographic information systems, ACM, 2010, 270–279.

13. Zhao L., Tang P., Huo L. Feature significance-based multibag-ofvisual-words model for remote sensing image scene classification. Journal of Applied Remote Sensing, 10(3):035004–035004, 2016.

14. Zhou W., Newsam S., Li C., Shao Z. Patternnet: a benchmark dataset for performance evaluation of remote sensing image retrieval. ISPRS Journal of Photogrammetry and Remote Sensing, 2018.

15. Cheng G., Han J.i, and Lu X. Remote sensing image scene classification: benchmark and state of the art. Proceedings of the IEEE, 105(10):1865–1883, 2017.

16. Basu S., Ganguly S., Mukhopadhyay S., DiBiano R., Karki M., Nemani R. Deepsat: a learning framework for satellite imagery. In Proceedings of the 23rd SIGSPATIAL International Conference on Advances in Geographic Information Systems, ACM, 2015, 37.

17. Каштан В. Ю., Шевцова О. С. Інформаційна технологія попередньої обробки супутникових зображень з використанням згорткової нейронної мережі. *Системні технології. Регіональний міжвузівський збірник наукових робіт*. – Випуск 1 (150). Дніпро, 2024. С. 36–50. DOI: 10.34185/1562-9945-1-150-2024-04.

18. Selmi L. Land Use and Land Cover Classification using a ResNet Deep Learning Architecture, 2022.

REFERENCES:

1. Solórzano, J. V., Mas, J. F., Gao, Y., Gallardo-Cruz, J. A. (2021). Land Use Land Cover Classification with U-Net: Advantages of Combining Sentinel-1 and Sentinel-2 Imagery. *Remote Sens*, *13*, 3600

2. Zhang, H., Wang, L., Tian, T., Yin, J. (2021). A Review of Unmanned Aerial Vehicle Low-Altitude Remote Sensing (UAV-LARS) Use in Agricultural Monitoring in China. *Remote Sens*, 13, 1221.

3. Peng, X., Han, W., Ao, J., Wang, Y. (2021). Assimilation of LAI Derived from UAV Multispectral Data into the SAFY Model to Estimate Maize Yield. *Remote Sens*, 13, 1094.

4. Lianze, T., Yong, L., Hongji, Z., Sijia, L. (2018). Summary of UAV Remote Sensing Application Research in Agricultural Monitoring. *Sci. Techno*l, 16, 122–124.

5. Vincent, G., Antin, C., Laurans, M., Heurtebize, J., Durrieu, S., Lavalley, C., Dauzat, J. (2017). Mapping plant area index of tropical evergreen forest by airborne laser scanning. A cross-validation study using LAI2200 optical sensor. *Remote. Sens. Environ*, 198, 254–266.

6. Rakhlin, A., Davydow, A., Nikolenko, S. (2018). Land cover classification from satellite imagery with u-net and lovász-softmax loss. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, Salt Lake City, UT, USA, 262–266.

7. Bossard, M., Feranec, J., Otahel, J. (2000). CORINE Land Cover Technical Guide: Addendum; European Environment Agency: Copenhagen, Denmark, Volume 40.

8. Zanaga, D., Van De Kerchove, R., De Keersmaecker, W., Souverijns, N., Brockmann, C., Quast, R., Wevers, J., Grosu, A., Paccini, A., Vergnaud, S., et al. (2021). ESA WorldCover 10 m 2020 v100; OpenAIRE: Los Angeles, CA, USA.

9. Makantasis, K., Karantzalos, K., Doulamis, A., Doulamis, N. (2015). Deep supervised learning for hyperspectral data classification through convolutional neural networks. In Proceedings of the 2015 IEEE International Geoscience and Remote Sensing Symposium (IGARSS), Milan, Italy, 4959–4962

10. Xie, C., Zhu, H., Fei, Y. (2022). Deep coordinate attention network for single image super-resolution. *IET Image Process*, 16, 273–284.

11. Kamilaris, A., Prenafeta-Boldú, F. X. (2018). Deep learning in agriculture: A survey. *Comput. Electron. Agric*, 147, 70–90.

12. Yang, Y., Newsam, S. (2010). Bag-of-visual-words and spatial extensions for land-use classification. In Proceedings of the 18th SIGSPATIAL international conference on advances in geographic information systems, ACM, 270–279.

13. Zhao, L., Tang, P., Huo, L. (2016). Feature significance-based multibag-ofvisual-words model for remote sensing image scene classification. *Journal of Applied Remote Sensing*, 10(3):035004–035004.

14. Zhou, W., Newsam, S., Li, C., Shao, Z. (2018). Patternnet: a benchmark dataset for performance evaluation of remote sensing image retrieval. *ISPRS Journal of Photogrammetry and Remote Sensing*.

15. Cheng, G., Han, J. i, & Lu, X. (2017). Remote sensing image scene classification: benchmark and state of the art. Proceedings of the IEEE, 105(10):1865–1883.

16. Basu, S., Ganguly, S., Mukhopadhyay, S., DiBiano, R., Karki, M., Nemani, R. (2015). Deepsat: a learning framework for satellite imagery. In Proceedings of the 23rd SIGSPATIAL International Conference on Advances in Geographic Information Systems, ACM, 37.

17. Kashtan, V. Yu., Shevtsova, O. S. (2024). Informatsiina tekhnolohiia poperednoi obrobky suputnykovykh zobrazhen z vykorystanniam zghortkovoi neironnoi merezhi. Systemni tekhnolohii. *Rehionalnyi mizhvuzivskyi zbirnyk naukovykh robit. – Vypusk* 1 (150),.36 – 50. DOI: 10.34185/1562-9945-1-150-2024-04. [in Ukrainian].

18. Selmi, L. (2022). Land Use and Land Cover Classification using a ResNet Deep Learning Architecture.

УДК 004.8
DOI https://doi.org/10.32782/IT/2024-3-7

Олег КОБИЛІН
кандидат технічних наук, доцент, завідувач кафедри інформатики, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0000-0003-0834-0475*

Ірина ВЕЧІРСЬКА
кандидат технічних наук, доцент кафедри інформатики, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0000-0001-7964-2361*

Анатолій АФАНАСЬЄВ
аспірант кафедри інформатики, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0009-0005-0707-981X*

Бібліографічний опис статті: Кобилін, О., Вечірська, І., Афанасьєв, А. (2024). Аналіз існуючих моделей глибинного навчання в задачах обробки природної мови. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 63–76, doi: https://doi.org/10.32782/IT/2024-3-7

АНАЛІЗ ІСНУЮЧИХ МОДЕЛЕЙ ГЛИБИННОГО НАВЧАННЯ В ЗАДАЧАХ ОБРОБКИ ПРИРОДНОЇ МОВИ

Обробка природної мови (NLP) є однією з найактуальніших галузей штучного інтелекту, що охоплює широкий спектр завдань, таких як аналіз емоцій, машинний переклад, розпізнавання мовлення та інші.

***Мета роботи:** Метою цього дослідження є всебічний аналіз продуктивності моделей глибинного навчання, включаючи рекурентні нейронні мережі (RNN), мережі довготривалої короткочасної пам'яті (LSTM) та керовані рекурентні блоки (GRU), у задачах NLP. Особлива увага приділяється ефективності цих моделей у завданнях аналізу емоцій.*

***Методологія:** Дослідження включає кілька етапів: збір та попередню обробку даних, реалізацію та навчання моделей RNN, LSTM і GRU на вибраних наборах даних, оцінку їхньої продуктивності за допомогою таких показників, як точність, пригадування та F1-score, а також аналіз ресурсних вимог моделей, особливо в умовах обмежених обчислювальних ресурсів. Крім того, у роботі проводиться порівняльний аналіз моделей за показниками їхньої масштабованості при роботі з великими обсягами даних.*

***Наукова новизна:** Дане дослідження пропонує детальний порівняльний аналіз ефективності RNN, LSTM та GRU в різних задачах NLP, з акцентом на їхній здатності обробляти послідовні дані та враховувати довготривалі залежності. Проведений аналіз виявляє, яка з моделей є найбільш ефективною в конкретних умовах, залежно від доступних ресурсів і специфіки даних.*

***Висновки:** В результаті дослідження було встановлено, що GRU показала найвищу продуктивність в аналізі емоцій, перевершуючи RNN і LSTM за точністю, пригадуванням і F1-score. LSTM виявилася оптимальною для роботи з великими обсягами даних, демонструючи високу ефективність і точність. RNN, хоча і забезпечує швидке навчання на невеликих наборах даних, поступається іншим моделям у точності, що робить її менш придатною для складних задач NLP. Отримані результати містять цінну інформацію для дослідників і практиків, які займаються застосуванням моделей глибинного навчання у задачах NLP.*

***Ключові слова:** глибинне навчання, рекурентні нейронні мережі, LSTM, GRU, обробка природної мови, аналіз емоцій.*

Oleg KOBYLIN
Ph.D., Associate Professor, Head of the Department of Informatics, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, oleg.kobylin@nure.ua
***ORCID:** 0000-0003-0834-0475*

Iryna VECHIRSKA
Ph.D., Associate Professor at the Department of Informatics, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, iryna.vechirska@nure.ua
***ORCID:** 0000-0001-7964-2361*

Anatolii AFANASIEV
Postgraduate Student at the Department of Informatics, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, anatolii.afanasiev@nure.ua
***ORCID:** 0009-0005-0707-981X*

To cite this article: Kobylin, O., Vechirska, I., Afanasiev, A. (2024). Analiz isnuiuchykh modelei hlybynnoho navchannia v zadachakh obrobky pryrodnoi movy [Analysis of existing deep learning models in natural language processing tasks]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 63–76, doi: https://doi.org/10.32782/IT/2024-3-7

ANALYSIS OF EXISTING DEEP LEARNING MODELS IN NATURAL LANGUAGE PROCESSING TASKS

Natural language processing (NLP) is one of the most relevant branches of artificial intelligence, covering a wide range of tasks such as emotion analysis, machine translation, speech recognition and others.

***Purpose of work:** The purpose of this study is to comprehensively analyze the performance of deep learning models, including recurrent neural networks (RNN), long-short-term memory (LSTM) networks, and guided recurrent units (GRU), in NLP tasks. Special attention is paid to the effectiveness of these models in emotion analysis tasks.*

***Methodology:** The study includes several steps: data collection and pre-processing, implementation and training of RNN, LSTM and GRU models on selected data sets, evaluation of their performance using indicators such as precision, recall and F1-score, and analysis of the resource requirements of the models, especially in conditions of limited computing resources. In addition, the paper provides a comparative analysis of models based on their scalability when working with large volumes of data.*

***Scientific novelty:** This study offers a detailed comparative analysis of the performance of RNNs, LSTMs, and GRUs in various NLP tasks, with an emphasis on their ability to process sequential data and account for long-term dependencies. The conducted analysis reveals which of the models is the most effective in specific conditions, depending on the available resources and the specifics of the data.*

***Conclusions:** As a result of the study, it was found that GRU showed the highest performance in emotion analysis, outperforming RNN and LSTM in terms of precision, recall and F1-score. LSTM proved to be optimal for working with large volumes of data, demonstrating high efficiency and accuracy. RNN, although it provides fast training on small data sets, is inferior to other models in accuracy, which makes it less suitable for complex NLP tasks. The obtained results contain valuable information for researchers and practitioners who are engaged in the application of deep learning models in NLP tasks.*

***Key words:** deep learning, recurrent neural networks, LSTM, GRU, natural language processing, sentiment analysis.*

Актуальність проблеми. Обробка природної мови (NLP) стала ключовою галуззю штучного інтелекту, яка кардинально змінила взаємодію комп'ютерів з людською мовою. Вибух нових застосувань, таких як текстові генератори та інтелектуальні чат-боти, демонструє значний вплив NLP на різні сфери. Значні успіхи в цій галузі стали можливими завдяки моделям глибинного навчання, які ефективно вирішують складні лінгвістичні завдання (DeepLearning. AI, н.д.). Це дослідження зосереджене на аналізі ключових моделей глибинного навчання, зокрема RNN, LSTM та GRU, які широко застосовуються в NLP.

Аналіз останніх досліджень і публікацій. Зростання значення NLP у повсякденному житті відображається в його використанні в таких галузях, як роздрібна торгівля, медицина та віртуальні асистенти. Програми, такі як чат-боти, інструменти перекладу та системи аналізу настроїв, демонструють універсальність NLP. Розмовні агенти на кшталт Alexa і Siri стають більш досконалими, а моделі, як GPT-3, вражають здатністю генерувати зв'язний текст. Google використовує NLP для покращення пошукової видачі, а соціальні мережі – для виявлення та фільтрації мови ворожнечі (James et al., 2013).

Моделі глибинного навчання здобули популярність завдяки здатності розпізнавати складні закономірності в лінгвістичних даних (Afanasieva et al., 2019). Це дослідження аналізує ефективність моделей RNN, LSTM і GRU у вирішенні різних задач NLP, таких як аналіз емоцій, машинний переклад, розпізнавання іменованих сутностей, виявлення спаму, генерація тексту та інші.

Незважаючи на значні досягнення, NLP ще стикається з такими проблемами, як упередженість моделей, незв'язність відповідей та періодична нестабільність поведінки. Це дослідження прагне оцінити сильні та слабкі сторони моделей глибинного навчання в завданнях NLP, надаючи цінну інформацію для дослідників і практиків (DeepLearning.AI, н.д.).

Мета дослідження. Мета цього дослідження полягає у всебічному та систематичному аналізі моделей глибинного навчання в галузі обробки природної мови. Досліджуються такі моделі, як рекурентні нейронні мережі, мережі довготривалої короткочасної пам'яті та керовані рекурентні блоки. Основна мета полягає в оцінці продуктивності цих моделей у різних задачах NLP, виявленні їхніх сильних і слабких сторін, а також аналізі нюансів у їхній продуктивності.

Цілі дослідження включають оцінку ефективності кожної моделі в задачах NLP, зокрема в аналізі емоцій, а також вивчення вимог до обчислювальних ресурсів кожної моделі з акцентом на масштабованість та ефективність. Це дозволить отримати уявлення про можливість їх практичної реалізації та виявити потенційні обмеження (Golian et al., 2022).

Методологія дослідження складається зі збору та попередньої обробки даних, реалізації та навчання моделей, використання показників ефективності для аналізу отриманих результатів та формулювання висновків.

Виклад основного матеріалу дослідження.

Рекурентні нейронні мережі (RNN) здатні ефективно обробляти послідовності різної довжини та моделювати часові залежності завдяки спільним параметрам, що дозволяє зменшити розмір моделі. Однак вони мають недоліки, такі як інтенсивність обчислень, складнощі з навчанням через проблему зникаючого градієнта та труднощі з обробкою довгих послідовностей.

Мережі довготривалої короткочасної пам'яті (LSTM) – це тип архітектури рекурентної нейронної мережі, розроблений для подолання проблем вивчення довготривалих залежностей у послідовних даних. У сфері обробки природної мови LSTM довела свою ефективність для таких завдань, як аналіз настроїв, переклад мови та розпізнавання емоцій (Nama, 2020).

LSTM добре підходять для задач, таких як аналіз настроїв, переклад мови та розпізнавання емоцій. Мережі LSTM ефективно моделюють довготривалі залежності, демонструють стійкість до зашумлених даних і мають високу гнучкість у застосуванні. Проте вони характеризуються обчислювальною складністю, схильністю до перенавчання, складністю налаштування гіперпараметрів і високими вимогами до обсягу даних.

Керований рекурентний блок (GRU). Керований рекурентний блок – це тип архітектури рекурентної нейронної мережі, призначений для послідовної обробки даних (Nama, 2020). GRU є спрощеною версією LSTM з меншою кількістю параметрів, що робить їх обчислювально ефективнішими та легшими у навчанні. GRU використовують вентильні механізми для вибіркового оновлення прихованого стану, що дозволяє їм моделювати залежності в послідовних даних, але вони можуть бути менш ефективними для дуже довготривалих залежностей.

Мережі GRU мають меншу обчислювальну складність, ефективно моделюють довготривалі залежності та швидше навчаються. Однак вони можуть бути менш ефективними для дуже довготривалих залежностей, схильні до перенавчання та потребують ретельного налаштування гіперпараметрів.

Отримані результати (експериментальне підтвердження). Для експериментів було обрано набір даних розпізнавання емоцій «Emotion Dataset for Emotion Recognition Tasks» з відкритих джерел (Pandey, н.д.). Цей набір даних містить англомовні повідомлення з Twitter та використовується для завдань розпізнавання емоцій. Він включає повідомлення, що виражають чотири різних емоцій: гнів, страх, радість, та сум. На табліці 1 наведені атрибути набору даних.

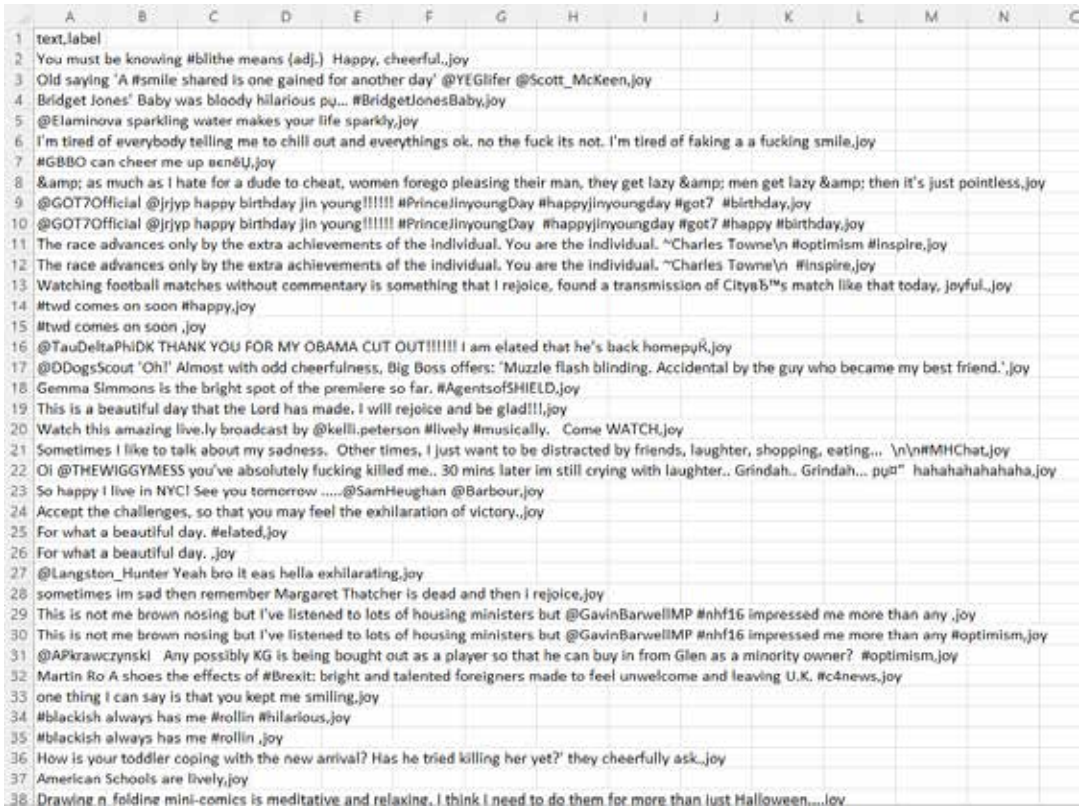
На рисунку 1 зображена частина даних (всього 3142) набору даних «Emotion Dataset for Emotion Recognition Tasks».

Експеримент 1 – Аналіз емоцій. Мета експерименту: аналіз емоцій забезпечує можливість виявлення та розпізнавання емоцій, виражених у текстових повідомленнях, що має значення в ряді сфер.

Таблиця 1

Атрибути набору даних

Атрибут	Опис
text (текст)	Текстова ознака, що містить повідомлення з Twitter. Це основний текст, який містить інформацію для аналізу емоцій.
label (мітка)	Класифікаційна мітка, що вказує на емоційний стан повідомлення. Має чотири можливих значень: – 0: гнів; – 1: страх; – 2: радість; – 3: сум.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	C
1	text,label														
2	You must be knowing #blithe means (adj.) Happy, cheerful.,joy														
3	Old saying 'A #smile shared is one gained for another day' @YEGlifer @Scott_McKeen,joy														
4	Bridget Jones' Baby was bloody hilarious рџ... #BridgetJonesBaby,joy														
5	@Elaminova sparkling water makes your life sparkly,joy														
6	I'm tired of everybody telling me to chill out and everythings ok. no the fuck its not. I'm tired of faking a a fucking smile,joy														
7	#GBBO can cheer me up вспёЏ,joy														
8	& as much as I hate for a dude to cheat, women forego pleasing their man, they get lazy & men get lazy & then it's just pointless,joy														
9	@GOT7Official @jrjyp happy birthday jin young!!!!!! #PrinceJinyoungDay #happyjinyoungday #got7 #birthday,joy														
10	@GOT7Official @jrjyp happy birthday jin young!!!!!! #PrinceJinyoungDay #happyjinyoungday #got7 #happy #birthday,joy														
11	The race advances only by the extra achievements of the individual. You are the individual. ~Charles Towne\n #optimism #inspire,joy														
12	The race advances only by the extra achievements of the individual. You are the individual. ~Charles Towne\n #inspire,joy														
13	Watching football matches without commentary is something that I rejoice, found a transmission of CityвЂ™s match like that today, joyful.,joy														
14	#twd comes on soon #happy,joy														
15	#twd comes on soon ,joy														
16	@TauDeltaPhiDK THANK YOU FOR MY OBAMA CUT OUT!!!!!! I am elated that he's back homepуЙ,joy														
17	@DDogsScout 'Oh!' Almost with odd cheerfulness, Big Boss offers: 'Muzzle flash blinding. Accidental by the guy who became my best friend.',joy														
18	Gemma Simmons is the bright spot of the premiere so far. #AgentsofSHIELD,joy														
19	This is a beautiful day that the Lord has made. I will rejoice and be glad!!!,joy														
20	Watch this amazing live.ly broadcast by @kelli.peterson #lively #musically. Come WATCH,joy														
21	Sometimes I like to talk about my sadness. Other times, I just want to be distracted by friends, laughter, shopping, eating... \n\n#MHChat,joy														
22	Oi @THEWIGGYMESS you've absolutely fucking killed me.. 30 mins later im still crying with laughter.. Grindah.. Grindah... рџ" hahahahahahaha,joy														
23	So happy I live in NYC! See you tomorrow .....@SamHeughan @Barbour,joy														
24	Accept the challenges, so that you may feel the exhilaration of victory.,joy														
25	For what a beautiful day. #elated,joy														
26	For what a beautiful day. ,joy														
27	@Langston_Hunter Yeah bro it eas hella exhilarating,joy														
28	sometimes im sad then remember Margaret Thatcher is dead and then i rejoice,joy														
29	This is not me brown nosing but I've listened to lots of housing ministers but @GavinBarwellMP #nhf16 impressed me more than any ,joy														
30	This is not me brown nosing but I've listened to lots of housing ministers but @GavinBarwellMP #nhf16 impressed me more than any #optimism,joy														
31	@APkrawczynski Any possibly KG is being bought out as a player so that he can buy in from Glen as a minority owner? #optimism,joy														
32	Martin Ro A shoes the effects of #Brexit: bright and talented foreigners made to feel unwelcome and leaving U.K. #c4news,joy														
33	one thing I can say is that you kept me smiling,joy														
34	#blackish always has me #rollin #hilarious,joy														
35	#blackish always has me #rollin ,joy														
36	How is your toddler coping with the new arrival? Has he tried killing her yet?' they cheerfully ask.,joy														
37	American Schools are lively,joy														
38	Drawing n foldine mini-comics is meditative and relaxing. I think I need to do them for more than just Halloween....joy														

Рис. 1. Фрагмент набору даних «Emotion Dataset for Emotion Recognition Tasks»

Методика експерименту: використання алгоритмів машинного навчання для побудови моделей, які можуть автоматично класифікувати текст за емоційними категоріями.

Метрики: accuracy (точність) визначає, наскільки точно модель класифікує емоції; precision вимірює, яку частку емоцій модель класифікує правильно відносно загальної кількості визначених моделлю емоцій; recall (пригадування) показує, яку частку емоцій модель виявляє відносно загальної кількості існуючих емоцій; F1-score (F1-оцінка) – комбінація точності та пригадування, що надає комплексну оцінку продуктивності моделі.

Експеримент з аналізу емоцій дозволяє створити та вдосконалювати моделі для виявлення емоцій у тексті, що має широкий спектр застосувань від соціальних мереж до різних галузей досліджень (Afanasieva et al., 2023).

Для написання коду для експериментів було використано мову програмування Python, бібліотеки та Jupyter Notebook для візуалізації результатів.

Рекурентні нейронні мережі (RNN). На першому етапі експерименту було завантажено набір даних із файлу ‘emotion-labels-test.csv’ за допомогою бібліотеки Pandas. Вхідні дані було розділено на текстові описи (X) та відповідні мітки класів (y). Для перетворення категоріальних емоційних міток у числовий формат було застосовано метод Label Encoding. Після цього дані було поділено на тренувальний і тестовий набори для забезпечення коректної оцінки продуктивності моделі.

Далі було здійснено токенізацію текстових даних та додано «padding», щоб усі послідовності мали однакову довжину. Для побудови моделі RNN було використано Embedding-шар, SimpleRNN-шар та Dense-шар. Як функцію втрат було обрано бінарну крос-ентропію, а для оцінки точності моделі – відповідну метрику.

Після тренування модель RNN використовувалася для прогнозування емоцій на тестовому наборі даних. Для оцінки ефективності моделі було розраховано такі показники, як точність (accuracy), точність класифікації (precision), пригадування (recall) та F1-оцінка (F1-score), що дало змогу здійснити комплексний аналіз продуктивності моделі задачі в аналізу емоцій.

Результати виконання експерименту (рис. 2-4) свідчать про те, що модель RNN неефективно справляється із завданням аналізу емоцій.

Проаналізуємо основні метрики. Точність моделі є надзвичайно низькою, становлячи приблизно 22%, що вказує на неефективність моделі у розрізненні різних категорій емоцій. Це може свідчити про упередженість моделі, яка

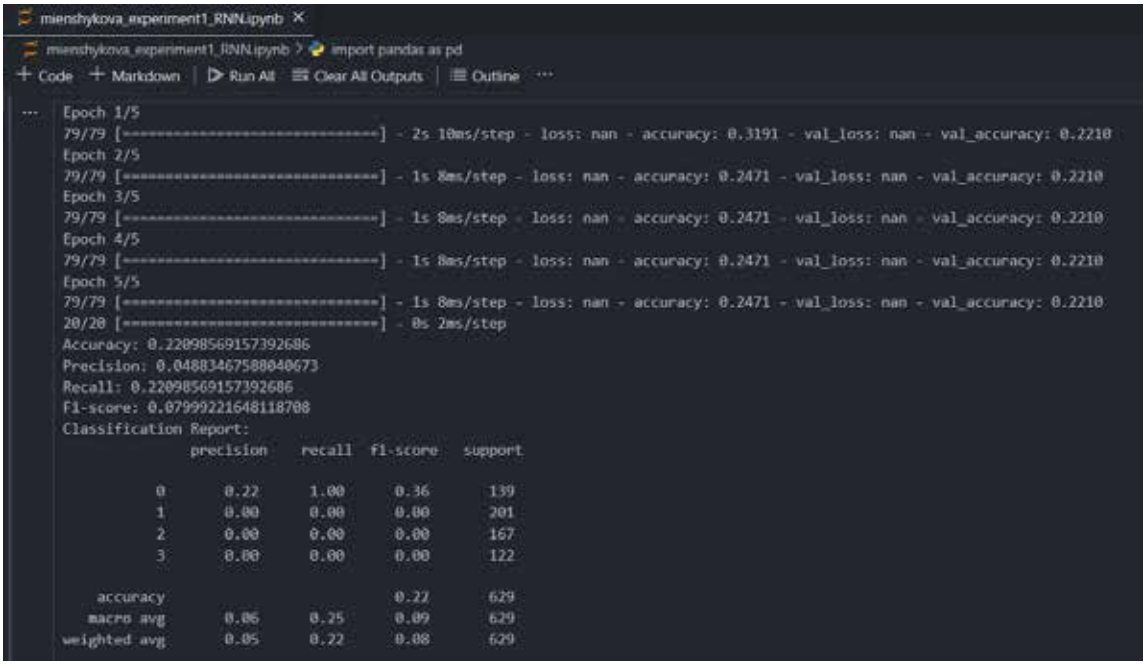


Рис. 2. Результати продуктивності моделі RNN на тестовому наборі даних

Рис. 3. Матриця плутанини для моделі RNN на тестовому наборі даних

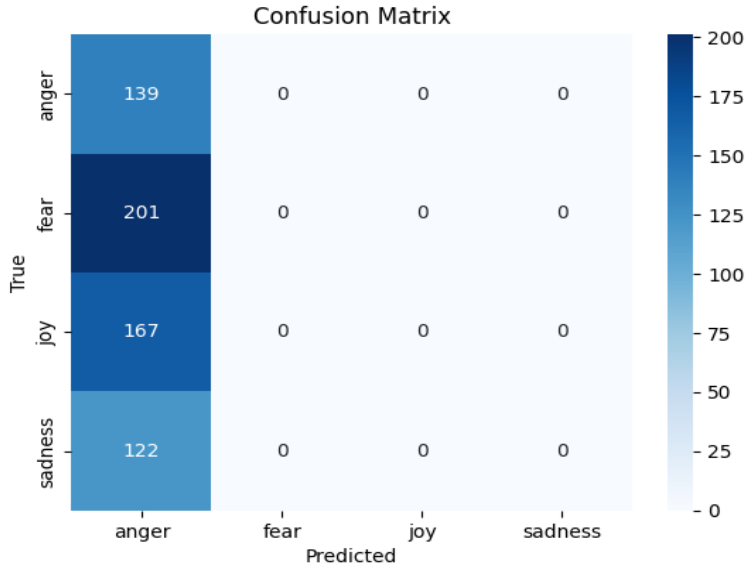


Рис. 4. Графік зміни втрат і точності моделі RNN під час навчання

схильна відносити більшість прикладів до певного класу.

Точність, пригадування та оцінка F1 для кожної категорії емоцій (0, 1, 2, 3) також виявилися дуже низькими, часто близькими до нуля. Це свідчить про те, що модель не здатна коректно ідентифікувати екземпляри кожного класу емоцій, що підтверджується низьким показником пригадування, який вказує на значну кількість пропущених істинно позитивних прикладів.

Матриця плутанини підтверджує низьку продуктивність моделі, демонструючи, що більшість прикладів прогнозуються як такі, що належать до класу 0. Такий дисбаланс у прогнозах призводить до низьких показників точності, пригадування та F1-оцінки для інших класів.

Зокрема, низька точність вказує на те, що коли модель прогнозує екземпляр як позитивний, це часто виявляється невірним. Низьке пригадування свідчить про те, що модель пропускає значну кількість реальних позитивних прикладів.

Мережі довготривалої короткочасної пам'яті (LSTM). Процес реалізації для моделі LSTM був аналогічний до процесу для RNN. Після завантаження та підготовки даних було створено модель LSTM, яка включала Embedding-шар, LSTM-шар та Dense-шар для багатокласової класифікації. Як функцію втрат використовували категоріальну крос-ентропію, а точність слугувала основною метрикою для оцінки продуктивності. Модель LSTM була використана для отримання прогнозів на тестовому наборі даних.

Результати виконання експерименту (рис. 5-7) показали значне покращення порівняно з попередньою моделлю, досягнувши точності приблизно 73,77%.

Проаналізуємо основні метрики. Модель продемонструвала загальну точність 73,77%, що вказує на її здатність коректно передбачати емоційні категорії.

Точність, пригадування та оцінка F1. Модель LSTM досягла високих показників точності, пригадування та F1-оцінки для класів 1 і 2, що свідчить про її ефективність у класифікації твітів, які належать до цих емоційних категорій. Однак клас 0 (емоційна категорія 0) демонструє нижчі показники точності, пригадування та F1-оцінки порівняно з іншими класами, що вказує на певні труднощі моделі у розпізнаванні цієї категорії. Клас 3 (емоційна категорія 3) показав помірні результати за всіма метриками.

Матриця плутанини. Матриця плутанини надає детальну розбивку прогнозів моделі для кожного класу, показуючи кількість істинно-позитивних, істинно-негативних, хибно-позитивних і хибно-негативних прогнозів. Клас 1 (емоційна категорія 1) мав найбільшу кількість істинно-позитивних прогнозів, що свідчить про ефективність моделі в ідентифікації цієї емоційної категорії. Водночас клас 0 (емоційна категорія 0)

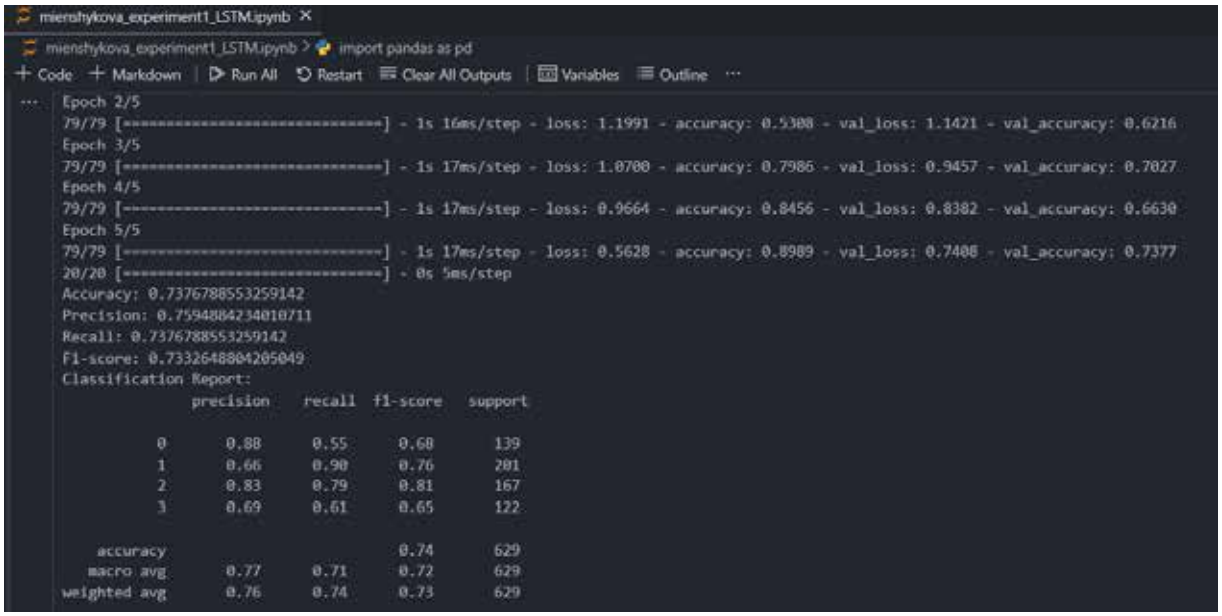


Рис. 5. Результати продуктивності моделі LSTM на тестовому наборі даних

Рис. 6. Матриця плутанини для моделі LSTM на тестовому наборі даних

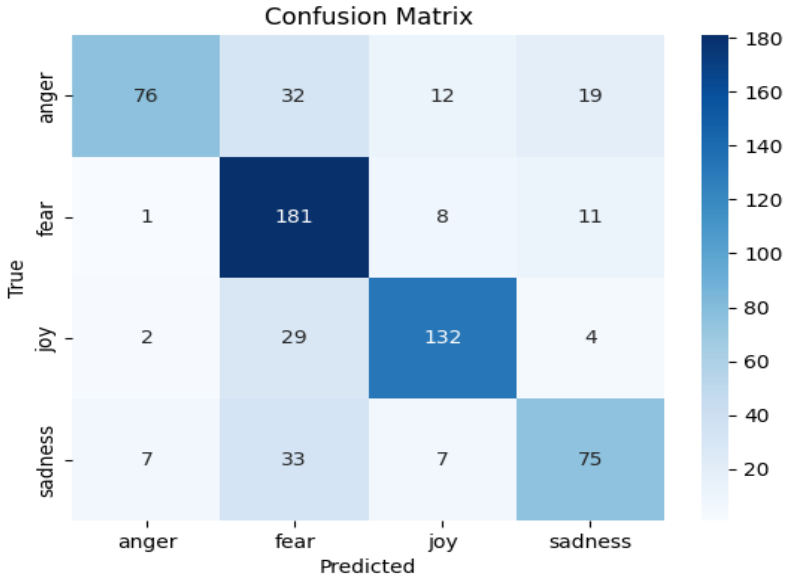


Рис. 7. Графік зміни втрат і точності моделі LSTM під час навчання

мав відносно високу кількість хибнонегативних результатів, що свідчить про тенденцію моделі пропускати випадки цієї емоційної категорії.

Керований рекурентний блок (GRU). У цьому експерименті було використано той самий набір даних, що й у попередніх моделях. Спочатку визначено розмір словника (vocab_size), розмір вектора вбудовування (embedding_dim) та максимальну довжину послідовності (max_length). Текстові дані було токенізовано, а послідовності доповнено до максимальної довжини. Для побудови моделі GRU використано Embedding-шар, GRU-шар з поверненням послідовності, GlobalMaxPooling1D та Dense-шар для багатокласової класифікації. Як функцію втрат було обрано категоріальну крос-ентропію, а точність слугувала основною метрикою оцінки моделі (Turuta et al., 2024). Модель навчалася на тренувальних даних протягом 10 епох з використанням валідаційного набору.

Результати виконання експерименту (рис. 8-10) показують, що модель GRU продемонструвала високу точність, пригадування та F1-оцінку.

Проаналізуємо основні метрики. Точність. Загальна точність моделі становить 82,22%, що свідчить про правильне передбачення емоційних категорій для 82,22% твітів у тестовому наборі. Середньозважена точність дорівнює 82,88%, а точність для окремих класів варіюється від 73% до 89%. Особливо високі показники спостерігаються для класів 0 і 2.

Пригадування. Середньозважений показник пригадування становить 82,22%, причому для

Рис. 8. Результати продуктивності моделі GRU на тестовому наборі даних

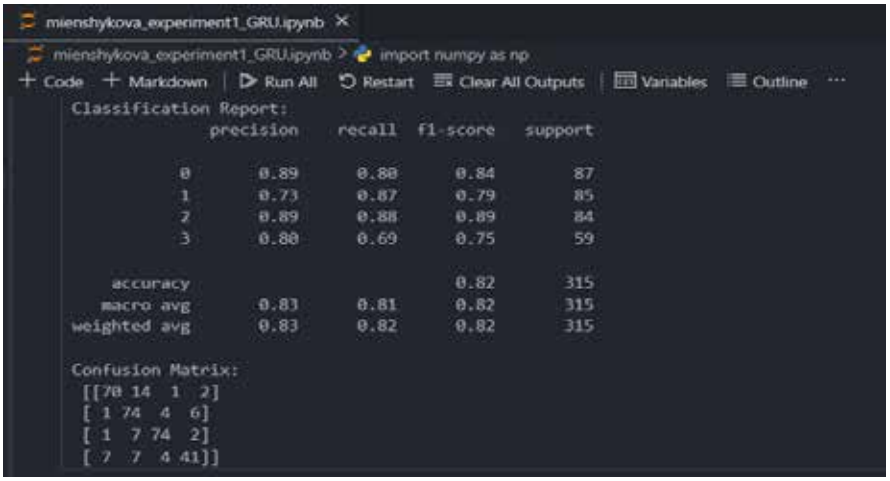


Рис. 9. Матриця плутанини для моделі GRU на тестовому наборі даних

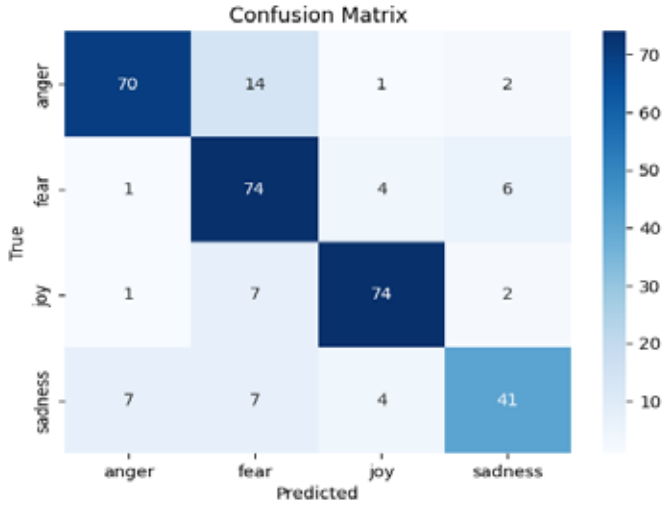


Рис. 10. Графік зміни втрат і точності моделі GRU під час навчання

окремих класів цей показник коливається від 69% до 88%. Найвищий рівень пригадування зафіксовано для класу 2.

Оцінка F1. Середньозважений показник F1 дорівнює 82,24%, що є гармонійним середнім між точністю та пригадуванням, і забезпечує збалансовану оцінку ефективності моделі.

Матриця плутанини. Матриця плутанини надає детальну розбивку прогнозів моделі для кожного класу. Вона показує, що модель працює добре для класів 0 і 2, проте має труднощі з класами 1 і 3, зокрема, плутає клас 1 з класом 3. Клас 2 (емоційна категорія 2) демонструє високу точність, пригадування та F1-оцінку. Водночас клас 1 (емоційна категорія 1) має нижчі показники у порівнянні з іншими класами, що вказує на потребу у вдосконаленні моделі для покращення класифікації цього класу. Матриця плутанини допомагає визначити конкретні області, де модель може потребувати вдосконалення, наприклад, зменшення кількості помилкових класифікацій між певними класами(James et al., 2013).

Експеримент 2 – Тест масштабованості. Тест масштабованості є важливим інструментом для оцінки ефективності моделі при збільшенні розміру даних. Він дозволяє зрозуміти, як змінюються час тренування та використання ресурсів, що особливо актуально у випадках, коли розмір набору даних може варіюватися.

Мета тесту масштабованості включає дослідження впливу збільшення розміру даних на час тренування моделі, що допомагає визначити, чи існує лінійна або нелінійна залежність між розміром даних та часом тренування, а також оцінку того, як збільшення розміру даних впливає на точність моделі, що дозволяє зрозуміти, чи поліпшується точність при збільшенні обсягу даних.

Рекурентні нейронні мережі. Результати виконання експерименту (рис. 11) показують, що із збільшенням розміру набору даних час навчання також зростає, що є очікуваною поведінкою. Це пояснюється тим, що більші набори даних вимагають більше обчислювальних ресурсів та часу для обробки.

Збільшення часу навчання не є лінійним і може залежати від таких факторів, як складність моделі та ефективність апаратного забезпечення. Точність моделі покращується зі збільшенням розміру набору даних, що свідчить про те, що більший обсяг даних сприяє кращій роботі моделі. Проте покращення точності не є строго лінійним, що вказує на можливе зменшення прибутковості від збільшення розміру набору даних. Це явище є поширеним у машинному навчанні, де початкові прирости точності більш значущі, ніж наступні.

Загалом, результати експерименту демонструють, що збільшення розміру набору даних позитивно впливає на точність моделі, однак для практичних застосувань важливо знайти баланс між розміром набору даних та наявними обчислювальними ресурсами.

Мережі довготривалої короткочасної пам'яті. LSTM показали очікувані результати в експерименті зі збільшення розміру набору даних (рис. 12). Час навчання зростав із збільшенням обсягу даних, що цілком прогнозовано, оскільки більші набори даних вимагають більше обчислювальних ресурсів. Збільшення часу навчання не було строго лінійним, але спостерігалося помітне зростання.

Що стосується точності, модель показала покращення результатів на тестовому наборі даних зі збільшенням обсягу навчальних даних. Менші набори даних, такі як 100 або 500 зразків, демонстрували нижчу точність, що було очікувано через обмеженість даних для навчання. Значне покращення точності спостерігалося при використанні більших наборів даних, таких як 10 000 або 20 000 зразків. Це вказує на те, що для невеликих наборів даних модель може не мати достатньо інформації для ефективного узагальнення, що призводить до зниження точності. У той же час, зі збільшенням розміру набору даних модель отримує більше прикладів для навчання, що позитивно впливає на її продуктивність.

Раптове підвищення точності для великих наборів даних може свідчити про здатність моделі навчатися більш складним закономірностям зі збільшенням обсягу даних. Однак при виборі розміру набору даних слід враховувати доступні ресурси і необхідність знайти баланс між часом навчання і точністю моделі.

Загалом, результати свідчать про те, що в цьому експерименті більший розмір набору даних призводить до кращої продуктивності моделі LSTM, проте при прийнятті рішень щодо оптимального розміру набору даних необхідно враховувати співвідношення між часом навчання і точністю.

Керований рекурентний блок. GRU у цьому експерименті показав очікувані результати зі збільшенням розміру набору даних (рис. 13). Час навчання моделі зростав із збільшенням обсягу даних, що є прогнозованим, оскільки більші набори даних вимагають більше обчислень для тренування моделі. На часову складність навчання впливає кількість зразків у наборі даних.

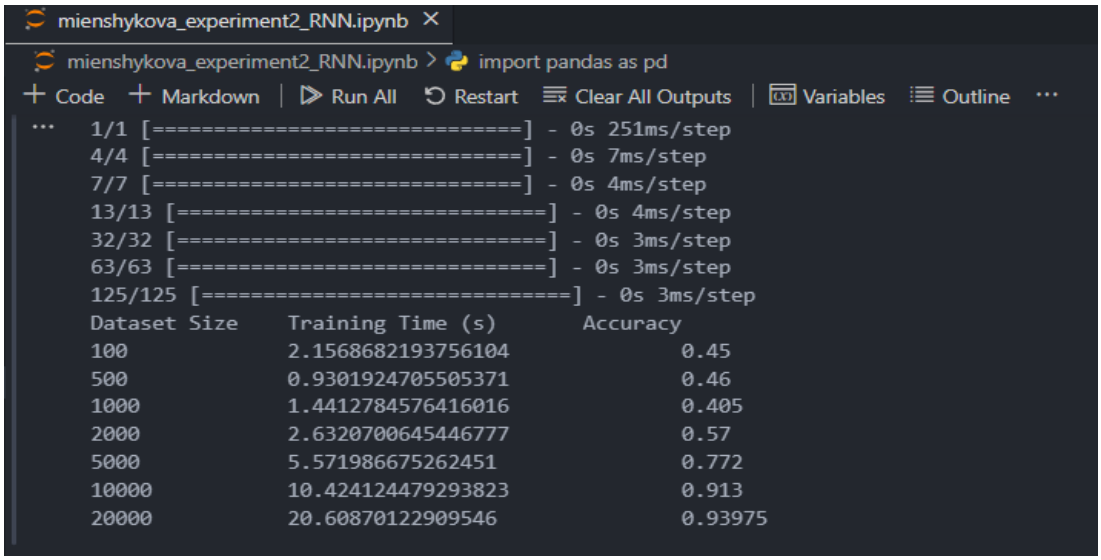


Рис. 11. Вплив розміру набору даних на час навчання та точність моделі RNN

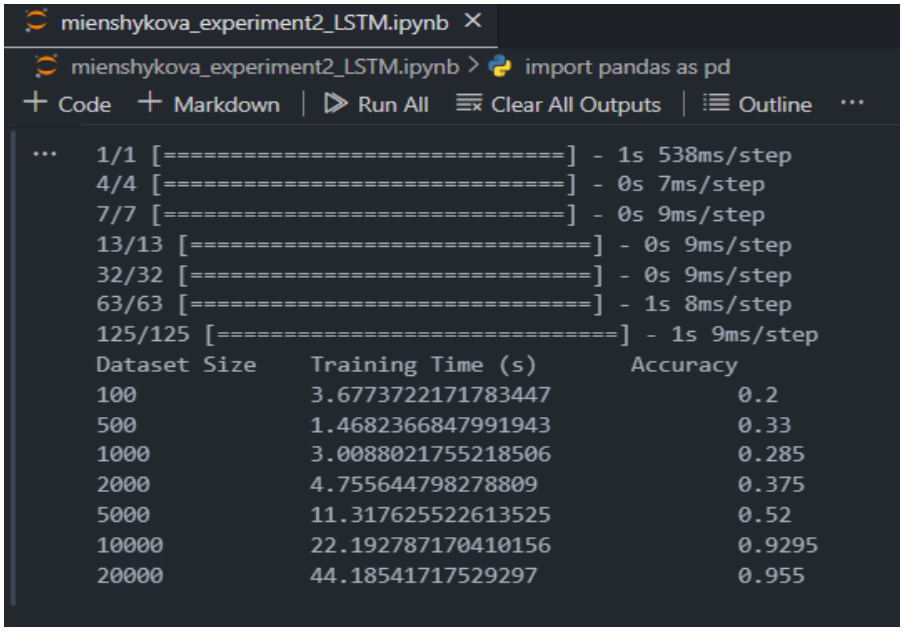


Рис. 12. Вплив розміру набору даних на час навчання та точність LSTM

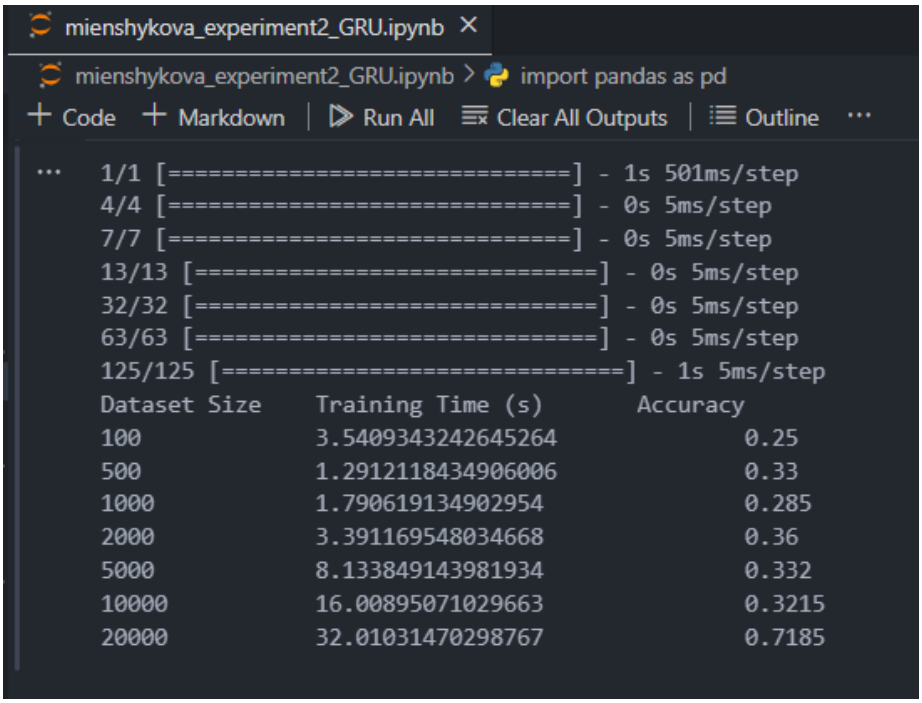


Рис. 13. Вплив розміру набору даних на час навчання та точність моделі GRU

Точність моделі на тестовому наборі даних варіювалася залежно від розміру навчального набору. Модель досягала відносно низької точності для невеликих наборів даних, наприклад, при використанні 100 зразків. Однак із збільшенням розміру набору даних точність покращувалася, досягаючи піку приблизно при 20 000 зразках. Після досягнення певного розміру набору даних покращення точності може зупинитися або навіть почати зменшуватися, що свідчить про потенційне зменшення прибутковості від подальшого збільшення обсягу даних.

Загалом, модель GRU продемонструвала типову поведінку у відповідь на зміну розміру набору даних, із збільшенням часу навчання та варіаціями у точності. Результати підкреслюють необхідність збалансованого підходу до вибору розміру набору даних, враховуючи як можливі переваги від підвищення точності, так і пов'язані з цим обчислювальні витрати.

Аналіз отриманих результатів. Результати експериментів (табл. 2) показують, що з трьох досліджуваних моделей GRU демонструє найвищу точність, за нею йде LSTM, тоді як RNN має найнижчу точність. Модель GRU також має найвищі значення Precision, Recall та F1-Score, що свідчить про її високу якість розпізнавання емоцій. LSTM показує хороші результати, проте поступається GRU за цими показниками. Модель RNN, навпаки, демонструє найнижчі результати серед трьох моделей, що вказує на її менш ефективне розпізнавання емоцій порівняно з LSTM та GRU.

Модель RNN має найнижчу точність та ефективність серед усіх моделей, але відзначається найменшим часом навчання. Це може бути корисним, якщо швидкість навчання є пріоритетом, хоча за це доводиться платити точністю результатів. Модель LSTM добре справляється із завданням емоційного аналізу, досягаючи значно кращих результатів у порівнянні з RNN, але трохи поступається GRU. Модель GRU забезпечує найкращі результати з точки зору точності, precision, recall та F1-Score, що робить її найпридатнішою для завдань емоційного аналізу, хоча вона може вимагати більших обчислювальних ресурсів.

Отже, GRU є найкращим варіантом для емоційного аналізу завдяки високим значенням точності та інших метрик. LSTM також може бути ефективним вибором, особливо якщо ресурси обмежені, тоді як RNN, незважаючи на швидке навчання, не є оптимальним вибором через низьку точність.

Тест масштабованості (табл. 3) показав, що всі три моделі демонструють збільшення часу навчання зі збільшенням розміру набору даних. Модель RNN має найменший час навчання для найменших наборів даних, але виявляється неефективною для більших обсягів. LSTM показує найкращі результати точності для всіх розмірів набору даних, але потребує більше часу

Таблиця 2

Експеримент 1 – Аналіз емоцій

Модель	Точність (Accuracy)	Точність (Precision)	Пригадування (Recall)	F1-score
RNN	0.22099	0.04883	0.22099	0.07999
LSTM	0.73768	0.75949	0.73768	0.73326
GRU	0.82222	0.82882	0.82222	0.82245

Таблиця 3

Експеримент 2 – Тест масштабованості

Модель	Розмір набору даних	Час навчання (с)	Точність
RNN	100	3.68	0.2
	500	1.47	0.33
	1000	3.01	0.285
	2000	4.76	0.375
	5000	11.32	0.52
	10000	22.19	0.9295
	20000	44.19	0.955
LSTM	100	3.68	0.2
	500	1.47	0.33
	1000	3.01	0.285
	2000	4.76	0.375
	5000	11.32	0.52
	10000	22.19	0.9295
	20000	44.19	0.955
GRU	100	3.54	0.25
	500	1.29	0.33
	1000	1.79	0.285
	2000	3.39	0.36
	5000	8.13	0.332
	10000	16.01	0.3215
	20000	32.01	0.7185

для навчання. Модель GRU також демонструє хороші результати, особливо при середніх та великих розмірах даних, хоча її точність може стабілізуватися або навіть зменшуватися при дуже великих наборах даних.

Модель RNN показує швидке навчання для невеликих обсягів даних, але її точність значно поступається LSTM та GRU, що робить її менш придатною для завдань з великими обсягами даних. LSTM залишається найкращим вибором для роботи з великими наборами даних, оскільки вона показує високу точність, хоча час навчання також збільшується. GRU є прийнятним варіантом для середніх та великих наборів даних, демонструючи більш ефективний час навчання порівняно з LSTM при прийнятних результатах точності.

Таким чином, вибір між LSTM та GRU може залежати від конкретного завдання, обсягів даних та доступних ресурсів. LSTM виявляється більш універсальною моделлю з високою точністю для різних обсягів даних, але важливо враховувати час навчання та ресурси при її виборі.

На обмежених ресурсах моделі демонструють різні результати. RNN досягає досить високої точності на низьких ресурсах і має найменший час навчання, що може бути перевагою на обмежених пристроях. LSTM показує високу точність на обмежених ресурсах, хоча її час навчання є вищим порівняно з RNN, але вона залишається працездатною на низьких ресурсах. GRU, хоча і швидша за LSTM, демонструє найнижчу точність серед трьох моделей на обмежених ресурсах, що вказує на втрату точності при швидкому навчанні.

Отже, LSTM є найефективнішою моделлю для використання на обмежених пристроях, зберігаючи високу точність. RNN може бути вибором у випадках, коли основний критерій – це швидкий час навчання. GRU, хоч і швидший за LSTM, але втрачає в точності на низьких ресурсах, що робить LSTM більш придатною для ефективного використання на обмежених пристроях.

Висновки. У ході експериментального дослідження було проведено аналіз моделей глибинного навчання – RNN, LSTM та GRU – в контексті обробки природної мови (NLP) за різними критеріями: емоційний аналіз, масштабованість та ефективність на обмежених ресурсах.

Перший експеримент, присвячений емоційному аналізу, показав, що модель GRU досягла найвищих показників accuracy, precision, recall та F1-Score. LSTM також продемонструвала ефективність, але трохи поступилася GRU за цими метриками. Модель RNN виявила найнижчу точність та загальну ефективність серед трьох досліджуваних моделей.

У другому експерименті, що тестував масштабованість моделей, було виявлено, що RNN є швидкою для роботи з невеликими наборами даних, але неефективною для більших обсягів. LSTM продемонструвала найвищу точність на великих наборах даних, залишаючись оптимальною моделлю для їх обробки. GRU показала хороші результати, особливо з середніми та великими розмірами даних.

У третьому експерименті, який перевіряв ефективність моделей на обмежених ресурсах, LSTM зберегла високу точність, підтвердивши свою ефективність у таких умовах. RNN показала відносно непогану точність і мала найменший час навчання, що може бути перевагою на пристроях з обмеженими ресурсами. GRU, хоч і працювала швидше, але втратила точність у порівнянні з LSTM та RNN на обмежених ресурсах.

Аналіз результатів підтверджує відповідність моделей їхнім перевагам і недолікам. RNN виявилася ефективною в обробці різної довжини послідовностей та моделюванні часових залежностей, проте мала проблеми із зникаючим градієнтом та інтенсивними обчисленнями. LSTM підтвердила свої переваги у моделюванні довгострокових залежностей та стійкості до зашумлених даних, але потребує великих обчислювальних ресурсів. GRU, у свою чергу, показала високу ефективність в обчисленнях і здатність обробляти довгострокові залежності, хоча й може бути менш ефективною в деяких завданнях порівняно з LSTM та має схильність до перенавчання.

Вибір між моделями залежить від конкретного завдання, доступних ресурсів та обсягу даних. LSTM є потужною для моделювання довгострокових залежностей, RNN може бути швидким варіантом для невеликих наборів даних, а GRU є ефективною для обмежених ресурсів.

Для емоційного аналізу рекомендовано використовувати GRU, оскільки вона показала найвищу точність і інші метрики. Якщо ресурси обмежені, LSTM може бути хорошим варіантом, оскільки забезпечує високу точність при менших витратах на обчислення. У завданнях, пов’язаних з великими обсягами даних, LSTM є оптимальним вибором завдяки своїй здатності до масштабування та високій точності. GRU також є хорошим варіантом для роботи із середніми та великими наборами даних, але слід враховувати можливі втрати точності при дуже великих наборах. Якщо ресурсів небагато,

LSTM забезпечує високу точність на обмежених пристроях, тоді як GRU може бути використана для більш швидкого навчання на середніх наборах даних.

Для подальших досліджень рекомендується проведення експериментів з іншими моделями глибинного навчання та тестування цих моделей на різних завданнях NLP, таких як машинний переклад або тематичне моделювання. Інтеграція з іншими технологіями, як-от автоматичне збирання даних або високопродуктивні обчислювальні системи, може підвищити ефективність моделей. Дослідження впливу складних даних на продуктивність, а також оптимізація моделей для роботи на обмежених пристроях можуть стати важливими напрямами для подальших експериментів.

Таким чином, LSTM є найбільш універсальною моделлю для роботи з великими обсягами даних та обмеженими ресурсами, забезпечуючи високу точність. GRU може бути ефективною для завдань з обмеженими ресурсами, проте слід враховувати можливу втрату точності. RNN може бути швидким рішенням для невеликих обсягів даних, але не є оптимальною моделлю для великих задач NLP.

Це дослідження є важливою точкою для подальшого вивчення та оптимізації моделей глибинного навчання для NLP-завдань. Наступні кроки включають розширення обсягу даних, оптимізацію гіперпараметрів та випробування моделей на інших завданнях обробки природної мови для досягнення більшої ефективності в реальних умовах.

ЛІТЕРАТУРА:

1. Natural Language Processing – DeepLearning.AI. URL: https://www.deeplearning.ai/resources/natural-language-processing/ (дата звернення: 05.09.2024).

2. Afanasieva I., Golian N., Hnatenko O., Daniiel Y., Onyshchenko K. Data exchange model in the Internet of Things concept. Telecommunications and Radio Engineering. New York, 2019. Vol. 78, № 10. P. 869–878.

3. Golian, V., Golian, N., Afanasieva, I., Halchenko, K., Onyshchenko, K., Dudar, Z. Study of Methods for Determining Types and Measuring of Agricultural Crops due to Satellite Images. 32nd International Scientific Symposium Metrology and Metrology Assurance, MMA 2022, Sozopol, Bulgaria.

4. Recurrent Neural Networks (RNN) – EDUCBA. URL: https://www.educba.com/recurrent-neural-networks-rnn/ (дата звернення: 05.09.2024).

5. Anish Nama. Understanding LSTM Architecture, Pros and Cons, and Implementation. Medium, 2020. URL: https://medium.com/@anishnama20/understanding-lstm-architecture-pros-and-cons-and-implementation-3e0cca194094 (дата звернення: 03.09.2024).

6. Anish Nama. Understanding Gated Recurrent Unit (GRU) in Deep Learning. Medium, 2020. URL: https://medium.com/@anishnama20/understanding-gated-recurrent-unit-gru-in-deep-learning-2e54923f3e2 (дата звернення: 02.09.2024).

7. Pandey P. Emotion dataset. Kaggle. URL: https://www.kaggle.com/datasets/parulpandey/emotion-dataset (дата звернення: 05.09.2024).

8. Afanasieva, I., Golian, N., Golian, V., Khovrat, A., Onyshchenko, K. Application of Neural Networks to Identify of Fake News. Computational Linguistics and Intelligent Systems (COLINS 2023): 7th International Conference, Kharkiv, 20 April – 21 April 2023: CEUR workshop proceedings, No. 3396. P. 346–358. URL: https://ceur-ws.org/Vol-3396/paper28.pdf (дата звернення: 02.09.2024).

9. Turuta O., Afanasieva I., Golian N., Golian V., Onyshchenko K., Suvorov D. Audio processing methods for speech emotion recognition using machine learning. MoMLet-2024: 6th International Workshop on Modern Machine Learning Technologies, 31 травня – 1 червня 2024 р., Львів-Шацьк, Україна. С. 75–108.

10. James, G., Witten, D., Hastie, T., Tibshirani, R. An Introduction to Statistical Learning with Applications in R. New York: Springer, 2013. 426 p.

REFERENCES:

1. DeepLearning.AI. (n.d.). Natural Language Processing. Retrieved from: https://www.deeplearning.ai/resources/natural-language-processing/

2. Afanasieva, I., Golian, N., Hnatenko, O., Daniiel, Y., & Onyshchenko, K. (2019). Data exchange model in the Internet of Things concept. Telecommunications and Radio Engineering, 78(10), 869–878.

3. Golian, V., Golian, N., Afanasieva, I., Halchenko, K., Onyshchenko, K., & Dudar, Z. (2022). Study of methods for determining types and measuring of agricultural crops due to satellite images. In Proceedings of the 32nd International Scientific Symposium Metrology and Metrology Assurance (MMA 2022), Sozopol, Bulgaria.

4. EDUCBA. (n.d.). Recurrent Neural Networks (RNN). Retrieved from: https://www.educba.com/recurrent-neural-networks-rnn/

5. Nama, A. (2020). Understanding LSTM Architecture, Pros and Cons, and Implementation. Medium. Retrieved from: https://medium.com/@anishnama20/understanding-lstm-architecture-pros-and-cons-and-implementation-3e0cca194094

6. Nama, A. (2020). Understanding Gated Recurrent Unit (GRU) in Deep Learning. Medium. Retrieved from: https://medium.com/@anishnama20/understanding-gated-recurrent-unit-gru-in-deep-learning-2e54923f3e2

7. Pandey, P. (n.d.). Emotion dataset. Kaggle. Retrieved from: https://www.kaggle.com/datasets/parulpandey/emotion-dataset

8. Afanasieva, I., Golian, N., Golian, V., Khovrat, A., & Onyshchenko, K. (2023). Application of neural networks to identify fake news. In Computational Linguistics and Intelligent Systems (COLINS 2023): 7th International Conference, Kharkiv, 20 April – 21 April 2023, CEUR Workshop Proceedings (Vol. 3396, pp. 346–358). Retrieved from: https://ceur-ws.org/Vol-3396/paper28.pdf

9. Turuta, O., Afanasieva, I., Golian, N., Golian, V., Onyshchenko, K., & Suvorov, D. (2024). Audio processing methods for speech emotion recognition using machine learning. In Proceedings of the 6th International Workshop on Modern Machine Learning Technologies (MoMLet-2024), Nay 31 – June 1, 2024, Lviv-Shatsk, Ukraine (pp. 75–108).

10. James, G., Witten, D., Hastie, T., & Tibshirani, R. (2013). An Introduction to Statistical Learning with Applications in R. New York: Springer.

UDC 004.9; 004.94
DOI https://doi.org/10.32782/IT/2024-3-8

Vitaliia KOIBICHUK
PhD Economics, Associate Professor, Head of the Department of Economic Cybernetics, Sumy State University, 57, Petropavlivska Str., Sumy, Ukraine, 40000, v.koibichuk@biem.sumdu.edu.ua
***ORCID:** 0000-0002-3540-7922*

Roman KOCHEREZHCHENKO
Master's Student, Sumy State University, 57, Petropavlivska Str., Sumy, Ukraine, 40000, r.kocherezhchenko@student.sumdu.edu.ua
***ORCID:** 0000-0001-7269-4177*

Kostiantyn HRYTSENKO
Candidate of Technical Sciences, Associate Professor at the Department of Economic Cybernetics, Sumy State University,, 57, Petropavlivska Str., Sumy, Ukraine, 40000, k.hrytsenko@biem.sumdu.edu.ua
***ORCID:** 0000-0002-7855-691X*

Valerii YATSENKO
Candidate of Technical Sciences, Associate Professor at the Department of Economic Cybernetics, Sumy State University, 57, Petropavlivska Str., Sumy, Ukraine, 40000, v.yatsenko@biem.sumdu.edu.ua
***ORCID:** 0000-0003-2316-3817*

Alina YEFIMENKO
PhD, Assistant at the Department of Economic Cybernetics, Sumy State University, 57, Petropavlivska Str., Sumy, Ukraine, 40000, a.yefimenko@uabs.sumdu.edu.ua
***ORCID:** 0000-0002-2810-0965*

To cite this article: Koibichuk, V., Kocherezhchenko, R., Hrytsenko, K., Yatsenko, V., Yefimenko, A. (2024). Alhorytmy protsedurnoi heneratsii ihrovoho kontentu za dopomohoiu hrafiv [Algorithms for procedural generation of game content using graphs]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 77–87, doi: https://doi.org/10.32782/IT/2024-3-8

ALGORITHMS FOR PROCEDURAL GENERATION OF GAME CONTENT USING GRAPHS

Developing unique gaming environments using algorithms based on graph data structures and procedural content generation can significantly reduce costs while increasing overall team productivity and eliminating the risk of stagnation in the development process.

***The purpose** of this research is to analyze, develop and visualize the operation of procedural content generation algorithms, as well as to study the prospects for their further use in the practical development of game projects.*

***The scientific novelty** is to use graphs for procedural generation of game content. This topic was chosen due to the fact that creating a game environment can be one of the main and most resource-intensive costs in the game production process. Procedural content generation can reduce these costs and speed up the development process. In fact, it is almost impossible to calculate what specific part of the team's productivity and business benefits procedural generation brings, since most discoveries in this area are a trade secret of most game studios, however, this only speaks of the opportunities and benefits that this approach brings.*

***The methodology** is based on The Python programming language as the main tool for studying algorithms, which was used to develop algorithms, create visualizations and examples of web servers for processing data generated by graphs.*

***Conclusion:** during development, differences and commonalities in the details of the implementation of algorithms, as well as the results of content generation, were studied. Differences in the generated graphs were also demonstrated. Examples of web servers illustrate the potential for further practical application of the developed algorithms. The results of the study can be used by developers of gaming environments and algorithms researchers to improve the efficiency of production processes.*

***Key words:** procedural generation, game development, development efficiency, development optimization.*

Віталія КОЙБІЧУК
кандидат економічних наук, доцент, завідувач кафедри економічної кібернетики, Сумський державний університет, вул. Петропавлівська, 57, м. Суми, Україна, 40000
***ORCID:** 0000-0002-3540-7922*

Роман КОЧЕРЕЖЧЕНКО
магістр, Сумський державний університет, вул. Петропавлівська, 57, м. Суми, Україна, 40000
***ORCID:** 0000-0001-7269-4177*

Костянтин ГРИЦЕНКО
кандидат технічних наук, доцент кафедри економічної кібернетики, Сумський державний університет, вул. Петропавлівська, 57, м. Суми, Україна, 40000
***ORCID:** 0000-0002-7855-691X*

Валерій ЯЦЕНКО
кандидат технічних наук, доцент кафедри економічної кібернетики, Сумський державний університет, вул. Петропавлівська, 57, м. Суми, Україна, 40000
***ORCID:** 0000-0003-2316-3817*

Аліна ЄФІМЕНКО
доктор філософії, асистент кафедри економічної кібернетики, Сумський державний університет, вул. Петропавлівська, 57, м. Суми, Україна, 40000
***ORCID:** 0000-0002-2810-0965*

Бібліографічний опис статті: Койбічук, В., Кочережченко, Р., Гриценко, К., Яценко, В., Єфіменко, А. (2024). Алгоритми процедурної генерації ігрового контенту за допомогою графів. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 77–87, doi: https://doi.org/10.32782/IT/2024-3-8

АЛГОРИТМИ ПРОЦЕДУРНОЇ ГЕНЕРАЦІЇ ІГРОВОГО КОНТЕНТУ З ВИКОРИСТАННЯМ ГРАФІВ

Розробка унікальних ігрових середовищ з використанням алгоритмів на основі графових структур даних та процедурної генерації контенту дозволяє суттєво скоротити витрати при одночасному підвищенні загальної продуктивності команди та усуненні ризику стагнації процесу розробки.

***Метою роботи** є аналіз, розробка та візуалізація роботи алгоритмів процедурної генерації контенту, а також вивчення перспектив їх подальшого використання у практичній розробці ігрових проектів.*

***Наукова новизна** полягає у використанні графів для процедурної генерації ігрового контенту. Ця тема була обрана у зв'язку з тим, що створення ігрового оточення може бути однією з основних і найбільш ресурсоємних витрат у процесі виробництва гри. Процедурна генерація контенту може зменшити ці витрати та пришвидшити процес розробки. Практично неможливо підрахувати, яку конкретно частину продуктивності команди та бізнес-вигоди приносить процедурна генерація, оскільки більшість інновацій у цій сфері є комерційною таємницею ігрових студій, однак це говорить лише про можливості та переваги, які несе в собі цей підхід.*

***Методологія** базується на мові програмування The Python як основному інструменті для вивчення алгоритмів, який використовувався для розробки алгоритмів, створення візуалізацій та прикладів веб-серверів для обробки даних, згенерованих графами.*

***Висновок:** під час розробки були вивчені відмінності та спільні риси в деталях реалізації алгоритмів, а також результати генерації контенту. Також було продемонстровано відмінності у згенерованих графах. На прикладах веб-серверів проілюстровано потенціал подальшого практичного застосування розроблених алгоритмів. Результати дослідження можуть бути використані розробниками ігрових середовищ та дослідниками алгоритмів для підвищення ефективності виробничих процесів.*

***Ключові слова:** процедурна генерація, розробка ігор, ефективність розробки, оптимізація розробки.*

Introduction. Procedural content generation (PGC) is considered one of the tools for creating a unique player experience in projects of various scales. Minimizing the cost of game design development, it allows you to automate the generation of game maps, dialogues and events (Togelius et al., 2011). Thus, the content of the game world, the environment of the character is enriched and opportunities for dynamic adaptation to the user's actions are created. The effective application of

PCC can compensate for shortcomings in design, gameplay mechanics, etc., and make such a gaming experience a special feature of the product (Van Der Linden et al., 2013).

Previously, the limited computing power of systems forced developers to save on memory and processor time, which prevented the use of this tool. However, with the development of technology, procedural generation has become not only possible, but also desirable for creating large and varied game universes.

In the context of traditional game design, where game environments are hand-crafted by teams of specialists, PGK offers an alternative approach that allows for the generation of infinitely diverse game scenarios and worlds. Using this approach not only reduces the dependence on the creative resources of the team and the efficiency of manual labor, but also opens new horizons for innovation in the industry. As a result, game implementation becomes more accessible to developers of various levels, while players gain access to inexhaustible content.

This study attracts special attention because it provides a unique opportunity to explore complex algorithmic and mathematical principles in the context of their practical application for creating dynamic and exciting game content. Using graphs as a basis for procedural generation allows modeling complex structures and relationships, opening new horizons for automating the creation of game worlds, levels, storylines, and dynamic game events. In addition, the PGK direction promotes the development of new methods of optimization and data analysis, as well as the application of graph theory in non-standard fields, such as data visualization and machine learning. This makes the researched technology very promising from both an academic and a practical point of view. In light of the constant development of the industry, its numerous innovations and the improvement of the quality of the gaming experience, the effective application of such algorithms can significantly expand the boundaries of what is possible in the development of game design

Statement of the problem. During the review of the literature, several works were studied to research issues related to procedural generation, its features, characteristics and opportunities for process optimization. To study procedural generation in general, its goals, capabilities and features, the following works were considered. In fact, there are not many scientific papers from which you can get the latest and most relevant information, since most technical open-source work takes place in game studios where most do not share the source code for analyzing algorithms. The first work that gives a general understanding of algorithms is «Procedural content generation for games: A survey», this material gave a general idea of the features of algorithms and their possible impact on development processes (Hendrikx et al., 2013). Another work, «Procedural content generation: Goals, challenges and actionable steps» allowed us to delve deeper not only into the technical details and challenges that a team that decides to use generative approaches in development may encounter, but also without the value that, with the right approach, gives a tangible increase in the productivity of the development team (Togelius et al., 2013). «What is procedural content generation? Mario on the borderline» gave a more thorough technical overview of the use of procedural generation in conditions of limited resources, which also gave insight into the possibilities of generating game landscapes of relatively large sizes, which is not possible in standard game design (Togelius et al., 2011). The remaining works mentioned in the work served as the technical and theoretical basis for the development and demonstration of algorithms. With their help, a strong and reliable basis was obtained for the practical implementation of algorithms using the graph data structure. **Thereby, the purpose of this research** is to analyze, develop and visualize the operation of procedural content generation algorithms, as well as to study the prospects for their further use in the practical development of game projects.

Methodology. For practical implementation, the general purpose programming language Python is used. It is chosen as one of the most popular languages, which has a convenient infrastructure with a large number of useful packages that simplify the solution of tasks. However, any application programming language can be used to implement these algorithms.

The development of all algorithms within this work will take place in several stages:

- Demonstration of pseudocode.
- Demonstration of working code in the chosen programming language.
- Visualization of the algorithm.

This will give understanding which algorithm is better to use for the needs of game designers.

To begin with, before the implementation of more complex algorithms, it is possible to show an easy version of the work of the library algorithm to demonstrate the practical possibilities of generation and visualization. The program code is shown in Figure 1, the results of the work on Figure 2. Having a basic understanding of the operation of some algorithms, as well as a visual demonstration

```python
def generate_graph(num_nodes, num_edges):
    G = nx.Graph()
    for i in range(num_nodes):
        G.add_node(i)
    while G.number_of_edges() < num_edges:
        node_a = random.randint(0, num_nodes - 1)
        node_b = random.randint(0, num_nodes - 1)
        if node_a != node_b:
            G.add_edge(node_a, node_b)
    return G

def visualize_graph(G):
    pos = nx.spring_layout(G)  # Location of nodes using the Fruchterman-Reingold algorithm
    nx.draw(G, pos, with_labels=True, node_color='lightblue', edge_color='gray')
    plt.show()

# Graph generation
num_nodes = 10  # number of nodes
num_edges = 15  # number of edges
G = generate_graph(num_nodes, num_edges)

# Graph visualization
visualize_graph(G)
```

Fig. 1. Program code for implementing the library algorithm for graph generation and visualization

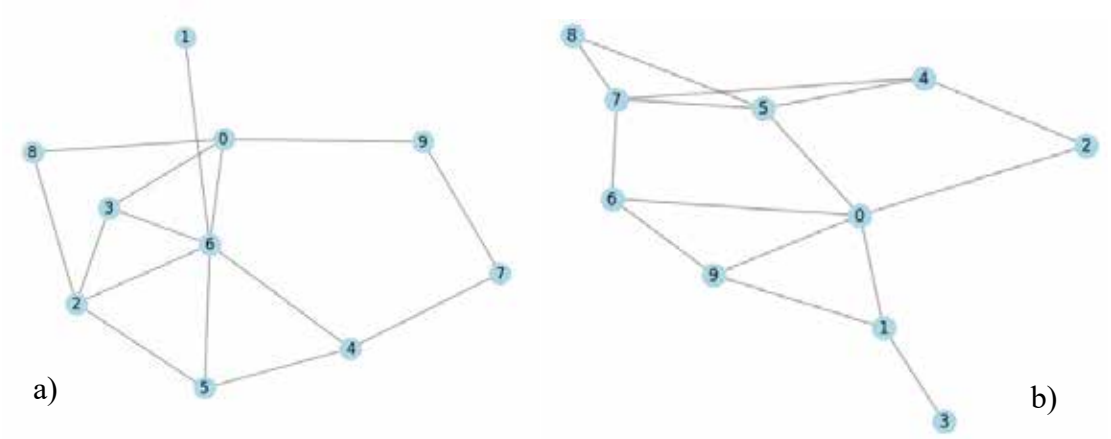


Fig. 2. The first result (a) and second result (b) of the work of the library algorithm

of the generated graph, that can help implementing algorithms.

Results. In order to generate a pseudocode (Figure 3) of the algorithm, we will generate the main steps of its operation:

- Graph initialization: We start with an empty graph and an initial node located at the origin of coordinates (0,0).
- Setting Directions: Define possible movements in the graph, which include movement to the left, right, down and up.
- Cycle for Random Wandering:

o Direction and Weight: At each iteration, we randomly select one of the specified directions and generate a random weight that affects the distance of the next step.

o Calculation of the Position of the Next Node: We determine the position of the next node using the position of the current node, to which we add the selected direction multiplied by the weight.

When the main steps are formed, we proceed to the formation of the pseudocode for the implementation of the algorithm.

This is one of the simplest variants of the algorithm, while the algorithm itself is quite simple. However, it should be borne in mind that without additional configuration, the result will be quite simple for the structure of the game environment.

Next step is the implementation the algorithm using the selected programming language Figure 4.

We will test the described algorithm and create the generation results. For clarity, we will perform two generation of Figure 5. According to the results shown in the corresponding figures, it can be concluded that the algorithm is suitable for non-deterministic game environments. That is, it can be used as a basis for other algorithms, or as an additional step in the graph processing chain.

Now we practically implement the algorithm of binary division of space. First, let's form the main steps of the algorithm:

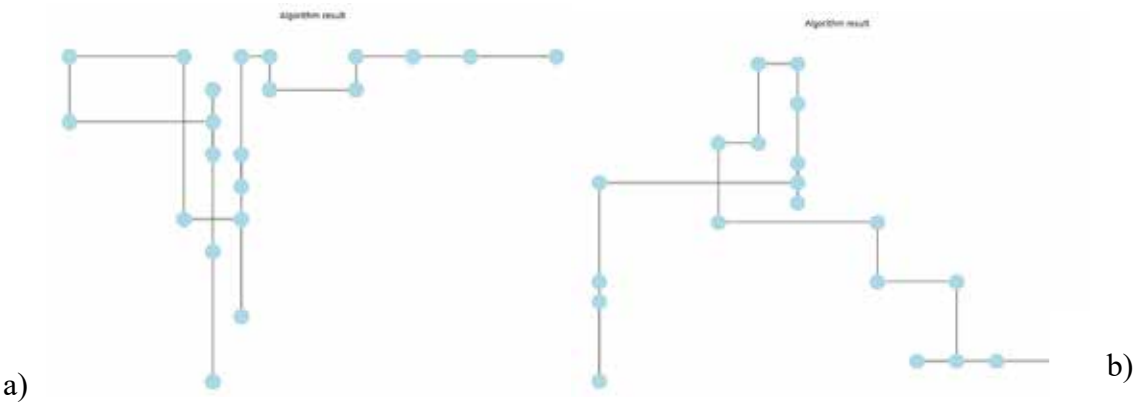
- Initialization: the initial area to be divided is selected.
- Recursive division: the selected area is divided into two parts using a straight line (or plane

```
Function random_walk(num_steps):
    Initialize an empty graph G
    Set the initial node as (0, 0) and add it to G

    Set directions as [(-1, 0), (1, 0), (0, -1), (0, 1)]  # Four possible moves: Left, Right, Down, Up

    Loop from 1 to num_steps:
        Choose a random direction from directions
        Generate a random weight between 1 and 5

        Compute next_node:
            next_node_x = current_node_x + direction_x * weight
            next_node_y = current_node_y + direction_y * weight
            next_node = (next_node_x, next_node_y)

        Add next_node to the graph G
        Connect current_node to next_node with an edge with the computed weight

        Update current_node to next_node

    Return graph G
```

Fig. 3. Drunkard's Walk algorithm pseudocode

```python
def random_walk(num_steps):
    G = nx.Graph()

    current_node = (0, 0)
    G.add_node(current_node)

    directions = [(-1, 0), (1, 0), (0, -1), (0, 1)]  # Left, Right, Down, Up

    for _ in range(num_steps):
        move = random.choice(directions)
        weight = random.randint(1, 5)
        next_node = (current_node[0] + move[0] * weight, current_node[1] + move[1] * weight)
        G.add_node(next_node)
        G.add_edge(current_node, next_node, weight=weight)
        current_node = next_node

    return G

# Number of steps
num_steps = 20
G = random_walk(num_steps)

# Visualization
plt.figure(figsize=(12, 8))
pos = {node: (node[0], node[1]) for node in G.nodes()}
edges = G.edges(data=True)

nx.draw(G, pos, with_labels=False, node_color='lightblue', node_size=500, font_size=16, font_color='darkred')
plt.title("Algorithm result")
plt.show()
```

Fig. 4. Implementation of the algorithm in Python



a) b)

Fig. 5. The first result (a) and second result (b) of the Drunkard's Walk algorithm

in 3D), which can pass vertically, horizontally or at any angle, depending on the task and the selection algorithm. This process continues recursively for each of the newly created parts until given criteria such as minimum part size are met.

- Stopping the algorithm: the recursion stops when each part reaches a certain minimum size or when the number of recursive divisions reaches a maximum limit.

We will describe the formed steps with the help of pseudocode Figure 6.

The main steps have been formed, let's move on to the software implementation using the selected programming language. Since the implementation turns out to be very voluminous – we will take it to the applications. Here we will describe exactly how the developed software part works:

- Room class – this class represents a room with given coordinates (x, y), width and height. It also calculates the center of the room, which is used for further calculations.
- The «_init_» method initializes the room with the given parameters and determines its center (Fig. 7).
- The «split» method divides a room into two smaller rooms (vertically or horizontally) based on which is greater: width or height. The choice of partitioning method depends on the aspect ratio of the room and the number of allowed partitions (max_splits) (Fig. 7).
- The «vertical_split» and «horizontal_split» methods perform their own splitting. They choose a position to break (not too close to the edges), create new rooms and return them (Fig. 7).
- «create_rooms» function – this function recursively divides the initial room into smaller ones until the maximum number of rooms is reached or until the possibility of division is exhausted. This

```
Function BSP(space, max_splits)
    If max_splits == 0 or the size of the space is below the minimum
        End recursion
    End if

    # Determine the axis of splitting (vertical or horizontal)
    If the width of the space is greater than the height
        axis = vertical
    Else
        axis = horizontal
    End if

    # Choose the splitting position within the space
    If axis == vertical
        split_position = random number between 1/4 and 3/4 of the width of the space
    Else
        split_position = random number between 1/4 and 3/4 of the height of the space
    End if

    # Create two new spaces
    left_or_top = create_space(start to split_position)
    right_or_bottom = create_space(split_position to end)

    # Recursive call for both newly created spaces
    BSP(left_or_top, max_splits - 1)
    BSP(right_or_bottom, max_splits - 1)
End function

# Main code
initial_space = define_initial_space()
BSP(initial_space, given_number_of_splits)
```

Fig. 6. Pseudocode for implementing the Binary Space Partitioning algorithm

```
class Room:
    def __init__(self, x, y, width, height):
        self.x = x
        self.y = y
        self.width = width
        self.height = height
        self.center = (self.x + self.width / 2, self.y + self.height / 2)

    def split(self, max_splits):
        if max_splits > 0:
            if self.width > self.height:
                return self.vertical_split(max_splits)
            else:
                return self.horizontal_split(max_splits)
        return None

    def vertical_split(self, max_splits):
        if max_splits > 0 and self.width > 10:
            split_pos = random.randint(self.width // 4, self.width * 3 // 4)
            left = Room(self.x, self.y, split_pos, self.height)
            right = Room(self.x + split_pos, self.y, self.width - split_pos, self.height)
            return left, right
        return None

    def horizontal_split(self, max_splits):
        if max_splits > 0 and self.height > 10:
            split_pos = random.randint(self.height // 4, self.height * 3 // 4)
            top = Room(self.x, self.y, self.width, split_pos)
            bottom = Room(self.x, self.y + split_pos, self.width, self.height - split_pos)
            return top, bottom
        return None
```

Fig. 7. Functions from BSP implementation: --init--, split, vertical_split, horizontal_split

provides control over the number of rooms in the final structure (Fig. 8).

• «build_graph» function – this function creates a graph where each room is a node. Nodes are connected by edges based on the distance between room centers, but only until the number of connections per room exceeds the specified limit (max_connections_per_room). This limits the degree of connectivity between rooms, which can be useful for creating more realistic room layouts (Fig. 9).

• «draw_graph» function – this function renders a graph using the NetworkX graph drawing library. It uses room positions to place nodes and shows the connections between them (Fig. 10).

Figure 11 shows running and visualization of the algorithm.

General execution flow: an initial room is created, it is divided into smaller rooms using the «create_rooms» function, After the division of rooms is complete, a graph is created from these rooms, the graph is visualized using the «draw_graph» function. The results of the algorithm can be seen in Figure 12.

From the obtained results, we can see that this particular algorithm is more suitable for practical problems, because it has the ability to fine-tune parameters that allow you to obtain different, but predictable results.

The practical application of graph generation algorithms consists in the use of generated structures – as a basic representation of game environments. However, simple visualization of the generated graph is of no practical value for further use. To obtain usable results, it is advisable to implement a program interface (API – Application Programming Interface) that provides output

```
def create_rooms(start_room, min_size, max_splits):
    rooms = []
    nodes_to_split = [(start_room, max_splits)]

    while nodes_to_split:
        current_room, splits_left = nodes_to_split.pop()
        if splits_left > 0:
            result = current_room.split(splits_left - 1)
            if result:
                left, right = result
                nodes_to_split.append((left, splits_left - 1))
                nodes_to_split.append((right, splits_left - 1))
            else:
                if current_room.width >= min_size and current_room.height >= min_size:
                    rooms.append(current_room)
        else:
            rooms.append(current_room)

        if len(rooms) >= 10:
            break

    return rooms
```

Fig. 8. BSP implementation functions: create_rooms

```
def build_graph(rooms, max_connections_per_room):
    G = nx.Graph()
    pos = {}  # Dictionary to hold positions of rooms
    connections = {room: 0 for room in rooms}

    for room in rooms:
        G.add_node(room)
        pos[room] = room.center  # Assigning position to each room node

    for room in rooms:
        potential_connections = sorted(
            [other_room for other_room in rooms if other_room != room],
            key=lambda x: math.sqrt((room.center[0] - x.center[0]) ** 2 + (room.center[1] - x.center[1]) ** 2)
        )
        for other_room in potential_connections:
            if connections[room] < max_connections_per_room and connections[other_room] < max_connections_per_room:
                G.add_edge(room, other_room, weight=round(math.hypot(room.center[0] - other_room.center[0], room.center[1] - other_room.center[1])))
                connections[room] += 1
                connections[other_room] += 1
            if connections[room] >= max_connections_per_room:
                break

    return G, pos
```

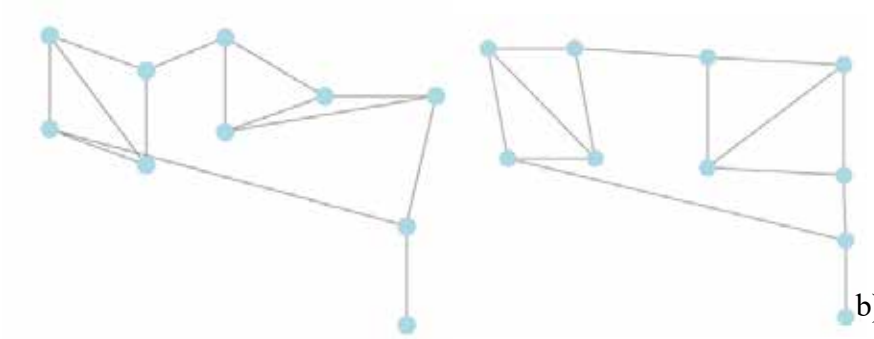
Fig. 9. Functions from BSP implementation: build_graph

```python
def draw_graph(G, pos):
    nx.draw(G, pos, with_labels=False, node_size=300, node_color='lightblue', edge_color='gray')
    nx.draw_networkx_edges(G, pos, edge_color='gray')
    plt.show()
```

Fig. 10. The draw_graph function

```python
initial_room = Room(0, 0, 100, 100)
max_splits = 5
max_connections_per_room = 3
rooms = create_rooms(initial_room, 10, max_splits)
G, pos = build_graph(rooms, max_connections_per_room)
draw_graph(G, pos)
```

Fig. 11. Running and visualization of the algorithm



a) b)

Fig. 12. The first result (a) and second result (b) of the BSP algorithm

data of the algorithm in a standardized format – for example, JSON.

API defines a set of interaction rules between software components, ensuring their compatibility and efficient data exchange. To create it, without complicating the basic code of the project, you can use the Flask web framework. It is designed for building simple web applications using the Python language. This tool is minimalistic, modular and scalable. The structure of the Flask program includes routing of URL requests, processing of HTTP methods (GET, POST, PUT, DELETE). It allows you to efficiently create RESTful APIs with CRUD functionality (create, read, update, delete data).

To begin with, let's create a simple server with the GET method to retrieve data from the graph. The implementation of the web server is shown in Figure 13. Here we import the necessary modules and then create a Flask instance. We leave the Generate_graph function unchanged.

Next, we define the route /graph/<int:num_nodes>/<int:num_edges> with the HTTP GET method. In this function, we will generate a graph using generate_graph. Then we convert it into node-link format using nx.node_link_data and return the result in JSON format using jsonify.

To run the program, execute the command python simple_graph.py in the terminal. As a trace, we get the JSON object of the graph by sending a GET request to «http://localhost:5000/graph/<num_nodes>/<num_edges>», where <num_nodes> and <num_edges> are replaced with the desired numbers.

For example, a query for «http://localhost:5000/graph/3/3» will return a graph JSON object with 3 nodes and 3 edges. The result of executing such a request is shown in Figure 14.

In this implementation, the placement of objects is not detailed, which opens perspectives for the development of a web server adapted to the specific requirements of users.

Similar to this implementation of the algorithm, other algorithms can be created to obtain similar graph structures. The next example of the implementation of the API for receiving data will create a server with a GET request to receive the results of generation according to the BSP (Binary Space Partitioning) algorithm. The implementation is described Figure 15.

```python
@app.route('/generate_graph', methods=['GET'])
def generate_graph():
    initial_room = Room(0, 0, 100, 100)
    max_splits = 5
    max_connections_per_room = 3
    rooms = create_rooms(initial_room, 10, max_splits)
    G, pos = build_graph(rooms, max_connections_per_room)

    nodes = [{'id': str(node), 'x': pos[node][0], 'y': pos[node][1]} for node in G.nodes]
    edges = [{'source': str(u), 'target': str(v), 'weight': G.edges[u, v]['weight']} for u, v in G.edges]
    graph_data = {'nodes': nodes, 'edges': edges}

    return jsonify(graph_data)

if __name__ == '__main__':
    app.run(debug=True)
```

Fig. 13. Web server route to receive BSP generation results


```
{
    "directed": false,
    "graph": {},
    "links": [
        {
            "source": 0,
            "target": 2
        },
        {
            "source": 0,
            "target": 1
        },
        {
            "source": 1,
            "target": 2
        }
    ],
    "multigraph": false,
    "nodes": [
        {
            "id": 0
        },
        {
            "id": 1
        },
        {
            "id": 2
        }
    ]
}
```


Fig. 14. The result of the request to receive graph data


```python
@app.route('/generate_graph', methods=['GET'])
def generate_graph():
    initial_room = Room(0, 0, 100, 100)
    max_splits = 5
    max_connections_per_room = 3
    rooms = create_rooms(initial_room, 10, max_splits)
    G, pos = build_graph(rooms, max_connections_per_room)

    nodes = [{'id': str(node), 'x': pos[node][0], 'y': pos[node][1]} for node in G.nodes]
    edges = [{'source': str(u), 'target': str(v), 'weight': G.edges[u, v]['weight']} for u, v in G.edges]
    graph_data = {'nodes': nodes, 'edges': edges}

    return jsonify(graph_data)

if __name__ == '__main__':
    app.run(debug=True)
```


Fig. 15. Web server route to receive BSP generation results

In this example, we create a Flask server with a single route /generate_graph. When executing a request with this route, the server generates a graph using the create_rooms and build_graph functions. It then converts the graph to JSON format using list inclusions. Graph nodes are

represented as dictionaries with id, x, and y keys, and edges are represented as dictionaries with source, target, and weight keys. The result of the generation is the edge and nodes arrays. «Edge» array has objects of type { «source»: string, target: string, weight: number}. The «Node» array has objects of type {«id»: string, x: float, y: float}. We return the received graph data in JSON format using the jsonify function from Flask.

Conclusions. In conclusion, among the main vectors for further development of the project, optimization for more complex and branched graph structures for the purpose of detailed modeling of the game world should be highlighted. Achieving this goal will require improving algorithmic solutions that provide greater flexibility in settings and optimization for working with large and complex graph data structures. In addition, the issue of integration with game engines is critical, which will optimize the development process for the specific context of game engines and speed up overall development cycles.

To successfully complete these tasks, it is necessary to consider various optimization methods, such as the use of more efficient search and data processing algorithms, as well as the use of modern technologies that reduce computational costs. Integration with game engines requires close collaboration with the engine development teams and a deep understanding of their architecture and capabilities. It is also important to pay attention to user experience, developing intuitive interfaces and tools, improving documentation and providing training materials.

The support of the developer community plays a key role in the successful development of the project. An active and engaged community can significantly speed up the development process by facilitating the sharing of experiences, suggestions for improvements, and collaborative problem solving. Regular meetings, webinars and conferences dedicated to discussing the current status of the project and plans for the future will facilitate this process.

Thus, the successful development of the project requires an integrated approach, including optimization of graph structures, integration with game engines, improvement of user experience and active support of the developer community. This is the only way to achieve your goals and create an innovative product that can change the approach to game development and modeling of game worlds.

BIBLIOGRAPHY:

1. Xia F., Liu J., Nie H., Fu Y., Wan L. and Kong X. «Random Walks: A Review of Algorithms and Applications» in IEEE Transactions on Emerging Topics in Computational Intelligence, April 2020, Volume 4, No. 2, pp. 95–107, doi: 10.1109/TETCI.2019.2952908.

2. Fan X., Li B., Sisson S. The binary space partitioning-tree process. International Conference on Artificial Intelligence and Statistics, March 2018, PMLR, pp. 1859–1867.

3. Ehrhardt G. The not-so-random Drunkard's walk, Journal of Statistics Education, 2013, vol. 21, no. 2, doi: 10.1080/10691898.2013.11889679.

4. Hendrikx M., Meijer S., Van Der Velden, J., Iosup A. Procedural content generation for games: a survey, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 2013, vol. 9, no. 1, p. 1–22.

5. Koesnaedi A., Istiono W. Implementation drunkard's walk algorithm to generate random level in roguelike games. International Journal of Multidisciplinary Research and Publications, 2022, vol. *5*, no. 2, p. 97–103.

6. Shaker N., Togelius J., Nelson M. J. Procedural content generation in games, 2016.

7. Togelius J., Kastbjerg E., Schedl D., Yannakakis G. N. What is procedural content generation? Mario on the borderline. Proceedings of the 2nd international workshop on procedural content generation in games, June 2011, pp. 1–6.

8. Cóth C. D. Binary space partitions: recent developments. Combinatorial and Computational Geometry, 2005, vol. 52, p. 525–552.

9. Van Der Linden R., Lopes R., Bidarra R. Procedural generation of dungeons. IEEE Transactions on Computational Intelligence and AI in Game*s*, 2013, vol. *6,* no. 1, p. 78–89.

REFERENCES:

1. Xia, F., Liu, J., Nie, H., Fu, Y., Wan, L. and Kong, X. (2020). «Random Walks: A Review of Algorithms and Applications» in IEEE Transactions on Emerging Topics in Computational Intelligence, April 2020, Volume 4, No. 2, pp. 95–107, doi: 10.1109/TETCI.2019.2952908 [in English].

2. Fan, X., Li, B., & Sisson, S. (2018). The binary space partitioning-tree process. International Conference on Artificial Intelligence and Statistics, March 2018, PMLR, pp. 1859–1867 [in English].

3. Ehrhardt, G. (2013). The not-so-random Drunkard's walk, Journal of Statistics Education, vol. 21, no. 2, doi: 10.1080/10691898.2013.11889679 [in English].

4. Hendrikx, M., Meijer, S., Van Der Velden, J., & Iosup, A. (2013). Procedural content generation for games: a survey, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 9, no. 1, p. 1–22 [in English].

5. Koesnaedi, A., & Istiono, W. (2022). Implementation drunkard's walk algorithm to generate random level in roguelike games. International Journal of Multidisciplinary Research and Publications, vol. *5*, no. 2, p. 97–103. [in English].

6. Shaker, N., Togelius, J., & Nelson, M. J. (2016). Procedural content generation in games [in English].

7. Togelius, J., Kastbjerg, E., Schedl, D., & Yannakakis, G. N. (2011). What is procedural content generation? Mario on the borderline. Proceedings of the 2nd international workshop on procedural content generation in games, June 2011, pp. 1–6 [in English].

8. Cóth, C. D. (2005). Binary space partitions: recent developments. Combinatorial and Computational Geometry, vol. 52, p. 525–552 [in English].

9. Van Der Linden, R., Lopes, R., & Bidarra, R. (2013). Procedural generation of dungeons. *IEEE* Transactions on Computational Intelligence and AI in Games, vol. *6,* no. 1, p. 78–89 [in English].

УДК 004.056.53(045)
DOI https://doi.org/10.32782/IT/2024-3-9

Анна КОРЧЕНКО
доктор технічних наук, професор, професор кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005
***ORCID:** 0000-0003-0016-1966*
***Scopus Author ID:** 56029291400*

Сергій МАЦЮК
кандидат технічних наук, доцент, доцент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005, matsiuk.s.m@nmu.one
***ORCID:** 0000-0001-6798-5500*
***Scopus Author ID:** 57189702975*

Кирило ДАВИДЕНКО
аспірант кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005
***ORCID:** 0009-0001-9209-1274.*

Бібліографічний опис статті: Корченко, А., Мацюк С., Давиденко, К. (2024). Огляд сучасних методів та засобв виявлення соціотехнічних атак. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 88–96, doi: https://doi.org/10.32782/IT/2024-3-9

ОГЛЯД СУЧАСНИХ МЕТОДІВ ТА ЗАСОБВ ВИЯВЛЕННЯ СОЦІОТЕХНІЧНИХ АТАК

Актуальність. *Стрімкий розвиток інформаційних технологій та інтенсивний обмін даними суттєво змінюють сучасне середовище кібербезпеки, створюючи нові загрози у вигляді кібератак та шахрайства. Особливу небезпеку становлять соціотехнічні атаки, які використовують психологічні маніпуляції для отримання конфіденційної інформації або доступу до захищених систем.* ***Мета.*** *З огляду на це, метою роботи є комплексний огляд існуючих рішень, технологій і методів, які можуть допомогти організаціям та приватним користувачам у боротьбі з соціотехнічними загрозами.* ***Методологія.*** *У статті проведено дослідження сучасних методів виявлення соціотехнічних атак, що використовують маніпулятивні техніки. Розглянуті різні підходи до детектування відповідних атак, включаючи сигнатурні, поведінкові, методи машинного навчання, аналіз метаданих, а також соціальні та психологічні підходи. Особливу увагу приділено інтерактивним і симуляційним методам, які дозволяють організаціям перевіряти свою готовність до атак шляхом моделювання реальних умов.* ***Наукова новизна.*** *Описані апаратні та програмні засоби за дев'ятьма критеріями (високий рівень захисту, централізоване управління, простота використання, інтеграція з іншими платформами, штучний інтелект, адаптивність, можливості роботи в офлайн-режимі, висока вартість, складність налаштування) для виявлення та блокування соціотехнічних атак, які надають багаторівневий захист від соціотехнічних загроз.* ***Висновки.*** *Отримані результати показують, що освітні та організаційні заходи залишаються ключовими для підвищення обізнаності користувачів та зменшення ризику успішних атак, а сучасні підходи до захисту від соціотехнічних загроз мають бути комплексними і включати як технічні рішення, так і навчання персоналу. Також є важливим, постійне вдосконалення існуючих заходів забезпечення безпеки і впровадження новітніх технологій для підвищення ефективності захисту інформаційних систем від соціотехнічних атак.*

Ключові слова: *кібербезпека, інформаційна безпека, соціальний інжиніринг, соціотехнічні атаки, методи соціотехнічних атак, класифікація соціотехнічних атак.*

Anna KORCHENKO
Doctor of Technical Sciences, Professor, Professor at the Department of Information Security and Telecommunications, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005,annakor@ukr.net
***ORCID:** 0000-0003-0016-1966*
***Scopus Author ID:** 56029291400*

Sergii MATSIUK
Assistant Professor at the Department of Information Security and Telecommunications, National Technical University Dnipro Polytechnic, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, matsiuk.s.m@nmu.one
ORCID: *0000-0001-6798-5500*
Scopus Author ID: *57189702975*

Kyrylo DAVYDENKO
Postgraduate Student at the Department of Information Security and Telecommunications, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, kirilldavy@gmail.com
ORCID: *0009-0001-9209-1274*

To cite this article: Korchenko, A, Matsiuk S., Davydenko, K. (2024). Ohliad suchasnykh metodiv ta zasobv vyiavlennia sotsiotekhnichnykh atak [Overview of modern methods and means of detecting of sociotechnical attacks]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 88–96, doi: https://doi.org/10.32782/IT/2024-3-9

OVERVIEW OF MODERN METHODS AND MEANS OF DETECTING OF SOCIOTECHNICAL ATTACKS

Relevance. *The rapid development of information technology and intensive data exchange are significantly changing the modern cybersecurity environment, creating new threats in the form of cyberattacks and fraud. Socio-technical attacks that use psychological manipulation to obtain confidential information or access to secure systems are particularly dangerous.* ***Objective.*** *Given this, the purpose of this paper is to provide a comprehensive review of existing solutions, technologies, and methods that can help organizations and private users combat sociotechnical threats.* ***Methodology.*** *The article studies modern methods of detecting sociotechnical attacks that use manipulative techniques. Various approaches to detecting such attacks are considered, including signature, behavioral, machine learning, metadata analysis, as well as social and psychological approaches. Particular attention is paid to interactive and simulation methods that allow organizations to test their preparedness for attacks by simulating real-world conditions.* ***Scientific novelty.*** *Hardware and software tools are described according to nine criteria (high level of protection, centralized management, ease of use, integration with other platforms, artificial intelligence, adaptability, offline capabilities, high cost, complexity of configuration) to detect and block sociotechnical attacks, which provide multi-level protection against sociotechnical threats.* ***Conclusions.*** *The findings show that educational and organizational measures remain key to raising user awareness and reducing the risk of successful attacks, and modern approaches to protecting against sociotechnical threats should be comprehensive and include both technical solutions and staff training. It is also important to continuously improve existing security measures and introduce the latest technologies to increase the effectiveness of protecting information systems from sociotechnical attacks.*

Key words: *cyber security, information security, social engineering, sociotechnical attacks, sociotechnical attack methods, classification of sociotechnical attacks.*

У сучасному кіберпросторі соціотехнічні атаки становлять одну з найбільших загроз для інформаційної безпеки організацій і приватних осіб. Соціотехнічні атаки, що включають фішинг, підробку особистих даних і інші маніпулятивні техніки, намагаються експлуатувати людську психологію для отримання несанкціонованого доступу до конфіденційної інформації та інших ресурсів. З огляду на стрімкий розвиток технологій і зростання кіберзагроз, ефективні методи детектування цих атак стали критично важливими для забезпечення безпеки інформаційних систем.

Актуальність дослідження сучасних методів детектування соціотехнічних атак підтверджується численними публікаціями та дослідженнями, що підкреслюють їх важливість у боротьбі з кіберзагрозами. Зокрема, вчені акцентують увагу на необхідності інтеграції новітніх технологій, таких як штучний інтелект і машинне навчання, для покращення ефективності систем безпеки. Інші джерела також зазначають, що існуючі методи потребують постійного вдосконалення та адаптації до нових тактик, використовуваних кіберзлочинцями.

Методи та засоби виявлення соціотехнічних атак є ключовими елементами захисту інформаційних систем та організацій від маніпуляцій, що спрямовані на людський чинник.

Виявлення соціотехнічних атак є складним завданням через їх орієнтацію на маніпулювання людською поведінкою, а не на прямий технічний вплив. Методи виявлення зазначених атак поділяються на кілька категорій, зокрема: технічні, поведінкові, аналітичні та освітні.

Метою статті є комплексний огляд існуючих рішень, технологій і методів, які можуть допомогти організаціям та приватним користувачам у боротьбі з соціотехнічними загрозами. Розуміння сучасних методів детектування дозволить знизити ризики, пов'язані з кіберзлочинністю, та покращити загальний рівень інформаційної безпеки.

Задача роботи полягає в огляді сучасних методів та засобів детектування соціотехнічних атак, а також у аналізі їх ефективності та обмежень. Пропонується розглянути різноманітні підходи, зокрема технології на основі штучного інтелекту, системи моніторингу та реагування, а також інтерактивні та симуляційні методи.

Далі розглянемо основні методи, які використовуються для виявлення соціотехнічних атак.

Сигнатурні методи базуються на створенні баз даних сигнатур (шаблонів) відомих атак, які порівнюються з вхідною інформацією, наприклад, антивірусні програми або системи виявлення вторгнень (IDS), які шукають специфічні моделі поведінки. Такі методи швидко виявляють відомі загрози, але є неефективними щодо нових або модифікованих атак (А. Корченко, 2019; Scarfone K., 2007).

Поведінкові методи (аналіз поведінки користувачів) направлені на виявлення відхилень у поведінці користувачів або систем, які можуть свідчити про соціотехнічну атаку. Це системи, що відстежують нетипову активність у мережі, наприклад, неочікувані запити на зміну пароля, спроби доступу до конфіденційних даних, раптові зміни в шаблонах роботи користувачів або незвичайні запити до серверів. Такі методи можуть виявити невідомі атаки або атаки, що змінюють поведінку, але вони мають високий рівень хибно позитивних спрацьовувань (Hee-Yong Kwon, 2022).

Методи машинного навчання та штучного інтелекту використовують класифікаційні моделі або нейронні мережі для прогнозування можливих атак на основі аналізу минулих інцидентів. Застосовують алгоритми машинного навчання для аналізу великих обсягів даних та пошуку аномалій або небезпечних патернів. Також, мають здатність до самонавчання і виявлення складних атак, що може бути недоступним для інших методів. Але зазначені методи потребують велику кількості даних для навчання, що спричиняє можливість появи хибних спрацьовувань (Hee-Yong Kwon, 2022; Moustafa N., 2019).

Контекстуальні методи базуються на аналізі контексту взаємодій і комунікацій, таких як аналіз змісту повідомлень електронної пошти, соціальних мереж, телефонних розмов тощо. Відповідні методи включають аналітичні інструменти для перевірки достовірності повідомлень і виявлення підозрілих або шахрайських комунікацій. Вони можуть ідентифікувати соціотехнічні атаки, такі як фішинг або шахрайство, але потребують складних алгоритмів для точного аналізу контенту і часто залежать від контексту застосування (Kisiel J., 2018).

Методи аналізу метаданих базуються на аналізі адрес електронної пошти, IP-адрес, шаблонів дзвінків та інших сигналів, які можуть вказувати на підозрілу активність, також орієнтовані на виявлення підроблених електронних листів шляхом аналізу метаданих повідомлень. Вони допомагають у швидкому виявленні несанкціонованих або підроблених комунікацій, але не завжди можуть бути точними, наприклад, якщо метадані підробляються (Кузьма К., 2017).

Соціальні та психологічні методи базуються на оцінці психологічних та соціальних аспектів поведінки працівників, що можуть бути використані зловмисниками для реалізації атак. Також, вони використовують опитування та соціальну інженерію для виявлення співробітників, які можуть бути більш вразливими до маніпуляцій. Дозволяють розпізнати потенційні уразливості, пов'язані з людським чинником але мають труднощі у вимірюванні психологічних показників та потребують необхідності у регулярному оновленні знань (Kevin D., 2003; Rahman T., 2021).

Методи на основі аналізу соціальних мереж направлені на виявлення шахрайських облікових записів або підозрілих повідомлень, що спрямовані на збір персональних даних. Також, включають аналіз поведінки користувачів у соціальних мережах для виявлення соціотехнічних атак, таких як фішинг або соціальні маніпуляції. Вони дозволяють ефективно аналізувати широкі потоки інформації у відкритих джерелах але працюють з великою кількістю даних і мають труднощі у відслідковуванні всіх можливих джерел (Войтович О.П., 2023).

Освітні та організаційні методи орієнтовані на навчання співробітників і користувачів щодо виявлення соціотехнічних атак та способів їх уникнення. Проводяться навчання співробітників, щодо розпізнавання ознак фішингових атак або інших типів шахрайства. В результаті їх використання зменшуються ризики реалізації атак через підвищення обізнаності користувачів але вони залежать від постійної підтримки та оновлення знань (Cyber.academy, 2024).

Інструменти моніторингу та реагування складаються з технічних рішень, які забезпечують безперервний моніторинг систем для виявлення підозрілої активності та негайного реагування. До них відносяться системи SIEM (Security Information and Event Management), які аналізують журнали подій у режимі реального часу. Вони мають високу оперативність виявлення атак, але потребують значних ресурсів для обробки значних обсягів даних (González-Granadillo G., 2021).

Інтерактивні та симуляційні методи (соціальна інженерія через симуляцію атак) використовують симуляції для створення довкілля, де проводяться тренування та тести для виявлення соціотехнічних атак, наприклад, проведення «фішингових тестів» для співробітників компанії або надсилання фальшивих фішингових листів для оцінки того, скільки працівників переходять за посиланням чи вводять свої облікові дані. Мають можливість оцінки реальної готовності організації до протидії атакам, а також значний ризик хибних висновків, якщо симуляції не відображають реальних умов (Bamanga Ahmad M., 2023; Forbes Advisor, 2024).

Ці методи часто використовуються в комбінації для підвищення ефективності та створення багаторівневої системи захисту від соціотехнічних атак, оскільки вони спрямовані на виявлення як технічних, так і людських аспектів цих загроз.

Існує низка програмних і апаратних засобів для виявлення та блокування соціотехнічних атак, які використовуються для захисту від кіберзагроз, таких як фішинг, спуфінг, маніпуляції та інші види атак, що враховують людський чинник.

Далі, порведемо огляд програмних та апаратних засобів для виявлення та блокування соціотехнічних атак.

Програмні засоби

1. Proofpoint – це комплексне рішення для захисту електронної пошти та запобігання фішинговим атакам, спаму та компрометації електронної пошти. Виявляє та блокує фішингові атаки, спуфінг, шкідливі вкладення та URL-адреси, а також забезпечує навчання користувачів для підвищення обізнаності про кіберзагрози (Proofpoint, 2024).

Перевагами зазначеного рішення є високий рівень захисту, що включає використання машинного навчання для виявлення фішингових атак та спроб компрометації електронної пошти. Має централізоване управління і пропонує єдину панель для управління безпекою електронної пошти та іншими загрозами. Забезпечує глибокий аналіз загроз з детальними звітами.

При розгляді **недоліків** proofpoint необхідно зауважити, що рішення потребує значних зусиль для початкового налаштування та інтеграції з існуючими системами, а також має високу вартість, що може бути проблемою для невеликих організацій.

2. Mimecast – це хмарна платформа, яка забезпечує багаторівневий захист електронної пошти, включаючи захист від фішингу, спаму, шкідливих програм, соціотехнічних атак **та** включає виявлення компрометації електронної пошти (Mimecast, 2024).

Її **перевагами** є інтуїтивно зрозумілий інтерфейс та легка інтеграція з іншими платформами. Ця платформа доступна з будь-якого місця, що забезпечує її гнучкість (має хмарне рішення). Також, добре зарекомендувала себе у виявленні та блокуванні загроз, пов'язаних з електронною поштою.

До **недоліків** можна віднести – залежність від інтернет з'єднання. Оскільки Mimecast це хмарна платформа, для її роботи потрібен стабільний інтернет. Також, вона має **о**бмежені можливості в офлайн-режимі, тобто не має можливості забезпечити повний захист, якщо підключення до інтернету відсутнє.

3. PhishMe (Cofense) – це платформа для навчання та симуляцій фішингових атак. Навчає співробітників розпізнавати фішингові атаки за допомогою реалістичних симуляцій, а також допомагає виявляти та реагувати на реальні загрози (Cofense, 2024).

Переваги платформи пов'язані з можливістю навчання персоналу, що підвищує обізнаність співробітників про фішингові атаки через регулярні симуляції. Створює фішингові сценарії, які відповідають реальним загрозам. Також, надає детальні звіти про реакцію співробітників на симуляції, що допомагає визначити слабкі місця.

До **недоліків** можні віднести, той факт, що платформа більше орієнтована на навчання, а не на безпосередній захист, а також занадто часті симуляції можуть призвести до «втоми від навчання», коли співробітники почнуть ігнорувати попередження.

4. KnowBe4 – це хмарна платформа для навчання кібербезпеці. Вона пропонує навчальні програми та симуляції соціотехнічних атак, включаючи фішинг, спуфінг та інші методи соціальної інженерії (KnowBe4, 2024).

Серед **переваг** можна виділити наявний широкий спектр тренінгів та симуляцій, що

охоплюють різні типи соціотехнічних атак. **Є** аналіз ефективності, який включає можливість відстеження прогресу співробітників і їхню здатність розпізнавати загрози. Платформа дозволяє адаптувати навчальні програми відповідно до потреб організації.

До **недоліків** можна віднести високу вартість для великих організацій з значною кількістю співробітників. А також, ефективність залежить від активної участі співробітників у навчанні.

5. Barracuda Sentinel – це рішення для захисту електронної пошти, яке використовує штучний інтелект для виявлення фішингових атак, спуфінгу та компрометації електронної пошти у реальному режимі часу (Barracuda, 2024).

Серед **переваг** можна виділити легку інтеграцію з хмарними сервісами Microsoft, що робить його зручним для організацій, які використовують цю платформу. Використання штучного інтелекту, дозволяє автоматично виявляти і блокувати загрози в реальному режимі часу. Також, є можливість виявлення атак на ранніх стадіях, запобігаючи їх поширенню.

До **недоліків** можна віднести залежність від Microsoft 365, тобто відповідне рішення оптимально працює тільки в зазначеному довкіллі, а користувачі інших платформ можуть не отримати всі переваги цього рішення.

6. **Microsoft Defender for Office 365** – це платформа для захисту від фішингу, шкідливих програм, шкідливих URL-адрес та компрометації електронної пошти, інтегрована в екосистему Microsoft (Microsoft, 2024).

До **переваг** можна віднести глибоку інтеграцію з продуктами Microsoft, що дозволяє забезпечити всебічний захист. Платформа використовує різні механізми виявлення загроз, включаючи захист від фішингу та шкідливих програм. Пропонує автоматизовані засоби для виявлення та реагування на загрози.

До **недоліків** можна віднести значну вартість, а повний захист, буде доступний лише у вищих планах підписки Microsoft 365, що може бути дорого для невеликих підприємств. Також є **з**алежність від екосистеми Microsoft, тобто оптимальне функціонування можна отримати тільки в межах Microsoft, що може обмежити його використання іншими користувачами.

7. **Mandiant ATP (advanced threat protection)** – це програмне рішення для виявлення, аналізу та реагування на складні кіберзагрози, здатне детектувати деякі аспекти соціотехнічних атак, але з певними обмеженнями. Це рішення використовує потужні інструменти для аналізу загроз, включаючи технології машинного навчання, розвідку загроз, та аналіз подій безпеки, а також може допомагати виявляти ознаки соціотехнічних атак, таких як фішинг, через аналіз поведінки користувачів і моніторинг мережевого трафіку (Mandiant, 2024).

Mandiant ATP працює як хмарне або локальне програмне забезпечення, яке можна інтегрувати в існуючі системи безпеки підприємства. Воно надає комплексний набір функцій для виявлення та реагування на кібератаки, включаючи аналіз поведінки, розслідування інцидентів, та забезпечення відповідності стандартам безпеки.

Серед **переваг** Mandiant ATP виділяють легкість інтегруватися з іншими продуктами безпеки, такими як SIEM або інші засоби управління інцидентами, що робить його частиною загальної стратегії кібербезпеки. Має глобальну базу даних загроз, яка постійно оновлюється, що дозволяє виявляти нові та змінювані загрози в режимі реального часу. Програмне рішення використовує передові технології, такі як машинне навчання і поведінковий аналіз, щоб ідентифікувати складні загрози, які можуть залишатися непоміченими іншими системами. Mandiant надає доступ до команди експертів, які можуть допомогти у випадку великих інцидентів, а також проводити аудит безпеки та навчання персоналу.

До **недоліків** можна віднести достатньо високу вартість, складність налаштування та використання, що вимагає високого рівня технічної обізнаності фахівців, залежність від зовнішньої інфраструктури, а також потребує значних обчислювальних ресурсів для аналізу даних, що може вплинути на продуктивність інших систем в організації.

Програмні засоби, такі як Proofpoint, Mimecast, PhishMe (Cofense), KnowBe4, Barracuda Sentinel, і Microsoft Defender for Office 365, Mandiant, пропонують комплексний захист від соціотехнічних атак, включаючи фішинг, спам, шкідливі програми та компрометацію електронної пошти. Вони використовують різні підходи, від машинного навчання і штучного інтелекту до навчання та симуляцій, для виявлення та запобігання загрозам. Хоча ці рішення мають свої переваги, такі як високий рівень захисту та інтуїтивно зрозумілі інтерфейси, їх вартість і залежність від специфічних платформ можуть бути обмеженням для деяких організацій.

Апаратні та апаратно-програмні засоби

1. Cisco Secure Email Gateway (раніше IronPort) – це апаратний шлюз для захисту

електронної пошти. Захищає корпоративну пошту від фішингових атак, спаму, шкідливих програм та інших загроз. Використовує багаторівневий захист для фільтрації вхідної та вихідної пошти (Cisco, 2024).

Серед **переваг** можна виділити високий рівень захисту, який ефективно захищає від складних фішингових атак і шкідливого програмного забезпечення, а також може фільтрувати вміст за різними параметрами, що підвищує загальний рівень безпеки. Засіб є **і**нтегрований з іншими продуктами Cisco та забезпечує гнучкість і ефективність у комплексних рішеннях безпеки.

До **недоліків** можна віднести складність налагодження та супроводу, що вимагає спеціальних знань для налаштування та підтримки. Також, має високу вартість, що може бути дорогим рішенням, особливо для малих і середніх компаній.

2. Palo Alto Networks WildFire – це апаратно-програмний комплекс для захисту від шкідливого програмного забезпечення. Виявляє та блокує шкідливе програмне забезпечення. Використовує технології глибокого аналізу трафіку та машинного навчання для виявлення загроз (Paloaltonetworks, 2024).

Серед **переваг є** використання машинного навчання, що дозволяє швидко ідентифікувати нові загрози. Має інтеграцію з іншими продуктами Palo Alto Networks, що в свою чергу при комплексному використанні забезпечує цілісну систему захисту. Здатен постійно вдосконалюватися завдяки вбудованому механізму самонавчання.

Серед **недоліків** можна виділити високу вартість, тобто є одним з найдорожчих рішень на ринку, а також має високу ресурсоємність, що потребує значних обчислювальних ресурсів для роботи.

3. SonicWall Email Security – це апаратне (або програмне) рішення для захисту та фільтрації електронної пошти, яке встановлюються в мережі і забезпечує захист від фішингових атак, спаму, шкідливих програм та інших загроз, пов'язаних з електронною поштою (SonicWall, 2024). Загалом, SonicWall Email Security пропонує рішення для захисту електронної пошти як у вигляді фізичних пристроїв, так і у вигляді програмних рішень, що дає можливість організаціям вибрати найбільш відповідний варіант для їхніх потреб.

До **переваг** цього рішення можна віднести інтуїтивно зрозумілий інтерфейс та простоту налаштування, високу продуктивність і точність фільтрації електронної пошти, інтеграцію з іншими рішеннями SonicWall для комплексного захисту.

Серед **недоліків** виділяють обмежену функціональність у порівнянні з конкурентами, а також вимагає фізичного простору і обладнання для розгортання і може потребувати обслуговування.

4. FortiGate пропонується у вигляді спеціалізованих пристроїв (апаратних брандмауерів), які можна встановити в мережі для забезпечення захисту від загроз. Ці пристрої виконують функції брандмауера, VPN, IPS/IDS, вебфільтрації та багато інших завдань у режимі реального часу.

Fortinet FortiMail – це апаратний шлюз для захисту електронної пошти. Забезпечує захист від фішингу, спаму та інших загроз, пов'язаних із електронною поштою. Використовує багатошарові механізми виявлення (Fortinet, 2024).

До **переваг** можна віднести ефективну фільтрацію та високу ефективність у виявленні та блокуванні небажаних повідомлень. Наявний широкий набір функцій, включаючи антивірусну перевірку, контроль спаму та інші засоби безпеки. Є можливість інтеграції **з** Fortinet Security Fabric, що в комплексному застосуванні підвищує загальний рівень безпеки, інтегруючись із іншими продуктами Fortinet.

Недоліки повязані зі складністю управління, що потребує належного налаштування та підтримки висококваліфікованими спеціалістами. Має обмежену масштабованість, що може бути менш ефективним для великих організацій із значною кількістю користувачів.

5. Sophos XG Firewall – це мережевий брандмауер, який захищає мережу від різних типів атак, включаючи фішинг і соціотехнічні загрози. Використовує глибокий аналіз трафіку та можливості захисту від загроз в режимі реального часу (News.sophos, 2024).

Серед **переваг** виділяють простоту використання та Інтуїтивно зрозумілий інтерфейс і зручність налаштування. Є інтегрована система безпеки яка об'єднує різні засоби захисту в єдиному рішенні. Також, є можливість отримання детальних звітів про загрози та активність в мережі.

До **наявних** недоліків можна віднести обмеження в налаштуванні, тобто засіб **є** менш гнучкий у порівнянні з деякими іншими рішеннями на ринку, а для отримання повного спектра функцій необхідно регулярно оновлювати підписки.

Апаратні засоби, такі як Cisco Secure Email Gateway, Palo Alto Networks WildFire, SonicWall Email Security, Fortinet FortiMail та Sophos XG

Таблиця 1

Порівняльна таблиця засобів виявлення та блокування соціотехнічних атак

№	Засіб	Критерії								
		Високий рівень захисту	Централізоване управління	Простота використання	Інтеграція з іншими платформами	Штучний інтелект	Адаптивність	Можливості роботи в офлайн-режимі	Висока вартість	Складність налаштування
1	Proofpoint	+	+	-	+	+	-	-	+	+
2	Mimecast	+	-	+	+	-	-	-	-	-
3	PhishMe (Cofense)	-	-	-	-	-	+	+	-	-
4	KnowBe4	-	-	-	-	-	+	+	+	-
5	Barracuda Sentinel	+	-	-	+	+	-	-	-	-
6	Microsoft Defender for Office 365	+	+	+	+	+	+	-	+	-
7	Mandiant ATP	+	+	-	+	+	+	-	+	+
8	Cisco Secure Email Gateway	+	+	-	+	-	-	+	+	+
9	Palo Alto Networks WildFire	+	-	-	+	+	+	+	+	-
10	SonicWall Email Security	+	+	+	+	-	-	+	-	+
11	Fortinet FortiMail	+	+	-	+	-	-	+	+	+
12	Sophos XG Firewall	+	+	+	+	+	-	+	-	+

Firewall, є потужними інструментами для забезпечення безпеки, надають комплексний захист від різних загроз, включаючи фішинг, шкідливі програми, атаки соціальної інженерії та мережеві атаки. Вони використовують передові технології, такі як машинне навчання та багатошаровий аналіз, для виявлення і блокування загроз в режимі реального часу. Незважаючи на високу ефективність та інтеграцію з іншими рішеннями безпеки, ці засоби потребують значних інвестицій і спеціалізованих знань для налаштування та підтримки, що може бути викликом для малих та середніх підприємств.

Відповідно до проведеного аналізу в табл. 1 за дев'ятьма критеріями (високий рівень захисту, централізоване управління, простота використання, інтеграція з іншими платформами, штучний інтелект, адаптивність, можливості роботи в офлайн-режимі, висока вартість, складність налаштування) інтегровано характеристики розглянутих засобів де відображається наявність або відсутність переваг та недоліків у відповідних рішеннях («+» означає наявність певного аспекту в продукті, а «-» – його відсутність).

Висновки. Слід зазначити, що програмні засоби виявлення та блокування соціотехнічних атак, часто пропонують більшу гнучкість і легкість використання, але можуть бути обмеженими в офлайн-режимі та залежати від інтернет-з'єднання. Апаратні засоби, з іншого боку, надають більш надійний захист і можуть бути інтегровані з іншими мережевими рішеннями, але вимагають значних фінансових вкладень і складні в налаштуванні.

ЛІТЕРАТУРА:

1. Анна Корченко. Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019. 361 с.

2. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST). NIST Special Publication 800-94. 2007.

3. Hee-Yong Kwon. Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods. Hee-Yong Kwon, Taesic Kim, Mun-Kyu Lee. Electronics 2022, *Special Issue Real-Time Control of Embedded Systems*. Vol. 11(6), Pp 867. doi.org/10.3390/electronics11060867.

4. Moustafa N., Hu J. Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Evaluation. IEEE Access, 2019, Vol. 7, Pp. 104821–104845. URL: https://doi.org/10.1109/ACCESS.2019.2932754 (дата звернення: 21.08.2024).

5. Kisiel J., O'Neill D. Contextual Analysis for Secure Communication: A Survey. *Computers & Security*, 2018, Vol. 74, Pp. 172–191. URL: https://doi.org/10.1016/j.cose.2018.01.002 (дата звернення: 18.08.2024).

6. Кузьма К., Зівенко В. Аналіз методів фільтрації електронної пошти від спаму. *Геометричне моделювання та інформаційні технології*, Миколаїв, № 1 (3), 2017, стр. 84–89.

7. Kevin D. Mitnick, William L. Simon. The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons, 2003. Computers – 368 pages.

8. Rahman T., Rohan R., Pal D. Human Factors in Cybersecurity: A Scoping Review. *In* Proceedings of the 12th International Conference on Advances in Information Technology (IAIT 2021), Bangkok, Thailand. ACM. 2021. URL: https://doi.org/10.1145/3468784.3468789 (дата звернення: 18.08.2024).

9. Войтович О. П., Буда А. Г., Головенько В. О. Дослідження методів аналізу соціальних мереж як середовища інформаційних війн. Сучасні інформаційні технології. 2023, стр. 76–80.

10. Cyber.academy. Підвищуємо кіберобізнаність громадського сектору України (cyber.academy). URL: https://www.cyber.academy/post/cyber_awareness_public_sector-1 (дата звернення: 19.08.2024).

11. González-Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors 2021, Vol. 21, Pp. 4759. URL: https://doi.org/10.3390/s21144759 (дата звернення: 19.08.2024).

12. Bamanga Ahmad M., Ahmed Shehu M. Enhancing Phishing Awareness Strategy Through Embedded Learning Tools: A Simulation Approach. *Archives of Advanced Engineering Science*. 2023, Vol. XX. Pp. 1–14. DOI:10.47852/bonviewAAES32021392.

13. Forbes Advisor. Best Phishing Simulators To Prepare Employees And Defend Your Network. URL: https://www.forbes.com/advisor/business/best-phishing-simulators/ (дата звернення: 20.08.2024).

14. Proofpoint. Products. URL: https://www.proofpoint.com/us (дата звернення: 21.08.2024).

15. Mimecast. Our Platform. URL: https://www.mimecast.com (дата звернення: 21.08.2024).

16. PhishMe Cofense. Products. URL: https://cofense.com (дата звернення: 21.08.2024).

17. KnowBe4. Products+Pricing. URL: https://www.knowbe4.com (дата звернення: 21.08.2024).

18. Barracuda. Products. URL: https://www.barracuda.com/ (дата звернення: 21.08.2024).

19. Microsoft. Microsoft Defender for Office 365. URL: https://www.microsoft.com/en-gb/security/business/siem-and-xdr/microsoft-defender-office-365 (дата звернення: 21.08.2024).

20. Mandiant. Products. URL: https://www.mandiant.com (дата звернення: 22.08.2024).

21. Cisco. Configure Cisco Security Awareness Integration with Cisco Secure Email Gateway – Cisco. URL: https://www.cisco.com/c/en/us/support/docs/security/secure-email-gateway/220332-configure-cisco-security-awareness-integ.html (дата звернення: 22.08.2024).

22. Network security. Products. URL: https://www.paloaltonetworks.com/network-security/wildfire (дата звернення: 22.08.2024).

23. SonicWall. Products. URL: https://www.sonicwall.com/products/secure-email/cloud-email-security (дата звернення: 22.08.2024).

24. Fortinet. Products A–Z. URL: https://www.fortinet.com/products/email-securityт (дата звернення: 22.08.2024).

25. Sophos Firewall. Products and Services. URL: https://news.sophos.com/en-us/2020/02/18/xg-firewall-v18-is-now-available/ (дата звернення: 22.08.2024).

REFERENCES:

1. Korchenko, Anna. (2019). Metody identyfikatsii anomalnykh staniv dlia system vyiavlennia vtorhnen [Methods of identifying abnormal states for intrusion detection systems]. Monohrafiia, Kyiv, TsP «Komprynt», 361 s.

2. Scarfone, K., Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST). NIST Special Publication 800-94.

3. Hee-Yong, Kwon. (2022). Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods. Hee-Yong Kwon, Taesic Kim, Mun-Kyu Lee. Electronics. *Special Issue Real-Time Control of Embedded Systems*. Vol. 11(6), Pp 867. doi.org/10.3390/electronics11060867.

4. Moustafa, N., Hu, J. (2019). Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Evaluation. IEEE Access, Vol. 7, Pp. 104821–104845. Retrieved from: https://doi.org/10.1109/ACCESS.2019.2932754 (date of access: 21.08.2024).

5. Kisiel, J., O'Neill, D. (2018). Contextual Analysis for Secure Communication: A Survey. *Computers & Security*, Vol. 74, Pp. 172–191. Retrieved from: https://doi.org/10.1016/j.cose.2018.01.002 (date of access: 18.08.2024).

6. Kuzma, K., Zivenko, V. (2017). Analiz metodiv filtratsii elektronnoi poshty vid spamu [Analysis of email spam filtering methods]. Heometrychne modeliuvannia ta informatsiini tekhnolohii, Mykolaiv, № 1 (3), str. 84–89.

7. Kevin, D. Mitnick, William, L. Simon. (2003). The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons, Computers. 368 pages.

8. Rahman, T., Rohan, R., & Pal, D. (2021). Human Factors in Cybersecurity: A Scoping Review. *In* Proceedings of the 12th International Conference on Advances in Information Technology (IAIT 2021), Bangkok, Thailand. ACM. Retrieved from: https://doi.org/10.1145/3468784.3468789 (date of access: 18.08.2024).

9. Voitovych, O. P., Buda, A. H., Holovenko, V. O. (2023). Doslidzhennia metodiv analizu sotsialnykh merezh yak seredovyshcha informatsiinykh viin [Study of methods of analysis of social networks as an environment of information wars. Suchasni informatsiini tekhnolohii. str. 76–80.

10. Cyber.academy. Pidvyshchuiemo kiberobiznanist hromadskoho sektoru Ukrainy (cyber.academy). Retrieved from: https://www.cyber.academy/post/cyber_awareness_public_sector-1 (date of access: 19.08.2024).

11. González-Granadillo, G., González-Zarzosa, S., Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors. Vol. 21, Pp. 4759. Retrieved from: https://doi.org/10.3390/s21144759 (date of access: 19.08.2024).

12. Bamanga Ahmad, M., Ahmed Shehu, M. (2023). Enhancing Phishing Awareness Strategy Through Embedded Learning Tools: A Simulation Approach. *Archives of Advanced Engineering Science*. Vol. XX. Pp. 1–14. DOI:10.47852/bonviewAAES32021392.

13. Forbes Advisor. Best Phishing Simulators To Prepare Employees And Defend Your Network. Retrieved from: https://www.forbes.com/advisor/business/best-phishing-simulators/ (date of access: 20.08.2024).

14. Proofpoint. Products. Retrieved from: https://www.proofpoint.com/us (date of access: 21.08.2024).

15. Mimecast. Our Platform. Retrieved from: https://www.mimecast.com (date of access: 21.08.2024).

16. PhishMe Cofense. Products. Retrieved from: https://cofense.com (date of access: 21.08.2024).

17. KnowBe4. Products+Pricing. Retrieved from: https://www.knowbe4.com (date of access: 21.08.2024).

18. Barracuda. Products. Retrieved from: https://www.barracuda.com/ (date of access: 21.08.2024).

19. Microsoft. Microsoft Defender for Office 365. Retrieved from: https://www.microsoft.com/en-gb/security/business/siem-and-xdr/microsoft-defender-office-365 (date of access: 21.08.2024).

20. Mandiant. Products. Retrieved from: https://www.mandiant.com (date of access: 22.08.2024).

21. Cisco. Configure Cisco Security Awareness Integration with Cisco Secure Email Gateway – Cisco. Retrieved from: https://www.cisco.com/c/en/us/support/docs/security/secure-email-gateway/220332-configure-cisco-security-awareness-integ.html (date of access: 22.08.2024).

22. Network security. Products. Retrieved from: https://www.paloaltonetworks.com/network-security/wildfire (date of access: 22.08.2024).

23. SonicWall. Products. Retrieved from: https://www.sonicwall.com/products/secure-email/cloud-email-security (date of access: 22.08.2024).

24. Fortinet. Products A-Z. Retrieved from: https://www.fortinet.com/products/email-securityт (date of access: 22.08.2024).

25. Sophos Firewall. Products and Services. Retrieved from: https://news.sophos.com/en-us/2020/02/18/xg-firewall-v18-is-now-available/ (date of access: 22.08.2024).

УДК 004.8
DOI https://doi.org/10.32782/IT/2024-3-10

Олег КОБИЛІН
кандидат технічних наук, доцент, завідувач кафедри інформатики, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0000-0003-0834-0475*

Ірина ВЕЧІРСЬКА
кандидат технічних наук, доцент кафедри інформатики, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0000-0001-7964-2361*

Олексій КРАВЧЕНКО
аспірант кафедри інформатики, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
***ORCID:** 0009-0000-7999-1406*

Бібліографічний опис статті: Кобилін, О., Вечірська, І., Кравченко, О. (2024). Порівняння нейронних мереж типу RNN та LSTM. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 97–107, doi: https://doi.org/10.32782/IT/2024-3-10

ПОРІВНЯННЯ НЕЙРОННИХ МЕРЕЖ ТИПУ RNN ТА LSTM

Дослідження спрямоване на виявлення переваг і недоліків різних підходів до обробки послідовних даних, що є важливим аспектом у задачах обробки природної мови, таких як аналіз настроїв, машинний переклад та генерація тексту.

***Мета роботи.** Мета роботи полягає в дослідженні ефективності різних архітектур нейронних мереж для задачі класифікації настроїв, з акцентом на порівнянні моделей RNN та LSTM.*

***Методологія.** У роботі розглянуто теоретичні аспекти функціонування рекурентних нейронних мереж (RNN) та мереж довготривалої короткочасної пам'яті (LSTM), які є спеціалізованими варіантами RNN. Було проведено експериментальне порівняння чотирьох різних моделей нейронних мереж, що включають прості рекурентні мережі (RNN), мережі LSTM, а також згорткові нейронні мережі (CNN), які застосовувалися для задачі класифікації настроїв. Для експерименту було обрано набір даних imdb_reviews, що містить огляди фільмів, призначені для бінарної класифікації настроїв (позитивний або негативний відгук). Реалізація та навчання моделей було виконано за допомогою бібліотек TensorFlow та Keras, що забезпечують інструментарій для ефективного виконання машинного навчання. Процес навчання та тестування моделей відбувався із застосуванням стандартних підходів до попередньої обробки текстових даних, таких як токенізація та підготовка послідовностей.*

***Наукова новизна.** Показано, що основною перевагою LSTM є здатність вирішувати проблему довгострокових залежностей, що робить їх більш ефективними для задач, де важливо враховувати контекст на довгих послідовностях даних. Експериментально підтверджено, що час навчання рекурентних нейронних мереж суттєво більший порівняно з нерекурентними моделями, проте вони демонструють трохи кращу точність.*

***Висновки.** Результати дослідження свідчать про те, що використання LSTM мереж є більш ефективним підходом для вирішення складних задач, які потребують врахування контексту на рівні послідовностей, що перевищують за довжиною типові фрагменти тексту. LSTM переважають їх завдяки здатності зберігати довготривалі залежності, що особливо важливо в задачах, де необхідно враховувати взаємозв'язок між віддаленими елементами даних.*

***Ключові слова:** рекурентна нейронна мережа, LSTM, RNN, класифікація настроїв, довгострокові залежності*

Oleg KOBYLIN
Ph.D., Associate Professor, Head of the Department of Informatics, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, oleg.kobylin@nure.ua
***ORCID:** 0000-0003-0834-0475*

Iryna VECHIRSKA
Ph.D., Associate Professor at the Department of Informatics, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, iryna.vechirska@nure.ua
***ORCID:** 0000-0001-7964-2361*

Oleksii KRAVCHENKO
Postgraduate Student at the Department of Informatics, Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, Ukraine, 61166, oleksii.kravchenko@nure.ua
***ORCID:** 0009-0000-7999-1406*

To cite this article: Kobylin, O., Vechirska, I., Kravchenko, O. (2024). Porivniannia neironnykh merezh typu RNN ta LSTM [Comparison of RNN and LSTM neural networks]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 97–107, doi: https://doi.org/10.32782/IT/2024-3-10

COMPARISON OF RNN AND LSTM NEURAL NETWORKS

The research aims to identify the advantages and disadvantages of different approaches to sequential data processing, which is an important aspect in natural language processing tasks such as sentiment analysis, machine translation, and text generation.

***The purpose of the work.** The purpose of the work is to investigate the effectiveness of different neural network architectures for the problem of sentiment classification, with an emphasis on comparing RNN and LSTM models.*

***Methodology.** The paper examines the theoretical aspects of the functioning of recurrent neural networks (RNN) and long-term short-term memory (LSTM) networks, which are specialized variants of RNN. An experimental comparison of four different neural network models, including simple recurrent networks (RNNs), LSTM networks, and convolutional neural networks (CNNs), applied to the sentiment classification task was conducted. For the experiment, the imdb_reviews dataset was chosen, which contains movie reviews intended for binary sentiment classification (positive or negative feedback). The implementation and training of the models was done using the TensorFlow and Keras libraries, which provide a toolkit for efficient machine learning. The process of training and testing the models took place using standard approaches to preprocessing textual data, such as tokenization and sequence preparation.*

***Scientific novelty.** It is shown that the main advantage of LSTM is the ability to solve the problem of long-term dependencies, which makes them more effective for tasks where it is important to take into account the context of long data sequences. It has been experimentally confirmed that the training time of recurrent neural networks is significantly longer compared to non-recurrent models, but they demonstrate slightly better accuracy.*

***Conclusions.** The results of the study indicate that the use of LSTM networks is a more effective approach for solving complex problems that require consideration of the context at the level of sequences exceeding in length typical fragments of text. LSTMs are superior to them due to the ability to preserve long-term dependencies, which is especially important in tasks where it is necessary to take into account the relationship between distant data elements.*

***Key words:** recurrent neural network, LSTM, RNN, sentiment classification, long-term dependencies.*

Актуальність проблеми. Рекурентні нейронні мережі (Recurrent Neural Network, RNN) – вид нейронних мереж, що використовуються в обробці природної мови (NLP) (Isakov, n.d.). Рекурентна нейромережа оцінює довільні пропозиції на основі того, як часто вони зустрічалися в текстах. З іншого боку, такі моделі генерують новий текст. Навчання моделі на поемах Шекспіра дозволить генерувати новий текст, схожий на Шекспіра.

Ідея RNN полягає у послідовному використанні інформації. У традиційних нейронних мережах мається на увазі, що це входи і виходи незалежні. Але для багатьох завдань це не підходить. Якщо ви хочете передбачити наступне слово у реченні, краще враховувати попередні слова. RNN називаються рекурентними, тому що вони виконують одну і ту ж задачу для кожного елемента послідовності, причому вихід залежить від попередніх обчислень.

Рекурентні нейронні мережі продемонстрували великий успіх у багатьох завданнях NLP. На цьому етапі слід згадати, що типом RNN, що найчастіше використовується, є LSTM, які набагато краще захоплюють (зберігають) довгострокові залежності, ніж RNN. LSTM – це, по суті, те саме, що й RNN, які ми розберемо в цьому досліджені, просто мають інший спосіб. обчислення прихованого стану.

Аналіз останніх досліджень і публікацій. В останні роки зростає інтерес до використання рекурентних нейронних мереж (RNN) у завданнях обробки природної мови (NLP), таких як аналіз настроїв, машинний переклад та генерація текстів. Значна частина досліджень зосереджена на покращенні здатності RNN працювати

з довгостроковими залежностями, що є критично важливим у таких завданнях. Однією з найважливіших подій стало введення мереж довготривалої короткочасної пам'яті (LSTM), які здатні вирішувати проблему зникнення градієнтів та забезпечувати ефективну обробку довгих послідовностей даних. Такі моделі були успішно застосовані в різних галузях, включаючи машинний переклад та розпізнавання мовлення. Дослідження, такі як роботи (Glek, n.d.; Hochreiter, 1991), заклали фундамент для подальшого розвитку цієї технології, а останні експерименти демонструють їхню високу ефективність у порівнянні з традиційними RNN.

Мета дослідження. Метою даного дослідження є порівняння ефективності різних архітектур рекурентних нейронних мереж для класифікації настроїв. Особлива увага приділяється порівнянню моделей RNN та LSTM на основі експериментальних результатів із використанням набору даних imdb_reviews. Важливим аспектом є вивчення здатності цих моделей обробляти довгострокові залежності, що впливають на точність класифікації настроїв у текстових послідовностях.

Виклад основного матеріалу дослідження. Люди не запускають розумовий процес із нуля у кожний момент часу. Читаючи статтю, ви розумієте значення кожного слова на основі значень попередніх слів. Думки мають властивість накопичуватися та впливати один на одного. Цей принцип використовується у мережах LSTM (Glek, n.d.).

Прості нейронні мережі не можуть цього зробити, і це серйозна вада. Уявіть, що ви хочете в реальному часі класифікувати події у фільмі. Незрозуміло, як звичайна нейронна мережа може використовувати знання про попередні події, щоб вивчити наступні.

Рекурентні нейронні мережі (РНМ) вирішують цю проблему. Через наявність циклів РНМ виглядають більш складними порівняно з простими нейронними мережами, але на справді між ними немає великої різниці. РНМ можна розглядати, як кілька копій однієї й тієї ж мережі, кожна із яких передає повідомлення наступнику.

В останні роки досягнуто успіху в застосуванні РНМ до широкого кола проблем: розпізнавання мовлення, лінгвістичне моделювання, переклад, опис зображень. На допомогу у вирішенні перерахованих задач прийшли LSTM (Bengio, Simard, & Frasconi, 1994). LSTM *(long short-term memory або довга короткострокова пам'ять) – тип рекурентної нейронної мережі, здатний навчатися довгостроковим залежностям. LSTM, які вперше було представлено в роботі (Hochreiter & Schmidhuber, 1997) та потім удосконалено та популяризовано іншими дослідниками, добро справляються з багатьма завданнями і досі широко застосовуються.* LSTM спеціально розроблено для усунення проблеми довгострокової залежності. Їхня спеціалізація – запам'ятовування інформації протягом тривалих періодів часу, тому їх практично не потрібно навчати (Hochreiter, 1991; Bengio, Simard, & Frasconi, 1994)!

Принцип роботи мережі LSTM. LSTM зменшує або збільшує кількість інформації про стан комірки, залежно від потреб. Для цього використовуються структури, що ретельно налаштовуються, які називаються гейтами.

Гейт – це «брама», яка пропускає або не пропускає інформацію. Гейти складаються з сигмовидного шару нейронної мережі та операції поточкового множення.

На виході сигмовидного шару видаються числа від нуля до одиниці, визначаючи скільки відсотків кожної одиниці інформації пропустити далі. Значення «0» означає «не пропустити нічого», значення «1» – «пропустити все».

Покрокова схема роботи мережі LSTM. LSTM має три такі гейти для контролю стану комірки.

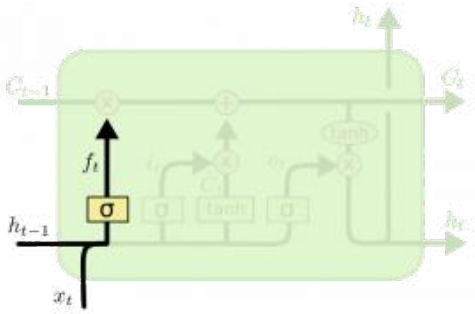
1. Шар втрати. На першому етапі LSTM потрібно вирішити, яку інформацію ми збираємося викинути зі стану комірки. Це рішення приймається сигмовидним шаром, званим шаром гейту втрати. Він отримує на вхід і видає число від 0 до 1 для кожного номера в стані комірки C. 1 означає «повністю зберегти», а 0 – «цілком видалити» (рис. 1).

2. Шар збереження. На наступному кроці потрібно вирішити, яку нову інформацію зберегти у стані комірки. Розіб'ємо процес на дві частини. Спочатку сигмоїдний шар, званий «шаром гейту входу», вирішує, які значення потрібно оновити. Потім шар tanh створює вектор нових значень-кандидатів C, які додаються до стан. На наступному етапі ми об'єднаємо ці два значення для оновлення стану (рис. 2).

3. Новий стан. Тепер оновимо попередній стан комірки для отримання нового стану **C**. Спосіб оновлення обрано, тепер реалізуємо саме оновлення.

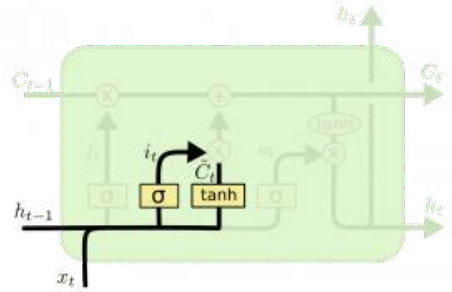
Помножимо старий стан на f**,** втрачаючи інформацію, яку вирішили забути. Потім додаємо i*C. Це нові значення кандидатів, які масштабуються залежно від того, як ми вирішили оновити кожне значення стану (рис. 3).

Нарешті, потрібно вирішити, що хочемо отримати на виході. Результат буде відфільтрованим



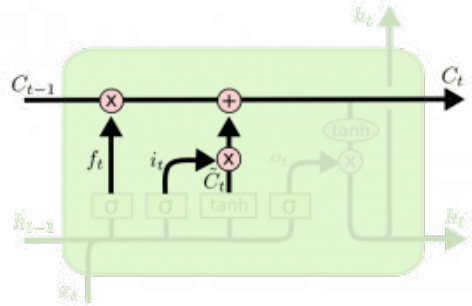
$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] \; + \; b_f\right)$$

Рис. 1. Шар втрати



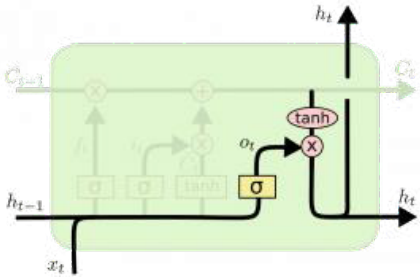
$$i_t = \sigma\left(W_i \cdot [h_{t-1}, x_t] \; + \; b_i\right)$$
$$\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] \; + \; b_C)$$

Рис. 2. Шар збереження



$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t$$

Рис. 3. Шар нового стану



$$o_t = \sigma\left(W_o \; [h_{t-1}, x_t] \; + \; b_o\right)$$
$$h_t = o_t * \tanh\left(C_t\right)$$

Рис. 4. Отримання результату на виході з комірки

станом комірки. Спочатку запускаємо сигмоїдний шар, який вирішує, які частини стану комірки виводити. Потім пропускаємо стан комірки через tanh (щоб розмістити всі значення в інтервалі [-1, 1]) і множимо його на вихідний сигнал сигмовидного гейту (рис. 4).

Описана вище схема традиційна для LSTM. Але не всі LSTM ідентичні. Насправді майже в кожній статті використовуються версії, що відрізняються. Відмінності незначні, але варто згадати деякі з них.

У популярному варіанті LSTM, представленому в (Gers & Schmidhuber, 2000), ми

дозволяємо шарам гейтів переглядати стан комірки (рис. 5).

На діаграмі вгорі «око» є у всіх гейтів, але в багатьох статтях він є лише в деяких гейтів.

Інший варіант – використання пов'язаних гейтів втрати та входу. Замість того, щоб окремо вирішувати, що забути, а до чого додати нову інформацію, ми ухвалюємо ці рішення одночасно. Ми забуваємо інформацію лише тоді, коли потрібно помістити щось нове на тому самому місці. Нові значення вносяться в стан лише тоді, коли ми забуваємо щось старіше (рис. 6).

Є багато інших варіантів LSTM, таких як PHC з гейтом глибини (Yao et al., 2015). Відомий також зовсім інший підхід до вирішення довгострокових залежностей, наведений у (Koutník et al., 2014).

Порівняння 4 моделей нейронних мереж при вирішенні задачі розпізнавання настроїв. У цьому розділі ми порівняємо 4 різні моделі нейронних мереж при вирішенні задачі розпізнавання (класифікації) настроїв. Ми будемо використовувати мову програмування Python та пакети Keras та TensorFlow. TensorFlow – це відкрите програмне забезпечення для машинного навчання та глибокого навчання, розроблене Google. TensorFlow зручний для використання в різних областях, включаючи великі обчислення, обробку природних мов, комп'ютерний зір і багато інших. Keras – це високорівневий інтерфейс для розробки нейронних мереж, який працює поверх TensorFlow та інших бібліотек машинного навчання.

Ми розглянемо практично розглянемо роботу таких шарів нейронних мереж як Flatten, LSTM, GRU, Convolution. Шари LSTM та GRU стосуються рекурентних нейронних мереж, тобто мереж для яких важливий порядок входів. Вони вже розглядались нами у розділі 2. Шар Flatten використовується для перетворення вхідних даних, які можуть мати багатовимірну форму, у одномірний вектор. Це особливо корисно, коли ви працюєте зі згортковими нейронними мережами (CNN), де виходи згорткових шарів можуть бути тривимірними (висота, ширина, глибина). В основі згорткових шарів (Convolution layer) нейронної мережі лежить операція згортки (рис. 7). Згортка – це процес додавання кожного елемента зображення до його сусідів, зважених ядром.

Одна з задач де порядок входів має значення, тобто бажане застосування рекурентних нейронних мереж, це задача побудови моделі, яка буде розрізняти почуття, навіть якщо слова, використані в двох реченнях, однакові.

1: Моїм друзям подобається фільм, але мені ні. --> негативний відгук

2: Моїм друзям не подобається фільм, але мені подобається. --> позитивний відгук

Ми розглянемо саме цю задачу і порівняємо поведінку 4 зазначених вище типів мереж при вирішенні цієї задачі.

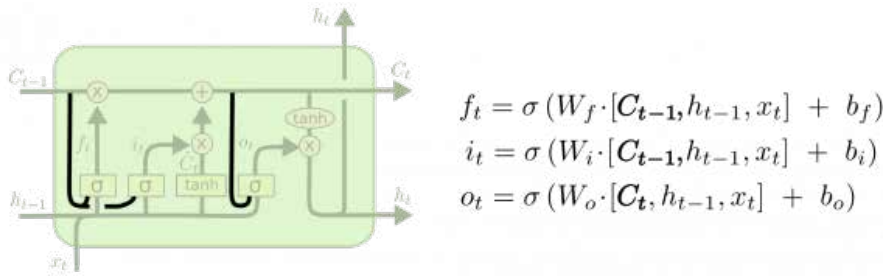


Рис. 5. Варіанті LSTM, де шари гейтів можуть переглядати стан комірки

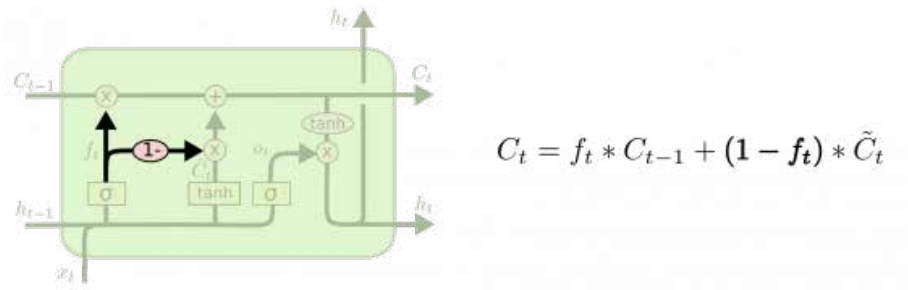


Рис. 6. Варіант LSTM з використанням пов'язаних гейтів втрати та входу

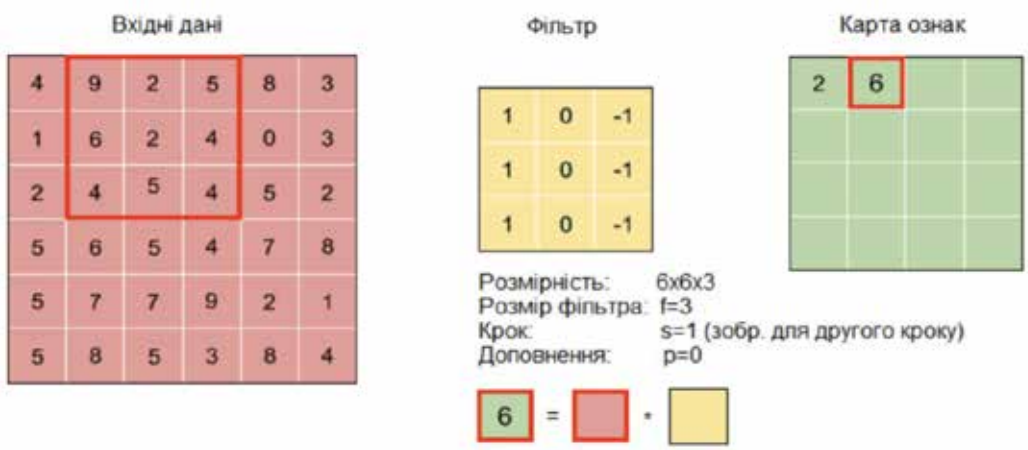


Рис. 7. Операція згортки

```
In 1
import tensorflow_datasets as tfds #4.9.2
# Download the plain text dataset
imdb, info = tfds.load('imdb_reviews', split='train', with_info=True)

df = tfds.as_dataframe(imdb, info)
df.head()
```

Executed at 2023.12.22 10:21:43 in 4s 340ms

```
WARNING:tensorflow:From D:\IdeaProjects\machine-learning\ml_venv\lib\site-packages\keras\src\losses.py:2976: The name tf
```

Out 1

5 rows × 2 columns pd.DataFrame

	label	text
0	0	b"This was an absolutely terrible movie. Don't be lured in by Christopher Walken or Michael Ironside. Both are great…
1	0	b'I have been known to fall asleep during films, but this is usually due to a combination of things including, reall…
2	0	b'Mann photographs the Alberta Rocky Mountains in a superb fashion, and Jimmy Stewart and Walter Brennan give enjoya…
3	1	b'This is the kind of film for a snowy Sunday afternoon when the rest of the world can go ahead with its own busines…
4	1	b'As others have mentioned, all the women that go nude in this film are mostly absolutely gorgeous. The plot very ab…

Рис. 8. Приклад зразків даних з цього датасету

В якості вхідних даних ми будемо використовувати вбудований у Tensorflow набір даних imdb_reviews. Це великий набір даних оглядів фільмів. Він саме створений для бінарної класифікації настроїв, що містить значно більше даних, ніж попередні еталонні набори даних. У набір входять 25 000 оглядів полярних оглядів фільмів для навчання та 25 000 для тестування. Існують додаткові немарковані дані для використання (рис. 8).

Перед усім імпортуємо необхідні залежності. Загрузимо датасет та виконаємо підготовку даних. Далі нам буде потрібно створити словник з нуля та сгенерувати доповнені послідовності. Ми це зробимо за допомогою класу Tokenizer і методу pad_sequences() (рис. 9).

Основною перевагою першої моделі є її простота. Інформацію щодо цієї моделі зображено на рис. 10.

На рис. 11 наведено результати навчання та валідації (тестування) моделі.

Модель LSTM є найбільш перспективною при вирішенні даної задачі. Інформацію щодо цієї моделі зображено на рис. 12.

На рис. 13 наведено результати навчання та валідації (тестування) моделі LSTM.

Модель GRU є спрощеним варіантом попередньої моделі та обчислення повинні займати менше часу. Інформацію щодо цієї моделі зображено на рис. 14.

На рис. 15 наведено результати навчання та валідації (тестування) моделі GRU.

Модель Convolution наведено на рис. 16. Ця модель є спрощеним варіантом попередньої моделі та обчислення повинні займати менше часу. Інформацію щодо цієї моделі зображено на рис. 17.

На рис. 18 наведено результати навчання та валідації (тестування) моделі Convolution.

```
# Parameters
vocab_size = 10000
max_length = 120
trunc_type='post'
oov_tok = "<OOV>"

# Initialize the Tokenizer class
tokenizer = Tokenizer(num_words = vocab_size, oov_token=oov_tok)

# Generate the word index dictionary for the training sentences
tokenizer.fit_on_texts(training_sentences)
word_index = tokenizer.word_index

# Generate and pad the training sequences
sequences = tokenizer.texts_to_sequences(training_sentences)
padded = pad_sequences(sequences,maxlen=max_length, truncating=trunc_type)

# Generate and pad the test sequences
testing_sequences = tokenizer.texts_to_sequences(testing_sentences)
testing_padded = pad_sequences(testing_sequences,maxlen=max_length)
```

Рис. 9. Створення словника та генерування доповнених послідовностей

```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 embedding (Embedding)       (None, 120, 16)           160000

 flatten (Flatten)           (None, 1920)              0

 dense (Dense)               (None, 6)                 11526

 dense_1 (Dense)             (None, 1)                 7

=================================================================
Total params: 171533 (670.05 KB)
Trainable params: 171533 (670.05 KB)
Non-trainable params: 0 (0.00 Byte)
_________________________________________________________________
```

Рис. 10. Детальна інформація про модель Flatten

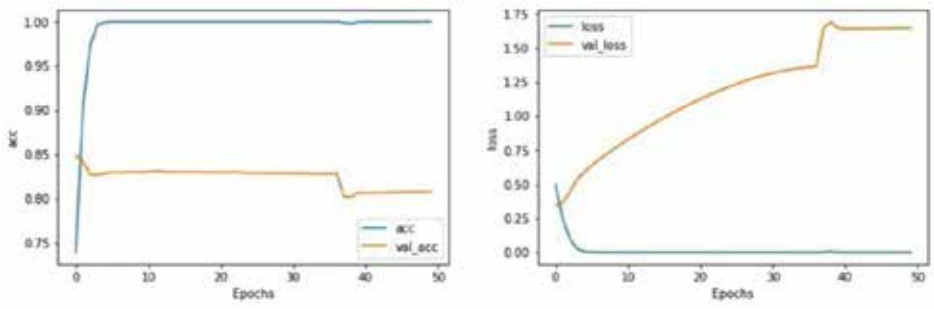


Рис. 11. Результати навчання та тестування моделі Flatten

Отже, тепер, коли ми отримали результати усіх 4 моделей, порівняємо їх. У першій моделі ми використовували слої embedding та flatten, за якими ми використовували, як і в інших моделях повнозв'язні слої. Модель містить 171 533 параметрами. Гарна точність перевірки (~80%), але явне перенавчання. Тренування займає лише близько 5 секунд на епоху.

При використанні моделі LSTM ми маємо 172941 параметр. При цьому навчання займає приблизно 43 секунди на епоху. Точність

```
Model: "sequential_1"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 embedding_1 (Embedding)     (None, 120, 16)           160000

 bidirectional (Bidirection  (None, 64)                12544
 al)

 dense_2 (Dense)             (None, 6)                 390

 dense_3 (Dense)             (None, 1)                 7

=================================================================
Total params: 172941 (675.55 KB)
Trainable params: 172941 (675.55 KB)
Non-trainable params: 0 (0.00 Byte)
_________________________________________________________________
```

Рис. 12. Детальна інформація про модель LSTM

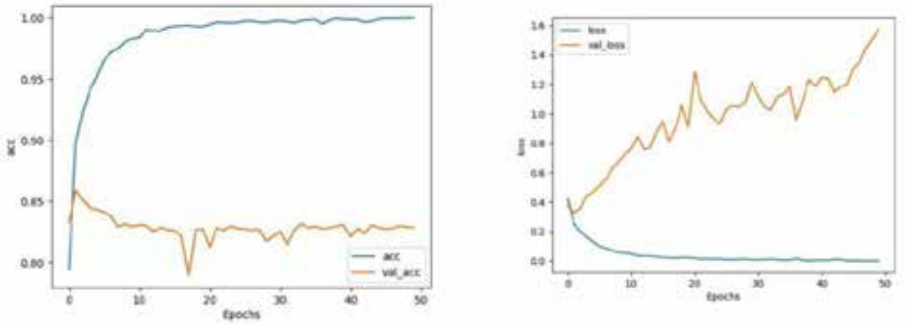


Рис. 13. Результати навчання та тестування моделі LSTM

```
Model: "sequential_2"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 embedding_2 (Embedding)     (None, 120, 16)           160000

 bidirectional_1 (Bidirecti  (None, 64)                9600
 onal)

 dense_4 (Dense)             (None, 6)                 390

 dense_5 (Dense)             (None, 1)                 7

=================================================================
Total params: 169997 (664.05 KB)
Trainable params: 169997 (664.05 KB)
Non-trainable params: 0 (0.00 Byte)
_________________________________________________________________
```

Рис. 14. Детальна інформація про модель GRU

перевірки краща (~83%), але є ще деяке перенавчання. При використанні двонаправленого GRU мережа має 169997 параметрів. Час навчання зменшиться до 20 секунд на епоху, і точність знову дуже хороша, під час тренувань і не надто погана під час перевірки (~82%), але мережа знову ж таки демонструє деяке перенавчання. Зі згортковою мережею ми маємо 171149 параметрів, і час навчання складає близько шести секунд на епоху, щоб наблизитися до 100-відсоткової точності під час навчання та близько 83 відсотків під час перевірки, але знову ж таки маємо перенавчання.

Висновки. Розглянто архітектури RNN, LSTM і GRU. Модель LSTM описуються складнішим набором рівнянь у порівнянні з простими нейронними мережами і є великим кроком у розвитку РНМ. Хоча наші моделі показали майже однакову точність, при цьому час навчання при використанні рекурентних нейронних мереж виявився значно більшим, тим не менш вони

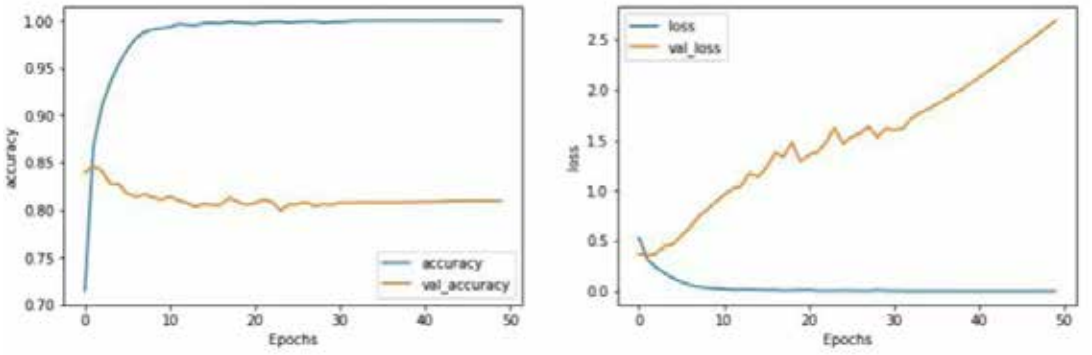


Рис. 15. Результати навчання та тестування моделі GRU

```
# Parameters
embedding_dim = 16
filters = 128
kernel_size = 5
dense_dim = 6

# Model Definition with Conv1D
model_conv = tf.keras.Sequential([
    tf.keras.layers.Embedding(vocab_size, embedding_dim,
input_length=max_length),
    tf.keras.layers.Conv1D(filters, kernel_size, activation='relu'),
    tf.keras.layers.GlobalAveragePooling1D(),
    tf.keras.layers.Dense(dense_dim, activation='relu'),
    tf.keras.layers.Dense(1, activation='sigmoid')
])

# Set the training parameters
model_conv.compile(loss='binary_crossentropy',optimizer='adam',metrics=['accurac
y'])

# Print the model summary
model_conv.summary()

NUM_EPOCHS = 10
BATCH_SIZE = 128

# Train the model
history_conv = model_conv.fit(padded, training_labels_final,
batch_size=BATCH_SIZE, epochs=NUM_EPOCHS, validation_data=(testing_padded,
testing_labels_final))

# Plot the accuracy and loss history
plot_graphs(history_conv, 'accuracy')
plot_graphs(history_conv, 'loss')
```

Рис. 16. Створення та навчання моделі Convolution

показують значно кращі практичні результати ніж звичайні РНМ при вирішенні більш складних завдань машинного перекладу, розпізнавання руху, генерації тексту та ін. Головною перевагою LSTM є їхня здатність уникнути проблеми зниклих та вибуваючих градієнтів, з якою стикаються звичайні РНМ, завдяки введенню спеціальних воріт (воріт забування, воріт входу, воріт виводу), які контролюють потік інформації в моделі.

```
Model: "sequential_3"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 embedding_3 (Embedding)     (None, 120, 16)           160000

 conv1d (Conv1D)             (None, 116, 128)          10368

 global_average_pooling1d (  (None, 128)               0
 GlobalAveragePooling1D)

 dense_6 (Dense)             (None, 6)                 774

 dense_7 (Dense)             (None, 1)                 7

=================================================================
Total params: 171149 (668.55 KB)
Trainable params: 171149 (668.55 KB)
Non-trainable params: 0 (0.00 Byte)
_________________________________________________________________
```

Рис. 17. Детальна інформація про модель Convolution

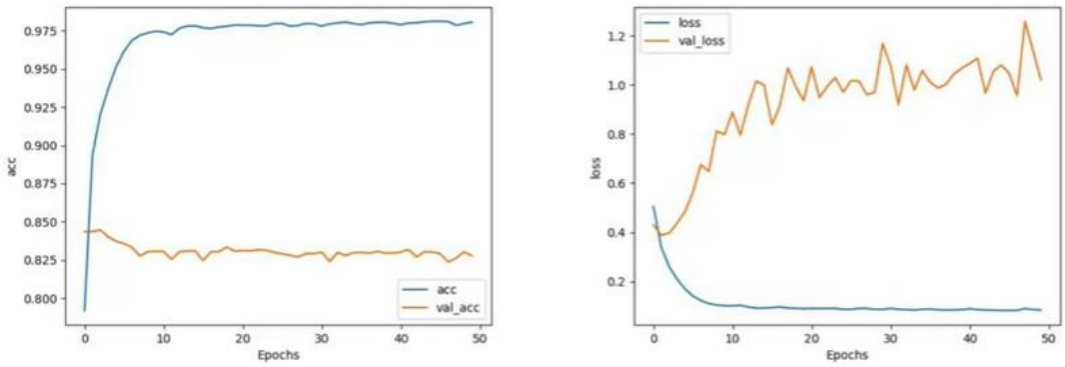


Рис. 18. Результати навчання та тестування моделі Convolution

ЛІТЕРАТУРА:

1. Ісаков С. Рекурентна нейронна мережа (RNN): типи, навчання, приклади. URL: https://neurohive.io/ru/osnovy-data-science/rekurrentnye-nejronnye-seti (дата звернення: 15.08.2024).

2. Глек П. LSTM – мережа довготривалої короткочасної пам'яті. URL: https://neurohive.io/ru/osnovy-data-science/lstm-nejronnaja-set (дата звернення: 15.08.2024).

3. Hochreiter S. Untersuchungen zu dynamischen neuronalen Netzen. Diploma, Technische Universität München, 1991. 31 с.

4. Bengio Y., Simard P., Frasconi P. Learning long-term dependencies with gradient descent is difficult. *IEEE Transactions on Neural Networks*. 1994. Vol. 5, № 2. С. 157–166.

5. Hochreiter S., Schmidhuber J. Long Short-Term Memory. *Neural Computation*. 1997. Vol. 9, № 8. С. 1735–1780.

6. Gers F.A., Schmidhuber J. Recurrent nets that time and count. Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. IJCNN 2000. Neural Computing: New Challenges and Perspectives for the New Millennium. Como, Italy, 2000. Vol. 3. С. 189–194.

7. Cho K., van Merrienboer B., Gulcehre C., Bougares F., Schwenk H., Bengio Y. Learning phrase representations using RNN encoder-decoder for statistical machine translation. In Conference on Empirical Methods in Natural Language Processing (EMNLP 2014). 2014.

8. Yao K., Cohn T., Vylomova K., Duh K., Dyer C. Depth-gated recurrent neural networks. arXiv, 2015. URL: http://arxiv.org/abs/1508.03790.

9. Koutník J., Greff K., Gomez F., Schmidhuber J. A clockwork RNN. 31st International Conference on Machine Learning, ICML 2014. 2014.

10. Greff K. et al. LSTM: A search space odyssey. *IEEE Transactions on Neural Networks and Learning Systems*. 2016. Vol. 28, № 10. С. 2222–2232.

11. Jozefowicz R., Zaremba W., Sutskever I. An Empirical Exploration of Recurrent Network Architectures. Proceedings of the 32nd International Conference on Machine Learning. PMLR 37:2342–2350. 2015.

12. Xu K. et al. Show, attend and tell: Neural image caption generation with visual attention. International conference on machine learning. PMLR, 2015.

REFERENCES:

1. Isakov, S. (n.d.). Recurrent neural network (RNN): Types, training, examples. Neurohive. Retrieved from https://neurohive.io/ru/osnovy-data-science/rekurrentnye-nejronnye-seti [in Ukrainian].

2. Glek, P. (n.d.). LSTM – long short-term memory neural network. Neurohive. Retrieved from https://neurohive.io/ru/osnovy-data-science/lstm-nejronnaja-set [in Ukrainian].

3. Hochreiter, S. (1991). Untersuchungen zu dynamischen neuronalen Netzen (Diploma thesis). Technische Universität München.

4. Bengio, Y., Simard, P., & Frasconi, P. (1994). Learning long-term dependencies with gradient descent is difficult. *IEEE Transactions on Neural Networks*, 5(2), 157–166.

5. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735–1780.

6. Gers, F. A., & Schmidhuber, J. (2000). Recurrent nets that time and count. In Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks (IJCNN 2000): Neural Computing: New Challenges and Perspectives for the New Millennium (Vol. 3, pp. 189–194). Como, Italy.

7. Cho, K., van Merrienboer, B., Gulcehre, C., Bougares, F., Schwenk, H., & Bengio, Y. (2014). Learning phrase representations using RNN encoder-decoder for statistical machine translation. In Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP 2014).

8. Yao, K., Cohn, T., Vylomova, K., Duh, K., & Dyer, C. (2015). Depth-gated recurrent neural networks. arXiv preprint arXiv:1508.03790.

9. Koutník, J., Greff, K., Gomez, F., & Schmidhuber, J. (2014). A clockwork RNN. In Proceedings of the 31st International Conference on Machine Learning (ICML 2014) (Vol. 5).

10. Greff, K., Srivastava, R. K., Koutník, J., Steunebrink, B. R., & Schmidhuber, J. (2016). LSTM: A search space odyssey. IEEE Transactions on Neural Networks and Learning Systems, 28(10), 2222–2232.

11. Jozefowicz, R., Zaremba, W., & Sutskever, I. (2015). An empirical exploration of recurrent network architectures. In Proceedings of the 32nd International Conference on Machine Learning (ICML 2015), PMLR 37, 2342–2350.

12. Xu, K., Ba, J., Kiros, R., Cho, K., Courville, A., Salakhutdinov, R., … & Bengio, Y. (2015). Show, attend and tell: Neural image caption generation with visual attention. In Proceedings of the International Conference on Machine Learning (ICML 2015), PMLR.

UDC 004.71
DOI https://doi.org/10.32782/IT/2024-3-11

Ivan LAKTIONOV
Doctor of Engineering Sciences, Docent, Professor at the Department of Computer Systems Software, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, Laktionov.I.S@nmu.one
ORCID: *0000-0001-7857-6382*
Scopus Author ID: *57194557735*

Oleksandr ZHABKO
Postgraduate Student at the speciality 123 Computer Engineering, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, Zhabko.O.S@nmu.one
ORCID: *0009-0002-7996-9115*

Grygorii DIACHENKO
PhD, Associate Professor at the Department of Electric Drive, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, Diachenko.G@nmu.one
ORCID: *0000-0001-9105-1951*
Scopus Author ID: *57201252081*

To cite this article: Laktionov, I., Zhabko, O., Diachenko, G. (2024). Rezultaty analizu efektyvnosti bezdrotovykh tekhnolohii obminu danymy pid chas pobudovy informatsiinykh system ahromonitorynhu [Results of the analysis of the effectiveness of wireless data exchange technologies when creating information systems for agro-monitoring]. *Computer Science, Software Engineering and Cyber Security*, 3, 108–115, doi: https://doi.org/10.32782/IT/2024-3-11

RESULTS OF THE ANALYSIS OF THE EFFECTIVENESS OF WIRELESS DATA EXCHANGE TECHNOLOGIES WHEN CREATING INFORMATION SYSTEMS FOR AGRO-MONITORING

Relevance. *The reliability of wireless networks is a critical aspect in modern infocommunication systems, especially given their widespread use in a variety of industries, including agriculture, healthcare, transportation, and industry. These networks must provide continuous and reliable communication, which is becoming increasingly important in the context of the growing number of connected devices and increasing requirements for quality of service (QoS). Reliability here includes the ability of a network to continue to function properly during and after failures, as well as ensuring secure data transmission.*

The main aim *is to conduct a comparative analysis of several architectures of neural networks in order to determine the most suitable for modeling the reliability of wireless networks. In the second part of the study, several wireless communication standards will be simulated using the selected algorithm, which will allow for a deeper analysis and draw conclusions about reliability.*

The research object *is the modern wireless communication standards and their effectiveness under various application conditions.* ***The research subject*** *is methods and models of comparison of the performance and characteristics of 5G, Wi-Fi, LTE, and Zigbee for different types of networks and applications.*

Conclusions. *The results emphasize that 5G is the most promising standard for applications requiring high data transfer speeds and low latency. Wi-Fi remains a popular choice for local networks, but its performance decreases over long distances and in environments with significant interference. LTE offers a good balance between coverage area and performance, while Zigbee is the least performant but effective for low-speed and energy-efficient IoT applications. Overall, the research results confirm that the choice of wireless communication standard depends on specific network requirements, including bandwidth needs, coverage area, latency, and energy efficiency.*

Key words: *wireless networks, reliability, neural networks, QoS, data transmission, network performance.*

Іван ЛАКТІОНОВ
доктор технічних наук, доцент, професор кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет «Дніпровська політехніка», пр. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
ORCID: *0000-0001-7857-6382*
Scopus Author ID: *57194557735*

Олександр ЖАБКО
здобувач вищої освіти за освітньо-науковим рівнем «Доктор філософії» за спеціальністю 123 Комп'ютерна інженерія, Національний технічний університет «Дніпровська політехніка», пр. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0009-0002-7996-9115*

Григорій ДЯЧЕНКО
кандидат технічних наук, доцент кафедри електропривода, Національний технічний університет «Дніпровська політехніка», пр. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0001-9105-1951*
***Scopus Author ID:** 57201252081*

Бібліографічний опис статті: Лактіонов, І., Жабко, О., Дяченко, Г. (2024). Результати аналізу ефективності бездротових технологій обміну даними під час побудови інформаційних систем агромоніторингу. *Computer Science, Software Engineering and Cyber Security*, 3, 108–115, doi: https://doi.org/10.32782/IT/2024-3-11

РЕЗУЛЬТАТИ АНАЛІЗУ ЕФЕКТИВНОСТІ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ОБМІНУ ДАНИМИ ПІД ЧАС ПОБУДОВИ ІНФОРМАЦІЙНИХ СИСТЕМ АГРОМОНІТОРИНГУ

Актуальність. *Надійність бездротових мереж є критично важливим аспектом у сучасних інфокомунікаційних системах, особливо з огляду на їх широке застосування в різноманітних галузях, включаючи сільське господарство, охорону здоров'я, транспорт та промисловість. Ці мережі мають забезпечувати безперервний і надійний зв'язок, що стає дедалі важливішим в умовах зростання числа підключених пристроїв та підвищення вимог до якості обслуговування (QoS). Надійність включає здатність мережі продовжувати функціонувати належним чином під час і після збоїв, а також забезпечення безпечної передачі даних.*

Метою роботи *є проведення порівняльного аналізу кількох архітектур нейронних мереж задля визначення найбільш придатної для моделювання бездротових мереж щодо оцінки їх надійності. Також у статті проведено дослідження методами моделювання кількох стандартів бездротового зв'язку за допомогою обраного алгоритму, що дозволило провести глибший аналіз і зробити висновки щодо надійності.*

Об'єктом дослідження *є сучасні стандарти бездротового зв'язку та їх ефективність у різних умовах застосування.* ***Предметом дослідження*** *є методи і моделі порівняння продуктивності та характеристик 5G, Wi-Fi, LTE та Zigbee для різних типів мереж і застосувань.*

Висновки: *результати моделювання підкреслюють, що 5G є найбільш перспективним стандартом для додатків, що вимагають високої швидкості передачі даних і низької затримки. Wi-Fi залишається популярним вибором для локальних мереж, але його продуктивність знижується на великих відстанях і в умовах великої кількості перешкод. LTE пропонує хорошу збалансованість між зоною покриття та продуктивністю, а Zigbee є найменш продуктивним, проте ефективним для низькошвидкісних і енергоефективних додатків IoT. Загалом, результати дослідження підтверджують, що вибір стандарту бездротового зв'язку залежить від конкретних вимог до мережі, включаючи потреби в пропускній здатності, зоні покриття, затримці та енергоефективності.*

Ключові слова: *бездротові мережі, надійність, нейронні мережі, QoS, передача даних, продуктивність мережі.*

The relevance of the scientific and applied research task. Reliability of wireless networks is a critically important aspect of modern infocommunication systems, especially considering their widespread use across various sectors, including healthcare, transportation, and industry. These networks must provide continuous and reliable connectivity, which becomes increasingly important as the number of connected devices grows and the demands for quality of service (QoS) increase. Reliability here includes the network's ability to continue functioning properly during and after failures, as well as ensuring the secure transmission of data (Sharma et al., 2023).

Various methods and algorithms are used to analyze and improve the reliability of wireless networks, with neural networks playing a significant role. Specifically, in studies of the reliability of neural networks used in critical systems, it has been found that even the best models can be prone to errors during deployment. In such cases, methods like SelfChecker and DeepInfer are employed to assess model reliability based on the analysis of the model's internal layers or conditions on input data, thereby enhancing the accuracy of reliability predictions (Pinconschi et al., 2024).

Aim and objectives of the article. The main aim of the article is to analyze and synthesize

approaches to enhancing the reliability of wireless networks by leveraging the latest advancements in neural network technologies, ensuring stable and secure operations in critical communication systems. To achieve the set aim, the following objectives need to be met:

– conduct a critical analysis and logical generalization of existing approaches to improving the reliability of wireless infocommunication networks;

– identify and examine the most effective architectural solutions and algorithms for enhancing network reliability, with a focus on neural networks;

– develop and evaluate structural models and algorithms for assessing the reliability of wireless networks using selected neural network architectures;

– provide recommendations for future research directions to advance the reliability of wireless communication systems, particularly in critical applications.

Comparative analysis of neural networks. For the comparative analysis, four main neural network architectures were selected: Multilayer Perceptron (MLP), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Transformers. These models were chosen based on their popularity in solving various tasks related to prediction and classification, as well as their potential suitability for analyzing the reliability of wireless networks (Muñoz-Zavala et al., 2024).

The main criteria for selection were:

– performance: the model's ability to provide high accuracy in complex conditions, which is important for reliability;

– noise resistance: the model's ability to maintain effectiveness in the presence of noise in the input data;

– computational complexity: an evaluation of resource requirements for running the models, especially in the context of real-time processing.

Architectures description:

– MLP (Multilayer Perceptron): a classic model with full connectivity between layers, capable of solving a wide range of tasks;

– CNN (Convolutional Neural Network): used for processing data with spatial dependencies, particularly effective for image analysis;

– RNN (Recurrent Neural Network): specializes in processing sequential data, such as text or time series;

– transformers: a modern architecture that has shown high efficiency in tasks where processing long sequences and complex contexts is important.

For comparing the selected neural networks, the following metrics were used:

– accuracy: the overall proportion of correct predictions, allowing the evaluation of the model's effectiveness;

Detail | Compact | Column

sort_id	date_d_m_y	time	sensor_id	sensor_ty...
1	5.02.2016	13:01:06	310	B
3	5.02.2016	13:01:16	306	B
6	5.02.2016	13:02:40	368	B
12	5.02.2016	13:03:32	367	B
20	5.02.2016	13:04:13	365	B
23	5.02.2016	13:04:45	302	B
31	5.02.2016	13:06:49	306	B
38	5.02.2016	13:09:06	367	B
45	5.02.2016	13:09:51	365	B
48	5.02.2016	13:10:20	302	B
56	5.02.2016	13:12:22	306	B
61	5.02.2016	13:13:38	368	B

Fig. 1. Dataset for further analysis (retrieved from kaggle.com/datasets/halimedogan/wireless-sensor-network-data/data)

– recall: reflects the model's ability to identify all actual positive cases;

– F1-score: the harmonic mean between accuracy and recall, allowing the assessment of balance between them.

To obtain quantitative and qualitative evaluations presented in Table 1, a series of experiments was conducted on synthetic and real data. Initially, datasets were collected and prepared that reflected various aspects of wireless networks, including traffic data, signal level, latency, and errors. Synthetic data were generated by simulating different scenarios of wireless networks, allowing for controlled parameters and the introduction of targeted noise (Zhu et al., 2023). Real data were obtained from existing datasets containing information on real operational conditions and potential failures.

The models were trained on training datasets with subsequent validation on test datasets that included cases with varying levels of noise. To increase the accuracy and stability of the results, the k-fold cross-validation method was used. Each model underwent several cycles of training and testing with different data distributions, reducing the impact of random factors (Wang et al., 2023).

Various public datasets collected from reputable sources were used for modeling and analyzing neural networks in the context of wireless network reliability research. The training and testing datasets were selected considering the specifics of the network scenarios under study, ensuring high modeling quality and relevance of the obtained results. In particular, the following sources were used to train the models:

1. Wireless Network Traffic Data (UCI Machine Learning Repository) is a dataset containing information about traffic in wireless networks. This dataset allows for modeling various aspects of network operation, including signal level analysis, latency, and errors. Using this dataset provided the opportunity to test the models under real wireless network operating conditions.

2. CICIDS 2017 Dataset (Canadian Institute for Cybersecurity) is a dataset for anomaly detection in networks, containing detailed information about various types of network traffic, including both normal traffic and traffic related to attacks. This dataset was used to evaluate the models' ability to detect anomalies in complex conditions.

3. IEEE Dataport Wireless Network Data is a platform providing access to datasets collected in real wireless networks. Choosing data from this platform ensured modeling and testing of neural networks under real conditions with varying levels of noise and other factors affecting network reliability.

The training data underwent preprocessing to ensure the correctness of the modeling:

1. Data Collection and Preprocessing: real data were collected from public sources such as UCI, CIC, and IEEE Dataport. The data were cleaned of potential artifacts and anomalies that could negatively impact the modeling results.

2. Statistical Characteristics Analysis: for each dataset, an assessment of the main statistical characteristics, such as mean, variance, median, and range, was conducted. This allowed for the evaluation of possible correlations between parameters and ensured high-quality model training.

3. Creation of Synthetic Data: to model various scenarios of wireless network operation, synthetic data were generated, including variations in noise levels and other network characteristics. This provided the opportunity to test the models in different conditions and evaluate their noise resistance.

The data preparation approach ensured high accuracy, stability, and realism of the modeling results, as confirmed in the presented results table (Table 1).

Based on the conducted analysis, transformers were chosen as the most suitable architecture for further research on the reliability of wireless networks. They demonstrated the highest results across all key metrics, indicating their ability to

Table 1

Comparison of neural network architectures by basic metrics

Neural Network Architecture	Accuracy	Recall	F1-Score	Noise Resistance	Computational Complexity
MLP (Multilayer Perceptron)	85%	82%	83%	Medium	Low
CNN (Convolutional Neural Network)	88%	85%	86.5%	High	High
RNN (Recurrent Neural Network)	84%	80%	82%	Medium	Medium
Transformer	92%	89%	90.5%	High	High
MLP (Multilayer Perceptron)	85%	82%	83%	Medium	Low

effectively handle the tasks presented in this study (Rafique et al., 2024).

The algorithm for using transformers in this research consists of several key stages as shown in Fig. 2.

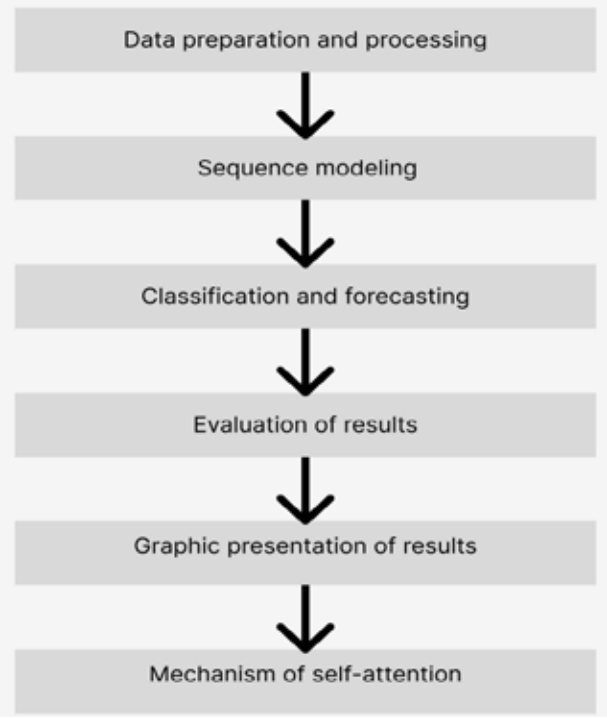


Fig. 2. The algorithm for using transformers

Thus, transformers will be used for time series analysis and reliability prediction of wireless networks, enabling the early detection of potential issues and the prevention of network failures.

Comparative modeling of wireless infocommunication standards. For this study, four wireless communication standards were selected: Wi-Fi, LTE, 5G, and Zigbee. These standards were chosen based on their relevance in modern wireless networks and their widespread application in various fields (Naidu et al., 2019).

– Wi-Fi: a standard for local area networks (LAN) that provides high data transmission speeds over relatively short distances. It is used in many consumer and industrial applications;

– LTE: a mobile communication standard that offers high bandwidth and serves as the foundation for modern cellular networks. It provides broad coverage and supports high mobility;

– 5G: a mobile communication standard that promises to significantly increase data transmission speeds, reduce latency, and improve connection reliability. 5G also supports a massive number of IoT connections (Alsabah et al., 2021);

– Zigbee: a standard designed for low-speed wireless networks with low power consumption, often used in IoT, smart homes, and industrial automation.

The standards were selected considering various aspects of their use and technological capabilities, allowing for a comprehensive study of reliability (Shilpa et al., 2022).

The modeling was conducted using the NS-3 simulation environment, a standard for network modeling. The main tools were Python for scripting and TensorFlow for integrating the transformer neural network, which was chosen in the previous stage of the study.

The study used real datasets on network traffic obtained from various sources, such as public databases like Kaggle and IEEE DataPort. The main simulation parameters included setting up network topology, configuring communication channels, and parameters for interference and network load (Shuaib et al., 2006).

Experiment stages:

1. Network topology creation: separate network scenarios were configured for each wireless communication standard (Wi-Fi, LTE, 5G, Zigbee). Network topologies reflecting real-world usage conditions were created:

– Wi-Fi: a local network with multiple access points (APs) and client devices, modeling an environment similar to an office or home;

– LTE and 5G: mobile communication scenarios with base stations and moving subscribers. These models reflect typical conditions of operator networks with varying numbers of users and traffic;

– Zigbee: a network consisting of sensor nodes, with low bandwidth and low power consumption, ideally suited for smart homes or IoT systems.

2. Communication channel configuration: the communication channel parameters were configured, such as frequency range, channel width, transmitter power, and interference level. Characteristic parameters corresponding to the specifications of each standard were used.

3. Traffic and load modeling: according to typical usage scenarios, characteristic types of traffic were modeled for each standard:

– Wi-Fi: high-speed internet traffic, streaming video, file transfer;

– LTE and 5G: high levels of mobile traffic with an emphasis on latency and bandwidth;

– Zigbee: low-speed sensor data traffic, simulating smart lighting systems or temperature sensors.

4. Neural network integration: a transformer neural network implemented on TensorFlow was used for analyzing and predicting network behavior. Its integration into NS-3 enabled predictions based on real data, significantly improving the

accuracy of the modeling and allowing for the consideration of nonlinear dependencies in network processes.

5. Results evaluation: the key performance parameters, such as average latency, bandwidth, packet loss rate, and power consumption, were assessed for each standard. These results were visualized as graphs, allowing for a comparison of the efficiency of different standards under various conditions (Raza et al., 2017).

Simulation results and parameter comparison are shown in Fig. 3 and Table 2.

Key evaluation parameters:

1. Average data transfer speed (Mbps):

– measurement: the average bandwidth was measured for each standard based on the transmission of large amounts of data under various conditions. Network load was simulated, including different types of traffic (e.g., streaming video, large files, sensor data for IoT);

– Wi-Fi: measured under moderate load and at distances up to 30 meters;

– LTE: measured in a mobile environment with multiple subscribers over a large coverage area;

– 5G: measured in densely urbanized areas with high-speed requirements;

– Zigbee: measured under low transmission power conditions, typical for IoT sensor networks.

2. Average latency (ms):

– measurement: latency was measured for data packets of various sizes in scenarios simulating real-world technology use. The latency was assessed based on the average time it takes for packets to travel from the source to the receiver;

– Wi-Fi: latency was measured under normal and increased network load;

– LTE: latency was evaluated in a mobile environment with subscriber movement;

– 5G: latency was measured in high-density device environments with stringent latency requirements (e.g., for VR/AR applications);

– Zigbee: latency was considered under low-power consumption conditions and frequent interference.

3. Packet loss (%):

– Measurement: packet loss was measured in each environment to assess the network's resilience to interference and overload. Scenarios with varying traffic intensity and the number of connected devices were used;

– Wi-Fi: stability was analyzed as the number of connected devices and distance increased;

– LTE: packet loss was evaluated in conditions of moving subscribers and high user density;

– 5G: packet loss was evaluated in high-density data transmission environments using different frequency bands;

– Zigbee: losses were analyzed under low bandwidth and energy-saving operating modes.

4. Interference resilience:

– measurement: this parameter was assessed based on simulations of the impact of different types of interference on network performance. Each scenario used models of radio frequency interference, multipath effects, and interference from other devices;

– Wi-Fi: resilience to radio frequency interference in multi-channel environments was considered;

– LTE: the network's ability to operate in overlapping base station coverage areas was analyzed;

– 5G: resilience to interference in new frequency bands, including millimeter waves, was evaluated;

– Zigbee: resilience in environments with significant low-frequency interference was assessed.

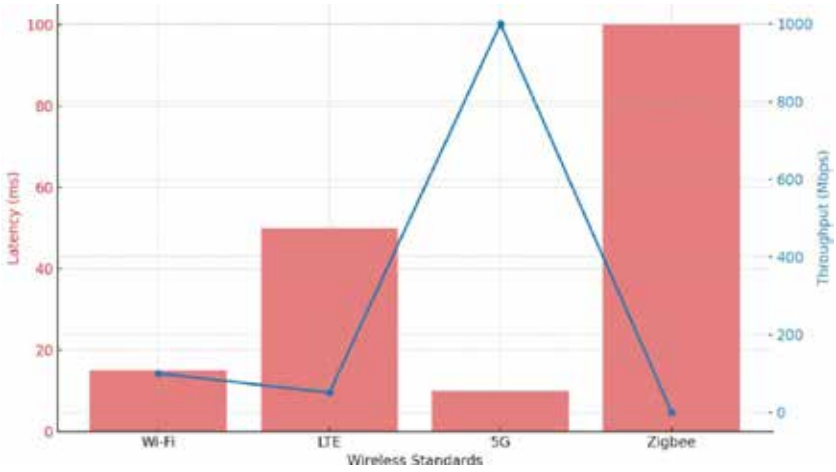


Fig. 3. Comparison of latency and throughput across wireless standards

Table 2

Main simulation parameters

Parameter	Wi-Fi	LTE	5G	Zigbee
Bandwidth	20 MHz	1.4-20 MHz	100 MHz	2.4 GHz
Maximum Speed	Up to 600 Mbps	Up to 300 Mbps	Up to 10 Gbps	Up to 250 kbps
Coverage Area	Up to 100 m	Up to 10 km	Up to 20 km	Up to 100 m
Latency	~1-10 ms	~20-30 ms	~1-2 ms	~30 ms

Table 3

Comparison of standard performance

Standard	Average Data Transfer Speed (Mbps)	Average Latency (ms)	Packet Loss (%)	Interference Resilience
Wi-Fi	150	5	2	Medium
LTE	100	25	1	High
5G	1000	1	0.5	High
Zigbee	0.2	30	5	Low

Simulation results:

– Wi-Fi demonstrated high data transfer speeds over short distances, but its reliability decreased with increasing distance and interference;

– LTE showed stable performance over long distances, but its data transfer speed was lower compared to Wi-Fi and 5G;

– 5G exhibited the highest data transfer speeds and low latency, making it the most promising standard for future applications requiring high reliability (Al-Fuqaha et al, 2015);

– Zigbee was the least performant but its energy efficiency and ease of configuration make it attractive for low-speed IoT applications.

Priority directions for further research. Based on the analysis and formulation of key requirements, the next steps involve addressing three crucial tasks:

1. Investigate methods to enhance 5G network performance in specialized environments, such as urban areas with high interference and remote rural areas, to ensure consistent high-speed data transfer and low latency.

2. Explore advanced technologies and algorithms to extend the effective range of Wi-Fi networks and mitigate performance degradation in environments with significant interference.

3. Develop strategies to optimize LTE networks, focusing on maximizing coverage while maintaining high performance, particularly in transitioning environments between urban and rural settings.

4. Study the potential for combining different wireless communication standards, such as 5G, Wi-Fi, LTE, and Zigbee, to create hybrid networks that can dynamically adapt to varying network requirements and conditions.

Conclusions. The results emphasize that 5G is the most promising standard for applications requiring high data transfer speeds and low latency. Wi-Fi remains a popular choice for local networks, but its performance decreases over long distances and in environments with significant interference. LTE offers a good balance between coverage area and performance, while Zigbee is the least performant but effective for low-speed and energy-efficient IoT applications. Overall, the research results confirm that the choice of wireless communication standard depends on specific network requirements, including bandwidth needs, coverage area, latency, and energy efficiency.

BIBLIOGRAPHY:

1. Sharma P., Khatri S. P., Kumar P. An intelligent healthcare system using IoT in wireless sensor network. *Sensors*. 2023. Vol. 23 (11). P. 1–14. https://doi.org/10.3390/s23115055.

2. Pinconschi E., Gopinath D., Abreu R., Păsăreanu C. S. Evaluating Deep Neural Networks in Deployment: A Comparative Study (Replicability Study). *arXiv preprint arXiv: arXiv:2407.08730v2*. 2024. https://doi.org/10.48550/arXiv.2407.08730

3. Muñoz-Zavala A. E., Macías-Díaz J. E., Alba-Cuéllar D., Guerrero-Díaz-de-León J. A. A Literature Review on Some Trends in Artificial Neural Networks for Modeling and Simulation with Time Series. *Algorithms*. 2024. Vol. 17 (2). P. 1–45. https://doi.org/10.3390/a17020076.

4. Zhu H., Zhang H., Lu W., Li X. Foreformer: An enhanced transformer-based framework for multivariate time series forecasting. *Neural Comp. and App*. 2023. Vol. 35. P. 14467–14480. https://doi.org/10.1007/s00521-023-08091-1.

5. Wang Y.-C., Houng Y.-C., Chen H.-X., Tseng S.-M. Network Anomaly Intrusion Detection Based on Deep Learning Approach. *Sensors*. 2023. Vol. 23 (4), P. 1–21. https://doi.org/10.3390/s23042171.

6. Rafique S. H., Abdallah A., Musa N. S., Murugan T. Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection–Current Research Trends. *Sensors*. 2024. Vol. 24 (6). P. 1–32. https://doi.org/10.3390/s24061968

7. Naidu G. A., Kumar J. Wireless Protocols: Wi-Fi SON, Bluetooth, ZigBee, Z-Wave, and Wi-Fi. In R. K. Singh & G. Kumar (Eds.), *Proceedings of the 5th International Conference on IT & Multimedia*. 2019. P. 229–239. https://doi.org/10.1007/978-981-13-3765-9_24.

8. Alsabah M., Naser M. A., Mahmmod B. M., Abdulhussain S. H., et al. 6G Wireless Communications Networks: A Comprehensive Survey. *IEEE Access*. 2021. Vol. 99. P. 1–9. https://doi.org/10.1109/ACCESS.2021.3124812.

9. Shilpa B., Radha R., Movva P. Comparative Analysis of Wireless Communication Technologies for IoT Applications. *Artificial Intelligence and Technologies*. 2022. P. 383–394. https://doi.org/10.1007/978-981-16-6448-9_39.

10. Shuaib K., Boulmalf M., Sallabi F., Lakas A. Co-existence of ZigBee and Wi-Fi: An Experimental Study. *Wireless Communications and Mobile Computing*. 2006. P. 1–6. https://doi.org/10.1109/WTS.2006.334532.

11. Raza U., Kulkarni P., Sooriyabandara M. Low Power Wide Area Networks: An Overview. *IEEE Communications Surveys & Tutorials*. 2017. Vol. 19, No. 2. P. 855–873. https://doi.org/10.1109/COMST.2017.2652320.

12. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surveys & Tutorials*. 2015. Vol. 17, No. 4. P. 2347–2376. https://doi.org/10.1109/COMST.2015.2444095.

REFERENCES:

1. Sharma, P., Khatri, S. P., Kumar, P. (2023). An intelligent healthcare system using IoT in wireless sensor network. *Sensors*. Vol. 23 (11). P. 1–14.

2. Pinconschi, E., Gopinath, D., Abreu, R., Păsăreanu, C. S. (2024). Evaluating Deep Neural Networks in Deployment: A Comparative Study (Replicability Study). *arXiv preprint arXiv: arXiv:2407.08730v2*.

3. Muñoz-Zavala, A. E., Macías-Díaz, J. E., Alba-Cuéllar, D., Guerrero-Díaz-de-León, J. A. (2024). A Literature Review on Some Trends in Artificial Neural Networks for Modeling and Simulation with Time Series. *Algorithms*. Vol. 17 (2). P. 1–45.

4. Zhu, H., Zhang, H., Lu, W., Li, X. (2023). Foreformer: An enhanced transformer-based framework for multivariate time series forecasting. *Neural Comp. and App*. Vol. 35. P. 14467–14480. DOI: 10.1007/s00521-023-08091-1

5. Wang, Y.-C., Houng, Y.-C., Chen, H.-X., Tseng, S.-M. (2023). Network Anomaly Intrusion Detection Based on Deep Learning Approach. *Sensors*. Vol. 23(4), 2171.

6. Rafique, S. H., Abdallah, A., Musa, N. S., Murugan, T. (2024). Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection–Current Research Trends. *Sensors*. Vol. 24 (6). P. 1–32.

7. Naidu, G. A., Kumar, J. (2019). Wireless Protocols: Wi-Fi SON, Bluetooth, ZigBee, Z-Wave, and Wi-Fi. In R. K. Singh & G. Kumar (Eds.), *Proceedings of the 5th International Conference on IT & Multimedia*. P. 229–239.

8. Alsabah, M., Naser, M. A., Mahmmod, B. M., Abdulhussain, S. H., et al. (2021). 6G Wireless Communications Networks: A Comprehensive Survey. *IEEE Access*. Vol. 99. P. 1–9.

9. Shilpa, B., Radha, R., Movva, P. (2022). Comparative Analysis of Wireless Communication Technologies for IoT Applications. *Artificial Intelligence and Technologies*. P. 383–394.

10. Shuaib, K., Boulmalf, M., Sallabi, F., Lakas, A. (2006). Co-existence of ZigBee and Wi-Fi: An Experimental Study. *Wireless Communications and Mobile Computing*. P. 1–6.

11. Raza, U., Kulkarni, P., Sooriyabandara, M. (2017). Low Power Wide Area Networks: An Overview. *IEEE Communications Surveys & Tutorials*. Vol. 19, No. 2. P. 855–873.

12. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surveys & Tutorials*. Vol. 17 (4). P. 2347–2376.

УДК 004.932:528.854
DOI https://doi.org/10.32782/IT/2024-3-12

Леонід МЕЩЕРЯКОВ
доктор технічних наук, професор, професор кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0002-9579-1970*
***Scopus-Author ID:** 57205282540*

Михайло АЛЕКСЄЄВ
доктор технічних наук, професор, завідувач кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0001-8726-7469*
***Scopus Author ID:** 8987142500*

Микола КУВАЄВ
кандидат технічних наук, науковий співробітник Інституту транспортних систем і технологій НАН України, вул. Писаржевського 5, м. Дніпро, Україна, 49000
***ORCID:** 0000-0002-8560-5433*
***Scopus Author ID:** 56996087200*

Михайло ПІМАХОВ
бакалавр кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005

Бібліографічний опис статті: Мещеряков Л., Алексєєв М., Куваєв М., Пімахов М. (2024). ArchViz додаток на основі Unreal Engine при візуалізації віртуальних середовищ. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 116–123, doi: https://doi.org/10.32782/IT/2024-3-12

ARCHVIZ ДОДАТОК НА ОСНОВІ UNREAL ENGINE ПРИ ВІЗУАЛІЗАЦІЇ ВІРТУАЛЬНИХ СЕРЕДОВИЩ

Функціонально ігрові рушії, що є основою відеоігор, можливо використовувати і для формування віртуальних середовищ. Особливо це важливо при створенні фотореалістичних демонстрацій та презентацій різних інформаційних продуктів, які повністю занурюють користувачів в такий віртуальний простір, що дозволяє збільшити відчуття присутності в реальному фізичному просторі. Програмно ці процедури можливо реалізувати в проектах ґрунтуючись на архітектурної візуалізації.

***Метою роботи** є представлення процесу практичної реалізації створення додатку віртуального середовища архітектурної візуалізації аудиторії університету за допомогою системи програмування Blueprint.*

***Методологія** забезпечення рішення архітектурної візуалізації складається в застосуванні розробки інтерактивного додатку ArchViz, що дозволяє досліджувати створену віртуальну аудиторію із можливістю широкої інтерактивної взаємодії з всіма основними її складовими елементами. Варто зазначити, що при розробці використано лише візуальне програмування Blueprint, що прискорює формування подібного додатку через можливість відображення наочно логіки взаємодій структурних елементів, і що також ніяк не впливає в цілому на оптимізацію проекту.*

***Наукова новизна** запропонованих рішень визначається тим, що завдяки використанню передових можливостей Unreal Engine, таких як система динамічного освітлення, глобальне освітлення в реальному часі та можливості високоточного рендерингу, додаток ArchViz досягає нового підвищеного рівня реалістичності та інтерактивності візуалізації віртуального середовища.*

***Висновки**. Розроблений інтерактивний ArchViz-додаток, може успішно використовуватись при проектуванні приміщень, так як має привабливу фотореалістичну комп'ютерну графіку та містить в собі інтерактивні можливості взаємодії з оточенням. Даний приклад Arch-Viz додатку може вплинути на проектування приміщення в цілому та створити попит на білдингові компанії, що використовують подібні програмні рішення через отримані враження користувача на етапі, коли реальне приміщення ще не існує.*

***Ключові слова:** віртуальний реалізм, інтерактивне, ArchViz, Unreal Engine, Blueprint, Niagara, ігровий рушій, архітектурна візуалізація.*

Leonid MESHCHERIAKOV
Doctor of Technical Sciences, Professor, Professor at the Department of Software Engineering, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, meshcheriakov.l.i@nmu.one
ORCID: *0000-0002-9579-19701970*
Scopus-Author ID: *57205282540*

Mykhailo ALEKSIEIEV
Doctor of Technical Sciences, Professor, Head of the Department of Software Engineering, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, aleksieiev.o.m@nmu.one
ORCID: *0000-0001-8726-7469*
Scopus Author ID: *8987142500*

Mykola KUVAIEV
Candidate of Technical Sciences, Researcher, Institute of Transport Systems and Technologies, National Academy of Sciences of Ukraine, 5, Pisarzhevsky Str., kuvaevnv@ukr.net
ORCID: *0000-0002-8560-5433*
Scopus Author ID: *56996087200*

Mykhailo PIMAKHOV
Bachelor at the Department of Computer System's Software, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, pimakhov.my.v@nmu.one

To cite of article: Meshcheriakov, L., Aleksieiev, M., Kuvaiev, M., Pimakhov, M. (2024). ArchViz dodatok na osnovi Unreal Engine pry vizualizatsii virtualnykh seredovyshch [ArchViz app based on Unreal Engine when visualizing virtual environments. Magazine]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 116–123, doi: https://doi.org/10.32782/IT/2024-3-12

ARCHVIZ APP BASED ON UNREAL ENGINE WHEN VISUALIZING VIRTUAL ENVIRONMENTS

Functionally, game engines, which are the basis of video games, can also be used to create virtual environments. This is especially important when creating exciting demonstrations and presentations of various information products or physical spaces that completely immerse users in such a virtual space, which allows to increase the feeling of presence as if in a real physical space. Programmatically, these procedures can be implemented in projects based on architectural visualization.

The aim *of the work is to present the process of practical implementation of creating a virtual environment application for architectural visualization of the university auditorium using the Blueprint programming system.*

The methodology *for providing a solution to the presented task consists in the application of the development of the interactive ArchViz application, which allows you to explore the created virtual audience with the possibility of interactive interaction with all its main elements. It is worth noting that only Blueprint visual programming was used in the development, which speeds up the development of such an application due to the possibility of visually displaying the logic of interactions, and which also does not affect the optimization of the project in general.*

The scientific novelty *of the proposed solutions is determined by the fact that, thanks to the use of advanced features of Unreal Engine 5, such as the dynamic lighting system, real-time global lighting and high-precision rendering capabilities, the ArchViz application reaches a new level of realism and interactivity of virtual environment visualization.*

Conclusions. *The developed interactive ArchViz application can be used in the design of premises, as it has attractive photorealistic computer graphics and contains interactive opportunities for interacting with the environment. This example of the Arch-Viz application can influence the perception of room design in general and create a demand for building companies using similar software solutions due to the received user impressions at the stage when the real room does not yet exist.*

Key words: *virtual realism, interactive, ArchViz, Unreal Engine, Blueprint, Niagara, game engine, architectural visualization.*

Актуальність проблеми. Величезна обчислювальна потужність сучасних персональних комп'ютерів знайшла застосування в різних інформаційних сферах, серед яких є і множина комп'ютерних ігор. Процедура створення відеоігор вимагає використання ігрового рушія і не зовсім відомо, що ігрові рушії можуть слугувати більш ширшим цілям, ніж просто розробка ігор.

Так їх можна використовувати і для формування віртуальних середовищ, для створення інформативних демонстрацій та презентацій продуктів або фізичних просторів, які не лише захоплюють, але й занурюють кінцевого користувача, дозволяючи йому, ґрунтуючись на проектах архітектурної візуалізації (*ArchViz*) з високим ступенем занурення, відчути простір так, ніби він присутній там фізично.

Використовуючи можливості ігрових рушіїв, компанії та розробники можуть отримати безліч можливостей для презентації своїх продуктів та візуалізації архітектурних споруд. Незалежно від того, чи це демонстрація проекту нерухомості, нової лінійки продуктів, чи захоплююча віртуальна прогулянка майбутнім закладом, потенціал використання ігрових рушіїв для демонстрацій є досить величезним. Завдяки своїй здатності створювати візуально приголомшливе інтерактивне середовище, ці додатки пропонують безпрецедентний рівень залучення потенційних інвесторів та клієнтів. Використовуючи можливості ігрових рушіїв та найсучасніші технології, компанії можуть створювати візуально вражаючі та захоплюючі проекти *ArchViz*, які занурюють користувачів у відповідне віртуальне середовище. Оскільки застосування інформаційних технологій продовжує стрімкий розвиток, можливості використання ігрових рушіїв для демонстрації різнотипових проектів будуть звичайно тільки швидко розширюватися,

Аналіз останніх досліджень і публікацій. Ігрові рушії слугують основою розробки ігор, пропонуючи широкий спектр можливостей та функцій, які спрощують процес та дають можливість розробникам втілювати свої творчі задуми в життя. Їх можна визначити як програмний фреймворк або платформу, яка надає розробникам набір інструментів, бібліотек та систем для створення, розробки і розгортання відеоігор, що слугує проміжною ланкою між кодом гри та апаратним забезпеченням, дозволяючи розробникам зосередитися на логіки та дизайні гри. Функціонально ігрові рушії можливо розділити на: рушій рендерингу, фізичні рушії, звукові рушії, включаючи штучний інтелект, сценарії та мови програмування, конвеєри ресурсів та редактори гри.

На даний час із популярних ігрових рушіїв можна виділити перед усе такі як *Unity, Unreal Engine* та *CryEngine. Unity* широко використовуваний ігровий рушій, відомий своєю універсальністю та простотою використання. *Unreal Engine* відомий своїми дуже широкими візуальними можливостями та високою точністю комп'ютерної графіки. Він надає такі розширені можливості як трасування променів світла у реальному часі та динамічне глобальне освітлення, що дозволяє розробникам створювати візуально вражаючі ефекти занурення. *CryEngine* в основному зосереджений на створенні найсучаснішої комп'ютерної графіки та реалістичних середовищ. Він відмінно справляється з рендерингом великих відкритих просторів, динамічних погодних систем та деталізованих моделей персонажів. Серед розглянутих, найбільш широко використовуваних двигунів, для розробки *ArchViz*-проекту найкращим виступає *Unreal Engine 5*, так як він є оптимальним за багатьма параметрами з усіх запропонованих, містить найновітніші технології та має можливість програмувати за допомогою системи *Blueprint*, яка є візуальною адаптацією мови *C++.*

Метою статті є представлення процесу практичної реалізації створення додатку віртуального середовища архітектурної візуалізації однієї з аудиторій університету за допомогою системи програмування *Blueprint*.

Виклад основного матеріалу. Вирішальне значення для ефективної розробки майбутнього проекту являється вивчення вимог до неї. Щоб розробити програмну систему, ці вимоги повинні бути визначені, виміряні, протестовані та пояснені. Специфікації функціональних вимог проекту, що формується − це опис функцій та їхніх атрибутів, який не містить жодних винятків чи протиріч. Також додаток має бути фотореалістичним та деталізованим, а також мати змогу використовувати систему сучасного реалістичного освітлення.

Опис використаних в проекті елементів та плагінів. Застосована в проекті система *VFX*-частинок реалізована за допомогою системи *Niagara*, ефекти для камери сформовані за допомогою елементу *PostProcessVolume*, погода реалізована завдяки паку *Ultra Dynamic Sky*, реалістичні матеріали були використані з безкоштовної бібліотеки *Quixel Bridge Megascans*, також для матеріалу візуалізації скла було застосовано плагін *Advanced Glass Material Pack*, для імпорту 3D-моделей проекту представленої аудиторії був використаний плагін *Datasmith*, а для *UI*-частини застосовано елемент *Widget,* та в цілому все програмувалось на основі системи *Blueprint*.

Основа опису функціоналу *Niagara* – це система візуальних ефектів наступного покоління в *Unreal Engine 5*. За допомогою *Niagara* технічний художник має можливість створювати додаткову функціональність самостійно, без

допомоги програміста. Система адаптивна та гнучка. Початківці можуть почати з модифікації шаблонів або прикладів поведінки, а досвідчені користувачі можуть створювати свої власні модулі. У системі *Niagara* є чотири основні компоненти: *Системи, Емітери, Модулі* та *Параметри*. Система *Niagara* – це контейнер для всього, що може знадобитись при побудові ефекту. Всередині цієї системи можуть бути розташовані різні блоки, які складаються в модуль для створення загального ефекту.

Опис функціоналу *Post Process Volume* – це спеціальний тип об'єму, який можна додати до рівня для доступу к функціям пост-обробки. Декілька об'ємів можуть бути розміщені для визначення вигляду певної області або встановлені для впливу на всю сцену. Можна додати *Post Process Volume* у свій рівень за допомогою панелі *Place Actors*. Після розміщення на рівні використовується панель *Details* при доступі до всіх можливих властивостей та функцій. Налаштування *Post Process Volume* є специфічними налаштуваннями для цього розміщеного об'єму та його взаємодії зі сценою та будь-якими іншими об'ємами *Post Process*, з якими вони можуть перекриватися. Наприклад, можна перемикати властивість *Infinite Extent*, щоб зробити цей об'єм *Post Process*, що впливає на все, що розміщено на сцені, або залишити його невстановленим, щоб вплинути лише на певну область сформованої сцени.

Функціонал пакету *Ultra-Dynamic Sky (UDS)* – це пак для *Unreal Engine 5*. *UDS* – це система неба, розроблена для більш динамічного та природного вигляду, ніж більшість попередніх рішень по візуалізації неба, пропонує велику гнучкість та можливості налаштування з інтерфейсом, що розроблений для підвищення простоти та швидкості обробки. За допомогою *Ultra-Dynamic Sky* можна налаштувати час доби і всі аспекти неба будуть оновлюватися разом з ним. Система має повністю динамічні хмари, місяць та зорі. Вбудоване освітлення з сонцем, місяцем та освітленням синхронізується з небом. Можна налаштувати хмарність від ясного неба до похмурого. Також є повна система погоди – *Ultra-Dynamic Weather*, яка додає до сформованої сцени дощ, сніг, блискавку та інші погодні сутності (Everett Gunther, 2022; Unreal Sensei, 2022).

Основа опису функціоналу *Quixel Bridge* – це плагін для *Unreal Engine 5*, який дозволяє отримати повний доступ до бібліотеки *Megascans* прямо у редакторі рівнів. Є можливість переглядати колекції, шукати конкретні активи та додавати активи до проектів *Unreal Engine*. *Quixel Bridge* для *Unreal Engine* встановлюється та активується за замовчуванням. Можна відкрити його з головної панелі інструментів: для цього потрібно натиснути кнопку *Створити*, а потім відповідно вибрати *Quixel Bridge*. Після відкриття *Bridge* потрібно увійти у свій обліковий запис *Epic Games*.

Опис функціоналу системи програмування *Blueprints* – це система візуального скриптування в *Unreal Engine 5*, яка дозволяє створювати геймплей без написання коду. За допомогою *Blueprint* можливо створювати логіку гри, інтерактивні об'єкти, інтерфейс користувача та багато іншого. *Blueprints* мають графічний інтерфейс, де можливо перетягувати та з'єднувати вузли для створення структури потрібної логіки. Вони мають ряд основних компонентів, таких як функції, змінні та події. Можна створювати свої власні *Blueprint* класи або унаслідуватися від існуючих класів *Unreal Engine*. Саме тому вся програмна частина розробляється логічними блоками через систему *Blueprints*.

Опис створення сцени. Керування від першого обличчя. Для створення *ArchViz* додатку було синтезовано новий проект *Unreal Engine 5* із шаблоном *First Person*. Після чого відкриється початковий рівень та інші панелі. Далі необхідно відкрити *BP_FirstPersonCharacter*, що знаходиться за шляхом *All->Content->FirstPerson->Blueprints* та видалити в ньому елемент *FirstPersonMesh*, щоб в *ArchViz*-проекті не було недоречних «роботичних рук». Також необхідно встановити постійну швидкість руху – для цього в елементі *Character Movement* встановлюється значення *Max Walk Speed* на 300. Також для того, щоб користувач не міг випадково застрягти у геометрії рівня, потрібно ввести заборону і для цього потрібно вимкнути параметр *Can Jump*.

Імпорт моделей та створення матеріалів. Для створення віртуальної аудиторії потрібно відкрити новий рівень та імпортувати заздалегідь сформовану *3D*-модель аудиторії. Тут використовується плагін *Datasmith* для *Autodesk 3ds Max* та *Datasmith Importer* для *Unreal Engine 5* (Pamir Garay, 2022; Shoun Foster, 2023).

Так як *Datasmith* – не досить досконалий плагін, то може виникнути проблема зникнення текстур з усіх об'єктів. Вона вирішується імпортом реалістичних матеріалів з безкоштовної бібліотеки *Quixel Bridge*, вбудованої у двигун. З цієї бібліотеки було імпортовано двадцять один матеріал, серед яких: різновиди дерев'яних і мармурових підлог, дерево, пластик, тканини та метал. Також були сформовані власні матеріали завдяки створенню *Master Material'y*

(рис. 1), що дозволяє синтезувати безліч матеріалів, беручи за референс один і той самий, таким чином позитивно впливаючи на оптимізацію всього проекту.

Master Material був створений з урахуванням усіх подальших потреб проекту, а саме: можливість зміни текстур, карт нормалей, карт *Ambient Occlusion*, карт шорсткості, можливість зменшувати та збільшувати текстури та карти, змінювати ступінь металевості матеріалу, ступінь його освітленості, ступінь його шорсткості та можливість зміни кольорової палітри текстури. Після створення цього *Master Material'y* було синтезовано множину об'єктів типу *Material Instance*, кожен з яких має свої значення.

Також було сформовано два окремих матеріали, що не відносяться до *Master Material*. Серед них перший – матеріал для жалюзі, що має у деякій мірі трохи пропускати сонячне проміння, тобто застосована технологія поверхневого розсіювання *Subsurface Shading*, а *Master Material*, створений раніше, не має такої можливості, тому цей матеріал було створено окремо. І окремо було створено матеріал *LampMaton* та *LampMaton_Inst* (*Material Instance*) для ламп на стелі, а також створено *LampMatParameter* для функціонування цих ламп (PrismaticaDev, 2023; Adam the Chips, 2022).

Оптимізація об'єктів та застосування матеріалів. Після завантаження та створення власних матеріалів, потрібно їх застосувати до *3D*-моделей так, щоб це не шкодило загальній оптимізації. Для цього достатньо об'єднати складні об'єкти в одну модель за допомогою опції *ConvertActors To Static Mesh*.

Після об'єднання, потрібно видалити схожі об'єкти та скопіювати один декілька разів у координати схожих об'єктів. Таким чином було об'єднано деталі однієї парти, деталі однієї навчальної дошки, видалено інші парти, та другу дошку, залишено лише один стілець, одну лампу на стелі, два види жалюзі (довгі і короткі) та повторно скопійовано всі ці об'єкти, після чого до кожної моделі на сцені було застосовано свій *Material Instance* (рис. 2).

Задання глобального освітлення та спецефектів. Існує декілька шляхів задання глобального освітлення: власноруч або плагінами/паками (наборами пакетів). В даному проекті використовується придбаний пак *Ultra-Dynamic Sky* задля економії часу та отримання фотореалістичного результату. Цей пак додається до проекту через лаунчер *Epic Games*. Таким чином, у вкладці *Details* для *Ultra_Dynamic_Sky* було задано стартовий час доби 09:36 ранку, ввімкнене параметр *Animate Time of Day*, параметру *Volumetric Cloud Rendering Mode* задано значення *Full Cinematic Quality*, ввімкнене параметри *Enable Fog Inside Clouds*, *Two Layers, Use Cloud Shadows, Simulate Real Sun, Simulate Real Moon* та *Simulate Real Stars*, задано дату 26.04.2024, задано координати широти і довготи згідно координат університету, узятих з *Google Maps*, а саме: для *Latitude* задано значення 48.455312, для *Longitude* задано значення 35.061639.

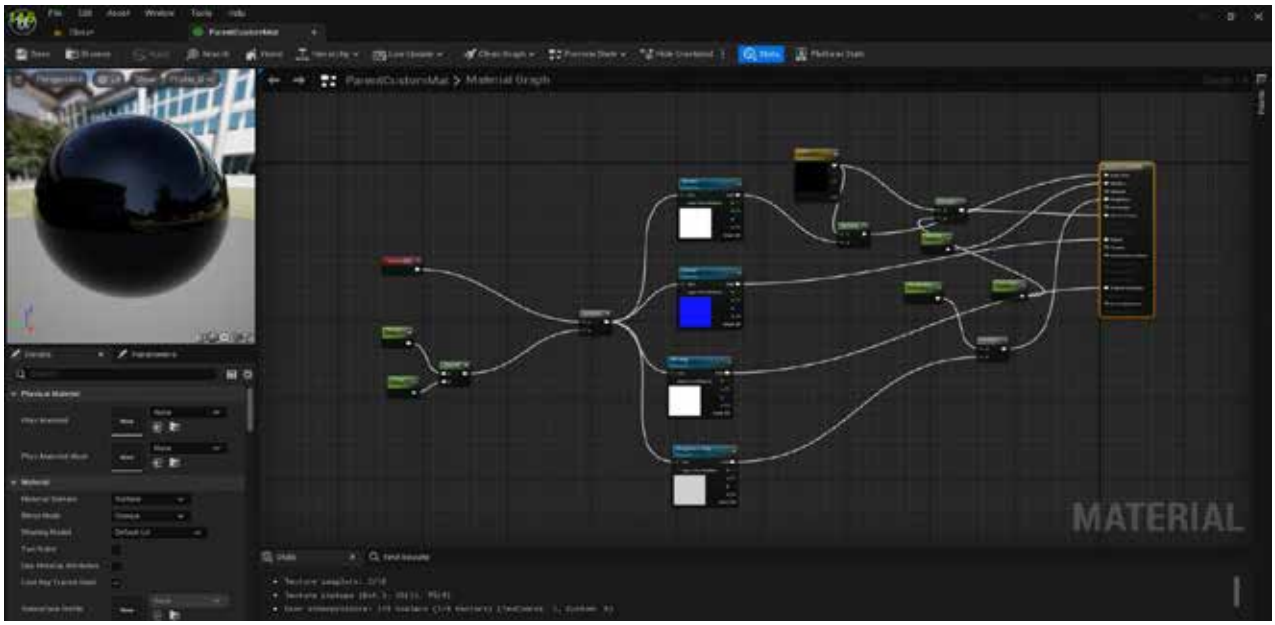


Рис. 1. Master Material

Рис. 2. Створене віртуальне середовище із застосованими матеріалами

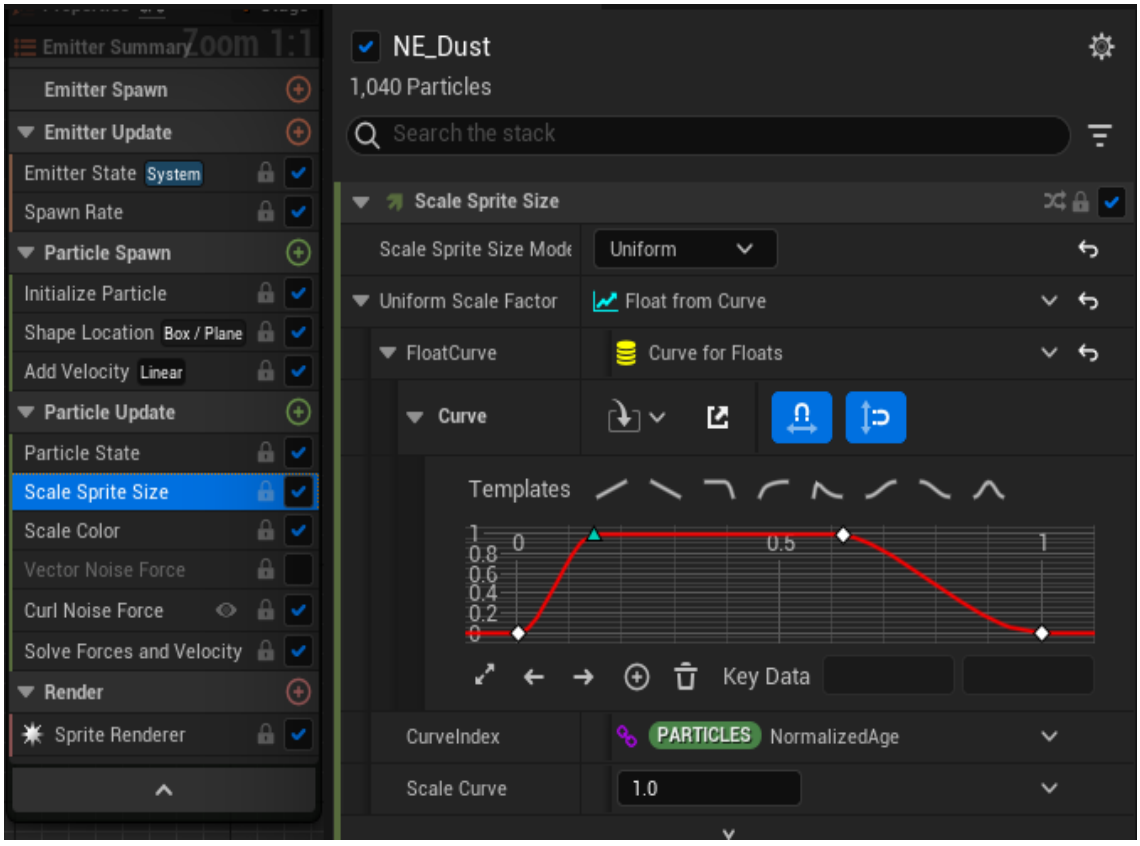


Рис. 3. Налаштування Scale Sprite Size

Також, для пост-процесінгу, до сцени було додано *PostProcessVolume* із набору стандартних інструментів, в якому були ввімкнені хроматична аберація, віньєтування, ввімкнене параметр *Infinite Extend (Unbound)* у розділі *Bloom* параметру *Method* задане значення *Convolution*, в розділі *Exposure* для *Metering Mode* задано значення *Manual*, ввімкнене параметр *Apply Physical Camera Exposure*, задані значення *Min Brightness*: 20, *Max Brightness*: 20, *Speed Up*: 3, *Speed Down*: 1, було ввімкнене *Dirt Mask* з інтенсивністю 2.048 та змінені інші основні параметри. На основі системи частинок *Niagara* для задання атмосфери сцени було створено систему літаючих пилинок. При налаштуванні системи було змінено такі параметри, як *Emitter State*, *Spawn Rate*, *Initialize Particle*, *Shape Location*, *Add Velocity*, *Particle State*, *Scale Sprite Size* (рис. 3), *Scale Color* (рис. 4), *Curl Noise Forse*, *Sprite Renderer*.

Таким чином, в результаті проведених проектних робіт із можливими спецефектами та освітленням, був досягнутий досить задовільний фотореалістичний *3D*-рендер в реальному часі для створеного віртуального середовища однієї з аудиторій університету (рис. 5).

Висновки. Розроблений інтерактивний *ArchViz*-додаток, може використовуватись при проектуванні приміщень, так як має привабливу фотореалістичну комп'ютерну графіку та містить в собі інтерактивні можливості взаємодії з оточенням: можливості підібрати підлогу зі списку запропонованих дизайнерами, або змінити колір крісла на один із списку, або взагалі замінити деякі крісла на диван и побачити, як саме його потрібно буде збирати. Можливо змінювати рішення з приводу проектування приміщення, дивлячись на те, як воно виглядатиме вдень, вночі, під світлом ламп, при ясній погоді або грозовій. Даний приклад *Arch-Viz* додатку може вплинути на уявлення проектування приміщення в цілому та створити попит на білдингові компанії, що використовують подібні програмні рішення через отримані враження користувача на етапі, коли реальне приміщення ще не існує. Варто зазначити, що при розробці було використано лише візуальне програмування *Blueprint*, що прискорює розробку подібного додатку через можливість побачити логіку наочно, і це ніяк не впливає на оптимізацію проекту та є досить простим в розумінні задач програмної інженерії.

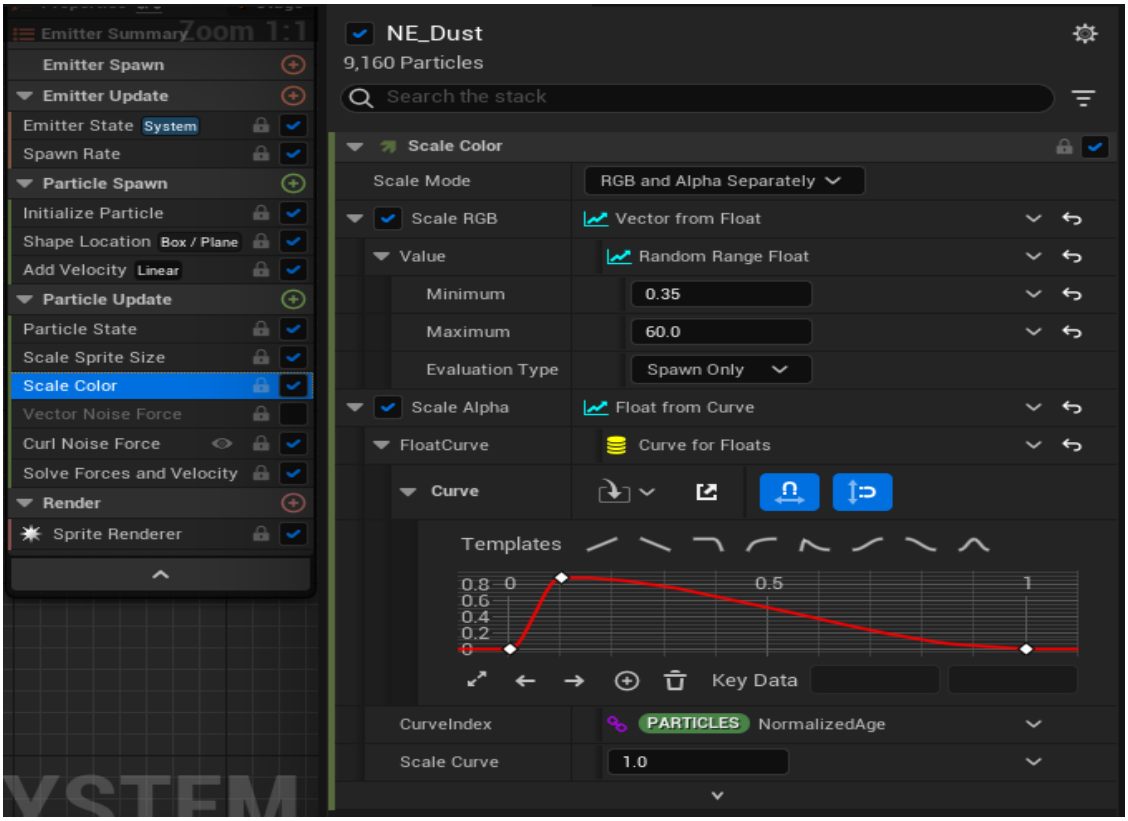


Рис. 4. Налаштування Scale Color

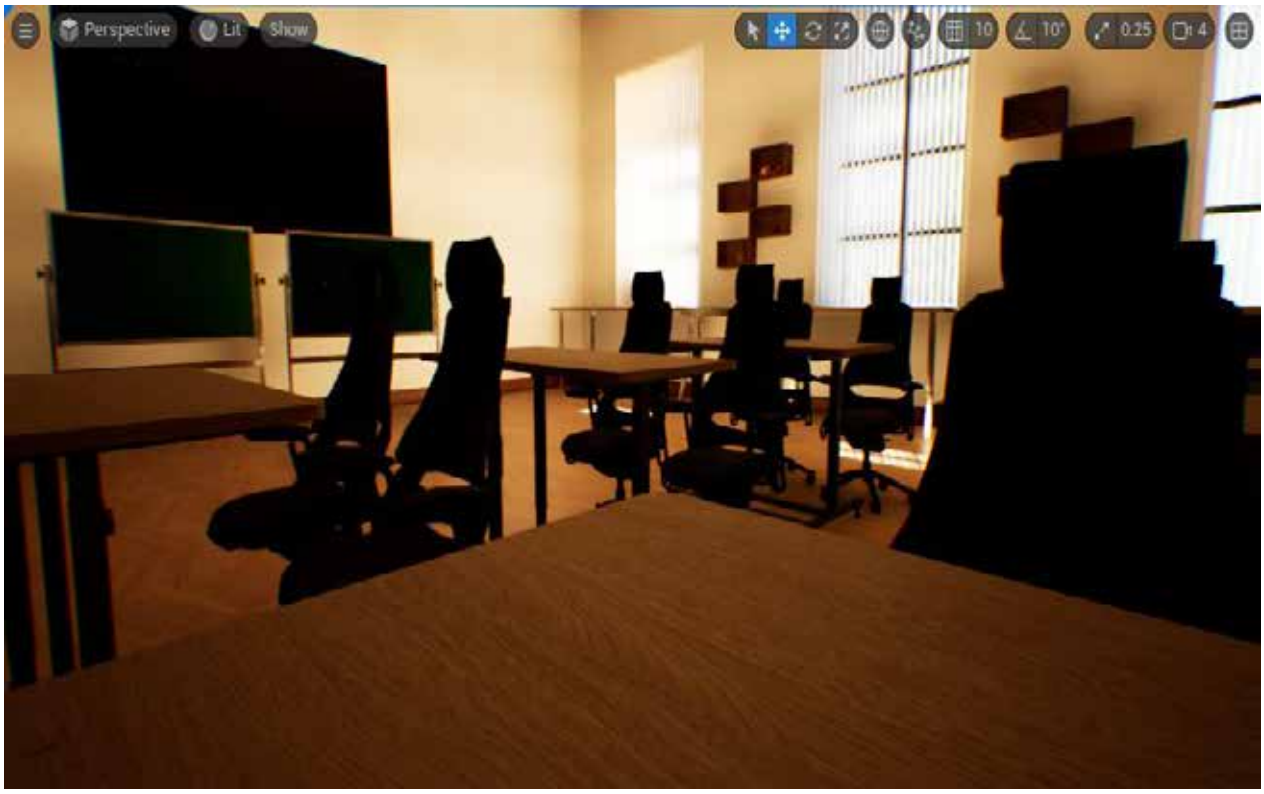


Рис. 5. Результат рендеру віртуального середовища в реальному часі

ЛІТЕРАТУРА:

1. Ultra Dynamic Sky – Product Video + Quick Start (UE5 Version): https://youtu.be/b52npy-XUdQ
2. Навчальний посібник з Unreal Engine 5 для початківців – початковий курс UE5: https://youtu.be/k-zMkzmduqI
3. Unreal Engine 5 Import A Scene By Datasmith From 3DS Max 2022.2: https://youtu.be/kSDDetL3bYg
4. Master Material Basics! Unreal 5 (Must KNOW workflow!): https://youtu.be/tT0ANO5sXso
5. Material Parameter Collection | 5-Minute Materials [UE5]: https://youtu.be/J2Qf5v9_uSY
6. How to convert placed actors/meshes into blueprints UE5: https://youtu.be/MSYki36PJh8

REFERENCES:

1. Ultra Dynamic Sky – Product Video + Quick Start (UE5 Version): https://youtu.be/b52npy-XUdQ
2. Навчальний посібник з Unreal Engine 5 для початківців – початковий курс UE5: https://youtu.be/k-zMkzmduqI
3. Unreal Engine 5 Import A Scene By Datasmith From 3DS Max 2022.2: https://youtu.be/kSDDetL3bYg
4. Master Material Basics! Unreal 5 (Must KNOW workflow!): https://youtu.be/tT0ANO5sXso
5. Material Parameter Collection | 5-Minute Materials [UE5]: https://youtu.be/J2Qf5v9_uSY
6. How to convert placed actors/meshes into blueprints UE5: https://youtu.be/MSYki36PJh8

UDC 004.932:528.854
DOI https://doi.org/10.32782/IT/2024-3-13

Leonid MESHCHERIAKOV
Doctor of Technical Sciences, Professor, Professor at the Department of Software Engineering, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, meshcheriakov.l.i@nmu.one
ORCID: *0000-0002-9579-19701970*
Scopus-Author ID: *57205282540*

Nataliia ULANOVA
Candidate of Technical Sciences, Associate Professor at the Department of Applied Mathematics, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, ulanova.n.p@nmu.one
ORCID: *0000-0001-8460-5266*

Vira PRYKHODKO
Candidate of Technical Sciences, Associate Professor at the Department of Applied Mathematics, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, prykhodko.v.v@nmu.one
ORCID: *0000-0002-5669-5927*

Mykhailo PIMAKHOV
Bachelor at the Department of Computer System's Software, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, pimakhov.my.v@nmu.one

To cite of article: Meshcheriakov, L., Ulanova, N., Prykhodko, V., Pimakhov, M. (2024). Prohramuvannia protsesiv keruvannia ta lohiky na stseni virtualnoi audytorii v seredovyshchi ArchViz [Programming control processes and logic on the stage of a virtual audience in the ArchViz environment]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 124–132, doi: https://doi.org/10.32782/IT/2024-3-13

PROGRAMMING CONTROL PROCESSES AND LOGIC ON THE STAGE OF A VIRTUAL AUDIENCE IN THE ARCHVIZ ENVIRONMENT

The scope of application of virtual models of the final product has great potential for presentation to consumers. By offering an interactive exploration of the virtual classroom space, users can interact with and manipulate various elements of the environment, gaining a deeper understanding of the space and its potential use.

The aim *of the work is to present the process of practical implementation of the creation of an application of a virtual environment for architectural visualization of a university classroom using the Blueprint programming system.*

The methodology *for ensuring the application of the development of the interactive application ArchViz, which allows you to explore the created virtual audience with the possibility of interactive interaction with all its main elements.*

The scientific novelty *of the proposed solutions is determined by the fact that through the use of advanced features of Unreal Engine 5, such as a dynamic lighting system, real-time global lighting, and high-precision rendering capabilities, the ArchViz application achieves a new increased level of realism and interactivity in visualizing the virtual environment.*

Conclusions. *The practical value of the study lies in the ability to comprehensively consider interior design options through virtual models without the need for physical reconstruction or presence in real space.*

Key words: *virtual realism, ArchViz, Blueprint, Niagara.*

Леонід МЕЩЕРЯКОВ
доктор технічних наук, професор, професор кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
ORCID: *0000-0002-9579-1970*
Scopus-Author ID: *57205282540*

Наталія УЛАНОВА
кандидат технічних наук, доцент кафедри прикладної математики, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0001-8460-5266*

Віра ПРИХОДЬКО
кандидат технічних наук, доцент кафедри прикладної математики, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0002-5669-5927*

Михайло ПІМАХОВ
бакалавр кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005

Бібліографічний опис статті: Мещеряков, Л., Уланова, Н., Приходько, В., Пімахов, М. (2024). Програмування процесів керування та логіки на сцені віртуальної аудиторії в середовищі ArchViz. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 124–132, doi: https://doi.org/10.32782/IT/2024-3-13

ПРОГРАМУВАННЯ ПРОЦЕСІВ КЕРУВАННЯ ТА ЛОГІКИ НА СЦЕНІ ВІРТУАЛЬНОЇ АУДИТОРІЇ В СЕРЕДОВИЩІ ARCHVIZ

Область застосування віртуальних моделей кінцевого продукту має в майбутнім великий потенціал для представлення споживачам. Пропонуючи інтерактивне дослідження простору віртуальної аудиторії, користувачі можуть взаємодіяти з різними елементами середовища та маніпулювати ними, отримуючи глибше розуміння простору та його потенційного використання.

***Метою роботи** є представлення процесу практичної реалізації створення додатку віртуального середовища архітектурної візуалізації аудиторії університету за допомогою системи програмування Blueprint.*

***Методологія** забезпечення застосування розробки інтерактивного додатку ArchViz, що дозволяє досліджувати створену віртуальну аудиторію із можливістю інтерактивної взаємодії з всіма основними її елементами.*

***Наукова новизна** запропонованих рішень визначається тим, що завдяки використанню передових можливостей Unreal Engine 5, таких як система динамічного освітлення, глобальне освітлення в реальному часі та можливості високоточного рендерингу, додаток ArchViz досягає нового підвищеного рівня реалістичності та інтерактивності візуалізації віртуального середовища.*

***Висновки.** Практична цінність дослідження полягає в можливості через віртуальні моделі здійснити всебічний огляд варіантів дизайну приміщень без необхідності фізичної реконструкції або присутності в реальному просторі.*

***Ключові слова:** віртуальний реалізм, ArchViz, Blueprint, Niagara.*

Актуальність проблеми. Прогнози щодо розвитку досліджень віртуального моделювання вказують на подальший прогрес у сфері додатків в середовищі *ArchViz.* Основною метою тут являється встановлення нового стандарту якості, використовуючи досягнення в області технологій, фотореальної графіки та інтерактивності, що надаються рушієм *Unreal Engine 5*. Розсуваючи межі можливого, очікується, що майбутні розробки ще більше підвищать реалістичність, занурення та зручність використання додатків *ArchViz*, встановлюючи нові стандарти для індустрії віртуального моделювання.

Аналіз останніх досліджень і публікацій. Методи створення інтерактивних *3D*-презентацій, зокрема у сфері архітектурної візуалізації, з використанням рушія *Unreal Engine 5* на даний час знаходять все більше застосування (Everett Gunther, 2022; Unreal Sensei, 2022). Причому самі ігрові рушії визначаються як програмний фреймворк або платформа, яка надає розробникам набір інструментів, бібліотек та систем для створення, розробки і розгортання відеоігор, що слугує проміжною ланкою між кодом гри та апаратним забезпеченням, дозволяючи розробникам зосередитися на логіки та дизайні гри. Із популярних ігрових рушіїв можна виділити перед усе такі як *Unity, Unreal Engine* та *CryEngine*. *Unity* широко використовуваний ігровий рушій, відомий своєю універсальністю та простотою використання. *Unreal Engine* відомий своїми дуже широкими візуальними можливостями та високою точністю комп'ютерної графіки. Він

надає такі розширені можливості як трасування променів світла у реальному часі та динамічне глобальне освітлення, що дозволяє розробникам створювати візуально вражаючі ефекти. *CryEngine* в основному зосереджений на створенні найсучаснішої комп'ютерної графіки та реалістичних середовищ. Серед розглянутих, найбільш широко використовуваних двигунів, для розробки *ArchViz*-проекту найкращим виступає *Unreal Engine 5*, як оптимальний за багатьма параметрами з усіх запропонованих, що містить найновітніші технології та має можливість програмувати за допомогою системи *Blueprint*.

Метою статті є представлення процесу практичної реалізації створення додатку віртуального середовища архітектурної візуалізації аудиторії університету за допомогою системи програмування *Blueprint*.

Виклад основного матеріалу. Для програмування взаємодії з оточенням на сцені віртуальної аудиторії було розроблено візуальний інтерфейс через клас *UserWidget*. Наверху по центру було вирішено розташувати годинник та слайдер для зміни часу. Слайдеру задано значення 960 (значення співпадає зі стартовим значенням часу в об'єкті *Ultra_Dynamic_Sky*) та величину кроку виставлено 0.000001 (Pamir Garay, 2022; Shoun Foster, 2023), щоб точність зміни часу залежала лише від роздільної здатності дисплею користувача. В якості годинника у віджет *LevelWidget* інтегровано віджет *UDS_Digital_Clock*, що йде у комплекті з *Ultra_Dynamic_Sky* та має пряму прив'язку до нього по параметру часу.

В правому верхньому куті розташовано панель для керування погодою. Ця панель складається з елементів *Slider*, *Image* та скопійовано елементи *Background* та *Background Blur* з віджету *UDS_Digital_Clock* для створення єдиного стилю. Після створення та розташування елементів, до кожного із них було застосовано прив'язку *Anchor*, аби незалежно від розміру вікна та роздільної здатності екрану, усі користувачі мали однакове розташування елементів інтерфейсу.

Після розробки візуальної складової користувацького інтерфейсу запрограмовані його елементи для досягнення бажаного функціоналу. У вкладці *Event Graph* до події *Event Construct* підключено блоки з отриманням інформації про об'єкти *Ultra_Dynamic_Sky* та *Ultra_Dynamic_Weather* та задано цим об'єктам змінні-референси (рис. 1) (PrismaticaDev, 2023; Adam the Chips, 2022).

Елементу *Slider_0* потрібно задати функціонал для зміни часу доби. Для цього, в розділі *Event Graph* обрано цей елемент та додано подію *On Value Changed*, що відповідає за те, що відбудеться при зміні значення даного елементу (рис. 2). У вхід *Set Time Of Day* прив'язано значення із плаваючою точкою *Value* із події *On Value Changed (Slider_0)*, а у вхід *exec* прив'язано вихід *exec* з блоку *Get All Actors Of Class*. Таким чином, логіка зміни часу користувачем буде така: якщо змінено значення слайдеру → відтворити зміну параметру часу на встановлене значення слайдеру для отриманого раніше об'єкту *Ultra_Dynamic_Sky* (референс до змінної *Time of Day*).

Після програмування зміни часу доби, потрібно запрограмувати зміну погоди. Для того, щоб користувач міг змінити погоду на потрібну необхідно додати зображення,

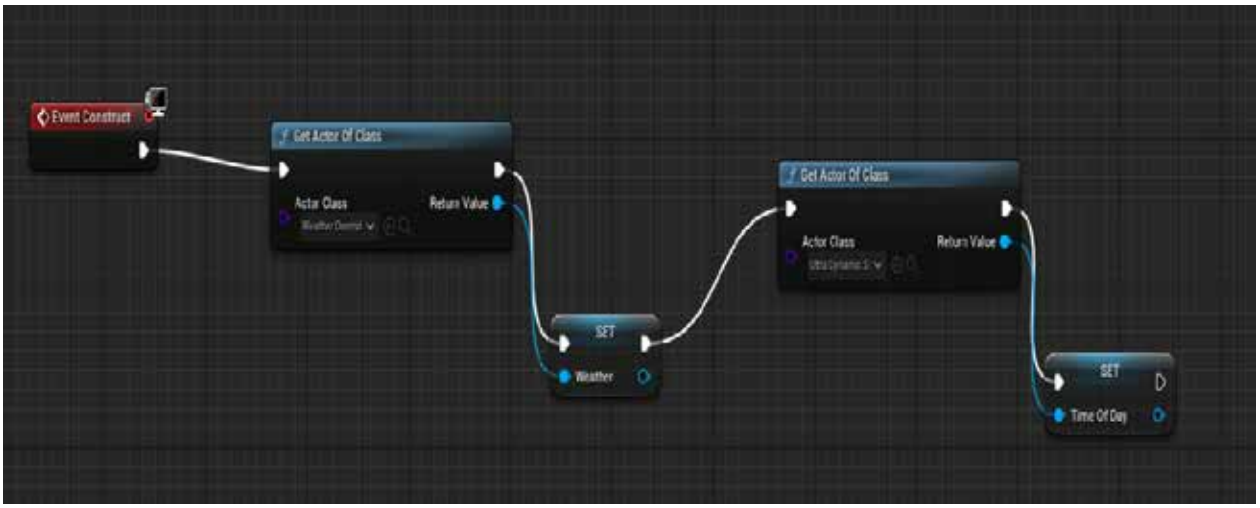


Рис. 1. Логіка *Ultra_Dynamic_Sky* та *Ultra_Dynamic_Weather*

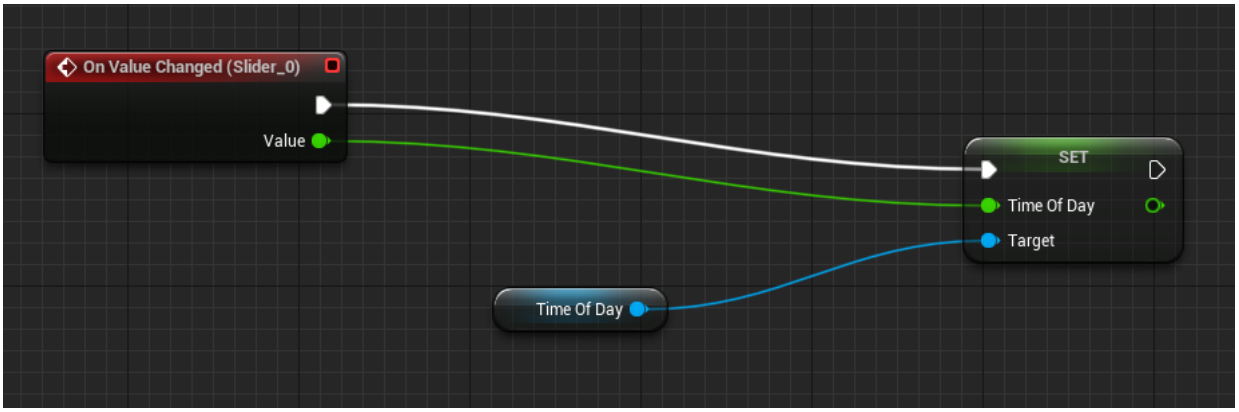


Рис. 2. Логіка для задання часу

що відповідатимуть заданому параметровому стану погоди. Зображення ідентифікації погоди залучено з сервісу *iconfinder.com*, відредаговано та змінено їх кольори на білий та створено з них додаткового зображення *partly_cloudy_weather_icon.png*. Усього використовується сім станів погоди: сонячна *(Clear_Skies)*, хмарна *(Cloudy)*, похмуро *(Overcast)*, частково хмарна *(Partly_Cloudy)*, дощ *(Rain)*, легкий дощ *(Rain_Light)* та дощ із грозою *(Rain_Thunderstorm)*. Кожному з цих станів відповідає своє зображення.

Після цього, в *Event Graph*, подібно до часу доби, але вже для елементу *Slider_1* створено подію *On Value Changed* та створено логічний ланцюг з блоків, логіка якого така: якщо змінено значення слайдеру то перетворити це значення в ціле число, а якщо це значення дорівнює порядковому номеру погоди на слайдері (*0 – 6*), то для отриманого раніше об'єкту задати відповідне значення погоди згідно його порядку та встановити відповідну піктограму в елемент *Image_0*.

Також, для інформування користувача про клавіші для керування оточенням, було створено окремий віджет з назвою *ControlsWidget*, що містить у собі напівпрозорий елемент *Backgound* та розмиття *Background Blur*.

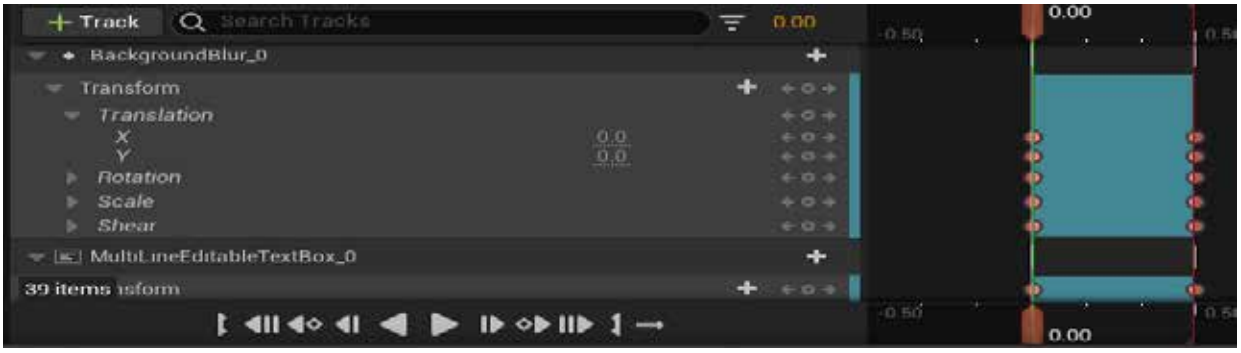
Після створення анімації шляхом проставлення кейфреймів та логіки віджету, досягнуто функціоналу, що дозволяє показати та приховати цей віджет із супроводженням плавної анімації (рис. 3).

Логіка сцени. На сцені віртуальної аудиторії присутні два об'єкти що мають містити в собі логіку для взаємодії з оточенням, а саме: настінний годинник та ноутбук. Ці два об'єкти повинні показувати поточний час доби на сцені в режимі реального часу із врахуванням можливості контролю часу користувачем. Так як проект вже містить в собі систему глобального освітлення, а саме *Ultra Dynamic Sky*, реалізація цього значно спрощується. Для того, щоб ноутбук мав відображення поточного часу, було створено віджет *PCTime*, який містить у собі лише елемент *Image* із скріншотом *OC Windows 11* та заздалегідь дубльований віджет *UDS_Digital_Clock*, але без фону та заданим чорним кольором шрифту.

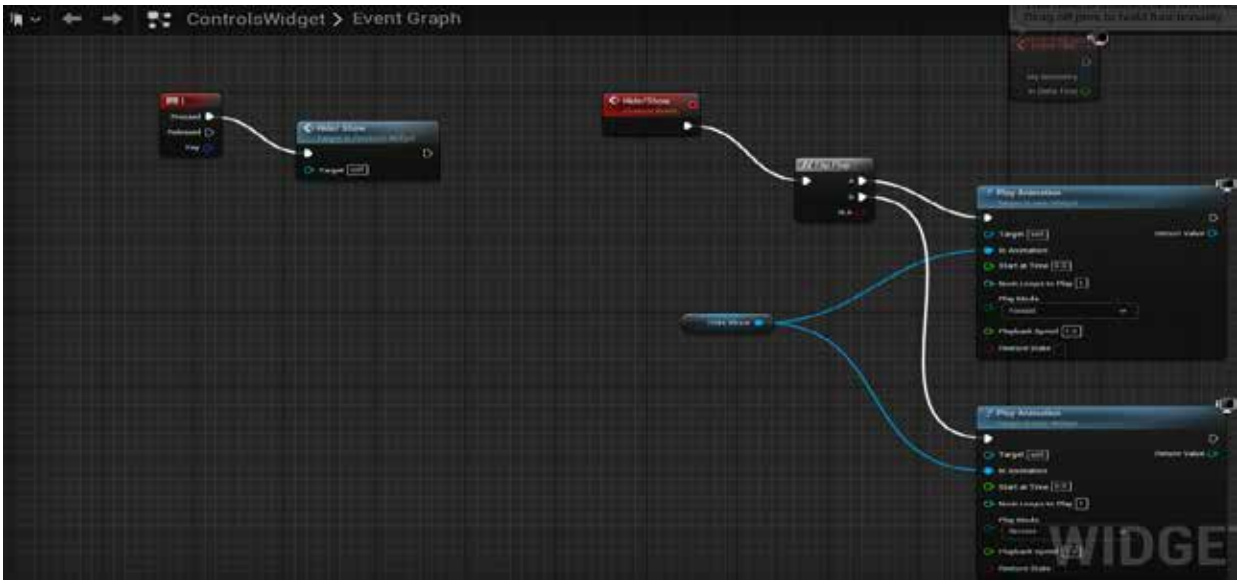
В подальшому створено об'єкт *PCTimeActor* класу *Actor* через розділ *Blueprint Class* та додано до нього елемент *Widget*, що посилається на *PCTime*. Це зроблено для можливості розміщення цього віджету у *3D*-просторі (рис. 4).

Після створення цього об'єкту, його було розміщено на координатах екрану ноутбуку. Таким чином отримано імітацію робочого ноутбуку через показання на ньому реального часу. А для того, щоб настінний годинник також показував поточний час, зі сцени було вилучено меші (об'єкти *Static Mesh*) годинникових стрілок та створено об'єкт *WallClock*, що містив у собі ці меші. Після цього годинникові стрілки було запрограмоване таким чином, щоб вони брали поточний час з компоненту *Ultra Dynamic Sky*, для часової стрілки бралося 1200%, а для хвилинної – 100% і здобуті значення застосовувались до власного обертання. Увесь цей код виконується кожний тік, що дозволяє стрілкам обертатися плавно, як це відбувається в реальному житті.

Також, на сцені містяться об'єкти з якими користувач може взаємодіяти самостійно. Серед них: лампи на стелі, підлога, крісла в лаундж-зоні та диван з піддонів, що початково знаходиться поза межами аудиторії. Кожен з цих видів об'єктів було запрограмовані. Так для ламп був написаний код з подіями, при запуску яких відбувається зміна значення параметру у *LampMatParameter* між станами вимкнено (значення *0.0*) та ввімкнене (значення *1.0*). Для



а.



б.

Рис. 3. Анімація та логіка *ControlsWidget*:
а. – анімація *ControlsWidget*; б. – логіка *ControlsWidget*

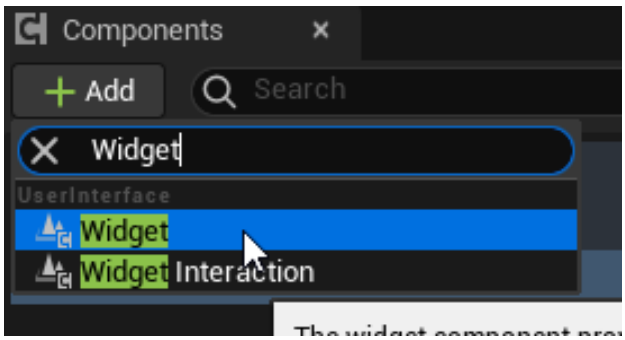


Рис. 4. Створення *PCTimeActor*, що містить в собі *PCTime*

захисту від випадкової взаємодії з лампами (взаємодія відбувається шляхом натиснення клавіші *E*) було вирішено поставити порядок блоку *Flip Flop* таким чином, щоб при першому натисненні на клавішу, до ламп застосовувалося значення «вимкнено». Саме тому після ввімкнення додатку, для найпершої взаємодії з лампами, клавішу потрібно буде натиснути двічі.

Інші об’єкти перед взаємодією при наведенні на них курсором миші, повинні мати обведення, для того аби виділятись на фоні інших об’єктів, що означає, що користувач збирається взаємодіяти саме з цим об’єктом. Також це обведення допоможе користувачу зрозуміти, які об’єкти на сцені взагалі є інтерактивними та з якими можна взаємодіяти. Для цього зі стандартного шаблону *Unreal Engine 4* було імпортовано матеріал для пост-процесінгу під назвою *M_Highlight* та додано його до *PostProcessVolume*.

Далі, для підлоги та стандартних крісел було застосовано один і той самий код з логікою, що запускається кожен тік: визначення стану користувача (чи знаходиться він в режимі редагування) → якщо так, то застосувати до об’єкту параметр глибини (для отримання обведення)

та якщо користувач кликне по об'єкту, з'явиться інтерфейс для зміни кольору, а якщо до цього було відкрито інтерфейс для редагування іншого об'єкту, то він закривається, а обведення того об'єкту припиняється, як при відведенні з нього миші або при виході з режиму редагування. Цей код міститься в кожному із вищезазначених об'єктів, але з різною варіативністю деяких змінних.

Також, для кожного з цих об'єктів було створено власний віджет-інтерфейс взаємодії. Але, існують три об'єкти, в яких є додатковий функціонал. З них – два крісла та один диван. Їх особливість полягає в тому, що при взаємодії з ними, відкривається інтерфейс, що окрім звичайного функціоналу зміни кольору містить в собі кнопку для взаємозаміни (крісла замінюються диваном, а диван – кріслами). Програмно віджети для взаємодії з цими об'єктами відрізняються наявністю виклика події заміни, яку містить у собі диван. Програмна частина спеціальних крісел ніяк не відрізняється від інших.

У дивану код такий самий, як і в інших об'єктів за винятком однієї особливості: він містить у собі анімації переміщення крісел за межі сцени й анімацію переміщення в аудиторію. Анімація є поступовою (показує, як збирається диван), унаслідок чого він не є одним об'єктом – це 5 різних об'єктів, пов'язаних між собою лише інтерфейсом зміни кольору й одночасним завданням обведення для всього дивана, щоб створити видимість цілісності виробу. Анімація зроблена переміщенням по заданим координатам за даний відрізок часу. Усі анімації переміщень мають тривалість 2 секунди, тож для всіх них використовується однаковий блок *Timeline*. Таким чином, було отримано можливість інтерактивної взаємодії з різними аспектами віртуального середовища: від заміни кольору підлоги та меблів до заміни їх типу.

Програмування керування. Для того, щоб користувач міг взаємодіяти зі створеним *User Interface*, перш за все, його потрібно вивести у робочу область дисплею. Для цього у *BP_FirstPersonCharacter* потрібно при запуску проекту (подія *Event BeginPlay*) створити ці віджети та додати їх до *Viewport* (рис. 5).

Після того, як інтерфейс був виведений на екран, потрібно додати гарячу клавішу *P* для того, щоб вмикався режим редагування (з'являвся курсор миші, який вже може взаємодіяти із віджетами та об'єктами, в налаштуваннях яких включена функція *Generate OnClick Events*) (рис. 6).

Також, користувачеві потрібно надати можливість наближувати картинку клавишею *C.* Принцип роботи: при затисненні клавіші *C* відбувається плавна анімація зменшення кута поля зору вдвічі, а при відпусканні клавіші *C* – програється зворотна анімація. Також, за допомогою глобальної змінної *Is Editing* було запрограмоване, щоб користувач не міг збільшувати зображення під час редагування. Так як було створено матеріал та набір параметрів для вмикання/вимикання штучного світла від ламп на стелі, потрібно задати гарячу клавішу *E* на цей функціонал.

Покращення візуального та звукового сприйняття додатку. Щоб покращити сприйняття додатку користувачем, було вирішено додати деякі елементи до проекту, а саме фонову музику, створену нейромережею *soundraw.io*. Спочатку було сформовано музикальну чергу із чотирьох треків за допомогою *Sound Cue* і названо *AmbientMusicCue* (рис. 7).

Після цього було створено об'єкт класу *Actor*, де прописана логіка для старту та закінчення програвання музики. Також є обов'язковим додати користувачеві можливість вмикати та вимикати фонову музику на клавішу *M*.

Для атмосферного вступу у віртуальне середовище, створено пост-процесінговий матеріал, що містить блакитну сітку на чорному фоні, щоб із самого початку надати

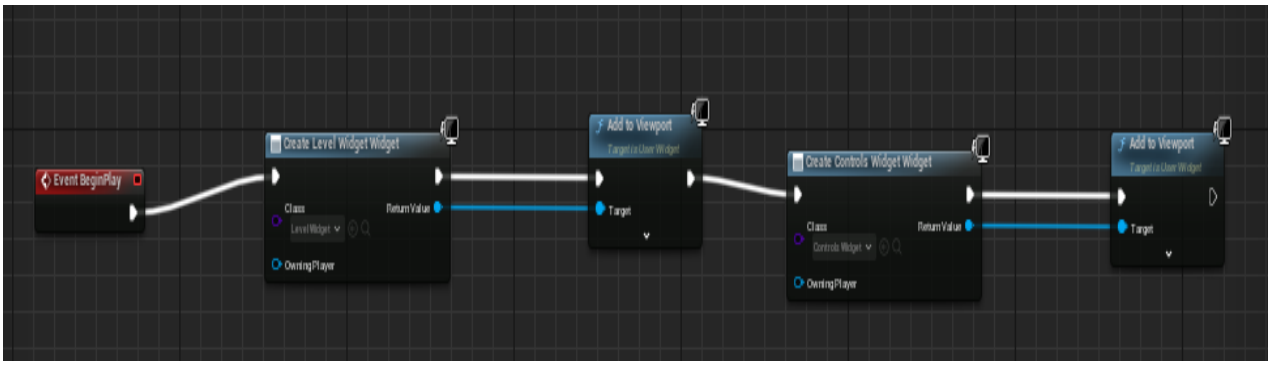


Рис. 5. Логіка виводу віджетів на екран

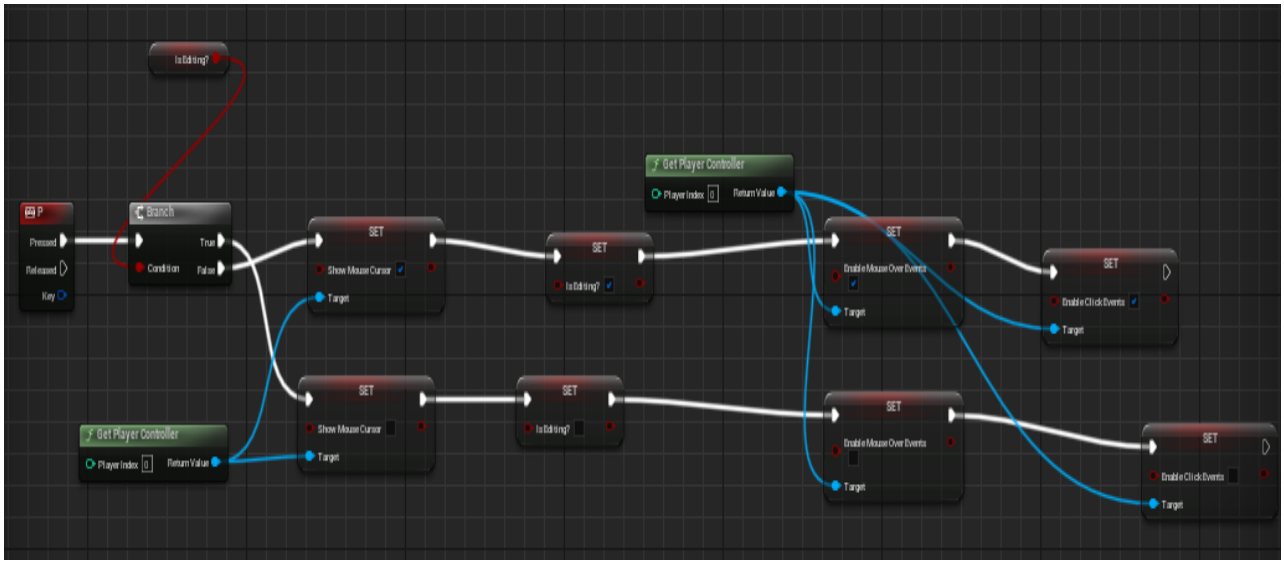


Рис. 6. Логіка вмикання та вимикання режиму редагування

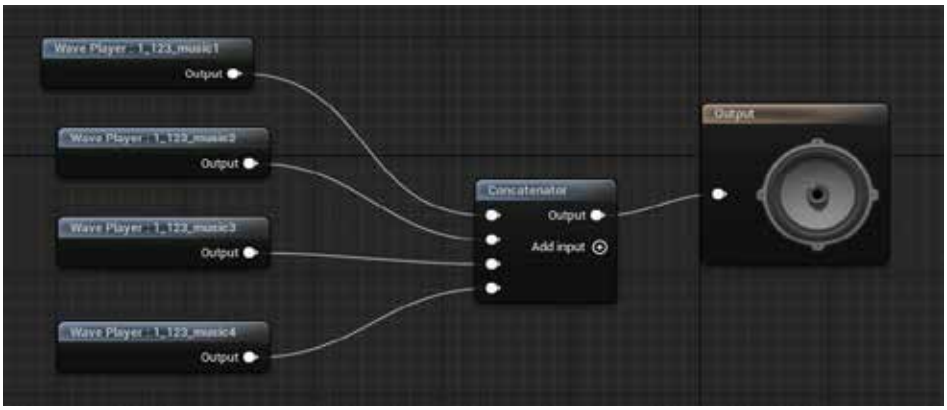


Рис. 7. Музикальна черга *AmbientMusicCue*

користувачеві розуміння того, що перед ним – саме віртуальне середовище, а не фотографія чи прирендер. Також було сформовано набір параметрів для цього матеріалу та створено параметр *Radius*. Після створення матеріалу та набору параметрів, було сформовано його *Material Instance* та додано до ще одного заздалегідь створеного *PostProcessVolume* через розділ *Post Process Materials*. А щоб фонова музика запрацювала з самого початку проекту та щоб відбувся ефект хвилі із сітки, створено логіку, що під'єднана до події *Event BeginPlay* у *BP_FirstPersonCharacter* ( ).

Щоб надати проекту ще більшого реалізму, було вирішено сформувати ефект зйомки з нагрудної камери. Для цього створено два об'єкти класу *CameraShake* і названо *Idle* та *Walk*. Ці об'єкти симулюють трясіння камери при статичному положенні та при ходьбі. Також, було створено пост-процесінговий матеріал, що створює ефект опуклої лінзи і ідентифіковано *M_Fisheye*, після чого створено його *Material Instance* та додано до заздалегідь доданого *PostProcessVolume* під назвою *PostProcessCamera* у *BP_FirstPersonCharacter*. Так як ефект зйомки з відеокамери повинен відбуватись постійно, було сформовано подію, яку далі була прив'язана до події *Event Tick*. А до кнопки що вмикає/вимикає цей ефект було прив'язано лише з задання стану симуляції (змінна *Videorecording Simulation*) та зміна стану застосування *PostProcessCamera*.

Демонстрацію візуального функціоналу сформованого *ArchViz* додатку через його скріншоти представлено на рис. 8. Розроблена модель має великий потенціал для застосування у представленні віртуальних моделей кінцевого продукту різним споживачам. Пропонуючи інтерактивне дослідження простору віртуальної аудиторії, користувачі мають широкі можливості взаємодіяти з різними елементами створеного середовища та маніпулювати ними,

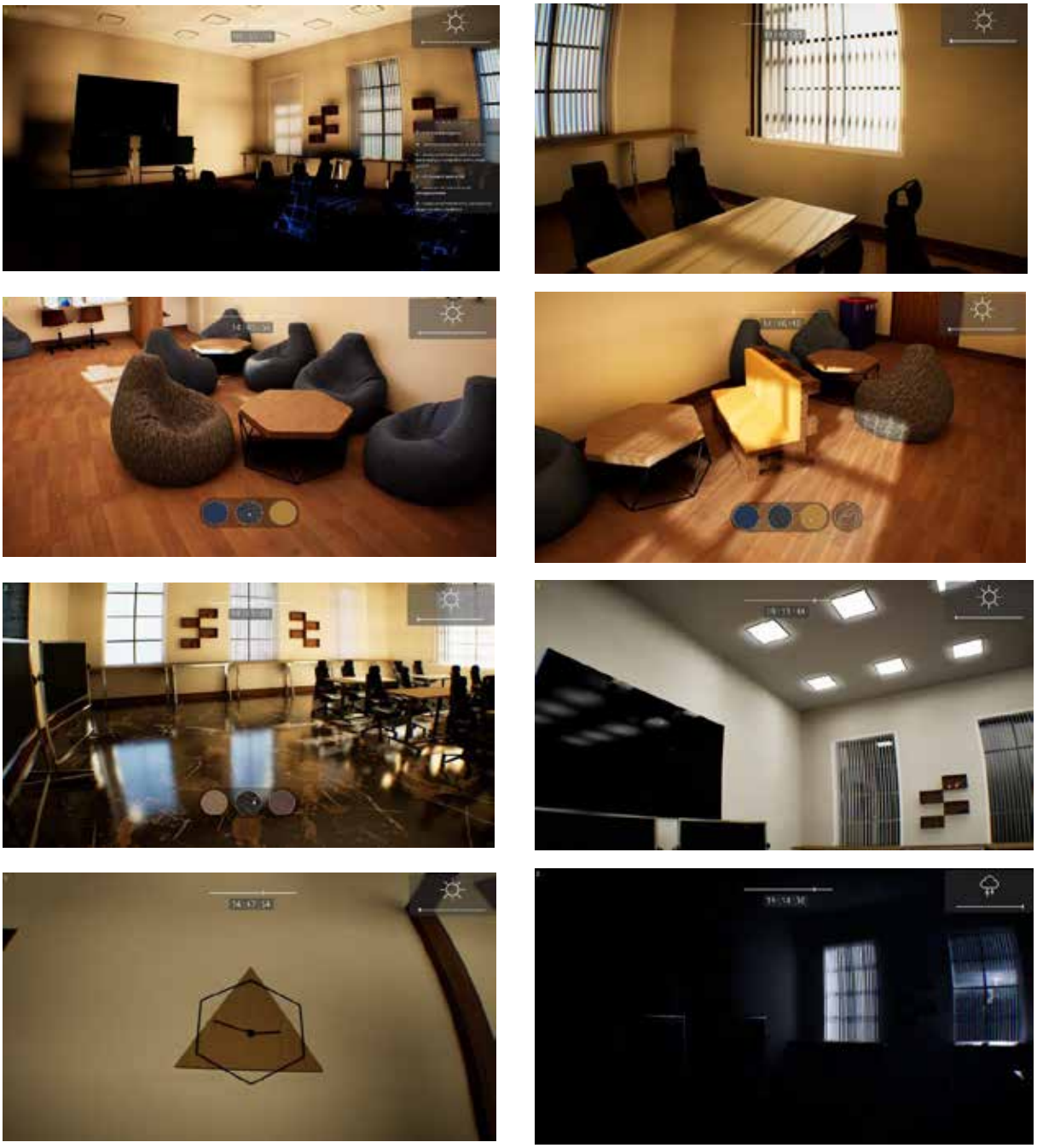


Рис. 8. Скріншоти *ArchViz* додатку з демонстрацією функціоналу

отримуючи глибше розуміння динамічних властивостей сформованого простору та його потенційного використання.

Висновки. Проведені експериментальні дослідження підтверджують позитивний прогноз подальшого прогресу у сфері розробки та використанні віртуальних моделей на базі додатків *ArchViz*. Таким чином, формується встановлення нових вимог до якості віртуального моделювання на основі використання досягнень в області технологій комп'ютерної графіки та інтерактивності, що надаються *Unreal Engine 5*. Розсуваючи межі можливого, очікується, що майбутні розробки ще більше підвищать реалістичність, занурення та зручність використання додатків *ArchViz*, встановлюючи нові стандарти в цьому напрямі для галузі інформаційних технологій.

ЛІТЕРАТУРА:

1. Ultra Dynamic Sky – Product Video + Quick Start (UE5 Version): https://youtu.be/b52npy-XUdQ
2. Навчальний посібник з Unreal Engine 5 для початківців – початковий курс UE5: https://youtu.be/k-zMkzmduqI
3. Unreal Engine 5 Import A Scene By Datasmith From 3DS Max 2022.2: https://youtu.be/kSDDetL3bYg
4. Master Material Basics! Unreal 5 (Must KNOW workflow!): https://youtu.be/tT0ANO5sXso
5. Material Parameter Collection | 5-Minute Materials [UE5]: https://youtu.be/J2Qf5v9_uSY
6. How to convert placed actors/meshes into blueprints UE5: https://youtu.be/MSYki36PJh8

REFERENCES:

1. Ultra Dynamic Sky – Product Video + Quick Start (UE5 Version): https://youtu.be/b52npy-XUdQ
2. Unreal Engine 5 Tutorial for Beginners – UE5 Starter Course: https://youtu.be/k-zMkzmduqI
3. Unreal Engine 5 Import A Scene By Datasmith From 3DS Max 2022.2: https://youtu.be/kSDDetL3bYg
4. Master Material Basics! Unreal 5 (Must KNOW workflow!): https://youtu.be/tT0ANO5sXso
5. Material Parameter Collection | 5-Minute Materials [UE5]: https://youtu.be/J2Qf5v9_uSY
6. How to convert placed actors/meshes into blueprints UE5: https://youtu.be/MSYki36PJh8

УДК 004.4`2 + 004.62
DOI https://doi.org/10.32782/IT/2024-3-14

Юрій МИРОНОВ
аспірант кафедри інформаційних технології та комп'ютерної інженерії, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0009-0006-0675-8033*
***Scopus Author ID:** 58765290900*

Леонід ЦВІРКУН
кандидат технічних наук, професор кафедри інформаційних технологій та комп'ютерної інженерії, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0002-5568-5516*
***Scopus Author ID:** 57209003910*

Бібліографічний опис статті: Миронов, Ю., Цвіркун, Л. (2024). Аналіз методів структурної оптимізації процесів неперервної інтеграції. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 133–139, doi: https://doi.org/10.32782/IT/2024-3-14

АНАЛІЗ МЕТОДІВ СТРУКТУРНОЇ ОПТИМІЗАЦІЇ ПРОЦЕСІВ НЕПЕРЕРВНОЇ ІНТЕГРАЦІЇ

Неперервна інтеграція є важливою практикою в сучасній розробці програмного забезпечення. Ця робота зосереджена на аналізі практичної ефективності застосування методів структурної оптимізації процесів неперервної інтеграції.

***Метою** цієї роботи є огляд і оцінка практичної ефективності різних методів структурної оптимізації, застосованих до процесів неперервної інтеграції в різноманітних програмних середовищах.*

***Методологія**: проведено систематичний огляд літератури із фокусом на публікаціях за останні п'ять років, щоб зафіксувати останні досягнення та нові тенденції в підвищенні ефективності процесів неперервної інтеграції. Для пошуку в академічних базах даних використовувалися такі ключові слова, як «неперервна інтеграція», «оптимізація неперервної інтеграції», «спрямований ациклічний граф», «пріоритизація завдань», «інкрементні збірки» та «паралельне тестування». Критерії огляду зосереджені на високоякісних досліджень, включаючи рецензовані статті в журналах, доповіді на конференціях і професійні публікації. Статті, які явно не зосереджувалися на підвищенні ефективності процесів неперервної інтеграції або не мали емпіричних доказів, були виключені з огляду. Крім того, було проведено експерименти для порівняльного аналізу ефективності та застосовності різних методів оптимізації для різних програмних рішень: S1 – застаріла багатомодульна монолітна система; S2 – веб-застосунок із сервісно-орієнтованою архітектурою; S3 – сучасний застосунок у хмарному середовищі; S4 – рішення «інфраструктура як код» зі складним багатоетапним процесом; S5 – рішення для автоматизації тестування, зосереджене на багатоетапних наскрізних тестах. Результати застосування кожного методу оптимізації були ретельно задокументовані, щоб підтвердити остаточні висновки. Аналіз ефективності базується на аналізі довжини критичного шляху процесу неперервної інтеграції у вигляді графу.*

***Наукова новизна** цього дослідження полягає у використанні методу порівняльного аналізу для оцінки ефективності застосування різних методів структурної оптимізації процесів неперервної інтеграції у складних програмних рішеннях у гібридних середовищах.*

***Результати** дослідження підкреслили неоднаковий вплив кожного методу структурної оптимізації на ефективність процесів неперервної інтеграції в різних рішеннях. Хоча загальна тенденція до більш ефективного виконання процесів очевидна в кожному випадку, ефективність кожного оцінюваного методу відрізняється від одного рішення до іншого. Схоже, що така варіація залежить від багатьох факторів, включаючи стек технологій, розмір кодової бази, внутрішні обмеження, а також розмір і складність процесу неперервної інтеграції. Виявлення цих факторів, а також оцінка методів структурної оптимізації в більшому масштабі для визначення кореляцій між цими факторами та ефективністю процесів неперервної інтеграції можуть стати питаннями майбутніх досліджень.*

***Ключові слова:** неперервна інтеграція, структурна оптимізація, розробка програмного забезпечення, обслуговування програмного забезпечення, оптимізація обчислень.*

Yurii MYRONOV
Postgraduate Student at the Department of Information Technology and Computer Engineering, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005
***ORCID:** 0009-0006-0675-8033*
***Scopus Author ID:** 58765290900*

Leonid TSVIRKUN
PhD, Professor at the Department of Information Technology and Computer Engineering, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005
***ORCID:** 0000-0002-5568-5516*
***Scopus Author ID:** 57209003910*

To cite this article: Myronov, Yu., Tsvirkun, L. (2024). Analiz metodiv strukturnoi optymizatsii protsesiv neperervnoi intehratsii [Analysis of continuous integration structural optimization methods]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 133–139, doi: https://doi.org/10.32782/IT/2024-3-14

ANALYSIS OF STRUCTURAL OPTIMIZATION METHODS FOR CONTINUOUS INTEGRATION PIPELINES

Continuous Integration (CI) is an essential practice in modern software development. This paper focuses on analyzing the practical efficiency of applying structural optimization techniques to continuous integration pipelines.

***The objective** of this work is to review and evaluate the practical efficiency of various structural optimization techniques applied to continuous integration pipelines in diverse software environments.*

***Methodology:** A comprehensive literature review was conducted, focusing on publications from the past ten years to capture recent advancements and emerging trends in CI efficiency improvements. The systematic search of academic databases used keywords such as «Continuous Integration», «CI optimization», «direct acyclic graph», «tasks prioritization», «incremental builds», and «parallel testing». Inclusion criteria ensured the selection of high-quality studies, including peer-reviewed journal articles, conference papers, and industry reports. Articles that did not explicitly focus on CI efficiency improvements or lacked empirical evidence were excluded from the review. Additionally, an experiment was conducted to perform a comparative analysis of the effectiveness and applicability of various optimization techniques across different software solutions: S1 – A legacy multi-module monolithic system; S2 – A web-based application with service-oriented architecture; S3 – A modern cloud-native application; S4 – An Infrastructure as a Code solution with a complex multi-staging pipeline; S5 – A test automation solution focused on multi-staged end-to-end tests. The results of applying each optimization technique were thoroughly documented to support final conclusions. The effectiveness analysis is based on the critical path length analysis of a directed acyclic graph representation of the Continuous Integration pipeline.*

***The novelty** of this research lies in using comparative analysis to evaluate the efficiency of applying various structural optimization techniques to complex software solutions in hybrid environments.*

***The results** of the research highlighted the uneven impact of each structural optimization technique on Continuous Integration pipeline efficiency across the different solutions. While an overall trend toward more effective pipeline execution is evident in each case, the effectiveness of each evaluated method varies from one solution to another. This variation appears to depend on multiple factors, including the technology stack, solution size, inherent limitations, and the size and complexity of the Continuous Integration pipeline. Identifying these factors, as well as evaluating structural optimization techniques on a larger scale to determine correlations between these factors and pipeline efficiency, could be a focus for future research.*

***Key words:** Continuous Integration, structural optimization, software development, software maintenance, computational optimization.*

Актуальність проблеми. Неперервна інтеграція стала фундаментальною практикою в розробці сучасного програмного забезпечення, полегшуючи систематичне тестування та інтеграцію змін програмного коду. Спочатку розроблені для вирішення проблем, пов'язаних з інтеграцією програмного коду, який змінюється одночасно багатьма інженерами, процеси неперервної інтеграції постійно змінюються і відповідно до вимог сучасних середовищ розробки, які характеризуються великими складними кодовими базами, над якими працюють розподілені команди фахівців. Основними об'єктами сучасних робіт у напрямку підвищення ефективності процесів неперервної інтеграції є прискорення зворотного зв'язку та ефективне управління ресурсами (Jin, Servant, 2021), що особливо стає важливим із зростанням популярності хмарних обчислень – підвищення ефективності процесів неперервної інтеграції

має на меті не тільки підвищення ефективності використання обчислювальних ресурсів, але й зниження операційних витрат і скорочення часу випуску нових версій програмного забезпечення. За своєю суттю, процеси неперервної інтеграції є набором взаємопов'язаних завдань обробки програмного коду, які оркеструються (конфігуруються, координуються, впроваджуються, виконуються на керуються) системою неперервної інтеграції в обчислювальному середовищі (Burdiuzha, 2023). Методи підвищення ефективності процесів неперервної інтеграції націлені на кожний з аспектів цих процесів, їх умовно можна поділити на такі категорії: методи оптимізації обчислювального середовища, методи оптимізації кодової бази, методи оптимізації засобів обробки початкового коду, методи оптимізації системи управління процесами, та методи структурної оптимізації (Tsvirkun, Myronov, 2023). Ця робота акцентує увагу на дослідженні методів структурної оптимізації процесів неперервної інтеграції, тобто на методах, які впливають на порядок виконання завдань неперервної інтеграції та їхні зв'язки з метою зменшення загального часу для виконання процесу неперервної інтеграції, безвідносно стану початкового коду, засобів обробки чи обчислювального середовища.

Аналіз останніх досліджень і публікацій. Дослідження методів підвищення ефективності процесів неперервної інтеграції, які можна віднести до категорії методів структурної оптимізації, стосується чотирьох основних напрямів: методу розпаралелювання завдань неперервної інтеграції, методу пріоритизації завдань, методу оптимізації взаємозв'язків завдань шляхом структурування їх у вигляді спрямованого ациклічного графу та методу умовного виконання завдань (Jin, Servant, 2021). Найбільш широко досліджується методи розпаралелювання та умовного виконання завдань, в останньому слід виділити такий напрямок дослідження як використання засобів машинного навчання та штучного інтелекту для розпізнавання змін початкового коду та інтелектуальної побудови переліку завдань неперервної інтеграції (Jin, Servant, 2023). У порівнянні з тим, кількість наукових досліджень методів оптимізації черги завдань та побудови зв'язків у вигляді спрямованого ациклічного графу є незначною (Stahl, 2017). Проаналізовані роботи зосереджені на визначенні впливу застосованих методів на процеси неперервної інтеграції, порівнюючи розроблені методи з аналогічними, однак не містять систематичних порівняльних досліджень з методами інших напрямів.

Мета дослідження. Робота має на меті дослідити вплив сучасних практики підвищення ефективності процесів неперервної інтеграції шляхом оптимізації структури завдань процесів та їхніх взаємозв'язків, на загальний час виконання процесів. Завдання дослідження – визначити ключові методи структурної оптимізації процесів неперервної інтеграції, та порівняти ефективність їх застосування у різноманітному середовищі програмного забезпечення.

Виклад основного матеріалу дослідження. Методи структурної оптимізації є однією з ключових категорій методів підвищення ефективності процесів неперервної інтеграції, і зосереджений на оптимізацію внутрішньої структури процесів та взаємозв'язків між задачами. Як інші методи підвищення ефективності процесів неперервної інтеграції, вони мають на меті пришвидшення зворотного зв'язку із розробниками програмного забезпечення, зменшення часу на виконання завдань обробки даних, а також зменшення кількості обчислювальних програмних ресурсів для виконання завдань.

Найбільш широко застосовуваним методом структурної оптимізації процесів неперервної інтеграції є *метод розпаралелювання завдань*. Цей метод спрямований, в першу чергу, на підвищення ефективності найбільш ресуроємного етапу – кроку тестування, шляхом одночасного виконання кількох завдань.

У традиційних системах неперервної інтеграції завдання тестування часто виконуються послідовно, що створює обмеження продуктивності процесів, особливо в проєктах із великою кількістю тестів. Паралельне тестування вирішує цю проблему, коли тести розподіляються між кількома процесорами або обчислювальними вузлами, що зменшує загальний час, який необхідний для виконання тестів, і прискорює цикл зворотного зв'язку.

Впровадження розпаралеленого тестування передбачає як налаштування програмних засобів тестування, так і зміну структури завдань неперервної інтеграції для одночасного виконання тестів, гарантуючи, що кожен тест ізольований від інших, щоб запобігти перешкодам і хибним результатам. Дослідження паралельного тестування постійно демонструють його ефективність у скороченні часу, яке необхідне для етапу тестування, залежно від складності та розміру набору тестів (Fallahzadeh та ін., 2023).

Скорочення часу призводять до швидшого зворотного зв'язку для розробників, що дозволяє швидше ідентифікувати та вирішувати проблеми. Відповідно до експериментальних

досліджень, особливу ефективність цей метод демонструє у великомасштабних і складних проєктах S1 та S5, у яких довге тестування може затримати випуск нових версій та збільшити витрати на розробку (таблиця 1). Однак впровадження паралельного тестування також пов'язане з ризиком отримання помилкових результатів (Bavand, 2021). При впровадженні методу розпаралелювання завдань тестування важливо проаналізувати потенційні особливості виконуваних тестів на предмет внутрішніх залежностей та доступу до спільних ресурсів.

Метод пріоритизації завдань в процесах неперервної інтеграції є найменш популярною практикою підвищення ефективності процесів, зокрема, через відсутність підтримки у багатьох системах неперервної інтеграції. Тим не менш, цей метод дозволяє забезпечувати більшу ефективність процесів шляхом керування чергою завдань. Спираючись на принципи теорії масового обслуговування, керування чергами в неперервної інтеграції полягає у встановленні пріоритетів завдань збірки, тестування і розгортання програмного забезпечення з метою мінімізації обмежень продуктивності процесів, а також оптимізації використання ресурсів. У теорії масового обслуговування завдання часто організовуються в пріоритетні черги, де важливіші завдання обробляються раніше за інші. Ця концепція безпосередньо застосовна до процесів неперервної інтеграції, де керування порядком і пріоритетом завдань може значно вплинути на загальну ефективність циклу розробки.

Наприклад, високопріоритетні збірки або критичні зміни можна розміщувати на початку черги, забезпечуючи їхню миттєву обробку, тоді як менш критичні завдання ставляться в чергу за ними. Іншим важливим аспектом керування чергами неперервної інтеграції є динамічне керування чергами, яке передбачає налаштування пріоритету завдань у режимі реального часу на основі поточних умов, таких як доступність ресурсів або терміновість конкретної збірки. Наприклад, якщо важливе впровадження нового коду затримується через обмеження ресурсів, система неперервної інтеграції може динамічно перерозподіляти ресурси або коригувати пріоритети завдань для вирішення проблеми, таким чином зберігаючи потік процесу неперервної інтеграції. Дослідження застосування теорії масового обслуговування в процесах неперервної інтеграції продемонстрували, що ефективне керування чергами може призвести до незначного покращення часу використання ресурсів і загальної ефективності неперервної інтеграції (Wang та ін., 2020)

Впроваджуючи пріоритетні черги, системи неперервної інтеграції можуть гарантувати, що найважливіші завдання вирішуються першими, зменшуючи ймовірність виникнення вузьких місць і забезпечуючи більш передбачуваний і надійний процес обробки даних. Поставлений експеримент показав, що впровадження цього методу дозволяє скоротити середній час виконання процесів неперервної інтеграції до 20% (таблиця 1), особливо у масштабних проєктах на декілька інженерних команд, що працюють в умовах обмежених ресурсів.

Ще одним непопулярним методом оптимізації процесів неперервної інтеграції є метод *організації завдань у вигляді спрямованого ациклічного графу*. Цей метод пропонує формалізований підхід для структурування складних процесів обробки даних. У моделі спрямованого ациклічного графу кожен вузол представляє завдання неперервної інтеграції, тоді як ребра між вузлами означають залежності між цими завданнями. Визначальною особливістю методу є гарантія того, що завдання неперервної інтеграції не залежать циклічно один від одного, і таким чином виключаються взаємоблокування або можливість появи нескінченних циклів.

Цей метод оптимізація за своєю суттю підходить для керування залежностями між

Таблиця 1

Експериментальне порівняння ефективності застосування методів структурної оптимізації процесів неперервної інтеграції

Метод структурної оптимізації	Оптимізація часу виконання процесів				
	S1	**S2**	**S3**	**S4**	**S5**
розпаралелювання завдань[1]	0,8n	0,9n	n	N/A[2]	0.8n
пріоритизація завдань	1,1	1,0	1,0	1,0	1,2
організація завдань CAГ	1,7	1,6	1,0	1,2	2,0
умовне виконання завдань	1,4	1,7	1,8	1,2	85,0

[1] n-ступінь паралелізації, n=>2.

[2] Через специфіку проєкту, застосування даного методу не є можливим.

завданнями неперервної інтеграції, які виникають у складних великих процесах. У класичних процесах неперервної інтеграції завдання одного етапу виконуються лише після завершення усіх завдань попереднього етапу. Тому застосування цього методу дозволяє системам неперервної інтеграції порушувати послідовність виконання етапів і виконувати завдання у встановленому порядку, гарантуючи, що завдання виконуються лише тоді, коли задовольняються їхні передумови.

Такий підхід підвищує ефективність процесу неперервної інтеграції, уникаючи непотрібних затримок і оптимізуючи порядок виконання завдань.

Як показують дослідження (Zheng та ін., 2024) та проведений експеримент (таблиця 1), організація завдань неперервної інтеграції у вигляді графів особливо ефективна у великих і складних проєктах із величезною кількістю залежностей, які обмежують продуктивність завдань обробки даних. Репрезентація цих залежностей у графічному виді (як правило, у вигляді діаграм Санкея) дозволяє проводити поглиблений аналіз цих місць і критичного шляху з метою впровадження інших методів оптимізації процесів неперервної інтеграції.

Однак ефективність цього методу залежить від точного визначення залежностей між завданнями і забезпечення того, що ці залежності контрольовані. У середовищах із дуже мінливими або непередбачуваними залежностями, застосування цього методу може спричиняти затримки в обробці даних або неефективне використання обчислювальних ресурсів (Lyu та ін., 2024). Незважаючи на це, за правильного впровадження, метод організації завдань у вигляді спрямованого ациклічного графу залишається потужним інструментом для підвищення ефективності процесів неперервної інтеграції.

Під методом *умовного виконання завдань* неперервної інтеграції розуміється вибірковий запуск завдань обробки даних на основі попередньо визначених правил або інтелектуального розпізнавання контексту змінених даних. Ця практика спрямована на оптимізацію використання ресурсів і скорочення часу процесу неперервної інтеграції шляхом виконання лише необхідних завдань, а не повторного запуску всього процесу для кожної зміни початкового коду. Традиційні системи неперервної інтеграції використовують заздалегідь визначені правила, такі як зміна файлів або ключові слова у змінюваних даних, для визначення переліку завдань для виконання.

Наприклад, тести можуть запускатися лише тоді, коли є зміни у файлах в певному каталозі, що зменшує час на виконання тестів. Хоча застосування методу у його традиційному виді, на основі правил, підвищує ефективність процесів неперервної інтеграції (таблиця 1), ручні налаштування вимагають постійної підтримки з боку інженерів, які повинні регулярно оновлювати правила в міру розвитку проєкту, щоб гарантувати відповідність правил найновішим змінам. У великомасштабних проєктах зі складними залежностями між задачами, впровадження методу у його традиційному варіанті може бути надто коштовним.

З метою подолання традиційних обмежень цього методу досліджуються інноваційні підходи, які використовують машинне навчання та штучний інтелект для прогнозування та інтелектуального визначення переліку завдань неперервної інтеграції на основі змін початкових даних. Одними з найбільш популярних підходів є SmartBuildSkip, BuildFast і HybridCISave. Підхід SmartBuildSkip базується на аналізі певних параметрів проєкту та внесених змін, беручи до уваги як нетехнічні показники, наприклад, робочий день, кількість інженерів і вік даних, так і аналізуючи конкретні зміни, внесені до початкового коду, що дозволяє ідентифікувати зміни які навряд чи створять нові проблеми, таким чином економлячи час і обчислювальні ресурси (Jin, Servant, 2020). Метод BuildFast використовує подібний підхід, але також звертає увагу на історичні результати завдань інтеграції, щоб вирішити, чи потрібна збірка, що значно підвищило якість прогнозування необхідних завдань порівняно із SmartBuildSkip (Chen та ін., 2020). HybridCISave, який має найновітніший підхід до умовного виконання завдань неперервної інтеграції, поєднує підходи на основі правил і прогнозування для гібридного рішення для оптимізації процесів збірки початкового коду і тестування. Наприклад, HybridCISave може спочатку визначати набір завдань за допомогою попередньо визначених правил, а потім уточнювати рішення щодо їх виконання за допомогою моделей машинного навчання, які передбачають ймовірність необхідності виконання завдання на основі останніх змін. Цей гібридний підхід врівноважує надійність конфігурацій на основі правил із гнучкістю прогнозних моделей, пропонуючи потужний інструмент для підвищення ефективності процесів неперервної інтеграції (Jin, Servant, 2023).

Дослідження показують, що такі інструменти, як HybridCISave, можуть зменшити кількість завдань неперервної інтеграції на 93%,

мінімально впливаючи на точність виявлення інтеграційних проблем. Ти не менш, слід мати на увазі, що точність прогнозів залежить від якості даних, які використовуються для навчання моделей, а неправильні прогнози можуть призвести до пропуску завдань, які насправді були необхідними. Гібридні підходи, такі як HybridCISave, зменшують цей ризик, поєднуючи узгодженість конфігурацій на основі правил із можливістю адаптації прогнозних моделей.

Висновки і перспективи подальших досліджень. У цій статті досліджено ряд сучасних методів оптимізації структури процесів неперервної інтеграції, кожен з яких спрямований на підвищення швидкості, ефективності та використання ресурсів робочих процесів розробки програмного забезпечення. Розглянуто як традиційні методи: паралельне виконання завдань, пріоритизація завдань та умовного виконання завдань, так і новітні методи інтелектуального визначення переліку завдань неперервної інтеграції.

Ці методи продемонстрували значні покращення ключових показників неперервної інтеграції, зокрема скорочення критичного шляху процесів і пришвидшення циклу зворотного зв'язку. Найбільш ефективними виявилися методи розпаралелювання завдань та умовного виконання завдань, вплив яких значною мірою перевищує вплив на швидкість виконання процесів неперервної інтеграції при використанні методів структуризації завдань у вигляді спрямованого ациклічного графу і пріоритизації завдань. Однак слід зазначити, що застосування цих методів не завжди є можливим, особливо у нетрадиційних проєктах програмного забезпечення, як-то проєкти, спрямовані на описання інфраструктурної конфігурації середовища.

Інтелектуальні підходи, хоч і багатообіцяючі, значною мірою залежать від якості навчальних даних і точності базових алгоритмів. Неправильна конфігурація може призвести до пропуску завдань, критичних для підтримки цілісності коду. Крім того, інтеграція із застарілими системами та забезпечення міжплатформної сумісності продовжують викликати занепокоєння, особливо для організацій, які переходять на хмарні середовища неперервної інтеграції.

Заглядаючи вперед, майбутні дослідження можуть зосередитися на вдосконаленні методів прогнозування необхідного переліку завдань неперервної інтеграції, впровадження цих методів для традиційних систем неперервної інтеграції, а також на більш ретельному і масштабному аналізі впливу методів пріоритизації завдань та організації їх у вигляді графів. З розвитком програмної інженерії впровадження передових методів підвищення ефективності неперервної інтеграції сприятиме підвищенню ефективності, масштабованості та гнучкості процесів розробки, що зрештою сприятиме швидшій і надійнішій доставці програмного забезпечення.

ЛІТЕРАТУРА:

1. Xianhao J., Servant F. What helped, and what did not? An Evaluation of the Strategies to Improve Continuous Integration. *43rd International Conference on Software Engineering*: Conference Proceedings., Madrid, 25–28 May 2021. P. 213–225.

2. Burdiuzha R. Building an effective CI/CD pipeline: A comprehensive guide. Medium.com. URL: https://gartsolutions.medium.com/building-an-effective-ci-cd-pipeline-a-comprehensive-guide-bb07343973b7 (date of access: 10.09.2024).

3. Tsvirkun L., Myronov Y. Challenges and Specificities of Adopting Continuous Integration within Scalable Cloud Environments. *IEEE 18th International Conference on Computer Science and Information Technologies (CSIT)*: Conference Proceedings, Lviv, 19–21 October 2023.

4. Xianhao J., Servant F. HybridCISave: A Combined Build and Test Selection Approach in Continuous Integration. *ACM Transactions on Software Engineering and Methodology*. 2023. Vol. 32, no. 4. P. 1–39.

5. Stahl D. Large scale continuous integration and delivery: Making great software better and faster: PhD thesis. Groningen, 2017. 257 p.

6. Fallahzadeh E., Bavand A. H., Rigby P. C. Accelerating Continuous Integration with Parallel Batch Testing. 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering: Conference Proceedings, San Francisco, 3–9 December 2023. New York.

7. Bavand A. H. The Impact of Parallel and Batch Testing in Continuous Integration Environments: Masters Thesis. Concordia University, 2021. 109 p.

8. Scalable build service system with smart scheduling service / K. Wang et al. *ISSTA 2020: Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis*: Conference Proceedings, 18–22 July 2020. New York, 2020. P. 456–462.

9. Zheng S., Adams B., Hassan A. E. Does using Bazel help speed up continuous integration builds?. *Empirical Software Engineering*. 2024. Vol. 29, no. 5.

10. Detecting Build Dependency Errors in Incremental Builds / J. Lyu et al. *ISSTA 2024: Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis*: Conference Proceedings, Vienna, 16–20 September 2024. New York, 2024. P. 1–12.

11. Xianhao J., Servant F. A cost-efficient approach to building in continuous integration. *ICSE '20: Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering*: Conference Proceedings, Seoul, 27 June – 19 July 2020. New York, 2020. P. 13–25.

12. BUILDFAST: History-Aware Build Outcome Prediction for Fast Feedback and Reduced Cost in Continuous Integration / B. Chen et al. *2020 35th IEEE/ACM International Conference on Automated Software Engineering (ASE)*: Conference Proceedings, Melbourne, 21–25 September 2020. 2024. P. 42–53.

REFERENCES:

1. Jin, X., & Servant, F. (2021). What helped, and what did not? An Evaluation of the Strategies to Improve Continuous Integration. In Proceedings of the *43rd International Conference on Software Engineering* (pp. 213–225). IEEE Press.

2. Burdiuzha, R. (2023). Building an effective CI/CD pipeline: A comprehensive guide. Retrieved from: https://gartsolutions.medium.com/building-an-effective-ci-cd-pipeline-a-comprehensive-guide-bb07343973b7.

3. Tsvirkun, L., & Myronov, Y. (2023). Challenges and Specificities of Adopting Continuous Integration within Scalable Cloud Environments. 2023 IEEE *18th International Conference on Computer Science and Information Technologies (CSIT)*, 1–4. doi:10.1109/CSIT61576.2023.10324010.

4. Xianhao, J., Servant, F. (2023). HybridCISave: A Combined Build and Test Selection Approach in Continuous Integration. *ACM Transactions on Software Engineering and Methodology*, 32(4).

5. Stahl, D. (2017). Large scale continuous integration and delivery: Making great software better and faster. [Thesis fully internal (DIV), University of Groningen]. University of Groningen.

6. Fallahzadeh, E., Bavand, A. H., & Rigby, P. C. (2023, November). Accelerating Continuous Integration with Parallel Batch Testing. Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 55–67. doi:10.1145/3611643.3616255

7. Bavand, A. (2021) The Impact of Parallel and Batch Testing in Continuous Integration Environments. Masters thesis, Concordia University.

8. Wang, K., Tener, G., Gullapalli, V., Huang, X., Gad, A., & Rall, D. (2020). Scalable build service system with smart scheduling service. In Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis (pp. 452–462). Association for Computing Machinery.

9. Zheng, Shenyu & Adams, Bram & Hassan, Ahmed E. (2024). Does using Bazel help speed up continuous integration builds?. *Empirical Software Engineering*. 29. 10.1007/s10664-024-10497-x.

10. Lyu, Jun & Li, Shanshan & Zhang, He & Zhang, Yang & Rong, Guoping & Rigger, Manuel. (2024). Detecting Build Dependency Errors in Incremental Builds. 1-12. 10.1145/3650212.3652105.

11. Jin, X., & Servant, F. (2020). A Cost-efficient Approach to Building in Continuous Integration. In 2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE) (pp. 13-25).

12. Chen, B., Chen, L., Zhang, C., & Peng, X. (2020). BUILDFAST: History-Aware Build Outcome Prediction for Fast Feedback and Reduced Cost in Continuous Integration. In 2020 35th IEEE/ACM International Conference on Automated Software Engineering (ASE) (pp. 42–53).

УДК 004.491.42
DOI https://doi.org/10.32782/IT/2024-3-15

Олег САВЕНКО
доктор технічних наук, професор, декан факультету інформаційних технологій, Хмельницький національний університет, вул. Інститутська 11, м. Хмельницький, Україна, 29016
***ORCID:** 0000-0002-4104-745X*
***Scopus Author ID:** 54421023400*

Максим ЧАЙКОВСЬКИЙ
аспірант кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет, вул. Інститутська 11, м. Хмельницький, Україна, 29016
***ORCID:** 0000-0002-9596-6697*
***Scopus Author ID:** 57220050568*

Бібліографічний опис статті: Савенко, О, Чайковський, М. (2024). Метод нечіткої класифікації зловмисного програмного забезпечення з використанням інтелектуального агента. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 140–148, doi: https://doi.org/10.32782/IT/2024-3-15

МЕТОД НЕЧІТКОЇ КЛАСИФІКАЦІЇ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ВИКОРИСТАННЯМ ІНТЕЛЕКТУАЛЬНОГО АГЕНТА

Мета дослідження: *розробка моделі інтелектуального агента в структурі мультиагентної системи для класифікації поліморфного зловмисного програмного забезпечення.* ***Методологія дослідження:*** *в зв'язку з тим, що чітко провести виявлення та класифікацію поліморфних вірусів є досить складною задачею і класифікація здійснюється в умовах невизначеності, тому вирішення даної задачі передбачає використання технологій штучного інтелекту, а саме нечіткої логіки (нечіткої класифікації).* ***Наукова новизна дослідження:*** *використання даного методу є другим етапом у запропонованому підході виявлення, аналізу та класифікації поліморфного зловмисного програмного забезпечення та передбачає використання нечіткого логічного висновку, який складається з наступних кроків: (1) визначення характеристик виявленого поліморфного зловмисного програмного забезпечення та формування дерева логічного висновку; (2) опис лінгвістичних змінних; (3) визначення функцій належності лінгвістичних термів; (4) формування бази знань системи нечіткого висновку; (5) отримання ймовірності належності досліджуваного файлу до поліморфного зловмисного програмного забезпечення різних рівнів складності; (6) нечітка класифікація поліморфних вірусів.* ***Висновки:*** *ефективність запропонованої методики, згідно проведеного експерименту, полягає в тому, що з усіх виявлених поліморфних вірусів у попередньому дослідженні (89) даний підхід дозволив здійснити їх класифікацію згідно рівнів складності (всі 89), а з 40 файлів, які не є поліморфним зловмисним програмним забезпеченням, було отримано 100 % вірних висновків. Тобто, даний підхід надав можливість із виявлених поліморфних вірусів здійснити їх класифікацію за рівнями складності із врахуванням належності до нечітких термів на рівні низький, нижче середнього, середній, вище середнього та високий, що є перевагою даного підходу. Виявлення належності поліморфного зловмисного програмного забезпечення до певного рівня складності дозволяє полегшити процес підбору необхідних методів для боротьби та їх знешкодження.*

Ключові слова: *інтелектуальний агент, мультиагентна система, поліморфне зловмисне програмне забезпечення, нечітка логіка, ймовірність, класифікація.*

Oleg SAVENKO
Doctor of Technical Sciences, Professor, Dean of the Faculty of Information Technologies, Khmelnytskyi National University, 11, Instytuts'ka Str., Khmelnytskyi, Ukraine, 29016, savenko_oleg_st@ukr.net
***ORCID:** 0000-0002-4104-745X*
***Scopus Author ID:** 54421023400*

Maksym CHAIKOVSKYI
Graduate Student at the Department of Computer Engineering and Information Systems, Khmelnytskyi National University, 11, Instytuts'ka Str., Khmelnytskyi, Ukraine, 29016, max.chaikovskyi@gmail.com
***ORCID:** 0000-0002-9596-6697*
***Scopus Author ID:** 57220050568*

To cite this article: Savenko, O, Chaikovskyi, M. (2024). Metod nechitkoi klasifikacii zlovmysnogo programnogo zabezpechennya z vykorystannyam intelektualnogo agenta [A method of fuzzy classification of malicious software using an intelligent agent]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 140–148, doi: https://doi.org/10.32782/IT/2024-3-15

A METHOD OF FUZZY CLASSIFICATION OF MALICIOUS SOFTWARE USING AN INTELLIGENT AGENT

Purpose: *development of an intelligent agent model in the structure of a multi-agent system for the classification of polymorphic malware. Research methodology: due to the fact that clearly identifying and classifying polymorphic viruses is a rather difficult task and classification is carried out under conditions of uncertainty, therefore, the solution of this problem involves the use of artificial intelligence technologies, namely fuzzy logic (fuzzy classification).* ***The scientific novelty of the study:*** *the use of this method is the second stage in the proposed approach to the detection, analysis and classification of polymorphic malware and involves the use of fuzzy logical inference, which consists of the following steps: (1) determining the characteristics of the detected polymorphic malware and forming a tree of logical inference ; (2) description of linguistic variables; (3) definition of functions belonging to linguistic terms; (4) formation of the knowledge base of the fuzzy inference system; (5) obtaining the probability of the investigated file belonging to polymorphic malware of different levels of complexity; (6) unclear classification of polymorphic viruses.* ***Conclusions:*** *the effectiveness of the proposed method, according to the conducted experiment, is that out of all detected polymorphic viruses in the previous study (89), this approach made it possible to classify them according to levels of complexity (all 89), and out of 40 files that are not polymorphic malicious software, 100% correct conclusions were obtained. That is, this approach made it possible to classify the detected polymorphic viruses by levels of complexity, taking into account belonging to vague terms at the level of low, below average, average, above average, and high, which is an advantage of this approach. Identifying the polymorphic malware belonging to a certain level of complexity makes it easier to select the necessary methods to combat and neutralize them.*

Key words: *intelligent agent, multiagent system, polymorphic malware, fuzzy logic, probability, classification.*

Актуальність проблеми. Для вирішення актуальної проблеми виявлення зловмисного програмного забезпечення (ЗПЗ) запропонована інтелектуальна мультиагентна система, відображена модель інтелектуального агента (ІА) для виявлення поліморфного ЗПЗ, а також визначення ймовірності його приналежності до різних рівнів складності поліморфних вірусів (тобто класифікація). В зв'язку з тим, що чітко провести виявлення та класифікацію поліморфних вірусів є досить складною задачею і класифікація здійснюється в умовах невизначеності, тому вирішення даної задачі передбачає використання технологій штучного інтелекту, а саме нечіткої логіки (нечіткої класифікації).

Аналіз останніх досліджень і публікацій. Поліморфний вірус відрізняється від звичайного вірусу способом маскування. Програмний код поліморфного ЗПЗ змінюється при кожному новому зараженні за допомогою шифрування. Скільки заражень – стільки й варіацій того самого вірусу. Але кожна модифікація, по суті, є новим екземпляром вірусу. У поліморфних вірусах для шифрування можна застосовувати складні криптографічні алгоритми. Тому, наприклад, антивірусний захист на основі сигнатурних баз безсилий проти просунутого поліморфного ЗПЗ. Для знешкодження поліморфних вірусів необхідне повне розшифрування їхнього «тіла» (Aboaoja et. al., 2022; Djenna et. al., 2023; Ganin et. al., 2020).

Поліморфні віруси прийнято класифікувати за рівнями поліморфізму (Nguyen, 2018). У найпростіших – олігоморфних вірусів – зустрічаються однакові ділянки коду, якими їх можна ідентифікувати за допомогою сигнатурних баз. Найскладніші з вірусів використовують пермутуючий код (permutation code): вони постійно змінюються лише на рівні підпрограм – інсталятора, шифрувальника, обробника переривань тощо. Тому досить актуальним є питання класифікації ЗПЗ (Abdullah et. al., 2023; Al-Andoli et. al., 2022; Atitallah et. al., 2022; Chaganti et. al., 2023; Goyal Manish, 2022; Qiao et. al., 2021; Vasan et. al., 2020; Xiao et. al., 2020).

Існують різні рівні складності поліморфного ЗПЗ **(**Nguyen, 2018). Рівень 1: для створення поліморфного вірусу вибирається схема з набору схем шифрування/дешифрування. Екземпляр вірусу матиме одну з цих схем у вигляді звичайного тексту. Відкритий ключ для цього шифрування можна надати багатьом користувачам для шифрування повідомлення. Це простий, так званий, «напівполіморфний» вірус. Рівень 2: процедура розшифровки вірусу містить одну або кілька постійних інструкцій, решта змінюється, алгоритм використовує змінні, наприклад, X_1 і X_2, але не змінну X_3, що дозволяє нескінченно змінювати X_3. Рівень 3: дешифрувальник вірусів містить невикористовувані функції або інструкції, такі як NOP, CLI та

STI тощо. Рівень 4: дешифратор вірусів використовує взаємозамінні інструкції та змінює їх порядок (змішування інструкцій). Рівень 5: на цьому рівні поліморфний вірус використовував усі перераховані вище методи. Крім того, алгоритм дешифрування може бути змінений. Рівень 6: перманентні віруси. Це найвищий рівень поліморфного вірусу, і його слід називати поліморфним вірусом тіла або метаморфічним вірусом. На цьому етапі весь основний код вірусу може бути змінений.

Значна кількість досліджень науковців присвячена різним методам, прийомам і підходам до аналізу та виявлення ЗПЗ (Akhtar & Feng, 2022; Chakraborty et. al., 2020; Choi et. al., 2020; Liu et. al., 2022; Lysenko et. al., 2015; Lysenko et. al., 2018; Savenko et. al., 2021).

Агент – обчислювальна система, поміщена у зовнішнє середовище, здатна взаємодіяти з нею, здійснюючи автономні раціональні дії для досягнення цілей (Ligo et. al., 2020; Taher et. al., 2023). Зазвичай для того, щоб вважатися «інтелектуальним» агент повинен мати наступні властивості: реактивність (reactivity) – агент повинен відчувати зовнішнє середовище та реагувати на зміни в ньому, здійснюючи дії, спрямовані на досягнення цілей; проактивність (pro-activeness) – агент повинен показувати керовану цілями поведінку, проявляючи ініціативу, здійснюючи дії спрямовані на досягнення цілей; соціальність (social ability) – агент повинен взаємодіяти з іншими сутностями зовнішнього середовища (іншими агентами, людьми тощо) для досягнення цілей.

Формальна модель ІА в багатоагентних системах, використовуючи дискретну математику, може бути описана як система окремих агентів, які взаємодіють один з одним. Кожен агент представлений як дискретна сутність із визначеним станом. Стан агента може змінюватися з часом відповідно до набору правил або функцій, які базуються на поточному стані агента та стані його середовища. Ці правила або функції можна виразити за допомогою різних дискретних математичних структур, таких як графіки, послідовності та набори. Наприклад, зв'язки між агентами можна представити у вигляді графа, де кожен вузол представляє агента, а кожне ребро представляє можливу взаємодію між двома агентами. Крім того, послідовність дій, які здійснює агент, можна представити як послідовність станів, де кожен стан відповідає дії. Набір усіх можливих дій для агента можна представити як набір, а стратегію агента можна визначити як функцію, яка відображає поточний стан агента на дію в цьому наборі.

Концепція багатоагентних систем (MAS) стала важливою темою інтересу в галузі штучного інтелекту (Dunets et. al., 2017; Pomorova et. al., 2013; Savenko et. al., 2020). Суть цих систем полягає в ІА, які є суб'єктами, здатними сприймати навколишнє оточення та виконувати дії самостійно або у співпраці з іншими для досягнення конкретних цілей. Формальна модель ІА, особливо коли вона побудована з використанням дискретної математики, пропонує надійну структуру для розуміння, проектування та вдосконалення цих складних систем.

Мультиагентна система, по суті, є сукупністю кількох взаємодіючих ІА. Кожен агент, у своїй найпростішій формі, є обчислювальною сутністю, яка відчуває своє оточення та реагує відповідно. Ці агенти здатні до автономної поведінки, можуть вчитися на своєму досвіді та мають здатність взаємодіяти з іншими агентами в системі.

У формальній моделі ІА зображується як окрема сутність із визначеним станом у системі. Ці стани динамічні та змінюються з часом відповідно до набору встановлених правил або функцій. Важливо, що ці правила або функції враховують поточний стан агента та конкретні умови в його середовищі.

Однією з головних переваг використання дискретної математики в цих моделях є можливість точного представлення та подальшого аналізу системи. Різноманітні структури в дискретній математиці, такі як графіки, послідовності та набори, можна ефективно використовувати для формулювання цих правил або функцій.

Наприклад, відносини між агентами всередині системи можна представити у вигляді графіка. На цьому графіку кожен вузол означає агента, а кожне ребро представляє потенційну взаємодію між двома агентами. Це візуальне представлення дозволяє чітко зрозуміти та проаналізувати взаємодію всередині системи.

Подібним чином серію дій, які виконує агент, можна представити як послідовність станів. Кожен стан у цій послідовності відповідає певній дії, яку виконує агент. Цей послідовний підхід забезпечує чітке, покрокове представлення дій агента, що дозволяє детально аналізувати та розуміти.

Крім того, повний діапазон можливих дій, доступних для агента в системі, може бути зображений як набір. Використовуючи цей підхід, ратегію агента можна визначити як функцію, яка відображає поточний стан агента на дію в цьому наборі. Цей метод забезпечує повний огляд усіх потенційних дій, сприяючи глибшому розумінню поведінки агента.

Мета дослідження. Метою дослідження є розробка моделі ІА в структурі мультиагентної системи для класифікації поліморфного ЗПЗ із використанням нечіткої логіки.

Виклад основного матеріалу дослідження. Нехай є множина файлів, які виконуються F_i, $i=\overline{1,K}$, які можуть містити зловмисні коди. Нехай є множина ІА A_j, $j=\overline{1,L}$, які мають розпізнати файли, які виконуються. Навколишнє середовище *NS* являє собою операційну систему комп'ютера, в якій взаємодіють як файли, які виконуються F_i з ІА A_j, так і ІА між собою. Передбачається, що для кожного файлу, що виконується F_i, $i=\overline{1,K}$ існує вектор ознак $S_i=\left[s_{i,1},s_{i,2},\ldots,s_{i,k}\right]$ з k елементів, який може містити зловмисні коди. У кожного ІА A_j, $j=\overline{1,L}$ також є вектор ознак $C_j=\left[c_{j,1},c_{j,2},\ldots,c_{j,l}\right]$ з l елементів, який визначає його самостійні цілі. При цьому вектори ознак і особливості програмних агентів, так і виконуваних файлів можуть відрізнятися один від одного.

Передбачається, що у ІА A_j є здатність ідентифікувати виконувані файли F_i в сенсорних областях за допомогою двовимірного масиву значень спорідненості (подібності).

$$SIM_{A_j,F_i}=\frac{1}{\left(1+P_{j,i}\right)};j=\overline{1,L};i=\overline{1,K}.,\qquad(1)$$

де $P_{j,i}=A_j-F_i$ – евклідова відстань.

Крім того, ІА також мають здатність повідомляти інформацію про виконувані файли іншим програмним агентам у комунікаційних областях. Проте, у даному дослідженні буде розглянуто окремий ІА в структурі мультиагентної системи.

Отже, задачею ІА є виявлення ЗПЗ (у даному дослідженні – поліморфного ЗПЗ), також досить важливим питанням є визначення рівня складності поліморфного ЗПЗ).

Тому необхідно розробити модель ІА для виявлення та аналізу поліморфного ЗПЗ з використанням нечіткої класифікації з метою встановлення ймовірності його належності до окремих рівнів складності поліморфних вірусів.

Розглянемо абстрактну модель ІА. У даному випадку агент будемо розглядати як набір:

$$A_j=(M_{NS},\ M_{SS},\ M_D,\ f_{ns},\ M_T,\ f_{new},\ f_{mng}),\qquad(2)$$

де M_{NS} – непуста скінчена множина станів зовнішнього навколишнього середовища;

M_{SS} – непуста скінчена множина самостійних цілей агента;

M_D – непуста скінчена множина дій агента;

$f_{ns}: M_{NS}\times M_D\rightarrow 2^{M_{NS}}$ – це функція поведінки зовнішнього навколишнього середовища, яка співставляє поточний стан зовнішнього навколишнього середовища та вибрану агентом дію непусту множину можливих наступних станів зовнішнього середовища;

M_T – непуста скінчена множина внутрішніх станів агента;

$f_{new}: M_T\times M_{NS}\rightarrow M_{NS}$ – це є функція оновлення стану, що зіставляє попереднього внутрішнього стану та нового стану зовнішнього середовища новий внутрішній стан агента;

$f_{mng}: M_T\rightarrow M_D$ є функція прийняття рішення, що зіставляє поточному внутрішньому стану агента певну дію.

У попередніх дослідженнях (Chaikovskyi et. al., 2024; Чайковський, 2024) був запропонований комплексний підхід до виявлення та аналізу поліморфного ЗПЗ. Дане дослідження є продовженням вказаних попередніх та передбачає здійснення нечіткої класифікації виявлених поліморфних вірусів згідно рівнів складності (рис. 1).

Належність поліморфного ЗПЗ до певного рівня складності описується наступною множиною: B = {Low, Low Medium, Medium, High Medium, High}.

Приймаючи елементи множини як назви нечітких змінних, їх формально можна представити наступним чином:

$$B=\{b_1,\ b_2,\ b_3,\ b_4,\ b_5\}\qquad(3)$$

Нечіткі змінні:

$$<b_i,\ X_B,\ M^i_E>;\ \text{де } M^i_E=\{x,\ \mu^i_E(x)\};$$
$$x\in X_B;\ X_B=[0;\ 100].\qquad(4)$$

На основі формули (4) введена лінгвістична змінна:

$$<\text{"Ймовірність\_належності\_ЗПЗ"},\ B,\ X_B>\qquad(5)$$

Набір функцій належності нечітких змінних (4) відображається у вигляді (рис. 2).

Таким чином, функції належності нечітких змінних мають такий узагальнений вигляд:

$$\mu^i(x)=\left\{\begin{array}{c}0,якщо\ x_i^d<x<x_i^a;\\ 1,якщо\ x_i^b\le x\le x_i^c;\\ \dfrac{x-x_i^a}{x_i^b-x_i^a},якщо\ x_i^a\le x<x_i^b;\\ \dfrac{x_i^d-x}{x_i^d-x_i^c},якщо\ x_i^c<x\le x_i^d\end{array}\right\}\qquad(6)$$

Для забезпечення високої ефективності роботи алгоритму класифікації найбільш важливим завданням є вибір області визначення функцій належності термів та способу завдання значень їхнього аргументу.

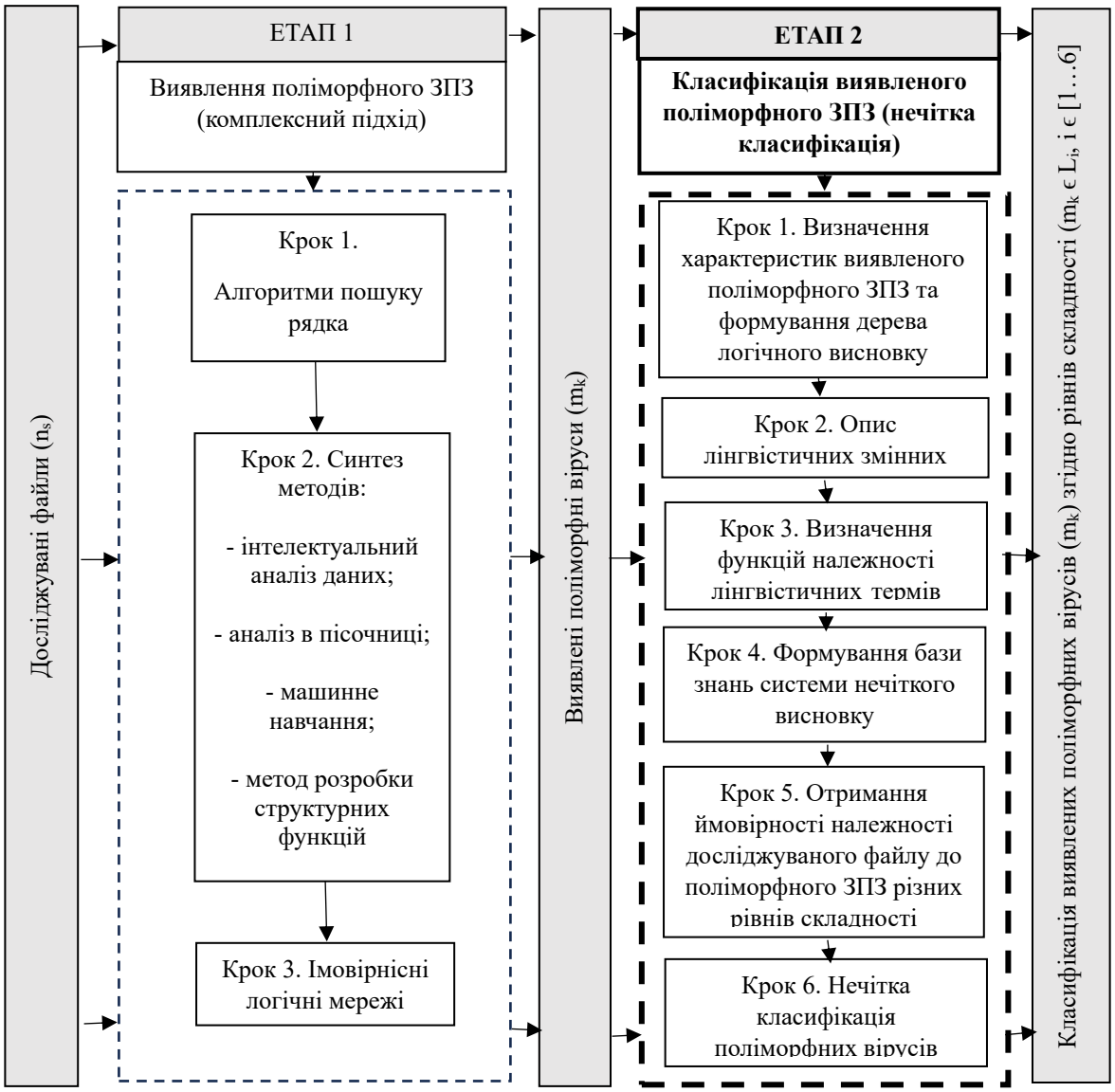


Рис. 1. Запропонований підхід для виявлення, аналізу та класифікації поліморфного ЗПЗ

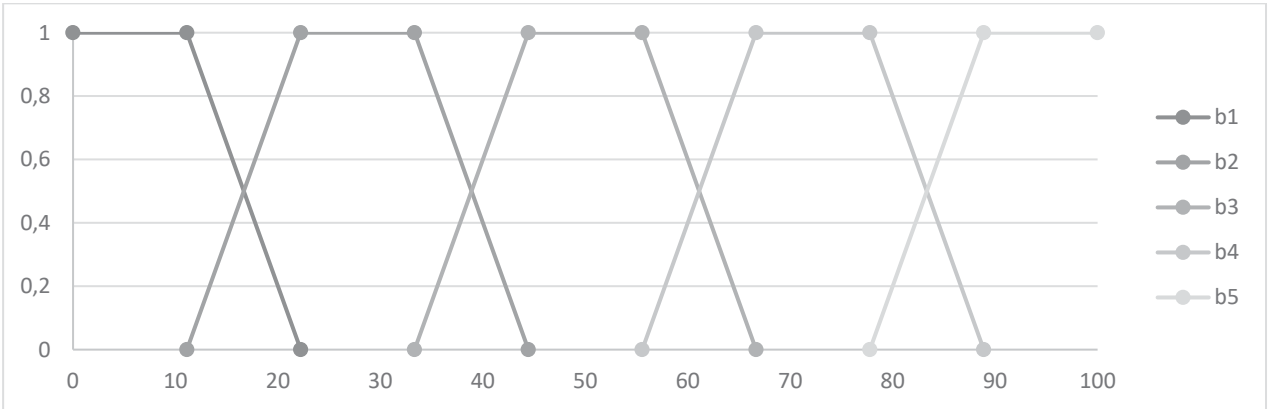


Рис. 2. Функції приналежності нечітких змінних лінгвістичної змінної ”Ймовірність_належності_ЗПЗ”

У даному дослідженні пропонується використовувати для класифікації спосіб оцінки лінгвістичної змінної, заснований на компонентах базових алгоритмів нечіткого висновку.

Також була згенерована база знань для кожного з рівнів складності поліморфного ЗПЗ, яка враховує інтерпретацію значень складових вектору ознак $S_i = \left[s_{i,1}, s_{i,2}, \ldots, s_{i,k} \right]$ у їх комплексному поєднанні для файлів, що виконуються.

В результаті використання нечіткого логічного висновку для кожного файлу, що виконується, було отримане числове значення (у %) ймовірності належності до кожного з рівнів складності поліморфного ЗПЗ.

Для визначення ефективності запропонованої методики була проведена серія експериментів. З усіх виявлених поліморфних вірусів (89) у попередньому дослідженні (Чайковський, 2024) даний підхід дозволив здійснити їх класифікацію згідно рівнів складності (всі 89). Також для перевірки надійності запропонованого підходу перевірялися файли, які не є поліморфним ЗПЗ. З 40 файлів, які не є поліморфним ЗПЗ, було отримано 100 % вірних висновків.

Нижче представлені точкові результати експерименту (таблиця 1-3).

Висновки і перспективи подальших досліджень. У дослідженні запропоновано модель ІА із використанням нечіткої класифікації для виявлення та аналізу поліморфного ЗПЗ. Ефективність запропонованої методики,

Таблиця 1

Результати експерименту для файлу, який не є поліморфним ЗПЗ

Рівень складності поліморфного зловмисного ПЗ	Розмірність універсуму (%)	Отримана ймовірність (%)	Значення функції належності для нечітких термів					Висновок
			Low	Low Medium	Medium	High Medium	High	
1	[0; 100]	0,00	0	0	0	0	0	Не є поліморфним зловмисним ПЗ
2		0,00	0	0	0	0	0	
3		0,00	0	0	0	0	0	
4		0,00	0	0	0	0	0	
5		0,00	0	0	0	0	0	
6		0,00	0	0	0	0	0	

Таблиця 2

Результати експерименту для згенерованого поліморфного ЗПЗ (варіант 1)

Рівень складності поліморфного зловмисного ПЗ	Розмірність універсуму (%)	Отримана ймовірність (%)	Значення функції належності для нечітких термів					Висновок
			Low	Low Medium	Medium	High Medium	High	
1	[0; 100]	0,00	0	0	0	0	0	Є поліморфним зловмисним ПЗ 2 рівня
2		75,00	0	0	0	1,00	0	
3		0,00	0	0	0	0	0	
4		0,00	0	0	0	0	0	
5		0,00	0	0	0	0	0	
6		0,00	0	0	0	0	0	

Таблиця 3

Результати експерименту для згенерованого поліморфного ЗПЗ (варіант 2)

Рівень складності поліморфного зловмисного ПЗ	Розмірність універсуму (%)	Отримана ймовірність (%)	Значення функції належності для нечітких термів					Висновок
			Low	Low Medium	Medium	High Medium	High	
1	[0; 100]	0,00	0	0	0	0	0	Є поліморфним зловмисним ПЗ 4 рівня
2		0,00	0	0	0	0	0	
3		0,00	0	0	0	0	0	
4		64,00	0	0	0,24	0,76	0	
5		0,00	0	0	0	0	0	
6		0,00	0	0	0	0	0	

згідно проведеного експерименту, полягає в тому, що з усіх виявлених поліморфних вірусів (89) даний підхід дозволив здійснити їх класифікацію згідно рівнів складності (всі 89), а з 40 файлів, які не є поліморфним ЗПЗ, було отримано 100 % вірних висновків. Тобто, даний підхід надав можливість виявити ті файли, які не є поліморфними вірусами, а із виявлених поліморфних вірусів здійснити їх класифікацію за рівнями складності із врахуванням належності до нечітких термів на рівні низький, нижче середнього, середній, вище середнього та високий, що є перевагою даного підходу. Виявлення належності поліморфного ЗПЗ до певного рівня складності дозволяє полегшити процес підбору необхідних методів для боротьби та їх знешкодження, у чому і полягає предмет наших подальших досліджень.

ЛІТЕРАТУРА:

1. Aboaoja F. A., Zainal A., Ghaleb F. A., Al-rimy B. A. S., Eisa T. A. E., Elnour A. A. H. Malware Detection Issues, Challenges, and Future Directions: A Survey. *Applied Sciences*. 2022. Vol. 12. № 17. P. 8482.

2. Djenna A., Bouridane A., Rubab S., Marou I.M. Artificial intelligence-based malware detection, analysis, and mitigation. *Symmetry*. 2023. Vol. 15. № 3. P. 677.

3. Ganin A., Quach P., Panwar M., Collier Z. A., Keisler J. M., Marchese D., Linkov I. Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis.* 2017. Vol. 40. №. 1. P. 183–199.

4. Nguyen V.T. (2018). A study of polymorphic virus detection. URL: https://doi.org/10.13140/RG.2.2.19853.79842 (дата звернення: 15.08.2023).

5. Abdullah M. A., YuY., Adu K., Imrana Y., Wang X., Cai J. HCL-classifier: CNN and LSTM based hybrid malware classifier for internet of things (IoT). *Future Generation Computer Systems*. 2023. Vol. 142. P. 41–58.

6. Al-Andoli M. N., Tan S. C., Sim K. S., Lim C. P., Goh P. Y. Parallel deep learning with a hybrid BP-PSO framework for feature extraction and malware classification. *Applied Soft Computing*. 2022. P. 109756.

7. Atitallah S. B., Driss M., Almomani I. A novel detection and multi-classification approach for IoT-malware using random forest voting of finetuning convolutional neural networks. *Sensors*. 2022. Vol. 22. № 11. P. 4302.

8. Chaganti R., Ravi V., Pham T.D. A multi-view feature fusion approach for effective malware classification using deep learning. *Journal of Information Security and Applications*. 2023. Vol. 72. P. 103402.

9. Goyal Manish K. R. AVMCT: API Calls Visualization based Malware Classification using Transfer Learning. *Journal of Algebraic Statistics*. 2022. Vol. 13. № 1. P. 31–41.

10. Qiao Y., Zhang W., Du X., Guizani M. Malware classification based on multilayer perception and Word2Vec for IoT security. *ACM Transactions on Internet Technology (TOIT)*. 2021. Vol. 22. № 1. P. 1–22.

11. Vasan D., Alazab M., Wassan S., Naeem H., Safaei B., Zheng Q. IMCFN: Image-based malware classification using fine-tuned convolutional neural network architecture. *Computer Networks*. 2020. Vol. 171. P. 107138.

12. Xiao G., Li J., Chen Y., Li K. MalFCS: An effective malware classification framework with automated feature extraction based on deep convolutional neural networks. *Journal of Parallel and Distributed Computing*. 2020. Vol. 141. P. 49–58.

13. Akhtar M. S., Feng T. Malware Analysis and Detection Using Machine Learning Algorithms. *Symmetry (Basel)*. 2022. Vol. 14. № 11. P. 2304.

14. Chakraborty A., Kriti K., Yateendra, Bennet Praba M.S. Polymorphic Malware Detection by Image Conversion Technique. *International Journal of Engineering and Advanced Technology (IJEAT).* 2020. Vol. 9. № 3. P. 2898–2903.

15. Choi S., Bae J., Lee C., Kim Y., Kim J. Attention-based automated feature extraction for malware analysis. *Sensors (Switzerland).* 2020. Vol. 20. № 10. P. 1–17.

16. Liu S., Feng P., Wang S., Sun K., Cao J. Enhancing malware analysis sandboxes with emulated user behavior. Computers and Security. 2022. Vol. 115. P. 102613.

17. Lysenko S., Pomorova O., Savenko O., Kryshchuk A., Bobrovnikova K. (2015). DNS-based Anti-evasion Technique for Botnets Detection. *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Warsaw, Poland, 24–26 September 2015. 2015. P. 453–458.

18. Lysenko S., Savenko O., Bobrovnikova K. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. *CEUR-WS*. 2018. Vol. 2104. P. 688–695.

19. Savenko B., Lysenko S., Bobrovnikova K., Savenko O., Markowsky G. Detection DNS Tunneling Botnets. *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Cracow, Poland, 22–25 September 2021. 2021.

20. Ligo A.K., Kott A., Linkov I. How to measure cyber-resilience of a system with autonomous agents: approaches and challenges. *IEEE Engineering Management Review*. 2021. Vol. 49. № 2. P. 89–97.

21. Taher F., AlFandi O., Al-kfairy M., Al Hamadi, H., Alrabaee S. DroidDetectMW: A Hybrid Intelligent Model for Android Malware Detection. *Applied Sciences.* 2023. Vol. 13. P. 7720.

22. Dunets O., Wolff C., Sachenko A., Hladiy G., Dobrotvor I. (2017). Multi-agent system of IT project plannin. *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Bucharest, 21–23 September 2017. 2017. P. 548–552.

23. Pomorova O., Savenko O., Lysenko S., Kryshchuk A. Multi-Agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic. *Communications in Computer and Information Science*. 2013. Vol. 370. P. 243–254.

24. Savenko O., Sachenko A., Lysenko S., Markowsky G., Vasylkiv N. Botnet Detection Approach based on the Distributed Systems. *International Journal of Computing*. 2020. Vol. 19. № 2. P. 190–198.

25. Chaikovskyi M., Chaikovska I., Sochor T., Martyniuk I., Lyhun O. Comprehensive approach to the detection and analysis of polymorphic malware. *CEUR-WS*. 2024. Vol. 3736. P. 312–323.

26. Чайковський М. Ю. Комплексний підхід до виявлення та аналізу поліморфного зловмисного програмного забезпечення. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2024. № 2. С. 42–50.

REFERENCES:

1. Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-rimy, B. A. S., Eisa, T. A. E., Elnour, A. A. H. (2022). Malware Detection Issues, Challenges, and Future Directions: A Survey. Applied Sciences. 12(17). https://doi.org/10.3390/app12178482

2. Djenna, A., Bouridane, A., Rubab, S., Marou, I.M. (2023). Artificial intelligence-based malware detection, analysis, and mitigation. Symmetry, 15(3), 677. https://doi.org/10.3390/sym15030677

3. Ganin, A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. Risk Analysis, 40(1), 183–199. https://doi.org/10.1111/risa.12891

4. Nguyen, V. T. (2018). A study of polymorphic virus detection. https://doi.org/10.13140/RG.2.2.19853.79842

5. Abdullah, M. A., Yu, Y., Adu, K., Imrana, Y., Wang, X., Cai, J. (2023). HCL-classifier: CNN and LSTM based hybrid malware classifier for internet of things (IoT). Future Generation Computer Systems, 142, 41–58. https://doi.org/10.1016/j.future.2022.12.034

6. Al-Andoli, M. N., Tan, S. C., Sim, K. S., Lim, C. P., Goh, P. Y. (2022). Parallel deep learning with a hybrid BP-PSO framework for feature extraction and malware classification. Applied Soft Computing, 131, 109756. https://doi.org/10.1016/j.asoc.2022.109756

7. Atitallah, S. B., Driss, M., Almomani, I. (2022). A novel detection and multi-classification approach for IoT-malware using random forest voting of finetuning convolutional neural networks. Sensors, 22(11), 4302. https://doi.org/10.3390/s22114302

8. Chaganti, R., Ravi, V., Pham, T. D. (2023). A multi-view feature fusion approach for effective malware classification using deep learning. Journal of Information Security and Applications, 72, 103402. https://doi.org/10.1016/j.jisa.2022.1034

9. Goyal Manish, K. R. (2022). AVMCT: API Calls Visualization based Malware Classification using Transfer Learning. Journal of Algebraic Statistics, 13(1), 31–41. https://doi.org/10.52783/jas.v13i1.59

10. Qiao, Y., Zhang, W., Du, X., Guizani, M. (2021). Malware classification based on multilayer perception and Word2Vec for IoT security. ACM Transactions on Internet Technology (TOIT), 22(1), 1–22. https://doi.org/10.1145/343675

11. Vasan, D., Alazab, M., Wassan, S., Naeem, H., Safaei, B., Zheng, Q. (2020). IMCFN: Image-based malware classification using fine-tuned convolutional neural network architecture. Computer Networks, 171, 107138. https://doi.org/10.1016/j.comnet.2020.107138

12. Xiao, G., Li, J., Chen, Y., Li, K. (2020). MalFCS: An effective malware classification framework with automated feature extraction based on deep convolutional neural networks. Journal of Parallel and Distributed Computing, 141, 49–58. https://doi.org/10.1016/j.jpdc.2020.03.012

13. Akhtar, M. S., Feng, T. (2022). Malware Analysis and Detection Using Machine Learning Algorithms. Symmetry (Basel), 14(11), 2304. https://doi.org/10.3390/sym14112304

14. Chakraborty, A., Kriti, K., Yateendra, Bennet Praba, M.S. (2020). Polymorphic Malware Detection by Image Conversion Technique. International Journal of Engineering and Advanced Technology (IJEAT), 9 (3), 2898–2903. https://doi.org/10.35940/ijeat.B4999.029320

15. Choi, S., Bae, J., Lee, C., Kim, Y., Kim, J. (2020). Attention-based automated feature extraction for malware analysis. Sensors (Switzerland), 20(10), 1–17. https://doi.org/10.3390/s20102893

16. Liu, S., Feng, P., Wang, S., Sun, K., Cao, J. (2022). Enhancing malware analysis sandboxes with emulated user behavior. Computers and Security, 115, 102613. https://doi.org/10.1016/j.cose.2022.102613

17. Lysenko, S., Pomorova, O., Savenko, O., Kryshchuk, A., Bobrovnikova, K. (2015). DNS-based Anti-evasion Technique for Botnets Detection. In Proc. of the 8-th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Warsaw, Poland, 453–458.

18. Lysenko, S., Savenko, O., Bobrovnikova, K. (2018). DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. CEUR-WS, 2104, 688–695.

19. Savenko, B., Lysenko, S., Bobrovnikova, K., Savenko, O., Markowsky, G. (2021). Detection DNS Tunneling Botnets. In Proc. of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IDAACS'2021, Cracow, Poland.

20. Ligo, A.K., Kott, A., Linkov, I. (2021). How to measure cyber-resilience of a system with autonomous agents: approaches and challenges. IEEE Engineering Management Review, 49(2), 89–97. https://doi.org/10.1109/EMR.2021.3074288

21. Taher, F., AlFandi, O., Al-kfairy, M., Al Hamadi, H., Alrabaee, S. (2023). DroidDetectMW: A Hybrid Intelligent Model for Android Malware Detection. Applied Sciences, 13, 7720. https://doi.org/10.3390/app13137720

22. Dunets, O., Wolff, C., Sachenko, A., Hladiy, G., Dobrotvor, I. (2017). Multi-agent system of IT project plannin". In Proc. of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, Romania, 548–552. https://doi.org/10.1109/IDAACS.2017.8095141

23. Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A. (2013). Multi-Agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic. Communications in Computer and Information Science, 370, 243–254. https://doi.org/10.1007/978-3-642-38865-1_16

24. Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G., Vasylkiv, N. (2020). Botnet Detection Approach based on the Distributed Systems. International Journal of Computing, 19(2), 190–198. https://doi.org/10.47839/ijc.19.2.1761

25. Chaikovskyi M., Chaikovska I., Sochor T., Martyniuk I., Lyhun O. (2024). Comprehensive approach to the detection and analysis of polymorphic malware. CEUR Workshop Proceedings, 3736, 312–323. Retrieved from: https://ceur-ws.org/Vol-3736/paper23.pdf

26. Chaikovskyi, M. (2024). Komplekcnui pidhid do vuyzvlennya ta analizu polimorfnogo zlovmysnogo programnogo zabezpechennya [Comprehensive approach to the detection and analysis of polymorphic malware]. Measuring and Computing Devices in Technological Processes, 2, 42–50 [in Ukrainian]. https://doi.org/10.31891/2219-9365-2024-78-5

УДК 004.491.42
DOI https://doi.org/10.32782/IT/2024-3-16

Євгеній СЄРГЄЄВ
аспірант кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет, вул. Інститутська, 11, Хмельницький, 29000
***ORCID:** 0009-0008-9877-9863*
***Scopus Author ID:** 59129893600*

Антоніна КАШТАЛЬЯН
кандидат технічних наук, докторанка, доцент, доцент кафедри фізики та електротехніки, Хмельницький національний університет, вул. Інститутська, 11, Хмельницький, Україна, 29000
***ORCID:** 0000-0002-4925-9713*
***Scopus Author ID:** 57218242499*

Василь КОВАЛЬЧУК
аспірант кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет, вул. Інститутська, 11, Хмельницький, Україна, 29000
***ORCID:** 0009-0008-7013-5919*

Олег САВЕНКО
доктор технічних наук, професор, професор кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет, вул. Інститутська, 11, Хмельницький, Україна, 29000
***ORCID:** 0000-0002-4104-745X*
***Scopus Author ID:** 54421023400*

Олег ІВАНЧЕНКО
доктор технічних наук, доцент, професор кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького 19, Дніпро, Україна, 49005
***ORCID:** 0000-0002-5921-5757*
***Scopus Author ID:** 57190132131*

Бібліографічний опис статті: Сєргєєв, Є., Каштальян, А., Ковальчук, В., Савенко, О., Іванченко, О. (2024). Ефективність і вдосконалення SAST у контексті SQL Injection вразливостей. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 149–158, doi: https://doi.org/10.32782/IT/2024-3-16

ЕФЕКТИВНІСТЬ І ВДОСКОНАЛЕННЯ SAST У КОНТЕКСТІ SQL INJECTION ВРАЗЛИВОСТЕЙ

Виявлення вразливостей безпеки на ранніх етапах розробки є критично важливим для забезпечення надійності програмного забезпечення. Статичний аналіз безпеки (SAST) широко використовується для виявлення потенційних вразливостей у коді. Однак складність сучасних методів та використання динамічних конструкцій у коді створюють виклики для SAST-інструментів, особливо у виявленні вразливостей типу SQL Injection, які можуть призвести до несанкціонованого доступу до даних.

***Метою статті** є дослідити ефективність методу статичного аналізу безпеки (SAST) у виявленні вразливостей типу SQL Injection та на основі експериментального аналізу запропонувати удосконалення цього методу для підвищення його ефективності.*

***Методологія** полягає у проведенні експериментального аналізу існуючих SAST-інструментів на здатність виявляти SQL Injection вразливості. Було використано набір тестових методів з відомими вразливостями для оцінки ефективності. На основі отриманих результатів ідентифіковано основні проблеми та розроблено удосконалення до методу статичного аналізу, які були впроваджені і протестовані для оцінки їхньої ефективності. Застосовано наукові методи синтезу, аналізу та порівняння.*

***Наукова новизна** полягає у розробці та впровадженні удосконалень до методу статичного аналізу безпеки, які підвищують ефективність виявлення вразливостей типу SQL Injection. Запропоновано нові*

алгоритми аналізу динамічних конструкцій у коді та обробки складних шаблонів запитів до баз даних, що раніше були недоступні для стандартних SAST-інструментів.

***Висновки**. Запропоновані удосконалення до методу статичного аналізу безпеки дозволяють значно покращити виявлення вразливостей типу SQL Injection, що підтверджується результатами експериментального аналізу. Це підкреслює важливість розвитку і впровадження передових технік у SAST-інструменти для забезпечення високого рівня безпеки програмного забезпечення.*

***Ключові слова:** вразливості, SAST-інструменти, SQL ін'єкції.*

Yevhenii SIERHIEIEV
PhD student at the Department at Computer Engineering and Information Systems, Khmelnytskyi National University, 11, Instytutska Str., Khmelnytskyi, Ukraine, 29000, ysierhieiev@gmail.com
***ORCID:** 0009-0008-9877-9863*
***Scopus Author ID:** 59129893600*

Antonina KASHTALIAN
PhD, Associate Professor at the Department of Physics and Electrical Engineering, Doctoral Staff, Khmelnytskyi National University, 11, Instytutska Str., Khmelnytskyi, Ukraine, 29000, yantonina@ukr.net
***ORCID:** 0000-0002-4925-9713*
***Scopus Author ID:** 57218242499*

Vasily KOVALCHUK
PhD Student at the Department of Computer Engineering and Information Systems, Khmelnitsky National University, 11, Instytutska Str., Khmelnytskyi, Ukraine, 29000, vasuli458@gmail.com
***ORCID:** 0009-0008-7013-5919*

Oleg SAVENKO
Doctor of Technical Sciences, Professor, Professor at the Department of Computer Engineering and Information Systems, Khmelnytskyi National University, 11, Instytutska Str., Khmelnytskyi, Ukraine, 29000, savenko_oleg_st@ukr.net
***ORCID:** 0000-0002-4104-745X*
***Scopus Author ID:** 54421023400*

Oleg IVANCHENKO
Doctor of Technical Sciences, Associate Professor, Professor at the Department of Computer Systems and Software, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, vmsu12@gmail.com;
***ORCID:** 0000-0002-5921-5757*
***Scopus Author ID:** 57190132131*

To site this article: Sierhieiev, Ye., Kashtalian, A., Kovalchuk, V., Savenko, O., Ivanchenko, O. (2024). Effektyvnist' i vdoskonalennia SAST v konteksti vrazlyvostei SQL Injection [Effectiveness and improvement of SAST in the context of SQL Injection vulnerabilities]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 149–158, doi: https://doi.org/10.32782/IT/2024-3-16

EFFECTIVNESS AND IMPROVEMENT OF SAST IN THE CONTEXT OF SQL INJECTION VULNERABILITIES

Identifying security vulnerabilities early in development is critical to ensuring software reliability. Static Security Analysis (SAST) is widely used to identify potential vulnerabilities in code. However, the complexity of modern applications and the use of dynamic constructs in the code create challenges for SAST tools, especially in detecting SQL Injection vulnerabilities that can lead to unauthorized access to data.

***The article aims** to investigate the effectiveness of the static security analysis method (SAST) in detecting vulnerabilities of the SQL Injection type and, based on experimental analysis, to propose improvements to this method to increase its effectiveness.*

***The methodology** consists of conducting an experimental analysis of existing SAST tools for the ability to detect SQL Injection vulnerabilities. A set of test applications with known vulnerabilities was used to evaluate performance.*

Based on the obtained results, the main problems were identified and improvements to the static analysis method were developed, which were implemented and tested to evaluate their effectiveness. Scientific methods of synthesis, analysis, and comparison are applied.

***The scientific novelty** consists in the development and implementation of improvements to the method of static security analysis, which increases the effectiveness of detecting vulnerabilities of the SQL Injection type. New algorithms for the analysis of dynamic structures in the code and processing of complex query patterns to databases, which were previously unavailable for standard SAST tools, are proposed.*

***Conclusions.** The proposed improvements to the method of static security analysis allow to significantly improve the detection of vulnerabilities of the SQL Injection type, which is confirmed by the results of experimental analysis. This emphasizes the importance of developing and implementing advanced techniques in SAST tools to ensure a high level of software security.*

***Key words:** vulnerabilities, SAST tools, SQL injections.*

Актуальність проблеми. Сучасне програмне забезпечення для виявлення вразливостей класифікується за групами відповідно до реалізованих у ньому конкретних методів пошуку вразливостей. Проте, важливим є не лише реалізація одного чи групи методів в спеціалізованих інструментах, а й розробка нових методів, які дозволять ефективніше знаходити та усувати вразливості. Тому, пропонується приділити значну увагу дослідженню існуючих аналітичних підходів та технологій, що використовуються для виявлення вразливостей, дослідити ефективність методу статичного аналізу безпеки (SAST) у виявленні вразливостей типу SQL Injection та на основі експериментального аналізу запропонувати удосконалення цього методу для підвищення його ефективності.

Аналіз останніх досліджень і публікацій. Дослідженню виявлення вразливостей в комп'ютерних системах для виявлення зловмисного програмного забезпечення (ЗПЗ) і комп'ютерних атак приділяють увагу багато дослідників. Науковці розробили багато різних методів виявлення вразливостей. Відомо, що невиявлені вразливості можуть призвести до значних витрат для IT компаній. Дослідження Myriam Dunn Cavelty показують, що швидке виправлення є важливим для уникнення втрат, пов'язаних з вразливістю та її публічним розголошенням (Cavelty, 2024). Вказано на значні витрати, пов'язані з недостатньою інфраструктурою тестування програмного забезпечення; тому необхідний інструмент для виявлення вразливостей.

Виявлення вразливостей SQL-ін'єкцій стало популярною темою досліджень у галузі інформаційної безпеки. Досліджено, що метод статичного аналізу безпеки (SAST) базується на детальному перегляді вихідного коду, бінарних файлів та бібліотек без їх виконання для виявлення потенційних вразливостей (Luo, 2022). Цей метод дозволяє ідентифікувати такі проблеми, як SQL-ін'єкції, XSS та інші типи вразливостей ще на етапі розробки (Wang, 2015). SAST використовує кореляційний аналіз, метрики вразливостей та моделювання загроз для визначення потенційних шляхів атак. Це підвищує ефективність виявлення вразливостей шляхом створення карт вразливостей та дерев атак на основі інформації з CWE (Common Weakness Enumeration) та CVE (Common Vulnerabilities and Exposures) (Charoenwet, 2024).

Однак, виявлено, що метод SAST має свої недоліки. Основні проблеми включають високу залежність від технічних ресурсів та потребу в постійному оновленні інструментів та методик, щоб відповідати новітнім викликам у сфері кібербезпеки. Крім того, SAST не може виявити вразливості, які проявляються лише під час виконання програми, що обмежує його ефективність у виявленні деяких типів атак (Do,2022). Запропоновано методику виявлення вразливості SQL-ін'єкції на основі трансформації програми для вирішення цієї проблеми, яка складається з двох етапів: трансформація програми та виявлення вразливості (Yuan, 2023).

Інструменти статичного аналізу (SAST) є практичним вибором для активного виявлення вразливостей у програмному забезпеченні під час розробки. Національна база даних про вразливості (NVD) у США (NVD, 2023) збирає загальні вразливості та експлойти (CVE), класифіковані через загальні слабкі місця (CWE) (Chen, 2023). NVD також класифікує ступінь небезпеки вразливостей, пов'язаних з конкретними CVE. SAST-інструменти розроблені для виявлення вразливостей, пов'язаних з CWE. Хоча багато SAST-інструментів можуть виявляти однакові вразливості, лише деякі з них можуть виявляти більш специфічні та складні CWE. NIST надає тестові набори SARD, які орієнтовані на найпоширеніші мови програмування для оцінки SAST-інструментів (NIST, 2023).

Серед проаналізованих досліджень можна виділити дві підгрупи: дослідження, що фокусуються на зручності використання і дослідження,

що фокусуються на адаптації та інтеграції інструментів у процеси компаній.

Також досліджено різні контексти, в яких розробники використовують статичні інструменти, такі як середовище розробки, огляд та безперервна інтеграція (Vassallo, 2018). Під час дослідження налаштування для цих контекстів було з'ясовано, що більшість розробників використовують однакові налаштування у всіх середовищах (IDE, безперервна інтеграція чи огляд). Було проведене опитування серед сорока двох учасників, а для підтвердження своїх висновків проведено інтерв'ю з одинадцятьма розробниками з шести компаній.

Ще один важливий експеримент на виявлення вразливостей безпеки за допомогою інструментів статичного аналізу описано в роботі (Smith, 2020). Було запрошено десять розробників з одного проекту виконати чотири завдання з використанням розширеної версії FindBugs. Учасників попросили усно пояснити свої думки, які автори використали для формулювання запитань. Потім вони використовували метод сортування карток для отримання відповідних висновків.

Крім того, досліджено, що SAST можна використовувати для виявлення 76% дефектів перевірки коду, що значно більше, ніж поточні інструменти, які їх успішно виявляють. Було виявлено, що інструменти SAST можуть бути ефективнішими і виявляти більше вразливостей при перевірці коду (Mehrpour, 2022).

Доведено, що SAST є практичним вибором для активного виявлення вразливостей програмного забезпечення під час його розробки (Shen, 2021). Також зазначено, що інтеграція методів статичного аналізу безпеки (SAST) може забезпечити більш комплексний підхід до забезпечення безпеки програмного забезпечення, поєднуючи автоматизовані рев'ю коду з детальним виявленням вразливостей (Tufano, 2023). Подальші дослідження повинні зосередитись на удосконаленні моделей для специфічних задач автоматизації та їх інтеграції з SAST для підвищення рівня безпеки програмних продуктів.

Виявлено розрив між заявленими можливостями SAST та їх фактичною ефективністю, що підкреслює необхідність покладатися на емпіричні дані (Esposito, 2024). Проаналізовано, що жоден інструмент не покриває всі типи вразливостей, тому рекомендується використовувати комбінацію різних SAST та доповнювати їх іншими методами, такими як ручний аналіз коду або машинне навчання, тобто майбутні зусилля мають бути спрямовані на підвищення повноти виявлення (зменшення пропущених вразливостей), навіть якщо це призведе до збільшення кількості помилкових спрацьовувань, оскільки невиявлені вразливості можуть мати серйозні наслідки для безпеки програмного забезпечення.

Метою дослідження є оцінка ефективності методу статичного аналізу безпеки (SAST) у виявленні вразливостей типу SQL Injection у програмному забезпеченні. Дослідження спрямоване на аналіз поточної здатності існуючих SAST-інструментів виявляти ці вразливості та розробку удосконалень, які підвищують їхню ефективність. Це досягається шляхом проведення експериментального аналізу, що дозволяє виявити основні обмеження та проблеми сучасних методів статичного аналізу.

Виклад основного матеріалу дослідження

Проаналізуємо SQL ін'єкцію, що сьогодні є не тільки широко поширеною вразливістю, а ще й однією з найнебезпечніших, за версією OWASP (Top 10 Application Security Risks). SQL (Structrued Query Language) – мова бази даних, яка використовується для додавання, видалення, зміни та запитувати дані в реляційній базі даних. Поки система використовує базу даних, з більшою частиною вона взаємодіє бази даних за допомогою операторів SQL.

Суть вразливості – це виконання довільного запиту до бази даних. Запит може бути будь-яким: на читання, запис, модифікацію та видалення будь-яких записів. Крім того, за певних обставин можна дістатися і до читання/запису локальних файлів або навіть до виконання коду. Все залежить від цілей, які переслідує зловмисник, від системи, що використовується, і того, як вона налаштована. Розглянемо типи SQL ін'єкцій.

• Класична SQL Injection – проста та легка в експлуатації. Дозволяє зловмисникові атакувати базу даних (БД) і одразу бачити результат атаки. Останнім часом трапляється нечасто.

• Error-based SQL Injection – трохи складніший і витратний за часом тип атаки, що дозволяє, на основі помилок СУБД, що виводяться, отримати інформацію про всю БД і дані, що зберігаються в ній. Експлуатується, якщо забули відключити виведення помилок.

• Boolean-based SQL Injection – одна зі «сліпих» ін'єкцій. Суть атаки зводиться до додавання спеціального підзапиту у вразливий параметр, який БД відповідатиме або «True», або, несподівано, «False». Атака не дозволяє відразу вивести всі дані БД «на екран» зловмиснику, але дозволяє, перебираючи параметри раз за разом, отримати вміст БД, хоча для

цього буде потрібно тимчасовий відрізок порівнянний зі вмістом БД.

• Time-based SQL Injection – наступна зі «сліпих» ін'єкцій. У цьому випадку зловмисник додає підзапит, що призводить до уповільнення або паузи роботи БД за певних умов. Таким чином, атакуючий, порівнюючи час відповіді на «True» і на «False» запити, символ за символом може отримати весь вміст БД, але часу піде на це більше, ніж у разі експлуатації Boolean-based атаки.

• Out-of-band SQL Injection – рідкісний тип. Атака може бути успішною лише за певних обставин, наприклад, якщо сервер БД може генерувати DNS- або HTTP-запити, що зустрічається нечасто. Також, як і Blind SQL, дозволяє посимвольно збирати інформацію про дані, що зберігаються там.

Виявлено, що основною причиною вразливостей SQL Injection є те, що розробники під час написання коду використовують метод конкатенації рядків для побудови SQL-запитів, які передаються до бази даних. В результаті, зловмисники можуть змінювати SQL-запит, вводячи ключові слова SQL або спеціальні символи. Внаслідок виконання такого запиту система зазнає атаки. Фундаментальною причиною є надмірна довіра до даних, введених користувачами, без належної фільтрації введення та без здійснення раціональної верифікації на стороні сервера, що дозволяє зловмиснику досягати своїх цілей, таких як крадіжка конфіденційної інформації системи або отримання контролю над сервером. На рис. 1 показано основні принципи та процеси атаки SQL Injection.

SQL injection є поширеним типом веб-вразливості, що дозволяє зловмиснику обійти механізми автентифікації та авторизації застосунку шляхом створення шкідливих SQL-запитів для отримання конфіденційних даних або виконання незаконних операцій з базою даних. У звичайному методі дані, як правило, вводяться користувачем і певним чином передаються до Backend-бази даних для відповідних запитів, оновлень та видалень. Якщо метод не належним чином фільтрує або не ухиляється від цих введених користувачем даних, зловмисник може вставити шкідливі SQL-інструкції у введення, що призводить до виконання методом неочікуваних запитів або дій, таких як видалення таблиць, вставка даних або витік конфіденційної інформації.

Розглянемо приклад ін'єкції SQL-коду у веб-застосунку. Багато методів приймають введення користувача і передають їх у попередньо визначений запит, який потім передається до бази даних для виконання. Якщо розробники не налаштують код додатка належним чином для захисту від неочікуваного введення даних користувачами, зміни структури бази даних, пошкодження даних або розкриття приватної та конфіденційної інформації можуть статися ненавмисно.

Наприклад, розглянемо сторінку входу CGI-методу, яка очікує ім'я користувача та відповідний пароль. Коли облікові дані вводяться, вони вставляються у шаблон запиту, такий як:

```
select * from mysql.user
where username=' «. $uid. « ' and
password=password(' «. $pwd. « ');
```

Замість дійсного імені користувача, зловмисник задає змінну $uid як рядок: ' or 1=1; --, що змушує CGI-скрипт створити наступний SQL-запит до бази даних:

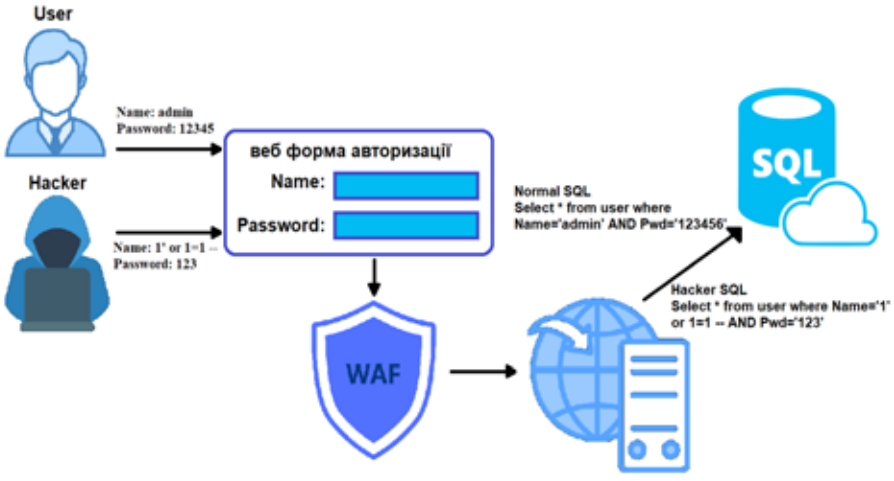


Рис. 1. Схема основних принципів та процесів атаки SQL Injection

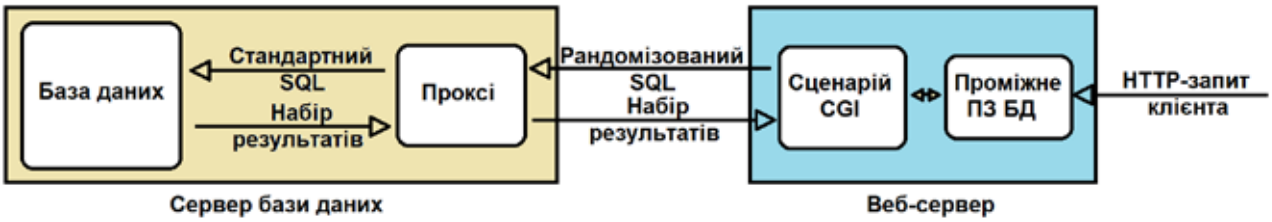


Рис. 2. Базові принципи проникнення SQL ін'єкції

```
select * from mysql.user
where username='' or 1=1; --' and
password=password('_any_text_');
```

Зауважимо, що одинарні лапки врівноважують лапки у попередньо визначеному запиті, а подвійне тире коментує решту SQL-запиту. Таким чином, значення паролю не має значення і може бути встановлено будь-яким рядком. Набір результатів запиту міститиме принаймні один запис, оскільки умова where є істинною. Якщо метод визначає дійсного користувача, перевіряючи, чи є набір результатів непорожнім, зловмисник може обійти перевірку безпеки.

Метод покращення SAST для захисту від SQL-ін'єкцій

Проаналізувавши дослідження науковців, було вирішено, як можна покращити SAST, щоб запобігти SQL Injection. Тому, запропоновано наступні дії.

1. Розробка та впровадження більш складних і спеціалізованих правил для виявлення SQL Injection. Ці правила повинні враховувати різні способи формування SQL-запитів, включаючи використання параметризованих запитів, ORM (Object-Relational Mapping) та інших засобів роботи з базами даних. Реалізувати це можна за допомогою виявлення шаблонів рядків, тобто SAST-інструменти повинні мати можливість виявляти місця в коді, де введення користувача об'єднується з SQL-запитами через конкатенацію рядків. Це можуть бути рядки, що містять ключові слова SQL, або змінні, які безпосередньо впливають на структуру запиту. Також треба запровадити аналіз використання ORM – це означає, що ORM-інструменти спрощують взаємодію з базами даних, але можуть також бути джерелом вразливостей, якщо використовуються неправильно. SAST-інструменти повинні мати правила для перевірки правильності використання ORM, включаючи перевірку наявності параметризації запитів та уникнення динамічних запитів.

2. Інтеграція з іншими інструментами безпеки. Інтеграція SAST-інструментів з іншими засобами безпеки, такими як динамічні аналізатори (DAST) та засоби безперервної інтеграції та доставки (CI/CD). Це дозволить отримати більш повну картину безпеки додатків і знизити ризик пропуску вразливостей. Реалізація вимагає синхронізацію з DAST, результати динамічного аналізу можуть бути використані для уточнення правил статичного аналізу. Наприклад, виявлені DAST-інструментом вразливості можуть вказати на проблемні місця в коді, які варто перевірити SAST-інструментом. Інтеграція з CI/CD дозволить автоматично сканувати код на кожному етапі розробки, що забезпечує постійну перевірку безпеки. SAST-інструменти можуть бути інтегровані в конвеєр CI/CD для регулярного аналізу коду при кожному коміті або зборці.

3. Автоматичне виправлення вразливостей вимагає розробку функціональності для автоматичного створення виправлень для виявлених вразливостей. Ці виправлення можуть включати рефакторинг коду для використання параметризованих запитів замість конкатенації рядків або впровадження належного очищення введених даних. Результатом буде автоматичне заміщення SQL-запитів: SAST-інструменти можуть автоматично знаходити місця в коді, де використовуються небезпечні SQL-запити, і пропонувати зміни для їх заміни на параметризовані запити. Це включає зміну синтаксису запиту та додавання відповідних параметрів. Також плюсом буде рефакторинг коду: Інструмент може автоматично генерувати патчі для коду, що виправляють вразливості, та надсилати їх розробникам для перевірки і впровадження. Це значно зменшує час, необхідний для усунення вразливостей.

4. Контекстуальний аналіз. Впровадження можливостей контекстуального аналізу, які дозволяють SAST-інструментам краще розуміти контекст, в якому використовуються SQL-запити. Це допоможе виявляти більш складні та приховані вразливості. Наприклад аналіз шляхів передачі даних, тобто SAST-інструменти можуть відстежувати шлях даних від точки введення до точки використання в SQL-запитах. Це допомагає виявити місця, де дані можуть бути змінені або неправильно оброблені. Також інструмент

повинен аналізувати контекст виконання SQL-запитів, включаючи умови, цикли та інші конструкції, які можуть впливати на безпеку запиту. Це дозволяє виявляти вразливості, які можуть бути приховані у складних логічних конструкціях.

Експеримент

Для оцінки ефективності нового методу статичного аналізу безпеки (SAST) у виявленні SQL Injection був проведений експеримент, використовуючи дані реальних комітів, що сприяли виникненню вразливостей.

1. Підготовка даних.

Було використано набір даних Vulnerability Contributing Commits (VCCs), наданий Iannone та ін., зібраний з проєктів GitHub, пов'язаних із вразливостями в базі даних CVE. Ми обрали VCCs за такими критеріями:

1. Мова програмування: проєкти, реалізовані на C або C++, оскільки ці мови дозволяють низькорівневі операції, що можуть призвести до вразливостей.

2. Призначений тип вразливості: VCCs, пов'язані з CVE, які мають призначений тип вразливості (CWE), зокрема SQL Injection.

3. Можливість компіляції: VCCs з проєктів, які можуть бути успішно скомпільовані, щоб забезпечити коректну роботу SAST-інструментів.

Схему процесу підготовки даних зображено на рис. 3.

2. Виконання експерименту.

Було обрано безкоштовні, активно підтримувані SAST-інструменти, які можуть працювати через командний рядок (CLI). Вибір інструментів базувався на попередніх дослідженнях та списку інструментів з NIST's Software Assurance Metrics And Tool Evaluation (SAMATE). Ми використовували найновіші стабільні версії інструментів, зокрема CodeChecker v6.24.1, CodeQL v1.15, Flawfinder v2.0.19 та інші, на автоматизованій платформі з використанням Docker-контейнерів для ізоляції середовища.

Попередження, згенеровані SAST-інструментами, були згруповані за типами вразливостей, зокрема за SQL Injection, шляхом мапінгу ідентифікаторів CWE відповідно до офіційної документації інструментів та стандартів CWE.

3. Аналіз та результати.

Було виміряно кількість VCCs, на яких SAST-інструменти могли надати попередження про SQL Injection. Результати показали, що новий метод SAST виявив вразливості у 78% обраних комітів. Цей показник було отримано шляхом співвідношення кількості виявлених вразливостей до загальної кількості VCCs, які відповідали нашим критеріям.

Аналіз продемонстрував, що пріоритизація на основі попереджень SAST дозволила

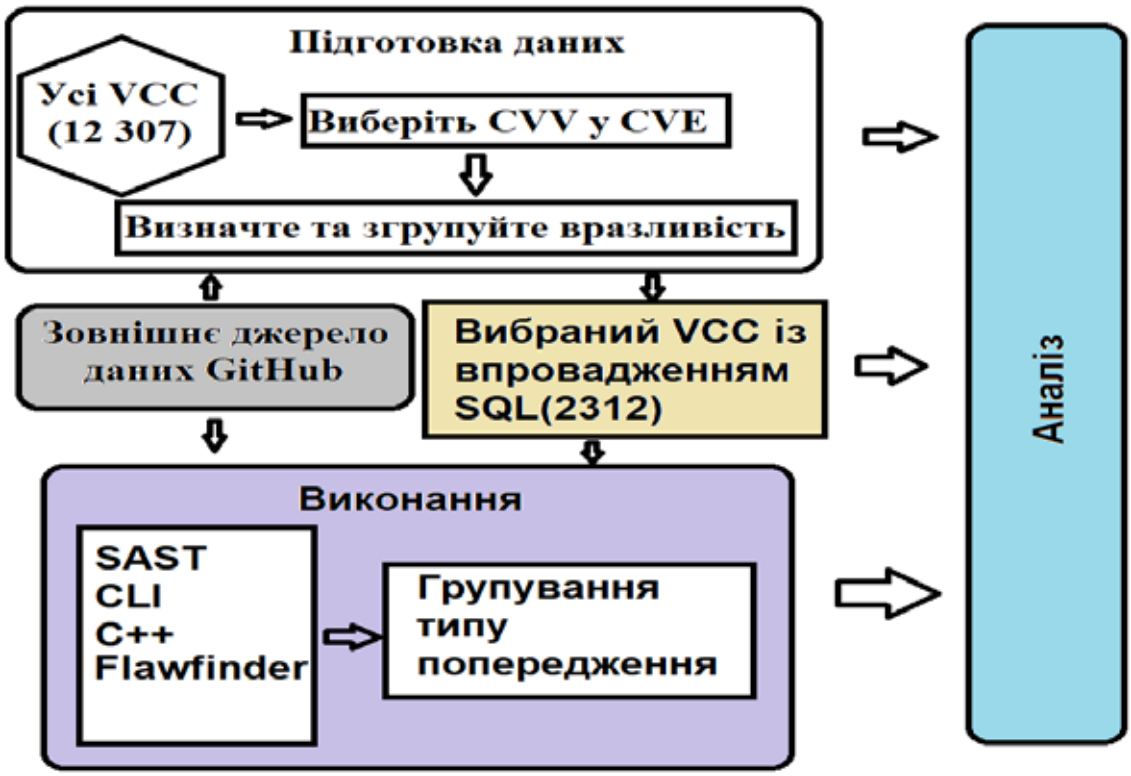


Рис. 3. Схема процесів при експерименті

рев'юерам виявити на 45% більше вразливих функцій при обмежених затратах зусиль. Це було досягнуто шляхом порівняння ефективності виявлення вразливостей з використанням та без використання пріоритизації.

Середній час обробки кожного коміту склав 12 хвилин, що було виміряно під час експерименту за допомогою нашої автоматизованої платформи. Це відповідає допустимому часу для автоматизованих тестів під час код-рев'ю, забезпечуючи інтеграцію процесу аналізу в робочий цикл розробки.

Висновки і перспективи подальших досліджень. У цьому дослідженні було розглянуто метод статичного аналізу безпеки (SAST) з особливим акцентом на виявлення вразливостей типу SQL Injection. Було проведено експеримент із використанням удосконаленого методу SAST, який включає розробку більш складних і спеціалізованих правил для виявлення SQL Injection та інтеграцію з іншими інструментами безпеки. Результати експерименту показали, що удосконалений метод SAST здатен виявляти вразливості типу SQL Injection у 78% випадків. Це свідчить про значне покращення порівняно з традиційними підходами, оскільки він дозволяє більш ефективно ідентифікувати специфічні типи вразливостей, підвищуючи загальний рівень захисту від кіберзагроз. Крім того, використання цього методу SAST дозволяє пріоритизувати перевірку змін у коді, що сприяє виявленню на 45% більше вразливих функцій при обмежених ресурсах для перевірки. Це підвищує ефективність процесу ревізії коду та забезпечує більш надійний захист програмного забезпечення.

Щодо часу обробки, середній час аналізу для кожного коміту склав 12 хвилин, що відповідає прийнятному часу для автоматизованих тестів під час процесу ревізії коду та демонструє, що удосконалений метод SAST є ефективним з точки зору продуктивності. Для підвищення безпеки програмного забезпечення було запропоновано кілька удосконалень методу SAST, включаючи розробку більш складних правил для виявлення SQL Injection, інтеграцію з іншими інструментами безпеки, автоматичне виправлення вразливостей та впровадження контекстуального аналізу.

Отже, результати нашого дослідження демонструють значний потенціал удосконаленого методу SAST у підвищенні ефективності виявлення вразливостей типу SQL Injection та забезпеченні більш надійного захисту програмного забезпечення. Майбутні дослідження можуть бути спрямовані на подальше вдосконалення інструментів SAST та їх інтеграцію з іншими методами забезпечення кібербезпеки.

ЛІТЕРАТУРА:

1. Cavelty M. D. The Politics of Cyber-Security. New York, 2024. P. 224. DOI: org/10.4324/9781003497080 (дата звернення: 19.08.2024).

2. Luo C., Li P., Meng W. T. TChecker: Precise Static Inter-Procedural Analysis for Detecting Taint-Style Vulnerabilities in PHP Applications. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security USA.* 07 November, 2022. P. 2175–2188. DOI: 10.1145/3548606.3559391.

3. Wang Y., Wang D., Zhao W., Liu Y. Detecting SQL Vulnerability Attack Based on the Dynamic and Static Analysis Technology. *IEEE 39th Annual Computer Software and Applications Conference*. 2015. P. 604–607. DOI: 10.1109/COMPSAC.2015.277.

4. Charoenwet W., Thongtanunam P., Pham V., & Treude, C. An Empirical Study of Static Analysis Tools for Secure Code Review. *In Proceedings of ACM SIGSOFT International Symposium on Software Testing and Analysis. ACM.* 2024. New York P. 13. DOI: 10.48550/arXiv.2407.12241.

5. Do L. N. Q., Wright J. R., Ali K. Why Do Software Developers Use Static Analysis Tools? A User-Centered Study of Developer Needs and Motivations. *IEEE Transactions on Software Engineering*. 2022. Vol. 48, № 3, P. 835–847. DOI: 10.1109/TSE.2020.3004525.

6. Yuan Ye, Yuliang Lu, Kailong Zhu, Hui Huang, Lu Yu and Jiazhen Zhao. A Static Detection Method for SQL Injection Vulnerability Based on Program Transformation. *Applied Sciences.* 2023. Vol. 13, № 21. DOI: 10.3390/app132111763.

7. NVD. National vulnerability database. 2023. URL: https://nvd.nist.gov/ (дата звернення: 19.08.2024).

8. Chen Z., Cao J. VMCTE: visualization-based malware classification using transfer and ensemble learning. *Computers, Materials & Continua.* 2023. № 75(2), P. 4445–4465. DOI:10.32604/cmc.2023.038639.

9. NIST. National institute of standards and technology. URL: https://www.nist.gov/(дата звернення: 19.08.2024).

10. Vassallo C., Panichella S., Palomba F., Proksch S., Zaidman A., Gall H. C., Context is king: The developer perspective on the usage of static analysis tools. *IEEE 25th International Conference on Software Analysis, Evolution and Reengineering (SANER).* 2018. P. 38–49. DOI: 10.1109/SANER.2018.8330195.

11. Smith M., Naiakshina A, Danilova A., Gerlitz E. On conducting security
developer studies with cs students: Examining a password-storage study with cs students, freelancers, and company developers. *Proceedings of the Conference on Human Factors in Computing Systems, Association for Computing Machinery.* 2020. P. 1–12. DOI: 10.1145/3290605.3300370.

12. Mehrpour S., LaToza T. D. Can static analysis tools find more defects? *Empir Software Eng*. 2023. Vol.28. № 5. DOI:10.1007/s10664-022-10234.

13. Shen S., Kolluri A., Dong Z., Saxena P., Roychoudhury A. Localizing vulnerabilities statistically from one exploit. *In Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*. 2021. P. 537–549. DOI:10.1145/3433210.3437528.

14. Tufano R., Dabić O., Mastropaolo A., Ciniselli M. and Bavota G. Code review automation: strengths and weaknesses of the state of the art. IEEE Transactions on Software Engineering, 2023. P. 1–16. DOI: 10.1109/TSE.2023.3348172.

15. Esposito M., Falaschi V., Falessi D. An Extensive Comparison of Static Application Security Testing Tools.2024. DOI: 10.13140/RG.2.2.12326.54085.

16. Esposito M., Moreschini S., Lenarduzzi V., Hästbacka D., Falessi D. Can we trust the default vulnerabilities severity? *In IEEE 23rd International Working Conference on Source Code Analysis and Manipulation (SCAM).* 2023. P. 265–270. DOI: 10.1109/SCAM59687.2023.00037.

17. Lysenko S, Lysenko S., Bobrovnikova K., Kharchenko V., Savenko O. IoT multi-vector cyberattack detection based on machine learning algorithms: traffic features analysis, experiments, and efficiency. *Algorithms.* 2022. Vol 15. № 7. P. 239. DOI: 10.3390/a15070239

18. Website of Our Study. Static Application Security Testing (SAST) Tools for Smart Contracts: How Far Are We? 2024. URL: https://sites.google.com/view/sc-sast-study-fse2024/home (Accessed on 29/07/2024).

19. Azman M., Marhusin M. F., Sulaiman R. Machine Learning – Based Technique to Detect SQL Injection Attack. *Journal of Computer Science.* 2021. № 17. P. 296–303. DOI:10.3844/jcssp.2021.296.303.

20. Medeiros P. I., Fonseca J., Neves N., Correia M., Vieira M. Benchmarking Static Analysis Tools for Web Security. in *IEEE Transactions on Reliability*. 2018. V. 67. № 3. P. 1159–1175. DOI: 10.1109/TR.2018.2839339.

21. Charoenwet W., Thongtanunam P., Pham V. T., Treude C. An Empirical Study of Static Analysis Tools for Secure Code Review. *In Proceedings of ACM SIGSOFT International Symposium on Software Testing and Analysis.* 2024. P. 13 DOI: 10.48550/arXiv.2407.12241.

22. Savenko B., Lysenko S., Bobrovnikova K., Savenko O., Markowsky G. Detection DNS tunneling botnets. *11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 22 September, 2021. P. 64–69. DOI: 10.1109/IDAACS53288.2021.9661022

REFERENCES:

1. Dunn Cavelty, M. (2024). The Politics of Cyber-Security (1st ed.). New York, Routledge https://doi.org/10.4324/9781003497080 [in English].

2. Luo, C., Li, P., Meng, W. T. (2022, November). TChecker: Precise Static Inter-Procedural Analysis for Detecting Taint-Style Vulnerabilities in PHP Applications. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security USA,* 2175–2188 https://doi.org/10.1145/3548606.3559391

3. Wang, Y., Wang, D., Zhao, W., Liu, Y. (2015, September). Detecting SQL Vulnerability Attack Based on the Dynamic and Static Analysis Technology. *IEEE 39th Annual Computer Software and Applications Conference*, 604–607 https://doi.org/10.1109/COMPSAC.2015.277

4. Charoenwet, W., Thongtanunam, P., Pham, V. & Treude, C. (2024). An Empirical Study of Static Analysis Tools for Secure Code Review. *In Proceedings of ACM SIGSOFT International Symposium on Software Testing and Analysis. ACM, New York, NY, USA, 13.* https://doi.org/10.48550/arXiv.2407.12241

5. Do L. N. Q., Wright J. R., Ali K. (2022, March). Why Do Software Developers Use Static Analysis Tools? A User-Centered Study of Developer Needs and Motivations. *IEEE Transactions on Software Engineering*, 48, (3), 835-847. https://doi.org/10.1109/TSE.2020.3004525

6. Yuan, Ye, Yuliang Lu, Kailong Zhu, Hui Huang, Lu Yu, and Jiazhen Zhao. (2023). «A Static Detection Method for SQL Injection Vulnerability Based on Program Transformation» *Applied Sciences* 13, (21): 11763. https://doi.org/10.3390/app132111763

7. NVD. (2023). National vulnerability database https://nvd.nist.gov/ [in English].

8. Chen, Z., Cao, J. (2023). VMCTE: visualization-based malware classification using transfer and ensemble learning. *Computers, Materials & Continua, 75(2),* 4445–4465. https://doi.org/10.32604/cmc.2023.038639

9. NIST. (2023). National institute of standards and technology. https://www.nist.gov/ [in English].

10. Vassallo, C., Panichella, S., Palomba, F., Proksch, S., Zaidman, A., Gall, H. C.(2018). Context is king: The developer perspective on the usage of static analysis tools. *IEEE 25th International Conference on Software Analysis, Evolution and Reengineering (SANER),* 38–49 https://doi.org/10.1007/S10664-019-09750-5/TABLES/9

11. Smith, M., Naiakshina, A, Danilova, A., Gerlitz, E. (2020). On conducting security developer studies with cs students: Examining a password-storage study with cs students, freelancers, and company developers. *Proceedings of the Conference on Human Factors in Computing Systems, Association for Computing Machinery.* pp. 1–12. https://doi.org/10.1145/3290605.3300370

12. Mehrpour, S., LaToza, T. D. (2023). Can static analysis tools find more defects? *Empir Software Eng* 28 (5). https://doi.org/10.1007/s10664-022-10234

13. Shen, S., Kolluri, A., Dong, Z., Saxena, P., Roychoudhury, A. (2021). Localizing vulnerabilities statistically from one exploit. *In Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*. 9781450382878 pp. 537–549. https://doi.org/10.1145/3433210.3437528

14. Tufano, R., Dabić, O., Mastropaolo, A., Ciniselli, M., and Bavota, G. (2023). Code review automation: strengths and weaknesses of the state of the art. IEEE Transactions on Software Engineering, 1–16. https://doi.org/10.1109/TSE.2023.3348172

15. Esposito, M., Falaschi, V., Falessi, D. (2024). An Extensive Comparison of Static Application Security Testing Tools. https://doi.org/10.13140/RG.2.2.12326.54085

16. Esposito, M., Moreschini, S., Lenarduzzi, V., Hästbacka, D., Falessi, D. (2023). Can we trust the default vulnerabilities severity? *In IEEE 23rd International Working Conference on Source Code Analysis and Manipulation (SCAM),* 265–270. https://doi.org/10.1109/SCAM59687.2023.00037

17. Lysenko, S., Bobrovnikova, K., Kharchenko, V. & Savenko, O. (2022). IoT multi-vector cyberattack detection based on machine learning algorithms: traffic features analysis, experiments, and efficiency. *Algorithms*, *15*(7), 239. https://doi.org/10.3390/a15070239

18. Website of Our Study. (2024). Static Application Security Testing (SAST) Tools for Smart Contracts: How Far Are We? https://sites.google.com/view/sc-sast-study-fse2024/ home (Accessed on 29/07/2024).

19. Azman, M., Marhusin, M. F., Sulaiman, R. (2021). Machine Learning-Based Technique to Detect SQL Injection Attack. *Journal of Computer Science. 17,* 296–303. https://doi.org/10.3844/jcssp.2021.296.303

20. Medeiros, P. I., Fonseca, J., Neves, N., Correia, M., Vieira, M. (2018, September). Benchmarking Static Analysis Tools for Web Security. in *IEEE Transactions on Reliability*, V. 67, (3), 1159–1175. https://doi.org/10.1109/TR.2018.2839339

21. Charoenwet, W., Thongtanunam, P., Pham, V. T., Treude, C. (2024). An Empirical Study of Static Analysis Tools for Secure Code Review. *In Proceedings of ACM SIGSOFT International Symposium on Software Testing and Analysis,* 13 https://doi.org/10.48550/arXiv.2407.12241

22. Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G. & Vasylkiv, N. (2020). Botnet detection approach based on the distributed systems. *International Journal of Computing*, *19*(2), 190–198. https://doi.org/10.47839/ijc.19.2.1761

УДК 004.056
DOI https://doi.org/10.32782/IT/2024-3-17

Ірина СТЬОПОЧКІНА
кандидат технічних наук, доцент кафедри інформаційної безпеки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», просп. Берестейський, 37, м. Київ, Україна, 03056
***ORCID:** 0000-0002-0346-0390*
***Scopus ID:**57927656500*

Костянтин ІЛЬЇН
асистент кафедри інформаційної безпеки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», просп. Берестейський, 37, м. Київ, Україна, 03056
***ORCID:** 0009-0004-5463-0996*

Бібліографічний опис статті: Стьопочкіна, І., Ільїн, К. (2024). Профілювання користувачів для підвищення стійкості персоналу об'єктів критичної інфраструктури до кібератак, які використовують людський фактор. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 159–168, doi: https://doi.org/10.32782/IT/2024-3-17

ПРОФІЛЮВАННЯ КОРИСТУВАЧІВ ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ ПЕРСОНАЛУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДО КІБЕРАТАК, ЯКІ ВИКОРИСТОВУЮТЬ ЛЮДСЬКИЙ ФАКТОР

Робота присвячена питанням підвищення стійкості співробітників об'єктів критичної інфраструктури до кібернетичних атак, успішність яких зумовлюється використанням слабкостей людського фактору. Кожна атака соціальної інженерії, яка є запорукою успіху подальшої кібернетичної атаки, експлуатує певні риси, притаманні індивіду. Також використовуються недоліки політики безпеки, притаманні підприємству, які роблять користувачів більш вразливими.

***Метою** даної роботи є збагачення засобів підвищення стійкості персоналу об'єктів критичної інфраструктури до атак соціальної інженерії, в частині засобів діагностичного профілювання, сполучених з тренувальними функціями, які базуються на опитуванні користувачів.*

***Новизна роботи.** Запропоновано підхід до попередження атак соціальної інженерії, заснований на виявленні особливостей, які роблять користувача вразливим до таких атак. Виділено сукупність факторів, присутність яких може бути діагностовано на основі опитування, запропоновано методику опитування та відповідний програмний засіб. На основі факторів побудовано булеві функції, які можуть бути використані при визначенні приналежності користувача до відповідного профілю.*

***Методологія.** Використано експертний метод для формування опитувальника. Вразливості (фактори), які експлуатуються кібератаками на критичну інфраструктуру, визначено в результаті узагальнення існуючих напрацювань в області дослідження. Розроблене програмне забезпечення використовує опитувальник в гнучкому форматі, на основі його створюючи інтерфейс спілкування з користувачем, а на основі відповідей користувача – формуючи результат його профілювання та розбір кейсів, присутніх в опитуванні.*

***Основні результати.** Запропоноване програмне забезпечення та відповідна методика підтримують превентивні засоби та заходи безпеки підприємства, може бути використане як у якості інструменту діагностики вразливостей, так і тренувального засобу. Булеві функції, які визначають приналежність до певного профіля – можуть бути використані при побудові формалізованої моделі внутрішнього порушника.*

***Висновки.** Тестування співробітників об'єктів критичної інфраструктури за розробленою методикою дозволило виявити серед опитуваних груп користувачів, які є вразливими до атак соціальної інженерії певних видів, незважаючи на високий рівень обізнаності в інформаційних технологіях. Запропоновані в роботі засоби є допоміжними в задачах підвищення стійкості персоналу об'єктів критичної інфраструктури до кібератак з використанням людського фактора.*

***Ключові слова:** стійкість, критична інфраструктура, кібератаки, соціальна інженерія, кібербезпека.*

Iryna STOPOCHKINA
Candidate of Technical Sciences, Associate Professor at the Information Security Department, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», 37, Beresteyskyi Ave., Kyiv, Ukraine, 03056, i.stopochkina@kpi.ua
***ORCID:** 0000-0002-0346-0390*
***Scopus ID:** 57927656500*

Kostiantyn ILIN
Assistant at the Information Security Department, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», 37, Beresteyskyi Ave., Kyiv, Ukraine, 03056, kostya.ilin_ipt@lll.kpi.ua
***ORCID:** 0009-0004-5463-0996*

To cite this article: Styopochkina I., Ilyin K. (2024). User profiling to increase the resilience of critical infrastructure personnel to cyberattacks that use the human factor. Information Technology: Computer Science, Software Engineering and Cyber Security, 3, 159–168, doi: https://doi.org/10.32782/IT/2024-3-17

USER PROFILING TO INCREASE RESILIENCE OF CRITICAL INFRASTRUCTURE PERSONNEL TO CYBER ATTACKS USING THE HUMAN FACTOR

The work is devoted to issues of increasing the resistance of employees of critical infrastructure objects to cybernetic attacks, the success of which is determined by the use of human factor weaknesses. Each social engineering attack, which is usually the key to the success of a subsequent cyber attack, exploits certain traits inherent in the individual. It also exploits flaws in enterprise-specific security policies that make users more vulnerable.

***The purpose** of this work is to enrich the means of increasing the resistance of personnel of critical infrastructure objects to social engineering attacks, in terms of diagnostic profiling tools combined with training functions based on user surveys.*

***The novelty of the work**. An approach to the prevention of social engineering attacks is proposed, based on the identification of features that make the user vulnerable to such attacks. A set of factors, the presence of which can be diagnosed on the basis of a survey, is identified, a methodology and a corresponding software tool are proposed. Based on the factors, Boolean functions have been built that can be used to determine whether the user belongs to the appropriate profile.*

***Methodology.** An expert method was used to form the questionnaire. Vulnerabilities (factors) that are exploited by cyberattacks on critical infrastructure are determined as a result of the generalization of existing developments in the field of research. The developed software uses the questionnaire in a flexible format, based on it creating a communication interface with the user, and based on the user's answers, forming the result of his profiling and analyzing the cases present in the survey.*

***Main results**. The proposed software and the corresponding methodology support preventive measures and security measures of the enterprise, can be used both as a tool for diagnosing vulnerabilities and as a training tool. Boolean functions that determine belonging to a certain profile can be used when building a formalized model of an internal violator.*

***Conclusions**. Testing of employees of critical infrastructure facilities according to the developed methodology made it possible to identify among the interviewed groups of users who are vulnerable to social engineering attacks of certain types, despite a high level of knowledge in information technologies. The tools proposed in the work are helpful in the tasks of increasing the resistance of personnel of critical infrastructure objects to cyber attacks using the human factor.*

***Key words:** resilience, critical infrastructure, cyber attacks, social engineering, cybersecurity.*

Актуальність задачі. Незважаючи на наявність великої кількості засобів та тренінгів із питань протидії соціальній інженерії, більше 50% успішних кібернетичних атак засновані саме на експлуатації людського фактора. Наразі значна кількість об'єктів критичної інфраструктури потерпає від атак соціальної інженерії, які є першим етапом для подальшого виконання зловмисних кібервпливів. Кількість таких атак лише підвищилась у воєнний час, таким чином, існуючі засоби протидії атакам з використанням людського фактора потребують збагачення та адаптації до особливостей об'єктів критичної інфраструктури. Зростання кількості та різноманітності успішних атак соціальної інженерії показує, що тренування реагування на конкретні приклади атак соціальної інженерії є лише частиною проблеми, інша частина полягає у причинах, чому працівник є вразливим до тих чи інших атак. Виявлення цих причин, або ж організаційних та соціальних факторів, систематизація їх ролі в експлуатації в ході кібератак є предметом даної роботи. Супутньою задачею є розробка тренінгового засобу, який можна гнучко модифікувати під потреби конкретного об'єкта критичної інфраструктури.

Аналіз досліджень та публікацій. Питання виявлення вразливостей користувача до атак соціальної інженерії розглядалось в попередніх роботах. Зокрема, (Cofense, 2024), в якому емулюються ситуації обходу SEG (Security Email Gateway). Недоліком цього рішення є те, що воно не враховує специфіку конкретного підприємства, не кастомізується, та переважно орієнтоване лише на атаки вектором пошти. Ресурс (Knowbe4, 2024) пропонує широкий спектр тренувань, які дозволяють виявити рівень обізнаності в області кібербезпеки користувачів,

провести симуляцію фішингових атак та надати кейси для опрацювання. Також, слід відзначити складність чи неможливість кастомізації запропонованих кейсів під потреби підприємства, і зосередженість переважно на фішингових атаках, залишаючи поза увагою інші способи соціальної інженерії. Інструменти (Barracuda Networks, 2019) мають схожі особливості та недоліки із вищезазначеними тренінговими засобами та відрізняється складністю використання. Сервіс (DataArt, 2024) надає засіб тестування шляхом емуляції реальних ситуацій для користувачів підприємства, проводячи тестування на проникнення з використанням соціальної інженерії. Такі засоби скоріше слугують для зрізу стану безпеки підприємства, ніж навчанню користувачів. Відповідно, подібні засоби мають під собою алгоритмічне наповнення, яке використовує дослідження актуальних кібератак з використанням людського фактора (Mataracioglu, 2011). Інші загальні ідеї анкетувань користувачів для покращення їх стійкості до атак соціальної інженерії надано в (Gamagedara Arachchilagea, 2014).

Спільною рисою вказаних та багатьох інших робіт та засобів є те, що вони спрямовані на навчання та/ або тестування користувачів на конкретних випадках атак соціальної інженерії, які досить швидко застарівають. Разом з цим, причина успішності відповідних атак, яка полягає у вразливості користувача, що не завжди пов’язана з його необізнаністю, залишається поза увагою. В даній роботі пропонується діагностичний засіб, який сполучений із принципом роботи тренінгового засобу. Запропоновано перелік соціальних та психологічних якостей особи, які роблять особистість вразливою до ряду атак соціальної інженерії. Запропоновано булеві функції для виявлення сукупності рис (профілів), які визначають підвищену вразливість користувача до пропозицій соціального інженера.

Дослідження людських особливостей, які роблять людину вразливою до атак соціальної інженерії, розпочато в роботах (Hadnagy, 2018; Mouton, 2016; Bhakta, 2015). Зокрема, робота (Bhakta, 2015) дає уявлення про побудову таксономії соціо-інженерних атак та їх зв’язок із факторами, які експлуатуються. В роботі (Shevchenko, 2022) розглянуто приклади популярних атак соціальної інженерії під час військового стану в Україні, що дає розуміння людських слабкостей, які експлуатуються.

Деякі із цих особливостей можна ліквідувати заздалегідь, безвідносно до типу атак, які можуть бути застосовані. Наприклад, вразливість користувача до ситуацій, які використовують страх перед керівництвом, або ж невміння відмовляти у незручному становищі, або ж надмірну довірливість. Опитувальний лист складається таким чином, щоби виявити насамперед такі вразливості, і, супутньо, пояснити опитуваному кейси, на яких базуються відповідні питання, у форматі тренінга. Концепт опитування та відповідного програмного засобу автори роботи представили в (Кузьмін, 2024), в даній роботі представлено розширений та поглиблений результат дослідження.

Супутньо, шляхом опитування виявляються недоліки політики безпеки підприємства критичної інфраструктури, які потенційно наражають на небезпеку в виді кібератак, які експлуатують людський фактор, приклади яких наведено в (Lee, 2016; Zetter, 2014; Gallagher, 2016; Liptak, 2016; Sanger, 2021; Tidy, 2021). Зокрема, в роботі (Lee, 2016) проаналізовано етапи кібер-атаки на українську енергетичну систему, в роботі (Zetter, 2014) надано інформацію по атаці на іранський ядерний об’єкт, в публікаціях (Gallagher, 2016; Liptak, 2016) висвітлено особливості атак на транспортну систему Сан-Франциско, в (Sanger, 2021; Tidy, 2021) надано факти по кібератаці на нафтопереробну систему Сполучених Штатів. Ці аналітичні роботи свідчать про вдале використання людського фактору та недоліки політики безпеки, що є запорукою успіху подальшої кібератаки.

Супутньою розв’язаною задачею даної роботи є виявлення ряду характеристик користувача, на які слід звертати увагу для запобіганню інсайдерства.

Нелояльність до компанії, корисливість, агресивність та інші ознаки – можуть слугувати індикаторами потенційно небезпечної ситуації. Перелік таких ознак, опис відповідних профілів та методику їх виявлення запропоновано в даній роботі.

Для виявлення подібних ознак пропонується використовувати підходи соціологічних досліджень, та уже сформовані опитувальні засоби, які пропонуються в роботах (Merecz, 2009; Andersen, 2002; Kersten, 2024; Vo, 2022; Bustamante, 2014; Test Partnership, 2023; Personal Work-Related Responsibility Test, 2016). Зокрема, роботи (Merecz, 2009; Andersen, 2002; Kersten, 2024) присвячені виявленню рівня агресивності, робота (Vo, 2022) розглядає питання вмотивованості на робочому місці, в роботі (Bustamante, 2014) розглянуті питання тестування працелюбності, звіт (Test Partnership, 2023) демонструє приклад комплексного тестування працівника по кількох напрямках,

звіт (PE Konsult Ltd., 2016) надає тест на відповідальність працівника. Засіб тестування (Parvez, 2024) спрямований на виявлення рівня корисливості. Особливості використання людського фактору при атаках на об'єкти критичної інфраструктури можна знайти в (Ghafir, 2018). Дослідження, пов'язані із виділенням людських характеристик, що сприяють соціальній інженерії, були здійснені в роботах (Krombholtz, 2013; Kronberg, 2015).

Мета роботи. Метою роботи є збагачення засобів підвищення стійкості персоналу об'єктів критичної інфраструктури до атак соціальної інженерії, в частині засобів профілювання, сполучених з тренувальними функціями, які базуються на опитуванні користувачів.

Виклад основного матеріалу.

Виділення сукупності вразливостей користувача. Виділимо характеристики користувача, які можуть сигналізувати про схильність до впливів соціальної інженерії.

Виділимо особистісні фактори, які можуть бути тригерами для різних атак соціальної інженерії: схильність до страхів, боязкість F; невміння відмовляти R; невміння обмежуватись при одержанні чогось (жадібність, в тому числі до роботи, азартність в іграх тощо) B; необережність A; необізнаність P; схильність до ліні чи прокрастинації L; байдужість I; непунктуальність U. В залежності від комбінації факторів можна виділити типові профілі осіб, які є схильними до певних атак соціальної інженерії. Кожен профіль визначається відповідною булевою функцією:

1) $P1 = F \cap R \cap I$, профіль, який відповідає м'якій людині, якою легко маніпулювати. Якщо вона навіть помітить порушення, простіше буде промовчати про це.

2) $P2 = B \cap L \cap P$ – профіль, який відповідає активній людині, яка прагне одержати різноманітні блага. Однак, схильна до лінощів, та не цікавиться можливими наслідками рішень. Це дозволяє соціальному інженеру пропонувати варіанти легкої наживи, та порушень кібербезпеки.

3) $P3 = A \cap I \cap U$ – профіль, який відповідає необережній людині, яка не є пунктуальною та уважною. Необізнаність підсилює вразливість до атак, які розраховані на імпульсивні, необдумані рішення.

4) $P4 = I \cap B \cap A$ – профіль, який відповідає людині, схильній до ризику, і достатньо байдужій до негативних наслідків власних дій.

В анкеті пропонуються питання, які відповідають факторам {F, R, B, A, P, L, I, P} чи їх комбінації. Вважається, що фактор присутній, і відповідна булева змінна істинна, коли опитування показало перевищення значення числової оцінки даного фактора над середнім по групі. Або, в цілях тренування, можна перевірити наявність у особи деяких із вказаних властивостей, які частіше експлуатуються соціальними інженерами.

З точки зору аналізу співробітника об'єкту критичної інфраструктури, який має доступ до критичної інформації та/або функцій системи, найбільш небезпечними особистісними факторами є: {A, P, I, U}. Вони можуть сигналізувати про невміння, чи небажання усвідомлювати важливість роботи, прийняття рішень, що є неприпустимим для співробітника об'єкта критичної інфраструктури індустріального типу.

Питання анкети, які містяться в опитувальнику соціотехнічного спрямування, спрямовані на виявлення розуміння співробітником політики безпеки підприємства, наявності чітких інструкцій та обмежень щодо небезпечних дій, та впровадження відповідних технічних засобів та організаційних заходів. Так само, питання анкети можуть згруповані по факторах, до яких в певних ситуаціях чутлива будь-яка людина: сильний вплив (F1), взаємність (F2), перевантаження (F3), недостача (F4), оманливі відносини (F5), терміновість (F6), соціальне схвалення (F7).

Ми можемо розрахувати $Q\left(\{F_i\}\right)$ – сумарний бал по одному чи кількох факторах. Кожна атака соціальної інженерії має свій паттерн, який використовує той чи інший фактор. Наприклад, вішинг часто експлуатує фактори F1, F3, F6. Претекстінг через месенджер використовує фактори F4, F5. Так само, різні види фішингових атак можуть використовувати F7, F2 або інші фактори.

В анкеті питання згруповані також по середовищах- векторах здіснення атаки. Виділено: фізичне середовище, електронну пошту, месенджер, веб-ресурси, соціальні мережі, телефон, особисте спілкування.

Застосунок для діагностування та тренінгів. Питання, варіанти відповідей до них та бали представлені у структурованому вигляді в форматі json. Парсер зчитує питання, і представляє їх та варіанти відповідей у користувацькому інтерфейсі.

Результати опитування узагальнюються у вигляді профілю, який побудований в вигляді «рози вітрів», в якості напрямків виділяються особистісні вразливості та вразливості загального виду (рис. 1). За описаною в питанні ситуацією наводиться пояснення для досягнення навчального ефекту. Опитування також

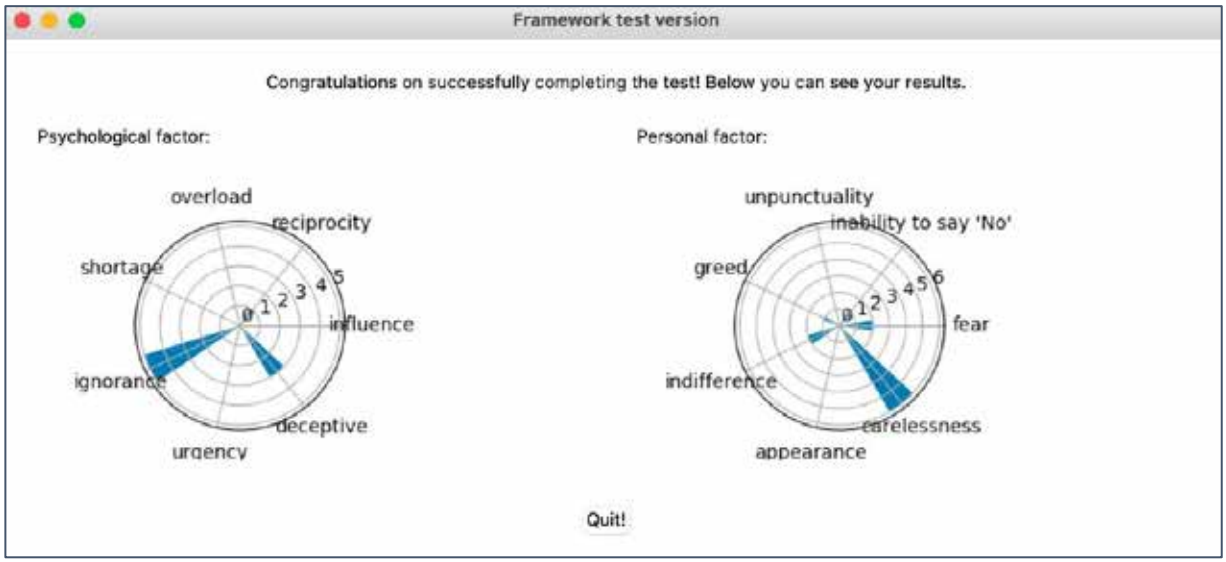


Рис. 1. Приклад візуалізації профілю користувача, який пройшов тестування

Таблиця 1

Результати опитування

Соціальні техніки		Соціо-фізичні		Соціо-технічні	
Враховані фактори	**Відсоток вразливих**	**Враховані фактори**	**Відсоток вразливих**	**Враховані фактори**	**Відсоток вразливих**
F,F1	40	F,F1	20	F7	30
R, F2	10	R,F2	30	B,F4	0
B,F4	60	U,F3	50	A,F2	20
A,F5	20	B,F4	20	P,A	20
P,F4	10	A,P,F4	60	A,F7	30
L,P,F6	0	P,I	40	F,F6	30
F,F6	0	F,F6	40	F,P	10
R	0	F5	60	P	0

дозволяє виявити певні недоліки організаційно-технічного характеру, які притаманні об'єкту критичної інфраструктури на якому здійснюється опитування. Зокрема, можна виявити відсутність заборон на встановлення стороннього програмного забезпечення, використання сторонніх носіїв, відсутність чітких режимно – перепускних правил, незахищений документообіг, незахищене ділове спілкування тощо. За запропонованою методикою було здійснено опитування працівників компаній, що віднесені до критичної інфраструктури, група дослідження складалась із 10 персон, обраних випадковим чином, високого рівня обізнаності в інформаційних технологіях (табл. 1). Основна мета експерименту – оцінити складність запропонованого опитувальника для обізнаного користувача, зручність його використання, та проілюструвати працездатність запропонованого програмного та інформаційного забезпечення діагностування. За відгуками респондентів, опитувальник не повинен бути надто довгим, оскільки увага опитуваного розсіюється, водночас, мала кількість питань може бути недостатньою для виявлення потенційної проблеми. Даний опитувальник було складено з 30 кейсів, по 10 ситуаційних питань на атаки, які ведуться через соціальне, соціо-технічне та соціо-фізичне середовище та можуть бути точкою входу для подальшої кібератаки.

За проведеним опитуванням було виявлено недоліки політики безпеки в організаціях, до яких належали опитувані, зокрема, стосовно використання месенджерів: 80%; документообігу: 30%; веб ресурсів: 90%; телефонії: 70%. Це потенційно наражає на небезпеку персонал, який працює з цими ресурсами.

Проблема інсайдерства та порушень кібербезпеки. За допомогою опитувань можна виявляти ознаки, які є потенційними тригерами здійснення порушень політики безпеки, що особливо важливо для об'єктів критичної інфраструктури. Одержану інформацію можна використовувати на етапі побудови моделі

порушника. Виділимо такі ознаки: відповідальність – V, корисливість – К, агресивність – А, працелюбність – Р, мотивація – М. При побудові профіля користувача можна використовувати функцію $f = f(V,K,A,P,M)$.

Складемо булеві функції f_i, за допомогою яких можна виділити потенційно вразливих з точки зору внутрішніх порушень працівників:

1) Незадоволений працівник, з ознаками агресії:

$$f_1 = (V \cup \neg V) \cap (K \cup \neg K) \cap A \cap (\neg M) \cap (P \cup \neg P);$$

2) Безвідповідальний та невмотивований працівник, потенційне джерело ненавмисних порушень безпеки:

$$f_2 = (\neg V) \cap (K \cup \neg K) \cap (A \cup \neg A) \cap (P \cup \neg P) \cap (\neg M),$$

3) Корисливий працівник $f_3 = (V \cup \neg V) \cap (K) \cap (A \cup \neg A) \cap (M \cup \neg M) \cap (P \cup \neg P)$; і його небезпечний підтип – корисливий, агресивний та невмотивований працівник, здатний на свідомі порушення безпеки: $F_1 = f_4 = (V \cup \neg V) \cap (K) \cap (A) \cap (\neg M) \cap (P \cup \neg P)$.

Вважаємо змінну булевої функції істинною, якщо її значення є вищим за середній рівень по групі.

Рівень комп'ютерної досвідченості персоналу та визначення схильності до порушень кібербезпеки визначають, який тип кіберпорушення може скоїти респондент та на якому саме рівні інформаційної системи.

Таким чином, модель порушника з урахуванням запропонованого підходу може включати такі ознаки:

– Тип порушника: 1)внутрішній (класифікація згідно запропонованого профілю, з виділенням рис V,K,A,M,P), 2)зовнішній (хакер, кіберкримінал, хактивіст, злочинне угруповування);

– Права по відношенню до системи (згідно розподілу прав доступу);

– Рівень кваліфікації (для внутрішніх – згідно тесту на знання інформаційно-комунікаційних технологій, обійманої посади). Цей рівень зазвичай визначається на технічній співбесіді при наймі працівників.

Для ілюстрації було проведено опитування 35 респондентів по 100 бальній шкалі, яке дозволило виявити відповідні риси (рис. 2-6). В якості опитуваних обрано співробітників колективу, які за посадовими обов'язками часто взаємодіють із сторонніми особами, і є потенційною «точкою входу» до інформаційної системи компанії.

Обчислено коефіцієнт кореляції для виявлення зв'язку між парами ознак по групі (табл. 3).

В досліджуваній групі відсутні представники профіля 1) (агресивний та невмотивований працівник), однак, є значна кількість осіб,

Рис. 2. Рівень корисливості респондентів 1-35

Рис. 3 Рівень відповідальності респондентів 1-35

Рис. 4. Рівень працелюбності респондентів 1-35

Рис. 5. Рівень вмотивованості респондентів 1-35

Рис. 6. Рівень агресивності респондентів 1-35

які відповідають типажу 2) – невмотивований та безвідповідальний, який може бути джерелом ненавмисних порушень безпеки, в тому числі і легкою жертвою соціального інженера. Істотна кількість працівників з підвищеним рівнем корисливості теж свідчить про потенційну небезпеку атак з використанням людського фактора.

Методика проведення опитування.

Методика для швидкого опитування на виявлення ознак потенційних вразливостей до атак соціальної інженерії складається з наступних кроків:

1) Опитуваний має бути попереджений про ціль опитування. Ціллю є не перевірка рівня знань чи навичок опитуваного, а виявлення того, які дії насправді можливі в умовах, де працює опитуваний, та варіанти його поведінки.

2) Кожен опитуваний незалежно проходить тестування з використанням програмного забезпечення, відмічаючи ті відповіді, які найбільше для нього підходять.

3) Використання сторонніх джерел при анкетуванні заборонене, відповіді на питання не потребують спеціальних знань. Час опитування має бути достатнім, щоб прочитати всі питання та зрозуміти їхню суть.

4) Для досягнення навчального ефекту, всі кейси, які пропонуються в опитувальнику та коментарі, надані програмою у відповідь, варто додатково розібрати та прокоментувати. Коментарі може надати штатний фахівець з кібербезпеки.

5) Програмне забезпечення за результатами опитування формує «профіль» опитуваного, відмічаючи його слабкі та сильні сторони. Чим вищий бал одержано користувачем по якомусь фактору, тим сильніше проявляється проблема в цьому напрямку. Сукупності особистісних та загально-людських факторів можуть утворювати комбінації, які небезпечні з точки зору вразливості до атак соціальної інженерії. Зокрема, це профілі $P1-P4$.

6) Фахівець з кібербезпеки за участю спеціаліста по людських ресурсах (HR) та, можливо, штатного психолога організації роблять висновки щодо необхідності проведення превентивної та коригуючої роботи стосовно виявлених вразливостей.

Опитування, яке може виявити схильності працівника до скоєння потенційних внутрішніх порушень політики безпеки, здійснюється із залученням штатного спеціаліста з проведення опитувань, за допомогою загальновідомих опитувальників на виявлення ознак корисливості, відповідальності (та безвідповідальності), вмотивованості (та невмотивованості), працелюбності (та ліні), агресивності. Завдяки опитуванню можна виявити ознаки, притаманні профілям $f_1 - f_4$. Булева змінна, яка входить до

Таблиця 2

Характеристики опитування по ознаках

Ознаки	Середнє	Відхил	Дисперсія
Відповідальність	32,5	10,2	104,8
Корисливість	27,0	10,2	104,7
Працелюбність	23,1	8,6	74,9
Мотивація	30,9	9,9	99,0
Агресивність	25,0	10,1	103,6

Таблиця 3

Коефіцієнти кореляції для пар ознак

Ознаки	Коефіцієнт кореляції
Корисливість, агресивність	0,79
Безвідповідальність, непрацелюбність	0,75
Невмотивованість, агресивність	-0,71
Невмотивованість, непрацелюбність	0,68
Невмотивованість, безвідповідальність	0,78

функції профіля, приймає значення «Істина», якщо результат респондента перевищує середнє по групі. Одержані результати можуть бути прийняті до відома при призначенні респондентів на відповідальні посади на об'єкті критичної інфраструктури.

Висновки. Опитування, проведене із використанням запропонованих у роботі методики та засобів, показало, що респонденти правильно реагують на шаблонні ситуації, однак, у випадку ситуацій, які містять елементи форс-мажору, оманливих відносин, чи одержання вигоди можуть несвідомо діяти за задумом соціального інженера. Таким чином, організації повинні приділити увагу тренінгам, які зачіпають саме такі, нестандартні ситуації, які можуть виникнути на об'єкті критичної інфраструктури.

Для запобігання цим атакам треба не лише тренувати персонал на стійкість до поширених атак соціальної інженерії, але й ліквідувати наявні людські вразливості. Робота над вразливостями персоналу може проводитись як із залученням психологів, так і шляхом організаційних заходів: підтримки доброзичливої атмосфери в колективі, підвищенні вмотивованості працівників, впровадження прозорих механізмів комунікації. Важливим є впровадження засобів та заходів політики безпеки.

Запропоновані в роботі профілі та методика не є підставою для остаточних суджень, вони лише є допоміжним діагностичним інструментом для попередження кібератак із використанням слабкостей людського фактора.

Перспективою подальших досліджень може бути розробка графа знань, для швидкого пошуку та ідентифікації відповідних вразливостей у взаємозв'язку із техніками соціальної інженерії.

Подяки. Автори висловлюють подяку Глібу Кузьміну, та Юлії Голубничій, випускникам НН ФТІ КПІ ім. Ігоря Сікорського, за допомогу в постановці практичних експериментів. Всі дослідження здійснювались із дотриманням вимог Закону України «Про захист персональних даних».

ЛІТЕРАТУРА:

1. Cofense. Phishing security awareness training. 2024. URL: https://cofense.com/

2. Knowbe4. New-School Security Awareness Training. 2024. URL: https://www.knowbe4.com/

3. Barracuda Networks. Barracuda Phishline. 2019. URL: https://assets.barracuda.com/assets/docs/dms/Barracuda_PhishLine_DS_US.pdf

4. DataArt. Social Engineering Test. 2024. URL:https://www.dataart.com/services/security/social-engineering-test

5. T. Mataracioglu, S. Ozkan. 2011. User awareness measurement for phishing attacks. Information Management & Computer Security, 19(4), 315-327. URL: arXiv:1108.2149

6. N. A. Gamagedara Arachchilagea, S. Love. Security awareness of computer users: A phishing threat avoidance perspective. 2014. DOI:10.1016/j.chb.2014.05.046

7. C. Hadnagy. The Science of Human Hacking. John Wiley & Sons, Inc., Indianapolis, USA. 2018.

8. F. Mouton, L. Leenen, & H. S. Venter. Social engineering attack framework*. Proceedings of the South African Institute of Computer Scientists and Information Technologists Conference.* ACM, New York, NY, USA. 2016. DOI:10.1109/ISSA.2014.6950510

9. P. Bhakta, M. A. Harris. Semantic analysis of dialogs to detect social engineering attacks. 2015. *DOI:10.1109/ICOSC.2015.7050843*

10. Shevchenko G., Stopochkina I., Babenko I., Peculiarities of phishing threats and preventive measures in the conditions of war in Ukraine // Theoretical and Applied Cybersecurity, Vol. 4 No. 1. 2022. https://doi.org/10.20535/tacs.2664-29132022.1.

11. Г. І. Кузьмін, І. В. Стьопочкіна, К. І. Ільїн. Розробка фреймворка для тестування співробітників критичної інфраструктури на вразливості до атаксоціальної інженерії. Матеріали Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», 13-17 травня 2024, м. Київ. С. 147–150. URL: conf.ipt.kpi.ua.

12. R. M. Lee, M. J. Assante, T. Conway. Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Industrial Control Systems. 2016. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

13. K. Zetter. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group. 2014. 433 p.

14. S. Gallagher. Ransomware locks up San Francisco public transportation ticket machines. Ars Technica. 2016. URL: https://arstechnica.com/information-technology/2016/11/san-francisco-muni-hit-by-black-friday-ransomware-attack/

15. A. Liptak. Hackers are holding San Francisco's light-rail system for ransom. *The Verge*. 2016. URL: https://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomware-cybersecurity-muni

16. D.E. Sanger, C. Krauss, N. Perlroth. Cyberattack Forces a Shutdown of a Top U.S. Pipeline. *The New York Times.* 2021. https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

17. J. Tidy. Colonial hack: How did cyber-attackers shut off pipeline? *BBC News*. 2021. https://www.bbc.com/news/technology-57063636

18. D. Merecz, M. Drabek, A. Mościcka-Teske. Aggression at the workplace – psychological consequences of abusive ecounter with coworkers and clients. International journal of occupational medicine and environmental health. 2009. № 22. P.243–260. DOI:10.2478/v10001-009-0027-2.

19. C.A.Andersen, B.J.Bushman. Human aggression. 2002. DOI:10.1146/annurev.psych.53.100901.135231

20. R. Kersten, T. Greitemeyer. Human aggression in everyday life: An empirical test of the general aggression model. 2024. https://doi.org/10.1111/bjso.12718

21. T.-T-D. Vo, C. Chen, K. Tuliao. Work Motivation: The Roles of Individual Needs and Social Conditions. Behavioral Sciences. 2022. 12(2):49. DOI: 10.3390/bs12020049

22. E. E. Bustamante, C. L. Davis, D. X. Marquez. A Test of Learned Industriousness in the Physical Activity Domain. 2014. DOI:10.5539/ijps.v6n4p12

23. Test Partnership. Simone Sample. 2023. TPAQ-45 Complete Profile. Full Report. URL: https://www.testpartnership.com/samplereports/sample-report-personality.pdf

24. PE Konsult Ltd. Personal Work-Related Responsibility Test (WRT). 2016. URL: https://www.pekonsult.ee/testid/Vastutus.pdf

25. H. Parvez. 'Am I selfish?' Quiz (Selfishness score). 2024. URL: https://www.psychmechanics.com/am-i-selfish-quiz/

26. I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour et al. Security threats to critical infrastructure: the human factor. 2018. DOI:10.1007/s11227-018-2337-2

27. K. Krombholtz. Social Engineering Attacks on the Knowledge Worker. Proceedings of the 6th International Conference on Security of Information and Networks. 2013. URL: https://publications.sba-research.org/publications/sig-alternate.pdf

28. B. Kronberg, J. Swanlund, H. Jeppsson. Social Engineering. A study in awareness and measures. 2015. URL: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=5474076&fileOId=5474079

REFERENCES:

1. Cofense. Phishing security awareness training. 2024. Retrieved from: https://cofense.com/

2. Knowbe4. New-School Security Awareness Training. 2024. Retrieved from: https://www.knowbe4.com/

3. Barracuda Networks. Barracuda Phishline. 2019. Retrieved from: https://assets.barracuda.com/assets/docs/dms/Barracuda_PhishLine_DS_US.pdf

4. DataArt. Social Engineering Test. 2024. Retrieved from:https://www.dataart.com/services/security/social-engineering-test

5. Mataracioglu, T., Ozkan, S. (2011). User awareness measurement for phishing attacks. *Information Management & Computer Security*, 19(4), 315–327. Retrieved from: arXiv:1108.2149

6. N. A. Gamagedara Arachchilagea, S. (2014). Love. Security awareness of computer users: A phishing threat avoidance perspective. DOI:10.1016/j.chb.2014.05.046

7. Hadnagy, C. (2018). The Science of Human Hacking. John Wiley & Sons, Inc., Indianapolis, USA.

8. Mouton, F., Leenen, L. & Venter, H. S. (2016). Social engineering attack framework. *Proceedings of the South African Institute of Computer Scientists and Information Technologists Conference*. ACM, New York, NY, USA. DOI:10.1109/ISSA.2014.6950510

9. Bhakta, P. & Harris, M. A. (2015). Semantic analysis of dialogs to detect social engineering attacks. *DOI:10.1109/ICOSC.2015.7050843*

10. Shevchenko, G, Stopochkina, I., Babenko, I. (2022). Peculiarities of phishing threats and preventive measures in the conditions of war in Ukraine. Theoretical and Applied Cybersecurity, Vol. 4 No. 1. DOI: https://doi.org/10.20535/tacs.2664-29132022.1.

11. G. Kuzmin, I. Stopochkina, K. Ilin. Development of framework for critical indfrastructure employee testing on social engineering vulnerabilities (in Ukrainian). Materials of All-Ukr. Scient. and Pract. Conference «Theoretical and applied problems of physics, mathematics and infromatics», 13-17th of May. 2024, Kyiv. P. 147–150.

12. Lee, R. M., Assante, M. J., Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Industrial Control Systems. Retrieved from: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

13. Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group. 433 p.

14. Gallagher, S. Ransomware locks up San Francisco public transportation ticket machines. Ars Technica. Retrieved from: https://arstechnica.com/information-technology/2016/11/san-francisco-muni-hit-by-black-friday-ransomware-attack/

15. Liptak, A. (2016). Hackers are holding San Francisco's light-rail system for ransom. *The Verge*. Retrieved from: https://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomware-cybersecurity-muni

16. Sanger, D. E., Krauss, C., Perlroth, N. (2021). Cyberattack Forces a Shutdown of a Top U.S. Pipeline. *The New York Times.* https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

17. Tidy. J. (2021). Colonial hack: How did cyber-attackers shut off pipeline? *BBC News*. https://www.bbc.com/news/technology-57063636

18. Merecz, D., Drabek, M., Mościcka-Teske, A. (2009). Aggression at the workplace – psychological consequences of abusive ecounter with coworkers and clients. *International journal of occupational medicine and environmental health*. № 22. P.243–260. DOI:10.2478/v10001-009-0027-2.

19. Andersen, C. A., Bushman, B. J. (2002). Human aggression. DOI:10.1146/annurev.psych.53.100901.135231

20. Kersten, R., Greitemeyer, T. (2024). Human aggression in everyday life: An empirical test of the general aggression model. https://doi.org/10.1111/bjso.12718

21. T.-T-D.Vo, Chen, C., Tuliao, K. (2022). Work Motivation: The Roles of Individual Needs and Social Conditions. Behavioral Sciences. 12(2):49. DOI: 10.3390/bs12020049

22. Bustamante, E. E., Davis, C. L., Marquez, D. X. (2014). A Test of Learned Industriousness in the Physical Activity Domain. DOI:10.5539/ijps.v6n4p12

23. Test Partnership. Simone Sample. TPAQ-45 Complete Profile. Full Report. 2023. Retrieved from: https://www.testpartnership.com/samplereports/sample-report-personality.pdf

24. PE Konsult Ltd. Personal Work-Related Responsibility Test (WRT). 2016. Retrieved from: https://www.pekonsult.ee/testid/Vastutus.pdf

25. Parvez, H. (2024). 'Am I selfish?' Quiz (Selfishness score). Retrieved from: https://www.psychmechanics.com/am-i-selfish-quiz/

26. Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H. et al. (2018). Security threats to critical infrastructure: the human factor. DOI:10.1007/s11227-018-2337-2

27. Krombholtz, K. et al. (2013). Social Engineering Attacks on the Knowledge Worker. Proceedings of the 6th International Conference on Security of Information and Networks. Retrieved from: https://publications.sba-research.org/publications/sig-alternate.pdf

28. Kronberg, B., Swanlund, J., Jeppsson, H. (2015). Social Engineering. A study in awareness and measures. Retrieved from: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=5474076&fileOId=5474079

УДК 004.891
DOI https://doi.org/10.32782/IT/2024-3-18

Марина ФАЛЕНКОВА
старший викладач кафедри інженерії програмного забезпечення, Чорноморський національний університет імені Петра Могили, вул. 68 Десантників 10, Миколаїв, Україна, 54000
***ORCID:** 0000-0001-7797-0142*
***Scopus Author ID:** 57222762475*

Бібліографічний опис статті: Фаленкова, М. (2024). Модернізація аварійно-попереджувальних систем суден шляхом інтеграції експертної системи підтримки прийняття рішень. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 169–179, doi: https://doi.org/10.32782/IT/2024-3-18

МОДЕРНІЗАЦІЯ АВАРІЙНО-ПОПЕРЕДЖУВАЛЬНИХ СИСТЕМ СУДЕН ШЛЯХОМ ІНТЕГРАЦІЇ ЕКСПЕРТНОЇ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

***Мета роботи** полягає у детальному вивченні та розробці ефективних методів і моделей для швидкої діагностики та усунення несправностей в електричних системах автоматизації суден. Зокрема, досліджується процес побудови дерев відмов і дерев рішень для ідентифікації дефектів у специфічних об'єктах діагностики та їх структурних одиницях, з акцентом на підвищення швидкості та точності виявлення несправностей. **Методологія.** У дослідженні використано інтегрований підхід до аналізу систем діагностики, що включає застосування сучасних методів побудови дерев відмов і дерев рішень. Пропонується новаторська система підтримки прийняття рішень (СППР), яка дозволяє підвищити ефективність процесів пошуку несправностей за рахунок використання математичних моделей. У дослідженні також здійснено систематизацію основних суб'єктивних та об'єктивних факторів, які впливають на час, що витрачається на відновлення системи після виявлення несправностей. Обґрунтовано необхідність переходу від паперової документації до електронної з використанням сучасних експертних систем, що значно прискорює та полегшує процеси технічного обслуговування.*

***Наукова новизна** роботи полягає у впровадженні нового підходу до підвищення ефективності аварійно-попереджувальних систем (АПС) суден завдяки використанню СППР, що базується на нових математичних моделях для діагностики несправностей. Впроваджена СППР дозволяє значно скоротити час на пошук несправностей, підвищити точність діагностики та знизити вплив людського фактора, що є критичним для забезпечення безпеки та стабільної роботи суднових систем.*

***Висновки.** Результати дослідження свідчать, що удосконалення аварійно-попереджувальних систем суден через впровадження СППР може суттєво покращити рівень безпеки та ефективності експлуатації суден. СППР не лише знижує ризики, пов'язані з технічними несправностями суднового обладнання, але й мінімізує можливі фінансові втрати, які можуть виникнути внаслідок аварійних ситуацій. Використання математичних моделей та алгоритмів для діагностики несправностей забезпечує швидке і точне реагування на аварійні ситуації, що є ключовим для безпечної експлуатації суден в умовах сучасного морського транспорту.*

***Ключові слова:** автоматизовані системи судна, експертна система, система підтримки прийняття рішень, об'єкт діагностики, пристрої електроавтоматики, складна технічна система, оператор, система моніторингу тривог.*

Maryna FALENKOVA
Senior Lecturer at the Department of Software Engineering, Petro Mohyla Black Sea National University, 10, 68-Desantnykiv Str., Mykolaiv, Ukraine, 54003, marynakotova@gmail.com
***ORCID:** 0000-0001-7797-0142*
***Scopus Author ID:** 57222762475*

To cite this article: Falenkova, M. (2024). Modernizatsiia avariino-poperedzhuvalnykh system suden shliakhom intehratsii ekspertnoi systemy pidtrymky pryiniattia rishen [Modernization of ship emergency warning systems by integrating an expert decision support system]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 169–179, doi: https://doi.org/10.32782/IT/2024-3-18

MODERNIZATION OF SHIP EMERGENCY ALARM SYSTEMS BY INTEGRATION OF AN EXPERT DECISION SUPPORT SYSTEM

Purpose of study *is to thoroughly investigate and develop efficient methods and models for the rapid diagnosis and troubleshooting of electrical systems in ship automation. The research focuses on the construction of fault trees and decision trees for defect identification in specific diagnostic objects and their structural units, with an emphasis on improving the speed and accuracy of fault detection.* ***Methodology.*** *An integrated approach was applied to analyze diagnostic systems, including the use of advanced methods for building fault trees and decision trees. A novel Decision Support System (DSS) is proposed, which enhances the efficiency of fault detection processes through the application of mathematical models. The study also systematizes the key subjective and objective factors that influence the time required for system recovery after faults are detected. The need for a shift from paper-based to electronic maintenance documentation, utilizing modern expert systems, is substantiated as a crucial step for accelerating and facilitating maintenance processes.*

Scientific novelty *of the work lies in the introduction of a new approach to improving the efficiency of ship emergency warning systems (EWS) through the use of a DSS based on innovative mathematical models for fault diagnostics. The implemented DSS significantly reduces the time required for fault detection, improves diagnostic accuracy, and minimizes the impact of human factors, which is critical for ensuring the safety and reliability of ship systems.*

Conclusions. *The results of the study indicate that enhancing ship emergency warning systems through the implementation of a DSS can substantially improve the safety and operational efficiency of ships. The DSS not only reduces risks associated with technical malfunctions of ship equipment but also minimizes potential financial losses that may arise from emergency situations. The use of mathematical models and algorithms for fault diagnostics ensures quick and accurate responses to emergencies, which is crucial for the safe operation of ships in modern maritime transport conditions.*

Key words: *automation devices, decision support system, expert system, diagnostic object, electromechanical complex technical system, operator, ship automated systems, alarm monitoring system.*

Аналіз досліджень і публікацій. Сучасні електронні технології знайшли широке застосування у сфері навігації. Водночас ускладнення конфігурації електрообладнання, збільшення його кількості та широке впровадження інтегрованої автоматизації на кораблях неминуче призводить до збільшення кількості відмов судових систем. Досвід експлуатації складних технічних систем показує, що основна частина часу витраченого на відновлення роботи пристроїв електроавтоматики (EAD), припадає на пошук дефектів. Актуальність статті полягає у необхідності знайти рішення для зменшення негативного впливу так званого «людського фактора» при експлуатації та технічному обслуговуванні суднового обладнання, що зазначено у резолюції IMO A.884(21). Включаючи, потребу в підвищенні безпеки екіпажу, а також збільшення експлуатаційного періоду електрообладнання суден.

Аналіз наукових праць показав, що багато дослідників вивчали проблему прогнозування і передбачення відмов систем суден. Розроблені та впроваджені методи допомогли знизити кількість відмов електрообладнання. Однак недоліком такого підходу є відсутність координації дій оператора при фактичній відмові, що може призвести до катастрофічних наслідків.

Принципи розробки експертних систем були описані ще в наукових працях А. Брукінга (Брукінг, 1980), К. Нейлора (К. Нейлор, 1991) та інших. Використання сучасних технологій у розробці інтелектуальних систем досліджували Р. Баженов і Д. Лопатін (Баженов, Лопатін, 2014). Також існує низка праць, що розглядають підходи до формування експертних груп. У роботах (Коваленко, Давиденко, Швед, 2019) запропоновано підхід, що дозволяє виділити групи експертів із «близькими» думками, проаналізувати їх з метою розробки фінальної (групової) оцінки, яка враховує думки (аргументи) кожного експерта. Б. Палюх та інші розглядали інтелектуальну систему підтримки прийняття рішень для управління складними об'єктами з використанням динамічних нечітких когнітивних карт (Палюх, Какатунова, Багузова, 2013). У дослідженнях Інституту електроенергетики США в галузі розробки та використання експертних систем особливу увагу приділено трьом основним напрямкам: управління, діагностика обладнання та інформаційна підтримка. Досвід розробок зарубіжних вчених описано в роботах (Морено, Еспехо, 2015; Ліберадо, 2015).

На даний час використовується і розробляється багато інформаційних систем, методів та інструментів для моніторингу та діагностики технічного стану електрообладнання (Крайник, Давиденко, Томаш, 2019, с. 258–262). Аналіз їх ефективності показує, що, поряд із багатьма конкретними перевагами, вони мають декілька недоліків (Афромєєв, 2013). Як правило, це методи вилучення інформації з досить великої кількості контрольних точок. У такому разі процес діагностики включає реалізацію

розгалужених алгоритмів, складність яких зростає із збільшенням розмірів діагностованого електричного кола.

Постановка проблеми. Процес усунення несправностей є найскладнішим під час ремонту електрообладнання. Щоб показати можливу кількість часу, витраченого на пошук і ремонт, був проведений експеримент на одному з контейнеровозів компанії Mediterranean Shipping Company (MSC) – судні MSC «LETIZIA». Ми використовували архівний журнал системи моніторингу тривог Kongsberg K-Chief 600, яка встановлена на контейнеровозі MSC «LETIZIA», побудованому у 2015 році. Загальна кількість параметрів, які контролюються AMS, складає 3410 одиниць (Консберг, 2013).

Дані про несправності судна, зафіксовані у судновому журналі протягом шести місяців, були умовно поділені за рівнем складності систем, у яких вони виникали, і підсумовані в таблиці, показаній у Таблиці 1. Метою експерименту було підрахувати середню кількість можливих причин цих несправностей, а також кількість можливих способів їх усунення та час, витрачений на їх усунення.

Загальна кількість несправностей, зафіксованих системою AMS за шість місяців. Початкові дані з журналу зведені у таблицю 2.

На основі отриманих даних ми будуємо варіаційний ряд спостережень за кількістю несправностей, що відбулися протягом шести місяців на судні, та кількістю їх можливих причин. Знайдемо відносну частоту подій за шість місяців W_i для кожного рівня складності систем.

$$W_i = \frac{N_i}{n}, \qquad (1)$$

де N_i – кількість несправностей на даному інтервалі; n – загальна кількість несправностей за шість місяців.

Підставляємо числові дані, отримуємо: $W_1 = 0.05$; $W_2 = 0.235$; $W_3 = 0.367$; $W_4 = 0.321$; $W_5 = 0.027$.

Таблиця 1

Таблиця несправностей системи моніторингу тривог Kongsberg K-Chief 600 на контейнеровозі MSC «LETIZIA»

Прості елементи	Прості системи	Системи середньої складності	Складні системи	Дуже складні системи
1. Pipe Duct BW level high.	1. Ballast valve 061 open fail.	1. SCU 0800 NET COMMERR.	1. Boiler burner swing out.	1. PTG synchronization fails.
2. HFO TK (PS) level high.	2. WBV064 Feedback fail.	2. Bilge water oil content is high.	2. SW cool. pump No.1 inverter abnormal.	2. Elevator abnormal.
…	…	…	…	…
24. ULS HFO Tk (PS) temp. low.	126. Heating temp. of oil st-by AE 1 too low.	198. Working air compressor fail.	168. EDG common alarm.	12. Bow thruster not operation.
Всього – 26	Всього – 123	Всього – 192	Всього – 168	Всього – 14

Таблиця 2

Таблиця вихідних даних

№	Змінна	Значення	Характеристики
1	M	180	Кількість днів, протягом яких фіксувалися несправності
2	n	523	Середня кількість несправностей за шість місяців
3	m	5	Кількість категорій несправностей за рівнем складності
4	X1	5	Середня кількість можливих причин несправності для простих елементів
5	X2	11	Середня кількість можливих причин несправності для простих систем
6	X3	18	Середня кількість можливих причин несправності для систем середньої складності
7	X4	23	Середня кількість можливих причин несправності для складних систем
8	X5	27	Середня кількість можливих причин несправності для дуже складних систем
9	N1	26	Піврічна середня частота несправностей для простих елементів
10	N2	123	Піврічна середня частота несправностей для простих систем
11	N3	192	Середня частота несправностей за шість місяців для систем середньої складності
12	N4	168	Піврічна середня частота несправностей для складних систем
13	N5	14	Піврічна середня частота несправностей для дуже складних систем

Знайдемо числові параметри: середнє значення і дисперсію.

Вибіркове середнє:

$$\underline{X_B} = \frac{1}{n}\sum_{i=1}^{m} N_i * X_i \approx 18 \qquad (2)$$

Дисперсія дискретної випадкової величини:

$$D_B = \frac{1}{n}\sum_{i=1}^{m}\left(X_i - \underline{X_B}\right)^2 = 30.12 \qquad (3)$$

Стандартне відхилення:

$$\sigma_B = \sqrt{30.12} \approx 5 \qquad (4)$$

Таким чином, середня кількість можливих причин випадкової несправності, зафіксованої системою AMS, $\underline{X_B} = 18$, зі стандартним відхиленням $\sigma_B = 5$.

Інтервал у межах одного сигма (ймовірність довіри 67%) для цієї випадкової величини становить від 13 до 23 можливих причин. Це означає, що навіть досвідчені електрики часто будуть витрачати досить багато часу на здогадки про причини поломок та їх усунення.

Методи дослідження. Техніка діагностики SAS (Автоматизовані системи корабля) включає ієрархічний принцип пошуку дефектів. На кожному етапі діагностики поступово уточнюється місце знаходження дефекту. Визначається несправний блок (структурно спроектований елемент OOD (об'єкт діагностики), який надіслав повідомлення про помилку). Виявлений блок діагностується з глибиною пошуку до вузла/елемента функціональної схеми тощо. Результатом є діагностика на рівні елемента функціональної схеми з глибиною пошуку до елемента принципової схеми.

Після підтвердження факту збою системи починається період пошуку дефекту. Оскільки основна частина часу від моменту збою до відновлення працездатності системи витрачається саме на пошук дефекту, ми розглянемо цей період детальніше.

Будь-яку технічну систему можна представити у вигляді дерева відмов, показаного на Рисунку 1.

На першому етапі реєструється факт відмови конкретної корабельної системи. Завдання спеціаліста, відповідального за працездатність систем – повернути систему зі стану несправності до робочого стану.

На другому етапі об'єкт діагностики умовно розбивається на його складові частини – структурні одиниці (SU), з'єднані послідовно. Для графічного подання SU зазвичай використовуються моделі OOD у вигляді структурних, функціональних, електромонтажних і принципових схем. Кожна SU може бути окремим модулем, блоком, вузлом, сектором тощо.

Спеціаліст обирає стратегію подальшого пошуку дефекту, тобто якими методами буде локалізовано несправність в конкретній SU. Існує три методи:

1. **Послідовний метод пошуку** – пошук дефекту здійснюється шляхом вимірювання сигналу в контрольних точках по черзі від однієї SU до іншої. Вихідний сигнал кожної SU перевіряється. Найбільш зручними моделями для вибору контрольних точок є принципові та структурні схеми OOD.

2. **Паралельний метод пошуку** – OOD розділяється на дві рівні або майже рівні частини при кожній перевірці, якщо кількість SU у OOD є парною або непарною.

3. **Комбінований метод пошуку** – комбінація послідовного і паралельного методів.

Універсальні алгоритми пошуку несправної SU представлені на Рисунку 2, де:

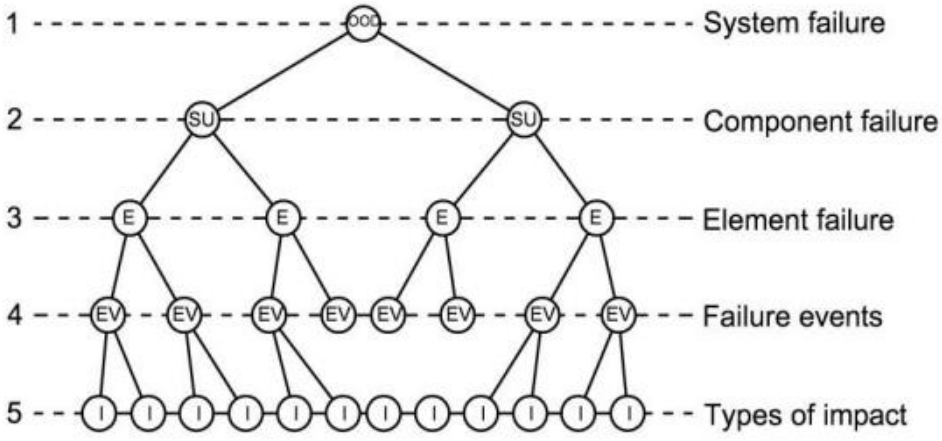
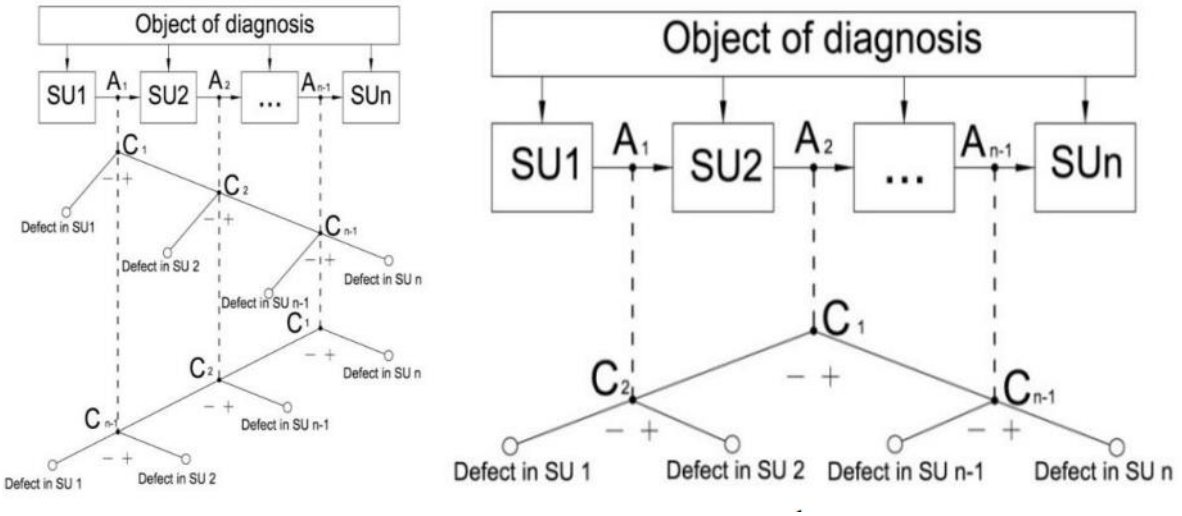


Рис. 1. Умовна схема побудови дерева відмов корабельної системи



а *б*

Рис. 2. Універсальні алгоритми пошуку дефектних SU: а – послідовним методом, б – паралельним методом

SU_1, SU_2, SU_n – структурні одиниці об'єкта діагностики.

A_1, A_2, A_{n-1} – контрольні точки (вихідні сигнали з кожної SU).

C_1, C_2, C_{n-2} – перевірки.

n – порядковий номер SU у схемі.

Послідовність перевірок під час пошуку дефекту представлена у вигляді графа (дерева), де вершини – це перевірки, а гілки вказують напрям переходу в залежності від результату перевірки, кінцеві вершини – це виявлені дефекти.

Перевірка дефекту в SU може проводитися двома способами: з початку до кінця і з кінця до початку.

Наприклад, для OOD, що складається з 4 структурних одиниць (n = 4), пошук виконується (див. Рис. 2): а) *послідовним методом.*

У першому випадку необхідно перевірити C_1 у точці A_1. Якщо сигнал знаходиться в допустимих межах, тоді перевірка C_2 повинна бути виконана у точці A_2, що визначить стан SU_2. Якщо результат перевірки негативний, дефект знаходиться у структурній одиниці. Якщо результат позитивний, необхідно виконати перевірку у наступній точці.

У другому випадку (з кінця до початку), якщо результат перевірки C_1 у точці A_{n-1} негативний, наступну перевірку C_2 слід виконати у точці A_{n-2} (A_2). Якщо результат позитивний, дефект знаходиться у SU_{n-1}; якщо результат негативний, виконується наступна перевірка.

В результаті послідовності перевірок пошук призводить до певного стану, що відповідає виявленню несправної SU.

b) паралельним методом.

Перша перевірка C_1 виконується у точці A_2. Якщо результат негативний, наступна перевірка C_2 виконується у точці A_1, що дозволяє визначити місце дефекту (SU_1 або SU_2). В іншому випадку, перевірка C_{n-1} призначається у точці A_{n-1}; це дозволяє визначити дефект у CE_{n-1} або CE_n.

На третьому етапі усунення несправності для дефектної SU будується дерево рішень. Для складання алгоритму пошуку дефекту у вигляді дерева рішень використовуються моделі OOD принципових схем, електромонтажних схем і схем з'єднань. SU розбивається на окремі взаємопов'язані вузли або прості елементи, і кожен з них перевіряється (див. Рисунок 3).

Алгоритм пошуку дефекту в SU являє собою дерево рішень у вигляді послідовних перевірок вузлів та елементів цієї SU. Перевірки виконуються різними методами в залежності від рішення оператора. Найбільш використовувані методи для перевірки ймовірних дефектів: зовнішній огляд, прозвонка, оцінка експлуатаційних даних, порівняння з робочим блоком, моделювання, тимчасова модифікація схеми, метод заміни, перевірка робочого режиму елемента, провокаційні впливи.

Для типових несправностей використовуються таблиці дефектів OOD. Після виявлення дефекту в SU починається четвертий етап аналізу причин. Визначається подія, яка призвела до дефекту цього елемента. Це може бути поганий контакт, корозія, окислення,

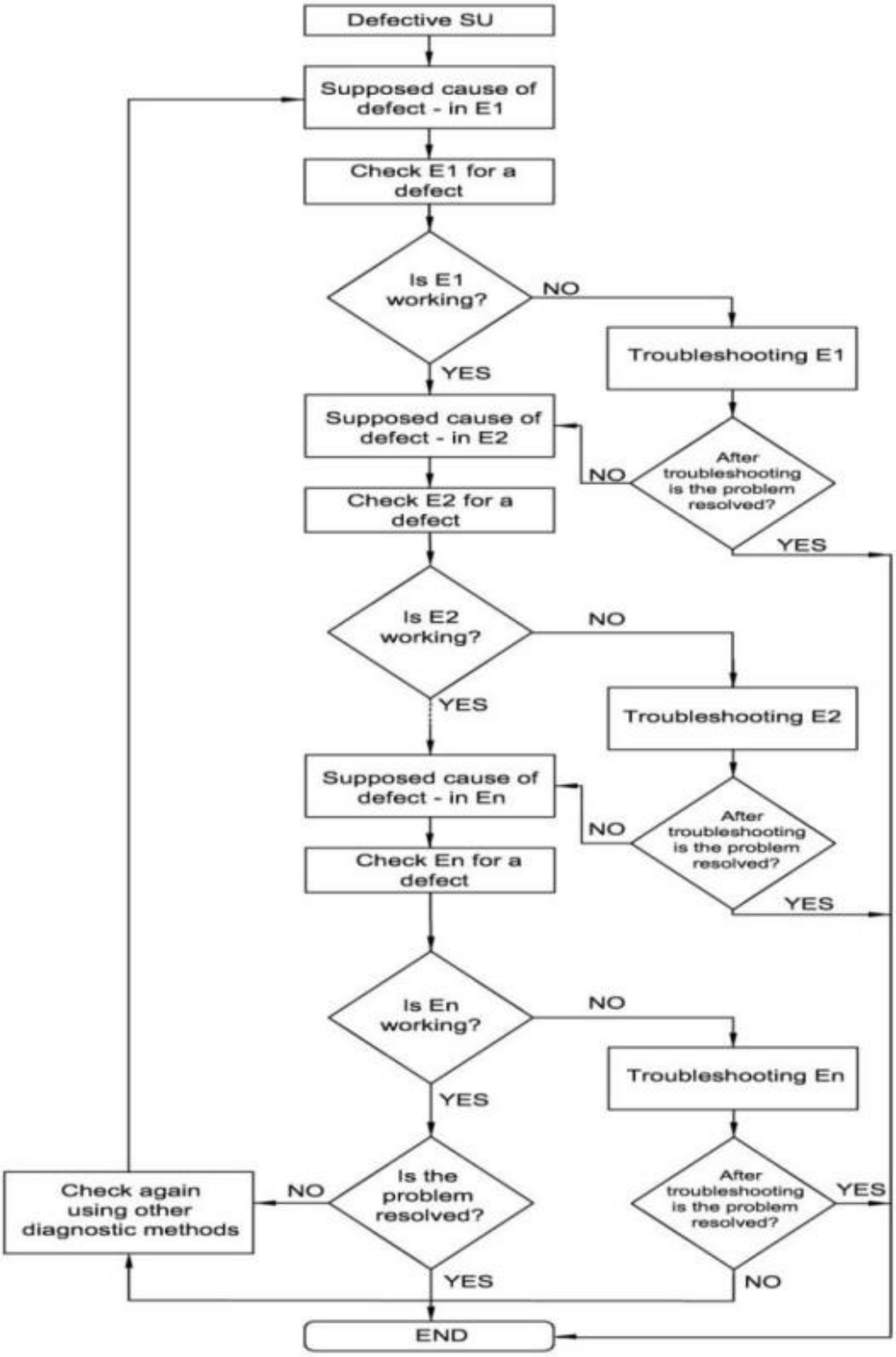


Рис. 3. Універсальний алгоритм пошуку дефектів в SU у вигляді дерева рішень

пробій ізоляції, стрибки напруги, перевантаження струму, дефект матеріалу тощо. Після усунення події, що призвела до відмови елемента, починається фінальний етап. На останньому етапі визначаються та усуваються види впливу, які сприяли виникненню події, що викликала відмову елемента OOD. Найпоширеніші типи впливу: температура, вологість, вібрація, механічні навантаження, електромагнітне керування, пил тощо.

Реалізація. Запропонована система буде побудована на основі знань, які включають

досвід експертів у галузі ремонту та усунення несправностей. База знань формується на основі експертних оцінок (експерти – це електрики з досвідом роботи не менше 5 років, а також суперінтенданти крюїнгових компаній з таким же досвідом). Система використовує підхід, який реалізує завдання розділення інформації, що зберігається в загальній базі даних, і безпосередньо в базі знань (набір таблиць рішень).

Для реалізації цього підходу використовуються змінні зв'язку (з'єднувальні таблиці). За допомогою цих таблиць зв'язку змінна з бази знань пов'язується з даними, що зберігаються у загальній базі даних обладнання, та готовими алгоритмами усунення несправностей.

Блок-схема експертної системи показана на Рисунку 4.

База знань включає знання та оцінки експертів щодо несправностей, а також бази даних зі структурними схемами, принциповими схемами елементів та компонентів, а також алгоритмами усунення несправностей.

Заповнення відбувається на основі суднових журналів. Фіксується кількість несправностей, виявлених системою APS для суден типу контейнеровоз. Для введення у базу даних несправності ранжуються за рівнем складності. Усі записи передаються до крюїнгової компанії суперінтендантом. База даних заповнюється на основі даних журналів, зібраних з усіх суден крюїнгу протягом усього періоду експлуатації.

Кінцевим продуктом є програмне забезпечення, яке надає оператору повну, але не надмірну інформацію про необхідну несправність, а також чітку послідовність дій для її швидкого усунення. На Рисунку 5 показані деякі вікна пропонованої експертної системи:

Операція прийняття рішення в експертній системі електрика судна виглядає так: зареєстрована помилка системи AMS вводиться у вікно системи. Користувач отримує усю необхідну документацію на блок, що видав сигнал помилки, а також набір стратегій для усунення несправності.

Висновки. Структурні, схематичні та технологічні варіанти підвищення надійності SAS обмежені, і більшість часу, витраченого обслуговуючим персоналом на відновлення працездатності суднового електрообладнання, витрачається на пошук несправностей. Очевидним способом усунення цих суперечностей є розробка методів, що мінімізують час, необхідний для пошуку та усунення несправностей. Терміни обробки і аналізу суднової документації скорочуються на 50%. Використовуючи пропоновану систему, час, необхідний для усунення причини несправності скорочується на 25-50%. В результаті впровадження системи отримано значно поліпшення якості прийнятих рішень.

Ця стаття чітко демонструє нагальну необхідність впровадження спеціальних інформаційних експертних систем, які при низькій кваліфікації обслуговуючого персоналу та низькій ефективності контролю об'єктів діагностики можуть швидко здійснювати пошук дефектів у несправній судновій системі.

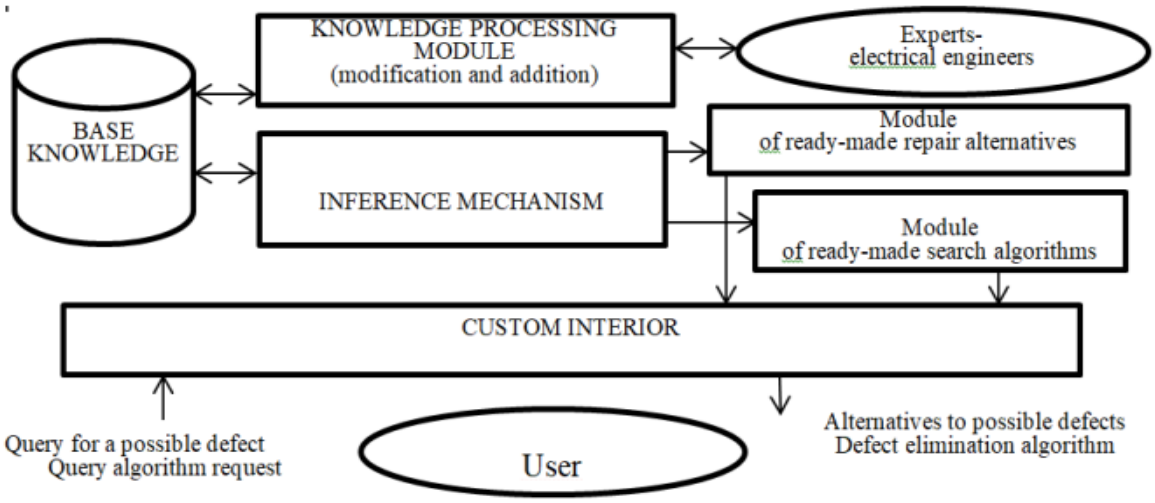


Рис. 4. Блок-схема експертної системи

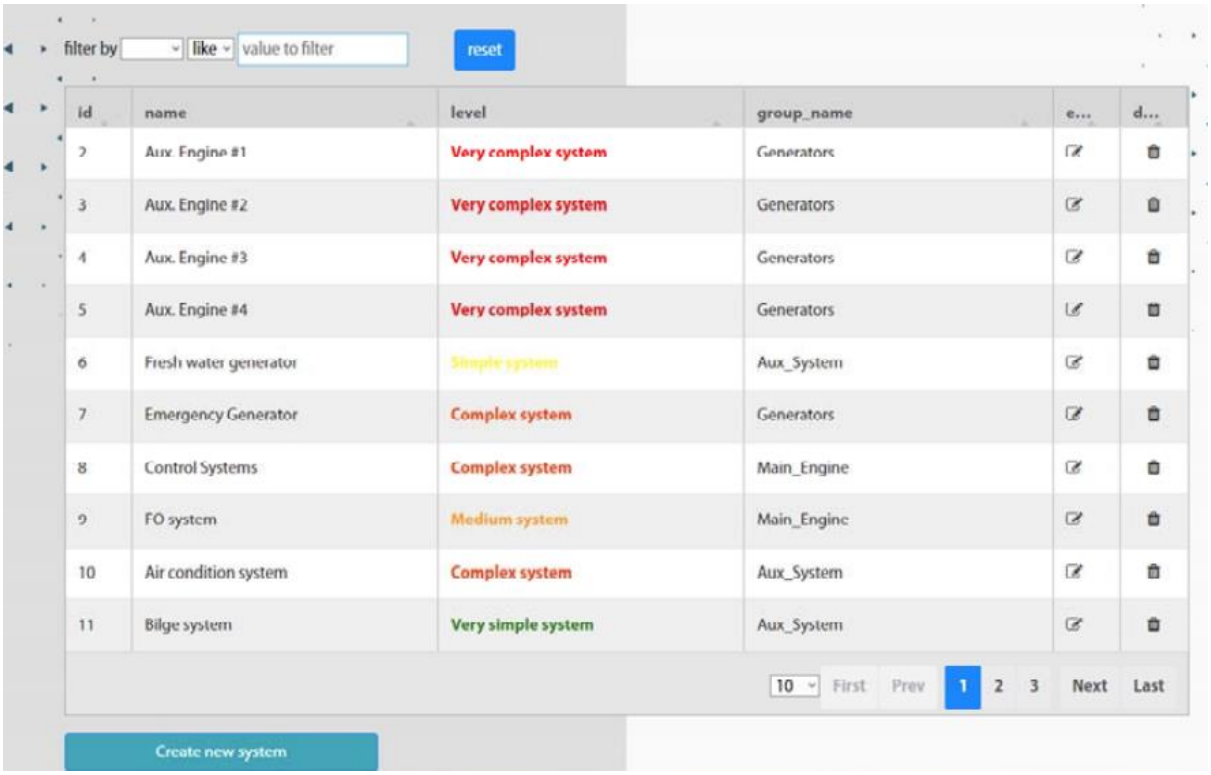


Рис. 5.1. Сторінка СППР з описом суднових систем

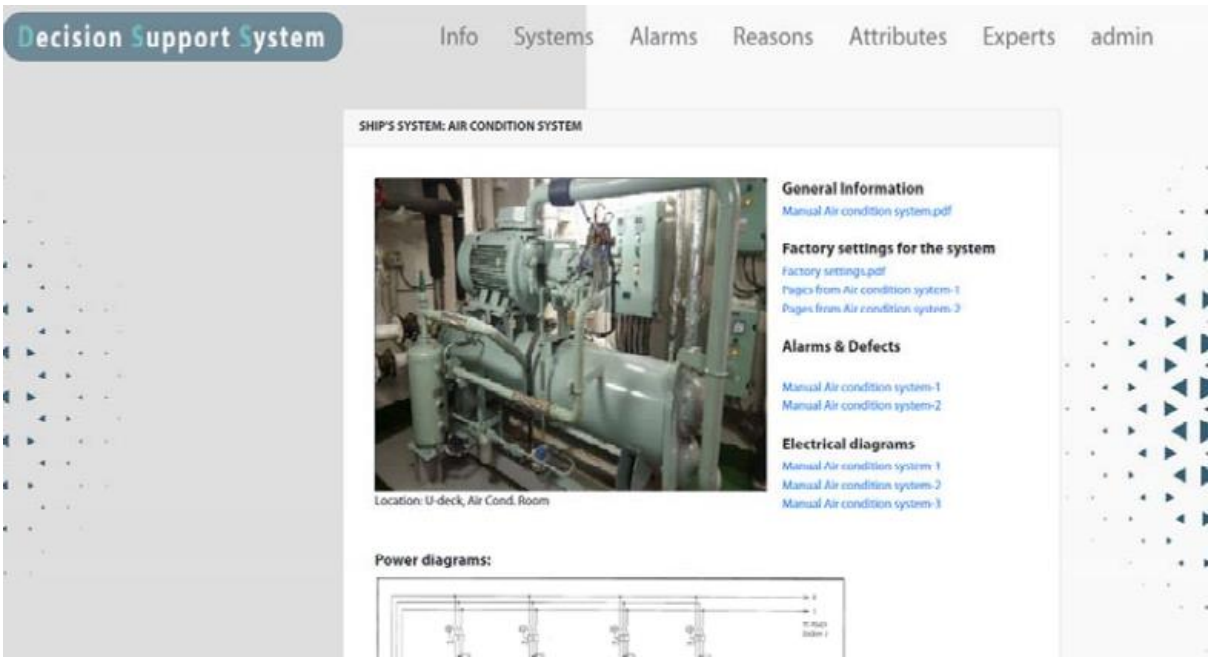


Рис. 5.2. Суднова система кондиціонування повітря

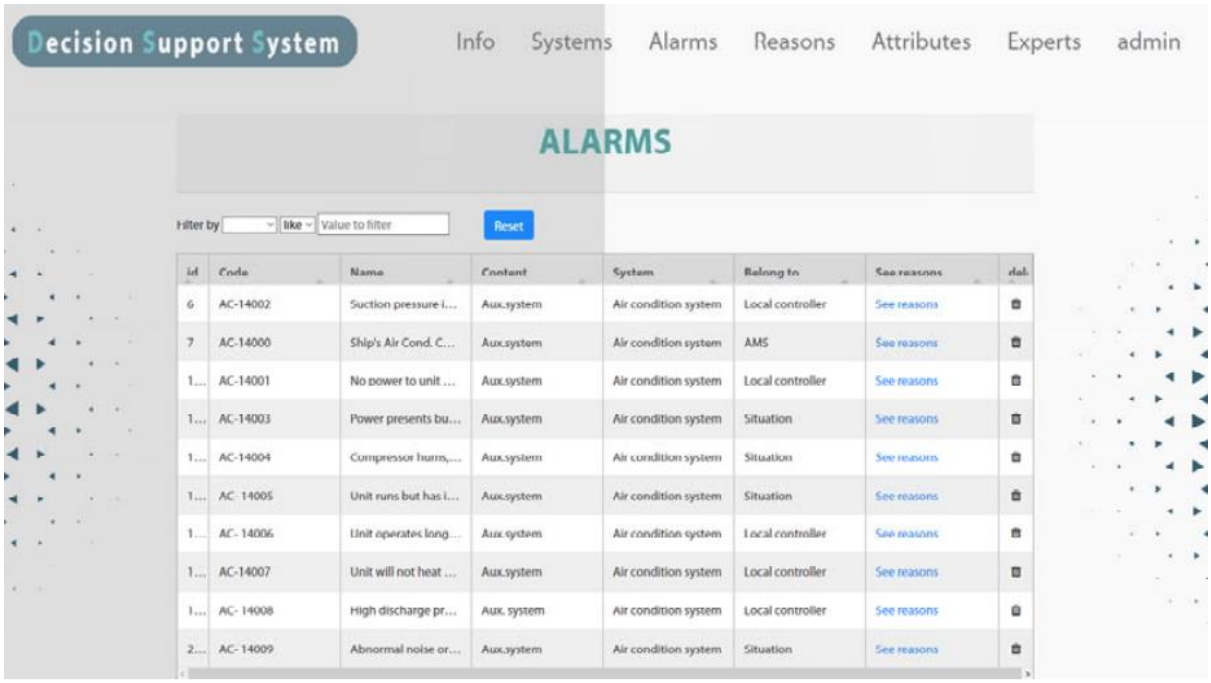


Рис. 5.3. Вікно СППР з описом всіх можливих несправностей суднової системи кондиціювання повітря

Рис. 5.4. Пошук необхідної несправності по конкретній системі

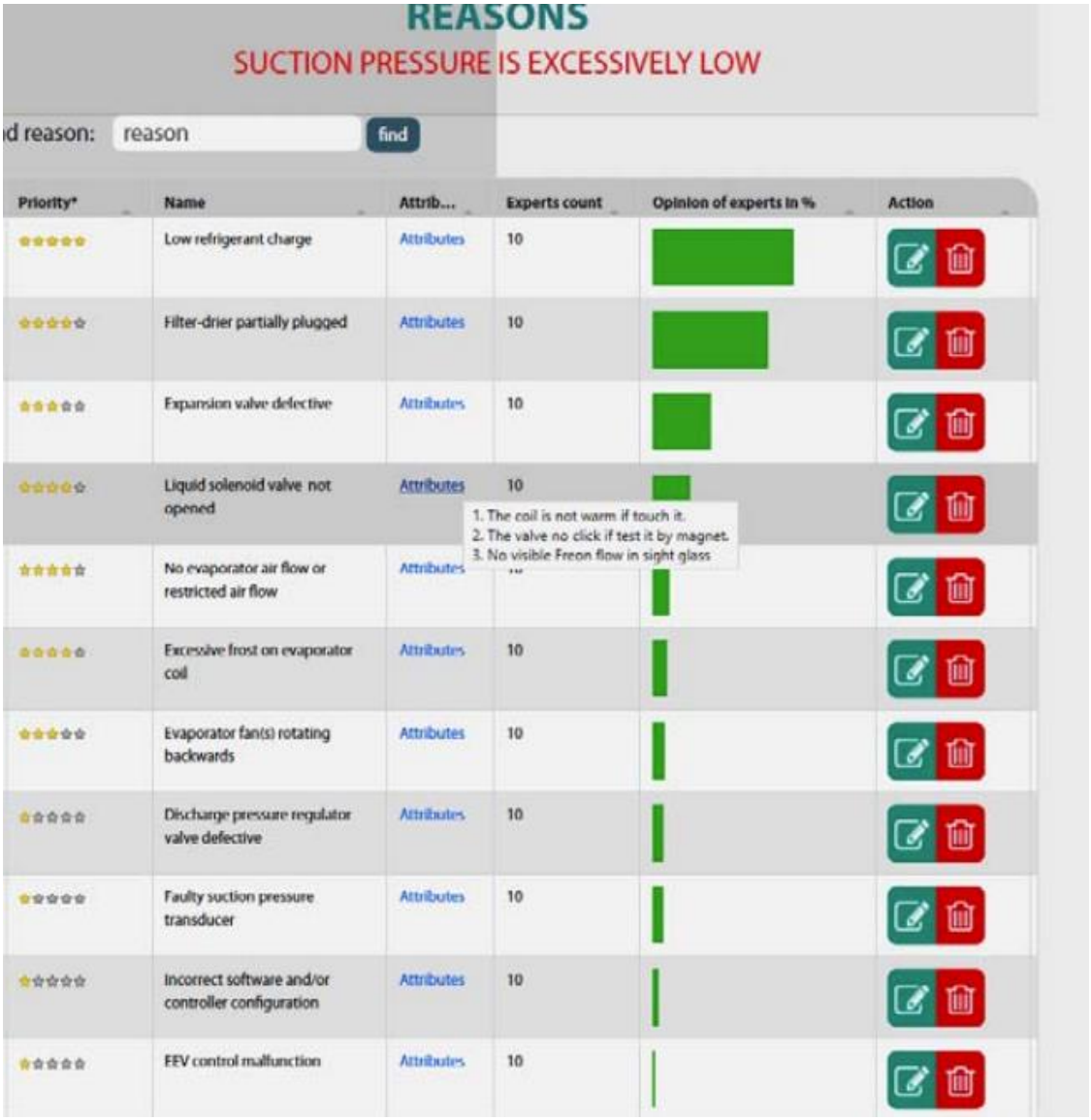


Рис. 5.5. Вікно СППР з можливими причинами конкретної несправності

ЛІТЕРАТУРА:

1. Брукінг А., Експертні системи. Принципи роботи і приклади, радіо і зв'язок. 1980.

2. Нейлор К.: Як створити власну експертну систему. Енергоатомиздат. 1991.

3. Баженов Р., Лопатін Д. Про застосування сучасних технологій у розвитку інтелектуальні системи. *Журнал наукових публікацій аспірантів і докторантів*. 2014.

4. Коваленко І., Давиденко Є. та Швед А. Формування узгоджених груп експертних свідчень на основі показників відмінності в теорії доказів. *Праці 14-ї міжнар. Конференція з комп'ютерних наук та інформаційних технологій (CSIT)*. Львів. 2019. С. 113–116. doi: 10.1109/STC-CSIT.2019.8929858

5. Швед А., Коваленко І., Давиденко Є. Метод виявлення узгоджених підгруп експертних оцінок у групі на основі мір відмінності в теорії доказів. *Досягнення інтелектуальних систем та обчислень IV. CCSIT.* Том 1080. 2019. С. 36–53. doi: 10.1007/978-3-030-33695-0_4

6. Палюх Б., Какатунова Т., Багузова О. Інтелектуальна система підтримки прийняття рішень для управління складними об'єктами за допомогою динамічних нечітких когнітивних карт, програмних продуктів і систем. *Програмні продукти та системи.* 2013.

7. Морено К., Еспехо Е. Оцінка продуктивності трьох механізмів висновку як експертних систем для ідентифікації режиму відмови у валах, аналіз інженерних відмов. 2015.

8. Ліберадо Е. Нова експертна система для визначення компенсаторів якості електроенергії. *Експертні системи. Додатки*. 2015.

9. Крайник Я., Давиденко Є. та Томаш В. Конфігурований вузол керування для бездротової сенсорної мережі. *Матеріали 3-ї міжнародної конференції з передових інформаційних та комунікаційних технологій (AICT)*. Львів. 2019. С. 258–262. doi: 10.1109/AIACT.2019.8847732

10. Афромєєв Е. Критерії технічної досконалості суден. 2005.

11. Консберг. Стандартна система сигналізації та моніторингу K-Chief 600. 2013.

12. Консберг. Керівництво по встановленню системи морської автоматизації. 2013.

REFERENCES:

1. Brooking, A. (1980). *Expert systems: Principles of work and examples*. Radio and communications.

2. Naylor, K. (1991). *How to build your own expert system*. Energoatomizdat.

3. Bazhenov, R., & Lopatin, D. (2014). On the application of modern technologies in the development of intelligent systems. *Journal of Scientific Publications of Graduate Students and Doctoral Students*.

4. Kovalenko, I., Davydenko, Y., & Shved, A. (2019). Formation of consistent groups of expert evidences based on dissimilarity measures in evidence theory. In *Proceedings of the 14th International Conference on Computer Sciences and Information Technologies (CSIT)* (pp. 113–116). Lviv. https://doi.org/10.1109/STC-CSIT.2019.8929858

5. Shved, A., Kovalenko, I., & Davydenko, Y. (2019). Method of detection of the consistent subgroups of expert assessments in a group based on measures of dissimilarity in evidence theory. In N. Shakhovska & M. Medykovskyy (Eds.), *Advances in Intelligent Systems and Computing IV* (pp. 36–53). CCSIT. https://doi.org/10.1007/978-3-030-33695-0_4

6. Palyukh, B., Kakatunova, T., & Baguzova, O. (2013). Intelligent decision support system for managing complex objects using dynamic fuzzy cognitive maps. Software Products and Systems.

7. Moreno, C., & Espejo, E. (2015). A performance evaluation of three inference engines as expert systems for failure mode identification in shafts. *Engineering Failure Analysis*.

8. Liberado, E. (2015). Novel expert system for defining power quality compensators. *Expert Systems with Applications*.

9. Krainyk, Y., Davydenko, Y., & Tomas, V. (2019). Configurable control node for wireless sensor network. In *Proceedings of the 3rd International Conference on Advanced Information and Communications Technologies (AICT)* (pp. 258–262). Lviv. https://doi.org/10.1109/AIACT.2019.8847732

10. Afromeev, E. (2005). *Criteria for the technical excellence of ships*.

11. Kongsberg. (2013a). *Standard K-Chief 600 Alarm and Monitoring System: Marine Automation System Installation Manual*.

12. Kongsberg. (2013b). *Kongsberg K-Chief 500/600 Marine Automation System Installation Manual*.

УДК 519.8: 338.4
DOI https://doi.org/10.32782/IT/2024-3-19

Тетяна ХОМ'ЯК
кандидат фізико-математичних наук, доцент, доцент кафедри системного аналізу та управління, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького 19, Дніпро, Україна, 49005
***ORCID:** 0000-0002-6177-2827*
***Scopus-Author ID:** 56997472200*

Олександр ПРУС
Студент, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького 19, Дніпро, Україна, 49005
***ORCID:** 0009-0002-6084-6617*

Бібліографічний опис статті: Хом'як, Т., Прус, О. (2024) Системний аналіз виявлення проблем системи освіти та шляхи їх вирішення. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 180–188, doi: https://doi.org/10.32782/IT/2024-3-19

СИСТЕМНИЙ АНАЛІЗ ВИЯВЛЕННЯ ПРОБЛЕМ СИСТЕМИ ОСВІТИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Одним із пріоритетних напрямків розвитку суспільства є освіта, тому що освіта – це здобуття базових навичок та знань, які будуть фундаментом для подальшого навчання та майбутньої реалізації людини.

Відомо, що якість освітнього процесу у містах та сільській місцевості в Україні значно відрізняється, що спричиняє нерівність можливостей учнів при вступі до вищих навчальних закладів.

***Метою роботи** є проведення аналізу результатів іспитів учнів, аналіз стану матеріально-технічного забезпечення в школах, аналіз віку та рівня освіти вчителів, а також визначення шляхів вирішення даної проблеми.*

З цією метою проведено аналіз результатів ЗНО минулих років та НМТ, матеріально-технічної бази шкіл, віку вчителів. Проведений аналіз підтвердив нерівність можливостей учнів шкіл за приналежністю до типу місцевості. Виявлено проблеми такої нерівності учнів та запропоновано шляхи їх вирішення.

***Ключові слова:** системний аналіз, освіта, зовнішнє незалежне оцінювання (ЗНО), національний мультитест (НМТ).*

Tetiana KHOMIAK
Candidate of Physics and Mathematics Science, Associate Professor, Associate Professor at the Department of System Analysis and Control, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, khomiak.t.v@nmu.one
***ORCID:** 0000-0002-6177-2827*
***Scopus-Author ID:** 56997472200*

Oleksandr PRUS
Student, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, prus.o.v @nmu.one
***ORCID:** 0009-0002-6084-6617*

To cite this article: Khomiak, T., Prus, O. (2024). Systemnyi analiz vyiavlennia problem systemy osvity ta shliakhy yikh vyrishennia [System analysis in identifying problems of the education system and potential ways of solving them]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 180–188, doi: https://doi.org/10.32782/IT/2024-3-19

SYSTEM ANALYSIS IN IDENTIFYING PROBLEMS OF THE EDUCATION SYSTEM AND POTENTIAL WAYS OF SOLVING THEM

One of the priority directions of the development of society is education, because education is the acquisition of basic skills and knowledge, which will be the foundation for further learning and future realization of a person.

It is known that the quality of the educational process in cities and rural areas in Ukraine is significantly different, which causes unequal opportunities for students when entering higher education institutions.

***The purpose** of the work is to analyze the results of students' exams, analyze the state of material and technical support in schools, analyze the age and level of education of teachers, as well as determine ways to solve this problem.*

For this purpose, an analysis of the results of the previous years' external independent assessments and national multitest, the material and technical base of schools, and the age of teachers was carried out. The conducted analysis confirmed the inequality of opportunities of school students according to the type of area. The problems of such inequality among students were identified and ways to solve them were proposed.

***Key words:** system analysis, education, external independent assessment, national multitest.*

Актуальність проблеми. Статтею 53 Конституції України та законом України про освіту від 05.09.2017 встановлено, що кожен має право на освіту. Повна загальна середня освіта є обов'язковою.

Держава забезпечує доступність і безоплатність дошкільної, повної загальної середньої, професійно-технічної, вищої освіти в державних і комунальних навчальних закладах; розвиток дошкільної, повної загальної середньої, позашкільної, професійно-технічної, вищої і післядипломної освіти, різних форм навчання; надання державних стипендій та пільг учням і студентам.

В Україні створюються рівні умови доступу до освіти. Ніхто не може бути обмежений у праві на здобуття освіти. Право на освіту гарантується незалежно від віку, статі, раси, стану здоров'я, інвалідності, громадянства, національності, політичних, релігійних чи інших переконань, кольору шкіри, місця проживання, мови спілкування, походження, соціального і майнового стану, наявності судимості, а також інших обставин та ознак.

Право особи на освіту може реалізовуватися шляхом її здобуття на різних рівнях освіти, у різних формах і різних видів, у тому числі шляхом здобуття дошкільної, повної загальної середньої, позашкільної, професійної (професійно-технічної), фахової передвищої, вищої освіти та освіти дорослих.

Згідно результатів міжнародного дослідження якості освіти PISA-2022, учні із сільської місцевості відстають від своїх однолітків з великих міст у читанні майже на п'ять років, у природничо-наукових дисциплінах – на чотири, а з математики – на понад чотири з половиною роки навчання.

Нерівність в системі освіти України зумовлена комплексом наступних факторів:

1. *Кадрові проблеми* (нестача педагогічних працівників, недостатня кваліфікація педагогічних кадрів);
2. *Обмеження ресурсів* (недостатнє фінансування, обмеження матеріально-технічної бази закладів освіти);
3. *Географічні фактори* (віддаленість шкіл, нерозвинена інфраструктура, недосконала система транспортного сполучення);
4. *Соціальні фактори* (соціальна сегрегація, низький рівень життя);
5. *Система освіти* (недостатня адаптованість навчальних програм для сільських шкіл);
6. *Інші фактори* (COVID-19, військовий стан в країні).

Таким чином, за визначеними потенційними проблемами, що наведені у вигляді дерева проблем (рис. 1) можна зазначити, що питання нерівності в системі освіти є актуальним і потребує аналізу основних факторів впливу.

Аналіз останніх досліджень і публікацій. Проблема якості шкільної освіти завжди була предметом наукового і практичного інтересу педагогів. Зміни суспільних пріоритетів в останнє десятиріччя окреслили нові аспекти категорії «якості освіти». Наведемо огляд останніх публікацій, які розглядають питання якості освіти в школах, аналізу та моніторингу результатів іспитів із ЗНО та НМТ.

Так, державна служба якості освіти презентувала результати дослідження про якість освіти у сільських школах. Учасникам фокус-груп було непросто порівняти якість освіти у міських школах та сільських школах. Думки респондентів щодо того, як відрізняється якість освіти у міських школах, розділилися, але все-таки є тенденція, що краще оцінюється якість у міських школах. 33% респондентів вважають, що у міських школах якість освіти краща проти 11%, які вважають, що якість освіти гірша. Ще 36%

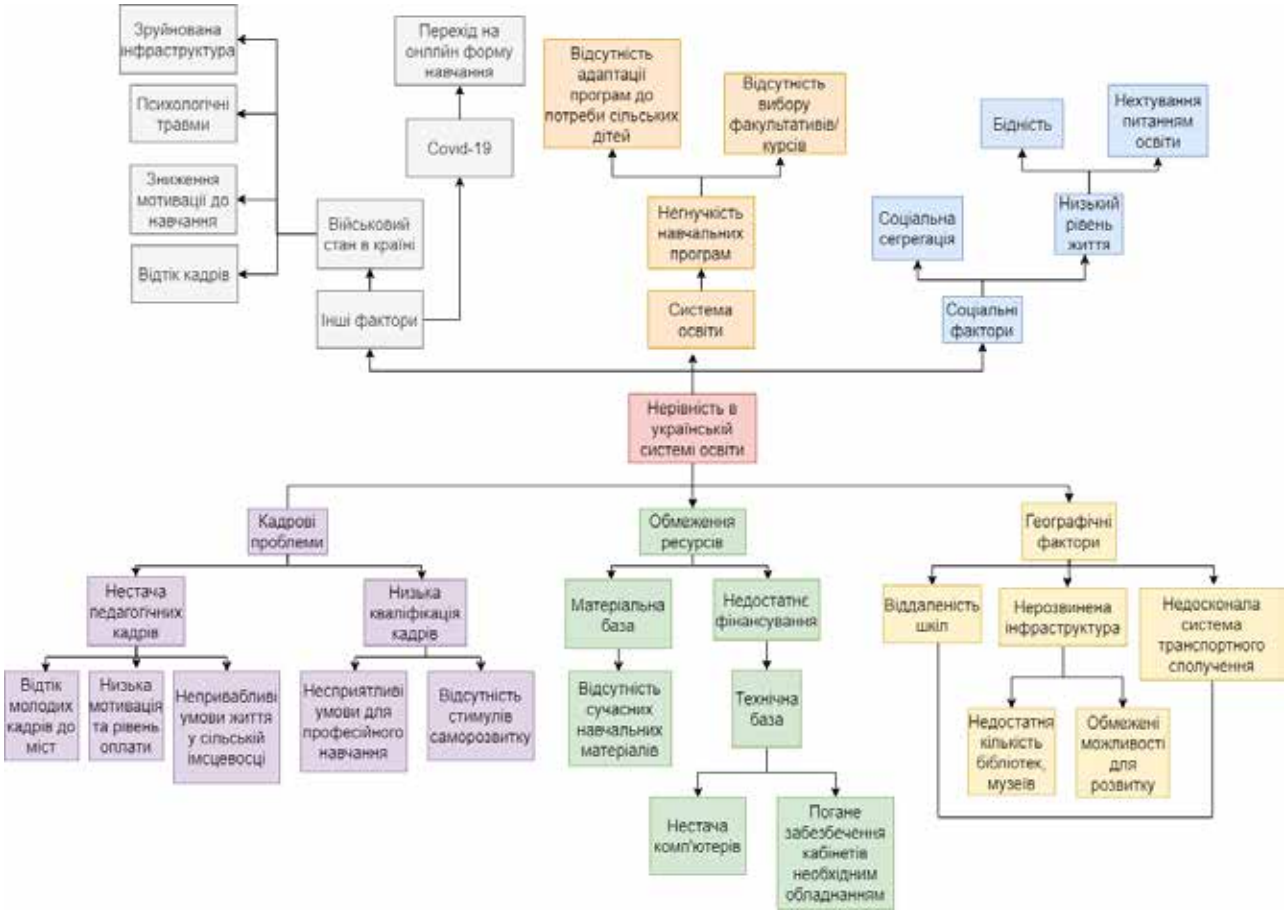


Рис. 1. Дерево проблем української системи освіти

вважають, що якість не відрізняється, а 21% не змогли відповісти на запитання. При цьому, серед респондентів з сіл та СМТ оцінки близькі: про те, що у міських школах якість освіти краща говорять, 35% респондентів у селах і 30% респондентів у СМТ. Про те, що якість освіти не відрізняється, говорять, відповідно, 39% і 32%, а про те, що якість освіти у міських школах гірше – 10% і 12%. Також зазначається, що здобування якісної освіти, на думку більшості учасників, залежить не лише від школи. Учасники дослідження вважають, що як в селі, так і в місті можна навчатися і за допомогою самоосвіти, ресурсів мережі інтернет. Водночас, підтримка, яку діти можуть отримати в закладі освіти від вчителів та інших учнів є цінною перевагою саме шкільного навчання. Продовження освіти і отримання якісної освіти діти все-таки у своїй більшості пов'язують із навчальними закладами у містах – це коледжі, університети, яких немає у сільських населених пунктах. Якість життя і самореалізація прямо чи опосередковано асоціюється в учнів саме з життям у місті. Так, респонденти, які вже визначилися із здобуттям подальшої освіти, пов'язують своє майбутнє із переїздом у міста або навіть за кордон.

Міністерство освіти і науки спільно з Державною службою якості освіти розробили методичні рекомендації з питань формування внутрішньої системи забезпечення якості освіти у закладах загальної середньої освіти. Рекомендації оприлюднено на сайті МОН (30 листопада 2020 року).

Методичні рекомендації орієнтовані на допомогу школам у внутрішньому забезпеченні якісної освіти. Згідно з документом, система забезпечення якісної освіти у школі повинна мати не лише зовнішні стимули (ЗНО, інституційний аудит, атестація та сертифікація педагогічних працівників тощо), а й внутрішні інструменти.

Розробці оптимальних методик та інноваційних підходів до організації дистанційного навчання школярів із врахуванням специфіки умов воєнного стану присвячено дослідження науковців (Червінська, 2024). Зазначене дозволило увиразнити проблему організації дистанційного навчання здобувачів шкільної освіти, розкрити її цілісно, виокремити практико зорієнтовані аспекти, визначити проблеми та схарактеризувати перспективи подальшого розвитку. За результатами проведеного дослідження запропоновано шляхи, вирішення цих проблем.

Особливості застосування маркетингового підходу в управлінні якістю шкільної освіти розглянуто в роботі Тимошко (Тимошко, 2024). Авторка наголошує на необхідності впровадження маркетингових стратегій у діяльність закладів загальної середньої освіти з метою підвищення їхньої ефективності в умовах ринкових відносин. Визначено основні функції маркетингу в освітньому процесі, які спрямовані на задоволення потреб споживачів освітніх послуг і створення позитивного іміджу навчального закладу. Особливу увагу приділено питанням якості освітніх послуг і ролі керівника.

Отже, виникає нагальна потреба в проведенні дослідження стану системи освіти в школах, яке буде ґрунтуватися на використанні доцільних математичних інструментів, для визначення причин нерівності учнів за типом місцевості при здачі ЗНО та НМТ.

Мета дослідження: проведення аналізу сучасного стану системи освіти в Україні, виявлення причин нерівності та визначення шляхів їх вирішення.

Виклад основного матеріалу дослідження. Для проведення дослідження в якості початкових даних взяті статистичні дані за результатами іспитів із ЗНО та НМТ відкритих джерел (zno.testportal.com.ua/opendata).

На рисунку 2 представлено результати здачі ЗНО учнів шкіл з різних дисциплін за типом місцевості. Це один із показників, який демонструє, з однієї сторони, наскільки добре викладався матеріал учням, а з іншої сторони – на скільки добре кожен учень зміг викладений матеріал засвоїти. Наведена діаграма свідчить про те, що існує значна нерівність у результатах іспитів між учнями з міст та сіл. А саме, учні сільських шкіл зазвичай мають нижчі результати із складання розглянутих предметів, що у подальшому, призводить до меншого відсотку вступу до ВНЗ.

На рисунку 3 наведено порівняльний аналіз результатів ЗНО та НМТ у різні часові проміжки, що дозволяє виявити залежність між результатами іспитів та місцем навчання.

Тож, у 2021 році спостерігається значне зниження відсотка тих, хто подолав поріг з математики та історії України як у сільській місцевості, так і в містах, порівняно з 2019 роком (рис. 3). Причиною цього могло бути те, що вчителі не мали відповідних знань та навичок для здійснення дистанційного навчання. Через те, навчання частково зводилося до самостійного опрацювання нового матеріалу. Під час дистанційного навчання зросло навантаження на учнів, особливо в частині виконання домашнього завдання. Водночас учні його не завжди виконували, а вчителі – не завжди перевіряли, що створило видимість навчального процесу та знецінило його суть.

На рисунку 4 представлено середній бал учнів (хто подолав поріг) за різними дисциплінами (математика, історія України, англійська мова,

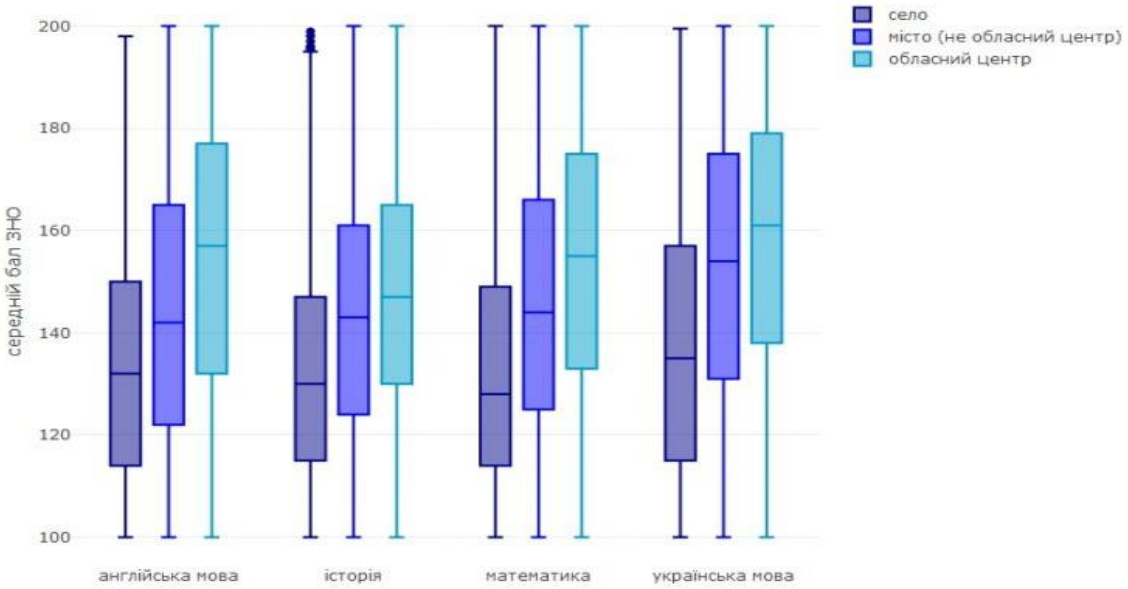
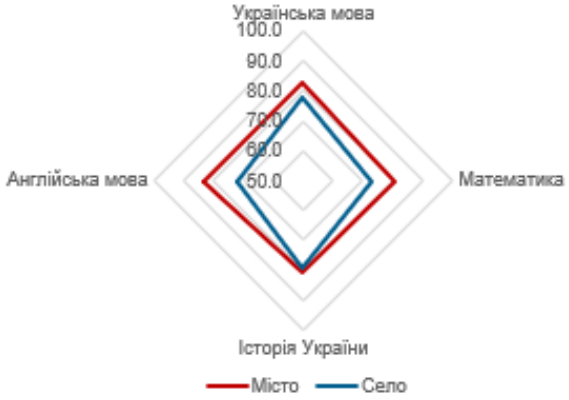
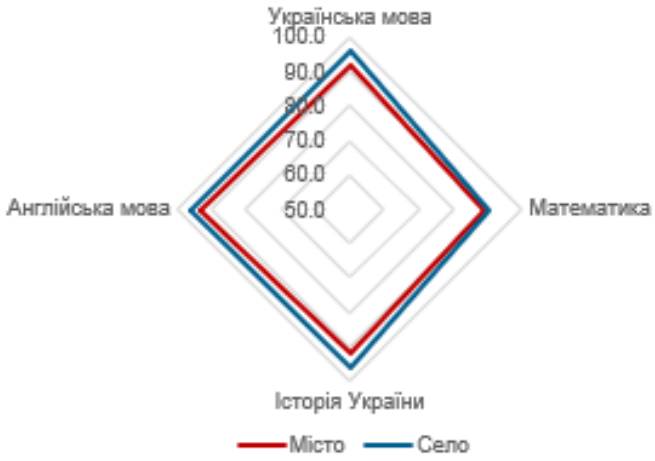


Рис. 2. Середній бал за результатами ЗНО випускників шкіл 2019 року у розрізі навчальних дисциплін за типом населеного пункту



а) результати ЗНО 2019 року

б) результати ЗНО 2021 року



в) результати НМТ 2023 року

Рис. 3. Відсоток учнів, які подолали поріг з різних навчальних дисциплін за типом населеного пункту

Отже, середній бал, за результатами розглянутих іспитів, у учнів із сільської місцевості нижчий за учнів із міст за всіма розглянутими предметами, незалежно від року та формату складання іспиту.

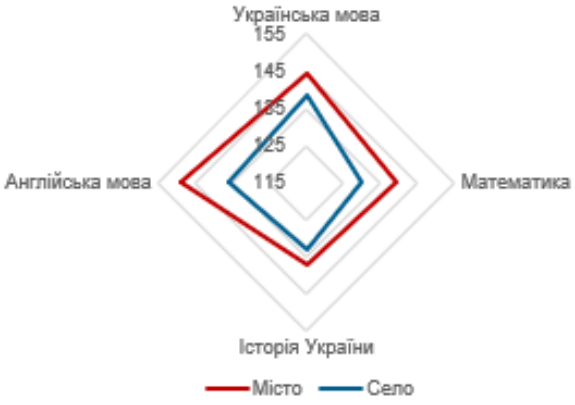
Важливо, що кожна людина індивідуальна та витрачає різну кількість своїх внутрішніх ресурсів на опанування матеріалу. Одному учню для опанування теми потрібен один урок, а іншому потрібні додаткові заняття. Виходячи із цього, результатів аналізу даного аспекту недостатньо для об'єктивної оцінки причин нерівності між учнями із сіл та міст. Хоча продемонстровані результати (рис. 3, рис. 4) свідчать про те, що залежність від типа місцевості існує. Але потребують детального аналізу інші потенційні фактори впливу.

Матеріально-технічне забезпечення шкіл відіграє важливу роль у формуванні освітнього процесу. За даними, наведеними на рисунку 5, відсоток шкіл, які не забезпечені належним обладнанням для проведення відповідних занять, у сільській місцевості вище, між у містах, що також негативно впливає на результат освітнього процесу.

Для прикладу, відсутність доступу до інтернету, чи неукомплектовані кабінети хімії необхідним обладнанням для навчального процесу, негативно впливають на успішність учнів.

Ключову роль у процесі передачі знань учням відіграють вчителі. Для ретельного аналізу проблеми, враховано також вік вчителів, адже молодші педагоги, як правило, мають більш актуальні знання.

а) результати ЗНО 2019 року



б) результати ЗНО 2021 року

в) результати НМТ 2023 року

Рис. 4. Середні бали учнів у розрізі навчальних дисциплін за типом населеного пункту

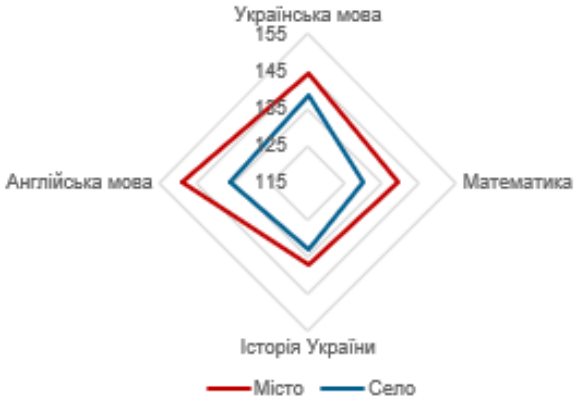
Наведена діаграма на рисунку 6 свідчить, що у віковій категорії до 30 років кількість вчителів у селах вища на 5%, ніж у селищах міського типу та містах. Цей факт має як позитивні сторони (вмотивованість педагога, наявність у нього свіжих підходів до навчання), так і негативні (відсутність досвіду роботи, нестабільність вчителя). Також, даний результат може бути обумовлений меншою конкретністю у сільській місцевості, та більшим шансом знайти першу роботу.

Не лише вік впливає на якість викладання вчителів, а й їх рівень освіти. Так, на рисунку 7 продемонстровано, що відсоток вчителів із середньої освітою та освітньо-кваліфікаційним рівнем молодшого спеціаліста у сільській місцевості більший, ніж у містах. Водночас, у містах вище відсоток вчителів із ступенем магістра. Тож, нестача вчителів з вищою освітою в сільській місцевості може негативно впливати на якість освіти.

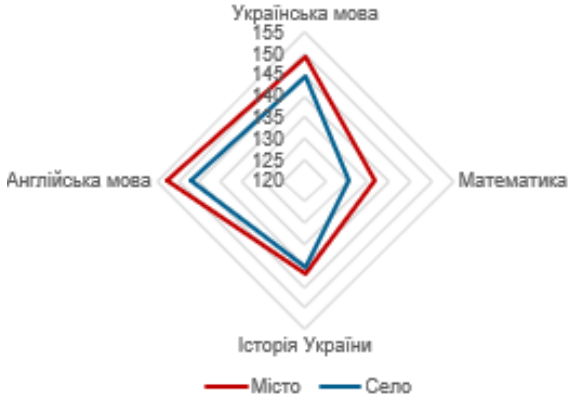
Провівши детальний аналіз, можна зробити висновок, що нерівність між міськими та сільськими учнями справді існує, та виділити наступні проблеми, а також запропонувати шляхи їх подолання (рис. 8).

Подальші дослідження можуть бути зосереджені на розробці моделі і бізнес-плану з відкриття приватної школи або додаткових підготовчих курсів з основних дисциплін для дітей із сільської місцевості. Також необхідним є розробка експертної системи для проведення тестування учнів з виявлення здібностей до майбутньої спеціальності. При цьому треба враховувати умови сьогодення, на основі яких відбувається формування ринку освітніх послуг.

а) результати ЗНО 2019 року



б) результати ЗНО 2021 року



в) результати НМТ 2023 року

Рис. 5. Відсоток шкіл за типом місцевості, який не забезпечений відповідним обладнанням

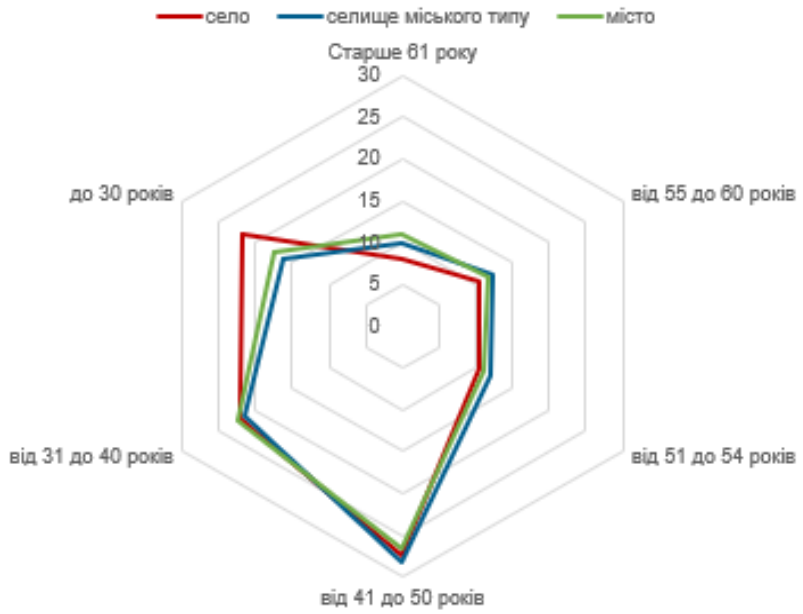


Рис. 6. Відсоток вчителів за віком та типом місцевості

Рис. 7. Розподіл вчителів за рівнем освіти

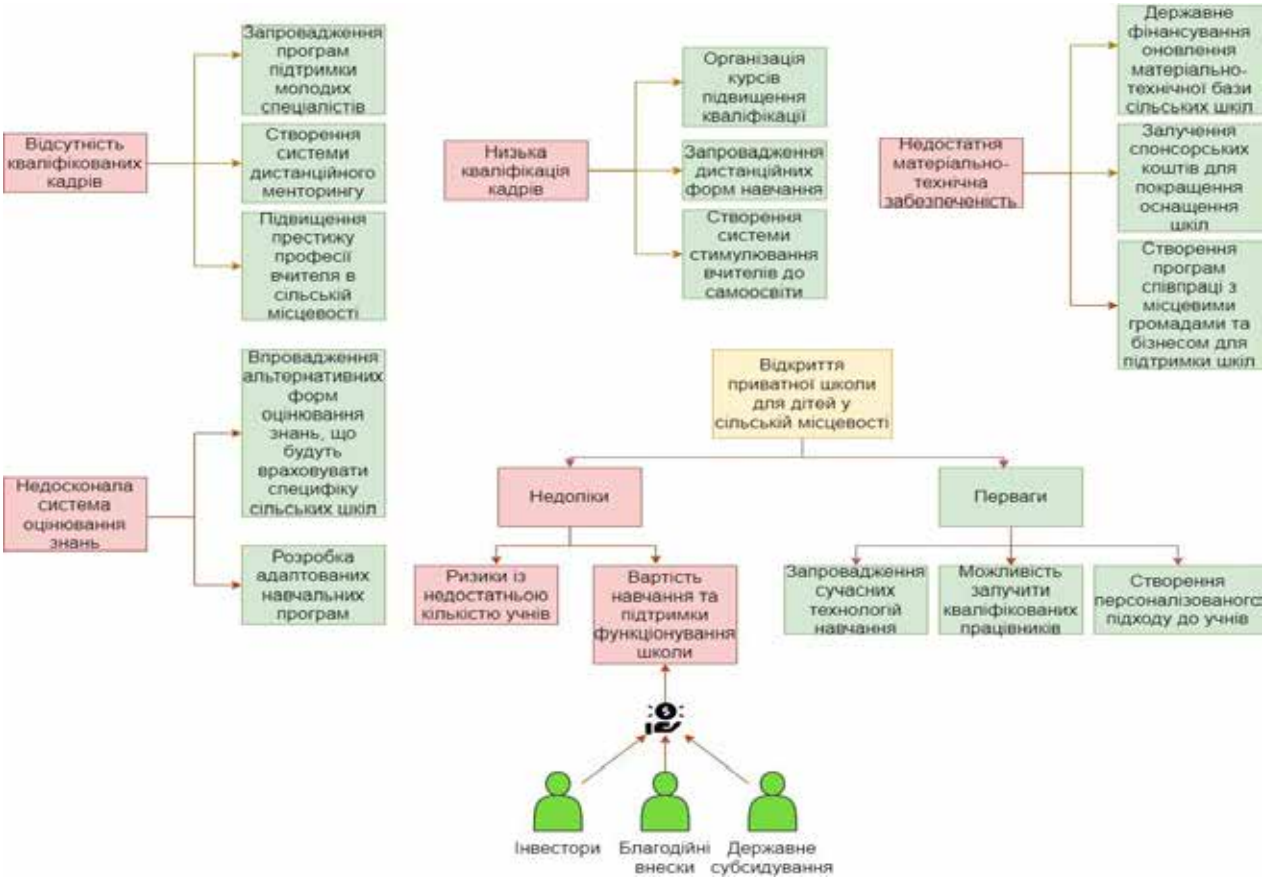


Рис. 8. Графічне зображення проблем закладів середньої освіти та шляхів їх вирішення

ЛІТЕРАТУРА:

1. Закон України про освіту: офіц. текст № 2145-VIII від 05 вересня 2017 р.: URL: https://zakon.rada.gov.ua/laws/show/1206-20#Text (дата звернення: 21.01.2024).

2. Конституція України. – URL: https://zakon.rada.gov.ua/laws/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 20.12.2023).

3. Внутрішня система забезпечення якості освіти у школах – розроблено методрекомендації від Міністерства освіти і науки України URL: https://mon.gov.ua/news/vnutrishnya-sistema-zabezpechennya-yakosti-osviti-u-shkolakh-rozrobleno-metodrekomendatsii (дата звернення: 23.12.2023). – Назва з екрану.

4. Державна служба якості освіти України URL: https://sqe.gov.ua/yakist-osvity-silski-shkoly-2021/ (дата звернення: 10.01.2024).

5. Національний звіт за результатами міжнародного дослідження якості освіти PISA-2022 / кол. авт.: Г. Бичко (осн. автор), Т. Вакуленко, Т. Лісова, М. Мазорчук, В. Терещенко, С. Раков, В. Горох та ін.; за ред. В. Терещенка та І. Клименко; Український центр оцінювання якості освіти. Київ, 2023. 395 с.

6. Статистичні дані із результатами іспитів ЗНО та НМТ. URL: https://zno.testportal.com.ua/opendata (дата звернення: 19.12.2023).

7. Червінська І., Червінський А., Никорак Я. Дистанційне навчання здобувачів шкільної освіти в умовах воєнного стану: реалії та перспективи розвитку. *Вісник Національного університету «Чернігівський колегіум» імені Т. Г. Шевченка*, *Серія: Педагогічні науки*. 2024. № 26(182). С. 145–150. DOI: 10.58407/visnik.242626

8. Тимошко Г. Особливості реалізації маркетингового підходу у процесі підвищення якості шкільної освіти. Збірник праць XIX Міжнародної наукової конференції «Сучасні досягнення в науці та освіті», 2024 р. Хмельницький: ХНУ. С. 17–24.

REFERENCES:

1. Zakon Ukrainy pro osvitu: ofits. tekst № 2145-VIII vid 05 veresnia 2017 p. [Law of Ukraine on education: officer. text No. 2145-VIII of September 5, 2017]: Retrieved from: https://zakon.rada.gov.ua/laws/show/1206-20#Text (date of application: 21.01.2024).

2. Konstytucia Ukrainy [Constitution of Ukraine]. – Retrieved from: https://zakon.rada.gov.ua/laws/254%D0%BA/96-%D0%B2%D1%80#Text (date of application: 20.12.2023).

3. Vnutrishnia systema zabezpechennua yakosti osvity y shkolah – rozrobleno metodrekomendacii vid Ministerstva osvity i nauki Ukrainy [The internal system of ensuring the quality of education in schools – method recommendations from the Ministry of Education and Science of Ukraine have been developed] Retrieved from: https://mon.gov.ua/news/vnutrishnya-sistema-zabezpechennya-yakosti-osviti-u-shkolakh-rozrobleno-metodrekomendatsii (date of application: 23.12.2023). – Name from the screen [in Ukrainian].

4. Dergavna slujba yakosti osvity Ukrainy [State Education Quality Service of Ukraine] Retrieved from: https://sqe.gov.ua/yakist-osvity-silski-shkoly-2021/ (date of application: 10.01.2024).

5. Nacionalnyi zvit za rezyltatamy mignarodnogo doslidgennya yakosti osvity PISA-2022 [National report on the results of the international study of the quality of education PISA-2022]. H. Bychko, T. Vakylenko, T. Lisova, M. Mazorchuk, V. Tereshchenko, S. Rakov, V. Goroh; V. Tereshchenko and I. Klimenko; Ukrainskiy centr ocinuvannia yakosti osvity. Kyiv, 2023. 395 p. [in Ukrainian].

6. Statystychni dani iz rezultatamy ispytiv ZNO ta NMT [Statistical data with the results of ZNO and NMT exams]. Retrieved from: https://zno.testportal.com.ua/opendata (date of application: 19.12.2023) [in Ukrainian].

7. Chervinska, I., Chervinskiy, A., Nikopak, Ya. (2024). Dystanciyne navchannia zdobyvachiv shkilnoi osvity v ymovah voennogo stanu: realii ta perspektyvy rozvutky [Distance learning of students of school education in the conditions of martial law: realities and prospects for development]. *Visnyk Nacionalnogo yniversytety «Chernigivskiy kolegium» imeni T. Shevchenka, Seria: Pedagogichni nauki.* № 26(182). P. 145–150. [in Ukrainian]. DOI: 10.58407/visnik.242626

8. Tymoshko, G. (2024). Osoblyvosti realizacii marketingovogo pidhody u processi pivyshennia yakosti shkilnoi osvity [Peculiarities of implementation of the marketing approach in the process of improving the quality of school education]. Collection of works XIX International scientific conference «Modern achievements in science and education», Khmelnickiy: KhNU. P. 17–24. [in Ukrainian].

ЗМІСТ

CONTENTS

НОТАТКИ

INFORMATION TECHNOLOGY: COMPUTER SCIENCE, SOFTWARE ENGINEERING AND CYBER SECURITY

Випуск 3

Коректура • Ірина Миколаївна Чудеснова

Комп'ютерна верстка • Андрій Олександрович Філатов

Підписано до друку: 29.11.2024. Формат 60x84/8. Гарнітура Arial.
Папір офсет. Цифровий друк. Ум. друк. арк. 22,55. Замов. № 1124/808. Наклад 300 прим.

Видавництво і друкарня – Видавничий дім «Гельветика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефон +38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@helvetica.ua
Свідоцтво суб'єкта видавничої справи
ДК № 7623 від 22.06.2022 р.