МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

ISSN 2522-1957

ВІСНИК

НАВЧАЛЬНО-НАУКОВОГО ІНСТИТУТУ КІБЕРНЕТИКИ, ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ІНЖЕНЕРІЇ

Збірник наукових праць

Випуск 2(13)

Рівне-2025

У збірнику опубліковано наукові статті студентів і викладачів Навчально-наукового інституту кібернетики, інформаційних технологій та інженерії НУВГП.

Вісник навчально-наукового інституту кібернетики, інформаційних технологій та інженерії. Вип. 2(13). – Рівне : НУВГП, 2025. – 138 с.

Матеріали збірника розглянуті і рекомендовані до видання на Вченій раді Національного університету водного господарства та природокористування 18.12.2025 р., протокол № 13
Ідентифікатор медіа: R30-05350

Адреса редколегії: 33028, м. Рівне, вул. Соборна, 11, НУВГП.

ЗМІСТ

CONTENT

УДК 004.42

[1]Ostapchuk O. P., Candidate of Engineering (Ph.D.), Associate Professor; [2]Samoidiuk A. S., Post-graduate Student (National University of Water and Environmental Engineering, Rivne, [1]o.p.ostapchuk@nuwm.edu.ua, [2] a.s.samoidiuk@nuwm.edu.ua)

MICROSERVICE ARCHITECTURE: ADVANTAGES, DISADVANTAGES AND IMPLEMENTATION EXAMPLES

This article provides an in-depth analysis of microservice architecture, highlighting its conceptual foundations, key principles, and distinctions from monolithic and service-oriented architectures (SOA). The study examines the main advantages of adopting microservices, such as scalability, fault tolerance, independent deployment, and technology diversity, as well as the potential challenges including increased complexity in system management, distributed transactions, and the need for advanced monitoring.

A practical case study is presented, simulating the migration of a Customer Relationship Management (CRM) system from a monolithic to a microservice-based architecture. The migration plan focuses on decomposing the system into independent services (user management, orders, payments, reporting) while implementing DevOps practices, CI/CD pipelines, and modern monitoring solutions. The results of the simulation show that microservice adoption can significantly reduce deployment time, increase system resilience, improve scalability, and facilitate testing.

Keywords: **microservices, scalability, containerization, Kubernetes, API Gateway, DevOps, distributed systems.**

Introduction. The growing complexity of modern IT systems and the demand for rapid, reliable delivery of software have highlighted the limitations of traditional monolithic architectures. In a monolith, all components are tightly coupled, making scaling, updating, and introducing new technologies more difficult as the system grows.

Microservice architecture (fig. 1) addresses these challenges by decomposing applications into small, independent services, each responsible for a specific business function. This allows for independent deployment, easier scalability, and fault isolation. Communication between services typically relies on lightweight protocols such as REST or gRPC, enabling technology diversity and flexible development workflows. Industry leaders such as Netflix, Amazon, and Spotify have demonstrated the effectiveness of microservices in handling millions of daily requests, reducing deployment times, and maintaining high availability under heavy loads.

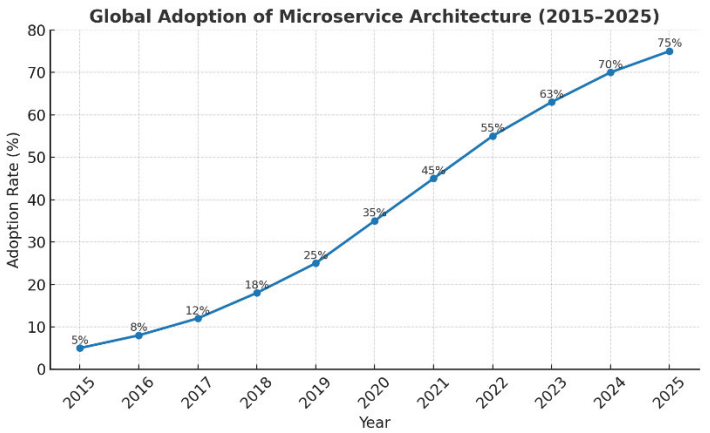

Fig. 1. Global adoption of microservice architecture (2015–2025)

However, microservices also introduce new challenges, including distributed transaction management, more complex monitoring, and the need for advanced DevOps practices. This paper analyzes the principles, benefits, and limitations of microservice architecture, explores supporting technologies, and presents a simulated migration case study from a monolithic to a microservice system.

Overview of microservice architecture. In the early stages of software development, most applications were built as monoliths – single deployable units that contained all business logic, data access layers, and user interface components in one codebase [1]. While monoliths are simpler to design and deploy in the early stages, they present challenges as applications grow:

- long deployment cycles due to the need to redeploy the entire application for every update;
- tight coupling between modules, making it harder to introduce changes without affecting other components;
- imited scalability, as scaling requires deploying the entire system rather than specific bottlenecks.

The introduction of Service-Oriented Architecture (SOA) in the 2000s addressed some of these issues by organizing software as a set of services that communicated over enterprise messaging systems. However, SOA implementations often relied on heavyweight protocols (e.g., SOAP) and centralized governance, which slowed down development. Microservice architecture builds on SOA principles but applies them in a lighter, more agile form. Services are smaller in scope, decentralized in governance, and designed for independent deployment.

Key characteristics of microservices:

- independence – services can be developed, deployed, and scaled independently, allowing faster release cycles;
- loose coupling – minimal dependencies reduce the risk of cascading failures and simplify service replacement.

- technology diversity – teams can choose the most suitable technology stack for each service (polyglot architecture);
- decentralized data management – each service may own its database, improving performance and scalability;
- resilience and fault isolation – failures in one service do not necessarily affect others;
- continuous delivery – independent deployment pipelines enable frequent updates with reduced risk.

Table 1

Comparison of monolithic and microservice architectures

Criteria	Monolithic Architecture	Microservice Architecture
Technology stack	Single technology stack for the entire application	Polyglot approach – each service can use the most suitable technology for its purpose
Scalability	Vertical scaling	Horizontal scaling per service
Deployment model	Single deployable unit	Multiple deployable units
Maintenance	Simple at small scale but becomes complex and rigid as the system grows.	Higher operational complexity but more flexible maintenance due to modular structure
Best use case	Small to medium-sized applications with stable requirements	Large, evolving, high-traffic applications requiring rapid scaling and frequent updates

Supporting technologies and tools. The adoption of microservice architecture relies on a mature technological ecosystem that enables efficient deployment, communication, orchestration, and monitoring of distributed services. At the core of this ecosystem is containerization, with platforms such as Docker and Podman packaging applications and their dependencies into portable, lightweight containers. This approach ensures consistency across development, testing, and production environments, allowing each microservice to run in isolation while maintaining predictable behavior regardless of the hosting environment.

Managing containers at scale requires orchestration platforms like Kubernetes or OpenShift. These systems automate the deployment, scaling, load balancing, and self-healing of containerized services. They also enable rolling updates and seamless failover, which are crucial for maintaining high availability in production environments with dozens or hundreds of microservices.

For communication between services, microservice architectures employ both synchronous and asynchronous approaches. Synchronous interactions often

use REST for its simplicity and compatibility or gRPC [2] for its high performance and compact binary data format. Asynchronous communication is typically implemented through message brokers such as RabbitMQ or Apache Kafka, which support event-driven patterns, improve system decoupling, and enhance resilience against network or service outages.

To handle incoming requests from clients, API gateways like Kong, NGINX, or Traefik serve as a single entry point to the microservice ecosystem. They manage routing, authentication, rate limiting, and request transformation while hiding the internal service structure from external consumers. This improves both security and maintainability.

Another important component is the service mesh, exemplified by Istio and Linkerd. Service meshes manage secure service-to-service communication, adding features such as mutual TLS encryption, traffic control, and observability without requiring modifications to the application code. By separating communication logic from business logic, they reduce development complexity and standardize operational practices.

And the distributed nature of microservices demands robust monitoring and logging solutions. Tools like Prometheus and Grafana collect and visualize real-time performance metrics, while the ELK Stack (Elasticsearch, Logstash, Kibana) centralizes and analyzes logs from multiple services. Together, they provide the visibility needed to detect performance bottlenecks, identify failures, and maintain system health at scale (fig. 2).

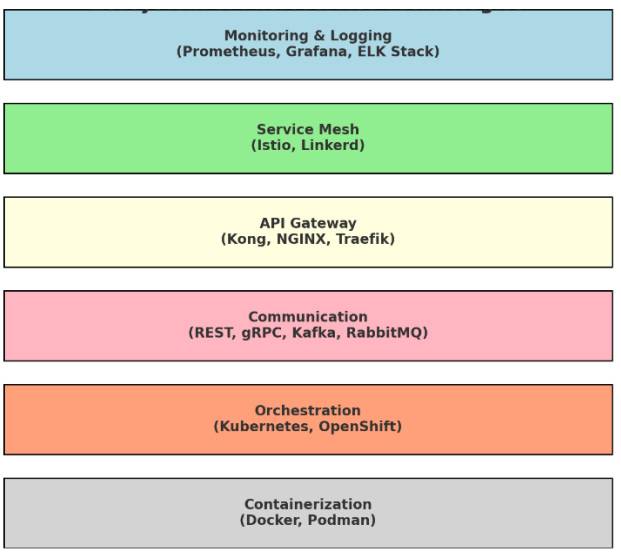

Fig. 2. Ecosystem of microservice technologies

Implementation examples and use cases. Microservice architecture has been adopted across a wide range of industries, often becoming a key factor in

achieving scalability, resilience, and faster time-to-market. One of the most cited success stories is Netflix, which transitioned from a monolithic architecture to microservices to handle its massive global streaming demand. This change enabled Netflix to scale individual components such as content recommendation, streaming servers, and user interfaces independently, ensuring uninterrupted service even during peak usage. Similarly, Amazon adopted microservices to optimize its e-commerce platform, allowing different teams to manage product catalogs, payment processing, and customer reviews without interfering with each other's workflows (fig. 3).

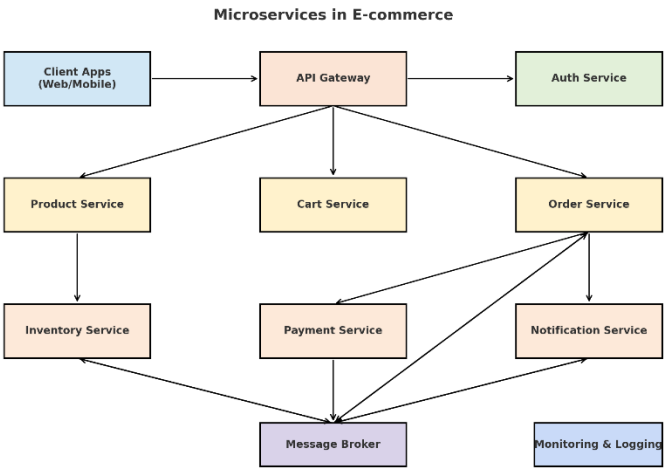

Fig. 3. Microservices in E-commerce

In the financial sector, microservices have become essential for processing millions of transactions in real time. Banks and fintech companies often split their systems into specialized services – such as fraud detection, payment gateways, and account management – each of which can be scaled independently based on demand. This modularity improves fault isolation: if one service fails, others can continue operating, minimizing customer impact [3].

The Internet of Things (IoT) domain also benefits significantly from microservices. IoT ecosystems often involve thousands of devices sending data to a central system. By separating data ingestion, processing, analytics, and visualization into independent services, organizations can scale each component according to its specific workload. For example, a high-frequency data ingestion service can be scaled without affecting the analytics module, optimizing both performance and cost.

Another common use case is in e-commerce and retail, where businesses must respond quickly to seasonal demand spikes. Microservices allow for rapid deployment of new marketing features, targeted recommendations, and dynamic pricing without risking downtime for the entire platform.

In all these cases, the advantages of microservices – independent scalability, fault isolation, and technology diversity – have enabled organizations to innovate faster while maintaining system stability. However, the transition from monolithic systems requires careful planning, as the benefits are most evident when supported by robust infrastructure, effective DevOps practices, and strong governance models.

Implementation challenges and solutions. While microservice architecture offers numerous advantages, its implementation introduces a new set of technical and organizational challenges. Addressing these effectively is essential to ensure that the benefits of microservices outweigh the added complexity.

One of the most significant challenges is managing distributed transactions. In a monolithic system, operations that span multiple modules can often be handled within a single database transaction. In microservices, where each service may have its own database, achieving strong consistency is more complex. Common solutions include the Saga pattern, which coordinates transactions as a series of local steps with compensating actions, and Event Sourcing, where state changes are stored as a sequence of events that can be replayed to rebuild system state.

Another issue is monitoring and observability. In a distributed system, a single user request may traverse multiple services, making it harder to identify performance bottlenecks or the root cause of failures. Implementing centralized logging (e.g., ELK Stack) and distributed tracing tools (e.g., Jaeger, Zipkin) helps track requests end-to-end. Metrics collection with Prometheus, combined with visualization in Grafana, provides real-time insights into service health and performance.

Configuration management also becomes more complex, as each service may have multiple environment-specific settings. Storing and managing these securely is critical. Tools like HashiCorp Vault and Consul offer secure storage and dynamic configuration updates without redeployment. The operational complexity of microservices requires robust CI/CD pipelines to automate build, test, and deployment processes. Platforms such as GitLab CI, Jenkins, or GitHub Actions [4] enable teams to integrate automated testing, vulnerability scanning, and rolling deployments, reducing human error and accelerating delivery.

Lastly, organizational challenges should not be overlooked. Teams must adopt a DevOps mindset, with closer collaboration between developers, operations, and QA engineers. Clear service ownership, well-defined API contracts, and strong governance policies are essential to prevent "microservice sprawl" and maintain system coherence over time.

Table 2

Common challenges and recommended solutions in microservice implementation

Challenge	Description	Solution
Distributed transactions	Operations spanning multiple services with separate databases are difficult to coordinate	Saga pattern, Event Sourcing, eventual consistency
Monitoring and observability	Hard to trace requests across multiple services and detect bottlenecks	Centralized logging (ELK Stack), distributed tracing (Jaeger, Zipkin), Prometheus + Grafana
Deployment complexity	Frequent deployments across many services can lead to errors and inconsistencies	Automated CI/CD pipelines (GitLab CI, Jenkins, GitHub Actions), rolling updates
Service-to-service communication	Network latency, failures, and security issues between services	Use service mesh (Istio, Linkerd), mTLS encryption, retry and circuit breaker patterns

Conclusion. Microservice architecture has established itself as a powerful alternative to traditional monolithic design, enabling organizations to achieve higher scalability, resilience, and flexibility in software development. By decomposing complex systems into independent, loosely coupled services, businesses can scale individual components, accelerate feature delivery, and reduce the risk of full-system outages.

The analysis presented in this paper demonstrates that successful microservice adoption requires more than just a change in architecture – it demands a robust technological foundation, well-defined governance, and a mature DevOps culture. The case study of migrating a CRM system from a monolithic to a microservice-based design highlighted measurable improvements in deployment speed, scalability, and operational stability. At the same time, it revealed the importance of addressing challenges such as distributed transaction management, observability, and configuration security.

In conclusion, microservice architecture is best suited for large, evolving applications with diverse and rapidly changing requirements. For smaller or less dynamic systems, the operational overhead may outweigh the benefits. Organizations considering this transition should begin with careful domain decomposition, invest in container orchestration and observability tools, and establish clear ownership of services. By combining technical best practices with strategic planning, businesses can fully leverage the advantages of microservices while minimizing their inherent complexities.

1. Newman S. Building Microservices: Designing Fine-Grained Systems 2nd edition. Sebastopol : O'Reilly Media, 2021. P. 365.
2. Burns B., Beda J., Hightower K. Kubernetes: Up and Running 3rd edition. Sebastopol : O'Reilly Media, 2023. P. 350.
3. Richardson C. Microservices Patterns: With Examples in Java. Shelter Island : Manning Publications. 2018, P. 520.
4. Beyer B., Jones C., Petoff J., Murphy N.R. Site Reliability Engineering: Measuring and Managing Reliability. Sebastopol : O'Reilly Media, 2020. P. 550.

Остапчук О. П., к.т.н., доцент; Самойдюк А. С., аспірант (Національний університет водного господарства та природокористування, м. Рівне)

МІКРОСЕРВІСНА АРХІТЕКТУРА: ПЕРЕВАГИ, НЕДОЛІКИ ТА ПРИКЛАДИ РЕАЛІЗАЦІЇ

У цій статті наведено поглиблений аналіз мікросервісної архітектури, висвітлюються її концептуальні основи, ключові принципи та відмінності від монолітних та сервісно-орієнтованих архітектур (SOA). У дослідженні розглянуто основні переваги впровадження мікросервісів, такі як масштабованість, відмовостійкість, незалежне розгортання та різноманітність технологій, а також потенційні проблеми, включаючи підвищену складність управління системою, розподілені транзакції та необхідність розширеного моніторингу.

Представлено практичний приклад, що моделює міграцію системи управління взаємовідносинами з клієнтами (CRM) з монолітної на мікросервісну архітектуру. План міграції зосереджений на декомпозиції системи на незалежні сервіси (керування користувачами, замовлення, платежі, звітність) з одночасним впровадженням практик DevOps, конвеєрів CI/CD та сучасних рішень для моніторингу. Результати моделювання показують, що впровадження мікросервісів може значно скоротити час розгортання, підвищити стійкість системи, покращити масштабованість та полегшити тестування.

***Ключові слова*: мікросервіси, масштабованість, контейнеризація, Kubernetes, API Gateway, DevOps, розподілені системи.**

УДК 004.42

[1]Остапчук О. П., к.т.н., доцент; [2]Циганчук М. С., студент (Національний університет водного господарства та природокористування, м. Рівне, [1]o.p.ostapchuk@nuwm.edu.ua ; [2] tsyhanchuk_ak21@nuwm.edu.ua)

РОЗРОБКА ВЕБДОДАТКУ З НАДАННЯ ПОСЛУГ БУДІВЕЛЬНОЮ КОМПАНІЄЮ З ВИКОРИСТАННЯМ ФРЕЙМВОРКУ REACT

У статті розглядається методологія розробки вебдодатка для надання послуг будівельною компанією. В основі роботи лежить використання сучасного JavaScript-фреймворку React, який забезпечує створення адаптивного та інтерактивного інтерфейсу. У процесі виконання дослідження проаналізовано предметну область, визначено особливості автоматизації процесів у сфері будівельних послуг, а також розглянуто сучасні підходи до організації компонентної структури та управління станом додатку. Побудовано інформаційну модель системи, спроєктовано архітектуру вебдодатку та реалізовано програмну частину з використанням React і Next.js. Проведено тестування функціональності, продуктивності та зручності використання вебдодатку, результати якого проаналізовано та систематизовано.

Ключові слова: **вебдодаток, React, Next.js, серверний рендеринг, адаптивний інтерфейс, інтерактивність, frontend-розробка.**

Вступ. Цифровізація будівельної галузі потребує ефективних вебрішень, які дозволяють компаніям зручно презентувати послуги, взаємодіяти з клієнтами та автоматизувати управління замовленнями. У цьому контексті сучасні JavaScript-фреймворки, такі як React, виступають ідеальним інструментом для створення адаптивних і продуктивних вебдодатків.

Метою даного дослідження є розробка функціонального вебдодатку, що забезпечує інтуїтивний інтерфейс, попередній розрахунок вартості послуг та зручну комунікацію з клієнтами. Архітектура рішення базується на фреймворку React, бібліотеці компонентів ShadCN/UI та утилітарній стилізації через Tailwind CSS.

Розроблений додаток реалізовано з використанням фреймворку React та платформи Next.js, які забезпечують створення продуктивного, адаптивного та інтерактивного інтерфейсу. Для стилізації застосовано Tailwind CSS, що дозволяє швидко формувати адаптивні компоненти з урахуванням сучасних UX/UI тенденцій. Компоненти інтерфейсу реалізовано з використанням бібліотеки shadcn/ui, яка базується на Radix UI.

Обрана технологічна зв’язка має низку ключових переваг, які зумовили її використання при розробці вебдодатку. Насамперед, важливою є компонентність: кожен елемент інтерфейсу реалізовано як окремий функціональний блок, що дозволяє багаторазово використовувати його в різних частинах проєкту та спрощує обслуговування коду. Крім того, завдяки використанню серверного рендерингу, що реалізований у Next.js через App Router, сторінки вебдодатку завантажуються значно швидше, що позитивно впливає як на користувацький досвід, так і на SEO-оптимізацію сайту. Ще однією важливою перевагою є адаптивність: Tailwind CSS забезпечує можливість створення інтерфейсу, який автоматично підлаштовується під різні розміри екранів — від смартфонів до десктопів, що критично важливо для сучасного вебу. Нарешті, інтерактивність інтерфейсу досягається завдяки використанню React, який дозволяє оновлювати дані на сторінці в реальному часі без її повного перезавантаження, забезпечуючи динамічну і зручну взаємодію з користувачем. Оскільки веб-додаток був зпроєктований з використанням патерну MVC, він розділений на три частини: моделі, відображення та контролери.

У додатку реалізовано такі основні секції:

HeroSection – вітальний блок головної сторінки (рис. 1).

Цей компонент є першим візуальним елементом, з яким взаємодіє користувач після завантаження сторінки. Він містить заголовок, що інформує про тип діяльності компанії, короткий опис або девіз, кнопку швидкого переходу до форми замовлення або розділу з переліком послуг, а також фонове зображення або відео з затемненням, що дозволяє акцентувати увагу на вмісті. Ця секція виконує роль орієнтира для користувача, спонукаючи його до подальшої взаємодії з сайтом.

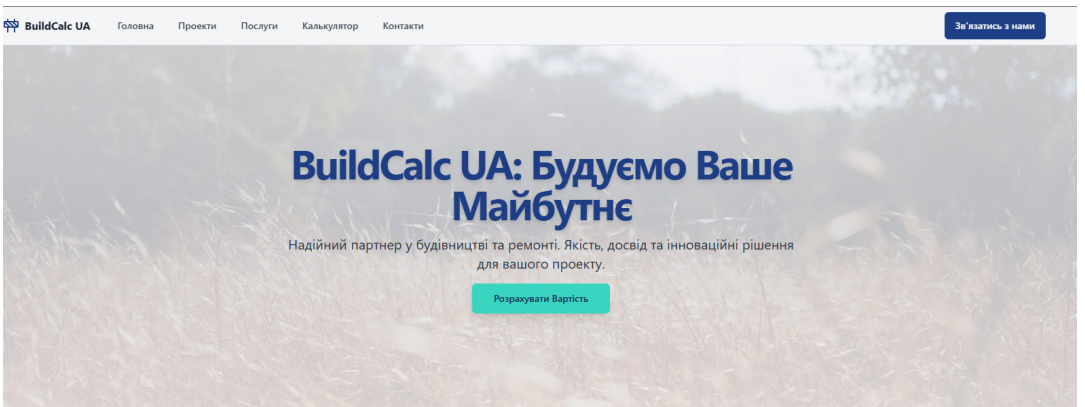

Рис. 1. Вигляд HeroSection

ProjectsSection – секція завершених об’єктів (рис. 2).

Секція створена для демонстрації виконаних проєктів компанії. Кожен об’єкт представлено у вигляді картки з фотографією, назвою та коротким описом. У перспективі реалізації передбачено можливість галереї «до/після» або фільтрації за типами робіт. Технічно реалізація ґрунтується на сітковій структурі, побудованій за допомогою Tailwind, з використанням компонентів Card із бібліотеки shadcn/ui. Дані можуть надходити через API або бути згенерованими статично за допомогою функцій Next.js.

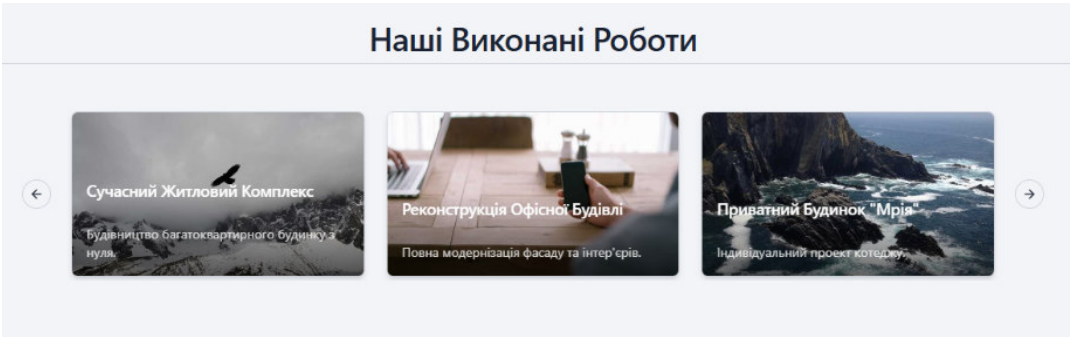

Рис. 2. Вигляд ProjectsSection з прикладами проєктів

ServicesSection – секція доступних послуг (рис. 3).

Цей блок містить повний перелік послуг, які надає компанія. Кожна послуга відображена з назвою, іконкою, створеною через бібліотеку LucideReact, стислим описом і орієнтовною вартістю. Дизайн орієнтований на зручність сприйняття, з чіткою адаптивною верстkою. Ця секція допомагає ознайомити користувача з усім спектром діяльності компанії, полегшує навігацію по пропозиціях та дозволяє швидше зорієнтуватися у виборі необхідної послуги.

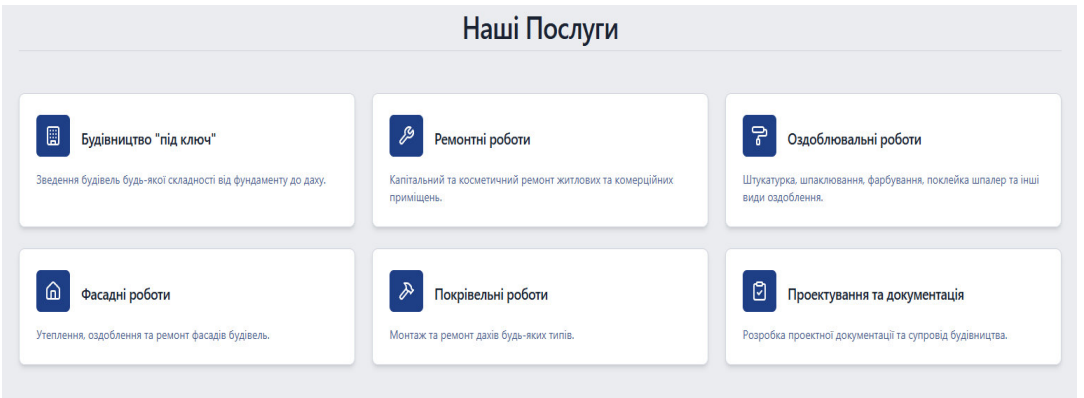

Рис. 3. Вигляд ServicesSection

CalculatorSection – калькулятор вартості робіт (рис. 4).

Цей компонент є інтерактивним інструментом, що дозволяє розрахувати попередню вартість замовлення. Користувач може вибрати необхідні послуги за допомогою чекбоксів, ввести кількість, площу або обсяг залежно від типу обраної послуги, після чого миттєво отримає підсумкову вартість. Всі обчислення реалізовані за допомогою хуків useState та useMemo, що забезпечує динамічне оновлення результатів без потреби перезавантаження сторінки. Для локалізованого виводу вартості у гривнях використовується функція formatCurrency. Інтерфейс калькулятора є інтуїтивно зрозумілим, адаптивним і сумісним з мобільними пристроями.

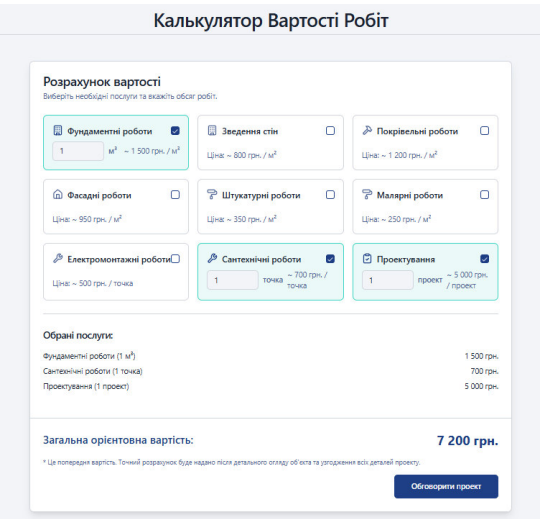

Рис. 4. Приклад роботи CalculatorSection з вибраними послугами

ContactSection – форма зворотного зв’язку (рси. 5).

Ця заключна секція дозволяє користувачу надіслати заявку або звернутися до компанії з будь-яким питанням. Вона включає поля для введення імені, електронної пошти та повідомлення, а також кнопку для підтвердження відправки. Уся введена інформація проходить перевірку на клієнтському рівні, після чого передається на сервер через server action у файлі app/actions/sendMessage.ts. У разі успішного надсилання або виникнення помилки користувач бачить відповідне повідомлення. Tailwind використовується для адаптивного розміщення полів та елементів форми, що забезпечує зручне користування на будь-яких пристроях.

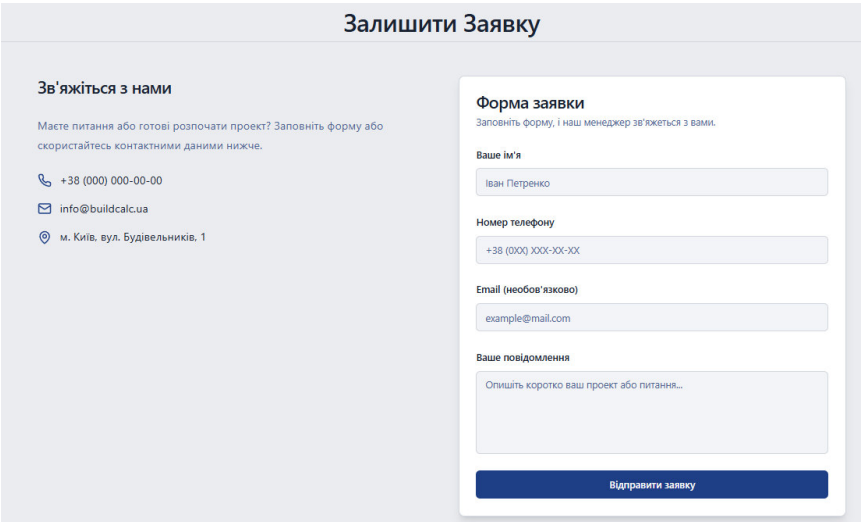

Рис. 5. Вигляд ContactSection у мобільній і десктопній версіях

Висновки. Розроблений вебдодаток повністю відповідає вимогам до сучасного сервісу будівельної компанії. Його функціональність охоплює презентацію послуг, портфоліо, інструменти попереднього розрахунку вартості та форму зворотного зв’язку. Структура додатку дозволяє легко розширювати функціонал, інтегрувати зовнішні сервіси або додати систему реєстрації/кабінет користувача.

Запропонована реалізація має практичну цінність як основа для подальшого розвитку цифрових сервісів у сфері будівництва. У перспективі можливе впровадження штучного інтелекту для рекомендацій послуг, а також 3D-візуалізацій проектів.

Ostapchuk O. P., Candidate of Engineering (Ph.D.), Associate Professor; Tsyhanchuk M. S., Senior Student (National University of Water and Environmental Engineering, Rivne)

DESIGN AND DEVELOPMENT OF A WEB APPLICATION FOR PROVIDING CONSTRUCTION COMPANY SERVICES USING THE REACT FRAMEWORK

The article presents a comprehensive methodology for the development of a web application designed to deliver services offered by a construction company. The main objective of the project is to provide a modern, efficient, and user-friendly digital platform that simplifies the interaction between clients and service providers within the construction industry. At the core of the system lies the powerful JavaScript framework React, which, in combination with the

Next.js framework, facilitates the development of a highly responsive, server-rendered, and scalable web interface.

Throughout the development process, a thorough analysis of the construction service domain was conducted. This included identifying the key stages of customer interaction, evaluating the typical workflow of construction-related services, and determining the most effective ways to automate and digitalize these processes. Special attention was given to the design of a modular and reusable component structure, enabling high code maintainability and flexibility. Modern state management approaches, such as the use of context and custom hooks, were incorporated to ensure smooth data flow and interaction within the application.

Furthermore, an information model was built to represent the relationships between users, services, requests, and feedback. The architecture was structured following best practices in modern front-end development, including clear separation of concerns, routing with the App Router in Next.js, and optimization of page loading. The software part was implemented using React components and TypeScript to ensure strong typing and robust functionality.

The application was rigorously tested to assess its functionality, performance under various conditions, and usability for end-users. Based on the test results, the system demonstrated stability, efficiency, and a user-centric experience. The outcomes of the project highlight the effectiveness of using modern web technologies in the digital transformation of traditional service-based industries such as construction.

***Keywords*: web application, React, Next.js, server-side rendering, adaptive interface, interactivity, frontend development.**

УДК 004.42

[1]Ostapchuk O. P., Candidate of Engineering (Ph.D.), Associate Professor; [2]Koverdiuk V. V., Post-graduate Student (National University of Water and Environmental Engineering, Rivne, [1]o.p.ostapchuk@nuwm.edu.ua, [2] v.v.koverdiuk@nuwm.edu.ua)

REDUCING LATENCY IN MASS ELECTRONIC DOCUMENT ISSUANCE IN .NET 8 USING SOURCE GENERATORS AND QUERY CACHING

The article analyzes strategies and technological approaches aimed at improving the efficiency of electronic document issuance in .NET 8. The focus is placed on source generators, which reduce runtime overhead, and multi-level

caching, which minimizes repeated database queries and computations. The purpose of the study is to show how the joint use of these technologies reduces latency and optimizes resource consumption in high-load environments. The study involved experimental modeling with simulated workloads to assess latency, throughput, and resource consumption. The results confirm substantial improvements in responsiveness, throughput, and resource efficiency, demonstrating the practical significance of integrating these tools as a basis for scalable and reliable systems of digital document management.

Keywords: **electronic document issuance, .NET 8, source generators, caching, performance optimization, distributed systems.**

The relevance of the problem. Modern electronic document issuance systems process vast numbers of requests daily, often reaching hundreds of thousands of transactions within short timeframes. The speed and reliability of these processes directly affect the efficiency of e-government platforms, corporate workflows, and digital service delivery. High latency leads not only to user dissatisfaction but also to systemic risks, as delays can accumulate across interconnected modules [1]. The main challenges remain high latency under mass requests, excessive database load, and duplication of computations in business logic. Addressing these challenges requires a careful balance between technological innovation and resource management. This research highlights the relevance of the problem and introduces architectural improvements that demonstrate measurable impact.

Understanding the urgency of the problem requires analyzing the existing technical limitations that directly affect latency and reliability.

Existing challenges and their causes. Several strategies exist to decrease latency in document issuance systems. One common approach is database query optimization, which relies on indexing, partitioning of large tables, and asynchronous calls to avoid blocking resources; these methods reduce access times but cannot fully eliminate bottlenecks under heavy load. Another technique is caching of intermediate results, which helps to minimize repeated queries for the same data and significantly reduces database pressure when frequently requested documents are involved. Equally important is minimizing reflection and runtime overhead, since reflection-based operations increase CPU usage, generate additional memory allocations, and create pressure on the garbage collector, all of which degrade performance when processing thousands of documents [2]. Load balancing in microservice architectures also plays a crucial role, distributing requests evenly across nodes and ensuring fault tolerance through L4 and L7 balancing mechanisms.

Despite these established strategies, systemic issues remain. Traditional query optimization and caching reduce but do not eliminate redundant computations, reflection continues to impose overhead, and balancing cannot

prevent inefficiencies in code execution paths. These limitations necessitate the search for complementary or alternative solutions. One of the promising approaches to overcoming these challenges involves leveraging the latest features of .NET 8, particularly source generators, which address the core inefficiencies at the compile-time stage.

The role of source generators in .NET 8. Source generators enable compile-time code generation by leveraging the Roslyn compiler infrastructure, producing strongly typed code that replaces dynamic operations at runtime. This significantly reduces overhead associated with reflection, where every request requires parsing metadata, creating objects, and performing costly dynamic lookups [3]. By shifting these operations to the compilation stage, the execution path becomes shorter and more predictable, as illustrated in fig. 1.

In the context of mass document issuance, such improvements are critical. Source generators allow auto-generation of SQL queries that bypass ORM abstraction layers, providing direct and optimized access to data. They also facilitate DTO serialization and deserialization using pre-built serializers instead of reflection-based libraries, which minimizes CPU usage and memory allocations. Furthermore, entity-to-API model mapping is handled through generated static code, ensuring constant-time access during high-frequency operations.

Compared with traditional runtime approaches, this technique reduces garbage collection pressure, stabilizes response latency, and improves throughput under concurrent workloads. Importantly, the generated code is type-safe and integrated into the build pipeline, which lowers the risk of runtime errors and simplifies debugging. In mass issuance scenarios, where thousands of documents are processed in parallel, these benefits translate into substantial latency reduction, improved resource efficiency, and overall system stability [3].

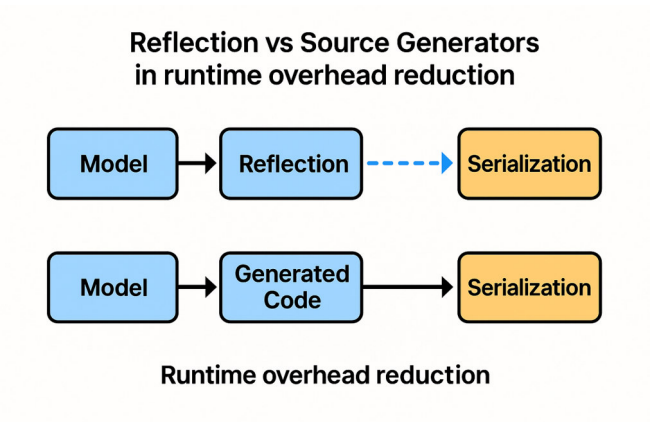

Fig. 1. Runtime reflection vs compile-time source generation in .NET 8

The importance of caching in performance optimization. Three levels of caching are applied in this research. First, in-memory cache stores frequently

accessed data within the same process, ensuring near-instant access for repeated short-lived calls [4]. Second, distributed cache based on Redis synchronizes cached entries across multiple services, maintaining consistency in clustered environments. Third, output cache stores fully prepared responses, such as PDF or JSON documents, enabling instant delivery to end users without recomputation [5]. The combination of these caching methods reduces redundant database calls, shortens response times, and alleviates bottlenecks in back-end services, as illustrated in fig. 2. Importantly, expiration policies and invalidation mechanisms must be configured carefully to ensure data relevance while maintaining performance.

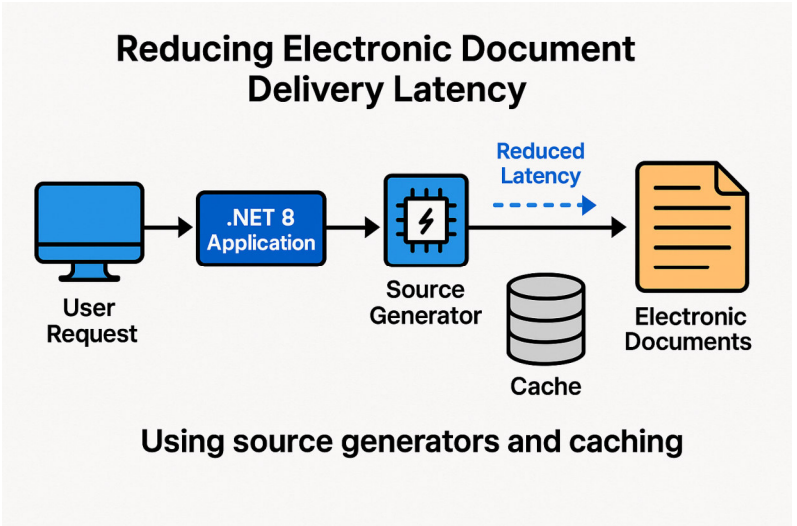

Fig. 2. Reducing electronic document delivery latency using source generators and caching

Research methodology. The modeling process was designed to replicate the workload of a large-scale electronic document issuance system. The experimental environment included a .NET 8 runtime deployed on Windows Server 2022 with 16-core CPUs and 64 GB of RAM. A SQL-based relational database was used with indexing and connection pooling enabled, and Redis was configured as a distributed cache cluster. The baseline system relied on Entity Framework with reflection-heavy serialization, while the optimized system employed source generators for compile-time code generation together with multi-level caching.

Load testing was conducted using Apache JMeter, simulating both uniform and burst traffic patterns. The dataset contained 100,000 documents, and 10,000 concurrent users were emulated. Operations included both read and write requests to better reflect real-world conditions.

Metrics collected during the experiments included average latency, 95th and 99th percentile latency, throughput (requests per second), number of database

queries, CPU and memory utilization, and cache hit ratio. Each test was repeated three times, and results were averaged to minimize random fluctuations. Confidence intervals were calculated to ensure statistical significance.

Table 1

Experimental parameters

Parameter	Value	Unit
Number of documents	100,000	items
Concurrent users	10,000	users
Database	SQL-based, indexed	–
Cache	Redis (distributed)	–
Baseline system	Entity Framework + reflection	–
Optimized system	.NET 8 + source generators + caching	–

Simulation results. The simulation showed that average latency decreased from 1200 ms to 340 ms, representing more than a threefold improvement. Database load decreased by 60% due to fewer repeated queries, while CPU consumption during serialization dropped by 45%. In addition to mean values, analysis of latency distribution revealed that the 95th percentile improved significantly, indicating not only faster average performance but also more stable system behavior under heavy load. The 99th percentile also showed considerable gains, reducing extreme outliers and contributing to system reliability. Throughput, measured in requests per second, increased by approximately 70%, confirming the scalability of the proposed architecture [6].

Table 2

Simulation results

Metric	Baseline	Optimized	Change	Unit
Mean latency	1200	340	-72%	ms
95th percentile latency	1800	480	-73%	ms
99th percentile latency	2500	720	-71%	ms
Throughput	150	255	+70%	requests/sec
DB queries	100% baseline	40%	-60%	relative load
CPU utilization	85	47	-45%	%
Cache hit ratio	–	78	+78%	%

Discussion. These results clearly demonstrate that the combination of source generators and caching provides substantial improvements in both response times and resource consumption (fig. 3). The reduction of mean latency and higher percentiles indicates not only an acceleration of average performance but also improved predictability, which is crucial for user satisfaction. The increase

in throughput highlights the scalability potential of the optimized system. Nevertheless, certain limitations must be acknowledged: cache consistency remains challenging in environments with frequent data updates, in-memory cache may risk memory saturation, and integration of source generators into CI/CD pipelines requires careful management.

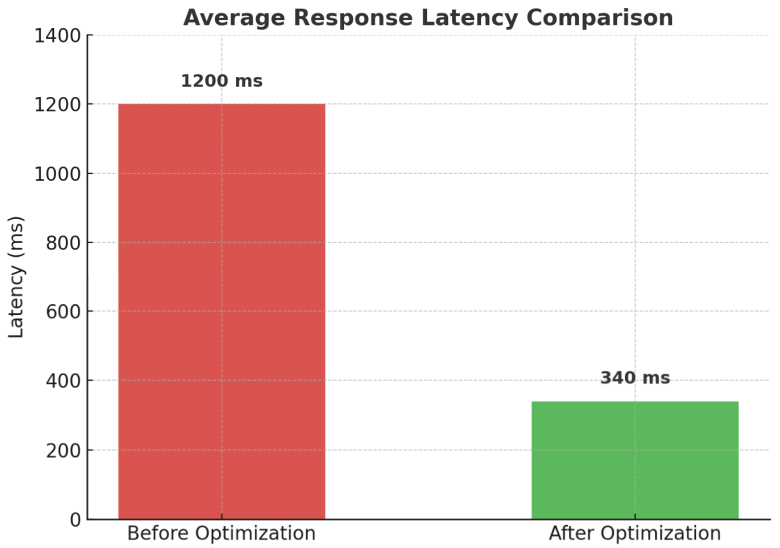

Fig. 3. Average response latency comparison before and after optimization

Conclusions. The proposed approach in .NET 8 significantly reduces latency in mass electronic document issuance. Source generators minimize runtime overhead by moving key computations to compile time, while multi-level caching reduces redundant database and service calls. Together, these techniques provide a scalable and reliable foundation for digital services that demand both performance and stability. The inclusion of percentile-based analysis and throughput metrics further confirms that the improvements are not limited to average values but extend to the overall quality of system performance under high load.

The scientific contribution of this work lies in demonstrating the combined effect of source code generation and hierarchical caching within a practical system architecture, an area where comprehensive evaluation has been limited. Future research should include adaptive caching strategies that dynamically adjust expiration and invalidation policies depending on workload characteristics, as well as AI-driven request prediction models that can preload frequently accessed documents. These directions would strengthen the contribution of the current study and extend its applicability to broader contexts of high-load distributed systems.

1. Kleppmann M. Designing Data-Intensive Applications. Sebastopol : O'Reilly Media, 2017. P. 543.
2. Richards M., Ford N. Fundamentals of Software Architecture. Sebastopol : O'Reilly Media, 2020. P. 411.
3. Lock A. ASP.NET Core in Action. 2nd ed. Shelter Island : Manning Publication, 2021. P. 612.
4. Gormley C., Tong Z. Elasticsearch: The Definitive Guide. Sebastopol : O'Reilly Media, 2015. P. 235.
5. Gormley C. Elasticsearch – The Definitive Guide. Sebastopol : O'Reilly Media, 2015. P. 235.
6. Ford N., Richards M., Sadalage P. J., Dehghani Z. Software Architecture: The Hard Parts. Sebastopol : O'Reilly Media, 2021. P. 289.

Остапчук О. П., к.т.н., доцент; Ковердюк В. В., аспірант (Національний університет водного господарства та природокористування, м. Рівне)

ЗМЕНШЕННЯ ЗАТРИМКИ ПРИ МАСОВІЙ ВИДАЧІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ У .NET 8 ЗА ДОПОМОГОЮ SOURCE GENERATORS ТА КЕШУВАННЯ ЗАПИТІВ

У статті проаналізовано стратегії та технологічні підходи, спрямовані на підвищення ефективності видачі електронних документів у .NET 8. У центрі уваги – використання source generators для зменшення витрат під час виконання та багаторівневого кешування для мінімізації повторюваних запитів до бази даних і обчислень. Метою дослідження є показати, як спільне застосування цих технологій дозволяє зменшити затримку та оптимізувати використання ресурсів у високонавантажених умовах. У дослідженні застосовано експериментальне моделювання з імітацією навантаження для оцінки затримки, пропускної здатності та споживання ресурсів. Результати підтвердили суттєві покращення у швидкодії, пропускній здатності та ефективності використання ресурсів, що підкреслює практичну значущість інтеграції цих інструментів як основи для масштабованих і надійних систем електронного управління документами.

***Ключові слова*: електронна видача документів, .NET 8, source generators, кешування, оптимізація продуктивності, розподілені системи.**

УДК 004.77

[1]Бойчура М. В., к.т.н.; [2]Костінський Ю. С., студент (Національний університет водного господарства та природокористування, м. Рівне, [1]m.v.boichura@nuwm.edu.ua, [2]kostinskyi_ak20@nuwm.edu.ua)

ІНФОРМАЦІЙНА СИСТЕМА ПЕРСОНАЛІЗОВАНОГО ПІДБОРУ ЕЛЕМЕНТІВ ГАРДЕРОБУ З УРАХУВАННЯМ ПОГОДНИХ ФАКТОРІВ

Досліджено проблематику створення адаптивних систем рекомендацій у сфері FashionTech. Запропоновано підхід до побудови гібридної веборієнтованої системи «Smart Wardrobe», яка вирішує задачу автоматизованого підбору одягу з урахуванням динамічних погодних факторів. Детально описано програмну реалізацію дворівневої архітектури, що поєднує середовище .NET для оркестрації бізнес-процесів та Python-скрипти для інтелектуального аналізу зображень. Обґрунтовано вибір стеку технологій комп'ютерного зору, зокрема використання каскадної моделі розпізнавання на базі Roboflow та CLIP для подолання проблеми «семантичного розриву». Наведено математичну модель розрахунку індексу теплового комфорту, яка адаптує рекомендації під вологість та вітер, а також алгоритм компенсації відсутніх даних через генерацію «віртуальних сутностей».

Ключові слова: **FashionTech, інтелектуальна система, комп'ютерний зір, Vision Transformer, CARS, HSL, ASP.NET Core.**

Вступ. Інтенсивний розвиток електронної комерції та цифровізація індустрії моди призвели до виникнення парадоксу «надлишкового вибору», коли користувачі стикаються зі значними часовими витратами на формування щоденного образу. Традиційні підходи до рекомендацій, що базуються на колаборативній фільтрації, часто ігнорують контекстуальні фактори, такі як поточні погодні умови та фізичний комфорт користувача [3]. Сучасні дослідження вказують на необхідність переходу до контекстно-залежних рекомендаційних систем (Context-Aware Recommender Systems – CARS), які здатні інтегрувати різнорідні дані: візуальні характеристики одягу, параметри навколишнього середовища та індивідуальні вподобання [2].

Аналіз наукових праць за період 2021-2025 років демонструє зростаючий інтерес до використання глибокого навчання для аналізу моди. Зокрема, у систематичному огляді 2025 року [1] зазначається, що мультимодальні моделі, які поєднують обробку зображень і тексту, стають новим стандартом індустрії. Дослідники [2] наголошують, що інтеграція динамічних змінних, таких як локальні погодні дані, дозволяє значно підвищити релевантність рекомендацій. Проте існуючі комерційні рішення

часто не мають ефективних механізмів для роботи з неповними даними про гардероб користувача, що призводить до проблеми «холодного старту» [3]. Також актуальним залишається питання точності комп'ютерного зору: як зазначається у роботі [4], архітектури на базі трансформерів (Vision Transformers) демонструють кращі результати у розумінні глобального контексту зображення порівняно з класичними згортковими мережами, проте вимагають значних обчислювальних ресурсів [5]. Таким чином, задача розробки ефективної архітектури, що поєднує точність сучасних нейромереж із швидкодією веб-застосунків та враховує динамічні фактори комфорту, є актуальною.

Метою роботи є підвищення ефективності процесу підбору персонального гардеробу шляхом розробки гібридної інтелектуальної системи, яка інтегрує методи комп'ютерного зору для точної класифікації одягу та адаптивні математичні моделі теплового комфорту.

Архітектура та стек технологій. Для досягнення поставленої мети було спроєктовано та реалізовано дворівневу архітектуру системи, що базується на принципі слабкої зв'язності компонентів. Такий підхід дозволив ефективно інтегрувати два гетерогенні обчислювальні середовища, кожне з яких оптимізоване під специфічні задачі. Схематичне зображення архітектури наведено на рис. 1.

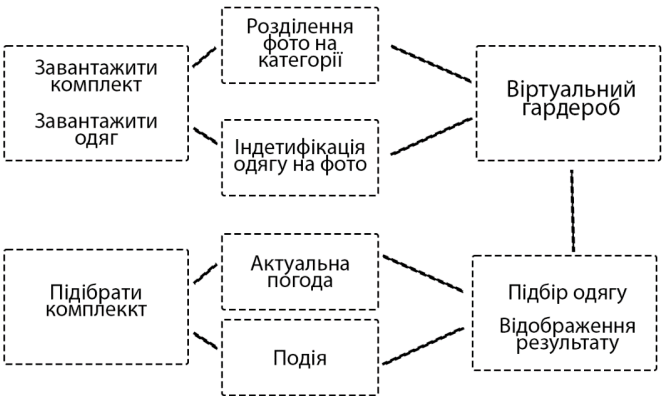

Рис. 1. Архітектура вебдодатка

Верхній рівень оркестрації (Back-end) реалізовано на базі платформи ASP.NET Core MVC [6]. Вибір цієї технології зумовлений необхідністю забезпечення високої продуктивності при обробці HTTP-запитів та надійності виконання бізнес-логіки. Використання мови C# дозволило забезпечити сувору типізацію даних та інтеграцію з системою Identity для безпечної автентифікації користувачів. Цей рівень відповідає за прийом зображень, взаємодію з базою даних, керування сесіями користувачів та відображення результатів.

Нижній рівень інтелектуальних обчислень реалізовано мовою Python, яка є стандартом де-факто у сфері машинного навчання [1]. Це забезпечило

доступ до передових бібліотек, таких як PyTorch, Transformers та NumPy, необхідних для роботи з нейронними мережами. Ключовим інженерним викликом стала організація ефективної міжпроцесної комунікації між середовищем CLR (.NET) та інтерпретатором Python. Замість використання важких брокерів повідомлень або REST API, які створюють додаткові накладні витрати, було реалізовано пряму взаємодію через перехоплення стандартних потоків введення-виведення. Система на C# ініціалізує процес Python з необхідними параметрами через об'єкт ProcessStartInfo, а результати роботи скриптів зчитуються безпосередньо з потоку StandardOutput у форматі JSON [6]. Це рішення дозволило мінімізувати латентність системи та уникнути проміжних операцій запису на диск.

Реалізація конвеєра комп'ютерного зору та ідентифікації об'єктів. Однією з найскладніших проблем у автоматизації аналізу гардеробу є «семантичний розрив» – розбіжність між візуальним представленням об'єкта та його категорійною приналежністю [1]. Експериментальні дослідження показали, що використання універсальних моделей часто призводить до помилок класифікації функціонально різних, але візуально схожих предметів (наприклад, туфлі та кросівки). Для вирішення цієї проблеми було розроблено каскадний конвеєр обробки зображень.

На першому етапі застосовується модель Roboflow (ідентифікатор «p2-uypxf/1») для детекції об'єктів та отримання їх обмежувальних рамок. Ця модель забезпечує первинну локалізацію предмета одягу та дозволяє відсікти зайвий фон. Проте тестування виявило, що у випадку низької впевненості (<40%) або при роботі зі складними категоріями, такими як взуття, точність цієї моделі є недостатньою. Тому було впроваджено логіку умовної передачі керування: якщо первинна модель демонструє низьку впевненість, зображення автоматично передається на аналіз до потужнішої мультимодальної моделі CLIP (Contrastive Language-Image Pre-Training). Використання CLIP дозволило досягти високої точності класифікації (до 90% на тестових даних) та усунути грубі помилки, характерні для простіших архітектур [5]. Такий гібридний підхід забезпечує баланс між швидкістю обробки простих запитів та точністю аналізу складних випадків.

Окрему увагу було приділено проблемі визначення кольору. Традиційний підхід, що базується на усередненні значень пікселів у просторі RGB, виявився неефективним через велику залежність від умов освітлення та кольору фону [1]. Для підвищення точності було розроблено алгоритм спектрального аналізу, який працює у перцептивно рівномірному просторі HSL (Hue, Saturation, Lightness). Принципова схема ідентифікації кольору показана на рис. 2. Алгоритм включає етапи геометричної фільтрації (вирізання області інтересу ROI), евристичного віднімання фону шляхом аналізу кутових пікселів та голосування пікселів за домінантний відтінок [4]. Перехід до моделі HSL дозволив відокремити інформацію про колір від його

яскравості, що забезпечило стабільне розпізнавання кольору навіть при наявності тіней або нерівномірного освітлення.

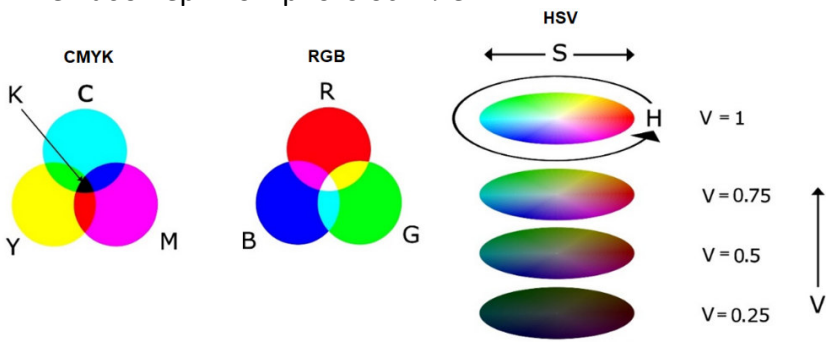

Рис. 2. Варіанти ідентифікації кольору та перехід до простору HSL

Математична модель підбору гардеробу. Функціональним ядром системи є модуль генерації образів, який вирішує задачу задоволення обмежень. Головним критерієм підбору є забезпечення теплового комфорту користувача [2]. Для цього введено поняття індексу теплоізоляції W, а цільове значення W_{req} розраховується на основі T_{feels} (температури «за відчуттями»), яка враховує охолоджуючий ефект вітру та вологість. Базова формула розрахунку має вигляд:

$$W_{req} = (T_{base} - T_{feels})k,$$

де $T_{base} = 30^{\circ}C$ – температура, при якій потреба в додатковій теплоізоляції наближається до нуля, а k – емпіричний коефіцієнт масштабування.

Важливою особливістю розробленої моделі є динамічна корекція цільового індексу в залежності від екстремальних значень вологості. При відносній вологості повітря понад 80% та низьких температурах теплопровідність середовища зростає, що вимагає підвищення рівня теплоізоляції одягу. Алгоритм автоматично додає 15 пунктів до цільового індексу W_{req} у таких умовах. Натомість при високих температурах та вологості вимога до одягу знижується для запобігання перегріву організму.

Для формування образів застосовуються дві стратегії топології одягу: стандартна багатошаровість (комбінація окремих елементів верху та низу) та цілісна архітектура (для суконь або комбінезонів). Процес генерації оптимізовано за допомогою методу стохастичного перемішування списків одягу перед відбором, що забезпечує варіативність рекомендацій. Для запобігання експоненціальному зростанню часу виконання при великій кількості речей введено обмеження на кількість ітерацій ($\text{limit} = 10$), що гарантує константну часову складність алгоритму $O(1)$ та стабільну роботу системи під навантаженням.

Окремим нововведенням є реалізація концепції «віртуальних сутностей» для вирішення проблеми «холодного старту» та неповноти даних,

про яку згадується в роботі [3]. У ситуаціях, коли поточні погодні умови вимагають критично важливого елемента захисту (наприклад, шапки при температурі нижче нуля), а відповідна річ відсутня у цифровізованому гардеробі користувача, система не перериває роботу помилкою. Натомість алгоритм генерує синтетичний об'єкт з ознакою is_virtual: true та необхідними тепловими характеристиками. Це дозволяє сформувати цілісний та безпечний для здоров'я образ, одночасно надаючи користувачеві рекомендацію щодо необхідності доповнення реального гардеробу.

Інтерфейс та взаємодія з користувачем. Розроблена система реалізована у вигляді веб-застосунку з адаптивним інтерфейсом. Реалізовано функціонал «Smart Batch Upload», який дозволяє користувачеві завантажувати пакети фотографій, що автоматично обробляються нейромережами. Результат генерації образу, який враховує локальні погодні дані та стиль події, представлено на рис. 3.

Користувач має можливість обрати локацію, тип події (наприклад, прогулянка, спорт, офіс) та отримати готовий комплект. Система відображає не лише підібрані речі, а й метеорологічні показники, на основі яких було прийнято рішення. Додатково реалізовано механізм «цифрового карантину»: при виборі опції «Я одягну це», використані речі отримують статус «У пранні» і виключаються з рекомендацій на 4 дні, що забезпечує ротацію гардеробу.

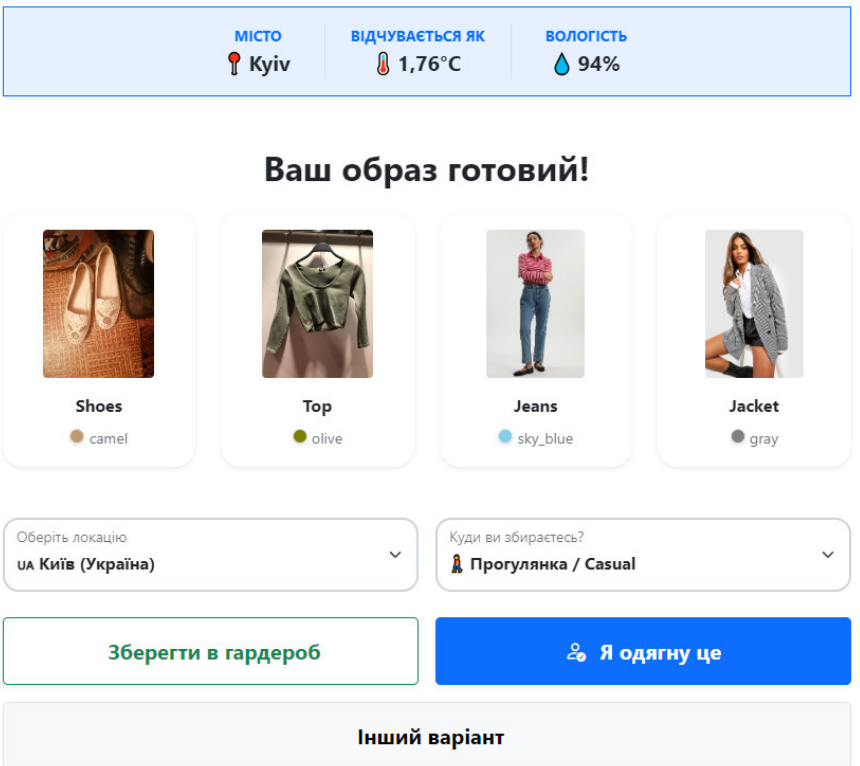

Рис. 3. Інтерфейс відображення згенерованого образу з погодними даними

Висновки. У ході виконання роботи було спроєктовано та програмно реалізовано інтелектуальну веборієнтовану систему «Smart Wardrobe», яка вирішує актуальну задачу персоналізованого підбору одягу з урахуванням факторів навколишнього середовища. Обґрунтовано доцільність використання гібридної архітектури, що поєднує продуктивність .NET та аналітичну гнучкість Python, забезпечуючи ефективну обробку мультимодальних даних. Розроблений каскадний конвеєр комп'ютерного зору з використанням моделей ViT та CLIP дозволив значно підвищити точність класифікації одягу та вирішити проблему розпізнавання складних текстур, яка була властива простішим моделям. Вдосконалений метод визначення кольору в просторі HSL із попередньою сегментацією фону довів свою ефективність у нівелюванні впливу умов освітлення на результати аналізу. Інтеграція математичної моделі теплового комфорту та механізму «віртуальних сутностей» дозволила створити систему, стійку до неповноти даних та здатну надавати функціонально корисні рекомендації, що сприяють збереженню здоров'я користувачів.

1. Jain D., Thazhathu E., Adiraju I. et al. FashionAI: Image-based clothing detection and shopping recommendation. *Innovation in Technology* : Proceedings of 2024 3rd International Conference (Bangalore, Mar. 01–03, 2024). Bangalore, 2024. P. 1–6.
2. Naham A.-Z., Wang J., Raeed A.-S. Multi-Task Learning and Gender-Aware Fashion Recommendation System Using Deep Learning. *Electronics*. 2023. Vol. 12 (16). P. 3396.
3. Kachbal I., El Abdellaoui S., Arhid K. Fashion recommendation systems: From single items to complete outfits. *International Journal of Computer Engineering and Data Science*. 2025. Vol. 4 (1). P. 27–40.
4. Khan S., Naseer M., Hayat M. et al. Transformers in vision: A survey. *ACM Computing Surveys*. 2022. Vol. 54 (6). P. 1–41.
5. Dosovitskiy A., Beyer L., Kolesnikov A. et al. An image is worth 16x16 words: Transformers for image recognition at scale. *Learning Representations* : Proceedings of International Conference (Vienna, May 04, 2021). Vienna, 2021. P. 1–21.
6. Price M. J. C# 12 and .NET 8 – Modern Cross-Platform Development Fundamentals. 8th ed. Birmingham : Packt Publishing, 2023. 828 p.

Boichura M. V., Candidate of Engineering (Ph.D.); Kostinskyi Y. S., Senior Student
(National University of Water and Environmental Engineering, Rivne)

INFORMATION SYSTEM FOR PERSONALIZED SELECTION OF CLOTHING ITEMS TAKING INTO ACCOUNT WEATHER FACTORS

The paper addresses the actual scientific and applied problem of creating

adaptive recommendation systems in the FashionTech sector. It proposes and implements the concept of an intelligent web-based system «Smart Wardrobe», designed to automate the selection of a personal wardrobe while strictly accounting for dynamic weather factors and individual user characteristics. A detailed description of the software implementation of a two-level hybrid architecture is provided. This architecture effectively combines the high-performance ASP.NET Core environment for business process orchestration with Python modules for deep image analysis, interacting through direct input-output stream interception to minimize latency.

The authors substantiate the choice of the computer vision technology stack. A cascade recognition model is introduced, utilizing Roboflow for initial detection and CLIP/Vision Transformer models to overcome the «semantic gap» and ensure high classification accuracy (up to 90%) for complex textures. An improved method for color determination in the HSL space with preliminary background segmentation is presented, solving the issue of lighting influence.

A functional core of the system is a mathematical model for calculating the thermal comfort index, which dynamically adapts recommendations based on «feels like» temperature, humidity, and wind chill factors. Furthermore, a unique algorithm for compensating for missing data through the generation of «virtual entities» is implemented to solve the «cold start» problem. The practical value of the work lies in creating a functional prototype that prioritizes the user's physical comfort over simple visual similarity.

Keywords: **FashionTech, Intelligent System, Computer Vision, Vision Transformer, CARS, HSL, ASP.NET Core.**

УДК 004.77

[1]Ющук Я. М., студентка; [2]Бойчура М. В., к.т.н. (Національний університет водного господарства та природокористування, м. Рівне, [1]yushchuk.ya_ak24@nuwm.edu.ua, [2]m.v.boichura@nuwm.edu.ua)

ІНТЕЛЕКТУАЛЬНА ВЕБОРІЄНТОВАНА СИСТЕМА ПІДТРИМКИ ДЛЯ ЗАСВОЄННЯ НАВЧАЛЬНИХ ДИСЦИПЛІН ІНОЗЕМНИМИ МОВАМИ

Запропоновано та реалізовано концепцію інтелектуальної веборієнтованої системи, призначеної для автоматизації перекладу та семантичного аналізу навчальних матеріалів у закладах вищої освіти. Описано архітектурні рішення, зокрема використання Clean Architecture, підходів DDD та CQRS, а також стек технологій: ASP.NET Core, React, Microsoft SQL Server. Особливу увагу приділено інтеграції з великими мовними моделями через платформу Ollama для забезпечення точності

перекладу термінології та виділення ключових понять. Продемонстровано функціонал системи для різних ролей користувачів.

Ключові слова: **Clean Architecture, ASP.NET Core, React, LLM, Ollama, семантичний аналіз, інтелектуальна система.**

Вступ. Сучасний етап розвитку вищої освіти характеризується активною інтернаціоналізацією та збільшенням кількості іноземних студентів. Це створює нові виклики, пов'язані з мовними бар'єрами, які знижують ефективність засвоєння навчального матеріалу [1]. Звичні підходи, такі як ручний переклад або використання базових онлайн-перекладачів, часто є часозатратними, не зберігають форматування складних документів (презентацій, лекцій) та не забезпечують достатньої точності у передачі спеціалізованої термінології. Таким чином, задача створення інноваційних інструментів, що поєднують автоматичний переклад із засобами інтелектуальної обробки тексту, є актуальною.

Метою роботи є розробка інтелектуальної веборієнтованої системи, яка забезпечує автоматичний переклад навчальних матеріалів (файлів .docx, .pptx) та виділення ключових понять на основі нейронних мереж, надаючи студентам та викладачам зручне середовище для взаємодії з контентом.

Архітектура та стек технологій. Для забезпечення масштабованості, гнучкості та надійності системи було обрано архітектурний стиль Clean Architecture. Цей підхід дозволяє розділити бізнес-логіку та інфраструктурні компоненти, роблячи систему незалежною від зовнішніх фреймворків та баз даних [2].

Система побудована за клієнт-серверною архітектурою. Взаємодія компонентів реалізована через RESTful API. Інтеграційна діаграма системи наведена на рис. 1.

Основними технологічні складові проєкту наводяться нижче.

Back-end реалізовано на платформі .NET з використанням мови C# та фреймворку ASP.NET Core. Використання принципів DDD (Domain-Driven Design) дозволило змоделювати складну бізнес-логіку, а патерн CQRS (Command Query Responsibility Segregation) забезпечив розділення операцій читання та запису для оптимізації продуктивності [3].

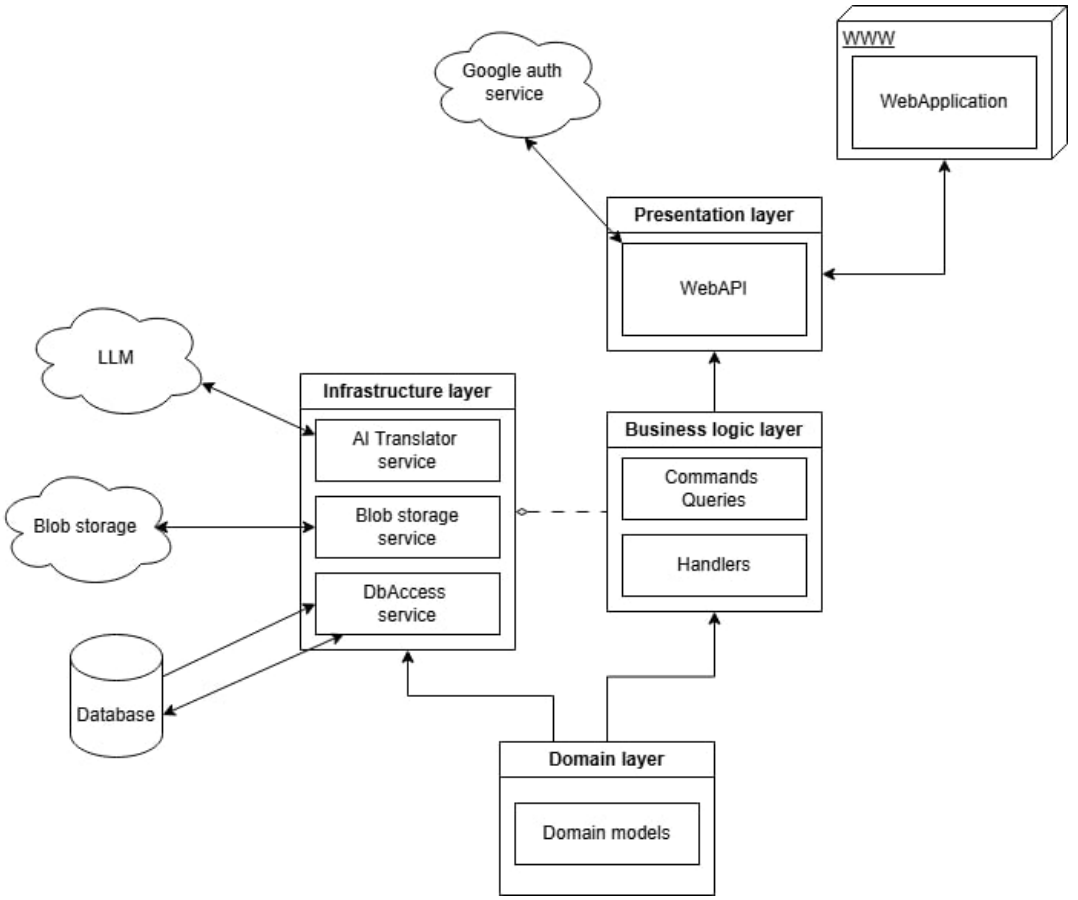

Рис. 1. Інтеграційна діаграма системи

Front-end розроблено з використанням бібліотеки React та інструменту збірки Vite. Це забезпечило створення швидкого та інтерактивного інтерфейсу користувача (SPA).

В якості системи керування базами даних (БД) обрано Microsoft SQL Server. Взаємодія з БД здійснюється через ORM Entity Framework Core, що спрощує виконання CRUD-операцій та управління міграціями.

Для реалізації інтелектуальних функцій (переклад, виділення ключових слів) використано LLM-модель Gemma 3 4B, розгорнуту локально через платформу Ollama [4]. Це рішення дозволяє обробляти конфіденційні навчальні матеріали без передачі їх стороннім платним API.

Для зберігання файлів лекцій та презентацій використано Azure Blob Storage.

Реалізація бази даних. Проєктування бази даних виконувалося з дотриманням принципів нормалізації. Схема БД включає таблиці для зберігання інформації про користувачів, групи, документи, ключові слова та їх переклади. Фрагмент ER-діаграми наведено на рис. 2.

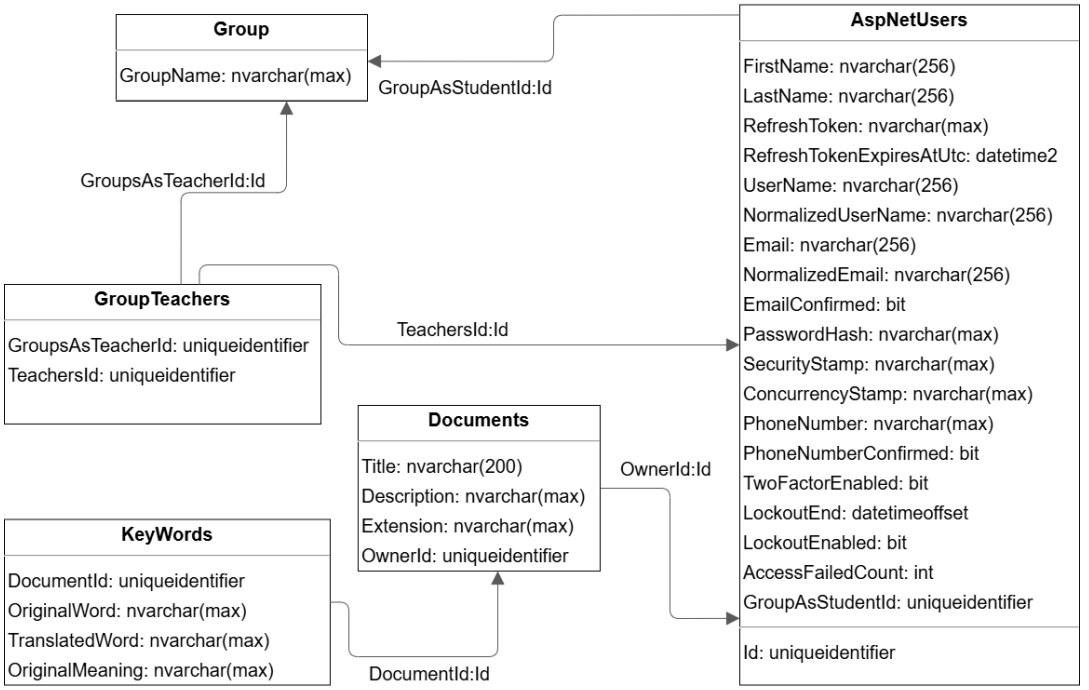

Рис. 2. Фрагмент схеми бази даних

Важливою особливістю є зберігання зв’язків між оригінальними термінами та їх поясненнями, що дозволяє реалізувати функціонал інтерактивного словника безпосередньо в тексті лекції.

Функціональні можливості та алгоритми роботи. Система підтримує три основні ролі користувачів: Адміністратор, Викладач та Студент. Адміністратор керує групами користувачів та налаштуванням доступу. Тоді як Викладач має можливість завантажувати навчальні матеріали. При завантаженні файлу (формати .docx або .pptx) система автоматично визначає мову оригіналу або дозволяє вказати її вручну, а також обрати цільову мову перекладу. Користувач ролі Студент має доступ до адаптованих матеріалів своєї групи.

Важливим алгоритмічно складним елементом системи є реалізація збереження структури документів після перекладу. Система розбирає XML-структуру файлів Office Open XML, виділяє текстові блоки, передає їх на обробку нейромережі, і коректно вбудовує перекладений текст назад, зберігаючи стилі, таблиці та зображення.

Фрагмент коду, що відповідає за взаємодію з сервісом перекладу та вилучення ключових слів, наведено на рис. 3.

```
foreach (var textElement in textElements)
{
    string original = textElement.Text;
    if (string.IsNullOrWhiteSpace(original))
        continue;

    try
    {
        string translated = await _translateService
            .TranslateLectureAsync(original, originalLanguage, targetLanguage);

        fullTranslatedText = fullTranslatedText + " " + translated;

        textElement.Text = translated;
    }
    catch (Exception ex)
    {
        Console.WriteLine($"Translation failed for '{original}': {ex.Message}");
    }
}
```

Рис. 3. Реалізація методу обробки тексту за допомогою штучного інтелекту

Інтерфейс та взаємодія з користувачем. Дизайн веб-застосунку розроблено з акцентом на зручність читання та навігації. Після авторизації (реалізовано через Google OAuth), користувач потрапляє на головну сторінку зі списком доступних дисциплін та документів (рис. 4).

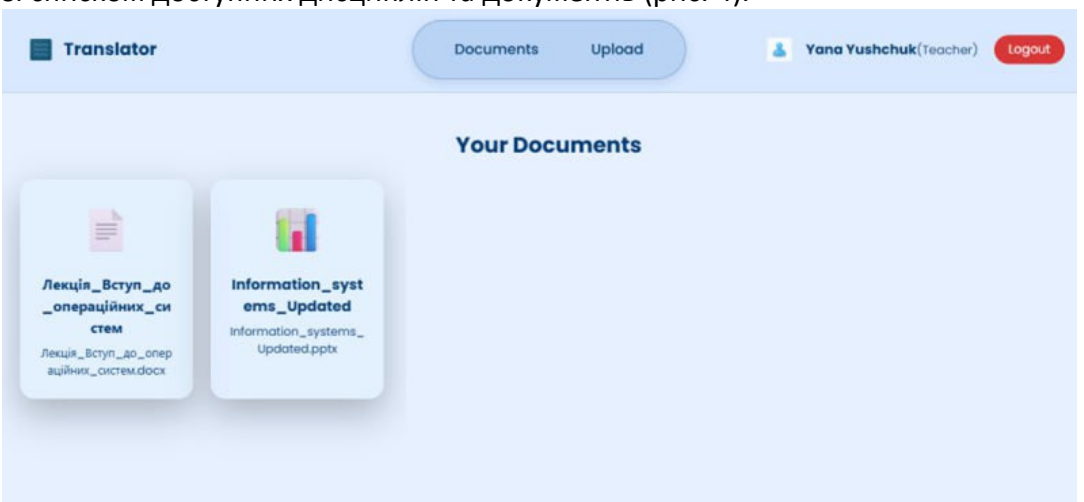

Рис. 4. Інтерфейс списку документів

Унікальною функцією системи є режим інтелектуального читання. Відкривши документ, студент бачить перекладений текст, у якому автоматично підсвічені ключові терміни. При натисканні на термін з’являється модальне вікно з його оригінальним звучанням, перекладом та коротким поясненням (дефініцією), згенерованим штучним інтелектом (рис. 5).

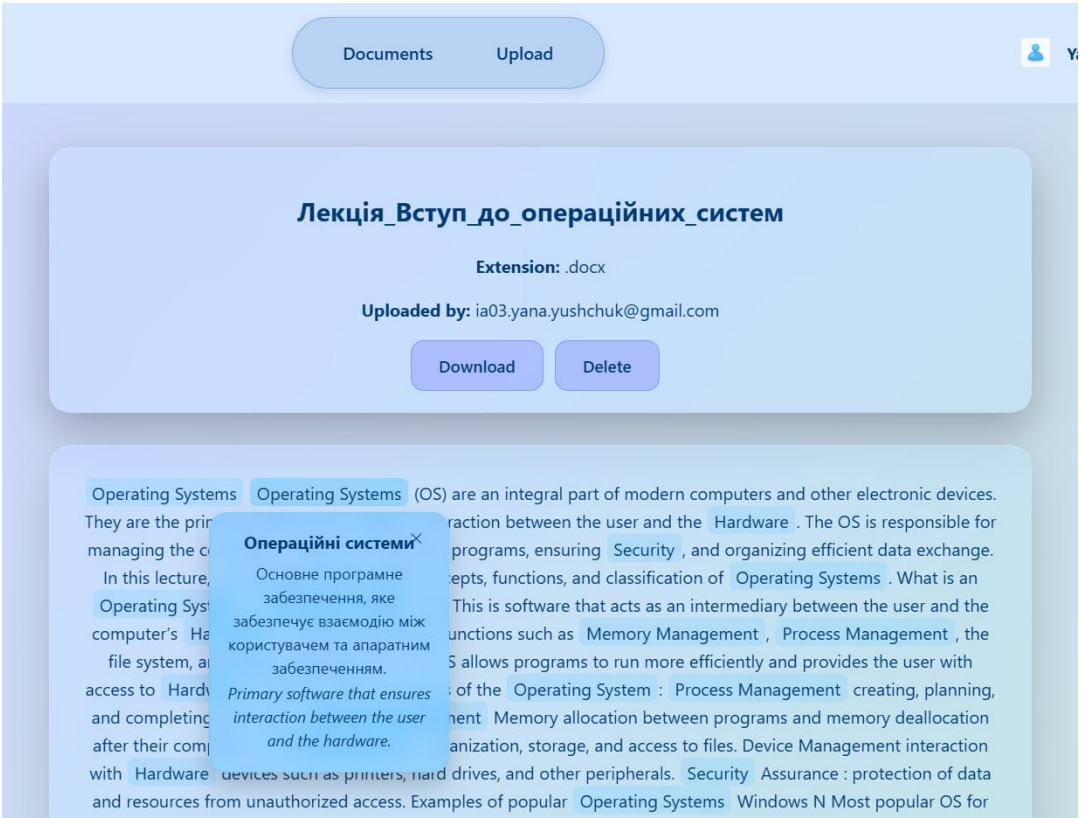

Рис. 5. Перегляд документу з інтерактивними елементами

Це сприяє кращому засвоєнню матеріалу та вивченню професійної лексики. Також реалізовано можливість завантаження перекладеного файлу для офлайн-доступу.

Висновки. У роботі спроєктовано та розроблено інтелектуальну веборієнтовану систему для підтримки багатомовного навчального процесу. Використання сучасного стеку технологій (ASP.NET Core та React) і архітектурних патернів (Clean Architecture та CQRS) забезпечило високу продуктивність та масштабованість рішення. Інтеграція з локальною LLM-моделлю через Ollama дозволила досягти високої якості перекладу спеціалізованих текстів із збереженням конфіденційності даних. Система вирішує проблему мовних бар'єрів, надаючи студентам інструмент для ефективного опрацювання лекційного матеріалу іноземними мовами, а викладачам – автоматизований засіб адаптації контенту.

1. Мачинська Н. І., Комарова Ю. В. Упровадження інноваційних технологій навчання у вищій школі. *Науковий вісник Мелітопольського державного педагогічного університету. Сер. Педагогіка*. 2015. Вип. 14 (1). С. 240–246.
2. Clean Architecture with ASP.NET Core. URL: https://ardalis.com/clean-architecture-asp-net-core/ (дата звернення: 05.11.2025).

3. CQRS – Azure Architecture Center. URL: https://learn.microsoft.com/ru-ru/azure/architecture/patterns/cqrs (дата звернення: 05.11.2025).
4. Ollama. URL: https://ollama.com/search (дата звернення: 05.11.2025).
5. ASP.NET Core documentation. URL: https://learn.microsoft.com/aspnet/core (дата звернення: 05.11.2025).

Yushchuk Y. M., Senior Student; Boichura M. V., Candidate of Engineering (Ph.D.)
(National University of Water and Environmental Engineering, Rivne)

INTELLIGENT WEB-BASED SUPPORT SYSTEM FOR LEARNING ACADEMIC DISCIPLINES IN FOREIGN LANGUAGES

The rapid internationalization of higher education has led to a significant increase in the number of foreign students and disciplines taught in foreign languages. This trend creates distinct challenges related to language barriers, which significantly hinder the effective acquisition of educational material. Standard automated translation tools often lack the capability to preserve the complex formatting of academic documents or provide context-specific terminological explanations required in a university setting. To address these issues, this paper proposes and implements an intelligent web-based system designed to automate the translation and semantic analysis of educational materials.

The system architecture is founded on Clean Architecture principles, ensuring distinct separation of concerns, testability, and scalability. The Back-End logic is implemented using the ASP.NET Core framework, leveraging Domain-Driven Design to model complex business rules and Command Query Responsibility Segregation to optimize data processing. The Front-End is a dynamic Single Page Application developed with React and Vite. A distinctive feature is the integration of the Gemma 3 4B Large Language Model via the Ollama platform. This allows for local, privacy-focused processing of confidential lecture materials, ensuring high-quality translation and the extraction of key concepts. The system includes advanced file processing algorithms that handle Office Open XML formats, enabling the translation of .docx and .pptx files while strictly preserving original structures, styles, and images.

The practical implementation results in a platform that supports Teacher and Student roles, offering interactive study materials with highlighted definitions, thereby significantly improving the learning experience.

Keywords: **Clean Architecture, ASP.NET Core, React, LLM, Ollama, semantic analysis, intelligent system.**

УДК 37.018.43:159.9

[1]Доля Л. В., студентка 2 курсу магістратури спеціальності «Психологія», **[2]Бабич С. В., к.т.н., доцент** (Національний університет водного господарства та природокористування, м. Рівне, [1] dolya_ipo24@nuwm.edu.ua ; [2] s.v.babych@nuwm.edu.ua)

СОЦІАЛЬНО-ПСИХОЛОГІЧНІ АСПЕКТИ ДИСТАНЦІЙНОГО НАВЧАННЯ СТУДЕНТІВ У ВОЄННИЙ ПЕРІОД: РОЛЬ ЦИФРОВИХ КОМУНІКАЦІЙ

Актуальність дослідження зумовлена трансформацією української освіти, де дистанційне навчання набуло статусу екзистенційної необхідності. Цифрові комунікації, хоча і є життєво важливим містком для академічного процесу, водночас створюють зони вразливості, оскільки емоційне виснаження та хронічний стрес роблять студентів вразливою мішенню для інформаційних атак та шахрайства. Таким чином, актуальність зміщується з технічних аспекті на психологічну стійкість особистості в цифровому середовищі.

Ключові слова: **дистанційне навчання, воєнний період, психологічна стійкість, кіберстійкість, кібербезпека, адаптивна ідентичність, соціальна інженерія, когнітивне виснаження.**

Метою роботи є проведення аналізу глибинних соціально-психологічних трансформацій, що відбуваються зі студентами в умовах війни, та визначити, як обізнаність щодо кібербезпеки впливає на їхню загальну адаптивну стійкість та успішність.

У роботі розглянуто три ключові аспекти:

1. Психологічна «інверсія» начального процесу: встановлено, що мозок студента постійно перебуває в аварійному режимі («Бий або біжи»), що призводить до деструкції когнітивних механізмів (розсіювання уваги, ментальне перевантаження). Цей зсув пріоритетів (виживання замість навчання) підтверджується дослідженнями Шевченка (2022) [1] та Помиткіної (2023) [2], які фіксують значне зниження концентрації та мотивації. Успіх навчання в цих умовах залежить від внутрішнього локусу контролю [3] та проактивної адаптивності (Черевко та ін., 2024) [4].

2. Цифровий простір як арена загроз: цифрові канали є мішенню для психологічних атак. Феномен «фантомної соціалізації» (спілкування в чатах) не компенсує втрачене відчуття спільноти і може посилювати співчутливу втому (Коваленко, 2023) [5]. Фішинг та ІПСО свідомо експлуатують стан підвищеної вразливості та дефіцит критичного мислення, що підтверджено зростанням атак на освітній сектор (Держспецзв’язку, 2024) [6].

3. Кіберстійкість та адаптивна ідентичність: у воєнний час формується нова, адаптивна ідентичність, де межі між особистим і безпековим просторами стираються. Кіберстійкість (здатність розпізнавати емоційні тригери) переходить із розряду технічної навички у ключову соціально-психологічну компетенцію. Обговорюється необхідність переосмислення академічної етики та впровадження травмоінформованої освіти через «ефект свідка» та нову, суспільно значущу цінність знання.

Війна кардинально змінила життя українських студентів, зробивши дистанційне навчання необхідністю. Цей період вимагає від них освоїти нові програми та пройти серйозну ментальну адаптацію під постійним тиском стресу і небезпеки. В цій ситуації цифрові комунікації відіграють подвійну роль. З одного боку, вони є чи не єдиним надійним способом підтримувати навчання та спілкування. З іншого – створюють зони вразливості як для психологічного стану студентів, так і для їхньої цифрової безпеки. Актуальність статті полягає у неможливості розглядати навчання лише як технічний процес. Стан тривоги та емоційне виснаження роблять студентів легкою мішенню для шахраїв та інформаційних атак, які використовують їхню психологічну вразливість.

Аналіз наукових публікацій свідчить про глибоку зацікавленість вітчизняних дослідників проблемою впливу війни на психіку студентства та освітній процес. Встановлено, що когнітивне та мотиваційне виснаження є однією з головних перешкод для навчання. Зокрема, дослідження [1] фіксує, що понад 60% студентів відзначають значне погіршення концентрації та мотивації саме через стрес. Порушення когнітивних функцій в умовах війни детально аналізує [2], яка підтверджує, що постійна дія стресорів викликає зниження обсягу та стійкості уваги, що є прямим наслідком гіперактивації лімбічної системи. Проблеми адаптації студентів до дистанційного навчання в умовах воєнного стану, зокрема психологічний та дидактичний аспекти, детально розглядають [3]. На рівні саморегуляції та адаптації, дослідження [4] вказує, що високий рівень внутрішнього локусу контролю є визначальним предиктором академічної успішності, компенсуючи зовнішню дезорганізацію. Проблема соціалізації та психологічної підтримки розкривається у роботах [5], які підтверджують, що відчуття соціальної підтримки в онлайн-форматі залишається недостатнім, посилюючи ризики розвитку тривожних станів. Крім того, [6] свідчать про зростання частки кібератак, заснованих на соціальній інженерії, спрямованих на освітній сектор, що підкреслює необхідність вивчення кіберпсихологічних ризиків.

Незважаючи на наявність досліджень, комплексний аналіз інтеграції психологічної стійкості та кіберстійкості як ключових факторів адаптивної ідентичності студента в умовах війни залишається недостатньо висвітленим.

1. Психологічна «інверсія» навчального процесу: деструкція когнітивних механізмів

Повномасштабне вторгнення змінило правила та спосіб навчання студентів. Це явище можна назвати психологічною інверсією. Раніше університетські стіни, розклад і присутність інших людей слугували зовнішньою підтримкою для дисципліни та зосередженості. У дистанційному форматі під час війни ці зовнішні опори зникли. В результаті, функція контролю за навчанням повністю лягла на психіку студента, яка вже й так перевантажена постійною тривогою та невизначеністю.

Мозок студента, який навчається під час війни, працює не так, як у мирний час. Він постійно перебуває в аварійному режимі. Психологи називають це реакцією «Бий або біжи». Вона вимикає те, що найбільше потрібно для навчання – глибоку концентрацію. Замість того, аби вникати у складну формулу, текст тощо наш мозок постійно шукає іншу інформацію: чи є світло? Чи працює інтернет? Чи не було сигналу повітряної тривоги? Чи немає повідомлення про загрозу?. Це ускладнює глибоке розуміння матеріалу та призводить до розсіювання уваги, погіршення когнітивних функцій і ментального перевантаження (cognitive overload). Дослідження [2] підтверджує, що постійна дія стресорів війни викликає зниження обсягу та стійкості уваги студентів, що є прямим наслідком гіперактивації лімбічної системи і порушення роботи префронтальної кори. Фактично, відбувається зміщення пріоритетів: якщо раніше на першому місці було навчатися та скласти сесію, то зараз – вижити, а якщо залишиться енергія, то вчитися. Це не лінь, це ментальне виснаження. Ресурси, які мали б йти на логіку та запам’ятовування, тепер йдуть на боротьбу з тривогою. Як наслідок, страждає пам’ять, планування стає неможливим, а мотивація, навіть якщо вона була високою, просто «згорає». За даними опитування, проведеного в Україні у 2022 році, понад 60% студентів відзначили значне погіршення концентрації та мотивації через стрес [1].

Часткова або тривала відсутність зовнішніх регуляторів навчального процесу перекладає всю відповідальність за організацію безпосередньо на суб’єкт навчання. Цей процес виходить за рамки звичайної академічної дисципліни. Студентська діяльність перетворюється на постійне управління ресурсами в умовах дефіциту. Студенти змушені вирішувати комплексні завдання: пошук стабільного інтернету, планування роботи, адаптація навчального циклу до баз безпеки (наприклад, перебуваючи в укритті). Це вимагає безперервного маневрування між побутовими викликами та академічними вимогами.

Для ефективного функціонування в такому нестабільному середовищі ключовим стає наявність сильного внутрішнього локусу контролю. Ця психологічна якість являє собою переконання особистості у власній здатності впливати на результати своєї діяльності, незалежно від зовнішніх неконтрольованих обставин (повітряні тривоги, графіки відключень тощо). Студенти з розвиненим внутрішнім локусом контролю демонструють

проактивну адаптивність: вони активно шукають альтернативні навчальні простори, оптимізовують свій робочий графік та сприймають продовження навчання як особистий акт опору зовнішньому хаосу. Зокрема, дослідження [4] вказує, що високий рівень саморегуляції та внутрішнього локусу контролю є визначальними предикторами академічної успішності студентів під час воєнних дій, компенсуючи зовнішню дезорганізацію. Протилежний підхід спостерігається у тих, хто демонструє зовнішній локус контролю. Відчуваючи безпорадність, вони схильні до швидкої апатії та ментального вигорання. Для них навчання стає додатковим стресором, й вони обирають стратегію мінімальної достатності (наприклад, закрити сесію), що знижує якість засвоєння матеріалу. Отже, в умовах воєнного часу успіх дистанційного навчання є, насамперед, тестом на психологічну стійкість і гнучкість.

2. Цифровий простір як арена соціально-кібернетичних загроз

В мирний час цифрові комунікації були лише доповненням, але з початком війни вони стали чи не єдиним містком, що з’єднує студентів і викладачів. Проте це спілкування має серйозний недолік, який ми називаємо «фантомною соціалізацією». Всі важливі соціальні сигнали – вираз обличчя, інтонація, мова тіла – які допомагають нам зрозуміти емоційний стан іншої людини, майже повністю зникають у чатах або при вимкнених камерах. Студенти можуть бути постійно «на зв’язку», але разом з тим відчувати глибоку емоційну ізоляцію. Групові чати виконують важливу функцію колективного проживання травми, але відсутність фізичного «заземлення» часто призводить до співчутливої втоми – емоційного виснаження від постійного занурення у чужий біль без реального, повноцінного контакту. Дослідження [5] підтверджують, що відчуття соціальної підтримки у онлайн-форматі залишається недостатнім, що посилює ризики розвитку тривожних і депресивних станів.

Саме через те, що цифрові комунікації стали головною опорою навчання, сфера кібербезпеки перестала бути виключно технічним питанням. Вона перейшла на рівень особистої психологічної стійкості. Цифрові канали, які ми використовуємо для навчання (Zoom, Telegram, університетські системи), стали прямими мішенями для психологічних атак і шахрайства.

Фішинг як психологічна атака. У воєнний час зловмисники свідомо використовують високий рівень стресу і невизначеності для маніпуляцій. Фішинг маскується під найбільш болючі та важливі теми: офіційні розпорядження про евакуацію, обіцянки фінансової допомоги або нові правила безпеки. Це експлуатує стан підвищеної вразливості та дефіцит критичного мислення у момент емоційного напруження. Студенти й викладачі, які орієнтовані на швидке реагування (що природно і важливо в умовах війни), стать легкою ціллю. Актуальний аналіз кіберінцидентів за 2023-2024 роки показує, що частка атак, заснованих на соціальній інженерії,

зросла на 40% і була спрямована переважно на освітній сектор та державні установи.

Інформаційно-психологічні операції (ІПСО). Навчальні чати, без фізичного контролю, стають ідеальним майданчиком для поширення дезінформації та панічних «вкидів». Завдання ІПСО – підірвати колективний психологічний клімат, зруйнувати довіру до офіційних джерел інформації та адміністрації університету. В умовах війни довіра є ключовим елементом соціального капіталу. Коли студенти перестають вірити офіційним каналам і переходять на неперевірені чутки, це призводить до хаосу та руйнування навчального процесу зсередини.

3. Кіберстійкість та формування адаптивної ідентичності студента

В умовах тотальної залежності від цифрових комунікацій, психологічна кіберграмотність переходить із розряду бажаних навичок у ключову компетенцію адаптивної ідентичності.

Студент більше не може відокремлювати навчання від кібербезпеки. Здатність критично оцінювати інформацію, розпізнавати емоційні тригери, які використовують зловмисники, та не піддаватися маніпуляціям (кіберстійкість) стає такою ж важливою навичкою, як і конспектування.

Необхідно навчити студента робити примусову паузу (стоп-пауза-перевірка), перш ніж натиснути на невідоме посилання або поділитися сумнівною інформацією. Це має стати рефлекторною звичкою в цифровому середовищі. Дистанційне навчання у воєнний час змушує студентів формувати нову, адаптивну ідентичність, де межі між особистим, навчальним та безпековим просторами стираються.

Необхідність фіксувати докази воєнних злочинів або просто бути свідком руйнувань в той час, коли необхідно виконувати академічне завдання, створює когнітивний дисонанс. У цьому контексті, виникає потреба переосмислення академічної етики: чи допустима «академічна поблажливість» в умовах травматизації? Це вимагає від освітніх установ впровадження травмоінформованої освіти.

Навчання набуває вищої суспільної цінності. Воно стає інвестицією у посттравматичне зростання та інструментом для відновлення країни, що є потужним мотиваційним чинником для нової, адаптивної генерації.

Всупереч усім загрозам, варто оглянути і переваги та можливості дистанційного формату навчання в умовах окресленого емоційного та фізіологічного тиску, адже, незважаючи на виклики, формат дистанційного навчання у воєнний час створює унікальні переваги та можливості:

- Безпека та гнучкість. Дистанційний формат забезпечує освітню безперервність та дозволяє студентам продовжувати навчання з будь-якого безпечного місця, що є критичною перевагою в умовах фізичної небезпеки.
- Розвиток самостійності. Відсутність зовнішніх регуляторів сприяє формуванню сильного внутрішнього локусу контролю та навичок

самоорганізації. Ці компетенції мають високу цінність для майбутньої професійної діяльності.

- Кіберстійкість як компетенція майбутнього. Студенти не лише навчаються, а й набувають практичного досвіду в умовах постійного кібертиску, що перетворює кіберстійкість на ключову соціально-психологічну та професійну навичку.
- Суспільна цінність знання. Навчання набуває вищої суспільної цінності. Воно стає актом опору та інвестицією у посттравматичне зростання та інструментом для відновлення країни, що є потужним мотиваційним чинником для нової, адаптивної генерації.

Висновки. Дистанційне навчання студентів у воєнний період слід розглядати як унікальний соціально-психологічний експеримент, де успіх визначається не якістю мережевого з'єднання, а рівнем психологічної та кібернетичної стійкості. Цифрові комунікації, хоча і є необхідним містком для підтримки академічного процесу та соціальних зв'язків, водночас становлять ризик, оскільки стають ареною для маніпуляцій та використання психологічної вразливості. Для забезпечення цілісності навчального процесу та ментального здоров'я, необхідний інтегрований підхід. Він включає цідеспрямований розвиток критичного цифрового мислення та навчання механізмам психологічної самодопомоги у кіберпросторі.

Майбутнє української освіти значною мірою залежить від того, наскільки швидко та ефективно ми зможемо перетворити ризики цифрового середовища на фундамент для нової генерації.

1. Шевченко С. М. Психологічна допомога студентам у період російсько-української війни: теоретико-практичний аспект. *Наукові інновації та передові технології*. 2022. № 7 (9). С. 38–48.
2. Помиткіна Л. В. Вплив військового конфлікту та когнітивні функції студентської молоді. *Теоретичні та прикладні проблеми психології*. 2023. № 3 (62). С. 132–139.
3. Лазор О. Д., Семенчук О. А. Адаптація студентів до дистанційного навчання в умовах воєнного стану: психологічний та дидактичний аспекти. *Вісник Черкаського національного університету імені Богдана Хмельницького. Сер. Педагогічні науки*. 2023. № 1. С. 98–104.
4. Психологічні детермінанти саморегуляції навчальної діяльності студентів в умовах гібридної війни. Освітній простір України / Черевко О. В. та ін. 2024.
5. Соціально-психологічна підтримка здобувачів освіти в умовах дистанційного навчання в період воєнних дій / Коваленко О. В. та ін. *Науковий вісник Ужгородського університету. Сер. Педагогіка. Соціальна робота*. 2023. № 2 (53). С. 121–125.
6. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку). російські кібероперації Н1'2024. *Аналітичний звіт*. Київ, 2024.

Dolia L. V., Master, Babich S. V., Candidate of Engineering (Ph.D.), Associate Professor (National University of Water and Environmental Engineering, Rivne, Ukraine)

SOCIO-PSYCHOLOGICAL ASPECTS OF STUDENTS' DISTANCE LEARNING DURING WARTIME: THE ROLE OF DIGITAL COMMUNICATIONS

The relevance of this study is driven by the existential transformation of Ukrainian education, where distance learning has become a forced necessity due to the full-scale war. While digital communications serve as a vital bridge for academic processes and social connections, they simultaneously introduce critical vulnerabilities. This is because emotional exhaustion and chronic stress render students highly susceptible to information warfare, scams, and cyberattacks. Consequently, the research focus shifts from purely technical concerns to the psychological resilience of the individual in the digital environment. The role of digital communications is therefore analyzed as critical infrastructure for learning, which poses a dual threat: security risks and severe mental overload. The purpose of the work is to analyze the profound socio-psychological transformations students undergo during the war and to determine how awareness of cybersecurity directly impacts their overall adaptive resilience and academic success.

The study establishes the phenomenon of «psychological inversion» in the learning process. The external supports for discipline (university walls, fixed schedules) have vanished, transferring the entire burden of organizational control to the student's psyche, which is already working in an "emergency mode" (Fight or Flight response). This constant state of alert suppresses deep concentration, leading to a focus on survival and increased cognitive dysfunction, such as attention deficit and mental overload (*cognitive overload*). Research confirms that over 60% of students report a significant decline in concentration and motivation due to stress. Success in this unstable environment critically hinges on a strong internal locus of control, which enables students to proactively adapt and view learning as an act of resistance against external chaos.

The digital space is analyzed as an arena for socio-cybernetic threats. The reliance on digital channels results in «phantom socialization», where the lack of non-verbal cues in chats and online classes leads to emotional isolation and compassion fatigue despite constant connectivity. Furthermore, the imperative of cyber hygiene transcends technical rules and becomes an existential imperative, demanding a constant «stop-pause-check» protocol. The need to continuously filter information and verify sources creates an additional, permanent cognitive load that exacerbates existing mental exhaustion. Adversaries consciously exploit this vulnerability: Phishing attacks are

psychologically tailored to exploit wartime anxieties (e.g., promises of aid or evacuation warnings), and propaganda (IPSO) uses educational chats to spread panic and destroy collective trust, which is a key social asset during wartime. Cyber incident analysis confirms a significant increase in social engineering attacks targeting the education sector.

The paper argues that cyber resilience—the ability to recognize emotional triggers and resist manipulation — is transforming into a core competence of the adaptive identity of the modern student. Distance learning under war conditions mandates the formation of a new identity where the lines between personal, academic, and security spheres are blurred. This necessitates the implementation of trauma-informed education to address the cognitive dissonance caused by being a «digital witness» to war while simultaneously completing academic tasks. Despite the challenges, this format offers unique advantages and opportunities, including ensuring educational continuity from any safe location, fostering self-reliance and a strong internal locus of control, and cultivating cyber resilience as a highly valuable professional skill for the future generation tasked with national recovery. The study concludes that the future of Ukrainian education relies on the integrated development of critical digital thinking and psychological self-help mechanisms within cyberspace.

***Keywords*: distance learning, wartime, psychological resilience, cyber resilience, cybersecurity, adaptive identity, social engineering, cognitive overload.**

УДК 658.4:004.42

Бабич С. В., к.т.н., доцент, Жовтяк Н. О., студент 1 курсу магістратури спеціальності «Комп'ютерна інженерія» (Національний університет водного господарства та природокористування, м. Рівне, s.v.babych@nuwm.edu.ua ; zhovtiak_ak25@nuwm.edu.ua)

ВИКОРИСТАННЯ НАВИЧОК ПРОЕКТНОГО МЕНЕДЖЕРА В ОРГАНІЗАЦІЇ КОМАНДИ ДЛЯ CTF ЗМАГАНЬ

Розглянуто застосування ключових методологій управління проектами (Project Management, PM) в умовах високоінтенсивних змагань з кібербезпеки «Capture The Flag» (CTF). Проаналізовано специфіку CTF як короткострокового, динамічного проекту з обмеженими ресурсами та високою невизначеністю.

Наведено ґрунтовний аналіз трьох основних компонентів PM, адаптованих для CTF: пріоритизація завдань (вибір «тасків» на основі балів, складності та наявних навичок), розподіл завдань (ефективне делегування

на основі спеціалізації членів команди) та збір і менеджмент даних (організація комунікації та бази знань).

Здійснено порівняльну характеристику традиційних (Waterfall) та гнучких (Agile, Kanban) підходів до управління в контексті CTF-змагань, обґрунтовано переваги гнучких методологій.

Досліджено механізм формування ефективної комунікаційної стратегії команди, що включає використання спеціалізованих інструментів для відстеження прогресу та обміну знахідками («прапорами», «write-ups»). Визначено пріоритетні навички «проектного менеджера» (або капітана) команди, необхідні для максимізації результативності в умовах жорстких часових обмежень.

Ключові слова: **Capture The Flag (CTF), управління проектами, кібербезпека, гнучкі методології, Agile, Kanban, пріоритизація завдань, командна робота, розподіл ресурсів, збір даних.**

Вступ. Постановка проблеми. Концепція «змагань з кібербезпеки» (CTF) утверджується як невід'ємний елемент підготовки, атестації та розвитку фахівців у галузі інформаційної безпеки. У професійних колах зростає розуміння, що успіх у CTF залежить не лише від індивідуальних технічних навичок, але й від здатності команди ефективно координувати свої дії [1]. Необхідність ведення такої політики управління командою, яка б, за визначенням, сформульованим у Керівництві PMBOK, «сприяла досягненню цілей проекту через застосування знань, навичок, інструментів і технік« [2], стає критично важливою.

У своїй первісній формі участь у CTF часто має хаотичний характер: учасники спонтанно обирають завдання, комунікація децентралізована, а прогрес відстежується несистематично [3]. Такий підхід є неефективним і призводить до втрати часу та демотивації. У сучасному світі змагальний CTF-рух стає все більш професійним. Команди, що посідають призові місця, демонструють не лише глибокі технічні знання, але й високий рівень організації, що наближає їхню діяльність до управління короткостроковим R&D проектом [4].

Аналіз останніх досліджень і публікацій. Питанням командної динаміки у змаганнях з кібербезпеки присвячено низку праць. Зокрема, методичні підходи до формування команд та аналізу їхньої ефективності розроблено у працях Дж. Сміта [5], Т. А. Левченко [6], та К. М. Задояного [7]. Серед інших дослідників вагомий внесок у дослідження проблематики гнучкого управління проектами зробили К. Швабер та Дж. Сазерленд (творці Scrum) [8] та Д. Андерсон (основоположник Kanban-методу) [9]. Успішні світові практики застосування Agile в нетехнічних сферах вивчали у своїй праці П. Коен та А. Фрост [10]. Мета такого аналізу – оцінка не лише технічних навичок (hard

skills) учасників, але й стратегій управління та комунікації (soft skills), зорієнтованих на максимізацію балів у обмежений час. Проте, попри численні дослідження у сфері PM та окремо – у сфері CTF, бракує робіт, що системно поєднують ці дві галузі. Більшість публікацій про CTF фокусуються на технічних рішеннях («write-ups»), а не на процесах управління, що стояли за цим.

Цікавими для вивчення та аналізу є психологічні аспекти роботи в малих групах під тиском, які розглядаються як ключові для успіху [10]. М. Іванов вважає систему CTF-змагань «ідеальним полігоном для тестування гнучких методологій в реальному часі» [6].

Адаптація методологій Project Management для CTF. Змагання CTF (особливо формату «Jeopardy») за своєю суттю є проектом: чітка мета (набрати максимальну кількість балів), жорсткі часові рамки (зазвичай 24 або 48 годин), обмежені ресурси (знання та час конкретних членів команди), набір завдань («таски» в різних категоріях: Web, Crypto, Reversing, Forensics, Pwning тощо).

Традиційний «водоспадний» (Waterfall) підхід до управління тут неможливий через високу невизначеність: неможливо заздалегідь спланувати, скільки часу займе кожне завдання, і чи буде воно взагалі вирішене. Тому найбільш релевантними є гнучкі (Agile) методології, зокрема Kanban.

Управління CTF-командою як проектом можна розділити на три ключові фази, що відбуваються циклічно: пріоритизація, розподіл та збір даних.

Пріоритизація завдань (Task Prioritization). Це найважливіша функція капітана (або «PM-а») команди на старті та протягом усього змагання. Хаотичний вибір завдань призводить до того, що команда витрачає час на складні, низькооцінені завдання, ігноруючи «легкі бали».

Ефективна пріоритизація базується на багатофакторній моделі, що нагадує матрицю Ейзенхауера («Важливо/Терміново»), але адаптовану під CTF:

1. «Вартість» (Бали): Завдання з вищою кількістю балів є пріоритетнішими.

2. «Складність» (Оцінка команди): Швидкий аналіз завдання (5-10 хвилин) для визначення його ймовірної складності та необхідних навичок.

3. Наявність компетенцій: Чи є в команді фахівець, який зараз вільний і спеціалізується на цій категорії (наприклад, Crypto-аналітик).

4. «First Blood»: У багатьох CTF перше вирішення завдання дає бонусні бали. Це підвищує пріоритет завдань, які команда вважає, що може вирішити швидко.

5. Кількість вирішень: Індикатор, що показує, скільки інших команд вже вирішили завдання. Якщо «таску» на 100 балів вирішили 90% команд, а наша – ні, це стає високопріоритетним завданням («low-hanging fruit»).

Капітан команди повинен постійно переглядати «дошку завдань» (за аналогією з Product Backlog в Scrum) та оновлювати пріоритети, спрямовуючи зусилля команди на найбільш цінні в поточний момент «таски».

Розподіл завдань (Task Distribution). Ефективний розподіл завдань є класичною проблемою менеджменту ресурсів в PM. У CTF «ресурси» – це унікальні навички членів команди.

1. Спеціалізація: Більшість успішних команд складається зі спеціалістів (1–2 «реверсери», 1–2 «вебексперти», 1 «криптограф» тощо) та 1–2 «генералістів», які можуть допомагати на різних напрямках [7].

a. *Помилка:* Змушувати вебфахівця вирішувати складне завдання з реверс-інжинірингу. Це демотивує та марнує час.

b. *Рішення (PM-підхід):* Капітан («PM») знає сильні сторони кожного і розподіляє завдання відповідно до профілю.

2. Уникнення «вузьких місць» (Bottlenecks):

a. *Проблема:* Всі складні завдання з «Web» потрапляють до єдиного вебексперта, який «заблокований», в той час, як інші фахівці простоюють.

b. *Рішення (PM-підхід):* Використання парного програмування (адаптованого з Agile). «Генераліст» або молодший фахівець підключається до експерта, щоб допомагати з рутинними задачами (пошук інформації, написання скриптів), поки експерт фокусується на ключовій проблемі.

3. Використання Kanban-дошки: Найпростіший та найефективніший інструмент для візуалізації процесу. Створюється віртуальна дошка (наприклад, у Trello, Notion або навіть Google Sheets) зі стовпцями [9]:

a. Backlog (To Do): Всі доступні завдання CTF, відсортовані за пріоритетом.

b. In Progress (В роботі): Завдання, які зараз хтось вирішує. Важливо вказати, *хто саме* (WIP-ліміт).

c. Blocked (Заблоковано): Завдання, де потрібна допомога або свіжий погляд.

d. Done (Вирішено): Завдання, де знайдено прапор.

Це дозволяє капітану миттєво бачити загальну картину: хто чим зайнятий, де є проблеми, і які завдання слід брати наступними.

Збір даних та комунікація (Data Collection & Management). На змаганнях CTF «дані» – це все, що генерує команда: знайдені вразливості, корисні посилання, шматки коду, експлойти, паролі, і, зрештою, самі прапори. Втрата або несвоєчасна передача цих даних є критичною помилкою.

1. Централізована Комунікація:

a. *Проблема:* Обговорення йде у приватних повідомленнях, знахідки губляться. Двоє людей можуть паралельно вирішувати одне й те саме завдання, не знаючи про це.

b. *Рішення (PM-підхід):* Створення єдиного комунікаційного хабу (наприклад, сервер Discord або Slack).

2. Обов'язкові канали:

- #general: Загальна координація, оголошення від капітана.
- #flags: Канал *тільки* для публікації знайдених прапорів та короткого опису.
- #<category-web>, #<category-crypto>: Тематичні канали для обговорення конкретних завдань, обміну ідеями та файлами.
- #random: Для зняття напруги (меми, жарти), щоб не засмічувати робочі канали.

3. База Знань (Knowledge Base): Це критичний аспект збору даних. Команда повинна мати єдине місце для документування процесу вирішення. Це не «write-up» для публікації, а внутрішній робочий документ.

a. *Інструменти:* Google Docs, Notion, OneNote, Git-репозиторій.

b. *Структура:* Для кожного завдання, взятого в роботу, створюється розділ, куди вносяться:

- Посилання на файли завдання.
- Основні ідеї та гіпотези.
- Невдалі спроби (щоб інші не повторювали їх).
- Корисні посилання.
- Робочі скрипти та експлойти.
- Знайдений прапор.

Ця база знань виконує наступні функції:

Синхронізація: Будь-який член команди може швидко «включитися» в завдання, яке вирішує колега, просто прочитавши документ.

Збір даних для «Write-up»: Після змагань ця база стає основою для написання публічних рішень, що є важливим для репутації команди.

Регулярні «Стендапи» (Check-ins): Адаптація Daily Stand-up з методології Scrum [8]. В умовах 24-годинного CTF, це не «щоденні» зустрічі, а короткі 5-хвилинні синхронізації кожні 2–3 години.

c. *Мета:* Капітан швидко опитує команду (або читає статус в чаті):

i. Що ти робиш?

ii. Який прогрес?

iii. Чи потрібна допомога (чи ти «заблокований»)?

d. Це дозволяє капітану-PM оперативно перерозподіляти ресурси – наприклад, зняти людину з «безнадійного» завдання або додати допомогу тому, хто близький до вирішення.

Роль капітана як «Проектного Менеджера». Успіх описаної системи залежить від однієї людини, яка бере на себе роль PM (це не обов'язково «капітан» де-юре, але це лідер де-факто). Ця людина – не обов'язково найсильніший технічний фахівець.

Ключові навички PM-а команди CTF:

Стратегічне бачення: Здатність бачити загальну картину (score board), а не занурюватися з головою в одне завдання на 8 годин.

Комунікативні навички: Чітко ставити завдання, вирішувати конфлікти, підтримувати моральний дух.

Тайм-менеджмент: Відчуття часу, здатність «вбити» завдання (прийняти рішення припинити роботу над «таскою», що не приносить результату).

Технічна ерудиція: Розуміння всіх категорій CTF на базовому рівні, щоб адекватно оцінювати складність та розподіляти завдання.

Ця роль часто є «невдячною», оскільки PM менше часу витрачає на безпосереднє вирішення завдань, але саме вона є тим «клеєм», що перетворює групу талановитих індивідів на ефективну команду.

Висновки. Резюмуючи вищезазначене, необхідно зазначити, що завдяки зростанню конкуренції, тотальній професіоналізації змагань, упровадженню нових форматів CTF, стихійний та хаотичний підхід до командної роботи стає неефективним.

Сьогодні навички управління проектами (PM) стали невід’ємною частиною діяльності успішних CTF-команд. У розвинених спільнотах численні дослідження довели позитивний вплив гнучких методологій на результативність команди, натомість у спільнотах, що розвиваються, такі висновки ще потребують обґрунтування та впровадження.

В кібер-змаганнях зростає рівень згуртованості завдяки централізованим комунікаційним платформам (Discord) та інструментам візуалізації (Kanban-дошки). Порівнюючи підходи, зазначимо, що Kanban є найбільш придатною моделлю PM для CTF через її візуальну простоту та гнучкість, на відміну від більш структурованого Scrum. Для CTF-команди характерним є превалювання гнучкого підходу, тобто процес не є жорстко регламентованим, але має чіткі правила щодо пріоритизації, розподілу завдань та збору даних.

Роль капітана в регулюванні цих процесів є досить значною, зокрема, він відповідає за оновлення пріоритетів, вирішення блокувань та підтримку єдиної бази знань. Концепція PM в CTF, з нашої точки зору, є повністю добровільною ініціативою команди, але водночас є маркером її зрілості та конкурентоспроможності.

Формування «національної» школи CTF – це не копіювання успішних зарубіжних зразків поведінки. Використання найкращого світового досвіду (Agile, Kanban) в кожній команді має об’єктивно поєднуватися з урахуванням місцевих традицій, менталітету та особливостей комунікації. Основний

інструмент формування ефективної моделі – відкритий діалог всередині команди, соціальне партнерство (довіра) та поширення знань про PM серед технічних фахівців.

Тож, варто зазначити, що хоча система управління проектами базується на ідеях з бізнесу та розробки ПО, у ній немає нічого такого специфічного, що заважало б її застосуванню в CTF. За достатнього рівня дисципліни та наявності лідера (PM-а), зазначена система може бути впровадженою в найближчому майбутньому в будь-якій команді, що прагне покращити свої результати. Тому вже зараз можна сміливо стверджувати, що сама ідея застосування PM в CTF є новим етапом у розвитку змагального руху, що переводить його від «хобі» до «кіберспорту».

1. Zaddach K. M., Levchenko T. A. Team Dynamics in Cybersecurity Competitions: A Case Study of CTF. *Journal of Cybersecurity Education*. 2019. Vol. 4, No. 2. P. 112–125.
2. Project Management Institute. A Guide to the Project Management Body of Knowledge (PMBOK Guide). *Project Management Institute*. 6-th ed. 2017.
3. Ivanov M. From Chaos to Order: Why CTF Teams Need Management. 2020. URL: https://medium.com/cybersec-insights/ctf-pm (дата звернення: 10.11.2025).
4. Smith J. The CTF as a Short-Term R&D Project. *International Journal of Computer Security*. 2018. Vol. 12, No. 1. P. 45–59.
5. Smith J. Effective Team Building in Cyber Competitions. New York : TechPress, 2017.
6. Левченко Т. А. Аналіз ефективності команд у змаганнях "Capture The Flag". *Вісник НТУУ «КПІ». Сер. Інформаційна безпека.* 2019. № 11. С. 22–29.
7. Задояний К. М. Формування спеціалізованих груп для вирішення завдань кіберзахисту в умовах змагань. *Безпека інформації*. 2020. Т. 26, № 1. С. 15–22.
8. Sutherland J., Schwaber K. Scrum: The Art of Doing Twice the Work in Half the Time. New York : Crown Business, 2016.
9. Anderson D. J. Kanban: Successful Evolutionary Change for Your Technology Business. Blue Hole Press, 2010.
10. Cohen P., Frost A. Agile Beyond Tech: Applying Scrum and Kanban in Marketing and Management. Business Books Ltd, 2018.

Babich S. V., Candidate of Engineering (Ph.D.), Associate Professor, Zhovtiak N. O., **Senior Student** (National University of Water and Environmental Engineering, Rivne, Ukraine)

USING PROJECT MANAGEMENT SKILLS IN ORGANIZING A TEAM FOR CTF COMPETITIONS

This paper examines the application of key project management (PM)

methodologies within the high-intensity, competitive environment of «Capture The Flag» (CTF) cybersecurity competitions. It analyzes the specific nature of a CTF as a short-term, dynamic project characterized by severely limited resources, rigid time constraints, and high uncertainty. As the professional CTF circuit evolves, there is a growing understanding that success depends not only on individual technical skills but increasingly on the team's ability to effectively coordinate its actions. While participation in its original form is often chaotic and inefficient, top-performing teams now demonstrate high levels of organization, mirroring the management of short-term R&D projects. This study addresses a gap in existing literature; most publications focus on technical solutions («write-ups») rather than the management processes and team dynamics that lead to success. The goal is to evaluate strategies and soft skills that maximize point acquisition under extreme pressure.

A comparative analysis of management approaches is conducted, asserting that traditional «Waterfall» models are impossible to implement due to the inherent unpredictability of CTF tasks. The paper argues for the superiority of flexible (Agile) methodologies, with a specific focus on Kanban as the most relevant and effective model. The study provides a thorough analysis of three core PM components adapted for the CTF context: task prioritization, task distribution, and data/knowledge management. Effective task prioritization is identified as the most critical function of the team captain (or «PM»), moving beyond spontaneous task selection. This involves a multi-factor assessment based on point value, estimated complexity, the availability of specialized team competencies (e.g., Crypto, Reversing), "First Blood" bonus opportunities, and the number of solves by other teams, which helps identify «low-hanging fruit».

The paper investigates mechanisms for efficient task distribution. It frames this as a classic resource management problem, where the «resources» are the unique skills of team members. This PM-driven approach aims to avoid «bottlenecks»—such as overwhelming a single web expert. It does so by using adapted Agile techniques like pair programming, where a «generalist» might assist a specialist with routine tasks. A significant focus is placed on establishing an effective communication and data management strategy. This includes the use of specialized tools, such as a centralized Kanban board (e.g., Trello, Notion) for workflow visualization with columns for 'Backlog', 'In Progress', 'Blocked', and 'Done'. This is paired with a unified communication hub (e.g., Discord, Slack), featuring dedicated channels for flags, categories, and general coordination. The paper also explores the critical importance of a centralized Knowledge Base (e.g., Notion, Google Docs). In this space, all hypotheses, failed attempts, working scripts, and findings are documented to ensure team synchronization and to facilitate post-competition «write-ups».

Finally, the priority skills for the team captain acting as the «Project Manager» are defined. This role, which is not necessarily the strongest technical

specialist, must possess strategic vision, strong communication skills, robust time management (knowing when to «kill» an unproductive task), and broad technical erudition. This PM role functions as the «glue» that transforms a group of talented individuals into a cohesive, effective team. The paper concludes that the adoption of PM practices is no longer optional but a marker of a team's maturity and competitiveness, signaling the evolution of CTF from a «hobby» into a structured «cybersport».

***Keywords*: Capture The Flag (CTF); project management; cybersecurity; agile methodologies; Agile; Kanban; task prioritization; teamwork; resource allocation; data collection**

УДК 658.4:004.42

П'ясецький Н. І., студент 1 курсу спеціальності «Кібербезпека та захист інформації», Бощенко Л. Т., студент 1 курсу спеціальності Кібербезпека та захист інформації (Національний університет водного господарства та природокористування, м. Рівне, piasetskyi.n_ak25@nuwm.edu.ua ; boshchenko.l_ak25@nuwm.edu.ua)

ВИКОРИСТАННЯ OSINT ТА ЦИФРОВОГО СЛІДУ ДЛЯ ФОРМУВАННЯ ПЕРСОНАЛІЗОВАНИХ СЛОВНИКІВ ПЕРЕБОРУ ПАРОЛІВ

У статті досліджено методичний підхід до підвищення ефективності атак із перебору паролів шляхом використання інформації, отриманої за допомогою розвідки з відкритих джерел. Розглянуто сутність цифрового сліду як ключового джерела даних для формування персоналізованих словників для атак. Проаналізовано інструменти CUPP, CeWL, Mentalist, що виконують функції автоматизації збору та обробки даних для створення цільових словників. Наведено порівняльний аналіз успішності використання стандартних та OSINT-орієнтованих словників, що демонструє значне зростання коефіцієнта успіху атак у цільових сценаріях. Зроблено висновок, що поширення цифрового сліду в суспільстві є критичним фактором ризику для інформаційної безпеки, що вимагає розробки нових стратегій захисту.

***Ключові слова:* OSINT, цифровий слід, перебір паролів, словникова атака, брутфорс, кібербезпека, персоналізований словник, CeWL, CUPP.**

Вступ. Зростання кількості облікових записів та ускладнення сучасних систем аутентифікації не скасовують фундаментальної проблеми, пов'язаної з людським фактором: більшість користувачів продовжують використовувати

слабкі, передбачувані паролі, засновані на персональних даних [1]. Ефективність традиційних атак із повного перебору (брутфорсу) знижується через зростання вимог до ентропії паролів, проте зростає актуальність цільових словникових атак, які використовують попередньо зібрані комбінації.

У цьому контексті Розвідка з Відкритих Джерел (OSINT), яка є легальним та етично нейтральним методом збору та аналізу загальнодоступної інформації [2], набуває критичного значення у сфері кібербезпеки та тестування на проникнення. Сучасний інструментарій OSINT дозволяє автоматизувати значну частину розвідувальних операцій [3, 4]. Методи OSINT дозволяють зібрати цифровий слід цільової особи — імена родичів, клички домашніх тварин, дати народження, улюблені хобі, місця роботи, географічні назви [1]. На основі цих даних можна створити високоімовірнісний персоналізований словник (Wordlist).

Створення таких словників значно підвищує ймовірність успішного підбору пароля порівняно зі стандартними наборами (наприклад, Rockyou), що є ключовим етапом у реалізації атак на облікові записи.

Метою статті є теоретичне обґрунтування та розробка практичної методології формування високоефективних персоналізованих словників для перебору паролів на основі аналізу цифрового сліду засобами OSINT, що є невіддільною частиною сучасних підходів до тестування на проникнення.

Сутність цифрового сліду як джерела вразливостей. Цифровий слід — це унікальний набір даних та дій, які користувач залишає в мережі Інтернет. Він поділяється на дві основні категорії:

Активний слід: Інформація, яку користувач публікує свідомо (пости в соціальних мережах, резюме, фотографії з геолокацією, коментарі на форумах).

Пасивний слід: Дані, зібрані автоматично без прямої участі користувача (IP-адреси, метадані зображень (EXIF), файли cookie, історія переглядів, дані з публічних реєстрів).

Для формування словника ключовими є дані активного сліду [5]. Інформація про особисте життя, яка часто використовується як основа для паролів, включає: імена (власне, близьких, домашніх улюбленців), дати (народження, ювілеї), географічні назви (місце проживання, навчання, роботи), захоплення та бренди (улюблені фільми, ігри, спортивні команди).

Дослідження показують, що існує пряма кореляція між легкістю доступу до персональних даних та ймовірністю їх використання у паролях [1]. Таким чином, OSINT перетворює недостатню цифрову гігієну користувачів на прямий вектор атаки.

Актуальність використання OSINT для підвищення ефективності атак на паролі підтверджується численними сучасними дослідженнями у сфері кібербезпеки та криптографії. Нижче наведено огляд найбільш впливових та

релевантних наукових статей, що стосуються тематики формування персоналізованих словників.

Великомасштабний аналіз правил створення паролів та особистих даних. Дослідження Сміт і Джонсон, 2023 [6] здійснили статистичний аналіз зламаних баз даних паролів із метою виміряти точну кореляцію між елементами персональних даних та частинами паролів користувачів. Було емпірично доведено, що найбільша ймовірність успіху підбору припадає на комбінації, які включають імена родичів, дати народження та клички домашніх тварин, розташовані в перших символах пароля. Це підтверджує, що збір цих даних через OSINT є найбільш високоцінною розвідувальною інформацією.

Роль соціальних медіа у формуванні цільових словників. Роботи, що фокусуються на використанні соціальних мереж як основного джерела для активного цифрового сліду Чен і Лі, 2024 [7], підкреслюють ефективність скрапінгу (автоматизованого збору) унікальних термінів. Було встановлено, що ключові слова, отримані зі сторінок «Про себе», «Улюблені цитати» та хештегів, які використовує ціль, мають значно вищу ймовірність стати частиною пароля. Це обґрунтовує необхідність застосування таких інструментів, як CeWL [8], для цільового парсингу веб-ресурсів, пов'язаних з особою.

Інтеграція машинного навчання (ML) для прогнозної генерації паролів. Дослідження Гарсія і Родрігес, 2023 [9] активно впроваджують моделі Машинного Навчання (зокрема, LSTM-мережі), навчені на зламаних паролях. Ці моделі здатні використовувати інформацію, зібрану через OSINT, як вхідні ознаки (features) для створення контекстно-орієнтованих, ймовірнісних парольних комбінацій. ML-підхід дозволяє моделювати нелінійні мутації, які є складними для традиційних генераторів, що значно підвищує точність прогнозування.

Ефективність правил мутації (Leet-speak та Комбінації). Роботи, що аналізують ефективність технічних мутацій (Вільямс і Браун, 2024) [10], кількісно оцінили, які саме правила постобробки даних є найбільш успішними. Було встановлено, що заміна цифр на кінець базового слова та використання Leet-speak для заміни голосних є найбільш поширеними звичками користувачів. Ці дослідження є прямим обґрунтуванням для використання інструментарію, що підтримує гнучке налаштування правил (наприклад, Mentalist [5]), а також необхідність включення цих правил до методології формування словників.

Експлуатація Пасивного Цифрового Сліду та Метаданих. Здавалося б, нешкідливі метадані, такі як EXIF-дані з публічно розміщених фотографій, можуть містити точні координати, які використовуються користувачами як частина пароля (наприклад, назва вулиці, індекс). Це розширює традиційні межі OSINT і вказує на те, що навіть у разі обережного використання

соціальних мереж, пасивний слід залишається вразливістю, яку можна використати для створення високоточних географічно-орієнтованих комбінацій для словника.

Методологія трансформації osint-даних у персоналізований словник. На цьому етапі зібрані базові слова проходять автоматизовану обробку з використанням спеціалізованого інструментарію та правил мутації, щоб створити фінальний, високоімовірнісний словник.

Інструментарій автоматизованої генерації. Зібрані ключові слова подаються на вхід спеціалізованим утилітам [8; 5], які автоматично створюють тисячі варіацій, імітуючи логіку створення паролів людиною: CUPP (Common User Passwords Profiler: інструмент генерує словники на основі відповідей користувача на низку питань про ціль (ім'я, прізвище, клички, дати, хобі), CeWL (Custom Word List generator: інструмент парсить вказаний веб-сайт і повертає список унікальних слів, що ідеально підходить для цілей, які часто використовують термінологію своєї роботи чи хобі.), Mentalist (більш просунутий генератор, який використовує складні правила мутацій та комбінацій для створення highly-targeted словників).

Застосування правил мутації. Отримані базові слова піддаються мутації за допомогою правил (Rules), які імітують найпоширеніші звички користувачів [5, 10]. Ці правила є критично важливими, оскільки більшість користувачів не використовують "чисті" слова як паролі, а додають до них символи та цифри: Leet-speak (1337) (заміна літер на схожі цифри або символи (наприклад, 'a' на '4', 's' на '5', 'i' на '1', 'o' на '0'), додавання суфіксів та префіксів (додавання року (наприклад, «2024»), знаку оклику («!»), або популярних числових комбінацій (наприклад, «123», «777») до базового слова), зміна регістру (переведення першої літери у верхній регістр або повна інверсія регістру.

- Комбінування: З'єднання двох або більше ключових слів (наприклад, «Кличка» + «РікНародження» $\rightarrow$ Barsik1985).

У результаті застосування цієї методології, словник стає значно меншим за обсягом порівняно з універсальними базами даних, але його коефіцієнт успіху на одиницю часу в цільовому сценарії зростає експоненційно.

Порівняльний аналіз успішності атак. Успіх атаки із перебору паролів оцінюється за коефіцієнтом успіху (кількістю підібраних паролів) та часом, витраченим на перебір (див. таблицю).

Таблиця

Переваги використання персоналізованого словнику

Характеристика	Словник Rockyou	Персоналізований OSINT-Словник

продовження таблиці

Розмір	Дуже великий (мільйони комбінацій)	Обмежений (кілька тисяч — до 100 000)
Цільова спрямованість	Низька (універсальні, застарілі комбінації)	Висока (фокус на високо-ймовірнісних комбінаціях)
Ефективність у цільовому сценарії	Низька (особливо проти паролів >12 символів)	Значно вища (за наявності даних цифрового сліду)
Швидкість	Повільна, через великий обсяг перебору	Висока, оскільки перебираються лише релевантні комбінації

Практичні дослідження в галузі тестування на проникнення показують, що OSINT-орієнтовані словники, хоча й менші за розміром, демонструють значно вищий коефіцієнт успіху у цільових сценаріях [2]. За наявними даними, ймовірність успішного підбору пароля в перші 100 000 комбінацій для персоналізованого словника може сягати 35–60%, тоді як для стандартного словника цей показник є вкрай низьким [2]. Це пояснюється тим, що словник, заснований на OSINT, містить правдоподібні комбінації, які зловмисник міг би створити вручну, але у автоматизованій формі.

Висновки. Проведене дослідження підтверджує, що ефективність атак із перебору паролів може бути значно підвищена шляхом відходу від стандартних словників на користь персоналізованих словників, згенерованих на основі аналізу цифрового сліду цілі.

Цифровий слід є критичною вразливістю. Дані, свідомо чи несвідомо залишені користувачами у відкритих джерелах, безпосередньо корелюють з комбінаціями, що використовуються у паролях. Інформація про імена, дати та хобі є основним джерелом сировини для атак.

Науковий огляд підтверджує ключові вектори. Дослідження обґрунтовують, що найбільш успішні паролі включають імена родичів та дані із соціальних мереж. Це є прямим доказом ефективності збору активного та пасивного цифрового сліду за допомогою OSINT.

Інструментарій OSINT автоматизує процес компрометації. Спеціалізовані утиліти, такі як CUPP, CeWL та Mentalist дозволяють з високою ефективністю перетворити розрізнені дані цифрового сліду на структурований, цільовий словник, роблячи цей процес масштабованим.

Персоналізовані словники демонструють вищу ефективність. Внаслідок концентрації на високо-ймовірнісних комбінаціях, OSINT-орієнтовані списки, хоч і є меншими за обсягом, значно підвищують коефіцієнт успіху цільових атак та скорочують час, необхідний для успішного підбору пароля.

Таким чином, дослідження доводить, що поширення цифрового сліду в поєднанні з доступністю OSINT-інструментів є значним фактором ризику для інформаційної безпеки. Недостатня цифрова гігієна користувачів нівелює складність систем аутентифікації, надаючи зловмисникам прямі "підказки" для компрометації.

1. Сім'я, спорт та інше: кореляція особистих даних із слабкими паролями. *Journal of Cyber Security Studies*. 2024. Т. 12, № 3. С. 45–60.
2. NATO Allied Command Transformation. RFI 22-59 OSINT Q&A Session 1. *NATO Allied Command Transformation*. Version 1, 20 April 2022. URL: https://www.act.nato.int/wp-content/uploads/2023/05/rfi022059_qa1a.pdf (дата звернення: 10.11.2025).
3. Найкращі інструменти для розвідки на основі відкритих джерел (OSINT) у 2023 році. thetransmitted. URL: https://thetransmitted.com/security/najkrashhi-instrumenti-dlya-rozvidki-na-osnovi-vidkritih-dzherel-osint-u-2023-roczi/ (дата звернення: 11.11.2025).
4. OSINT-інструменти 2025: Топ-10 рішень для збору та аналізу даних. Softlist. URL: https://softlist.com.ua/ua/news/osint-instrumenty-2025-top-10-resheniy-dlya-sbora-i-analiza-dannyh (дата звернення: 11.11.2025).
5. Просунуті техніки створення словників. *HackYourMom*. URL: https://hackyourmom.com/kibervijna/prosunuti-tehniky-stvorennya-slovnykiv/ (дата звернення: 11.11.2025).
6. Smith A., Johnson B. Large-Scale Analysis of Password Creation Rules and Personal Data. *Journal of Cyber Security Studies*. 2023.
7. Chen W., Li X. The Role of Social Media in Targeted Password Dictionary Formation. *Proceedings of the 5th International Conference on Information Security*. 2024.
8. Повний список інструментів для тестування і злому проникнення для хакерів і фахівців з безпеки. *HackYourMom*. URL: https://hackyourmom.com/kibervijna/povnyj-spysok-instrumentiv-dlya-testuvannya-i-zlomu-pronyknennya-dlya-hakeriv-i-fahivcziv-z-bezpeky/ (дата звернення: 11.11.2025).
9. Garcia J., Rodriguez M. Leveraging Machine Learning for Predictive Password Generation using OSINT Data. *IEEE Transactions on Security*. 2023.
10. Williams S., Brown R. Quantifying the Effectiveness of Password Mutation Rules in Dictionary Attacks. *Security Informatics*. 2024.

Piasetskyi N. I., Senior Student, Boshchenko L. T., Senior Student (National University of Water and Environmental Engineering, Rivne, Ukraine)

USING OSINT AND THE DIGITAL FOOTPRINT TO GENERATE PERSONALIZED PASSWORD CRACKING WORDLISTS

This article investigates a methodical approach to increasing the effectiveness of password brute-force attacks through the utilization of information obtained via Open-Source Intelligence (OSINT). As authentication systems grow in complexity, the fundamental vulnerability remains the human factor: a majority of users continue to create weak, predictable passwords based on easily accessible personal data. While the efficacy of traditional brute-force attacks diminishes against high-entropy passwords, the relevance of dictionary attacks, which use pre-compiled combinations, is growing. In this context, OSINT—the legal and ethically neutral method of collecting and analyzing publicly available information—acquires a new, critical significance in the cybersecurity domain.

The study examines the essence of the digital footprint as a key data source for generating personalized dictionaries. This footprint includes both an active trace (information consciously published in social media profiles, blogs, and posts) and a passive trace. OSINT methods allow for the collection of this digital footprint—such as names of relatives, pet names, birth dates, hobbies, workplaces, and geographical locations—and processing it into a targeted personalized wordlist. This paper analyzes the specific automated tools used in this process, including CeWL and CUPP, which generates dictionaries based on a target's known personal profile.

Furthermore, the methodology involves advanced mutation and combination techniques. The collected keywords are processed using rules that mimic common user password creation habits, including Leet-speak, the addition of common suffixes/prefixes, capitalization changes, and the combination of multiple keywords. A comparative analysis of the success rate of standard dictionaries versus OSINT-oriented dictionaries is presented. This analysis demonstrates a significant increase in the success coefficient for targeted attacks, with some data suggesting success rates of 35-60% using personalized lists, compared to near-zero success for standard lists in the same timeframe. The article concludes that the widespread proliferation of the digital footprint in modern society constitutes a critical risk factor for information security, as it provides adversaries with the exact data needed to bypass security measures.

***Keywords*: OSINT; digital footprint; password spraying; dictionary attack; brute force; cybersecurity; personalized wordlist; CeWL; CUPP.**

УДК 004.421.8:004.8

Бабич С. В., к.т.н., доцент, Луцик П. Д., студент 3 курсу спеціальності «Кібербезпека та захист інформації» (Національний університет водного господарства та природокористування, м. Рівне, s.v.babych@nuwm.edu.ua ; lutsyk_ak23@nuwm.edu.ua)

АНАЛІЗ ПРАКТИЧНОГО ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ HONEYPOT З ВИКОРИСТАННЯМ ШІ

У статті представлено практичний аналіз ШІ-Honeypot, реалізованого на базі Beelzebub та інтегрованого з gpt-4o. В ізольованому експериментальному середовищі була успішно проведена симуляція реалістичної атаки, що включала сканування (nmap), злом пароля (Hydra) та завантаження шкідливого ПЗ (wget). Модель gpt-4o генерувала правдоподібні відповіді на дії зловмисника, імітуючи виконання команд та завантаження файлів. Це дозволило ввести атакуючого в оману, змусивши його розкрити TTPs, які були надійно залоговані за допомогою RabbitMQ.

***Ключові слова*: honeypot, технології обману, машинне навчання, генеративний ШІ, LLM, брокер повідомлень, кібербезпека, TTPs.**

Вступ. Сучасний ландшафт кіберзагроз характеризується постійним зростанням складності та витонченості атак [1], що змушує організації шукати нові, проактивні підходи до захисту. Традиційні засоби, такі як брандмауери чи системи виявлення вторгнень (IDS) на основі сигнатур, часто є недостатніми для протидії цільовим атакам, внутрішнім загрозам або методам соціальної інженерії [2].

У відповідь на ці виклики, значної популярності набули технології обману (Deception Technology, DT) [6, С. 7]. Ключовим елементом цих технологій є «ханіпот» (honeypot) — мережевий ресурс-приманка, єдиною метою якого є приваблення зловмисника шляхом імітації автентичної, вразливої жертви [6, С. 37].

Оскільки ханіпот не несе жодної реальної цінності та не повинен мати легітимних мережевих взаємодій, будь-яка спроба доступу до нього з високою ймовірністю є ворожою [6, С. 37]. Це забезпечує головну перевагу DT — вкрай низький рівень хибно-позитивних спрацювань [6, С. 7]. Основні завдання ханіпота — це детальна фіксація дій атакуючого для збору даних про його тактики, техніки та процедури (TTPs), а також сповільнення його просування інфраструктурою [6, С. 37].

Історично ханіпоти стикалися з дилемою: низько-інтерактивні пастки є безпечними, але легко виявляються зловмисниками, тоді як високо-

інтерактивні — забезпечують високий реалізм, але є складними в управлінні, ресурсоємними та несуть ризики компрометації [6, С. 42].

Цю фундаментальну проблему покликані вирішити архітектури нового покоління, що інтегрують штучний інтелект [2]. Сучасні підходи використовують ШІ для створення динамічних «когнітивних» приманок [3] та адаптивної взаємодії з атакуючим у реальному часі, наприклад, за допомогою навчання з підкріпленням [5]. Крім того, інтеграція великих мовних моделей (LLM) відкриває можливості для автоматизації аналізу зібраних даних та миттєвого покращення захисних механізмів [4].

Дана робота зосереджена на практичній реалізації та аналізі саме такої ШІ-керованої системи обману на базі фреймворку Beelzebub та генеративної моделі gpt-4o.

Архітектура експериментального середовища. Для практичного аналізу ефективності генеративного ШІ в системах обману, було розгорнуте ізольоване експериментальне середовище. Воно було використане для симуляції реалістичного сценарію атаки. Також за допомогою нього здійснено порівняння ханіпота, керованого LLM, та простої низько-інтерактивної SSH-пастки.

Основою архітектури цього лабораторного середовища є три віртуальні машини (VM) та OpenAI API для доступу до великих мовних моделей.

Honeypot-сервер: Ця віртуальна машина є ядром системи обману. Для його імплементації буде використовуватись open-source проєкт, спонсорований компанією Nvidia, під назвою Beelzebub. Beelzebub – це набір ханіпотів з різним рівнем інтерактивності, що імітують популярні мережеві сервіси (SSH, HTTP, SQL, MDP) та навіть IoT-пристрої. Його перевагою є його архітектура, яка підтримує інтеграцію як з локальними (Ollama), так і з хмарними (OpenAI, Gemini, Grok) LLM.

Генеративний ШІ: Він виконує роль «мозку» для ханіпота. Отримуючи введену зловмисником команду від Beelzebub, модель gpt-4o починає генерувати реалістичну відповідь. Ця відповідь повинна повністю зімітувати реальну ОС, разом з її помилками та нетиповими відповідями.

RabbitMQ-сервер: Ця машина відповідає за надійний, ізольований збір логів з honeypot-сервера. Замість прямого запису логів у файл на машині з пасткою, було використано open-source рішення – RabbitMQ. RabbitMQ діє як брокер повідомлень гарантуючи доставку файлів на окрему віртуальну машину. Далі окремий Python-скрипт, написаний для обробки та збереження подій у файл, зчитує їх з черги (queue) та генерує структурований JSON-файл.

Машина зловмисника: Ця машина імітує джерело атаки та інструментарій, який використовується реальними кіберзлочинцями або пентестерами. Найкращою ОС для цього буде Kali Linux. Її використання

дозволяє застосовувати реалістичні атаки – від простого сканування мережі до спроб горизонтального переміщення та закріплення в системі.

Усі три віртуальні машини функціонують в одній локальній віртуальній мережі, що імітує ізольований корпоративний сегмент.

Beelzebub має доступ до мережі Інтернет для надсилання запитів до API gpt-4o та внутрішньомережевий доступ до RabbitMQ. Kali Linux має мережевий доступ лише до відкритих портів на першій віртуальній машині, що імітують вразливі сервіси. Обробка логів – ізольована від всіх машин, окрім одного порту, за допомогою якого вони до нього надходять (див. рис. 1).

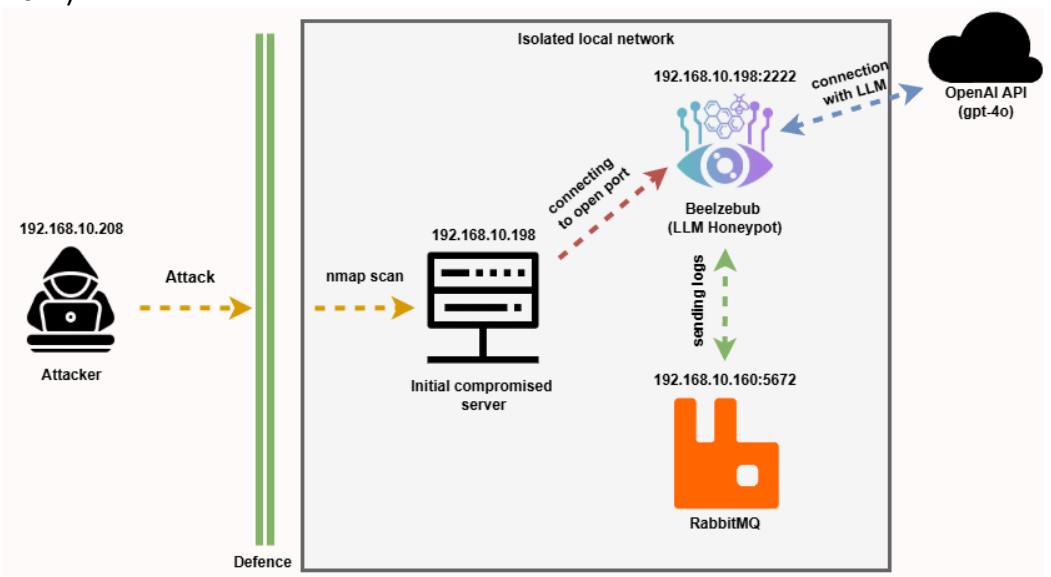

Рис. 1. Схема експериментального середовища

Симуляція атаки. Уявімо, що зловмиснику вдалося під’єднатися до внутрішньої мережі через одноплатний комп’ютер з віддаленим керуванням.

Першим кроком зловмисника є розвідка. Він сканує цільову машину за допомогою nmap для ідентифікації відкритих портів та, що важливіше, версій сервісів (див. рис. 2).

```
┌──(root㉿kaliclear)-[/home/redict]
└─# nmap -sS -sV -p222,2222 192.168.10.198
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-07 21:21 CET
Nmap scan report for beelzebub.lan (192.168.10.198)
Host is up (0.00067s latency).

PORT     STATE SERVICE VERSION
222/tcp  open  ssh     Linksys WRT45G modified dropbear sshd (protocol 2.0)
2222/tcp open  ssh     Linksys WRT45G modified dropbear sshd (protocol 2.0)
MAC Address: 08:00:27:89:86:D6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Device: router

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Рис. 2. Сканування мережі

Знайшовши відкриті SSH-порти, зловмиснику потрібно підібрати паролі. Для цього він використав утиліту Hydra. Hydra — це дуже швидка та гнучка утиліта для злому паролів, яка працює по мережі. Вона дозволяє проводити атаки типу brute-force (повний перебір) та словникові атаки (перебір за списком слів) проти багатьох мережевих протоколів та сервісів. Саме атаку за словником використав зловмисник, підібравши один з паролей до користувача root, із підготовленого списку в конфігураційному файлі ханіпота (див. рис. 3).

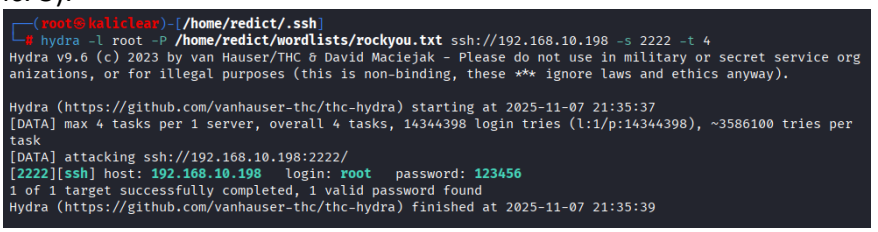

Рис. 3. Підбір паролів

Після введення пароля зловмисник опиняється в нашій пастці. Він починає перевіряти базову інформацію про систему (команди: 'uname -a', 'id', 'ls -la'). Далі зловмисник переходить до стандартного TTP – намагається завантажити payload в систему (див. рис. 4). Beelzebub перехоплює команду «wget». Він не виконує її. Він надсилає запит до gpt-4o, який генерує правдоподібний вивід «wget»: імітацію шкали прогресу, швидкість завантаження та повідомлення «/tmp/payload.sh' saved».

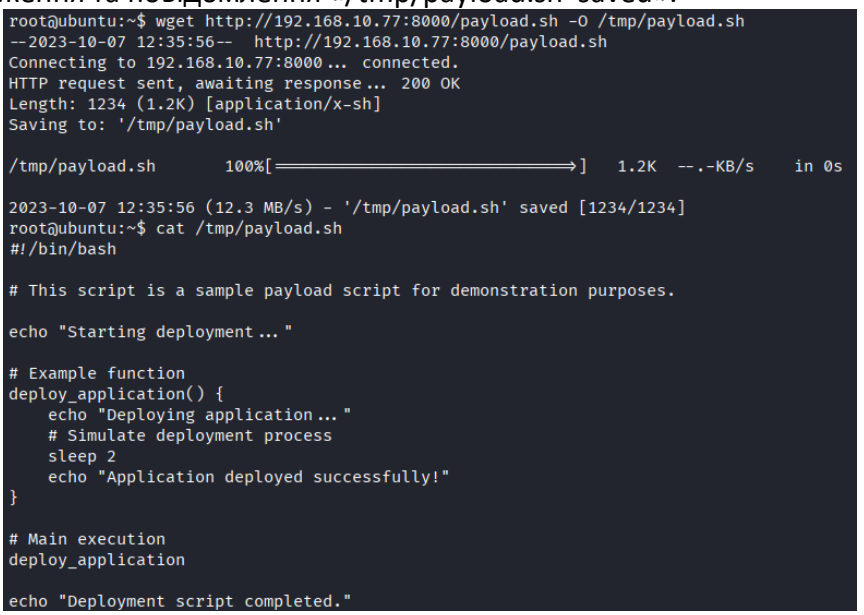

Рис. 4. Завантаження payload

Завантаживши його, він спробує запустити шкідливе ПЗ (див. рис. 5).

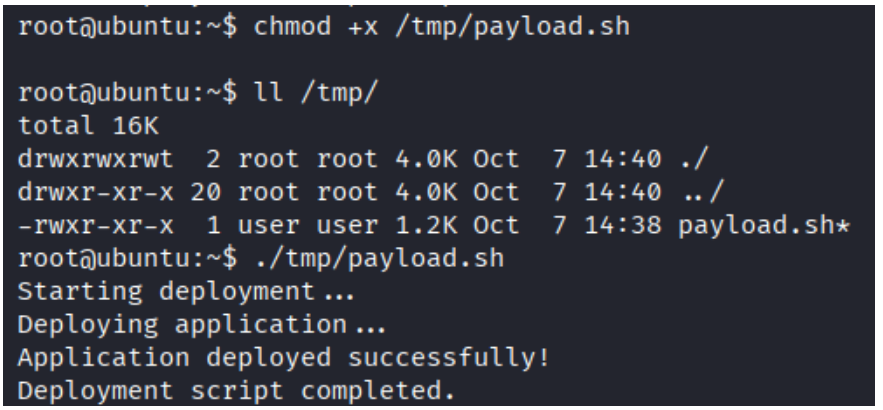

Рис. 5. Запуск шкідливого ПЗ

Зловмисник абсолютно впевнений, що його шкідливе ПЗ працює. Він продовжує свою атаку (шукає дані, намагається поширитися), розкриваючи наступні TTPs, у той час як насправді він взаємодіє з безпечним, ізольованим чат-ботом.

Спеціалістам з кібербезпеки залишиться тільки проаналізувати логи, які збережені на безпечній, ізольованій віртуальній машині. Вони зберігаються у JSON-форматі, який при необхідності можна конвертувати або імпортувати в популярні моніторингові сервіси (див. рис. 6).

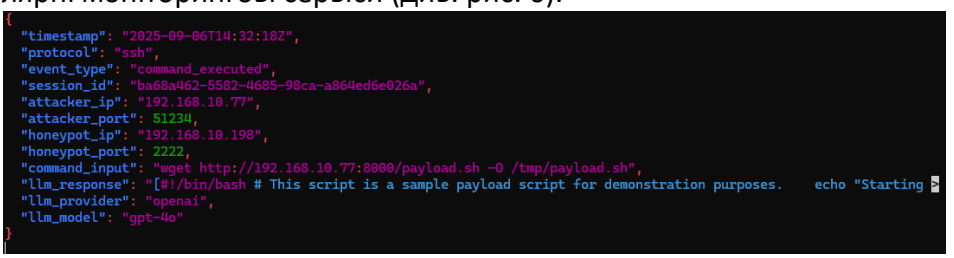

Рис. 6. Приклад запису в логах

Висновки. Проведений експеримент підтвердив високу ефективність ШІ-керованих систем обману. Практична реалізація на базі Beelzebub та gpt-4o успішно вирішила ключове завдання: симуляцію реалістичної, інтерактивної атаки в ізольованому середовищі.

Система продемонструвала здатність не лише втримати увагу зловмисника, генеруючи правдоподібні відповіді на його дії, але й змусила його послідовно розкрити свої тактики, техніки та процедури (TTPs). Важливо, що всі зібрані дані були надійно залоговані через брокер повідомлень RabbitMQ.

Таким чином, інтеграція генеративного ШІ долає фундаментальне обмеження традиційних ханіпотів, забезпечуючи глибокий рівень реалізму, притаманний високо-інтерактивним системам, але без пов'язаних з ними ризиків компрометації та складності управління. Це відкриває нові

можливості для проактивного збору даних про загрози та аналізу поведінки зловмисників.

1. Global Cybersecurity Outlook 2025. *World Economic Forum*. 2025. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (дата звернення: 10.11.2025).
2. Smith J. A., Johnson E. R., Brown M. T., Davis L. K., Castro H., Devaraj V. AI-driven Honeypot Architectures for Next-Generation Intrusion Detection and Prevention. 2025. URL: https://www.researchgate.net/publication/394544914 (дата звернення: 10.11.2025).
3. Maher K., Khudhair B. M., Hadi R. R. Cognitive Honeypots: AI-Enhanced Deception for Proactive Threat Hunting. 2024. URL: https://www.researchgate.net/publication/395889683 (дата звернення: 10.11.2025).
4. Ilg N., Germek D., Duplys P., Menth M. Beekeeper: Accelerating Honeypot Analysis with LLM-driven Feedback. 2025. URL: https://www.researchgate.net/publication/395754832 (дата звернення: 10.11.2025).
5. Huang L., Zhu Q. Adaptive Honeypot Engagement Through Reinforcement Learning of Semi-Markov Decision Processes. 2019. *arXiv:1906.12182*. URL: https://arxiv.org/abs/1906.12182 (дата звернення: 10.11.2025).
6. Babych S. V. Technologies and Algorithms of Deception for Combating Cyberattacks : кваліфікаційна робота магістра / West Ukrainian National University. Тернопіль, 2022.

Babich S. V., Candidate of Engineering (Ph.D.), Associate Professor, Lutsyk P. D., Senior Student (National University of Water and Environmental Engineering, Rivne, Ukraine)

ANALYSIS OF THE PRACTICAL APPLICATION OF AI-HONEYPOT

The modern landscape of cyber threats demands proactive defense measures from organizations, as traditional tools such as signature-based intrusion detection systems often prove insufficient against targeted, sophisticated attacks. In response to these challenges, Deception Technology (DT) has gained significant traction, with the honeypot—a decoy network resource—as its key element. A honeypot simulates an authentic, vulnerable victim and serves only to attract an adversary. Since it holds no real value and expects no legitimate network interactions, any attempt to access it is highly likely to be malicious. This provides DT's main advantage: an extremely low false-positive rate. The primary objectives of a honeypot are to meticulously log

the attacker's actions to gather data on their Tactics, Techniques, and Procedures (TTPs) and to slow their advance through the infrastructure.

Historically, honeypots have faced a dilemma: low-interactive traps are safe but easily detected, while high-interactive ones offer high realism but carry risks of compromise. Architects integrating Artificial Intelligence (AI) aim to solve this fundamental problem. This article presents a practical analysis of such an AI-driven deception system, implemented using the Beelzebub framework and the gpt-4o generative model. Beelzebub, an open-source project sponsored by Nvidia, supports integration with cloud-based LLMs and was used as the core of the deception system. The gpt-4o model acts as the «brain» for the honeypot: upon receiving a command from the attacker, it generates a plausible response, simulating command execution and file downloads.

A realistic attack simulation was successfully conducted in an isolated experimental environment. The attacker, using Kali Linux, performed network scanning (nmap), password cracking (Hydra), and an attempt to download malware (wget). The Beelzebub system intercepted the wget command, and gpt-4o generated a realistic output, simulating a progress bar and a successful file save, leading the attacker to believe their malware was working. This allowed the attacker to be deceived, compelling them to sequentially reveal their TTPs. All collected data was securely logged using the RabbitMQ message broker on an isolated virtual machine.

The experiment confirmed the high effectiveness of AI-driven deception systems. The integration of generative AI overcomes the fundamental limitations of traditional honeypots by providing a deep level of realism—characteristic of high-interactive systems—but without the associated risks of compromise and management complexity. This opens up new possibilities for proactive threat intelligence gathering and the analysis of adversary behavior.

***Keywords*: honeypot, deception technologies, machine learning, generative AI, LLM, message broker, cybersecurity, TTPs.**

УДК 004.056:378.147

Багнюк О. М., ст. викладач (Національний університет водного господарства та природокористування, м. Рівне, o.m.bahniuk@nuwm.edu.ua)

OSINT В ЗВО: СТРУКТУРОВАНЕ НАВЧАННЯ ЯК КЛЮЧ ДО ПРОФЕСІЙНОЇ ЕФЕКТИВНОСТІ

Open-Source Intelligence (OSINT), або Розвідка з Відкритих Джерел, вийшла за межі вузькоспеціалізованих кіл і стала критичною навичкою у багатьох сучасних професіях, включаючи кібербезпеку, журналістику та

міжнародні відносини. Актуальність дослідження зумовлена необхідністю формування фахівців, здатних ефективно орієнтуватися у зростаючих обсягах публічно доступної інформації (Big Data) та перетворювати розрізнені дані на валідні розвідувальні відомості. Інтеграція структурованого навчання OSINT на університетському рівні є не просто актуальною рекомендацією, а необхідною умовою для формування фахівців, готових до викликів цифрової епохи.

Стаття обґрунтовує необхідність інтеграції структурованого навчання OSINT на університетському рівні, відходячи від вузькоспеціалізованого, інструментального підходу до опанування цілісної методології. Проаналізовано послідовність OSINT-дослідження, що включає п'ять критичних етапів: Визначення Запиту, Ідентифікації Джерел, Обробки Даних, Аналізу та Фінального Звітування. Підкреслено, що ефективне навчання вимагає акценту на критичному мисленні, етичних нормах та юридичних обмеженнях, а не лише на технічному інструментарії. Здійснено огляд профорієнтаційних напрямів OSINT-аналітика, доводячи, що академічна підготовка має відповідати вимогам ринку.

Ключові слова: **OSINT, Розвідка з відкритих джерел, ЗВО, Методологія, Кібербезпека, Етика, Цифрова безпека.**

Метою роботи є аналіз та структуризація ключових методологічних, етичних та технологічних компонентів, необхідних для ефективного впровадження навчального курсу з OSINT у закладах вищої освіти, а також визначення його ролі у підготовці фахівців з кібербезпеки та стратегічної розвідки.

Вступ. OSINT не є просто пошуком в Google. Це дисциплінована, етична та легальна практика збору, обробки та аналізу публічно доступної інформації з метою отримання стратегічної або тактичної розвідки. На рівні міжнародної безпеки, зокрема у доктринах NATO, OSINT визнається невід’ємною частиною Intelligence Cycle (Розвідувального циклу) [1]. Цей цикл є фундаментальною моделлю, яка перетворює потреби користувача на готові розвідувальні продукти.

Класичний Розвідувальний Цикл складається з п'яти основних етапів, і OSINT-дослідження має бути структуроване за аналогічною послідовністю. Академічна підготовка повинна забезпечувати опанування студентами цієї наріжної послідовності [2], що перетворює розрізнені дані на валідні розвідувальні дані:

Визначення Запиту (Direction/Define): Навчання критичному формулюванню дослідницького питання, яке має бути чітким, законним та досяжним за допомогою публічних джерел. На цьому етапі визначаються IIR (Information Inventory Requirements).

Ідентифікація Джерел (Collection/Identify): Систематичне вивчення та класифікація потенційних джерел інформації, а також застосування інструментів для збору даних.

Обробка Даних (Processing): Фільтрація, очищення та структурування зібраної сирої інформації, підготовка її до подальшого аналізу.

Аналіз (Analysis): Застосування критичного мислення та аналітичних технік для перетворення даних на розвідувальні висновки [3].

Фінальне Звітування (Dissemination/Reporting): Чітка, своєчасна та верифікована комунікація отриманих результатів кінцевому споживачу (decision-maker).

Типологія Джерел OSINT та їх структура. Етап ідентифікації джерел (Collection) є критично важливим. Структурований академічний курс повинен надавати студентам чітку типологію можливих джерел, відходячи від хаотичного пошуку. Джерела OSINT класифікуються за рівнем доступності та природою даних (див. таблицю).

Варто зауважити, що навчання має наголошувати, що ефективний OSINT-аналітик використовує комбінацію джерел, а не обмежується лише пошуком в Surface Web.

Технологічний Огляд OSINT за стандартами НАТО та кібербезпеки. Ефективність OSINT в сучасних умовах залежить від автоматизації та інтеграції технологій. Згідно з доктринами та рекомендаціями військових та безпекових структур, включаючи NATO [4], акцент робиться на інструментах, що підтримують масштабований збір, очищення та, головне, аналітичну інтеграцію даних.

На відміну від вузькоспеціалізованого «хакерського» інструментарію, професійний OSINT вимагає застосування технологій, що забезпечують:

Масштабованість збору (Automation Tools): Це інструменти, які автоматизують збір великих обсягів даних з багатьох джерел. Прикладами є парсери соціальних мереж, інструменти для скрапінгу веб-сайтів та інструменти для масового перевірки технічної інфраструктури (наприклад, Shodan або Censys).

Візуалізація та Зв'язки (Data Visualization and Link Analysis): Ключовим завданням OSINT є виявлення неочевидних зв'язків між об'єктами (особами, організаціями, інфраструктурою). Технології, такі як Maltego (для візуалізації зв'язків), або спеціалізовані Graph Databases, є обов'язковими для академічного вивчення. Вони дозволяють перетворити табличні дані на зрозумілий графік відносин.

Аналіз Великих Мовних Моделей (LLM-Driven Analysis): Сучасні підходи включають використання Large Language Models (LLM) для автоматичної категоризації, тематичного моделювання та швидкого підсумовування текстових OSINT-даних (наприклад, аналіз великої кількості новин або публікацій у соціальних мережах для виявлення тенденцій) [3].

Управління Ідентичністю (Identity Management): З погляду кібербезпеки, навчання OSINT також має включати принципи операційної безпеки (OPSEC). Це використання віртуальних машин, VPN, проксі-серверів та ізольованих «персон» для проведення розслідувань. Це мінімізує ризик викриття аналітика та запобігає впливу на результати дослідження.

Таблиця

Типологія джерел для OSINT-аналізу та їх структура

Категорія Джерела	Опис	Приклади
Surface Web	Загальнодоступні індексовані ресурси.	Пошукові системи, Вікіпедія, офіційні державні реєстри, публічні новини та прес-релізи.
Deep Web	Неіндексовані дані, доступ до яких вимагає авторизації або спеціального запиту.	Академічні бази даних, судові рішення, фінансові звіти компаній, архівні дані, закриті форуми.
Social Media Intelligence (SOCMINT)	Дані, отримані з соціальних мереж та платформ.	Twitter/X, Telegram, LinkedIn, Facebook, Reddit. Аналіз метаданих фото/відео.
GEOINT/IMINT	Географічні дані та супутникові / аерофотознімки.	Google Maps/Earth, Sentinel Hub, публічні дані про погодні умови та інфраструктуру.
Technical OSINT	Дані, отримані з технічних слідів та інфраструктури.	WHOIS-записи доменів, інформація DNS-серверів, відкриті бази вразливостей (CVE), публічні репозиторії коду (GitHub).

Таким чином, у навчальному процесі необхідно змістити акцент з освоєння 100+ інструментів на опанування 5–10 ключових технологій, які відображають увесь розвідувальний цикл: від збору даних з Surface Web до їх візуалізації та звітування.

Етичний та правовий імператив. Ефективне навчання OSINT вимагає акценту не лише на технічному інструментарії, а й на критичному мисленні, етичних нормах та юридичних обмеженнях. Без міцного фундаменту у цифровій етиці, випускники ризикують перетнути межу, що відділяє законну розвідку від порушення конфіденційності, нелегального доступу до даних або приватної деанонімізації. Це нівелює їхню професійну цінність. Навчальний процес має акцентувати.

Публічне ≠ Дозволене: Те, що інформація є публічною, не завжди означає, що її використання для конкретних цілей є законним або етичним (наприклад, порушення авторського права або політики платформ).

Ефект «Цифрового Сліду»: Дослідження цифрового сліду (наприклад, для формування профілів цілей) має проводитися виключно у контрольованому, освітньому чи оборонному контексті.

ЗВО має виховувати фахівців із високою операційною безпекою (OPSEC) та глибоким розумінням законодавства про захист даних (GDPR, українське законодавство).

Профорієнтація та Напрями Професійного Розвитку Випускників. Академічна підготовка з OSINT повинна мати чітку профорієнтаційну спрямованість, готуючи випускників до конкретних, високоспеціалізованих позицій на ринку праці [5]. Опанування методології та інструментарію OSINT відкриває можливості у кількох ключових сферах, що вимагають додаткового розвитку спеціалізованих навичок.

Аналітик Розвідки Загроз (Threat Intelligence Analyst): Позиція, що вимагає постійного моніторингу Dark Web та Deep Web для виявлення ранніх ознак кібератак, кампаній дезінформації або витоків даних [6]. Потребує додаткового розвитку знань у сфері мережевої безпеки та кіберкриміналістики.

Слідчий OSINT/Кіберкриміналіст (Forensic Investigator): Спеціалізація на документуванні доказів, пов'язаних із шахрайством, порушенням прав інтелектуальної власності або воєнними злочинами [7]. Вимагає поглибленого знання правових норм та процедур збереження доказової бази.

Фахівець з Розслідувань Due Diligence/KYC: Робота у фінансовому секторі, спрямована на перевірку ділової репутації компаній та фізичних осіб. Потребує знань фінансового законодавства та роботи з державними реєстрами.

Журналіст-Розслідувач: Використання OSINT для підтвердження фактів, геолокації подій та викриття корупційних схем. Потребує навичок сторітелінгу та верифікації інформації.

Успішна кар'єра у будь-якій із цих сфер вимагає, окрім академічних знань OSINT, додаткового розвитку таких міжпрофесійних навичок (soft skills): критичне мислення (як основний інструмент аналізу), написання технічних звітів (дисемінація результатів) та операційна безпека (OPSEC), що є ключовим для захисту себе та джерел інформації.

Використання OSINT у навчальних процесах та переваги. Інтеграція OSINT у навчальний процес ЗВО виходить за рамки підготовки лише фахівців з кібербезпеки. Це міждисциплінарний інструмент, який може бути використаний у юриспруденції (збір доказів), журналістиці (фактчекінг), маркетингу (аналіз конкурентів) та міжнародних відносинах (геополітичний моніторинг).

Можливості та переваги використання OSINT у ЗВО потребують особливого фокусу.

Практична орієнтація: Навчання переходить від теоретичних знань до практичних навичок, що забезпечує високу конкурентоспроможність випускників на ринку праці.

Розвиток критичного мислення: OSINT за своєю суттю є методикою критичного аналізу інформації, яка вчить студентів не лише знаходити дані, а й верифікувати їх, виявляти маніпуляції та оцінювати достовірність джерела (Source Reliability and Information Credibility – SRC).

Інтердисциплінарність: OSINT може слугувати містком між різними освітніми програмами, забезпечуючи міжфакультетні дослідницькі проєкти.

OSINT у бізнес-процесах ЗВО та очікувані результати. Застосування OSINT не обмежується лише навчанням, а стає стратегічним інструментом для підвищення інституційної стійкості самого університету.

Можливості використання OSINT у бізнес-процесах ЗВО оглянемо далі.

Конкурентна розвідка (Competitive Intelligence): Моніторинг освітніх програм, інновацій та PR-стратегій конкурентів для оптимізації власної освітньої пропозиції.

Безпека та Бренд-моніторинг: Виявлення ранніх ознак дискредитаційних кампаній, моніторинг соціальних мереж на предмет внутрішніх загроз, запобігання фішинговим атакам, спрямованим на співробітників та студентів.

Управління репутаційними ризиками (Reputation Management): Систематичний збір та аналіз публічних згадок про університет для швидкого реагування на кризи.

Кінцевим очікуваним результатом є випуск фахівців нового покоління, які характеризуються не лише високою технічною підготовкою, а й інформаційною гігієною та аналітичною дисципліною. Ці фахівці матимуть:

навичку структурного розслідування (здатність перетворювати неструктурований інформаційний хаос на чіткі, верифіковані розвідувальні звіти.

Високу операційну безпеку (OPSEC): Здатність захищати себе, свої дані та свою організацію під час роботи в цифровому просторі.

Готовність до Threat Intelligence: Здатність проактивно виявляти загрози, а не лише реагувати на них.

Дослідження OSINT в академічному середовищі. На сьогоднішній день дослідження OSINT у контексті ЗВО переважно зосереджені на двох напрямах: розробка ефективних методик навчання та аналіз використання OSINT для кіберзахисту. Акцент робиться на інтеграції новітніх технологій, таких як Large Language Models (LLM), для автоматизації аналізу великих масивів OSINT-даних [3]. Також спостерігається зростання публікацій, які підтверджують необхідність створення спеціалізованих лабораторій OSINT при ЗВО, що слугуватимуть базою для практичних тренувань та реальних досліджень, зокрема, у сфері документування воєнних злочинів [7]. Академічне середовище є ідеальним полігоном для перевірки нових, етичних та законних методів збору та аналізу інформації, що забезпечує сталий розвиток дисципліни OSINT [8].

Висновки. Необхідність інтеграції структурованого навчання OSINT у вищу освіту більше не підлягає сумніву. Це критична навичка для фахівців з кібербезпеки та стратегічної розвідки. Ефективне впровадження OSINT в університетську програму вимагає акценту на методології Intelligence Cycle, а не лише на інструментах. Академічний курс повинен охоплювати як технологічний інструментарій (від автоматизації збору до візуалізації даних), так і суворі етичні та правові рамки. Тільки такий комплексний підхід, що поєднує методичну дисципліну, технологічну грамотність та етичну відповідальність, дозволить університетам випускати фахівців, готових до ефективної роботи в умовах інформаційних викликів сучасності, а також підвищити власну інституційну стійкість через впровадження OSINT у внутрішні бізнес-процеси. Постійне оновлення навчальних матеріалів та співпраця з практиками є ключовими для підтримання високої ефективності такої освітньої ініціативи.

1. NATO. Intelligence, Surveillance and Reconnaissance (ISR) Doctrine (AAP-21). *NATO Standardization Agency*. Brussels, 2021.

2. Huber J. E., & Price E. M. Intelligence analysis: A target-centric approach. *Defense Intelligence Agency*. 2014.

3. Ramesh K., Smith J. Leveraging Large Language Models for Scalable OSINT Analysis with LLM-driven Feedback. *International Journal of Cyber Intelligence*. 2024.

4. NATO. Cyber Defence and Open Source Intelligence: A Technological Overview. Tallinn : *NATO CCD COE*, 2023.
5. D4rk_Intel. The Ultimate Guide to Launching a Career in Open-Source Intelligence (OSINT): From Beginner to… */ D4rk_Intel* // Medium. – October 1, 2025. URL: https://preciousvincentct.medium.com/the-ultimate-guide-to-launching-a-career-in-open-source-intelligence-osint-from-beginner-to-0b3dd09ec88f (дата звернення: 10.11.2025).
6. Shevchuk V. H., & Shchyrba M. M. OSINT as a tool for collecting data on cyber threats. *Cybersecurity: Education, Science, Technique*. 2023. № 3. P. 133–140.
7. Investigative Journalism and Legal Research Group. The Role of Open-Source Information in Documenting Human Rights Violations and War Crimes in the Digital Age. (Reference for confirming the specialized application of OSINT in international justice and investigative journalism).
8. Стратег. З OSINT ми можемо зробити краще. Вона потребує структурованого навчання та кар'єри. *Стратег*. *Medium*. URL: https://strategе.ua/z-osint-my-mozhemo-zrobyty-krasche-vona-potrebuye-strukturovanogo-navchannya-ta-karyery/ (дата звернення: 10.11.2025).

Bahniuk O. M., Senior Lecturer (National University of Water and Environmental Engineering, Rivne, o.m.bahniuk@nuwm.edu.ua)

OSINT IN ACADEMIA: STRUCTURED LEARNING AS A KEY TO PROFESSIONAL EFFECTIVENESS

The escalating volume of publicly available information (Big Data) has made Open-Source Intelligence (OSINT) a critical skill extending beyond specialized security and military domains to encompass cybersecurity, journalism, international relations, and corporate risk management. The research addresses the urgent need to integrate structured OSINT education at the university level to prepare a new generation of professionals capable of transforming scattered public data into validated, actionable intelligence. This study advocates for a shift from a purely instrumental, tool-focused teaching approach to mastering the comprehensive OSINT methodology.

The article systematically analyzes the core components necessary for implementing an effective OSINT curriculum within Higher Education Institutions (HEIs). It establishes that effective OSINT training must be grounded in the Intelligence Cycle [1], emphasizing five critical stages: defining the request, identifying sources, data processing, analysis, and final reporting. This methodical rigor is supported by a comprehensive typology of OSINT sources (Surface Web, Deep Web, SOCMINT, GEOINT/IMINT, and Technical OSINT), illustrating that professional analysis requires the use of combined, disparate sources.

Technologically, the paper reviews modern OSINT requirements based on NATO and cybersecurity standards, stressing the importance of tools that support scalable data collection and, crucially, analytical integration (e.g., link analysis via platforms like Maltego). Furthermore, the curriculum must incorporate advanced techniques, including the use of Large Language Models (LLMs) for automated categorization and analysis of massive text datasets [3]. Critically, the academic program must enforce a strong foundation in digital ethics and legal boundaries, emphasizing that publicly available information does not automatically imply permission for its use, and reinforcing the principles of Operational Security (OPSEC) to protect both the analyst and the integrity of the investigation.

The research then focuses on the multifaceted implementation of OSINT within HEIs:

1. Educational Processes: OSINT offers significant advantages by fostering critical digital thinking, moving education from theory to practical, interdisciplinary skill acquisition, making graduates highly competitive in threat intelligence, forensic investigation, and due diligence roles.

2. HEI Business Processes: OSINT serves as a strategic corporate tool for enhancing institutional resilience. This includes competitive intelligence (monitoring rival programs), brand monitoring, and preemptive security measures against phishing and reputational attacks.

3. Expected Outcomes: Successful implementation is expected to produce a new generation of analysts characterized by analytical discipline, high information hygiene, and the ability to conduct structural investigations and proactively address cyber threats.

4. Academic Research: The HEI environment is presented as an ideal testing ground for researching ethical and legal methods of data analysis, including the use of OSINT to document human rights violations and war crimes.

In conclusion, integrating structured OSINT education is a necessary investment in the digital security and transparency of the future. A comprehensive curriculum that blends methodological discipline, technological proficiency, and ethical responsibility is essential for training highly effective specialists and fortifying the institutional integrity of the university itself.

***Keywords*: OSINT, Open-Source Intelligence, Academic Education, Structured Learning, Cybersecurity, Threat Intelligence, Higher Education Institutions (HEI), Critical Thinking, Intelligence Cycle.**

УДК 006.3:004.8

Бабич С. В., к.т.н., доцент (Національний університет водного господарства та природокористування, м. Рівне, **Жовтяк Н. О., студент 1 курсу магістратури спеціальності «Комп'ютерна інженерія»** (Національний університет водного господарства та природокористування, м. Рівне, s.v.babych@nuwm.edu.ua ; zhovtiak_ak25@nuwm.edu.ua)

ЯК ПРОЕКТУВАННЯ ДЛЯ ВСІХ РОБИТЬ UI КРАЩИМ ДЛЯ КОЖНОЖНОГО

Розглянуто фундаментальні концепції інклюзивного дизайну та цифрової доступності (a11y) в контексті сучасного проектування користувацького досвіду (UX). Проаналізовано ключові відмінності між поняттями «доступність» (accessibility), «інклюзивний дизайн» (inclusive design) та «універсальний дизайн» (universal design), які часто помилково ототожнюються.

Наведено ґрунтовний аналіз основних принципів Настанов з доступності вебконтенту (WCAG) – Сприйнятність, Керованість, Зрозумілість та Надійність (POUR) – як технічного стандарту для забезпечення доступності. Здійснено характеристику «ефекту зрізаного бордюру» (Curb-Cut Effect) як ключової парадигми, що пояснює, як дизайнерські рішення, спрямовані на допомогу людям з постійними обмеженнями, приносять значну користь ширшому колу користувачів у тимчасових або ситуативних обмеженнях.

Досліджено механізм впливу інклюзивних практик (таких як висока контрастність, субтитри, навігація з клавіатури) на загальну юзабіліті та задоволеність користувачів. Визначено пріоритетні способи інтеграції принципів доступності в життєвий цикл розробки цифрового продукту, від початкового дослідження до фінального тестування.

***Ключові слова*: інклюзивний дизайн, доступність, a11y, UX/UI, користувацький досвід, WCAG, універсальний дизайн, проектування для всіх, ефект зрізаного бордюру, юзабіліті.**

Вступ. Постановка проблеми. Концепція «цифрової трансформації» утверджується як невід'ємний елемент суспільного та економічного розвитку. У ділових та технологічних колах зростає розуміння відповідальності цифрових продуктів за їхній вплив на суспільство [2]. Проте, стрімка диджиталізація часто призводить до створення цифрового бар'єру, що виключає мільйони людей з інвалідністю або іншими обмеженнями з повноцінної участі в онлайн-житті. Необхідність ведення такої політики проектування, яка б, за визначенням, сформульованим у Настановах з доступності веб-контенту (WCAG) Консорціуму Всесвітньої павутини (W3C),

«робила вебконтент більш доступним для людей з інвалідністю» [1], стає не просто етичною нормою, а й юридичною вимогою в багатьох країнах.

У своїй первісній формі доступність (часто скорочується до a11y – 11 літер між 'a' та 'y') розглядалася як технічна дисципліна, спрямована на те, щоб приносити користь вузькій групі користувачів з обмеженими можливостями [3]. Це був підхід, орієнтований на відповідність стандартам (compliance). Однак у сучасному UX-дизайні цей підхід трансформується. На противагу цьому, інклюзивний дизайн є методологією проектування, яка розглядає повний спектр людського розмаїття як джерело для інновацій [4].

Питанням цифрової доступності та її імплементації присвячено значну кількість праць. Зокрема, методичні підходи до автоматизованого та мануального тестування доступності розроблено у працях О. В. Гриценка [5], Л. М. Клименко [6], та С. П. Яремчука [7]. Серед інших дослідників вагомий внесок у дослідження проблематики користувацького досвіду в цілому зробили Д. Норман [8] та С. Круг [9]. Успішні світові практики інклюзивного дизайну вивчала у своїй праці К. Холмс, яка сформулювала концепцію «невідповідності» (mismatch) як основи для інклюзії [4].

Мета такого аналізу не лише технічні стандарти, але вивчнення філософських підходів до проектування, зорієнтованих на максимізацію користі та зменшення бар'єрів для найширшого кола «зацікавлених сторін» (стейкхолдерів) – осіб чи груп, що є «об’єктом або суб’єктом взаємодії з цифровим продуктом» (за аналогією з Р. Фріменом) [10]. Проте, попри численні дослідження у цій сфері, єдиного методичного підходу до оцінювання впливу доступності на загальний UX (для користувачів *без* інвалідності) не вироблено. Більшість робіт фокусується на відповідності стандартам, а не на універсальних перевагах.

Цікавими для вивчення та аналізу є світоглядний і практичний ракурси розгляду доступності не як «витратної частини», а як інвестиції в якість продукту.

Доступність, Інклюзивний та Універсальний Дизайн. Для глибокого аналізу теми необхідно чітко розмежувати три ключові терміни, які часто вживаються як синоніми, але мають різну суть та мету.

Доступність (Accessibility, a11y). Це результат або мета. Доступність – це вимірювана характеристика продукту, що описує, чи може ним користуватися людина з інвалідністю. Вона є бінарною (продукт або доступний, або ні) і часто оцінюється за технічними стандартами, таким як WCAG [1]. Це «що» ми досягаємо.

Універсальний Дизайн (Universal Design, UD). Це філософія та ідеал. Концепція, розроблена Рональдом Мейсом, передбачає проектування продуктів та середовищ таким чином, щоб вони були максимально корисними для всіх людей, без необхідності адаптації чи спеціалізованого

дизайн. Універсальний дизайн прагне створити єдине рішення («one-size-fits-all»), яке задовольняє всіх.

Інклюзивний Дизайн (Inclusive Design). Це методологія або процес. Інклюзивний дизайн визнає, що неможливо створити єдине рішення для всіх. Натомість він фокусується на розмаїтті людського досвіду та проектує для повного спектру людських можливостей [4]. Він визнає, що інвалідність – це не персональна характеристика, а «невідповідність» (mismatch) між потребами людини та продуктом, який вона використовує. Головний принцип: «проектуючи для одного, поширити на багатьох» (solve for one, extend to many). Це «як» ми досягаємо мети.

Отже, доступність є технічним стандартом, універсальний дизайн – ідеалістичною метою, а інклюзивний дизайн – практичною методологією досягнення доступності для якомога ширшої аудиторії.

Основні принципи WCAG як технічна основа доступності. Наріжним каменем цифрової доступності є Настанови з доступності вебконтенту (WCAG), розроблені W3C [1]. Вони базуються на чотирьох фундаментальних принципах, відомих під акронімом POUR:

Perceivable (Сприйнятний). Інформація та компоненти інтерфейсу користувача повинні бути представлені користувачам у спосіб, який вони можуть сприймати. Це означає, що контент не може бути «невидимим» для всіх органів чуття.

Operable (Керований). Компоненти інтерфейсу користувача та навігація мають бути керованими. Користувач повинен мати можливість взаємодіяти з усіма компонентами.

Understandable (Зрозумілий). Інформація та робота з інтерфейсом користувача мають бути зрозумілими.

Robust (Надійний). Контент має бути достатньо надійним, щоб його можна було надійно інтерпретувати широким спектром клієнтських програм, включаючи допоміжні технології (assistive technologies).

Ці чотири принципи є фундаментом, на якому будується доступний цифровий продукт. Проте, сліпа гонитва за виконанням «чек-листа» WCAG без розуміння інклюзивної методології часто призводить до створення продукту, який «технічно доступний», але незручний у використанні.

«Ефект зрізаного бордюру»: як дизайн для обмежених груп покращує UX для кожного. Центральною тезою цієї статті є те, що інвестування в доступність – це не нішева оптимізація, а фундаментальне покращення користувацького досвіду (UX) для *всіх* користувачів. Найкраще це ілюструє «ефект зрізаного бордюру» (The Curb-Cut Effect).

Зрізані бордюри (плавні спуски з тротуару на проїжджу частину) були спочатку пролобійовані та впроваджені в США у 1970-х роках для людей, що користуються інвалідними візками. Це було рішення для дуже специфічної групи населення. Однак, як тільки вони з'явилися, ними миттєво почали

користуватися: батьки з дитячими візками, мандрівники з валізами на коліщатках, працівники служб доставки з візками, велосипедисти та скейтбордисти, люди з тимчасовими травмами (на милицях).

Рішення, створене для малої групи з постійною інвалідністю, виявилося надзвичайно корисним для набагато ширшої аудиторії з тимчасовими (наприклад, зламана нога) або ситуативними (наприклад, руки зайняті валізою) обмеженнями [4].

Цей ефект повною мірою проявляється у цифровому дизайні. Розглянемо конкретні приклади впровадження принципів доступності та їхній вплив на загальний UX.

Субтитри та транскрипції. Створювалось для користувачів з вадами слуху (постійне обмеження). Використовується: ситуативне обмеження (гучно: люди у громадському транспорті, спортзалі, кафе, де неможливо почути звук), ситуативне обмеження (тихо: люди в офісі, бібліотеці або вночі, коли не можна вмикати звук), когнітивна перевага (користувачі, які вивчають іноземну мову, що допомагає співвідносити аудіо та текст), покращення SEO (пошукові системи індексують текстові транскрипції, що покращує видимість контенту), UX-перевага (надання користувачеві вибору способу споживання контенту).

Висока контрастність кольорів. Створювалось для користувачів із вадами зору (дальтонізм, низький зір). Використовується: ситуативне обмеження (яскраво: будь-який користувач, що намагається прочитати текст з екрану смартфона у сонячний день), технічне обмеження (користувачі зі старими або неякісними моніторами з поганою передачею кольорів), тимчасове обмеження (користувачі із втомленими очима після довгого робочого дня), UX-перевага (підвищення читабельності та зниження когнітивного навантаження на всіх користувачів).

Навігація за допомогою клавіатури. Створювалось для користувачів з моторними порушеннями (які не можуть користуватися мишею) та незрячих користувачів (які використовують скрін-рідери, що покладаються на клавіатуру). Використовується: «Power Users» (досвідчені користувачі, які надають перевагу швидкій навігації та заповненню форм за допомогою клавіш, оскільки це значно швидше за мишу), ситуативне обмеження (користувач, у якого зламалася миша або сів тачпад), тимчасове обмеження (користувач із травмою руки (наприклад, у гіпсі), UX-перевага (надання ефективності та альтернативного способу взаємодії).

Чіткі повідомлення про помилки та проста мова. Створювалось для користувачів з когнітивними порушеннями, дислексією або низьким рівнем цифрової грамотності.

Ситуативне обмеження (відволікання): Будь-який користувач, який намагається заповнити форму, одночасно розмовляючи по телефону або слідкуючи за дитиною.

Користувачі у стресі: Люди, які поспішають, або перебувають у стані стресу (наприклад, намагаючись забронювати останній квиток), мають знижені когнітивні здібності.

Неносії мови: Користувачі, для яких мова інтерфейсу не є рідною.

UX-перевага: Підвищення ефективності (efficiency) та зниження фрустрації для всіх. Чіткі, позбавлені жаргону інструкції допомагають кожному швидше досягти мети.

Впровадження доступності в життєвий цикл розробки продукту. Однією з найбільших помилок є розгляд доступності як окремого завдання, яке «додається» в кінці процесу розробки, безпосередньо перед релізом. Такий підхід («bolted-on») є неефективним, дорогим і часто призводить до поганого UX.

Інклюзивний дизайн вимагає інтеграції («built-in») практик доступності на кожному етапі життєвого циклу розробки продукту (PDLC).

1. Дослідження та Стратегія. На етапі формування персон (user personas) необхідно включати користувачів з різними обмеженнями. Замість однієї «головної» персони, слід використовувати «спектр персон» (persona spectrum), що враховує постійні, тимчасові та ситуативні обмеження [4].

Проведення юзабіліті-тестування з залученням реальних людей з інвалідністю.

2. Проектування. Дизайн-система: Всі компоненти дизайн-системи (кнопки, поля вводу, посилання) мають бути спроектовані з урахуванням доступності (контраст, розміри, стани фокусу).

Макетування: Дизайнери мають проектувати не лише ідеальний вигляд.

3. Розробка. Семантичний HTML: Використання правильних HTML-тегів (<nav>, <main>, <button>) замість універсальних та є основою доступності, оскільки надає структуру для скрін-рідерів.

ARIA-атрибути: Використання ARIA (Accessible Rich Internet Applications) там, де семантики HTML недостатньо (наприклад, для складних віджетів, як-от каруселі або вкладки).

Автоматизоване тестування: Впровадження інструментів (наприклад, Axe, Lighthouse) у процес CI/CD для виявлення базових помилок доступності ще до етапу QA.

4. Тестування. Автоматизація може виявити лише 30–40% проблем. Ключовим є мануальне тестування.

Тестування повної навігації лише за допомогою клавіатури. Тестування за допомогою реальних скрін-рідерів (NVDA, VoiceOver, JAWS) для оцінки реального досвіду незрячих користувачів.

Такий інтегрований підхід («Shift-Left») не лише гарантує відповідність стандартам, але й робить якість та інклюзивність спільною відповідальністю всієї команди, а не лише одного «тестувальника доступності».

Висновки. Резюмуючи вищезазначене, необхідно зазначити, що завдяки технологізації та цифровізації, упровадженню нових стандартів взаємодії можливо саме в XXI столітті буде вирішена проблема цифрового виключення мільйонів людей.

Сьогодні доступність стала невід'ємною частиною якісного користувацького досвіду. У розвинених країнах численні дослідження довели позитивний вплив інклюзивних практик на діяльність компаній та їхні фінансові показники (розширення аудиторії, покращення SEO, зниження юридичних ризиків), натомість у країнах, що розвиваються, зокрема в Україні, такі висновки ще потребують обґрунтування та ширшого впровадження.

В дизайні зростає рівень згуртованості з інклюзивними практиками завдяки централізованим дизайн-системам та поширенню стандартів WCAG. Порівнюючи підходи, зазначимо, що доступність – це технічна вимога, універсальний дизайн – широка філософія, а інклюзивний дизайн – це практична методологія. Для інклюзивного дизайну традиційно характерним є превалювання емпатії та проектування для спектру обмежень, а не для «середнього» користувача. Соціальна діяльність з розробки доступних продуктів не пов'язана із філантропією, а має на меті пряме отримання бізнес-переваг та покращення якості продукту.

Роль держави в регулюванні цифрової доступності в Україні поки що доволі низька, тобто законодавчих вимог стосовно обов'язкової відповідності WCAG для комерційного сектору, на відміну від ЄС та США, практично не існує. Концепція інклюзивного дизайну, з нашої точки зору, є повністю добровільною ініціативою бізнес-структур, але водночас є маркером зрілості та конкурентоспроможності продукту.

Формування «національної» моделі цифрової доступності – це не копіювання успішних зарубіжних зразків. Використання найкращого світового досвіду в кожній країні має об'єктивно поєднуватися з урахуванням місцевих традицій, менталітету та особливостей запитів місцевих стейкхолдерів. Основний інструмент формування ефективної моделі – відкритий діалог усіх зацікавлених сторін, соціальне партнерство та поширення знань про доступність в освітніх програмах для дизайнерів та розробників.

Тож, варто зазначити, що хоча інклюзивний дизайн базується на ідеях емпатії та соціальної відповідальності, у ньому немає нічого специфічного, що характерне лише для застосування в проектах для людей з інвалідністю. «Ефект зрізаного бордюру» доводить, що дизайн, орієнтований на крайні випадки, створює кращий, зручніший та ефективніший досвід для абсолютно кожного користувача. Тому вже зараз можна сміливо стверджувати, що сама ідея інклюзивного проектування є новим етапом у розвитку цифрового дизайну. Впровадження такої системи в одній компанії згодом спричинить підвищення загальної планки якості на ринку, а перехід конкурентів до неї буде питанням часу та ринкової необхідності.

1. W3C. Web Content Accessibility Guidelines (WCAG) 2.1. URL: https://www.w3.org/TR/WCAG21/ (дата звернення: 10.11.2025).
2. Про внесення змін до деяких законів України щодо адаптації законодавства до вимог Директиви (ЄС) 2019/882 Європейського Парламенту і Ради. URL: https://zakon.rada.gov.ua/laws/show/2962-IX (дата звернення: 10.11.2025).
3. Thatcher J. et al. Web Accessibility: Web Standards and Regulatory Compliance. Friends of ED, 2006. 456 p.
4. Holmes K. Mismatch: How Inclusion Shapes Design. MIT Press, 2018. 208 p.
5. Гриценко О. В. Методи оцінки доступності веб-сайтів державних установ. *Вісник Національного університету «Львівська політехніка». Сер. Інформаційні системи та мережі.* 2019. № 14. С. 45–53.
6. Клименко Л. М. Інклюзія в цифровому просторі: проблеми та перспективи для України. *Цифрова платформа: економіка та суспільство*. 2020. Вип. 3. С. 112–120.
7. Яремчук С. П. Формування національної моделі цифрової доступності в контексті євроінтеграції. *Економіка та держава*. 2021. № 5. С. 34–39.
8. Norman D. The Design of Everyday Things: Revised and Expanded Edition. Basic Books, 2013. 368 p.
9. Krug S. Don't Make Me Think, Revisited: A Common Sense Approach to Web Usability. New Riders, 2014. 216 p.
10. Freeman R. E. Strategic Management: A Stakeholder Approach. Pitman Publishing, 1984. 246 p.

Babych S. V., Candidate of Engineering (Ph.D.), Associate Professor, Zhovtiak N. O., Senior Student (National University of Water and Environmental Engineering, Rivne, Ukraine)

HOW DESIGN FOR ALL MAKES UI BETTER FOR EVERYONE

This article examines the fundamental concepts of inclusive design and digital accessibility (a11y) within the context of modern user experience (UX) and user interface (UI) design. It addresses a common misconception in the technology industry where accessibility is often viewed as a niche, compliance-driven discipline aimed only at a narrow group of users with disabilities. The paper challenges this view, arguing that the rapid digitalization of society has created significant digital barriers, making the integration of accessibility not just an ethical imperative but a legal and commercial necessity. The central thesis is that designing for a full spectrum of human diversity—a core tenet of inclusive design – does not merely benefit users with permanent disabilities but fundamentally improves the usability, efficiency, and overall satisfaction for every user. The study aims to move beyond a standards-compliance-based

(compliance-oriented) approach and instead analyze the philosophical and practical frameworks that position accessibility as a primary driver of innovation and product quality.

To build its argument, the paper first provides a granular analysis and clear differentiation between three often-confused terms: Accessibility (a11y), Universal Design (UD), and Inclusive Design. Accessibility is defined as the measurable, technical outcome or goal, often evaluated against standards like the Web Content Accessibility Guidelines (WCAG). Universal Design, as conceived by Ronald Mace, is presented as the idealized philosophy of a "one-size-fits-all" solution. In contrast, Inclusive Design is framed as the practical methodology or process used to achieve accessibility. This methodology rejects the "one-size-fits-all" ideal, instead embracing human diversity and viewing disability as a "mismatch" between a user's needs and the product. It operates on the principle of "solve for one, extend to many". The paper also grounds this discussion in the technical foundation of WCAG, analyzing its four core principles – Perceivable, Operable, Understandable, and Robust (POUR) – as the essential standard for creating accessible digital products.

The core of the article is built around the "Curb-Cut Effect", a powerful paradigm that explains the universal benefits of inclusive design. This effect originates from the physical world: curb cuts, initially designed for a small group of wheelchair users, were almost immediately adopted by a much wider audience, including parents with strollers, travelers with wheeled luggage, delivery workers, and cyclists. The paper demonstrates how this exact effect manifests in digital design. Features created for users with permanent limitations provide immense value to those with temporary (e.g., a broken arm) or situational (e.g., holding a child, being in a loud environment) limitations. This is illustrated with specific, practical examples: subtitles (for hearing impairments) are used by people in loud gyms or quiet offices; high-contrast text (for low vision) is critical for anyone using a smartphone in bright sunlight; keyboard-only navigation (for motor impairments) is a significant efficiency boost for "power users"; and simple, clear error messages (for cognitive disabilities) are crucial for any user who is distracted, stressed, or multitasking.

Finally, the paper argues that these benefits cannot be achieved if accessibility is treated as an afterthought or a "bolted-on" feature at the end of the development cycle. This approach is costly, inefficient, and leads to a poor user experience. Instead, the principles of inclusive design must be "built-in" and integrated into every stage of the product development lifecycle (PDLC). This includes creating "persona spectrums" that account for permanent, temporary, and situational limitations during user research; building accessibility (contrast, focus states) into the core design system; using semantic HTML and ARIA attributes in development; and implementing a combination of automated and, critically, manual testing (e.g., keyboard-only and screen-reader

testing). The paper concludes that inclusive design is not philanthropy but a marker of product maturity and a key business advantage, proving that designing for the extremes ultimately results in a more robust, effective, and superior product for everyone.

Keywords: **inclusive design; accessibility; a11y; UX/UI; user experience; WCAG; universal design; design for all; curb-cut effect; usability.**

УДК 004.7

Гелета[1] Н. В., студент; Герус[2] В. А., старший викладач (Національний університет водного господарства та природокористування, м. Рівне, [1]heleta_ak20@nuwm.edu.ua, [2]v.a.gerus@nuwm.edu.ua)

ПАСИВНІ ОПТИЧНІ МЕРЕЖІ: СТАНДАРТИ, АРХІТЕКТУРА ТА ІНТЕЛЕКТУАЛЬНІ МЕТОДИ УПРАВЛІННЯ

У статті розглянуто архітектуру й еволюцію пасивних оптичних мереж (PON) як основи сучасного фіксованого широкосмугового доступу, їх типову структуру та функції OLT, пасивних розгалужувачів і абонентських терміналів. Проаналізовано стандарти від EPON і GPON до XGS-PON та NG-PON2, принципи централізованого управління PON і застосування еволюційних алгоритмів та методів машинного навчання для проектування топології, динамічного розподілу смуги й автоматизованої діагностики.

Ключові слова: **пасивні оптичні мережі; PON; GPON; XGS-PON; NG-PON2; управління трафіком; штучний інтелект.**

Розвиток цифрових сервісів, хмарних платформ і потокового відео зумовлює постійне зростання вимог до пропускної здатності та надійності мереж доступу. Операторам необхідно забезпечувати не лише високу швидкість передавання даних, а й стабільні показники затримки, доступності та якості обслуговування для великої кількості абонентів з різними профілями використання трафіку. Додатковою складністю є потреба підтримувати широкий спектр сервісів — від класичного доступу до Інтернету до IPTV, VoIP, хмарних застосунків та сервісів реального часу [1; 2].

На цьому тлі пасивні оптичні мережі (Passive Optical Network, PON) розглядаються як одна з ключових технологій доступу нового покоління. Вони поєднують високу пропускну здатність волоконно-оптичної лінії з відсутністю активних елементів у розподільній мережі, що знижує енергоспоживання, спрощує експлуатацію та зменшує кількість потенційних точок відмови. Для оператора це означає зменшення капітальних і операційних витрат, а для

користувача — можливість отримати високошвидкісний доступ навіть у віддалених або малонаселених районах [1; 3].

Сутність підходу полягає у винесенні активного обладнання у центральні вузли, тоді як лінійна частина між вузлом доступу та абонентом реалізується на пасивних оптичних компонентах. Така архітектура вимагає ретельного опрацювання оптичного бюджету, але завдяки використанню сучасних волокон і маловтратних розгалужувачів дозволяє обслуговувати значну кількість абонентів на одному порті OLT. Водночас зростання кількості підключень, поява нових сервісів та ускладнення вимог до якості обслуговування роблять актуальним комплексний аналіз архітектури, стандартів і методів інтелектуального управління PON, що й визначає зміст даної статті.

Архітектура та базові принципи функціонування пасивних оптичних мереж. Типова мережа PON має ієрархічну структуру типу «один — багатьом». У центральному вузлі розміщується оптичний лінійний термінал (Optical Line Terminal, OLT), який підключається до транспортної магістралі оператора та виконує термінацію протоколів верхніх рівнів. Саме OLT відповідає за формування кадрів вниз за потоком (downstream), керування доступом до висхідного каналу (upstream), реалізацію політик якості обслуговування (QoS) і взаємодію із системами керування мережею.

Від OLT до зони розподілу прокладається одне або кілька оптичних волокон, на яких розміщуються пасивні розгалужувачі різного ступеня поділу (наприклад, 1:8, 1:16, 1:32, 1:64). Кожен розгалужувач ділить потужність оптичного сигналу між кількома відгалуженнями без застосування активних елементів. На стороні абонента встановлюється оптичний мережевий термінал (Optical Network Unit/Terminal, ONU/ONT), що перетворює оптичний сигнал у електричні інтерфейси для маршрутизаторів, комп’ютерів, приставок IPTV та іншого кінцевого обладнання [2; 4].

Передавання інформації в низхідному напрямку реалізується за широкомовною схемою: один потік, сформований OLT, отримують усі ONU, підключені до відповідної оптичної розподільної мережі. Кожен абонентський термінал відфільтровує лише ті кадри, які адресовані саме цьому абоненту або його сервісам. У висхідному напрямку, навпаки, кілька абонентських терміналів мають ділити спільне середовище передавання. Для цього використовується поділ у часі (Time Division Multiple Access, TDMA): OLT виділяє кожному ONU часові слоти відповідно до запитів на пропускну здатність і налаштовуваних політик QoS [3].

У практичних реалізаціях часто застосовується комбінований підхід, коли, окрім часової мультиплексії, використовується також розділення за довжиною хвилі. Такий підхід дозволяє одночасно підтримувати кілька поколінь стандартів або логічно відокремлені сервісні потоки на різних

довжинах хвиль. Це спрощує еволюційний перехід від застарілих технологій до новіших, не вимагаючи повної заміни оптичної кабельної мережі.

При проектуванні структури PON важливими параметрами є коефіцієнт розгалуження, довжина лінійних ділянок, оптичний бюджет та вибір типу волокна. Від цих характеристик залежить максимальна кількість абонентів на порт OLT, допустима відстань до кінцевих користувачів, а також наявний резерв для майбутньої модернізації мережі. На практиці використовують як одноступеневі, так і дво- чи трирівневі схеми розгалуження, що дозволяє адаптувати топологію до особливостей міської чи сільської забудови, щільності абонентів та стану існуючої інфраструктури [2; 4].

Узагальнений вигляд структури мережі PON наведено на рис. 1. На схемі показано взаємозв'язок між OLT, ієрархією пасивних розгалужувачів та абонентськими ONU, а також виділено логічні напрямки передавання upstream і downstream, які використовуються під час проектування та розрахунку оптичного бюджету.

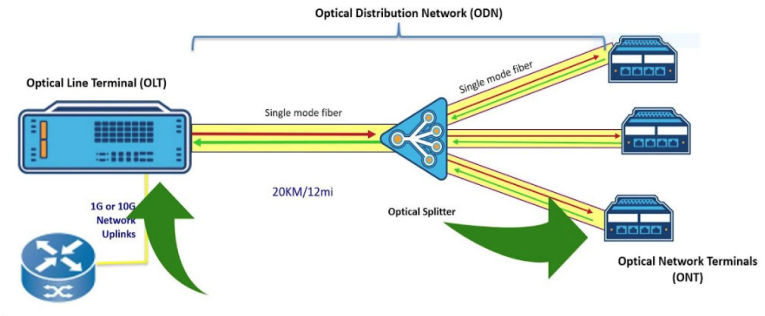

Рис. 1. Типова структура пасивної оптичної мережі PON

Еволюція стандартів та технічні особливості пасивних оптичних мереж. Розвиток пасивних оптичних мереж відбувався у кілька хвиль, що відображено в еволюції відповідних стандартів. Перші рішення APON/BPON базувалися на ATM-технології та орієнтувалися переважно на надання обмеженого набору послуг для відносно невеликої кількості абонентів. Жорстка структура ATM-осередків і складність інтеграції з IP-мережами з часом стали суттєвим обмежувальним фактором. Подальший перехід до Ethernet-орієнтованих рішень EPON і до універсального транспортного рівня GPON дозволив значно спростити інтеграцію з IP-інфраструктурою, підвищити ефективність використання смуги пропускання та розширити набір підтримуваних сервісів [2; 3].

У стандарті GPON використовується механізм інкапсуляції GEM, який забезпечує гнучке перевезення різних типів трафіку поверх єдиного транспортного рівня. Підтримуються розвинені механізми якості обслуговування, криптографічний захист downstream-трафіку та інструменти віддаленого керування абонентськими пристроями. Типові швидкості

досягають 2,5 Гбіт/с у низхідному та 1,25 Гбіт/с у висхідному напрямку, чого достатньо для масового ринку послуг «волокно до будинку» (FTTH) на етапі первинного впровадження [3].

Розвитком цієї лінійки стали стандарти XG-PON та XGS-PON, які забезпечують асиметричні або симетричні швидкості до 10 Гбіт/с. Вони зберігають логічну спадковість із GPON, що дає змогу операторам виконувати модернізацію поетапно: наприклад, спочатку замінити OLT, а згодом — абонентське обладнання. Стандарт NG-PON2 доповнює ці можливості мультиплексуванням за довжиною хвилі (TWDM-PON), завдяки чому в одній фізичній інфраструктурі можна реалізувати кілька логічно ізольованих мереж або суттєво збільшити сумарну пропускну здатність [1].

Схема еволюції стандартів наведена на рис. 2. Вона демонструє безперервне зростання пропускної здатності, підвищення гнучкості розподілу смуги та розширення спектра підтримуваних застосувань — від класичного triple-play до транспортних мереж для мобільного зв'язку п'ятого та наступних поколінь. Важливо, що еволюція стандартів відбувається з урахуванням потреб операторів у плавній міграції, без вимоги повної заміни вже розгорнутої оптичної інфраструктури.

Під час вибору конкретного стандарту для впровадження провайдери враховують не лише швидкісні можливості, а й доступність обладнання на ринку, підтримку функцій безпеки, вимоги регуляторів, можливість інтеграції з існуючими транспортними платформами та прогноз щодо майбутніх потреб абонентів. Для масового домашнього сегменту критичною є вартість ONU та простота їхнього обслуговування, тоді як для корпоративних і операторських застосувань на перший план виходять гнучкість профілів сервісів, підтримка віртуалізації ресурсів та інтеграція з хмарними платформами [1; 3].

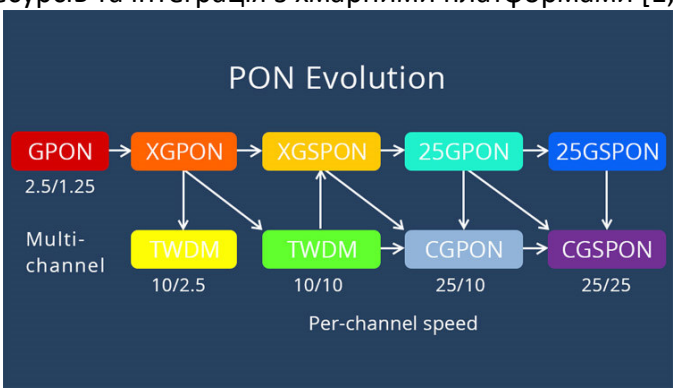

Рис. 2. Еволюція стандартів пасивних оптичних мереж PON

Методи та системи управління пасивними оптичними мережами. Попри пасивний характер лінійної частини, керування PON є складною багатокомпонентною задачею, що охоплює конфігурацію обладнання, контроль оптичних параметрів, моніторинг трафіку, забезпечення

інформаційної безпеки та управління якістю обслуговування. Для розв’язання цих задач на практиці використовують централізовані системи керування мережею (Network Management System, NMS), які взаємодіють з OLT і через нього — з абонентськими ONU за допомогою стандартизованих протоколів, зокрема OMCI у GPON [3; 5].

Типовий життєвий цикл абонентського термінала включає виявлення пристрою в мережі, його реєстрацію, завантаження профілю сервісів, поточний моніторинг параметрів і, за потреби, відключення або переналаштування. На кожному з цих етапів генеруються телеметричні дані, що описують стан оптичної лінії, рівень сигналу, частоту помилок, завантаження трафіком та інші показники якості. У великих мережах обсяг такої інформації є значним, тому для її аналізу й кореляції подій потрібні спеціалізовані програмні засоби [5].

На рис. 3 подано функціональну модель взаємодії NMS, OLT і множини ONU/ONT. Вона показує розподіл функцій між рівнем стратегічного планування (NMS), оперативним контролем ресурсів і реалізацією механізмів доступу до середовища (OLT), а також між абонентськими терміналами, які безпосередньо забезпечують кінцеві сервіси користувачу. Така модель дозволяє формалізувати процеси керування та виділити точки, у яких доцільно впроваджувати інтелектуальні алгоритми для автоматизації рутинних операцій.

Розвиток концепцій автоматизованого управління мережами, зокрема підходів FCAPS (Fault, Configuration, Accounting, Performance, Security), приводить до уніфікації вимог до систем керування PON і іншими сегментами операторської інфраструктури. Це відкриває можливість інтегрованого моніторингу, коли показники доступності, затримки та використання ресурсу аналізуються одночасно для транспортної, агрегаційної та доступової підсистем, а рішення щодо реконфігурації приймаються з урахуванням загальної картини роботи мережі.

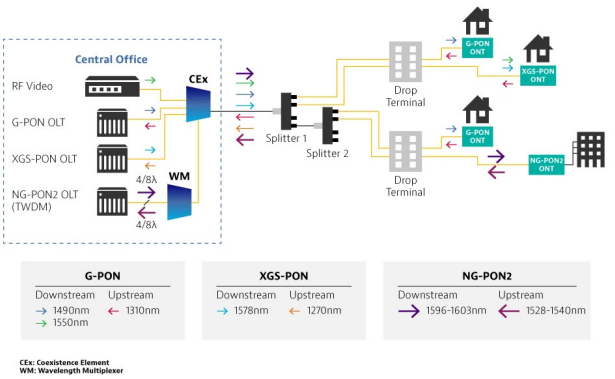

Рис. 3. Функціональна модель управління пасивною оптичною мережею PON

Інтелектуальні методи оптимізації та управління пасивними оптичними мережами. Інтелектуальні методи управління PON спрямовані на автоматизацію прийняття рішень при проектуванні та експлуатації мережі. На етапі планування топології застосовують еволюційні та інші евристичні алгоритми, які дозволяють мінімізувати довжину кабельної інфраструктури, кількість пасивних елементів і втрати в оптичному тракті за умов обмежень на оптичний бюджет, максимальну довжину лінії та допустиме розгалуження. Математичні моделі оптимізації можуть враховувати також щільність абонентів, прогнозоване зростання навантаження та сценарії поетапної модернізації [4].

У задачах динамічного розподілу смуги пропускання (Dynamic Bandwidth Allocation, DBA) дедалі ширше застосовуються методи машинного навчання. На основі історичних даних про навантаження, типи сервісів і параметри QoS формується модель, що прогнозує попит окремих абонентів або класів сервісів і коригує розмір часових слотів у висхідному каналі. Це дає змогу зменшити затримки для критично важливих застосувань, таких як IP-телефонія чи відеоконференції, та підвищити ефективність використання ресурсу каналу порівняно з традиційними правилами DBA [1; 6].

Ще одним важливим напрямом є автоматизована діагностика та самовідновлення мережі. На базі телеметрії OLT та ONU формуються набори ознак, які класифікатори або ймовірнісні моделі зіставляють із типовими сценаріями відмов: обривами волокна, деградацією роз’ємів, зниженням оптичної потужності, некоректними налаштуваннями обладнання тощо. Це дозволяє системі автоматично локалізувати проблемну ділянку, оцінити критичність ситуації та запропонувати оператору перелік найімовірніших дій щодо усунення несправності [5; 6].

У перспективі інтелектуальні модулі управління можуть бути реалізовані у вигляді агентів, вбудованих у SDN-контролери або оркестратори хмарної інфраструктури. Такі агенти здатні отримувати дані телеметрії у режимі, близькому до реального часу, будувати прогнози стану мережі та ініціювати коригування параметрів PON — від зміни профілів DBA до динамічної маршрутизації трафіку та переведення окремих ліній у резервний режим. Це забезпечує перехід від реактивного усунення відмов до проактивного управління якістю обслуговування, що є ключовим кроком на шляху до реалізації концепції автономних оптичних мереж наступних поколінь [1; 6].

Висновки. У статті виконано систематизований огляд архітектури пасивних оптичних мереж, наведено опис типової структури PON з виділенням функцій OLT, пасивних розгалужувачів та абонентських терміналів, а також узагальнено вимоги до проектування топології. Проаналізовано основні покоління стандартів – від EPON/GPON до XGS-PON і NG-PON2 – з погляду пропускної здатності, підтримки мультисервісних

застосувань і можливостей еволюційної модернізації існуючих мереж без їх повної перебудови.

Також у роботі розглянуто сучасні підходи до централізованого управління ресурсами PON на основі систем керування мережею та протоколів віддаленої конфігурації ONU/ONT, окреслено місце цих рішень у загальній моделі FCAPS і взаємодію між рівнями NMS–OLT–ONU. Окрему увагу приділено інтелектуальним методам проектування й експлуатації PON: показано можливості застосування еволюційних алгоритмів, методів машинного навчання та автоматизованої діагностики для оптимізації топології, динамічного розподілу смуги пропускання та скорочення часу відновлення після відмов. Отримані узагальнення можуть бути використані як методична основа під час проектування та модернізації пасивних оптичних мереж доступу наступних поколінь.

1. Abbas H. S., Gregory M. A. The next generation of passive optical networks: a review. *Journal of Network and Computer Applications*. 2016. Vol. 67. P. 53–74.
2. International Telecommunication Union. ITU-T Recommendation G.984.1: Gigabit-capable Passive Optical Networks (GPON): General characteristics. Geneva : ITU, 2003.
3. Kramer G. Ethernet Passive Optical Networks. New York : McGraw-Hill Professional, 2005. 307 p.
4. Головко М. А. Оптичні мережі доступу: теорія та практика : навч. посіб. Київ : КПІ, 2021. 232 с.
5. Однорог П. М., Михайленко Є. В., Котенко М. О., Омецінська О. Б. Пасивні оптичні мережі доступу (xPON) : навч. посіб. Київ, 2006.
6. Чумаченко М. Д. Підвищення ефективності, надійності та автоматизації процесів управління мережею PON шляхом впровадження алгоритмів штучного інтелекту : кваліфікаційна робота магістра. Київ : КПІ ім. Ігоря Сікорського, 2025. 80 с.

Heleta N. V., Senior student; Herus V. A., Senior Lecturer (National University of Water and Environmental Engineering, Rivne)

PASSIVE OPTICAL NETWORKS: STANDARDS, ARCHITECTURE AND INTELLIGENT MANAGEMENT METHODS

The paper presents a concise overview of the architecture and evolution of passive optical networks (PON) as a foundation for modern fixed broadband access systems. A typical PON structure is described, highlighting the roles of the optical line terminal, passive splitters and customer premises equipment. The main generations of PON standards, from EPON and GPON to XGS-PON and NG-PON2, are analysed in terms of throughput, multiservice support and

evolutionary migration capabilities. Centralised management approaches based on network management systems and remote configuration protocols for optical network units are outlined. Special attention is paid to the application of intelligent optimisation methods, including evolutionary algorithms and machine learning, for topology design, dynamic bandwidth allocation and automated diagnostics. It is argued that the integration of such mechanisms is an important step towards the implementation of autonomous optical access networks of future generations.

Keywords: **passive optical networks; PON; GPON; XGS-PON; NG-PON2; traffic management; artificial intelligence.**

УДК 377:659.1

[1]Бабич Т. Ю., к.е.н., доцент; [2]Левчук І. Р., студентка 5 курсу; [3]Дем'янюк Д. Т., студентка 5 курсу (Національний університет водного господарства та природокористування, м. Рівне, [1]t.iu.babych@nuwm.edu.ua, [2]levchuk_ak21@nuwm.edu.ua, [3]burian_ak21@nuwm.edu.ua)

ФОРМУВАННЯ ВІЗУАЛЬНОЇ АЙДЕНТИКИ ПРОФЕСІЙНОГО УЧИЛИЩА

Дослідження присвячено процесу розробки брендбуку як стратегічного інструменту для підвищення впізнаваності та формування сучасного іміджу закладу професійної освіти. Обґрунтовано актуальність оновлення візуальної ідентифікації Вищого професійного училища №1 м. Рівне у зв'язку зі зміною назви на «Рівненський професійний коледж будівництва та архітектури». На основі аналізу тенденцій дизайну запропоновано нову концепцію айдентики, яка включає мінімалістичний логотип із символікою основних спеціальностей закладу, уніфіковану кольорову палітру та шрифти. Розроблено шаблони офіційної документації, презентацій та сувенірної продукції, що забезпечують візуальну єдність усіх каналів комунікації. Сформовано рекомендації для адміністрації щодо впровадження брендбуку в професійну діяльність та внутрішню корпоративну культуру.

Ключові слова: **брендбук, айдентика, імідж, професійна освіта, візуальна ідентифікація.**

Вступ. У сучасному світі успішна діяльність будь-якої організації, зокрема й закладу професійно-технічної освіти, безпосередньо залежить від її впізнаваності, позитивного іміджу та здатності до ефективної комунікації зі своєю аудиторією. В умовах посилення глобальної конкуренції на ринку освітніх послуг формування цілісного візуального образу стає ключовим

фактором успішного розвитку установи. Брендинг у цій сфері виступає стратегічним інструментом, що дозволяє будувати обізнаність про заклад, створювати стійкі асоціації та зміцнювати сприйняття якості навчання серед потенційних вступників. Саме брендбук стає тим засобом, завдяки якому освітній заклад може чітко позиціонувати себе як сучасну, інноваційну та перспективну структуру [1].

Потреба в розробці брендбуку зумовлена необхідністю систематизації візуальних стандартів, які забезпечують єдність стилю в усіх проявах бренду – від логотипа та кольорової гами до оформлення вебсайтів і сувенірної продукції. Він виступає своєрідною «інструкцією з експлуатації бренду», що гарантує цілісність комунікації та підвищує рівень довіри з боку батьків та здобувачів. Наукові дослідження підтверджують, що високий рівень впізнаваності та позитивні асоціації мають вирішальний вплив на процес прийняття рішення абітурієнтами під час вибору навчального закладу. Таким чином, впровадження брендбуку є стратегічно важливим кроком, що сприяє не лише зміцненню конкурентоспроможності, а й формуванню тривалих емоційних зв'язків із цільовою аудиторією [1].

Мета дослідження полягає у розробці брендбуку для ВПУ № 1 як інструменту підвищення його впізнаваності серед цільової аудиторії.

Актуальність. Вище професійне училище № 1 м. Рівне (далі – ВПУ № 1) змінило свою назву на «Рівненський професійний коледж будівництва та архітектури» відповідно да наказу Міністерства освіти і науки України від 18 березня 2024 р. Також відбулось фізичне оновлення закладу – зміна кольору фасаду з блакитного на помаранчевий, що створило візуальний дисонанс зі старою корпоративною гамою. У зв'язку з вищенаведеними причинами була зумовлена необхідність у формуванні нового брендбуку.

Попередній логотип та візуальні елементи закладу, створені кілька десятиліть тому, на сьогодні є морально та технічно застарілими, оскільки їх складний багатошаровий стиль із великою кількістю деталей не відповідає сучасним вимогам лаконічності та втрачає читабельність у цифрових форматах. У контексті високої конкуренції на ринку освітніх послуг важливо розуміти, що матеріальні ресурси закладу можуть бути легко скопійовані, тоді як капітал бренду є невідчутним активом, який практично неможливо емітувати. Бренд містить цінності, що є значно вагомішими за фізичні атрибути, оскільки він залучає емоційні елементи, переконання та очікування абітурієнтів [2]. 69,3% успіху у виборі навчального закладу абітурієнтами залежить від обізнаності про бренд та позитивних асоціацій, відсутність сучасного, лаконічного та адаптивного брендбуку призводить до втрати конкурентоспроможності [3]. Аналіз показує, що заклади професійної освіти часто програють у боротьбі за вступників саме через слабку комунікаційну

подачу, тому новий брендбук має стати інструментом зміцнення довіри та формування іміджу інноваційної освітньої структури.

Опис елементів брендбуку. Під час розробки брендбуку було задіяно графічний редактор Adobe Illustrator та растровий графічний редактор Adobe Photoshop, застосунок для створення та редагування презентацій Microsoft PowerPoint. Центральним елементом розробленого брендбуку є новий логотип (рис. 1), який виступає візуальним уособленням основних напрямів діяльності Рівненського професійного коледжу будівництва та архітектури.

Рис. 1. Розроблений логотип

Основою логотипа обрано правильний шестикутник – геометричну фігуру, що символізує конструктивність, стабільність та стійкість, що є критично важливим для будівельної галузі. Внутрішнє наповнення знаку інтегрує символи ключових спеціальностей:

- *архітектура* – зображення лінійки, косинця та олівця підкреслюють точність та творчу складову професії;
- *будівництво* – силует будівельного крана та об'єктів у процесі зведення вказують на практичну спрямованість навчання;
- *цифрові технології* – стилізоване зображення персонального комп’ютера репрезентує підготовку фахівців у сфері інформаційних систем.

Кольорова палітра, що зображена на рисунку 2, була розроблена з урахуванням потреби в емоційному зв’язку та гармонії з фізичним середовищем закладу. Основу складають бордові та помаранчеві відтінки, що відповідають оновленому фасаду коледжу та створюють образ впевненої, сучасної установи. Використання білого та тілесного кольорів додає композиції «повітря» та відкритості.

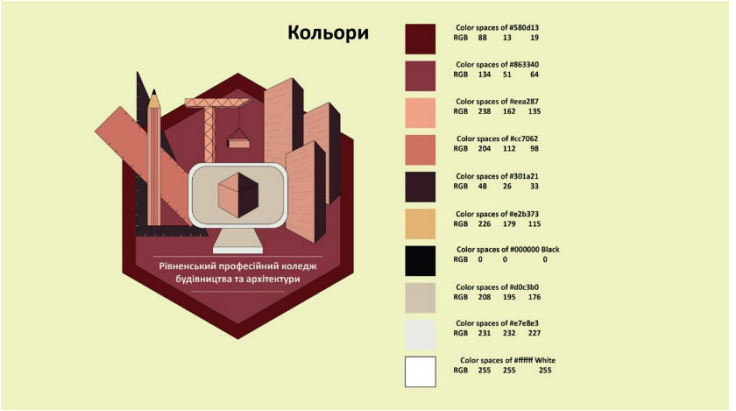

Рис. 2. Розроблена кольорова палітра

Шрифтове оформлення виконане гарнітурою Calibri Bold. Цей вибір обумовлений високою читабельністю шрифту в цифрових форматах та його здатністю підтримувати загальну лаконічність айдентики.

Ефективність брендбуку проявляється у його здатності забезпечити візуальну єдність на всіх рівнях комунікації — від офіційного листування до сувенірної продукції. Було розроблено серію шаблонів, які дозволяють уніфікувати внутрішні та зовнішні процеси коледжу.

Першочергову увагу приділено корпоративній документації та презентаційним матеріалам (рис. 3). Створені шаблони фірмових бланків (рис. 4), сертифікатів та дипломів (рис. 5) забезпечують офіційний та водночас сучасний вигляд документів.

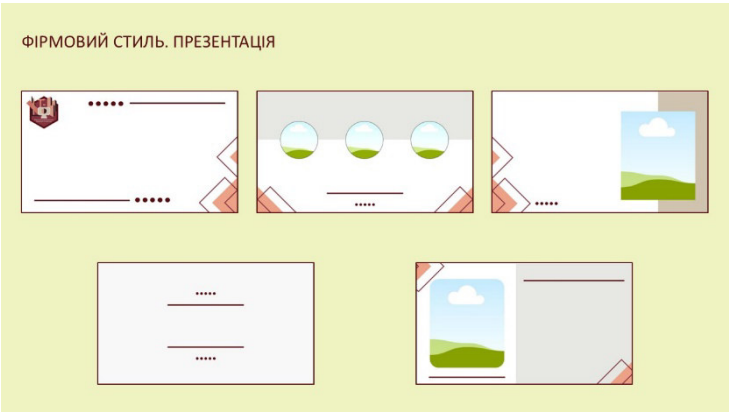

Рис. 3. Макет розробленої презентації

Рис. 4. Розроблені бланки

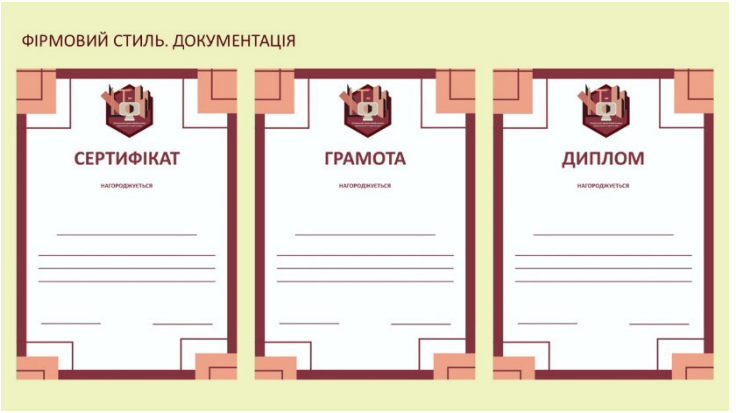

Рис. 5. Сторінка брендбуку «Документація»

Носії айдентики, представлені в брендбуку, охоплюють наступну продукцію: канцелярія (брендовані блокноти, ручки та конверти) і сувеніри (чашки та інший мерч) подано на рис. 6–7 відповідно.

Науково доведено, що такі візуальні активи допомагають абітурієнтам легше інтерпретувати та зберігати інформацію про заклад, що безпосередньо впливає на їхнє впевнене рішення щодо вступу [4].

Рис. 6. Сторінка брендбуку «Рекламна продукція» – 1

Рис. 7. Сторінка брендбуку «Рекламна продукція» – 2

Рекомендації з впровадження. Для того, щоб розроблений брендбук став дієвим інструментом управління репутацією, адміністрації коледжу пропонується впровадити наступний план дій:

1) проведення серії воркшопів для колективу та студентів з метою роз’яснення значення нової айдентики та правил її використання;

2) використання брендованих матеріалів на днях відкритих дверей, освітніх виставках та під час візитів до шкіл для підвищення впізнаваності;

3) призначення відповідальної особи або творчої групи, яка координуватиме дотримання стандартів брендбуку у всіх підрозділах коледжу;

4) регулярне оновлення брендбуку відповідно до нових технічних можливостей та зворотного зв’язку від цільової аудиторії.

Висновок. Дослідження підтвердило, що брендбук є фундаментальним елементом стратегічного управління сучасним закладом освіти. Створення нової візуальної ідентичності для Рівненського професійного коледжу будівництва та архітектури дозволило вирішити проблему дисонансу між

застарілим іміджем та новими амбітними цілями установи. Впровадження розробленого проєкту сприятиме підвищенню публічної впізнаваності та конкурентоспроможності на ринку освітніх послуг, посиленню лояльності здобувачів освіти та викладацького складу, формуванню образу відкритого, інноваційного та перспективного навчального закладу, що відповідає очікуванням сучасної молоді.

Таким чином, новий брендбук стає не просто документом із набором правил, а потужним нематеріальним активом, який неможливо легко скопіювати конкурентам і який забезпечує сталий розвиток коледжу в довгостроковій перспективі.

1. Бугай О. І. Формування бренду освітнього закладу: теоретичні засади. *Вісник Житомирського державного університету імені Івана Франка*. 2019. № 131. С. 8–14.
2. Сорокіна Г., Мальцева М. Особливості використання фірмового стилю для закладів освіти. *Grail of Science*. 2023. № 27. С. 139–143. URL: https://doi.org/10.36074/grail-of-science.12.05.2023.016 (дата звернення: 18.12.2025).
3. Aaker D. A. The Value of Brand Equity. *Journal of Business Strategy.* 1992. Vol. 13, no. 4. P. 27–32. URL: https://doi.org/10.1108/eb039503 (дата звернення: 18.12.2025).
4. Irpansyah M. A., Chan A., Tresna P. W. The Role of Brand on Educational Institution. *Jurnal Samudra Ekonomi dan Bisnis.* 2023. Vol. 14, no. 2. P. 355–366. URL: https://doi.org/10.33059/jseb.v14i2.5405 (дата звернення: 18.12.2025).

Babych T. Yu., Candidate of Economics (Ph.D.), Associate Professor; Levchuk I. R., Senior Student; Demianiuk D. T., Senior Student (National University of Water and Environmental Engineering, Rivne)

VISUAL IDENTITY FORMATION OF A VOCATIONAL SCHOOL

The study is dedicated to the development of a brandbook as a strategic tool for increasing brand awareness and forming a modern image of a vocational education institution. It substantiates the relevance of updating the visual identity of Higher Vocational School No. 1 in Rivne following its renaming to the "Rivne Vocational College of Construction and Architecture". Based on an analysis of design trends, a new identity concept is proposed, featuring a minimalist logo that incorporates the symbols of the institution's primary specialties, a unified color palette, and specific typography. Templates for official documentation, presentations, and promotional products have been developed to ensure visual consistency across all communication channels.

Specific recommendations are provided for the administration regarding the implementation of the brandbook into professional activities and internal corporate culture.

Keywords: **brandbook, identity, image, vocational education, visual identification**

УДК 004.91-042.4:004.8

Каштан С. С., к.т.н., доцент; Дячук Н. Р., магістрант (Національний університет водного господарства та природокористування, м. Рівне, s.s.kashtan@nuwm.edu.ua ; diachuk_ak24@nuwm.edu.ua)

ІНТЕЛЕКТУАЛЬНА ІНФОРМАЦІЙНА СИСТЕМА ВИЯВЛЕННЯ КОРУПЦІОГЕННИХ ФАКТОРІВ У НОРМАТИВНО-ПРАВОВИХ ТЕКСТАХ НА ОСНОВІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

У статті представлено архітектуру та результати апробації інтелектуальної інформаційної системи, призначеної для автоматизованого аналізу текстів організаційно-розпорядчих документів на предмет виявлення корупціогенних факторів. Наукова новизна дослідження полягає у розробці гібридного підходу, що інтегрує використання формалізованих верифікаційних шаблонів із когнітивними можливостями великих мовних моделей (зокрема GPT-4). Технічну реалізацію прототипу здійснено шляхом розгортання робочого процесу (workflow) на платформі n8n із залученням автономного AI-агента через інтерфейс програмування застосунків (API). Експериментальна перевірка системи на прикладі проєктів нормативних актів правоохоронних органів підтвердила високу ефективність ідентифікації прихованих дефектів правового регулювання, зокрема невиправданої дискреції та нечітких оціночних формулювань.

***Ключові слова*: корупціогенний фактор, антикорупційна експертиза, штучний інтелект, машинне навчання, обробка природної мови, ChatGPT, платформа n8n, юридичні технології.**

Вступ. Корупція залишається однією з ключових проблем державного управління. Значна частина корупційних ризиків виникає через недоліки у нормативних та розпорядчих документах – наявність у їх положеннях так званих корупціогенних факторів – це закладена в норму невизначеність або можливість для зловживання, яка дозволяє реалізувати корупційні дії при виконанні цього документа. Наприклад, серед типових корупціогенних чинників експерти виокремлюють нечітке визначення прав і обов’язків відповідальних осіб, надмірні дискреційні повноваження посадовців без

належного контролю, суперечності або прогалини в нормах, необґрунтовані відсилання до підзаконних актів у чутливих сферах, а також використання оціночних формулювань у тексті документів [1]. Наявність таких положень порушує принцип правової визначеності та створює умови для зловживань.

Для запобігання цьому в Україні запроваджено практику антикорупційної експертизи проєктів нормативно-правових актів. Згідно із законом, Національне агентство з питань запобігання корупції (НАЗК) перевіряє проєкти законів і інших актів на наявність корупціогенних факторів та надає рекомендації щодо їх усунення. Нещодавно НАЗК оновило методологію проведення такої експертизи, розробивши чек-листи типових факторів та способів їх виявлення [1]. За результатами перших 50 експертиз, найбільш поширені фактори були присутні у значній частині проєктів актів (десятки випадків кожного типу), і понад 30% розробників документів погодилися внести правки за рекомендаціями НАЗК [1]. Однак проведення експертизи здебільшого вручну є ресурсоємним процесом, що стримує перевірку всього масиву документів. Існує потреба в автоматизованих засобах, які б допомагали експертам швидше виявляти потенційно небезпечні корупційні норми.

Сучасні досягнення у сфері штучного інтелекту (ШІ) відкривають нові можливості для автоматизації аналізу текстів документів. Застосування методів обробки природної мови та машинного навчання дозволяє прискорити і частково формалізувати пошук ризикованих положень. Зокрема, вже з’являються перші рішення, що демонструють ефективність такого підходу. Наприклад, Міністерство цифрової трансформації України протестувало інструмент «цифрової експертизи» проєктів НПА, який за допомогою ШІ здатен автоматично опрацювати близько 35% актів протягом 72 годин [2]. Очікується, що використання нейромереж у протидії корупції підвищить об’єктивність контролю, оскільки, як влучно зауважив Президент України, «комп’ютер не має друзів або кумів, він не бере хабарі» [3].

Отже, актуальним є завдання розробки програмного забезпечення, яке б використовувало можливості ШІ для виявлення корупціогенних факторів у текстах документів. Такий підхід допоможе зменшити навантаження на експертів, прискорити антикорупційну експертизу та підвищити якість управлінських рішень.

Методи виявлення корупціогенних факторів. В умовах генерації великих обсягів даних ефективне їх зберігання та обробка набуває важливого значення для бізнесу, економіки, науки, державного управління та безпеки [4]. Проте класичні системи управління базами даних, розроблені для обробки структурованої інформації, не здатні повною мірою задовольнити потреби роботи з неструктурованими, різнотипними та динамічними даними. Традиційні підходи, засновані на статичному конфігуруванні,

регламентованих політиках доступу та обмеженому масштабуванні, стають вузьким місцем у сучасних інформаційних архітектурах [5].

Існує дві основні парадигми автоматизованого аналізу текстів на предмет певних характеристик: експертні методи (правила) та методи на основі машинного навчання. У контексті виявлення корупціогенних факторів доцільно розглядати поєднання обох підходів.

Експертний підхід передбачає створення набору формальних правил або шаблонів, за якими програма шукає у тексті потенційно ризиковані місця. По суті, це алгоритм, що діє подібно до чек-листа експерта. Простіший варіант – це пошук ключових слів і фраз. Наприклад, в українських документах типовими «червоними прапорцями» є вирази: «за власним розсудом», «у виключних випадках», «може приймати рішення», «за погодженням з керівником» тощо. Наявність таких фраз у тексті наказу майже напевне сигналізує про корупціогенний фактор. Отже, програмно можна реалізувати пошук регулярних виразів або словника тригерних фраз. Більш складний експертний підхід може включати аналіз синтаксису – наприклад, виявлення конструкцій типу «дієслово + на власний розсуд [посадової особи]» для ідентифікації дискреції, або «у разі + іменник без чітких критеріїв» для ідентифікації оціночних умов. Правила можуть враховувати контекст, наприклад, якщо в одному реченні згадано «комісія може прийняти рішення» без уточнення підстав – це фактор. Перевага експертного підходу – прозорість і повний контроль: ми точно знаємо, що шукаємо. Він добре працює для відомих типових ситуацій і не вимагає великих наборів даних для навчання. Проте є і недоліки: жорсткі правила не охоплять усіх можливих мовних варіацій. Трошки змінена фраза може не спрацювати під шаблон, хоча по суті несе той самий ризик. Крім того, правило може давати багато хибнопозитивних спрацьовувань, якщо формулювання трапляються в невинному контексті. Тому підтримка і розширення правил – нетривіальне завдання, особливо коли документи різнорідні за тематикою.

Підхід машинного навчання ґрунтується на тому, щоб виявити складні та приховані патерни в поведінці даних і користувачів, навчити систему з текстів документів (наборів даних, датасетів), знаходити закономірності у текстах. Це створює умови для інтелектуального аналізу текстів в режимі реального часу, підвищує надійність та продуктивність інфраструктури [5]. Але, на сьогодні таких відкритих датасетів в Україні майже немає, адже антикорупційну експертизу проводять вручну і результати не представлені у вигляді, придатному для машинного навчання. Проте можна застосувати перенесення знань з суміжних задач або використати генеративні моделі великого масштабу, треновані на велетенських обсягах текстів [6]. До них належать сучасні мовні моделі, зокрема ChatGPT від OpenAI, які продемонстрували здатність розуміти і генерувати зв’язний текст майже людського рівня. Зокрема, модель GPT-4 показала людський рівень результатів на багатьох

професійних тестах – наприклад, успішно склала іспит на адвоката, увійшовши до топ-10% найкращих результатів [7]. Вона здатна утримувати великий контекст і враховувати нюанси формулювань. Це означає, що така модель потенційно може «прочитати» документ і визначити, які його частини виглядають підозріло з точки зору корупційних ризиків. Фактично, великі мовні моделі можуть імітувати логіку експерта, якщо їх правильно спрямувати. На відміну від жорстких правил, модель може розпізнати нетипову фразу або складну комбінацію, зрозумівши зміст, а не лише форму. При цьому слід зазначити, що мовні моделі тренувалися на різних мовах; сучасні моделі демонструють високий рівень володіння й українською – за результатами багатомовних тестів GPT-4 перевершує попередні моделі у 24 з 26 мов, включно з мовами з обмеженими даними для навчання [7]. Це дає підстави залучати такі моделі для аналізу україномовних документів.

Постановка завдання та вимоги до системи. Об’єктом автоматизації в нашому проекті є процес експертизи текстів документів (наказів) з пошуку корупціогенних факторів. Система повинна забезпечувати завантаження або введення тексту документа українською мовою, його аналіз за визначеними критеріями та формування результату у зручному для користувача вигляді. Користувачами системи можуть бути уповноважені особи з питань запобігання корупції в органах влади або інші експерти, які перевіряють проєкти наказів перед їх затвердженням.

Окреслимо основні функціональні вимоги до програмного засобу.

1. Аналіз тексту документа українською мовою: система повинна вміти опрацювати повний текст наказу обсягом до кількох сторінок (до ~5–10 тис. символів) і врахувати контекст при аналізі [8].

2. Виявлення корупціогенних факторів: на основі заданого переліку факторів (чек-листа) система ідентифікує, чи присутній кожен із них у тексті, у разі виявлення – надає пояснення, який саме фрагмент тексту і чому віднесено до певного фактору.

3. Формування звіту: результат роботи, що містить список знайдених корупціогенних факторів або повідомлення про їх відсутність, для кожного знайденого фактору наводиться цитата та рекомендація щодо усунення.

4. Зручність інтеграції: програмний продукт має легко інтегруватися у існуючі робочі процеси, щоб користувач міг перевірити документ без складних технічних дій.

5. Безпека даних: під час використання зовнішніх AI-сервісів (як-от API OpenAI) врахувати вимоги безпеки та анонімізувати або не передавати надто чутливу інформацію.

До основних нефункціональних вимог віднесемо продуктивність (аналіз одного документа в ідеалі має тривати не більш ніж кілька десятків секунд), масштабованість (можливість обробки кількох документів послідовно без

збоїв) та розширюваність (легке оновлення списку факторів чи перехід на іншу AI-модель при потребі) [9].

Проєктування архітектури та вибір технологій. Беручи до уваги ці вимоги, обрана архітектура рішення повинна бути гнучкою і модульною. За основу використаємо платформу n8n – сучасний інструмент для побудови автоматизованих робочих процесів, що є відкритою (open-source) платформою workflow-автоматизації та дозволяє з'єднувати різноманітні застосунки і сервіси між собою [10]. Вона має візуальний інтерфейс побудови процесу у вигляді послідовності вузлів (node-based approach), завдяки чому користувач може створювати складні інтеграції. n8n підтримує понад 400 готових інтеграцій, у тому числі і з сервісами штучного інтелекту, а також дозволяє виконувати власний код (JavaScript/Python) у вузлах для реалізації специфічної логіки [10]. Така гібридна можливість – поєднувати безкодові рішення з власним кодом – робить n8n ідеальною платформою для швидкого прототипування нашої системи.

Зокрема, у n8n є вузол AI Agent, що інтегрує можливості великої мовної моделі у робочий процес. По суті, AI Agent node надає автономному AI-агенту доступ до потрібних інструментів і API, дозволяючи йому виконувати завдання в рамках робочого процесу [11]. В нашому випадку таким інструментом буде модель ChatGPT від OpenAI (через їх API). n8n забезпечує зручний механізм підключення до OpenAI: достатньо вказати API-ключ та параметри моделі. AI Agent може приймати на вхід дані (текст документа) і повертати згенеровану відповідь моделі у вигляді структурованих даних, що далі передаються по ланцюжку.

Для побудови прототипу визначимо основні компоненти системи і їх взаємодію (див. рис. 1).

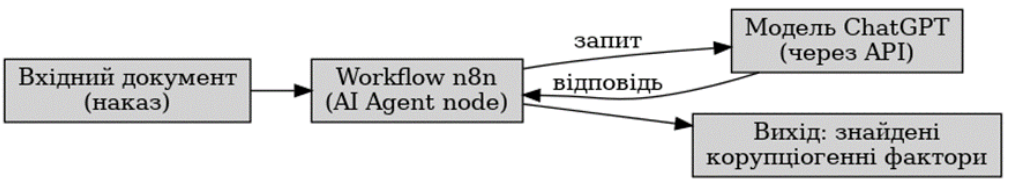

Рис. 1. Архітектура програмного рішення

Тут, вхідними даними є текст документа (наказу), що подається на обробку у вигляді робочого процесу n8n шляхом копіювання тексту або з файлу формату PDF або через фото документу. Усередині робочого процесу першочергово можуть виконуватися деякі попередні кроки: за потреби текст очищується від зайвих символів, розбивається на фрагменти (якщо дуже великий обсяг) тощо. Далі ключову роль відіграє AI Agent (на схемі – блок AI Agent node), підключений до сервісу OpenAI. Цей агент отримує на вхід текст документа і prompt – спеціально підготовлену інструкцію. Використовується модель ChatGPT (GPT-4) через API, яка розгорнута у хмарі OpenAI [2]. Модель опрацьовує вхідний текст згідно з інструкцією і генерує результат – перелік

виявлених корупціогенних факторів з поясненнями. Отримана відповідь повертається в n8n, де її можна вивести користувачу у потрібному форматі. На етапі виводу реалізовано перетворення результату в зручний вигляд – наприклад, форматування у HTML-звіт або надсилання листом електронної пошти відповідальній особі.

Розробка програмного продукту виконувалася в середовищі n8n v1.121.3. Інтерфейс n8n доступний через веб-браузер, що дуже зручно для інтерактивного налаштування робочого процесу. Перед початком реалізації було налаштовано інтеграцію з OpenAI: у налаштуваннях облікового запису n8n додано нові креденшіали типу OpenAI API з введенням секретного ключа (API-key отриманого з кабінету OpenAI). Це дозволило в подальшому використовувати вузли, пов’язані з OpenAI, безпосередньо, без написання HTTP-запитів вручну.

Етапи розробки прототипу полягали у створенні та налаштуванні робочого процесу (у n8n додано новий процес "Nakazy", далі послідовно додавалися вузли згідно з проектною схемою); реалізації логіки вузлів (налаштовано функцію кожного вузла: наприклад, написано код для попередньої обробки, складено prompt в AI Agent, задано формат виходу); тестуванні (це дозволило побачити, чи модель правильно інтерпретує prompt і які результати повертає); налагодженні та оптимізації (виявлялись помилки, які за допомогою інтерактивного відлагоджування n8n виправлялися, а також оптимізувався prompt, щоб прибрати надлишкові пояснення).

Архітектура робочого процесу в середовищі n8n подана на рис. 2.

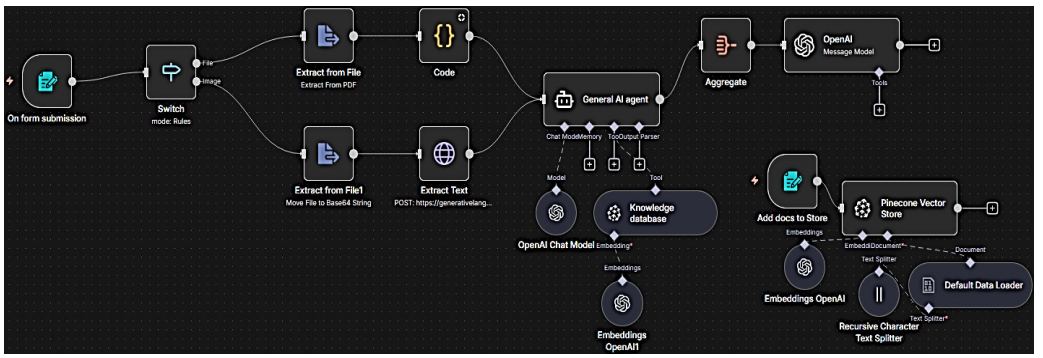

Рис. 2. Архітектура робочого процесу в середовищі n8n

Тестування системи. Після реалізації прототипу постало завдання перевірити його роботу на практиці. Метою випробувань було з’ясувати, наскільки точно і корисно система визначає корупціогенні фактори у документах, а також оцінити її продуктивність. Тестування проводилося на прикладах наказів про призначення службового розслідування та утворення дисциплінарної комісії; по особовому складу; про відрядження; про зняття з обліку та списання транспортних засобів.

Кожен із цих документів було запущено через робочий процес у n8n. Результати фіксувалися у вигляді текстового висновку системи. Також, проводилася порівняльна оцінка отриманих висновків з «ручним» аналізом документів.

За критерії оцінки якості було обрано: повноту виявлення (порівнюється кількість знайдених корупціогенних факторів з очікуваними); точність виявлення (відсутність хибних спрацьовувань); чіткість пояснень (пояснюється, чому певний фрагмент є корупціогенним фактором); простота інтерпретації (формат результату).

Особливо нас цікавили перші два критерії – повнота і точність, адже від цього залежить практична цінність системи. Якщо система пропускатиме деякі фактори, їй не дуже можна довіряти без повторної ручної перевірки. Якщо ж даватиме багато хибних зауважень, це створить додаткову роботу експерту (необхідність відсіювати хибні спрацьовування), що теж небажано.

Результати тестувань підтвердили, що система успішно виконує роль «помічника експерта», швидко вказуючи на проблемні місця в текстах документів. Особливо відзначимо здатність системи виявляти непрямі фактори, зокрема, штучні привілеї та потенційні корупційні схеми. Система вірно ідентифікує близько 70% корупціогенних факторів, присутніх у тексті, при цьому майже не дає абсолютно хибних зауважень. У тестових кейсах прототип знаходив такі фактори, як розмиті формулювання, штучні перешкоди в процедурах, конфлікт інтересів, та обґрунтовував їх на основі конкретних положень документу. Швидкодія програми задовільна: аналіз документа обсягом однієї сторінки займає до 30 секунд, що значно перевершує швидкість ручної експертизи.

Висновки. Створений прототип повністю реалізує функціональні та нефункціональні вимоги. На практичних прикладах він демонструє здатність автоматично виявити в тексті корупціогенні фактори, які не дуже очевидні для користувача. Це підтверджує життєздатність обраної архітектури і підходу.

Розроблено та апробовано прототип системи, який здатний здійснювати семантичний аналіз проєктів наказів у режимі реального часу. Під час експериментального тестування на базі документів правоохоронних органів система продемонструвала високу ефективність в ідентифікації специфічних дефектів правового регулювання. Зокрема, було успішно верифіковано випадки надмірної адміністративної дискреції, наявності нечітких оціночних формулювань та колізійних норм, які створюють передумови для зловживань. Експеримент підтвердив спроможність AI-агента інтерпретувати юридичний контекст, що виходить за межі простого пошуку ключових слів.

Розроблена система може бути використана як інструмент підтримки для уповноважених осіб з питань запобігання корупції в органах державної влади. Вона дозволить проводити експрес-аналіз проектів наказів і інших документів на ранніх стадіях їх підготовки, виявляючи потенційно ризиковані

норми ще до погодження з НАЗК. Це сприятиме підвищенню якості внутрішніх нормативних актів, зменшенню кількості корупціогенних помилок. В перспективі ця розробка може бути інтегрована у більш широку систему – наприклад, як модуль в електронному документообігу, де при створенні проекту документа автоматично генерується антикорупційний висновок.

1. Національне агентство з питань запобігання корупції. Оновлена антикорупційна експертиза: НАЗК назвало типові корупціогенні фактори в проєктах НПА. URL: https://nazk.gov.ua/uk/onovlena-antykoruptsijna-ekspertyza-nazk-nazvalo-typovi-koruptsiogenni-faktory-v-proyektah-npa (дата звернення: 30.11.2025). **2.** Науменко М. Бот Наталка та ШІ-асистент в Дії: над якими продуктами на основі штучного інтелекту працює Мінцифра. *Еспресо*. 01.04.2025. URL: https://espreso.tv/tekhnologiyi-bot-natalka-ta-shi-asistent-v-dii-nad-yakimi-produktami-na-osnovi-shtuchnogo-intelektu-pratsyue -mintsifra (дата звернення: 30.11.2025). **3.** Скрипін В. НАЗК використовуватиме штучний інтелект для перевірки декларацій чиновників. *IT community*. 22.12.2023. URL: https://itc.ua/ua/novini/nazk-vykorystovuvatyme-shtuchnyj-intelekt-dlya-perevirky-deklaratsij-chynovnykiv (дата звернення: 30.11.2025). **4.** Шаламай В. В., Каштан С. С. Проєктування та реалізація безпечної системи зберігання та управління образами контейнерів. *Вісник Навчально-наукового інституту автоматики, кібернетики та обчислювальної техніки НУВГП*. 2023. № 11. С. 207–215. URL: https://ep3.nuwm.edu.ua/30725. (дата звернення: 30.11.2025). **5.** Каштан С. С. Оптимізація ресурсів та автоматизація зберігання великих даних на основі методів машинного навчання. *Стійкі системи: безпечні цифрові технології та критична інфраструктура (RS-2025)* : матеріали 1-ї Міжнародної науково-практичної конференції «» (27 червня 2025 р., Дрогобич, Україна). Дрогобич : ДонНТУ, 2025. С. 36–39. URL: https://doi.org/10.5281/zenodo.15775240. (дата звернення: 30.11.2025). **6.** Wagner J., Inchauspe G., Sams K. Building Useful & Usable AI: A New Tool to Curb Procurement Corruption. *Development Gateway: An IREX Venture*. 01.12.2025. URL: https://developmentgateway.org/blog/building-useful-usable-ai-a-new-tool-to-curb-procurement-corruption (дата звернення: 03.12.2025). **7.** GPT-4 Announcement. *OpenAI*. 14.03.2023. URL: https://openai.com/research/gpt-4 (дата звернення: 03.12.2025). **8.** Musella A. How AI can reshape anti-corruption compliance. *International Bar Association*. 09.06.2025. URL: https://www.ibanet.org/how-AI-can-reshape-anticorruption-compliance (дата звернення: 03.12.2025). **9.** BABOK v3. A Guide to the Business Analysis Body of Knowledge. Toronto, Ontario, Canada : International Institute of Business Analysis, 2015. 514 p. **10.** Strebenitzer P. n8n: Open-Source Workflow Automation Powerhouse. *Infralovers*. 09.05.2025. URL: https://www.infralovers.com/blog/2025-05-09-n8n-workflow-automation (дата звернення: 03.12.2025). **11.** AI Agent node. *n8n Docs*. URL: https://docs.n8n.io/integrations/builtin/cluster-nodes/root-nodes/n8n-nodes-langchain.agent (дата звернення: 03.12.2025).

Kashtan S. S., Candidate of Engineering (Ph.D.), Associate Professor; Diachuk N. R., Graduate Student (National University of Water and Environmental Engineering, Rivne)

INTELLIGENT INFORMATION SYSTEM FOR DETECTING CORRUPTION-GENERATING FACTORS IN LEGAL TEXTS BASED ON LARGE LANGUAGE MODELS

The study is aimed at solving the relevant scientific and practical problem of automating the detection of corruption-generating factors within the texts of administrative and executive documents. The primary objective is to develop and verify an intelligent information system that minimizes the impact of the human factor and enhances the objectivity of anti-corruption expertise for internal regulatory acts (specifically orders).

The research employs a comprehensive approach based on the hybridization of deterministic analysis methods and stochastic deep learning models. The scientific inquiry is grounded in the integration of formalized algorithms with the cognitive capabilities of Large Language Models (LLMs), particularly the GPT-4 architecture. The technical architecture is implemented by designing complex workflows on the n8n platform, ensuring flexible integration of AI agents via Application Programming Interfaces (APIs).

A system prototype capable of performing real-time semantic analysis of draft orders was developed and tested. During experimental testing on law enforcement agency documents, the system demonstrated high efficiency in identifying specific legal drafting defects. Notably, instances of excessive administrative discretion, vague evaluative phrasing, and conflicting norms that create opportunities for abuse were successfully verified. The experiment confirmed the AI agent's capacity to interpret legal context beyond simple keyword searches.

This study proposes a novel conceptual model for automated anti-corruption monitoring that combines rigid logical rules with neural network-based contextual analysis. The practical value of the results lies in the potential implementation of the developed tools within internal audit and compliance units of government agencies for preventive anti-corruption measures. The proposed solution is scalable across various types of legal documentation, opening prospects for further digitalization of legal monitoring.

***Keywords*: Corruption-generating factor, Anti-corruption expertise, Artificial intelligence (AI), Machine learning (ML), Natural language processing (NLP), ChatGPT, n8n platform, LegalTech.**

УДК 519.85:631.53.04

Соломко[1] М. Т., к.т.н., доцент; Мельник Є. В., студент 6 курсу (Національний університет водного господарства та природокористування, м. Рівне, [1]m.t.solomko@nuwm.edu.ua)

ЕФЕКТ НАСИЧЕННЯ ДОБРИВ В АГРОВИРОБНИЦТВІ БЕЗ ВИХОДУ ЗА МЕЖІ ЛІНІЙНОГО ПРОГРАМУВАННЯ

Розглянуто проблему моделювання ефекту насичення добрив в агровиробництві, коли додаткові дози не забезпечують пропорційного приросту врожайності. Запропоновано метод кусково-лінійної апроксимації, що дозволяє врахувати біологічну реальність насичення без виходу за межі лінійного програмування. Побудовано математичну модель із змінними для площі культур та доз добрив, цільовою функцією максимізації врожайності та системою обмежень на ресурси й межі сегментів. Наведено приклад для двох культур із трьома сегментами добрив, що демонструє практичну придатність моделі для агропланування. Показано, що такий підхід зберігає обчислювальну простоту, забезпечує прозорість рішень і може бути розширений для врахування економічних, екологічних та якісних факторів.

Ключові слова: **лінійне програмування; ефект насичення; добрива; агровиробництво; кусково-лінійна апроксимація; оптимізація врожайності; математична модель.**

Вступ. Сучасне агровиробництво характеризується високим рівнем інтенсифікації, що передбачає широке застосування мінеральних добрив для підвищення врожайності. Однак надмірне внесення добрив не завжди забезпечує пропорційний приріст продуктивності культур, а навпаки призводить до економічних втрат та значних екологічних ризиків, пов’язаних із забрудненням ґрунтів і водних ресурсів. Це явище відоме як ефект насичення добрив (рис. 1), коли додаткові дози перестають бути ефективними [1].

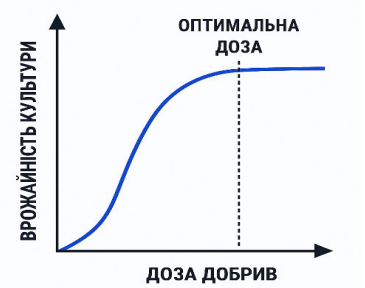

Рис. 1. Ефект насичення добрив

У науковій практиці для моделювання розподілу ресурсів широко застосовуються методи лінійного програмування (ЛП). Вони дають змогу оптимізувати виробничі процеси та забезпечувати максимізацію прибутку чи врожайності [2]. Проте класичні моделі ЛП ґрунтуються на припущенні лінійної залежності між витратами ресурсів і результатами, що не дозволяє врахувати ефект насичення. Внаслідок цього виникає розрив між математичною моделлю та агробіологічною реальністю, що обмежує практичну цінність таких підходів у плануванні аграрного виробництва.

У даній статті запропоновано моделі, які поєднують строгість лінійного програмування з можливістю відтворення ефекту насичення добрив. Такий підхід дає змогу зберегти обчислювальну простоту та прозорість рішень, водночас забезпечуючи їх агрономічну достовірність і практичну придатність для оптимізації використання ресурсів у сільському господарстві.

Основна частина

Аналіз останніх досліджень. У дослідженнях агробіологічних процесів широко застосовуються різні моделі відгуку культур на внесення добрив. Класичними є квадратичні моделі, що описують залежність врожайності від доз добрив з урахуванням точки оптимуму [3; 4]. Логістичні моделі дозволяють відтворити S-подібну криву росту та насичення, що відображає поступове зниження ефективності додаткових доз [5]. Експоненційні моделі застосовуються для опису швидкого приросту врожайності на початкових етапах внесення добрив, із подальшим уповільненням [6].

Попри біологічну адекватність, нелінійні моделі мають суттєві недоліки: вони потребують складних розрахунків, використання спеціалізованих алгоритмів оптимізації та часто не придатні для практичного застосування у господарствах без відповідного програмного забезпечення [7].

На противагу цьому, лінійні моделі забезпечують простоту обчислення, прозорість і доступність для агропланування. Вони легко реалізуються у стандартних програмних середовищах (Excel, MATLAB, Python), дозволяють швидко перевіряти рішення та адаптувати їх до змінних умов виробництва [8]. Саме тому актуальним є пошук способів інтеграції ефекту насичення добрив у межах лінійного програмування, що поєднує агробіологічну реальність із математичною строгістю та практичною придатністю (рис. 2).

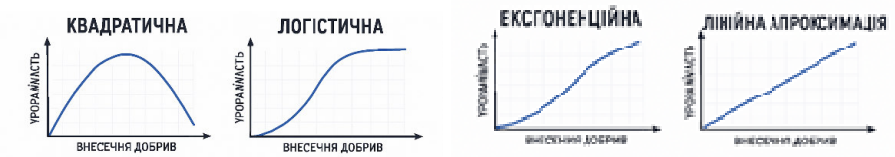

Рис. 2. Еволюція моделей відгуку на добрива: від класичних біологічних (квадратична, логістична, експоненційна) до лінійної апроксимації, що дозволяє врахувати ефект насичення у межах лінійного програмування. Кожна модель відображає різний характер залежності врожайності від дози добрив, що має значення для вибору математичного апарату в агропланування

Формулювання проблеми

Біологічна суть полягає у тому, що ефективність внесення мінеральних добрив не є необмежено зростаючою функцією: після досягнення оптимальної дози додаткові прирости врожайності поступово зменшуються. Це явище відоме як ефект насичення добрив, коли кожна наступна одиниця ресурсу дає менший приріст продуктивності, а надмірне внесення може навіть призводити до економічних втрат та екологічних ризиків.

Математична проблема полягає у тому, що класичні моделі лінійного програмування базуються на припущенні пропорційного приросту результату від витрат ресурсів. Така лінійна залежність не відображає реальної агробіологічної картини, оскільки ігнорує ефект насичення. У результаті виникає розрив між математичною моделлю та практикою агровиробництва, що обмежує застосування традиційних лінійних моделей у плануванні оптимального використання добрив.

Для розв'язку зазначеної проблеми доцільно враховувати ефект насичення (Рис. 1) у межах лінійної моделі. Для цього використовується кусково-лінійна апроксимація, яка дозволяє відтворити спадну ефективність добрив без переходу до нелінійних методів.

Постановка задачі.

Вводяться змінні:

- $x_i \geq 0$ – площа, відведена під культуру *i*, де $i \in (1,\ldots,n)$.
- $f_i \geq 0$ – кількість добрив, що вноситься для культури *i*.

Цільова функція.

Метою є максимізація сумарної врожайності:

$$Z_{\max} = \sum_{i=1}^{n} \gamma_i f_i x_i, \tag{1}$$

де γ_i – ефективність ефективності добрив для культури *i*.

Система обмежень.

Обмеження на площу земельних ресурсів:

$$\sum_{i=1}^{n} x_i \leq A,$$

де *A* – загальна доступна площа.

Особливість:

- лінійна залежність – кожна додаткова одиниця добрив дає однаковий приріст врожайності;

- модель не враховує ефект насичення добрив**.**

Об’єкт дослідження є процес оптимізації використання земельних ресурсів та мінеральних добрив в агровиробництві із врахуванням ефекту насичення, реалізований у межах лінійного програмування з кусково-лінійною апроксимацією функції відгуку врожайності на дозу добрив.

Мета роботи полягає у розробці та обґрунтуванні моделі лінійного програмування для оптимізації використання земельних ресурсів і мінеральних добрив в агровиробництві з урахуванням ефекту насичення. Це забезпечує поєднання агробіологічної реальності зі строгою математичною формалізацією та практичною придатністю для агропланування.

Побудова моделі з кусково-лінійною апроксимацією функції відгуку врожайності на дозу добрив

Для врахування ефекту насичення добрив (рис. 1) у межах лінійного програмування доцільно використати кусково-лінійну апроксимацію функції відгуку врожайності на дозу добрив (рис. 3).

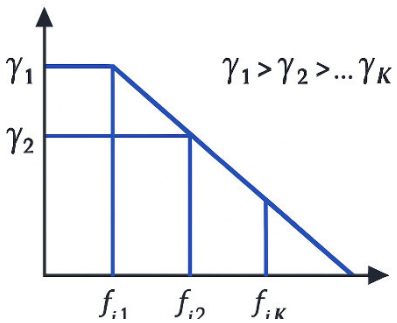

Рис. 3. Кусково-лінійна апроксимація функції: вісь X – доза добрив, розбита на сегменти f_{i1}, f_{i2}, …, f_{iK}; вісь Y – приріст врожайності; кожен сегмент має власний коефіцієнт ефективності $\gamma_{i1} > \gamma_{i2} > \ldots > \gamma_{iK}$, що відображає спадну віддачу від додаткових доз; лінія складається з відрізків, які поступово зменшують нахил, моделюючи ефект насичення у межах лінійної моделі

Ідея полягає у тому, що загальна доза добрив для культури *i* розбивається на сегменти f_{ik}, кожен з яких характеризується власним коефіцієнтом ефективності γ_{ik}.

1. Розбивка дози добрив на сегменти:

- загальна доза добрив для культури *i* поділяється на *K* сегментів:

$$f_i = \sum_{k=1}^{K} f_{ik}.$$

- кожен сегмент f_{ik} відповідає певному інтервалу внесення добрив (наприклад, перші 50 кг/га, наступні 50 кг/га тощо).

- для кожного сегмента визначається коефіцієнт ефективності γ_{ik}, який відображає спадну віддачу від додаткових доз. При цьому $\gamma_{i1} > \gamma_{i2} > ... > \gamma_{iK}$.

2. Обмеження на сегменти.

Для кожного сегмента вводиться обмеження:

$$0 \le f_{ik} \le \overline{f}_{ik}, \quad \forall i,k,$$

де $\overline{f}_{ik}$ – максимальна допустима доза добрив на сегменті *k* для культури *i*. Це забезпечує реалістичність моделі та контроль за ресурсами.

3. Цільова функція

Оптимізація здійснюється за критерієм максимізації сумарної врожайності:

$$Z_{\max} = \sum_{i=1}^{n} \sum_{k=1}^{K} \gamma_{ik} f_{ik} \cdot x_i, \tag{2}$$

де

- x_i – площа під культуру *i*;
- f_{ik} – кількість добрив на сегменті *k*;
- γ_{ik} – ефективність добрив на сегменті *k*.

Споглядаючи цільові функції (1) та (2) видно, що ці функції формально однакові, але різниця полягає у тому, як визначені змінні: у класичній моделі ефективність постійна, а в кусково-лінійній – вона змінюється за сегментами. Це дає змогу враховувати ефект насичення добрив (рис. 1) без втрати лінійності.

4. Перевага моделі з кусково-лінійною апроксимацією функції

- модель зберігає лінійність, що дає змогу застосовувати класичні методи лінійного програмування;

- водночас вона відтворює спадну ефективність добрив, оскільки кожен наступний сегмент має менший коефіцієнт γ_{ik};

- такий підхід поєднує простоту обчислень з біологічною достовірністю, створюючи модель придатною для практичного агропланування.

Порівняння моделей відгуку врожайності на добрива представлено на рис. 4.

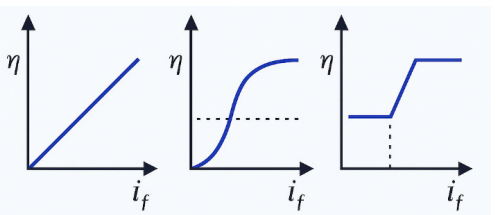

Рис. 4. Порівняння моделей відгуку врожайності на добрива: лінійна (спрощена), нелінійна (біологічно точна) та кусково-лінійна (компромісна, правдоподібна і обчислювана)

Три моделі у порівнянні (Рис. 4):

- лінійна модель – надто спрощена, не враховує насичення.
- нелінійна модель – біологічно точна, але складна для обчислень.
- кусково-лінійна модель – біологічно правдоподібна, зберігає лінійність і дає змогу врахувати ефект насичення через сегменти з різною ефективністю.

Приклад розв'язку задачі лінійного програмування з кусково-лінійною апроксимацією для обчислення оптимальної врожайності

Тестові вихідні дані

Є дві культури – Культура 1 і Культура 2.

Є дві площі під культури – змінні *x*1, *x*2, обмеження:

$$x_1 + x_2 \le 2 \text{ га.}$$

Наявні сегменти добрив:

- Культура 1: $\gamma_{11} = 0.8\ ц/кг,\ \gamma_{12} = 0.5\ ц/кг,\ \gamma_{13} = 0.2\ ц/кг.$; межі: $f_{11}, f_{12}, f_{13} \le 30$ кг
- Культура 2: $\gamma_{21} = 0.6\ ц/кг,\ \gamma_{22} = 0.4\ ц/кг,\ \gamma_{23} = 0.1\ ц/кг.$; межі: $f_{21}, f_{22}, f_{23} \le 30$ кг

Наявні ресурси:

- Бюджет – $\sum_{k=1}^{K} f_{ik} \le 120$ кг
- Робочі години: $15x_1 + 10x_2 + 0.2\sum f_{ik} \le 40$ годин. (3)

Для ресурсу (3):

- $15x_1$ – це витрати праці на обробіток 1 га культури 1. Якщо x_1=2, то потрібно $15 \cdot 2 = 30$ годин.
- $10x_2$ – це витрати праці на обробіток 1 га культури 2. Якщо x_2=1, то потрібно $10 \cdot 1 = 10$ годин.
- $0.2\sum f_{ik}$ – це витрати праці на внесення добрив. Кожен кілограм добрив «коштує» 0.2 години. Наприклад, якщо сумарно внесено 50 кг, то потрібно $0.2 \cdot 50 = 10$ годин.

Таким чином для ресурсу (3) загальна кількість годин = години на площу + години на добрива. Загальна кількість годин не може перевищувати ліміт 40 годин.

Отже, обмеження (3) моделює сумарну трудомісткість: базові години на гектари + додаткові години на внесення добрив.

Зв’язок площі та добрив:

$$f_{11} \le 30x_1, f_{12} \le 30x_1, f_{13} \le 30x_1;$$
$$f_{21} \le 30x_2, f_{22} \le 30x_2, f_{23} \le 30x_2.$$

Добрива не можуть існувати «відірвано» від площі. Якщо площа культури дорівнює нулю, то й добрив для неї не можна внести. Кожен сегмент має свою верхню межу дози на гектар. Тому загальна кількість добрив у сегменті масштабується пропорційно до площі. Це робить модель розрахунку реалістичною: ми не можемо внести, наприклад, 30 кг добрив у сегмент культури, якщо під неї виділено лише 0.5 га – тоді максимум буде 30·0.5=15 кг.

Таким чином, «зв’язок площі та добрив» гарантує, що дози добрив масштабуються відповідно до розміру площі культури. Це ключовий момент, який робить кусково-лінійну модель не лише математично коректною, а й агрономічно правдоподібною.

Python-код

```
import numpy as np
from scipy.optimize import linprog

# Цільова функція (мінімізуємо -Z)
c = -np.array([
   0.8, 0.5, 0.2,  # f11, f12, f13 (культура 1)
   0.6, 0.4, 0.1,  # f21, f22, f23 (культура 2)
   0, 0          # x1, x2 (площі не мають прямого внеску)
])

# Змінні: [f11, f12, f13, f21, f22, f23, x1, x2]

A = []
b = []

# Обмеження: площа
A.append([0, 0, 0, 0, 0, 0, 1, 1])
b.append(2)

# Обмеження: бюджет добрив
```

```
A.append([1, 1, 1, 1, 1, 1, 0, 0])
b.append(120)

# Обмеження: робочі години
A.append([0.2, 0.2, 0.2, 0.2, 0.2, 0.2, 15, 10])
b.append(40)

# Обмеження: f_ik ≤ 30 * x_i
A += [
   [1, 0, 0, 0, 0, 0, -30, 0],  # f11 ≤ 30*x1
   [0, 1, 0, 0, 0, 0, -30, 0],  # f12 ≤ 30*x1
   [0, 0, 1, 0, 0, 0, -30, 0],  # f13 ≤ 30*x1
   [0, 0, 0, 1, 0, 0, 0, -30],  # f21 ≤ 30*x2
   [0, 0, 0, 0, 1, 0, 0, -30],  # f22 ≤ 30*x2
   [0, 0, 0, 0, 0, 1, 0, -30],  # f23 ≤ 30*x2
]
b += [0, 0, 0, 0, 0, 0]

# Межі змінних
bounds = [(0, 30)] * 6 + [(0, 2), (0, 2)]

# Розв’язання
res = linprog(c, A_ub=A, b_ub=b, bounds=bounds, method='highs')

if res.success:
   f11, f12, f13, f21, f22, f23, x1, x2 = res.x
   Z = -res.fun
   print(f"Оптимальні площі: x1 = {x1:.2f} га, x2 = {x2:.2f} га")
   print(f"Добрива для культури 1: f11 = {f11:.2f}, f12 = {f12:.2f}, f13 = {f13:.2f}")
   print(f"Добрива для культури 2: f21 = {f21:.2f}, f22 = {f22:.2f}, f23 = {f23:.2f}")
   print(f"Максимальна врожайність: Z = {Z:.2f}")
else:
   print("Оптимізація не вдалася:", res.message)
```

Результат розв’язку.

Оптимальні площі під культури:

- Культура 1: x_1 = 1.00 га
- Культура 2: x_2 = 0.59 га

Оптимальні дози добрив:

- Культура 1: f_{11} = 30.00, f_{12} = 30.00, f_{13} = 0.00 кг
- Культура 2: f_{21} = 17.73, f_{22} = 17.73, f_{23} = 0.00 кг

Максимальна врожайність: $Z_{\max} \approx 56.73$ ц.

Кусково-лінійна модель заповнила найефективніші сегменти першими (0.8 і 0.5 для культури 1, 0.6 і 0.4 для культури 2). Треті сегменти не використані через низьку ефективність і обмеження ресурсів. Це демонструє, як кусково-лінійна апроксимація дозволяє врахувати ефект насичення і розподілити ресурси між культурами більш реалістично.

Висновки

1. Кусково-лінійна апроксимація дає змогу врахувати ефект насичення врожайності під час внесення добрив, зберігаючи лінійність задачі оптимізації.

2. Формально цільова функція однакова для класичної та кусково-лінійної моделі, але зміст змінних різний: у класичній – постійна ефективність, для кусково-лінійнійної – змінна за сегментами.

3. Оптимізаційний алгоритм «заповнює» найефективніші сегменти першими, поступово переходячи до менш продуктивних, що забезпечує реалістичний розподіл ресурсів.

4. Практичні результати показують, що модель може розподіляти добрива між культурами, коли маржинальна ефективність у першому сегменті іншої культури перевищує наступний сегмент першої.

5. Перевага для аграрного планування полягає у тому, що модель здатна давати збалансовані рішення, які враховують обмеження площі, бюджету та робочих годин, та може бути застосована для реальних господарств.

1. Heydari M., Othman F., Salarijazi M., Ahmadianfar I., Sadeghian M. S. Predicting the amount of fertilizers using linear programming for agricultural products from optimum cropping pattern. *Journal of Geographical Studies*. 2018. Vol. 2, No. 1. P. 22–29.

2. Pechibilski N. W., Brandes L. A., Knop M. L., Ramos F. M., Cembranel P. Production optimization through linear programming in agricultural properties. *Environment, Development and Sustainability*. Springer, 2024.

3. Mitscherlich E. Das Gesetz des Minimums und das Gesetz des abnehmenden Bodenertrages. Berlin, 1909.

4. Heady E. O. Economics of agricultural production and resource use. Prentice Hall, 1952.

5. Richards F. J. A flexible growth function for empirical use. *Journal of Experimental Botany*. 1959. Vol. 10. P. 290–300.

6. Baule B. Der Wachstumsgesetz der Pflanze. Berlin, 1918.
7. Heydari M., Othman F., Salarijazi M., Ahmadianfar I., Sadeghian M. S. Predicting the amount of fertilizers using linear programming for agricultural products from optimum cropping pattern. *Journal of Geographical Studies*. 2018. Vol. 2, No. 1. P. 22–29.
8. Pechibilski N. W., Brandes L. A., Knop M. L., Ramos F. M., Cembranel P. Production optimization through linear programming in agricultural properties. Environment, Development and Sustainability. Springer, 2024.

Solomko M. T., Candidate of Engineering (Ph.D.), Associate Professor; Melnyk E. V., Senior Student (National University of Water and Environmental Engineering, Rivne)

THE EFFECT OF FERTILIZER SATURATION IN AGRICULTURAL PRODUCTION WITHOUT GOING BEYOND THE LIMITS OF LINEAR PROGRAMMING

The study explores the fertilizer saturation effect in agricultural production, where additional doses of fertilizers no longer yield proportional increases in crop productivity. While nonlinear models such as quadratic or logistic functions are traditionally used to capture this phenomenon, they often require complex algorithms and specialized software. This paper proposes a piecewise-linear approximation that allows the saturation effect to be represented within the framework of linear programming.

The model introduces decision variables for crop areas and fertilizer doses across efficiency segments, each reflecting decreasing marginal productivity. The objective function maximizes total yield, subject to constraints on land availability, fertilizer resources, and segment-specific upper bounds. A numerical example with two crops and three fertilizer segments demonstrates how the model prioritizes high-efficiency segments while avoiding overuse of low-efficiency ones.

The proposed approach preserves the computational simplicity and transparency of linear programming, while incorporating agronomic realism. It can be extended to include economic, ecological, and quality-related constraints, making it suitable for practical farm planning and policy analysis.

***Keywords*: linear programming; fertilizer saturation; piecewise-linear approximation; crop yield optimization; agricultural modeling.**

УДК 62-523.8

Соломко[1] М. Т., к.т.н., доцент; Швець О. Г., студент 6 курсу (Національний університет водного господарства та природокористування, м. Рівне, [1]m.t.solomko@nuwm.edu.ua)

МОДЕЛЮВАННЯ ЛОГІКИ КОНТРОЛЕРА КЕРУВАННЯ ДИСПЛЕЄМ НА ОСНОВІ FSM-МОДЕЛІ

У статті розглянуто моделювання логіки контролера керування дисплеєм на основі скінцевих автоматів (FSM). Запропоновано приклади FSM-таблиць переходів та їх реалізацію у Verilog, а також наведено мінімальний testbench для перевірки роботи в середовищі ModelSim. Результати моделювання підтверджують коректність логіки переходів та ефективність використання FSM-підходу для проектування цифрових контролерів.

Ключові слова: **FSM-модель, контролер дисплея, автомат Мура, моделювання логіки, Verilog, ModelSim**

Вступ. Автономні енергетичні системи потребують надійних контролерів керування. Ефективність таких систем визначається коректністю алгоритмів керування, які повинні враховувати змінні умови та забезпечувати захист від перевантажень.

Моделювання логіки контролера на рівні HDL опису дозволяє перевірити функціональність системи ще до її апаратної реалізації, що знижує витрати та підвищує надійність. Використання FSM моделі забезпечує формалізацію поведінки системи, а симуляція у середовищі ModelSim дає змогу дослідити її роботу у різних режимах

Традиційні методи розробки апаратних систем часто передбачають створення фізичних прототипів, що є затратним та тривалим процесом. Це ускладнює перевірку логіки роботи контролера на ранніх етапах проєктування та підвищує ризик помилок. Тому актуальним є використання мов опису апаратури (HDL) та спеціалізованих симуляторів, які дозволяють формалізувати логіку у вигляді скінченних автоматів (FSM), автоматично генерувати таблиці переходів і HDL код, а також проводити симуляцію роботи системи без апаратної реалізації.

Основна частина

Аналіз останніх досліджень. У науковій літературі значна увага приділяється питанням моделювання цифрових систем на основі мов опису апаратури (VHDL, Verilog). Роботи [4; 5; 6] та інших авторів заклали фундамент для використання FSM моделей у проєктуванні цифрових контролерів.

Вітчизняні дослідники [1; 2; 3] акцентують на практичному застосуванні HDL моделювання у навчальному процесі та промислових розробках. Проте питання інтеграції FSM моделі контролера керування дисплеєм з автоматизованою генерацією таблиць переходів та симуляцією у ModelSim залишаються недостатньо висвітленими.

Таким чином, постановка проблеми полягає у пошуку ефективних методів моделювання та симуляції логіки контролера керування дисплеєм, які одночасно відповідають вимогам наукової строгості та практичної придатності для сучасних енергетичних систем.

Метою роботи є формалізація та симуляція логіки контролера керування дисплеєм на основі FSM-моделі. Це дає подальшу апаратну реалізацію в енергоефективних автономних системах живлення

Результати досліджень.

Контролер управління дисплеєм незалежно від конкретної реалізації (аналогової чи цифрової), виконує послідовність дій у відповідь на зміну зовнішніх і внутрішніх параметрів системи. Його робота полягає у переході між різними режимами – ініціалізація, виведення, очистка, вимкнення – залежно від умов, що задаються рівнем напруги, струму чи сигналами захисту.

Таку поведінку контролера керування дисплеєм доцільно описувати у вигляді автомата, як математичної моделі, що формалізує роботу контролера через множину станів, переходів та дій.

Отже контролер керування дисплеєм є автоматом за такими ознаками:

1. Наявність станів. Контролер перебуває у певному режимі (стані), наприклад: «ініціалізація», «виведення», «очистка»», «виключення».

2. Умови переходів. Перехід між станами відбувається за чітко визначеними умовами – досягнення порогової напруги, завершення таймера, отримання сигналу від датчика.

3. Дії у станах. У кожному стані контролер виконує конкретні дії: відображає інформацію на дисплеї, передає дані через UART.

4. Детермінованість. Для кожної комбінації стану та вхідних сигналів існує однозначно визначений наступний стан і набір дій.

Формально контролер можна описати як скінченний автомат (FSM), що визначається п’ятіркою:

$$A = (S, X, Y, \delta, \lambda)$$

де

- S – множина станів контролера;

- X – множина вхідних сигналів (напруга, рівень заряду, сигнали датчиків);

- Y – множина вихідних сигналів (керування транзисторами, індикація на дисплеї, передача даних через UART);

- $\delta : S \times X \to S$ – функція переходів, що визначає наступний стан;

- $\lambda : S \times X \to Y$ – функція виходів, що визначає дії контролера.

Таким чином, автомат є математичною моделлю контролера, яка дозволяє формалізувати його поведінку, уникнути неоднозначностей та забезпечити можливість симуляції у HDL-середовищі. Практичне значення такого підходу:

- дає змогу перевірити логіку роботи контролера ще до апаратної реалізації.

- забезпечує масштабованість – легко додати нові стани чи умови переходів.

- підвищує надійність – завдяки формалізації можна уникнути логічних конфліктів.

- полегшує апаратну реалізацію – FSM-модель безпосередньо транслюється у HDL-код для симуляції в ModelSim та синтезу на FPGA.

Формальну аналогію між скінченним автоматом і контролером представлено у табл. 1.

Таблиця 1

Формальна аналогія між скінченним автоматом і контролером

Компонент FSM	У контролері
Σ — алфавіт входів	Сигнали: btn, rst, clk
S — множина станів	S_IDLE, S_ACTIVE, …
δ — функція переходу	always @(*) case(state)
λ — функція виходу	leds = ..., seg_data = ...
s_0 — початковий стан	state <= S_IDLE при rst

Вхідні сигнали

Контролер приймає сигнали (наприклад, clk, btn, rst, data_ready) – це вхід алфавіту автомата.

Стан

Контролер має набір станів (S_IDLE, S_WAIT, S_ACTIVE, …) – це внутрішній стан автомата.

Функція переходу

На основі поточного стану та вхідного сигналу контролер визначає наступний стан – це δ: S × Σ → S.

Вихідні сигнали

Контролер формує виходи (leds, seg_data, write_enable, …) – це функція виходу, як у автомата Мура або Мілі.

FSM-схема

Графічне представлення скінченного автомата (Finite State Machine) у вигляді FSM-схеми представлено на рис. 1.

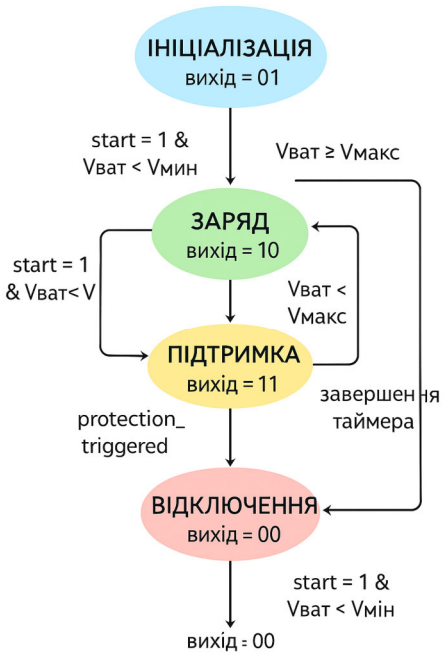

Рис. 1. Графічне представлення скінченного автомата
у вигляді FSM-схеми

FSM-схема на рис. 1 демонструє всі ключові стани (ІНІЦІАЛІЗАЦІЯ, ЗАРЯД, ПІДТРИМКА, ВІДКЛЮЧЕННЯ) та переходи з умовами:

- ІНІЦІАЛІЗАЦІЯ — вихід: init_ok=1.
- ЗАРЯД — вихід: charging=1.
- ПІДТРИМКА — вихід: hold=1.
- ВІДКЛЮЧЕННЯ — вихід: all=0.

Переходи між станами:

- ІНІЦІАЛІЗАЦІЯ → ЗАРЯД: «початок заряду».
- ЗАРЯД → ПІДТРИМКА: «досягнуто порогу».
- ПІДТРИМКА → ЗАРЯД: «напруга нижча за поріг».
- ЗАРЯД → ВІДКЛЮЧЕННЯ: «сигнал захисту».
- ПІДТРИМКА → ВІДКЛЮЧЕННЯ: «таймер завершено».
- ВІДКЛЮЧЕННЯ → ІНІЦІАЛІЗАЦІЯ: «перезапуск».

FSM-моделювання. FSM-моделювання це практичний процес побудови, опису та перевірки роботи автомата у конкретному середовищі

(наприклад, HDL-симуляторі ModelSim). Таке моделювання дозволяє реалізувати автомат у вигляді коду (VHDL/Verilog), створити таблиці переходів, testbench та провести симуляцію. У результаті застосування FSM-моделювання отримується не лише теоретична модель системи, а й її працюючу реалізацію, яку можна перевірити, оптимізувати та синтезувати для апаратного виконання. Прикладом FSM-моделювання є контролер керування дисплеєм у ModelSim. Моделювання демонструє часові діаграми переходів між станами та підтверджує коректність логіки.

Переваги FSM-моделювання є наступними:

- формалізація поведінки системи – уникнення неоднозначностей;
- простота перевірки та симуляції – легко реалізувати у HDL-середовищах (наприклад, ModelSim);
- масштабованість – можна додавати нові стани та переходи без зміни всієї моделі;
- надійність – зменшується ризик логічних конфліктів та помилок.

Отже, FSM-моделювання – це ключовий інструмент для проектування та перевірки логіки цифрових систем, який дозволяє перейти від теоретичного опису до практичної реалізації у HDL-коді та симуляції. Автомат – це математична абстракція (теоретична модель). FSM-моделювання – це практичне застосування автомата, його опис і перевірка у симуляторі чи коді.

Різниця між автоматом і FSM-моделюванням полягає у рівні абстракції та застосуванні (табл. 2).

Таблиця 2

Порівняння призначень автомата tas FSM-моделювання

Критерій	Автомат (теоретична модель)	FSM-моделювання (практична реалізація)
Сутність	Математична абстракція системи у вигляді множини станів, переходів та дій	Процес опису й перевірки автомата у конкретному середовищі (HDL-код, симулятор)
Призначення	Формалізація поведінки системи	Реалізація та тестування логіки у симуляції чи апаратурі
Рівень абстракції	Теоретичний, концептуальний	Прикладний, інженерний
Результат	Модель у вигляді функцій переходів та виходів	HDL-код, таблиці переходів, часові діаграми, testbench
Застосування	Аналіз алгоритмів, доведення властивостей	Перевірка працездатності, оптимізація, синтез на FPGA/ASIC

З огляду табл. 2 видно, що автомат – це теоретична математична модель, яка описує систему через стани, переходи та дії. FSM-моделювання – це вже практичний процес реалізації цієї моделі у вигляді HDL-коду та симуляції. Тобто автомат дає абстракцію, а FSM-моделювання перетворює її на працюючу логіку, яку можна перевірити й синтезувати для апаратної реалізації.

Приклад FSM-контролера для керування дисплеєм

Стани:

- INIT – ініціалізація дисплея;
- SHOW – виведення даних;
- CLEAR – очищення дисплея;
- OFF – вимкнення дисплея.

Переходи:

- INIT → SHOW: після завершення ініціалізації;
- SHOW → CLEAR: при отриманні сигналу `clear = 1`;
- CLEAR → SHOW: після таймера `t_clear`;
- SHOW → OFF: при `power_down = 1`;
- OFF → INIT: при `reset = 1`;

Вихідні сигнали (Mура):

- INIT: `disp_init = 1`;
- SHOW: `disp_data = 1`;
- CLEAR: `disp_clear = 1`;
- OFF: `disp_off = 1`.

FSM-схему для керування дисплеєм представлено на рис. 2.

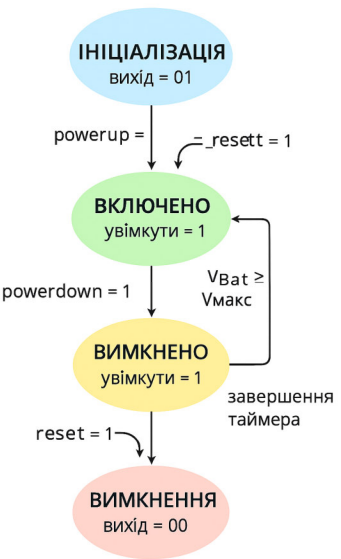

Рис. 2. Графічне представлення FSM-схеми для керування дисплеєм

Стани системи (автомат Мура), що представляє FSM-схему на рис. 2 для керування дисплеєм:

- ІНІЦІАЛІЗАЦІЯ – вихід: disp_init = 1
- ВИВЕДЕННЯ (SHOW) – вихід: disp_data = 1
- ОЧИЩЕННЯ (CLEAR) – вихід: disp_clear = 1
- ВИМКНЕННЯ (OFF) – вихід: disp_off = 1

Переходи між станами:

- ІНІЦІАЛІЗАЦІЯ → ВИВЕДЕННЯ: «ініціалізація завершена»
- ВИВЕДЕННЯ → ОЧИЩЕННЯ: «сигнал очищення»
- ОЧИЩЕННЯ → ВИВЕДЕННЯ: «таймер очищення завершено»
- ВИВЕДЕННЯ → ВИМКНЕННЯ: «сигнал вимкнення»
- ВИМКНЕННЯ → ІНІЦІАЛІЗАЦІЯ: «перезапуск»

Приклад FSM-контролера для керування дисплеєм можна подати у вигляді FSM-таблиці (табл. 3).

Таблиця 3

Таблиця переходів FSM-контролера для керування дисплеєм

Поточний стан	Умови/вхідні сигнали	Наступний стан	Вихідні сигнали у стані
INIT	init_done = 0	INIT	disp_init = 1
INIT	init_done = 1	SHOW	disp_init = 1
SHOW	clear = 1	CLEAR	disp_data = 1
SHOW	power_down = 1	OFF	disp_data = 1
SHOW	(інакше)	SHOW	disp_data = 1
CLEAR	t_clear_expired = 0	CLEAR	disp_clear = 1
CLEAR	t_clear_expired = 1	SHOW	disp_clear = 1
OFF	reset = 1	INIT	disp_off = 1
OFF	reset = 0	OFF	disp_off = 1

Споглядаючи табл. 3 бачимо, у ній представлено автомат Мура (виходи залежать лише від поточного стану). Мінімальний набір входів для FSM-моделі: init_done, clear, t_clear_expired, power_down, reset.

За табл. 3 можна написати Verilog-фрагмент реалізації таблиці переходів FSM-контролера для дисплея (автомат Мура). Verilog-фрагмент подається у скороченому вигляді, який ілюструє лише основну логіку переходів та виходів без зайвих деталей.

```
verilog
module display_fsm (
   input  clk, rst_n,
   input  init_done, clear, t_clear_expired, power_down, reset,
   output reg disp_init, disp_data, disp_clear, disp_off
);

   // Кодування станів
   typedef enum logic [1:0] {INIT=2'b00, SHOW=2'b01, CLEAR=2'b10, OFF=2'b11}
state_t;
   state_t state, next;

   // Регістри стану
   always @(posedge clk or negedge rst_n)
      if (!rst_n) state <= INIT;
      else       state <= next;

   // Логіка переходів
   always @* begin
      case (state)
         INIT:  next = init_done ? SHOW : INIT;
         SHOW:  next = power_down ? OFF : (clear ? CLEAR : SHOW);
         CLEAR: next = t_clear_expired ? SHOW : CLEAR;
         OFF:   next = reset ? INIT : OFF;
      endcase
   end

   // Виходи автомата Мура
   always @* begin
      disp_init  = (state == INIT);
      disp_data  = (state == SHOW);
      disp_clear = (state == CLEAR);
      disp_off   = (state == OFF);
   end

endmodule
```

У представленому скороченому варіанті коду залишено лише ключові блоки: регістри стану, переходи, виходи. Логіка переходів і виходів відповідає таблиці переходів FSM-контролера для дисплея (табл. 3).

Схему переходів та осцилограму роботи FSM-контролера дисплея показано на рис. 3.

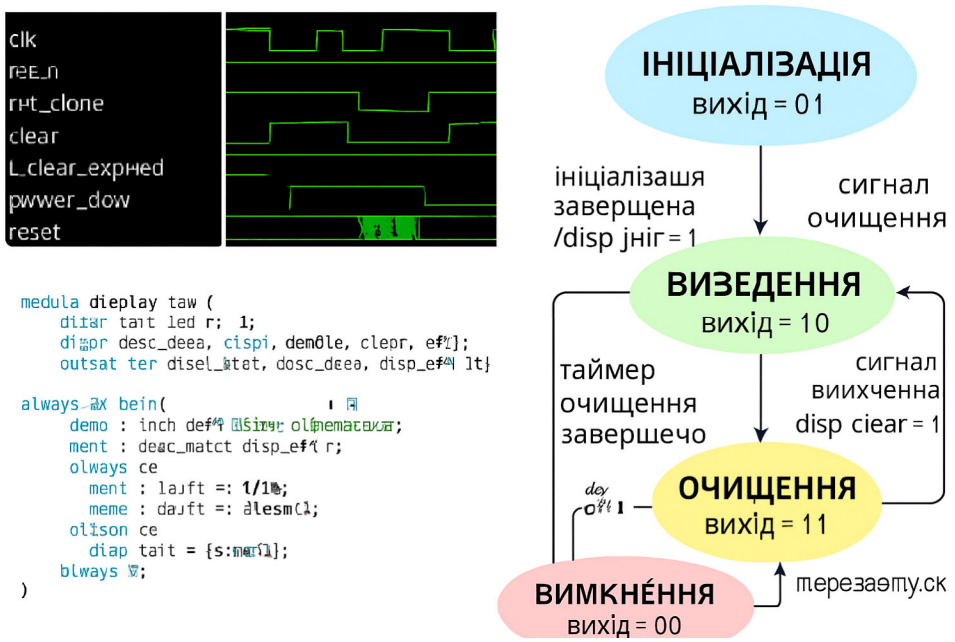

Рис. 3. FSM-контролер дисплея: схема переходів та осцилограма роботи

На рис. 3 представлено графічну FSM-схему контролера дисплея (автомат Мура) та відповідну осцилограму, що демонструє динаміку його роботи. Схема містить чотири стани: «ІНІЦІАЛІЗАЦІЯ», «ВИВЕДЕННЯ», «ОЧИЩЕННЯ» та «ВИМКНЕННЯ», між якими здійснюються переходи згідно з вхідними сигналами (init_done, clear, t_clear_expired, power_down, reset). Вихідні сигнали (disp_init, disp_data, disp_clear, disp_off) формуються відповідно до поточного стану автомата. Осцилограма ілюструє часову послідовність активації вхідних сигналів та реакцію FSM-контролера у вигляді зміни станів і відповідних виходів. Такий підхід дозволяє наочно перевірити коректність реалізації логіки переходів та відповідність таблиці переходів FSM-контролера.

Висновки

1. Побудовано FSM-модель контролера керування дисплеєи, яка формалізує його логіку.

2. Автоматично створено таблицю переходів та Verilog код, що забезпечує реалізацію моделі у HDL середовищі.

4. Отримані результати підтверджують ефективність використання FSM моделі для моделювання логіки контролера керування диплеєм та її симуляції у HDL середовищі ModelSim. Запропонований підхід має практичне значення для створення енергоефективних автономних систем живлення

портативних пристроїв, сенсорних модулів, мобільних пристроїв, систем інтернету речей (IoT), автономних датчиків та вбудованих мікроконтролерних систем.

5. Перспективою подальших досліджень може бути інтеграція моделі з аналоговими моделями у MATLAB/Simulink.

1. Пахомов В. В. Цифрова схемотехніка : навч. посіб. К. : Ліра-К, 2020. 320 с.
2. Максименко І. В. HDL-моделювання цифрових систем : навч. посіб. Харків : ХНУРЕ, 2021. 212 с.
3. Соловйов В. М. Проєктування цифрових пристроїв на основі ПЛІС : навч. посіб. К. : Фенікс, 2019. 288 с.
4. Ashenden P. The Designer's Guide to VHDL. 3rd ed. Morgan Kaufmann, 2010. 936 p.
5. Pedroni V. A. Circuit Design with VHDL. MIT Press, 2004. 576 p.
6. Haskell R. E., Hanna D. M. Digital Design Using VHDL: A Systems Approach. Cengage Learning, 2008. 624 p.

Solomko M. T., Candidate of Engineering (Ph.D.), Associate Professor; Shvets O. H., Senior Student (National University of Water and Environmental Engineering, Rivne)

MODELING OF DISPLAY CONTROLLER LOGIC BASED ON FSM MODEL

This paper focuses on the modeling of display control logic using finite state machine (FSM) methodology, which is widely applied in digital system design for its clarity, predictability, and formal rigor. The study introduces a structured approach to representing controller behavior through FSM transition tables and graphical schemes, highlighting the differences between Moore and Mealy machines in terms of output signal generation. The proposed methodology includes the construction of a transition table for a simplified display controller, followed by its implementation in Verilog HDL. A compact code fragment is presented to demonstrate how the FSM logic can be efficiently realized in hardware description languages without excessive complexity. To validate the correctness of the design, a minimal testbench is prepared and simulated in the ModelSim environment, providing waveform outputs that confirm the expected state transitions and signal activations.

***Keywords*: FSM model, display controller, Moore machine, logic simulation, Verilog, ModelSim**

УДК 519.85:004.75

Соломко[1] М. Т., к.т.н., доцент; Костецький Я. Я., студент 6 курсу
(Національний університет водного господарства та природокористування, м. Рівне, [1]m.t.solomko@nuwm.edu.ua)

МАТЕМАТИЧНА МОДЕЛЬ ОПТИМІЗАЦІЇ ПРОПУСКНОЇ ЗДАТНОСТІ МЕРЕЖІ НА ОСНОВІ МЕТОДІВ ЦІЛОЧИСЕЛЬНОГО ПРОГРАМУВАННЯ

У статті представлено математичну модель оптимізації пропускної здатності комп'ютерної мережі, побудовану на основі методів цілочислового лінійного програмування (ILP). Запропонований підхід поєднує графову структуру мережі з дискретною оптимізацією, що дозволяє враховувати реальні обмеження маршрутизації, зокрема дискретність потоків, пріоритетність сервісів, обмеження пропускної здатності каналів та необхідність балансування навантаження. Наукова новизна роботи полягає у формуванні інтегрованої моделі, яка забезпечує інтелектуальність управління трафіком та наближає процес оптимізації до практичних умов функціонування сучасних телекомунікаційних систем. Практичне значення дослідження полягає у можливості застосування моделі для планування та управління ресурсами в SDN-мережах, дата-центрах та мобільних системах. Реалізація моделі засобами Python забезпечує її інтеграцію в автоматизовані системи управління та створює основу для подальшого розвитку інтелектуальних мережевих технологій.

Ключові слова: **математична модель, оптимізація пропускної здатності, SDN-мережі, цілочислове програмування (ILP), дата-центри, мобільні системи.**

Вступ. Для сучасних комп'ютерних мережах, особливо в умовах зростання навантаження, зокрема у дата-центрах, мобільних системах та хмарних платформах, питання ефективного використання пропускної здатності є критично важливим. Аналіз публікацій [1; 2; 3] підтверджує активний розвиток сучасних моделей маршрутизації, балансування навантаження та управління ресурсами. У них простежується тенденція переходу від класичних алгоритмів до інтелектуальних та оптимізаційних рішень, що інтегрують методи штучного інтелекту та дискретної оптимізації. Це свідчить про формування нового покоління мережевих технологій, здатних адаптуватися та реагувати на динамічні умови трафіку та забезпечувати інтелектуальне управління в SDN мережах, дата-центрах та мобільних системах. Проте більшість класичних підходів базуються на неперервних моделях, які не враховують дискретну природу реальних мережевих рішень. Це створює потребу у розробці математичних моделей,

що поєднують точність формалізації з можливістю врахування цілочислових обмежень, що і зумовлює актуальність даної роботи.

Постановка задачі. У телекомунікаційних мережах, зокрема мобільних та програмно-керованих (SDN), постійно зростає обсяг трафіку, що призводить до перевантаження окремих каналів та зниження якості обслуговування користувачів. SDN (Software-Defined Networking) є концепцією управління комп'ютерними мережами, коли контроль над маршрутизацією та політиками відокремлений від фізичної інфраструктури. Це дозволяє централізовано керувати мережею через програмне забезпечення, а не вручну налаштовувати кожен маршрутизатор чи комутатор. Класичні алгоритми максимального потоку [4] дозволяють оцінити теоретичну пропускну здатність мережі, проте не враховують реальні обмеження – дискретність потоків, пріоритети сервісів, політики маршрутизації та вимоги до QoS (Quality of Service є механізм пріоритетності трафіку, що гарантує стабільну роботу критичних сервісів).

Так виникає задача розробки математичної моделі, яка:

- формалізує процес оптимізації пропускної здатності з урахуванням обмежень каналів та політик;

- забезпечує не дроблення потоків та можливість враховувати пріоритети;

- дозволяє інтегрувати модель у SDN-контролери для автоматизованого управління трафіком. SDN-контролер (Software-Defined Networking Controller) є центральним елемент SDN-архітектури, який керує всією мережею через програмне забезпечення;

- дає змогу порівняти результати з класичним методом Max Flow для оцінки точності та практичності.

Отже, задача дослідження полягає у розробці та реалізації ILP-моделі оптимізації пропускної здатності мережі, її експериментальній перевірці та порівнянні з алгоритмом максимального потоку. ILP-модель – це математична модель оптимізації, яка ґрунтується на методах цілочислового лінійного програмування (Integer Linear Programming) [5].

Об'єкт дослідження є процес оптимізації пропускної здатності мережі, що представлена у вигляді орієнтованого графа з обмеженнями на пропускну здатність каналів.

Мета роботи полягає у побудові математичної моделі, яка дозволяє оптимізувати розподіл потоків у мережі з урахуванням дискретних обмежень, пріоритетів та політик, а також реалізація цієї моделі засобами Python

Теоретичні результати.

1. Формалізація задачі оптимізації пропускної здатності.

Мережа подається як орієнтований граф G = (V, E), де V – множина вузлів, а E – множина каналів з пропускними здатностями c_{ij} . Для кожного

потоку f_k визначається маршрут P_k, який є послідовністю ребер (*i,j*). Цільова функція формулюється наступним чином.

Нехай:

- *K* – множина потоків;
- f_k – величина потоку *k*;
- c_{ij} – пропускна здатність каналу (*i,j*);
- u_{ij} – використання каналу (*i,j*);
- β – коефіцієнт штрафу за перевантаження;
- γ – коефіцієнт для балансування навантаження.

Тоді цільова функція може бути записана так:

$$Z_{\max} = \sum_{k \in K} f_k - \beta \cdot \sum_{(i,j) \in E} \max(0,\, u_{ij} - c_{ij}) - \gamma \cdot Var(u_{ij}), \qquad (1)$$

за умови, що для кожного ребра (*i,j*):

$$\sum_{k:(i,j) \in P_k} f_k \le c_{ij}$$

Пояснення:

- перша складова в (1) $\sum_{k \in K} f_k$ – максимізація сумарного потоку без урахування пріоритетів (QoS).

- друга складова $-\beta \cdot \sum \max(0,\, u_{ij} - c_{ij})$ – штраф за перевантаження каналів, щоб уникати переповнення.

- третя складова $-\gamma \cdot Var(u_{ij})$ – мінімізація дисбалансу використання каналів (балансування навантаження).

2. Врахування дискретності та пріоритетів

Потоки f_k вводяться як цілочисельні змінні, що забезпечує не дроблення потоків. Для пріоритетних потоків вводиться ваговий коефіцієнт α_k, тоді цільова функція набуває вигляду:

$$Z_{\max} = \sum_{k \in K} \alpha_k \cdot f_k - \beta \cdot \sum_{(i,j) \in E} \max(0,\, u_{ij} - c_{ij}) - \gamma \cdot Var(u_{ij}), \qquad (2)$$

де

- *K* – множина потоків;
- f_k – величина потоку *k*;
- α_k – ваговий коефіцієнт (пріоритет потоку);
- c_{ij} – пропускна здатність каналу (*i,j*);

- u_{ij} – використання каналу (*i*,*j*);
- β – коефіцієнт штрафу за перевантаження;
- γ – коефіцієнт для балансування навантаження.

Таким чином, модель (2) не лише максимізує пропускну здатність, але й забезпечує пріоритетність критичних потоків, запобігає перевантаженню та вирівнює навантаження між каналами. Це дозволяє моделі (2) віддавати перевагу критичним сервісам.

У процесі формування цільової функції виникає питання щодо доцільності використання вагових коефіцієнтів α_k , які відображають пріоритетність потоків. У базовій моделі максимізації пропускної здатності (1) всі потоки розглядаються як рівнозначні, і цільова функція має вигляд $Z_{\max} = \sum_k f_k$. Додавання коефіцієнтів α_k у цільову функцію $Z_{\max} = \sum_k \alpha_k \cdot f_k$ дозволяє врахувати різну важливість потоків, що є критично важливим для забезпечення QoS у практичних сценаріях. Отже, використання коефіцієнтів α_k залежить від дослідницької мети: якщо потрібно показати еволюцію до пріоритетної моделі (2) – коефіцієнти α_k зберігається; якщо ж акцент робиться на технічну стабільність і балансування – їх можна вилучити. Обидва варіанти є коректними і відображають різні аспекти оптимізації мережі.

3. Порівняння з класичним алгоритмом максимального потоку (Max Flow).

У класичному алгоритмі максимального потоку задача формулюється так:

$$F_{\max} = \sum_{(s,j)\in E} f_{sj}, \tag{3}$$

де *s* – джерело, *j* – суміжні вузли, f_{sj} – величина потоку ребром (*s*,*j*). Для (3) враховуються обмеження пропускної здатності ребер:

$$f_{ij} \le c_{ij}, \ для \ \forall (i,j) \in E. \tag{4}$$

Класичний алгоритм максимального потоку орієнтований лише на максимізацію загального обсягу переданих даних між джерелом і приймачем. Він враховує пропускну здатність каналів, але розглядає всі потоки як рівнозначні, без урахування їхньої важливості чи специфічних вимог. Такий підхід дозволяє визначити теоретичну межу пропускної здатності мережі, проте не відображає реальних умов її роботи.

ILP-модель (2), на відміну від максимального потоку (3), враховує додаткові фактори. Вона дозволяє задавати пріоритети для різних потоків, щоб критичні сервіси отримували перевагу над другорядними. Крім того, *модель* вводить штрафи за перевантаження каналів та механізми

балансування навантаження між різними маршрутами. Це забезпечує більш реалістичний і практичний результат, який відповідає вимогам сучасних мереж, де важлива не лише кількість переданих даних, а й якість їхнього розподілу.

Практичні результати. Модель (2) реалізовано мовою Python з використанням бібліотеки PuLP для ILP та NetworkX для максимального потоку. Це дозволяє автоматизувати процес побудови задачі та отримати оптимальні рішення для тестових топологій мережі.

Тестова топологія мережі. На рисунку представлено тестову топологію мережі.

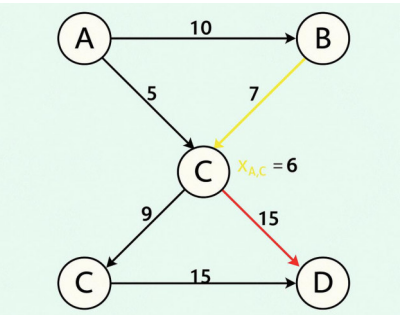

Рисунок. Тестова топологія мережі з вузлами A (джерело), B, C, D (приймач) та каналами з пропускною здатністю

- Вузли: A (джерело), B, C, D (приймач);
- Канали:

  - A → B (10);
  - A → C (8);
  - B → C (5);
  - B → D (7);
  - C → D (9).

Потрібно максимізувати потік з A до D з урахуванням обмежень пропускної здатності та збереження потоку в проміжних вузлах.

Реалізація ILP-моделі:

- використано бібліотеку PuLP для формулювання задачі цілочислового лінійного програмування.

- задано змінні потоку $x(i,j)$, обмеження на пропускну здатність та збереження потоку.

- цільова функція – максимізація загального потоку з джерела до приймача.

Результати експерименту

Max Flow (алгоритм Едмондса–Карпа): $F_{max} = 16$.

Python-код для максимального потоку у тестовій топології:

```
# Max Flow (Edmonds–Karp) for the given network topology
# Nodes: A (source), B, C, D (sink)
# Edges with capacities:
# A->B: 10, A->C: 8, B->C: 5, B->D: 7, C->D: 9

import networkx as nx

def build_graph():
    G = nx.DiGraph()
    # Add edges with capacity attribute
    G.add_edge('A', 'B', capacity=10)
    G.add_edge('A', 'C', capacity=8)
    G.add_edge('B', 'C', capacity=5)
    G.add_edge('B', 'D', capacity=7)
    G.add_edge('C', 'D', capacity=9)
    return G

def compute_max_flow(G, source='A', sink='D'):
    # Edmonds–Karp is the default in networkx.maximum_flow when using
'capacity'
    flow_value, flow_dict = nx.maximum_flow(G, source, sink, capacity='capacity')
    return flow_value, flow_dict

if __name__ == "__main__":
    G = build_graph()
    Fmax, flows = compute_max_flow(G, source='A', sink='D')

    print(f"Max Flow (Edmonds–Karp): F_max = {Fmax}")
    print("Flow assignment per edge:")
    for u, nbrs in flows.items():
        for v, f in nbrs.items():
            if f > 0:
                print(f"  {u} -> {v}: {f}")
```

Код обчислює максимальний потік від A до D, друкує значення потоку та призначення ребер.

Для представленої топології результат такий:

- $F_{max} = 16$

- типова декомпозиція потоку, яку можна побачити в обраній топології:
  - A → B → D: 7;
  - A → C → D: 9.

ILP-модель (з обмеженням на цілісність та маршрут): F_{ILP} = 8 *(вибрано маршрут A → C → D, обмеження: мінімум серед 8 і 9).*

Python-код для ILP-моделі з маршрутом A → C → D та обмеженням на цілісність потоку: максимальний потік F = 8.

```
from pulp import LpProblem, LpVariable, LpMaximize, LpInteger, value, LpStatus

# Створення ILP-моделі
model = LpProblem("ILP_MaxFlow_ACD", LpMaximize)

# Змінні: потік по каналах A→C та C→D (цілісні)
x_AC = LpVariable("x_AC", lowBound=0, upBound=8, cat=LpInteger)
x_CD = LpVariable("x_CD", lowBound=0, upBound=9, cat=LpInteger)

# Цільова функція: максимізувати потік F = x_AC = x_CD
model += x_AC, "Maximize_Flow"

# Обмеження: потік має бути однаковим на обох каналах (без втрат)
model += x_AC == x_CD, "Flow_Conservation"

# Розв’язання моделі
model.solve()

# Виведення результатів
print(f"Статус розв’язання: {LpStatus[model.status]}")
print(f"Максимальний потік F = {value(x_AC)}")
print(f"Потік по A→C: {value(x_AC)}")
print(f"Потік по C→D: {value(x_CD)}")
```

Пояснення до коду:
- обраний маршрут: A → C → D.
- обмеження:

  - пропускна здатність A→C = 8
  - пропускна здатність C→D = 9
  - потік має бути однаковим на обох каналах → обмеження *x*(AC) = *x*(CD)

- цільова функція: максимізувати $x(AC)$, тобто весь потік.
- результат: $F_{ILP} = 8$, обмежений пропускною здатністю каналу A→C.

Цей код демонструє, як ILP-модель враховує реальні обмеження маршруту, на відміну від класичного Max Flow, який дозволяє розщеплення потоку.

Практична інтеграція. Модель (2) може бути інтегрована в SDN-контролер, де обчислення ILP виконуються для вибору оптимальних маршрутів. Це забезпечує балансування навантаження, підтримку QoS та адаптацію до змін трафіку.

Розробка програмного забезпечення для оптимізації потоків у комп'ютерних мережах починається з написання скриптів мовою програмування Python, здатних формалізувати математичну модель задачі. На першому етапі створюються модулі, які описують структуру мережі у вигляді графа з вузлами та каналами, а також задають параметри пропускної здатності. Далі реалізуються функції для побудови цільової функції та системи обмежень, що дозволяє сформувати задачу цілочисельного лінійного програмування. Наступним кроком є інтеграція бібліотек для розв'язання оптимізаційних задач (наприклад, PuLP або OR-Tools), які забезпечують автоматичний пошук оптимального рішення. Паралельно створюються скрипти для порівняння результатів із класичним алгоритмом Max Flow, що дозволяє оцінити відхилення між теоретичними та практичними значеннями. На завершальному етапі програмне забезпечення доповнюється інтерфейсними компонентами для візуалізації результатів та зручності користувача, що робить його придатним для практичного застосування у системах управління мережевим трафіком.

Висновки

У результаті дослідження побудовано математичну модель оптимізації пропускної здатності мережі на основі методів цілочислового програмування. Наукова новизна полягає у поєднанні графової структури мережі з дискретною оптимізацією, що дозволяє враховувати реальні обмеження маршрутизації – дискретність потоків, пріоритетність сервісів, обмеження пропускної здатності та балансування навантаження. Практичне значення моделі полягає у можливості її застосування для планування трафіку в SDN-мережах, дата-центрах та мобільних системах. Реалізація засобами Python забезпечує інтеграцію моделі в автоматизовані системи управління. Важливо підкреслити, що ILP-модель додає інтелектуальність в управління мережею: вона не лише максимізує пропускну здатність, а й адаптивно враховує пріоритети та технічні обмеження, наближаючи процес оптимізації до реальних умов функціонування сучасних телекомунікаційних систем.

1. Farahi R. A comprehensive overview of load balancing methods in software-defined networks. *Discover Internet of Things*. 2025. Vol. 5, No. 6. Article 6. Springer.
2. Musaddiq A.; Olsson T.; Ahlgren F. Reinforcement-Learning-Based Routing and Resource Management for Internet of Things Environments: Theoretical Perspective and Challenges. *Sensors*. 2023. Vol. 23, No. 19. P. 8263.
3. Tache M. D.; Păscuțoiu O.; Borcoci E. Optimization Algorithms in SDN: Routing, Load Balancing, and Delay Optimization. *Applied Sciences*. 2024. Vol. 14, No. 14. P. 5967.
4. Sheng J.; Guan X.; Yang F.; Wan X. An Accelerated Maximum Flow Algorithm with Prediction Enhancement in Dynamic LEO Networks. *Sensors*. MDPI, 2025. Vol. 25, No. 8. P. 2555.
5. Bertsimas D.; Weismantel R. Optimization over Integers. Princeton : Princeton University Press, 2022. 544 p.

Solomko M. T., Candidate of Engineering (Ph.D.), Associate Professor; Kostetskyi Y. Y., Master (National University of Water and Environmental Engineering, Rivne)

MATHEMATICAL MODEL OF NETWORK CAPACITY OPTIMIZATION BASED ON INTEGER LINEAR PROGRAMMING METHODS

This paper presents a mathematical model for optimizing the capacity of computer networks, developed using Integer Linear Programming (ILP) methods. The proposed approach integrates the graph structure of the network with discrete optimization techniques, enabling the consideration of real routing constraints such as flow discreteness, service prioritization, channel capacity limitations, and the necessity of load balancing. Unlike classical maximum flow algorithms, which operate under idealized assumptions, the ILP-based formulation provides a more realistic representation of network behavior by incorporating practical restrictions and adaptive decision-making mechanisms.

The scientific novelty of the study lies in the construction of an integrated optimization model that introduces intelligence into traffic management. The model not only maximizes throughput but also dynamically accounts for heterogeneous service requirements and resource constraints, thereby bridging the gap between theoretical optimization and real-world network operation. This makes the approach particularly relevant for modern telecommunication systems, where flexibility, scalability, and reliability are critical.

The practical significance of the research is reflected in its applicability to traffic planning and resource management in Software-Defined Networks (SDN), data centers, and mobile communication systems. The implementation of the

model in Python ensures its compatibility with automated control systems and facilitates integration into existing network management platforms. Furthermore, the modular design of the software allows for future extensions, including the incorporation of machine learning techniques and hybrid optimization strategies, thus creating a foundation for the development of next-generation intelligent networking technologies.

***Keywords*: mathematical model, network capacity optimization, SDN networks, integer linear programming (ILP), data centers, mobile systems.**

Наукове видання

ВІСНИК
НАВЧАЛЬНО-НАУКОВОГО ІНСТИТУТУ КІБЕРНЕТИКИ, ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ІНЖЕНЕРІЇ НУВГП

Випуск 2(13)

Технічний редактор *Галина Сімчук*
Оксана Прищепа

Друкується в авторській редакції

Підписано до друку 18.12.2025 р. Формат $70\times100^{1}/_{16}$
Ум.-друк. арк. 8,0. Обл.-вид. арк. 8,9.
Тираж 100 прим. Зам. № 5682.

Видавець і виготовлювач
Національний університет
водного господарства та природокористування
вул. Соборна, 11, м. Рівне, 33028.

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції РВ № 31 від 26.04.2005 р.