

**ВІЙСЬКОВИЙ ІНСТИТУТ КИЇВСЬКОГО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА**

ЗБІРНИК НАУКОВИХ ПРАЦЬ

**ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА**

Виходить 4 рази на рік

№ 90

Згідно з наказом МОН №1188 від 24.09.2020, п. №156 Додатку 5 "Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка" включено до категорії "Б" за спеціальностями:

- F4 Системний аналіз та наука про дані (124);
- F6 Інформаційні системи і технології (126);
- K6 Забезпечення військ (сил) (254);
- K7 Озброєння та військова техніка (255).

**MILITARY INSTITUTE OF TARAS SHEVCHENKO NATIONAL
UNIVERSITY OF KYIV**

**COLLECTION OF SCIENTIFIC WORKS
OF THE MILITARY INSTITUTE OF TARAS SHEVCHENKO NATIONAL
UNIVERSITY OF KYIV**

It comes out 4 times a year

№ 90

According to the Order of the Ministry of Education and Science No. 1188 from 09/24/2020, item No. 156 of Appendix 5 "Collection of scientific works of the Military Institute of Taras Shevchenko National University of Kyiv" is included in category "B" by specialties:

- F4 System analysis and date scsence (124);
- F6 Information systems and technologies (126);
- K6 Supply of troops (forces) (254);
- K7 Armament and military equipment (255).

KYIV – 2026

УДК 621.43

ББК 32-26.8-68.49

Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2026. № 90. 126 с.

Голова редакційної колегії:

Євген КРАСНИКОВ

доктор наук з державного управління

Члени редакційної колегії:

Ігор ПАМПУХА

Григорій СИТНИК

Тетяна ЗАПОРОЖЕЦЬ

Алла КОЖИНА

Євгеній ТАРАН

Вікторія ГУРА

Тетяна ПАЛАМАРЧУК

Галина ЗАВОРІТНЯ

Олесь КОВАЛЬ

Марія ЯРМОЛЬЧИК

Юзеф ДОБРОВОЛЬСЬКИЙ

Олег ФАРІОН

Олег МАШКОВ

Юрій РЕПЛО

Ольга САЛЬНИКОВА

Пьотр ГАВЛІЧЕК

Міхал ТЛОН

кандидат технічних наук, доцент;

доктор наук з державного управління, професор

доктор наук з державного управління, доцент;

доктор наук з державного управління, професор;

кандидат політичних наук, доцент;

кандидат економічних наук, доцент;

кандидат наук з державного управління;

кандидат політичних наук, доцент;

доктор філософії з фінансів, банківської справи та страхування;

доктор філософії з психології;

кандидат технічних наук, доцент, старший науковий співробітник;

доктор військових наук, професор;

доктор технічних наук, професор.

доктор військових наук, професор

доктор наук з державного управління, старший науковий співробітник;

доктор наук (габілітований) з національної безпеки, доцент;

доктор економіки та фінансів

Редакційна колегія прагне до покращення змісту та якості оформлення видання і буде вдячна авторам та читачам за висловлювання зауважень і побажань.

Зареєстровано Міністерством юстиції України, свідоцтво про державну реєстрацію друкованого засобу масової інформації – серія KB № 11541 – 413P від 21.07.2006 р.

Відповідно до наказу МОН України від 24.09.2020 № 1188 "Збірник наукових праць ВІКНУ імені Тараса Шевченка" внесено до категорії "Б" (технічні науки).

Зареєстровано: Національною радою України з питань телебачення та радіомовлення. Рішення №1450 від 25.04.2024 р. Ідентифікатор медіа: R30-05126.

Затверджено на засіданні Вченої ради ВІКНУ від 19.03.26 р., протокол № 8.

Відповідальна за макет:

Петренко М.М.

Відповідальність за новизну і достовірність наведених результатів, тактико-технічних та економічних показників і коректність висловлювань несуть автори. Точка зору редколегії не завжди збігається з позицією авторів. Усі матеріали надруковані в авторській редакції.

Усі статті, що публікуються в збірнику, проходять обов'язкове рецензування, яке здійснюється за анонімною формою як для авторів, так і для рецензентів. Незважаючи на перевірку статей на антиплагіат, остаточну відповідальність за плагіат несуть автори.

Видання безкоштовне.

Примірники збірників знаходяться у: Національній бібліотеці України ім. В.І. Вернадського, науковій бібліотеці ім. М. Максимовича, бібліотеці Військового інституту та в наукових бібліотеках України згідно зі списком МОН. Електронна версія збірника розміщена на відповідних сайтах.

Видання індексується Google Scholar, Open Ukrainian Citation Index (OUCI), Exaly, CoLab.

Адреса редакції: 03189, м. Київ, вул. Юлії Здановської, 81. Наклад 50 прим.

Ел. адреса: collection.works@knu.ua

Офіційний сайт журналу: <https://digest.mil.knu.ua>

UDC 621.43

LBC 32-26.8-68.49

Collection of scientific works of the Military Institute of Taras Shevchenko National University of Kyiv. K.: VIKNU, 2026. № 90. 126 p.

Chairman of the editorial board:

Yevgen KRASNYKOV

Doctor of Science in Public Administration,;

Members of the editorial board:

Ihor PAMPUKHA

Candidate of Technical Sciences, Associate Professor;

Hryhorii SYTNYK

Doctor of Science in Public Administration, Professor;

Tetiana ZAPOROZHETS

Doctor of Science in Public Administration, Associate Professor;

Alla KOZHYNA

Doctor of Science in Public Administration, Professor;

Yevhenii TARAN

Candidate of Political Sciences, Associate Professor;

Viktoriya GURA

Candidate of Economics, Associate Professor;

Tetiana PALAMARCHUK

Candidate of Public Administration;

Halyna ZAVORITNYA

Candidate of Public Administration, Associate Professor;

Oles KOVAL

PhD in Finance, Banking and Insurance;

Maria YARMOLCHYK

Doctor of Philosophy;

Yuzef DOBROVOLSKYI

Candidate of Technical Sciences, Associate Professor;

Oleh FARION

Doctor of Military Sciences, Professor;

Oleg MASHKOV

Doctor of Technical Sciences, Professor;

Iurii REPILO

Doctor of Military Sciences, Professor;

Olha SALNIKOVA

Doctor of Science in Public Administration, Associate Professor;

Piotr GAWLICZEK

PhD (habilitated) in National Security, Associate Professor

Michal THLON

Doctor Economics & Finance

The editorial board strives to improve the content and quality of the publication and will be grateful to the authors and readers for their comments and wishes.

Registered by the Ministry of Justice of Ukraine, certificate of state registration of printed mass media – KV series No. 11541 – 413P from 07/21/2006.

Registered by the National Council of Ukraine on Television and Radio Broadcasting. Ruling No. 1450 of April 25, 2024. Media ID: R30-05126.

In accordance with the Order of the Ministry of Education and Science of Ukraine from September 24, 2020 No. 1188, "Collection of Scientific Works of the Military Institute of Taras Shevchenko National University of Kyiv" is included in category "B" (technical sciences).

Approved at the meeting of the Scientific Council of VIKNU from 19.03.26, prot. №8.

Responsible for the layout:
Petrenko M.

The authors are responsible for the novelty and reliability of the given results, tactical-technical and economic indicators and the correctness of statements. The point of view of the editorial board does not always coincide with the position of the authors. All the materials are printed in the author's edition.

All articles published in the collection undergo a mandatory review, which is carried out anonymously for both authors and reviewers. Despite checking the articles for anti-plagiarism, the final responsibility for plagiarism lies with the authors.

The publication is free.

Copies of the collections are in the National Library of Ukraine named after V.I. Vernadsky, in the scientific library named after M. Maksymovych, in the library of the Military Institute and in the scientific libraries of Ukraine according to the list of the Ministry of Education and Science. The electronic version of the collection is posted on the relevant websites.

The publication is indexed by Google Scholar, Open Ukrainian Citation Index (OUCI), Exaly, CoLab.

Address of the editorial office: 03189, Kyiv, Yulia Zdanovskaya street, 81. Edition of 50 copies.

E-mail address: collection.works@knu.ua

Official website of the journal: <https://digest.mil.knu.ua>

ЗМІСТ

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

Долінчук К.О. Генерація синтетичних радіочастотних сигналів для навчання моделей глибокого навчання у сценаріях електронної боротьби	7
Каберник В.О., Ольшевський С.В. Порівняльний аналіз контактного та безконтактного методів визначення електропровідності водних розчинів	17
Целованський Т.Р. Температурно-адаптивне керування затримками пам'яті DDR у сучасних обчислювальних системах	29

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Бабич Т.А., Сашнюва М.В., Радзівська О.В., Дьяконенко Д.К. Автоматизоване розгортання вразливих навчальних середовищ із застосуванням моделі мінімальних привілеїв	35
Вознюк Я.І., Гахович С.В., Радзівська О.В., Бойко І.В. Система автоматизованого розгортання кластерного середовища	51
Гахович С.В., Бабич Т.А., Савченко Т.В., Деркач Є.Р. Автоматизована система ізольованих імітаційних середовищ для дослідження кіберзагроз	65
Сашнюва М.В., Вознюк Я.І., Черкасов Д.І., Маслов П.С. Система автоматизованого контролю відповідності конфігурацій мережевих пристроїв вимогам кібербезпеки	77

ЗАГАЛЬНІ ПИТАННЯ

Добровольський Ю.Б., Дубик О.М., Ярмольчик М.О. Наближення нормативної бази державної авіації України до стандартів НАТО	93
Савчук Д.В., Георгадзе О.А. Основні фактори, що впливають на ефективність відновлення боєздатності військової частини	103
Дані про авторів	114
Алфавітний покажчик	116
Редакційна політика та етичні норми	117
Порядок подання і оформлення статей до "Збірника наукових праць Військового інституту Київського національного університету імені Тараса"	119

CONTENTS

MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES

Dolinchuk K. Generation of synthetic radio frequency signals for training deep learning models in electronic warfare scenarios	7
Kabernyk V., Olszewski S. Comparative analysis of contact and contactless methods for determining the electrical conductivity of aqueous solutions	17
Tselovanskyi T. Temperature-adaptive management of DDR memory latencies in modern computing systems	29

INFORMATION TECHNOLOGIES

Babych T., Sashnova M., Radziievska O., Dyakonenko D. Automated deployment of vulnerable training environments using the least-privilege model	35
Vozniuk Y., Hakhovych S., Radziievska O., Boiko I. Automated cluster environment deployment system	51
Hakhovych S., Babuch T., Savchenko T., Derkach E. Automated system of isolated emulation environments for cyber threat research	65
Sashnova M., Vozniuk Y., Cherkasov D., Maslov P. Automated compliance control of network device configurations with cybersecurity requirements	77

GENERAL QUESTIONS

Dobrovolskyi Y., Dubyk O., Yarmolchyk M. Aligning Ukraine's state aviation regulatory framework with NATO standards	93
Savchuk D., Heorhadze O. Main factors affecting the effectiveness of restoring the combat capability of a military unit	103

Data on Authors	114
Alphabetical Index	116
Editorial policy and ethical standard	117
The order of submission and registration of articles to the "Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv"	119

ГЕНЕРАЦІЯ СИНТЕТИЧНИХ РАДІОЧАСТОТНИХ СИГНАЛІВ ДЛЯ НАВЧАННЯ МОДЕЛЕЙ ГЛИБОКОГО НАВЧАННЯ У СЦЕНАРІЯХ ЕЛЕКТРОННОЇ БОРОТЬБИ

Розвиток стійких систем дистанційної локалізації та аналізу потужних сигналів завад і протидії критично залежить від наявності великих і різноманітних навчальних наборів даних. Традиційний збір даних за допомогою професійного радіообладнання та польових випробувань є дорогим, тривалим і часто обмеженим технічними та регуляторними чинниками. Синтетичне генерування радіочастотних сигналів із використанням сучасних генеративних моделей глибокого навчання пропонує привабливу альтернативу: моделі навчаються статистичній структурі реальних сигналів і каналів, а потім формують реалістичні послідовності I/Q із керованими параметрами.

У цій статті запропоновано метод синтезу RF-сигналів на основі VQ-VAE у поєднанні з авторегресивним Transformer. Запропонована схема навчається розподілу реальних RF-сигналів і генерує синтетичні послідовності, умовно задані типом модуляції, відношенням сигнал/шум (SNR) та каналом поширення. Експериментальні результати на наборі з 500 000 комплексних послідовностей показали, що архітектура VQ-VAE + Transformer досягає середньоквадратичної похибки реконструкції (MSE) 0.0245 та кореляції спектрограм 0.948, перевершуючи базові моделі GAN, VAE, WGAN і diffusion за якістю та часом навчання.

Ключові слова: синтетичні RF-сигнали; генеративні моделі; VQ-VAE; Transformer; аугментація даних; завади; електронна боротьба; класифікація модуляції.

Вступ. Сучасні системи електронної боротьби (ЕБ) та протидії БПЛА потребують точного виявлення, класифікації та локалізації потужних джерел завад і перешкод у широкому спектрі оперативних умов [1, 2, 12]. У таких сценаріях канали зв'язку, навігації та телеметрії зазнають навмисних перешкод, що погіршують якість сервісу або повністю зривають виконання місії [12, 13].

Методи глибокого навчання показали високу ефективність у задачах автоматичної класифікації модуляцій, спектрального зондування та локалізації RF-випромінювачів [6, 11, 14, 15]; однак їх результативність обмежена доступністю репрезентативних навчальних даних. Збір RF-наборів з реальними сигналами завад за допомогою лабораторних або польових стендів потребує дорогого обладнання, узгоджених експериментів і, в багатьох випадках, спеціальних дозволів [3, 16].

Синтетичне генерування RF-сигналів із використанням генеративного глибокого навчання є привабливою альтернативою [4–7, 10]. Навчаючись статистичним властивостям реальних сигналів і каналів, генеративні моделі можуть створювати великі обсяги реалістичних I/Q -даних із керованими параметрами. Синтетичні сигнали можуть використовуватися для доповнення обмежених реальних наборів даних, для покриття рідкісних або екстремальних умов, а також для систематичного моделювання ефективності алгоритмів.

У цій роботі розроблено та експериментально верифіковано повний конвеєр синтетичної генерації RF-сигналів, орієнтований на навчання моделей глибокого навчання для задач, пов'язаних із ЕБ.

Аналіз останніх досліджень і публікацій. Останні дослідження у сфері радіочастотного аналізу та електронної боротьби підтверджують, що ефективність моделей глибокого

навчання у задачах розпізнавання модуляцій, спектрального зондування та локалізації випромінювачів істотно залежить від якості подання сигналу, попередньої обробки та репрезентативності навчальної вибірки [6, 11, 14, 15]. Водночас збір реальних RF-даних залишається дорогим і технічно складним, тому все більшої уваги набувають підходи, пов'язані з аугментацією даних і синтетичним генеруванням I/Q-послідовностей [3, 16]. У цьому контексті базовими для наряду стали генеративні моделі GAN, VAE та diffusion, які створили методологічну основу для подальшого розвитку засобів синтезу RF-сигналів [4,5,7].

У низці сучасних праць показано, що для задач генерації сигналів найбільш перспективними є моделі, які поєднують стискання сигналу в латентному просторі з подальшим послідовнісним моделюванням. Зокрема, підхід VQ-VAE забезпечує дискретне та стійке латентне представлення сигналу [8], а Transformer-моделі дають змогу ефективно відтворювати послідовності кодів з урахуванням умов генерації [9]. Практичну доцільність таких архітектур для data augmentation підтверджують і нові дослідження синтезу сигналів, де VQ-VAE у поєднанні з Transformer або близькими генеративними підходами розглядається як ефективна основа для побудови реалістичних RF-вибірок [10].

Окремий інтерес становлять найновіші роботи, присвячені адаптації diffusion-підходів безпосередньо до RF-даних. Так, у дослідженні RF-Diffusion запропоновано часово-частотну diffusion-модель для генерації високоякісних радіосигналів, яка продемонструвала переваги над низкою попередніх генеративних рішень для Wi-Fi та FMCW-сценаріїв [23]. Отже, сучасний стан досліджень свідчить, що використання архітектури VQ-VAE + Transformer у цій роботі є обґрунтованим і відповідає актуальній тенденції переходу до більш структурованих, керованих і якісних методів синтезу RF-сигналів для задач електронної боротьби та автоматичного розпізнавання модуляцій [6, 10].

1. Моделі RF-сигналів та каналів.

1.1. Модульовані RF-сигнали. Ми розглядаємо аналогові та цифрові схеми модуляції, які зазвичай використовуються в системах зв'язку та придушення [17]. Комплексну базову огинаючу модульованого RF-сигналу можна записати як $s(t) = a(t) \cdot \exp(j(2\pi f_c t + \varphi(t)))$, де $a(t)$ – амплітудна огинаюча, f_c – несуча частота, а $\varphi(t)$ – фазова складова, що кодує інформацію та модуляцію. Таблиця 1 узагальнює типи модуляції, використані в цій роботі, та їхні основні характеристики.

Таблиця 1 – Огляд типів модуляції, використаних у дослідженні

Тип модуляції	Клас	Примітки
AM	Аналогова	Зміни амплітуди навколо несучої частоти; вузькосмугове мовлення.
FM	Аналогова	Частотні відхилення; стійка до амплітудного шуму.
PM	Аналогова	Фазові відхилення; часто поєднується з FM.
BPSK	Цифрова	Стійка бінарна фаза; підходить для низького SNR.
QPSK	Цифрова	2 біти на символ; баланс між стійкістю та спектральною ефективністю.
M-PSK	Цифрова	Вища спектральна ефективність; чутливіша до шуму.
M-QAM	Цифрова	Амплітудно-фазове кодування; широко використовується в стандартах.
FSK	Цифрова	Частотна маніпуляція; підходить для простих приймачів.
OFDM	Цифрова	Мультиносійна; висока спектральна ефективність; чутлива до нелінійностей.

Для чисельної обробки безперервний сигнал подано як дискретну комплексну I/Q-послідовність $s[n] = I[n] + jQ[n]$, вибірка якої здійснюється з частотою f_s , що задовольняє критерій Найквіста відносно смуги сигналу B , тобто $f_s \geq 2B$.

1.2. Спотворення каналу. Під час поширення через бездротовий канал RF-сигнал зазнає низки спотворень, які необхідно відобразити в синтетичних даних [18,19]:

- Додавання білого гаусівського шуму (AWGN), що моделюється як $y[n] = s[n] + w[n]$, де $w[n]$ – комплексний гаусовий шум із нульовим математичним сподіванням та дисперсією σ^2 , що визначається цільовим SNR.

- Багатопроменеве завмирання, описане коефіцієнтом каналу Rayleigh h , так що $y[n] = h \cdot s[n] + w[n]$, де h – комплексна випадкова величина з раліївським розподілом модуля.

- Часова затримка та доплерівський зсув, що приводять до $y[n] = h \cdot s[n - n_d] \cdot \exp\left(j2\pi \frac{f_d n}{f_s}\right) + w[n]$, де n_d – затримка в семплах, а f_d – доплерівське зміщення частоти.

- Нелінійні спотворення через насичення підсилювача потужності, які моделюються за допомогою амплітудного кліпінгу або поліноміальних моделей.

Таблиця 2 якісно підсумовує ці ефекти каналу та їхній вплив на моделі, що навчаються.

Таблиця 2 – Спотворення каналу та їхній вплив

Спотворення	Опис моделі	Вплив на моделі навчання
AWGN	Додавання гаусівського шуму	Погіршує SNR; перевіряє стійкість до шуму.
Rayleigh fading	Випадковий комплексний коефіцієнт h	Спричиняє швидкі завмирання; потребує різноманітності.
Delay & Doppler	Часовий зсув і частотний зсув	Спотворює фазу; впливає на синхронізацію.
Нелінійності	Кліпінг амплітуди, поліноміальний підсилювач	Створює спектральне розширення та додаткові спотворення.

2. Генеративні моделі для синтезу RF-сигналів.

2.1. Генеративні змагальні мережі (GAN). Генеративні змагальні мережі (GAN) складаються з генератора G та дискримінатора D , які навчаються в постановці мінімаксової гри. Генератор відображає вектор шуму z синтетичний зразок $\hat{x} = G(z)$, тоді як дискримінатор намагається відрізнити реальні зразки x від згенерованих. Стандартна функція втрат GAN має вигляд

$$\min_G \max_D \mathbb{E}_x[\log D(x)] + \mathbb{E}_z[\log (1 - D(G(z)))]. \quad (1)$$

Умовні GAN (conditional GAN, CGAN) розширюють цю схему, вводячи додаткову умову c (наприклад, клас модуляції, рівень SNR) як у генератор, так і в дискримінатор, що дає змогу генерувати RF-сигнали, умовні за класом c . Хоча GAN успішно застосовуються до зображень та аудіосигналів, їх навчання для RF-сигналів часто є нестабільним, із колапсом мод і високою чутливістю до вибору гіперпараметрів.

2.2. Варіаційні автокодери (VAE). Варіаційні автокодери (VAE) поєднують енкодер $q_\phi(z | x)$, латентний простір і декодер $p_\theta(x | z)$. Енкодер відображає вхідні зразки x у розподіл у латентному просторі, який зазвичай параметризується гаусовим розподілом із математичним сподіванням $\mu(x)$ та дисперсією $\sigma^2(x)$. Декодер відновлює $\hat{x}$ з латентних векторів z . Функція навчання – це нижня оцінка правдоподібності (evidence lower bound, ELBO):

$$L_{VAE} = \mathbb{E}_{q_\phi(z|x)}[-\log p_\theta(x | z)] + \text{KL}\left(q_\phi(z | x) \parallel p(z)\right), \quad (2)$$

де перший доданок є втратою відновлення, а другий – дивергенцією Кульбака – Лейблера відносно апіорного розподілу $p(z)$.

VAE забезпечують гладкий латентний простір, але схильні формувати надто згладжені

синтетичні хвильові форми та можуть мати труднощі з відтворенням тонких фазових деталей RF-сигналів.

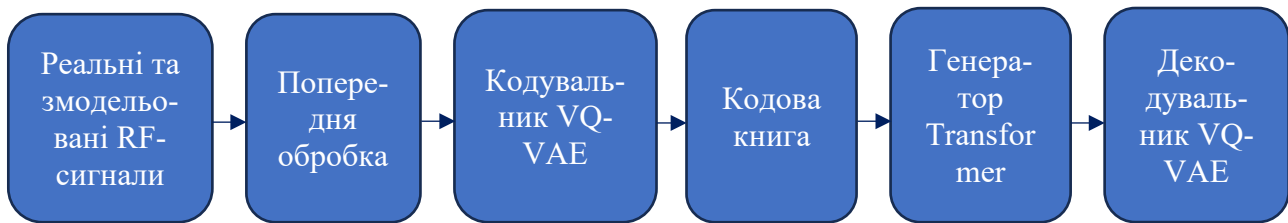
2.3. Дифузійні моделі. Дифузійні моделі генерують дані, навчаючись відтворювати зворотний процес поступового додавання шуму. У прямому процесі до чистого зразка додається гаусовий шум відповідно до заданого графіка дисперсії; далі нейронну мережу навчають апроксимувати зворотну динаміку очищення від шуму. Дифузійні моделі досягають найкращої на сьогодні якості для зображень і аудіо, а останні дослідження також розглядають їх застосування для генерації вібраційних та RF-сигналів, однак вони є обчислювально затратними через велику кількість кроків денойзингу.

2.4. Векторно-квантизовані автокодекери (VAE) та авторегресивні Transformer. Щоб краще відобразити дискретну структуру RF-сигналів і водночас забезпечити ефективну генерацію, ми використовуємо Vector Quantized Variational Autoencoder (VQ-VAE) у поєднанні з авторегресивним Transformer. Енкодер f_{enc} перетворює вхідну I/Q-послідовність x у набір латентних векторів, які квантуються за допомогою навченої кодової книги, а декодер f_{dec} відновлює сигнал із квантизованого латентного представлення [8]. Функцію втрат VQ-VAE можна записати як:

$$L_{\text{VQ-VAE}} = L_{\text{rec}} + \| \text{sg}[z_e] - e \|_2^2 + \beta \| z_e - \text{sg}[e] \|_2^2, \quad (3)$$

де L_{rec} – похибка відновлення, z_e – вихід енкодера, e – вектор кодової книги, $\text{sg}[\cdot]$ позначає операцію stop-gradient, а β – коефіцієнт commitment loss.

Після навчання VQ-VAE кожен сегмент сигналу подається у вигляді послідовності дискретних кодів. Далі авторегресивний Transformer моделює розподіл над цими кодами з урахуванням умовної інформації c , наприклад класу модуляції та SNR. На етапі генерації він послідовно прогнозує токени за розподілом $p(\text{token}_t | \text{token}_{<t}, c)$, після чого декодер VQ-VAE перетворює їх назад у синтетичний I/Q-сигнал. На рисунку 1 концептуально показано повний конвеєр синтезу.



Рисунки 1 – Запропонований конвеєр синтезу RF-даних на основі VQ-VAE та Transformer

3. Побудова синтетичного набору даних.

3.1. Збір і попередня обробка реальних даних. Запропонована методика починається зі збирання репрезентативного набору реальних RF-сигналів, релевантних для цільового сценарію EW. Сигнали зберігаються як комплексні I/Q-послідовності, дискретизовані з частотою f_s , вибраною відповідно до критерію Найквіста для максимальної смуги сигналу.

Попередня обробка включає:

- Нормалізацію амплітуди: масштабування I/Q-відліків до діапазону $[-1, 1]$.
- Видалення DC-зсуву: віднімання середнього значення вибірки для усунення статичних зміщень.
- Нормалізацію довжини: сегментування або доповнення нулями всіх послідовностей до фіксованої довжини N (наприклад, 1024 відліки).
- Вікновування: застосування вікна Ганна для зменшення спектральних витоків перед часово-частотним аналізом.

Таблиця 3 узагальнює основні параметри набору даних, використані в експериментах.

Таблиця 3 – Основні параметри синтетичного RF-набору даних

Параметр	Значення
Кількість сигналів	500 000 комплексних I/Q-послідовностей
Типи модуляції	2FSK, 4ASK, 8PSK, 16PSK, 32QAM, 64QAM, OFDM-256
Частота дискретизації	200 кГц
Довжина сегмента	1024 відліки (5.12 мс)
Діапазон SNR	-20 дБ ... 20 дБ із кроком 2 дБ

3.2. Навчання VQ-VAE. Енкодер VQ-VAE обробляє попередньо підготовлені I/Q-сегменти та формує латентні вектори, упорядковані як послідовність нижчої часової роздільної здатності. Під час навчання ініціалізується та оновлюється кодова книга з K елементів, у якій кожному латентному вектору призначається найближчий кодовий запис. Декодер відновлює I/Q-сегмент із квантизованої латентної послідовності.

VQ-VAE навчається на змішаному наборі даних, що містить як реальні, так і змодельовані сигнали, які охоплюють множину типів модуляції та умов каналу, описаних у розділі 2. Цільова функція оптимізації є зваженою сумою втрати відновлення (наприклад, MSE) та втрат кодової книги й commitment loss [8].

3.3. Навчання генератора Transformer. Після збіжності VQ-VAE кожен навчальний сегмент кодується у послідовність індексів кодів. Ці токен-послідовності разом із умовними мітками (тип модуляції, SNR, тип каналу) використовуються для навчання авторегресивного Transformer із багатоголовою самоувагою [9, 24]. На кожному кроці модель отримує раніше згенеровані токени та умовний вектор і прогнозує розподіл для наступного токена.

На етапі генерації токен-послідовності вибираються з навченої моделі Transformer за допомогою жадібного декодування або nucleus sampling і подаються на декодер VQ-VAE для отримання синтетичних I/Q-сигналів.

4. Експериментальна постановка та оцінювання.

4.1. Набір даних і розбиття. Для оцінювання запропонованого підходу було сформовано набір даних із 500 000 комплексних I/Q-послідовностей. Набір випадково розбитий на підмножини навчання, валідації та тестування у співвідношенні 70/15/15, причому всі типи модуляції та всі рівні SNR були представлені в кожній підмножині.

4.2. Метрики якості синтетичних сигналів. Ми застосували кілька взаємодоповнювальних метрик для оцінювання якості синтетичних сигналів. Середньоквадратична помилка відновлення (MSE) вимірює відхилення між початковими та відновленими хвильовими формами. Кореляція спектрограм, визначена як коефіцієнт кореляції Пірсона між спектрограмами реальних і відновлених сигналів, характеризує збереження часово-частотної структури. Додатково використовуються топологічні метрики precision і recall у відповідному ознаковому просторі, наприклад після вбудовування за допомогою embedding-мережі, щоб оцінити, наскільки добре синтетичні зразки покривають багатовид реальних сигналів без появи хибних мод. У Таблиці 4 наведено ці показники для VQ-VAE + Transformer.

Таблиця 4 – Метрики якості для VQ-VAE + Transformer на RF-наборі даних

Метрика	Значення
MSE реконструкції	0.0245
Кореляція спектрограм	0.948
Topological precision	0.92
Topological recall	0.88

4.3. Базові архітектури. Було порівняно архітектуру VQ-VAE + Transformer з кількома базовими моделями: класичним GAN, VAE, WGAN та дифузійною моделлю, адаптованою для 1D комплексних послідовностей. Для кожної моделі вимірювався час навчання, Fréchet-подібна відстань (FID) між ознаками реальних і синтетичних сигналів, а також метрика різноманітності. Результати узагальнено в Таблиці 5.

Таблиця 5 – Порівняння генеративних моделей для синтезу RF-сигналів

Архітектура	Час навчання	FID	Різнорманітність
GAN	8 год	35.2	0.75
VAE	3 год	48.5	0.82
WGAN	10 год	28.7	0.79
Diffusion	6 год	12.1	0.91
VQ-VAE + Transformer	5 год	10.5	0.94

Запропонована архітектура VQ-VAE + Transformer демонструє найкращі значення FID і різноманітності за конкурентного часу навчання, поєднуючи переваги дискретного латентного подання та потужного послідовнісного моделювання.

Рисунок 2 візуалізує відносну продуктивність різних генеративних моделей з точки зору FID та різноманітності.



Рисунок 2 – Продуктивність генеративних моделей для синтезу RF-сигналів (FID і різноманітність)

4.4. Вплив синтетичних даних на класифікацію модуляції. Щоб кількісно оцінити вплив синтетичних даних на подальші задачі, ми навчали CNN-класифікатор модуляції на наборах із різною часткою синтетичних і реальних сигналів [6, 11].

Таблиця 6 – Вплив синтетичних даних на CNN-класифікацію модуляції

Частка синтетичних даних	Точність при SNR= 0 дБ	Точність при SNR= -10 дБ	Час навчання
0%	88.5%	72.3%	1.0 год
20%	89.7%	75.1%	0.9 год
30%	92.1%	78.6%	0.8 год
50%	93.8%	81.2%	0.7 год
70%	94.5%	82.9%	0.6 год

Результати показують, що додавання синтетичних даних суттєво підвищує стійкість за низького SNR і скорочує час навчання. Оптимальна частка синтетичних даних становить приблизно 40–50 % навчального набору. Рисунок 3 ілюструє залежність точності класифікації при SNR = -10 дБ від частки синтетичних сигналів у наборі.

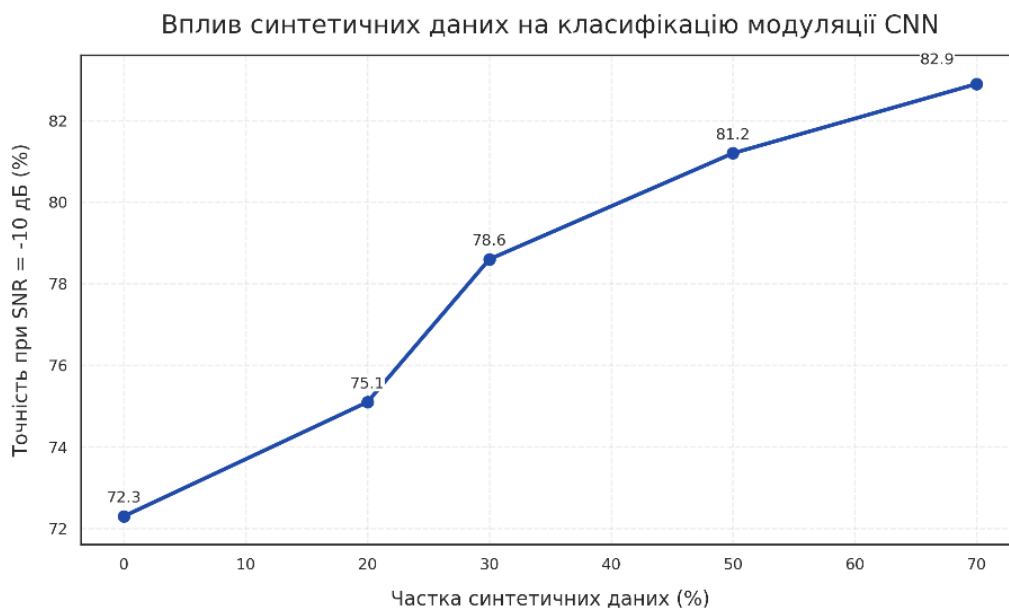


Рисунок 3 – Точність CNN-класифікації модуляції за SNR = -10 дБ залежно від частки синтетичних даних

Експериментальні результати показали, що синтетичні RF-дані можуть суттєво підвищити ефективність подальших задач радіочастотного навчання за умови їх збалансованого використання. Найкраще співвідношення між якістю узагальнення та продуктивністю було досягнуто тоді, коли частка синтетичних зразків становила приблизно 40–50 % навчальної вибірки. Це підтверджує, що синтетичні RF-дані доцільно використовувати як доповнення до реальних вимірювань, а не як повну заміну.

Висновки. У цій роботі запропоновано повний фреймворк для генерації синтетичних RF-сигналів на основі архітектури VQ-VAE + Transformer та продемонстровано його переваги для навчання моделей глибокого навчання в сценаріях електронної боротьби. Запропонований підхід забезпечує високу достовірність і різноманітність сигналів, перевершуючи базові моделі GAN, VAE, WGAN і diffusion за значеннями FID та кореляції спектрограм при збереженні прийнятної часу навчання. Показано, що доповнення CNN-класифікатора модуляції синтетичними даними суттєво підвищує точність у режимі низького SNR та скорочує час навчання. Загалом частка синтетичних даних на рівні близько 40–50 % забезпечила найкращий баланс між продуктивністю та узагальненням, що підтверджує практичну доцільність використання синтетичних RF-даних для подолання дефіциту та вартості реальних вимірювань у задачах EW і counter-UAV. Подальші дослідження будуть спрямовані на розширення фреймворку синтезу на складніші каналні моделі, зокрема частотно-селективне завмирання та апаратні спотворення, вивчення дифузійних генераторів RF-сигналів, а також інтеграцію конвеєрів синтетичних даних у системи реального часу для EW і RF-сенсингу.

ЛІТЕРАТУРА

1. Parallax Advanced Research. *Cognitive Electronic Warfare and the Fight for Spectrum Superiority* // Parallax Advanced Research. 2025. URL: <https://parallaxresearch.org/news/blog/cognitive-electronic-warfare-and-fight-spectrum-superiority> (дата звернення: 06.06.2026).

2. Inzpire. *The future is now: machine learning in electromagnetic warfare* // Inzpire. 2024. URL: <https://www.inzpire.com/news/the-future-is-now-machine-learning-in-electromagnetic-warfare> (дата звернення: 14.06.2026).
3. Mind UA. *REB: shcho tse i yak zasoby radioelektronnoi borotby protydiyut vorozhym raketam (РЕБ: що це і як засоби радіоелектронної боротьби протидіють ворожим ракетам)* // Mind.ua. 2024. URL: <https://mind.ua/publications/20269499-reb-shcho-ce-i-yak-zasobi-radioelektronnoyi-borotbi-protidyut-vorozhim-raketam> (дата звернення: 21.06.2026).
4. Goodfellow I., Pouget-Abadie J., Mirza M., Xu B., Warde-Farley D., Ozair S., Courville A., Bengio Y. *Generative adversarial nets* // *Advances in Neural Information Processing Systems* 27 / eds. Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, K. Q. Weinberger. Red Hook, NY : Curran Associates, Inc., 2014. p. 2672–2680. DOI: 10.48550/arXiv.1406.2661.
5. Kingma D. P., Welling M. *Auto-Encoding Variational Bayes* // International Conference on Learning Representations (ICLR 2014). Banff, AB, Canada, 2014. 14 p. DOI: 10.48550/arXiv.1312.6114.
6. Clark W. H. IV, Hauser S. C., Headley W. C., Michaels A. J. *Training data augmentation for deep learning radio frequency systems* // *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*. 2021. Vol. 18, No. 3. P. 217–237. DOI: 10.1177/1548512921991245.
7. Ho J., Jain A., Abbeel P. *Denoising diffusion probabilistic models* // *Advances in Neural Information Processing Systems* 33 (NeurIPS 2020). Red Hook, NY : Curran Associates, Inc., 2020. DOI: 10.48550/arXiv.2006.11239.
8. Van den Oord A., Vinyals O., Kavukcuoglu K. *Neural discrete representation learning* // *Advances in Neural Information Processing Systems* 30 (NeurIPS 2017). Red Hook, NY : Curran Associates, Inc., 2017. DOI: 10.48550/arXiv.1711.00937.
9. Razavi A., Van den Oord A., Vinyals O. *Generating diverse high-fidelity images with VQ VAE 2* // *Advances in Neural Information Processing Systems* 32 (NeurIPS 2019). Red Hook, NY : Curran Associates, Inc., 2019.
10. Kaasaragadda Y. V. N. *Efficient signal synthesis for data augmentation using generative AI* : Master's thesis. Glassboro, NJ : Rowan University, 2025. URL: <https://rdw.rowan.edu/etd/3376> (дата звернення: 21.06.2026).
11. Liu K., Zhang C., Zhao X., Wang Y., Zhang Y. *Radio frequency database construction and modulation recognition in wireless sensor networks* // *Sensors*. 2022. Vol. 22, No. 15. Article 5715. DOI: 10.3390/s22155715.
12. Sormayli J., Darvishi M., Zarrinnegar K., Mosavi M. R. *Real-time jamming detection using windowing and hybrid machine learning models for pre-saturation alerts* // *Scientific Reports*. 2025. Vol. 15, No. 1. Article 24748. DOI: 10.1038/s41598-025-10567-0.
13. GlobalSecurity. *Electronic warfare* // GlobalSecurity.org. [6. p.]. URL: <https://www.globalsecurity.org/military/systems/ground/ew.htm> (дата звернення: 14.06.2026).
14. Morehouse T., Montes C., Zhou R. *Faster region-based CNN spectrum sensing and signal identification in cluttered RF environments* // *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*. 2023.
15. Chen M., Mao X., Wang X. *Performance analysis of deep neural networks for direction of arrival estimation of multiple sources* // *IET Signal Processing*. 2023. Article e12178. DOI: 10.1049/sil2.12178.
16. Panoradio. *Overview of open datasets for RF signal classification* // Panoradio-SDR. 2025. URL: <https://panoradio-sdr.de/overview-of-open-datasets-for-rf-signal-classification/> (дата звернення: 14.06.2026).
17. IEEE. *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz*. IEEE Std 802.11ac 2013. New York IEEE, 2013.
18. CRFS. *Radio Direction Finding Techniques and Applications for EW and SIGINT* // CRFS Blog. 2024. URL: <https://www.crfs.com/blog/radio-direction-finding-techniques-and-applications-for-ew-and-sigint> (дата звернення: 17.06.2026).
19. Quasar. *Direction Finding and Geolocation Solutions* // Quasar.ai. [6. p.]. URL: <https://www.quasar.ai> (дата звернення: 14.07.2026).
20. Riyaz S., Sankhe K., Ioannidis S., Chowdhury K. *Deep learning convolutional neural networks for radio fingerprinting* // *IEEE Communications Magazine*. 2018. Vol. 56, No. 4. p. 146–152. DOI: 10.1109/MCOM.2018.1800153.

21. Caillon A., Esling P. *RAVE: a variational autoencoder for fast and high-quality audio synthesis* // *arXiv*. 2021. arXiv:2111.05011. 18 p. DOI: 10.48550/arXiv.2111.05011.
22. Sohl-Dickstein J., Weiss E. A., Maheswaranathan N., Ganguli S. *Deep unsupervised learning using nonequilibrium thermodynamics* // *Proceedings of the 32nd International Conference on Machine Learning (ICML 2015)* // *JMLR Workshop and Conference Proceedings*. 2015. Vol. 37. p. 2256–2265.
23. Chi G., Yang Z., Wu C., Xu J., Gao Y., Liu Y., Han T. X. *RF-Diffusion: Radio Signal Generation via Time-Frequency Diffusion* // *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking (ACM MobiCom'24)*. New York : Association for Computing Machinery, 2024. DOI: 10.1145/3636534.3649348.

REFERENCES:

1. Parallax Advanced Research (2025) *Cognitive Electronic Warfare and the Fight for Spectrum Superiority*.
2. Inzpire (2024) *The future is now: machine learning in electromagnetic warfare*.
3. Mind UA (2024) *РЕБ: що це і як засоби радіоелектронної боротьби протидіють ворожим ракетам*.
4. Goodfellow, I. et al. (2014) 'Generative Adversarial Nets', *NeurIPS*.
5. Kingma, D. P. and Welling, M. (2014) 'Auto-Encoding Variational Bayes', *ICLR*.
6. Clark, W. H. et al. (2020) 'Training Data Augmentation for Deep Learning Radio Modulation Classification', *arXiv*.
7. Ho, J. et al. (2020) 'Denoising Diffusion Probabilistic Models', *NeurIPS*.
8. van den Oord, A. et al. (2017) 'Neural Discrete Representation Learning', *NeurIPS*.
9. Razavi, A. et al. (2019) 'Generating Diverse High-Fidelity Images with VQ-VAE-2', *NeurIPS*.
10. Kaasaragadda, Y. et al. (2025) *Efficient Signal Synthesis for Data Augmentation using Generative AI*.
11. Liu, K. et al. (2022) 'Radio Frequency Database Construction and Modulation Recognition', *IEEE Sensors Journal*.
12. Sormayli, J. et al. (2025) 'Real-Time Jamming Detection Using Windowing and Hybrid Models', *Scientific Reports*.
13. HSC (2025) *Які бувають види РЕБ*.
14. Morehouse, T. et al. (2023) 'Faster Region-Based CNN Spectrum Sensing', *arXiv*.
15. Chen, M. et al. (2023) 'Performance Analysis of Deep Neural Networks for Direction of Arrival Estimation', *IEEE*.
16. Panoradio (2025) *Overview of Open Datasets for RF Signal Classification*.
17. IEEE (2013) *802.11ac: Physical Layer Specifications*.
18. CRFS (2024) *Radio Direction Finding Techniques and Applications for EW and SIGINT*.
19. Quasar (2024) *Direction Finding and Geolocation Solutions*.
20. Riyaz, S. et al. (2018) 'Deep Learning Convolutional Neural Networks for Radio Fingerprinting', *IEEE Communications Magazine*.
21. Caillon, A. et al. (2021) 'RAVE: a variational autoencoder for fast and high-quality audio synthesis', *ICLR*.
22. Sohl-Dickstein, J. et al. (2015) 'Deep Unsupervised Learning using Nonequilibrium Thermodynamics', *ICML*.
23. Chi G., Yang Z., Wu C., Xu J., Gao Y., Liu Y., Han T. X. *RF-Diffusion: Radio Signal Generation via Time-Frequency Diffusion* // *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking (ACM MobiCom'24)*. New York : Association for Computing Machinery, 2024. doi: 10.1145/3636534.3649348.

GENERATION OF SYNTHETIC RADIO FREQUENCY SIGNALS FOR TRAINING DEEP LEARNING MODELS IN ELECTRONIC WARFARE SCENARIOS

For the development of robust systems for remote localization and analysis of powerful jamming and countermeasure signals, a critical aspect is the availability of large and diverse training datasets. Traditional data collection using professional radio equipment and field testing is expensive, time-consuming, and often limited by technical and regulatory factors. Synthetic generation of radio frequency signals using state-of-the-art generative deep learning models offers an attractive alternative: models learn the statistical structure of real signals and channels, and then generate realistic I/Q sequences with controllable parameters. This article proposes an RF signal synthesis method based on VQ-VAE combined with an autoregressive Transformer. The proposed scheme learns the distribution of real RF signals and generates synthetic sequences conditionally specified by the modulation type, signal-to-noise ratio (SNR), and propagation channel. Experimental results on a dataset of 500,000 complex sequences showed that the VQ-VAE + Transformer architecture achieves a mean squared reconstruction error (MSE) of 0.0245 and a spectrogram correlation of 0.948, outperforming baseline GAN, VAE, WGAN, and diffusion models in terms of quality and training time.

Keywords: synthetic RF signals, generative models, VQ-VAE, Transformer, data augmentation, jamming, electronic warfare, modulation classification.

ПОРІВНЯЛЬНИЙ АНАЛІЗ КОНТАКТНОГО ТА БЕЗКОНТАКТНОГО МЕТОДІВ ВИЗНАЧЕННЯ ЕЛЕКТРОПРОВІДНОСТІ ВОДНИХ РОЗЧИНІВ

Метою дослідження є порівняльний аналіз контактного вимірювання електропровідності водних розчинів та імпедансного підходу, який розглядається як перший етап побудови безконтактного сенсора для визначення електропровідності. У роботі використано двоелектродний контактний датчик електропровідності з коефіцієнтом комірки $K = 0.993 \text{ см}^{-1}$.

Для одного й того самого зразка води міського походження проаналізовано довготривалий дрейф прямого контактного каналу та досліджено вплив значення опорного резистора на точність визначення модуля імпедансу електролітної комірки у схемі подільника напруги змінного струму з керованим вибором опорного елемента. Комутація опорних резисторів номіналами від 1 кОм до 220 кОм здійснювалася аналоговим мультиплексором CD4051 під керуванням мікроконтролера STM32G431, а вхідна та вихідна напруги оцифровувалися вбудованим аналого-цифровим перетворювачем.

Експериментально встановлено, що прямий контактний канал для незмінного зразка води демонструє відносний дрейф електропровідності близько 12.03 %, зумовлений поляризаційними процесами на межі електрод–електроліт, формуванням подвійного електричного шару та повільною динамікою приелектродного шару. Показано, що навіть спрощений одночастотний імпедансний тракт суттєво зменшує вплив повільних дрейфових процесів порівняно з прямим контактним каналом, а найменша похибка визначення модуля імпедансу, яка становить 0.21 %, досягається за умови узгодження опорного резистора з модулем досліджуваного імпедансу, що повністю відповідає теоретичному мінімуму коефіцієнта похибки.

На основі отриманих результатів обґрунтовано доцільність подальшого переходу до безконтактного вимірювання електропровідності через аналіз повної форми спектра електрохімічного імпедансу в широкому частотному діапазоні, що дозволить одержувати не лише інтегральний показник провідності, а й додаткові інформативні параметри, пов'язані з концентрацією та рухливістю іонів у розчині.

Ключові слова: електрохімічний імпеданс, електропровідність, безконтактний сенсор, електролітна комірка, опорний резистор, подільник напруги, дрейф, поляризація електродів, STM32G431, CD4051.

Вступ. Використання компактних контактних датчиків електропровідності є простим і доступним засобом оперативного контролю якості води. Разом з тим прямий контакт електродів з розчином робить результат чутливим до поляризаційних процесів, стану поверхні електродів, температури та паразитних ємнісних ефектів. Унаслідок цього навіть для незмінного зразка води вимірювальний канал може демонструвати повільний систематичний дрейф, який не пов'язаний зі зміною хімічного складу проби [1, 11, 13]. Для задач екологічного моніторингу водних ресурсів, де потрібно відстежувати невеликі зміни властивостей середовища у часі, така нестабільність є принциповим обмеженням, що робить актуальним пошук стабільніших вимірювальних підходів.

Аналіз останніх досліджень і публікацій. Дрейф та варіабельність вихідного сигналу контактних датчиків електропровідності при повторних вимірюваннях зразків міської води детально проаналізовано у [1], де показано систематичний характер зсуву, не пов'язаного зі зміною складу проби. Перспективним шляхом подолання цієї проблеми є перехід від прямого вимірювання електропровідності до аналізу електрохімічного імпедансу. У безконтактних EIS-сенсорах інформаційним параметром стає не лише інтегральний омичний опір, а й форма частотної залежності активної та реактивної складових імпедансу, що відкриває можливість роздільного аналізу концентрації та рухливості іонів і зменшує вплив повільних дрейфових

процесів завдяки роботі на частотах, значно вищих за характерні частоти поляризаційного зсуву [2, 4-10]. Питання адаптивного вибору опорного опору в портативних імпедансних вимірювачах розглянуто у [3], а принципи, обмеження та сучасні тенденції ємнісно-зв'язаної безконтактної кондуктометрії узагальнено у [4-7].

Теоретико-методологічна база електрохімічної імпедансної спектроскопії сформована у працях, присвячених еквівалентним схемам, діаграмам Найквіста, елементу Варбурга, СРЕ-моделям, перевірці коректності спектрів та підходам до інверсії імпедансних даних [16-28]. Окремий напрям становить ємнісно-зв'язана безконтактна кондуктометрія, що розвивалася від перших реалізацій C4D у капілярному електрофорезі до сучасних оглядів інструментальних схем і застосувань [4-15]. Нормативні та метрологічні вимоги до визначення електропровідності води, а також контекст онлайн-моніторингу якості води розглядаються у стандартах і оглядових роботах [29-41]. Для побудови мініатюрних сенсорів важливими є також результати з імпедансних сенсорних і біосенсорних систем, апаратної реалізації АЦП, мультиплексування та вибору вимірювальної архітектури [42-50].

Виділення невирішених раніше частин загальної проблеми. Незважаючи на наявні результати, залишається недостатньо дослідженим питання кількісного порівняння стабільності прямого контактного каналу та імпедансного тракту для однієї й тієї самої електролітної комірки, а також експериментального обґрунтування вимог до вибору опорного елемента вимірювального тракту як етапу побудови безконтактного EIS-сенсора.

Мета статті. Метою роботи є порівняльний аналіз поведінки прямого контактного каналу вимірювання електропровідності та імпедансного вимірювання для тієї самої електролітної комірки у схемі змінного струму. Такий підхід дає змогу не лише показати обмеження контактного методу, а й експериментально обґрунтувати вимоги до вибору опорного елемента у майбутньому безконтактному сенсорі [3].

Виклад основного матеріалу

Теоретичні передумови дослідження. У прямому контактному каналі електропровідність розчину визначається через омичний опір комірки. Для двоелектродного датчика з коефіцієнтом комірки K_{cell} справедливий вираз:

$$\sigma = \frac{K_{cell}}{R} \quad (1)$$

У цьому випадку будь-яка повільна зміна опору електродного інтерфейсу безпосередньо переходить у похибку визначення електропровідності. Для кількісної оцінки довготривалого дрейфу зручно використовувати відносне відхилення:

$$\delta_{\sigma} = \frac{\sigma_{max} - \sigma_{min}}{\sigma_{min}} \cdot 100 \% \quad (2)$$

Для імпедансного вимірювання електролітна комірка включається до схеми подільника напруги змінного струму. На комірку з модулем імпедансу $|Z_x|$ та опорний резистор R_{ref} подається гармонічний сигнал амплітуди V_{in} , а на комірці формується вихідна напруга V_{out} . Для модуля імпедансу маємо:

$$V_{out} = V_{in} \frac{|Z_x|}{R_{ref} + |Z_x|} \quad (3)$$

$$|Z_x| = R_{ref} \frac{V_{out}}{V_{in} - V_{out}} \quad (4)$$

У більш загальному вигляді, якщо перейти до амплітудного коефіцієнта передачі та комплексного імпедансу, отримуємо співвідношення:

$$K(\omega) = \frac{V_{out}(\omega)}{V_{in}(\omega)} \quad (5)$$

$$Z(\omega) = \frac{K(\omega)R}{1 - K(\omega)} \quad (6)$$

З аналізу похибки такого методу випливає, що її величина визначається коефіцієнтом:

$$s(\omega) = 2 + \frac{R}{|Z(\omega)|} + \frac{|Z(\omega)|}{R} \quad (7)$$

Мінімум цього коефіцієнта реалізується за умови:

$$R_{ref} \approx |Z_x| \quad (8)$$

Саме ця умова була покладена в основу експериментального підбору опорного резистора у цій роботі.

Для майбутнього безконтактного EIS-сенсора електролітний об'єм описується еквівалентною схемою, у якій активний опір розчину R_s , зарядопереносний опір R_{ct} , ємність подвійного шару C_{dl} та дифузійна складова Warburg формують частотну залежність імпедансу [8-10, 12]:

$$Z_{cell}(\omega) = R_s + \frac{1}{\frac{1}{R_{ct}} + j\omega C_{dl}} + Z_W(\omega) \quad (9)$$

Для ділянки Нернста характерна частота:

$$\omega_N = \frac{1}{R_{ct} C_{dl}} \quad (10)$$

а дифузійна частина у першому наближенні описується імпедансом Варбурга:

$$Z_W(\omega) = \sigma_W \frac{1-j}{\sqrt{\omega}} \quad (11)$$

Узагальнена діаграма Найквіста, наведена на рисунку 1, демонструє, що форма годографа містить окремі ділянки, чутливі до концентрації та рухливості іонів. Саме ця властивість і робить безконтактний імпедансний підхід принципово інформативнішим за інтегральне пряме вимірювання електропровідності [2, 4-10].

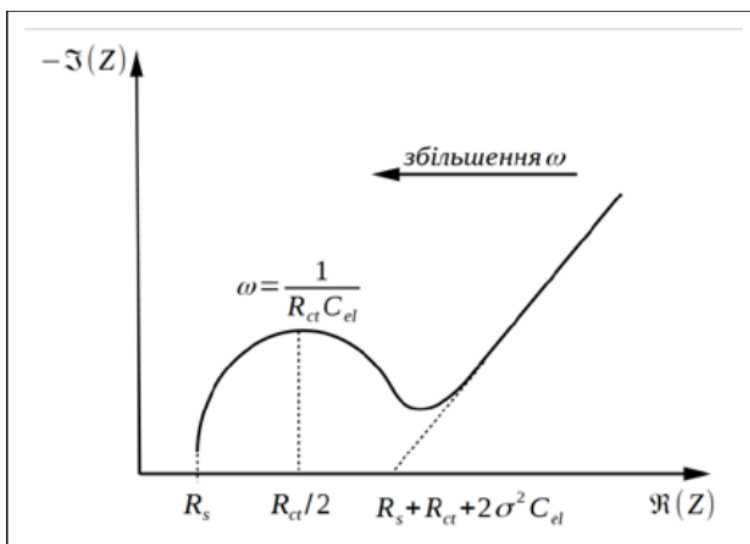


Рисунок 1 – Узагальнена діаграма Найквіста електрохімічної комірки як теоретична основа імпедансного підходу

Методика експериментальних досліджень. Експериментальна установка включала двоелектродний контактний датчик електропровідності з коефіцієнтом комірки $K = 0.993 \text{ см}^{-1}$. У прямому каналі датчик працював на частоті збудження близько 1 кГц. Аналоговий сигнал реєструвався та перераховувався у температурно компенсовані значення електропровідності для однієї й тієї самої проби води міського походження.

Для аналізу імпедансного підходу ту саму електролітну комірку було включено до схеми подільника напруги на базі STM32G431. Вхідна напруга становила 3.3 В, а частота збудження також підтримувалася поблизу 1 кГц, що дозволило порівнювати результати в однаковому частотному діапазоні. Вхідна та вихідна напруги оцифровувалися вбудованим АЦП мікроконтролера.

Для зміни значення опорного елемента використовувався аналоговий мультиплексор CD4051, до входів якого були підключені резистори 1 кОм, 4.7 кОм, 10 кОм, 47 кОм, 100 кОм та 220 кОм. Така схема дозволяла швидко комутувати R_{ref} і дослідити вплив співвідношення між R_{ref} та $|Z_x|$ на точність вимірювання. Для кожного значення опорного резистора фіксувалися V_{in} , V_{out} , розраховане значення $|Z_x|$ та відносна похибка.

Результати експериментальних досліджень та їх практичне значення. У прямому контактному каналі для незмінного зразка води було виконано 50 послідовних вимірювань. Вихідна напруга зростає від 1.68 В до 1.77 В, а температурно компенсована електропровідність – від 1.58 до 1.77 мС/см. Це відповідає відносному дрейфу електропровідності приблизно 12.03 %, що прямо вказує на систематичний зсув, пов'язаний з поляризацією електродів та повільною динамікою приелектродного шару (рис. 2).

шару в часі (рис. 1).

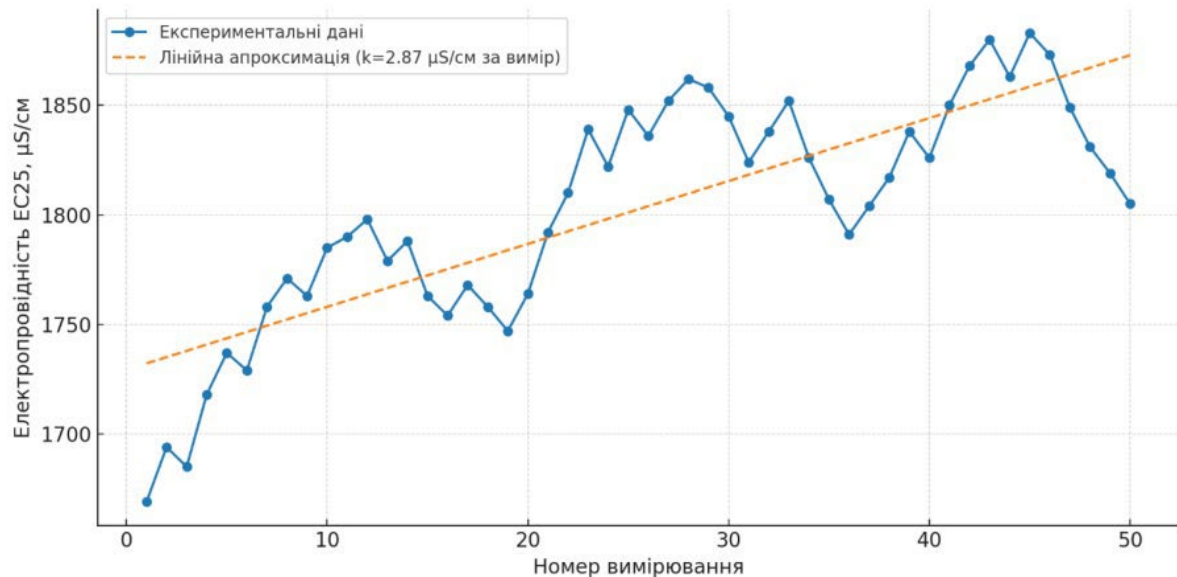


Рисунок 2 – Експериментальна динаміка вихідного сигналу контактного сенсора електропровідності для одного й того самого зразка води

Для того самого сенсора далі було досліджено імпедансний вимірювальний тракт при різних значеннях опорного резистора. Результати експерименту наведено в таблиці 1.

Таблиця 1 – Результати визначення модуля імпедансу електролітної комірки при різних значеннях опорного резистора

№	Опорний резистор, Ом	Вхідна напруга, В	Напруга на комірці, В	$ Z_x $, Ом	Похибка, %
1	1 000	3.30	2.73	4650	1.06
2	4 700	3.30	1.65	4710	0.21
3	10 000	3.30	1.06	4760	1.27
4	47 000	3.30	0.31	5050	7.45
5	100 000	3.30	0.16	5200	10.64
6	220 000	3.30	0.07	5480	16.60

Для наведених у таблиці значень коефіцієнт узгодження $L = R_{ref} / |Z_x|$ дорівнює 0.215, 0.998, 2.101, 9.307, 19.231 та 40.146 відповідно, а коефіцієнт похибки $s(\omega)$ – 6.865, 4.000, 4.577, 11.414, 21.283 та 42.171. Таким чином, експериментальні дані прямо підтверджують теоретичний мінімум похибки поблизу умови $R_{ref} \approx |Z_x|$ (рис. 3, рис. 4).

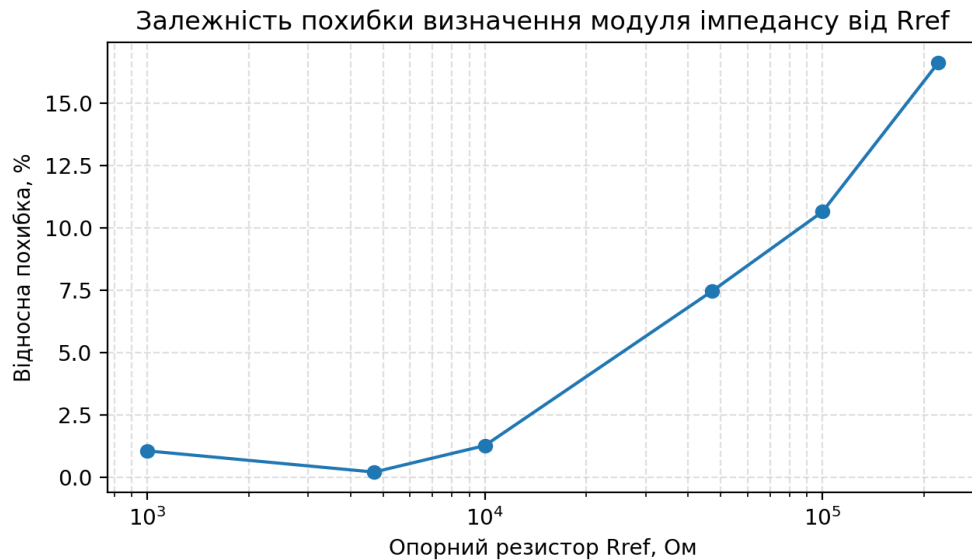


Рисунок 3 – Залежність відносної похибки визначення модуля імпедансу від значення опорного резистора

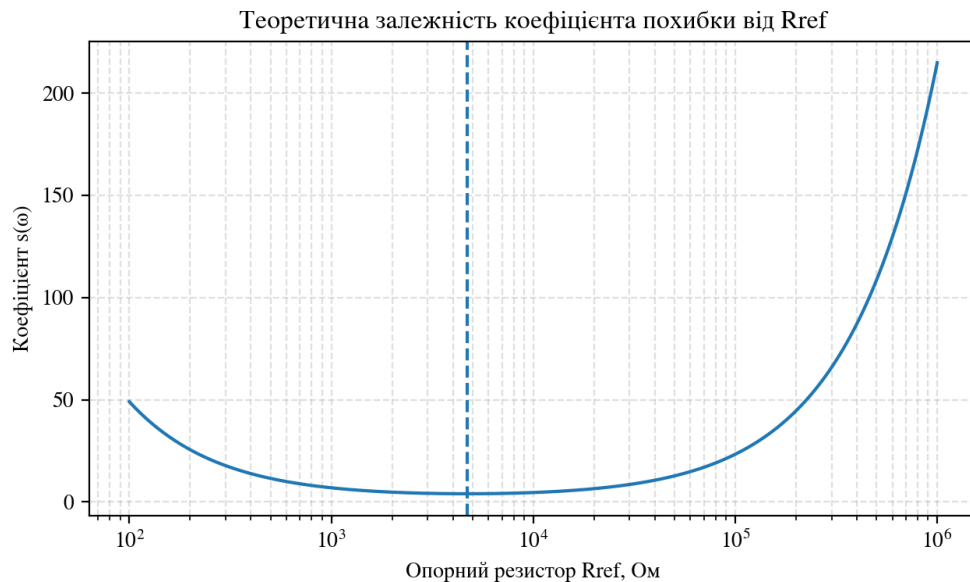


Рисунок 4 – Теоретична залежність коефіцієнта похибки $s(\omega)$ від значення опорного резистора для $|Z_x| \approx 4.7 \text{ кОм}$

Наведені результати показують, що прямий контактний канал навіть за сталої температури та незмінного складу проби демонструє помітний дрейф. Його джерелом є не вимірюваний показник як такий, а перебудова електродного інтерфейсу, формування подвійного шару та повільні процеси релаксації заряду. Саме тому контактне вимірювання інтегральної електропровідності виявляється недостатньо стабільним для задач, де потрібно відслідковувати невеликі зміни властивостей середовища у часі.

Імпедансний тракт працює за іншою логікою: замість безпосереднього використання абсолютного вихідного рівня реєструється відношення V_{out}/V_{in} у схемі змінного струму. Це дозволяє істотно зменшити вплив повільних зсувів і перенести акцент з інтегрального омичного опору на частотну поведінку електролітної комірки. Уже в одночастотному режимі при правильно підбраному R_{ref} вдалося отримати похибку лише 0.21 %, що більш ніж у п'ятдесят разів менше за зафіксований відносний дрейф електропровідності у прямому контактному каналі (рис. 5).

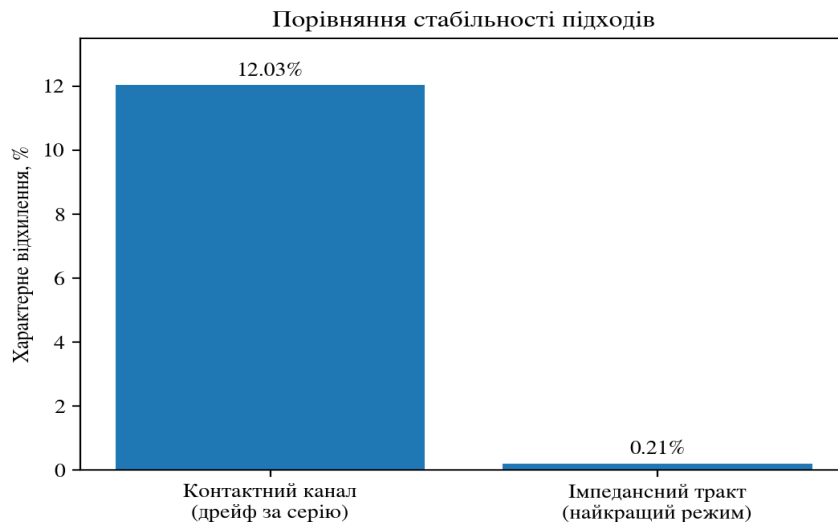


Рисунок 5 – Порівняння характерного відхилення для прямого контактного каналу та найкращого режиму імпедансного тракту

Таблиця 1, рис. 3 і рис. 4 показують, що мінімум похибки реалізується при $R_{ref} = 4.7$ кОм, тобто у випадку, коли опорний резистор за порядком величини збігається з модулем досліджуваного імпедансу. Це повністю узгоджується з теоретичним мінімумом коефіцієнта $s(\omega)$. При переході до $R_{ref} = 47$ кОм, 100 кОм та 220 кОм похибка швидко зростає, оскільки напруга на комірці стає занадто малою, а внесок шуму, квантової похибки АЦП та паразитних параметрів схеми збільшується.

Разом з тим поточна реалізація ще не є безконтактним сенсором у повному розумінні. По-перше, у цій роботі визначався лише модуль імпедансу, тоді як фазова складова не реєструвалася. По-друге, сама електролітна комірка залишалася контактною, тому електродна поляризація повністю не усувалася, а лише ставала менш впливовою для результату. По-третє, використання CD4051 додає власний опір відкритого каналу та паразитні ємності, що особливо помітно при малих опорах і може вносити систематичну похибку.

Отже, проведений експеримент слід розглядати як важливий інженерний етап на шляху до безконтактного вимірювання провідності через імпеданс. Він показує, що вибір опорного елемента не є другорядним конструктивним параметром, а безпосередньо визначає точність вимірювального тракту. У майбутньому перехід від контактної комірки до безконтактного EIS-сенсора дозволить поєднати переваги стабільнішого імпедансного методу з аналізом форми спектра, тобто одержувати не лише інтегральний показник провідності, а й додаткові інформативні параметри, пов'язані з концентрацією та рухливістю іонів.

Висновки. Експериментально встановлено, що прямий контактний канал вимірювання електропровідності для сталого зразка води демонструє відносний дрейф близько 12.03 %, що зумовлено поляризаційними процесами на межі електрод–електроліт.

Показано, що при переході до імпедансного тракту на основі подільника напруги та вимірювання відношення V_{out}/V_{in} точність визначення модуля імпедансу суттєво залежить від вибору опорного резистора.

Мінімальна похибка 0.21 % досягається при $R_{ref} = 4.7$ кОм, тобто за умови узгодження опорного резистора з модулем досліджуваного імпедансу. Це узгоджується з теоретичним мінімумом коефіцієнта похибки $s(\omega)$.

Навіть у спрощеній одночастотній реалізації імпедансний підхід є значно стійкішим до повільних дрейфових зсувів, ніж пряме контактне вимірювання електропровідності.

Отримані результати обґрунтовують подальший перехід до безконтактного сенсора електропровідності на основі методу електрохімічного імпедансу, у якому будуть використані не лише значення модуля, а й повна форма спектра у широкому частотному діапазоні.

ЛІТЕРАТУРА:

1. Каберник В.О., Ольшевський С.В. Аналіз дрейфу та варіабельності вихідного сигналу контактних датчиків електропровідності при повторних вимірюваннях зразків міської води. *Proceedings of the Conference on Electronic Measurement and Instrumentation*. Kyiv, Ukraine. 2025. с. 45-49.
2. Ольшевський С.В., Бех І.І., Каберник В.О. Вдосконалення систем екологічного моніторингу водних ресурсів шляхом застосування безконтактних сенсорів електрохімічного імпедансу. *Екологічні науки*. 2024. № 2(53). с. 39-49.
3. Wang X., Zhao H., Wang A., Dong Z., Fan Y., Zhai Z. A Portable Impedance Spectroscopy Measurement Method Through Adaptive Reference Resistance. *IEEE Access*. 2021. Vol. 9. p. 88011-88018. DOI: 10.1109/ACCESS.2021.3077308.
4. Tůma A., Kubáň P. Capacitively coupled contactless conductivity detection: Principles, limitations and recent trends. *Analytical Methods*. 2012. Vol. 4. No. 1. p. 25-33. DOI: 10.1039/C1AY05424A.
5. Kubáň P., Hauser P.C. A review of the recent achievements in capacitively coupled contactless conductivity detection. *Analytica Chimica Acta*. 2008. Vol. 607. No. 1. P. 15-29. DOI: 10.1016/j.aca.2007.11.045.
6. Kubáň P., Hauser P.C. Ten years of axial capacitively coupled contactless conductivity detection for CZE - a review. *Electrophoresis*. 2009. Vol. 30. No. 1. p. 176-188. DOI: 10.1002/elps.200800478.
7. Kubáň P., Hauser P.C. Capacitively coupled contactless conductivity detection for microseparation techniques - recent developments. *Electrophoresis*. 2011. Vol. 32. No. 1. p. 30-42. DOI: 10.1002/elps.201000354.
8. Kubáň P., Hauser P.C. Contactless conductivity detection for analytical techniques - developments from 2014 to 2016. *Electrophoresis*. 2017. Vol. 38. No. 1. p. 95-114. DOI: 10.1002/elps.201600280.
9. Kubáň P., Hauser P.C. Contactless conductivity detection for analytical techniques: Developments from 2016 to 2018. *Electrophoresis*. 2019. Vol. 40. No. 1. p. 124-139. DOI: 10.1002/elps.201800248.
10. Hauser P.C., Kubáň P. Capacitively coupled contactless conductivity detection for analytical techniques - Developments from 2018 to 2020. *Journal of Chromatography A*. 2020. Vol. 1632. Article 461616. DOI: 10.1016/j.chroma.2020.461616.
11. Hauser P.C., Kubáň P. Contactless conductivity detection for capillary electrophoresis - developments from 2020 to 2024. *Electrophoresis*. 2025. DOI: 10.1002/elps.202400217.
12. Zemmann A.J., Schnell E., Volgger D., Bonn G.K. Contactless conductivity detection for capillary electrophoresis. *Analytical Chemistry*. 1998. Vol. 70. No. 3. p. 563-567. DOI: 10.1021/ac9707592.
13. Fracassi da Silva J.A., do Lago C.L. An oscillometric detector for capillary electrophoresis. *Analytical Chemistry*. 1998. Vol. 70. No. 20. p. 4339-4343. DOI: 10.1021/ac980185g.
14. Brito-Neto J.G.A., Fracassi da Silva J.A., Blanes L., do Lago C.L. Understanding capacitively coupled contactless conductivity detection in capillary and microchip electrophoresis. Part 1. Fundamentals. *Electroanalysis*. 2005. Vol. 17. No. 13. p. 1198-1206. DOI: 10.1002/elan.200503237.
15. Brito-Neto J.G.A., Fracassi da Silva J.A., Blanes L., do Lago C.L. Understanding capacitively coupled contactless conductivity detection in capillary and microchip electrophoresis. Part 2. Peak shape, stray capacitance, noise, and actual electronics. *Electroanalysis*. 2005. Vol. 17. No. 13. P. 1207-1214. DOI: 10.1002/elan.200503238.
16. Barsoukov E., Macdonald J.R. (eds.). *Impedance Spectroscopy: Theory, Experiment, and Applications*. 3rd ed. Hoboken: Wiley, 2018. 560 p. DOI: 10.1002/9781119381860.
17. Orazem M.E., Tribollet B. *Electrochemical Impedance Spectroscopy*. 2nd ed. Hoboken: Wiley, 2017. 768 p. DOI: 10.1002/9781119363682.
18. Lasia A. *Electrochemical Impedance Spectroscopy and its Applications*. New York: Springer, 2014. 367 p. DOI: 10.1007/978-1-4614-8933-7.
19. Bard A.J., Faulkner L.R., White H.S. *Electrochemical Methods: Fundamentals and Applications*. 3rd ed. Hoboken: Wiley, 2022. 1104 p. ISBN: 978-1-119-33406-4. URL: <https://books.wiley.com/titles/9781119334064/>
20. Zoski C.G. (ed.). *Handbook of Electrochemistry*. Amsterdam: Elsevier, 2007. 935 p. DOI: 10.1016/B978-0-444-51958-0.X5000-9.
21. Newman J., Thomas-Alyea K.E. *Electrochemical Systems*. 3rd ed. Hoboken: Wiley-Interscience, 2004. 672 p. ISBN: 978-0-471-47756-3. URL: https://books.google.com/books/about/Electrochemical_Systems.html?id=vArZu0HM-xYC
22. Randles J.E.B. Kinetics of rapid electrode reactions. *Discussions of the Faraday Society*. 1947. Vol. 1. P. 11-19. DOI: 10.1039/DF9470100011.

23. Brug G.J., van den Eeden A.L.G., Sluyters-Rehbach M., Sluyters J.H. The analysis of electrode impedances complicated by the presence of a constant phase element. *Journal of Electroanalytical Chemistry and Interfacial Electrochemistry*. 1984. Vol. 176. No. 1-2. p. 275-295. DOI: 10.1016/S0022-0728(84)80324-1.
24. Hsu C.H., Mansfeld F. Technical note: Concerning the conversion of the constant phase element parameter Y_0 into a capacitance. *Corrosion*. 2001. Vol. 57. No. 9. P. 747-748. DOI: 10.5006/1.3280607.
25. Boukamp B.A. A package for impedance/admittance data analysis. *Solid State Ionics*. 1986. Vol. 18-19. Part 1. p. 136-140. DOI: 10.1016/0167-2738(86)90100-1.
26. Ciucci F., Chen C. Analysis of electrochemical impedance spectroscopy data using the distribution of relaxation times: A Bayesian and hierarchical Bayesian approach. *Electrochimica Acta*. 2015. Vol. 167. p. 439-454. DOI: 10.1016/j.electacta.2015.03.123.
27. Effendy S., Song J., Bazant M.Z. Analysis, design, and generalization of electrochemical impedance spectroscopy (EIS) inversion algorithms. *Journal of The Electrochemical Society*. 2020. Vol. 167. No. 10. Article 106508. DOI: 10.1149/1945-7111/ab9c82.
28. Halleman N., Howey D., Battistel A., Saniee N.F., Scarpioni F., Wouters B., La Mantia F., Hubin A., Widanage W.D., Lataire J. Electrochemical impedance spectroscopy beyond linearity and stationarity - a critical review. *Electrochimica Acta*. 2023. Vol. 466. Article 142939. DOI: 10.1016/j.electacta.2023.142939.
29. ASTM D1125-23. Standard Test Methods for Electrical Conductivity and Resistivity of Water. West Conshohocken: ASTM International, 2023. 8 p. DOI: 10.1520/D1125-23.
30. ISO 7888:1985. Water quality - Determination of electrical conductivity. Geneva: International Organization for Standardization, 1985. 6 p.
31. APHA, AWWA, WEF. Standard Methods for the Examination of Water and Wastewater. Method 2510B: Conductivity - Laboratory Method. Standard Methods Online. URL: https://www.nemi.gov/methods/method_summary/5702/
32. U.S. Environmental Protection Agency. Method 120.1: Conductance (Specific Conductance, μmhos at 25°C). Approved for NPDES, Editorial Revision 1982. URL: <https://nepis.epa.gov/Exe/ZyPURL.cgi?Dockey=P101AVQP.txt>
33. World Health Organization. Guidelines for drinking-water quality: fourth edition incorporating the first and second addenda. Geneva: World Health Organization, 2022. 614 p. ISBN: 978-92-4-004506-4.
34. Storey M.V., van der Gaag B., Burns B.P. Advances in on-line drinking water quality monitoring and early warning systems. *Water Research*. 2011. Vol. 45. No. 2. p. 741-747. DOI: 10.1016/j.watres.2010.08.049.
35. Banna M.H., Imran S., Francisque A., Najjaran H., Sadiq R., Rodriguez M., Hoorfar M. Online drinking water quality monitoring: Review on available and emerging technologies. *Critical Reviews in Environmental Science and Technology*. 2014. Vol. 44. No. 12. p. 1370-1421. DOI: 10.1080/10643389.2013.781936.
36. Lambrou T.P., Anastasiou C.C., Panayiotou C.G., Polycarpou M.M. A low-cost sensor network for real-time monitoring and contamination detection in drinking water distribution systems. *IEEE Sensors Journal*. 2014. Vol. 14. No. 8. p. 2765-2772. DOI: 10.1109/JSEN.2014.2316414.
37. Banna M.H., Najjaran H., Sadiq R., Imran S.A., Rodriguez M., Hoorfar M. Miniaturized water quality monitoring pH and conductivity sensors. *Sensors and Actuators B: Chemical*. 2014. Vol. 193. p. 434-441. DOI: 10.1016/j.snb.2013.12.002.
38. Zhou B., Bian C., Tong J., Xia S. Fabrication of a miniature multi-parameter sensor chip for water quality assessment. *Sensors*. 2017. Vol. 17. No. 1. Article 157. DOI: 10.3390/s17010157.
39. Geetha S., Gouthami S. Internet of things enabled real time water quality monitoring system. *Smart Water*. 2017. Vol. 2. Article 1. DOI: 10.1186/s40713-017-0005-y.
40. Pasika S., Gandla S.T. Smart water quality monitoring system with cost-effective using IoT. *Heliyon*. 2020. Vol. 6. No. 7. Article e04096. DOI: 10.1016/j.heliyon.2020.e04096.
41. Droujko J., Molnar P. Open-source, low-cost, in-situ turbidity sensor for river network monitoring. *Scientific Reports*. 2022. Vol. 12. Article 10341. DOI: 10.1038/s41598-022-14228-4.
42. Grossi M., Riccò B. Electrical impedance spectroscopy (EIS) for biological analysis and food characterization: a review. *Journal of Sensors and Sensor Systems*. 2017. Vol. 6. p. 303-325. DOI: 10.5194/jsss-6-303-2017.
43. Lisdat F., Schäfer D. The use of electrochemical impedance spectroscopy for biosensing. *Analytical and Bioanalytical Chemistry*. 2008. Vol. 391. No. 5. P. 1555-1567. DOI: 10.1007/s00216-008-1970-7.
44. Daniels J.S., Pourmand N. Label-free impedance biosensors: Opportunities and challenges. *Electroanalysis*. 2007. Vol. 19. No. 12. p. 1239-1257. DOI: 10.1002/elan.200603855.

45. Yang L., Bashir R. Electrical/electrochemical impedance for rapid detection of foodborne pathogenic bacteria. *Biotechnology Advances*. 2008. Vol. 26. No. 2. p. 135-150. DOI: 10.1016/j.biotechadv.2007.10.003.
46. Patil R.S., Juvekar V.A., Nalage U. An electrochemical technique for measurements of electrical conductivity of aqueous electrolytes. *arXiv preprint*. 2017. arXiv:1712.07382.
47. STMicroelectronics. STM32G431C6 product page: Mainstream Arm Cortex-M4 MCU 170 MHz with 32 Kbytes Flash memory and medium analog integration. Geneva: STMicroelectronics. URL: <https://www.st.com/en/microcontrollers-microprocessors/stm32g431c6.html>
48. Texas Instruments. CD405xB CMOS Single 8-Channel Analog Multiplexer or Demultiplexer With Logic-Level Conversion: Datasheet SCHS047O Rev. O. Dallas: Texas Instruments, 2026. 48 p.
49. Kester W. (ed.). *The Data Conversion Handbook*. Burlington: Newnes, 2005. 953 p. DOI: 10.1016/B978-0-7506-7841-4.X5000-3.
50. Kester W. *ADC Architectures III: Sigma-Delta ADC Basics*. Tutorial MT-022. Norwood: Analog Devices, 2008. 12 p.

REFERENCES:

1. Kabernyk, V.O. and Olshevskiy, S.V. (2025), “Analiz dreifu ta variabelnosti vykhidnoho syhnalu kontaktnykh datchykyv elektroprovidnosti pry povtornykh vymiryuvanniakh zrazkiv miskoi vody” [Analysis of drift and variability of the output signal of contact conductivity sensors during repeated measurements of urban water samples], *Proceedings of the Conference on Electronic Measurement and Instrumentation*, Kyiv, Ukraine, pp. 45-49.
2. Olshevskiy, S.V., Bekh, I.I. and Kabernyk, V.O. (2024), “Vdoskonalennia system ekolohichnoho monitorynhu vodnykh resursiv shliakhom zastosuvannia bezkontaktnykh sensoriv elektrokhimichnoho impedansu” [Improvement of water resources ecological monitoring systems through the use of contactless electrochemical impedance sensors], *Ekolohichni nauky*, No. 2(53), pp. 39-49.
3. Wang, X., Zhao, H., Wang, A., Dong, Z., Fan, Y. and Zhai, Z. (2021), “A Portable Impedance Spectroscopy Measurement Method Through Adaptive Reference Resistance”, *IEEE Access*, Vol. 9, pp. 88011-88018. DOI: 10.1109/ACCESS.2021.3077308.
4. Tůma, A. and Kubáň, P. (2012), “Capacitively coupled contactless conductivity detection: Principles, limitations and recent trends”, *Analytical Methods*, Vol. 4, No. 1, pp. 25-33. DOI: 10.1039/C1AY05424A.
5. Kubáň, P. and Hauser, P.C. (2008), “A review of the recent achievements in capacitively coupled contactless conductivity detection”, *Analytica Chimica Acta*, Vol. 607, No. 1, pp. 15-29. DOI: 10.1016/j.aca.2007.11.045.
6. Kubáň, P. and Hauser, P.C. (2009), “Ten years of axial capacitively coupled contactless conductivity detection for CZE - a review”, *Electrophoresis*, Vol. 30, No. 1, pp. 176-188. DOI: 10.1002/elps.200800478.
7. Kubáň, P. and Hauser, P.C. (2011), “Capacitively coupled contactless conductivity detection for microseparation techniques - recent developments”, *Electrophoresis*, Vol. 32, No. 1, pp. 30-42. DOI: 10.1002/elps.201000354.
8. Kubáň, P. and Hauser, P.C. (2017), “Contactless conductivity detection for analytical techniques - developments from 2014 to 2016”, *Electrophoresis*, Vol. 38, No. 1, pp. 95-114. DOI: 10.1002/elps.201600280.
9. Kubáň, P. and Hauser, P.C. (2019), “Contactless conductivity detection for analytical techniques: Developments from 2016 to 2018”, *Electrophoresis*, Vol. 40, No. 1, pp. 124-139. DOI: 10.1002/elps.201800248.
10. Hauser, P.C. and Kubáň, P. (2020), “Capacitively coupled contactless conductivity detection for analytical techniques - Developments from 2018 to 2020”, *Journal of Chromatography A*, Vol. 1632, Article 461616. DOI: 10.1016/j.chroma.2020.461616.
11. Hauser, P.C. and Kubáň, P. (2025), “Contactless conductivity detection for capillary electrophoresis - developments from 2020 to 2024”, *Electrophoresis*. DOI: 10.1002/elps.202400217.
12. Zemann, A.J., Schnell, E., Volgger, D. and Bonn, G.K. (1998), “Contactless conductivity detection for capillary electrophoresis”, *Analytical Chemistry*, Vol. 70, No. 3, pp. 563-567. DOI: 10.1021/ac9707592.
13. Fracassi da Silva, J.A. and do Lago, C.L. (1998), “An oscillometric detector for capillary electrophoresis”, *Analytical Chemistry*, Vol. 70, No. 20, pp. 4339-4343. DOI: 10.1021/ac980185g.
14. Brito-Neto, J.G.A., Fracassi da Silva, J.A., Blanes, L. and do Lago, C.L. (2005), “Understanding capacitively coupled contactless conductivity detection in capillary and microchip electrophoresis. Part 1. Fundamentals”, *Electroanalysis*, Vol. 17, No. 13, pp. 1198-1206. DOI: 10.1002/elan.200503237.

15. Brito-Neto, J.G.A., Fracassi da Silva, J.A., Blanes, L. and do Lago, C.L. (2005), "Understanding capacitively coupled contactless conductivity detection in capillary and microchip electrophoresis. Part 2. Peak shape, stray capacitance, noise, and actual electronics", *Electroanalysis*, Vol. 17, No. 13, pp. 1207-1214. DOI: 10.1002/elan.200503238.
16. Barsoukov, E. and Macdonald, J.R. (eds.) (2018), *Impedance Spectroscopy: Theory, Experiment, and Applications*, 3rd ed., Wiley, Hoboken, 560 p. DOI: 10.1002/9781119381860.
17. Orazem, M.E. and Tribollet, B. (2017), *Electrochemical Impedance Spectroscopy*, 2nd ed., Wiley, Hoboken, 768 p. DOI: 10.1002/9781119363682.
18. Lasia, A. (2014), *Electrochemical Impedance Spectroscopy and its Applications*, Springer, New York, 367 p. DOI: 10.1007/978-1-4614-8933-7.
19. Bard, A.J., Faulkner, L.R. and White, H.S. (2022), *Electrochemical Methods: Fundamentals and Applications*, 3rd ed., Wiley, Hoboken, 1104 p. ISBN: 978-1-119-33406-4. Available at: <https://books.wiley.com/titles/9781119334064/>
20. Zoski, C.G. (ed.) (2007), *Handbook of Electrochemistry*, Elsevier, Amsterdam, 935 p. DOI: 10.1016/B978-0-444-51958-0.X5000-9.
21. Newman, J. and Thomas-Alyea, K.E. (2004), *Electrochemical Systems*, 3rd ed., Wiley-Interscience, Hoboken, 672 p. ISBN: 978-0-471-47756-3. Available at: https://books.google.com/books/about/Electrochemical_Systems.html?id=vArZu0HM-xYC
22. Randles, J.E.B. (1947), "Kinetics of rapid electrode reactions", *Discussions of the Faraday Society*, Vol. 1, pp. 11-19. DOI: 10.1039/DF9470100011.
23. Brug, G.J., van den Eeden, A.L.G., Sluyters-Rehbach, M. and Sluyters, J.H. (1984), "The analysis of electrode impedances complicated by the presence of a constant phase element", *Journal of Electroanalytical Chemistry and Interfacial Electrochemistry*, Vol. 176, No. 1-2, pp. 275-295. DOI: 10.1016/S0022-0728(84)80324-1.
24. Hsu, C.H. and Mansfeld, F. (2001), "Technical note: Concerning the conversion of the constant phase element parameter Y_0 into a capacitance", *Corrosion*, Vol. 57, No. 9, pp. 747-748. DOI: 10.5006/1.3280607.
25. Boukamp, B.A. (1986), "A package for impedance/admittance data analysis", *Solid State Ionics*, Vol. 18-19, Part 1, pp. 136-140. DOI: 10.1016/0167-2738(86)90100-1.
26. Ciucci, F. and Chen, C. (2015), "Analysis of electrochemical impedance spectroscopy data using the distribution of relaxation times: A Bayesian and hierarchical Bayesian approach", *Electrochimica Acta*, Vol. 167, pp. 439-454. DOI: 10.1016/j.electacta.2015.03.123.
27. Effendy, S., Song, J. and Bazant, M.Z. (2020), "Analysis, design, and generalization of electrochemical impedance spectroscopy (EIS) inversion algorithms", *Journal of The Electrochemical Society*, Vol. 167, No. 10, Article 106508. DOI: 10.1149/1945-7111/ab9c82.
28. Halleman, N., Howey, D., Battistel, A., Saniee, N.F., Scarpioni, F., Wouters, B., La Mantia, F., Hubin, A., Widanage, W.D. and Lataire, J. (2023), "Electrochemical impedance spectroscopy beyond linearity and stationarity - a critical review", *Electrochimica Acta*, Vol. 466, Article 142939. DOI: 10.1016/j.electacta.2023.142939.
29. ASTM D1125-23 (2023), *Standard Test Methods for Electrical Conductivity and Resistivity of Water*, ASTM International, West Conshohocken, 8 p. DOI: 10.1520/D1125-23.
30. ISO 7888:1985 (1985), *Water quality - Determination of electrical conductivity*, International Organization for Standardization, Geneva, 6 p.
31. APHA, AWWA and WEF, *Standard Methods for the Examination of Water and Wastewater*, Method 2510B: Conductivity - Laboratory Method, *Standard Methods Online*. Available at: https://www.nemi.gov/methods/method_summary/5702/
32. U.S. Environmental Protection Agency (1982), *Method 120.1: Conductance (Specific Conductance, μmhos at 25 °C)*, Approved for NPDES, Editorial Revision 1982. Available at: <https://nepis.epa.gov/Exe/ZyPURL.cgi?Dockkey=P101AVQP.txt>
33. World Health Organization (2022), *Guidelines for drinking-water quality: fourth edition incorporating the first and second addenda*, World Health Organization, Geneva, 614 p. ISBN: 978-92-4-004506-4.
34. Storey, M.V., van der Gaag, B. and Burns, B.P. (2011), "Advances in on-line drinking water quality monitoring and early warning systems", *Water Research*, Vol. 45, No. 2, pp. 741-747. DOI: 10.1016/j.watres.2010.08.049.

35. Banna, M.H., Imran, S., Francisque, A., Najjaran, H., Sadiq, R., Rodriguez, M. and Hoorfar, M. (2014), "Online drinking water quality monitoring: Review on available and emerging technologies", *Critical Reviews in Environmental Science and Technology*, Vol. 44, No. 12, pp. 1370-1421. DOI: 10.1080/10643389.2013.781936.
36. Lambrou, T.P., Anastasiou, C.C., Panayiotou, C.G. and Polycarpou, M.M. (2014), "A low-cost sensor network for real-time monitoring and contamination detection in drinking water distribution systems", *IEEE Sensors Journal*, Vol. 14, No. 8, pp. 2765-2772. DOI: 10.1109/JSEN.2014.2316414.
37. Banna, M.H., Najjaran, H., Sadiq, R., Imran, S.A., Rodriguez, M. and Hoorfar, M. (2014), "Miniaturized water quality monitoring pH and conductivity sensors", *Sensors and Actuators B: Chemical*, Vol. 193, pp. 434-441. DOI: 10.1016/j.snb.2013.12.002.
38. Zhou, B., Bian, C., Tong, J. and Xia, S. (2017), "Fabrication of a miniature multi-parameter sensor chip for water quality assessment", *Sensors*, Vol. 17, No. 1, Article 157. DOI: 10.3390/s17010157.
39. Geetha, S. and Gouthami, S. (2017), "Internet of things enabled real time water quality monitoring system", *Smart Water*, Vol. 2, Article 1. DOI: 10.1186/s40713-017-0005-y.
40. Pasika, S. and Gandla, S.T. (2020), "Smart water quality monitoring system with cost-effective using IoT", *Heliyon*, Vol. 6, No. 7, Article e04096. DOI: 10.1016/j.heliyon.2020.e04096.
41. Droujko, J. and Molnar, P. (2022), "Open-source, low-cost, in-situ turbidity sensor for river network monitoring", *Scientific Reports*, Vol. 12, Article 10341. DOI: 10.1038/s41598-022-14228-4.
42. Grossi, M. and Riccò, B. (2017), "Electrical impedance spectroscopy (EIS) for biological analysis and food characterization: a review", *Journal of Sensors and Sensor Systems*, Vol. 6, pp. 303-325. DOI: 10.5194/jsss-6-303-2017.
43. Lisdat, F. and Schäfer, D. (2008), "The use of electrochemical impedance spectroscopy for biosensing", *Analytical and Bioanalytical Chemistry*, Vol. 391, No. 5, pp. 1555-1567. DOI: 10.1007/s00216-008-1970-7.
44. Daniels, J.S. and Pourmand, N. (2007), "Label-free impedance biosensors: Opportunities and challenges", *Electroanalysis*, Vol. 19, No. 12, pp. 1239-1257. DOI: 10.1002/elan.200603855.
45. Yang, L. and Bashir, R. (2008), "Electrical/electrochemical impedance for rapid detection of foodborne pathogenic bacteria", *Biotechnology Advances*, Vol. 26, No. 2, pp. 135-150. DOI: 10.1016/j.biotechadv.2007.10.003.
46. Patil, R.S., Juvekar, V.A. and Nalage, U. (2017), "An electrochemical technique for measurements of electrical conductivity of aqueous electrolytes", *arXiv preprint*, arXiv:1712.07382.
47. STMicroelectronics, STM32G431C6 product page: Mainstream Arm Cortex-M4 MCU 170 MHz with 32 Kbytes Flash memory and medium analog integration, STMicroelectronics, Geneva. Available at: <https://www.st.com/en/microcontrollers-microprocessors/stm32g431c6.html>
48. Texas Instruments (2026), CD405xB CMOS Single 8-Channel Analog Multiplexer or Demultiplexer With Logic-Level Conversion: Datasheet SCHS047O Rev. O, Texas Instruments, Dallas, 48 p.
49. Kester, W. (ed.) (2005), *The Data Conversion Handbook*, Newnes, Burlington, 953 p. DOI: 10.1016/B978-0-7506-7841-4.X5000-3.
50. Kester, W. (2008), *ADC Architectures III: Sigma-Delta ADC Basics*, Tutorial MT-022, Analog Devices, Norwood, 12 p.

Kabernyk V., D.Sc. Olszewski S.

COMPARATIVE ANALYSIS OF CONTACT AND CONTACTLESS METHODS FOR DETERMINING THE ELECTRICAL CONDUCTIVITY OF AQUEOUS SOLUTIONS

The purpose of this study is a comparative analysis of the direct contact measurement of the electrical conductivity of aqueous solutions and the impedance-based approach, which is considered as the first stage in the development of a contactless sensor for determining the conductivity of aqueous solutions. A two-electrode contact conductivity sensor with a cell constant $K = 0.993 \text{ cm}^{-1}$ was used in this work. For the same sample of municipal water, the long-term drift of the direct contact channel was analyzed, and the influence of the reference resistor value on the accuracy of determining the impedance modulus of the electrolytic cell in an AC voltage divider circuit with controlled selection of the reference element was investigated. The switching of reference resistors with nominal values from 1 kΩ to 220 kΩ was performed by a CD4051 analog multiplexer controlled by an STM32G431 microcontroller, while the input and output voltages were digitized by the built-in analog-to-digital converter. It was experimentally established that the

direct contact channel demonstrates a relative conductivity drift of about 12.03 % for an unchanged water sample, which is caused by polarization processes at the electrode–electrolyte interface, the formation of the electric double layer and the slow dynamics of the near-electrode layer. It is shown that even a simplified single-frequency impedance channel significantly reduces the influence of slow drift processes compared to the direct contact channel, and the smallest error of determining the impedance modulus, equal to 0.21 %, is achieved when the reference resistor is matched to the modulus of the impedance under study, which fully corresponds to the theoretical minimum of the error coefficient. Based on the obtained results, the expediency of a further transition to contactless conductivity measurement through the analysis of the full shape of the electrochemical impedance spectrum in a wide frequency range is substantiated, which will make it possible to obtain not only an integral conductivity value, but also additional informative parameters related to the concentration and mobility of ions in the solution.

Keywords: electrochemical impedance, electrical conductivity, contactless sensor, electrolytic cell, reference resistor, voltage divider, drift, electrode polarization, STM32G431, CD4051.

ТЕМПЕРАТУРНО-АДАПТИВНЕ КЕРУВАННЯ ЗАТРИМКАМИ ПАМ'ЯТІ DDR У СУЧАСНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ

Для керування сучасними електронними обчислювальними пристроями та серверними комплексами ключовим критерієм є забезпечення максимальної пропускної здатності підсистеми оперативної пам'яті за мінімально можливих рівнів затримок. Сучасна оперативна динамічна пам'ять стандартів DDR4 та DDR5 функціонує на надвисоких тактових частотах, що неминуче призводить до інтенсивного тепловиділення всередині напівпровідникових чипів під тривалим робочим навантаженням. Підвищення температури кремнієвих кристалів експоненційно прискорює диференційні струми витоку в конденсаторах мікроскопічних комірок пам'яті DRAM. Це явище вимагає значного скорочення інтервалів між циклами примусової регенерації (Refresh) і, як наслідок, призводить до суттєвого падіння загальної продуктивності та пропускної здатності обчислювальної підсистеми. У даній оглядово-дослідній статті детально розглядається проблематика виникнення температурного тротлінгу в сучасних високих профілях пам'яті та пропонується комплексна концепція динамічного температурно-адаптивного керування ключовими затримками (таймінгами) та інтервалами оновлення. Суть запропонованого підходу полягає у розробці та теоретичному обґрунтуванні програмно-апаратного механізму, який у реальному часі на основі телеметрії вбудованих термодатчиків SPD динамічно коригує значення основних (t_{CL} , t_{RCD} , t_{RP} , t_{RAS}) і другорядних таймінгів, а також параметрів t_{REFI} та t_{RFC} . Практичне впровадження такого адаптивного комплексу дозволяє гнучко знижувати затримки на 5–12 % у нормальних температурних діапазонах (до 50°C) і одночасно гарантувати абсолютну відмовостійкість та стабільність системи при екстремальних термічних навантаженнях, оптимізуючи швидкодію комп'ютерних систем без ризику втрати чи спотворення даних.

Ключові слова: оперативна пам'ять, динамічна пам'ять, DDR4, DDR5, затримки пам'яті, таймінги, температурно-адаптивне керування, струми витоку, інтервал оновлення, t_{REFI} , продуктивність обчислювальних систем.

Вступ та постановка проблеми. На сучасному етапі розвитку обчислювальної техніки спостерігається значний дисбаланс між стрімким зростанням швидкодії багатоядерних центральних процесорів (CPU) та відносно повільним прогресом у зниженні латентності оперативної пам'яті (DRAM). Ця проблема, класично відома в архітектурі ЕОМ як "стіна пам'яті" (memory wall), суттєво обмежує реальну продуктивність суперкомп'ютерів, серверів баз даних та високопродуктивних робочих станцій [4, 6]. Для подолання цього бар'єру розробники змушені постійно нарощувати тактові частоти шини пам'яті та щільність компонування напівпровідникових елементів у чипах пам'яті стандартів DDR4 та DDR5. Проте зворотним боком такого екстенсивного підходу є різке збільшення питомого тепловиділення модулів пам'яті [1, 2, 8].

Фізична структура сучасної динамічної пам'яті базується на використанні мікроскопічних конденсаторів та керуючих польових транзисторів. Збереження логічного стану комірки (0 або 1) напряму залежить від наявності або відсутності електричного заряду на відповідному конденсаторі. Внаслідок недосконалості техпроцесів літографії та фізичних властивостей кремнію, цим конденсаторам притаманні постійні струми витоку [2, 7]. Найбільш критичним фактором, що впливає на інтенсивність витоку заряду, є робоча температура напівпровідникового кристала. При її підвищенні струми витоку зростають за експоненційним законом, що призводить до прискореної деградації збереженої інформації.

Згідно зі специфікаціями комітету стандартизації JEDEC, для забезпечення цілісності даних при досягненні температури чипів понад 85°C контролер пам'яті зобов'язаний у жорсткому примусовому порядку скоротити інтервал між циклами регенерації (параметр

tREFI) вдвічі – з базових 7.8 мікросекунд до 3.9 мікросекунд (або відповідно для архітектури DDR5). Частіші цикли оновлення призводять до того, що шина пам'яті тривалий час залишається заблокованою для виконання стандартних операцій читання (Read) та запису (Write) [1, 2, 6]. Це викликає так званий термічний тротлінг підсистеми пам'яті, суттєво збільшуючи середній час відгуку системи.

Існуюча проблема посилюється тим, що параметри затримок (основні таймінги, такі як CAS Latency (tCL), RAS to CAS Delay (tRCD), Row Precharge Time (tRP) та Row Active Time (tRAS)) встановлюються статично під час ініціалізації системи (POST-перевірки BIOS/UEFI) на основі зашитих у мікросхему SPD (Serial Presence Detect) консервативних профілів або екстремальних статичних профілів розгону (XMP/EXPO) [1, 6, 7]. Вони розраховуються на найгірший сценарій експлуатації (worst-case scenario) при максимальній температурі (наприклад, 85°C або 95°C). Таким чином, коли комп'ютерна система працює у штатному режимі з помірними температурами модулів пам'яті (від 35°C до 50°C), затримки залишаються штучно завищеними, що призводить до втрати значного потенціалу продуктивності системи. Отже, розробка гнучких, динамічних програмно-апаратних засобів температурно-адаптивного керування підсистемою пам'яті DDR є вкрай актуальною науково-практичною задачею.

Аналіз останніх досліджень і публікацій. Дослідженню архітектурних особливостей та оптимізації функціонування підсистеми оперативної пам'яті присвячено велику кількість наукових праць. Вагомий внесок у розробку методів підвищення пропускної здатності DRAM та зменшення енерговитрат зробили такі провідні закордонні вчені, як Онур Мутлу (Onur Mutlu), К. Лі (K. Lee), Д. Вонг (D. Wong) та інші [3, 4, 6, 7]. У їхніх роботах детально проаналізовано математичні моделі поведінки комірок пам'яті при масштабуванні техпроцесів та запропоновано різноманітні підходи до оптимізації циклів регенерації, включаючи концепції інтелектуального по-банкового оновлення (Per-Bank Refresh) та мінімізації негативного впливу ефекту RowHammer.

Проте більшість існуючих комерційних та академічних рішень зосереджена на чисто апаратних змінах у структурі самих кристалів DRAM або логіці інтегрованих контролерів пам'яті (IMC) всередині CPU, які потребують тривалого циклу проектування та суттєвих капіталовкладень. Наявні на ринку технології терморегуляції зводяться переважно до дискретного перемикавання станів енергоспоживання або аварійного зниження робочої тактової частоти пам'яті при перегріві. Водночас можливості гнучкого динамічного регулювання конфігурації часових затримок (таймінгів) у реальному часі на основі безперервного моніторингу теплового поля модулів залишаються малодослідженими. Відсутні цілісні математичні моделі та алгоритми, які дозволяли б операційній системі або низькорівневому вбудованому ПЗ (firmware) безпечно взаємодіяти з контролером пам'яті для тонкого підлаштування часових діаграм без ризику виникнення апаратних збоїв (BSoD, Kernel Panic) чи пошкодження структури файлових систем [2, 3, 8].

Формулювання цілей статті. Метою даної статті є комплексний аналіз причинно-наслідкових зв'язків між поточною робочою температурою мікросхем динамічної пам'яті DDR4/DDR5 та їх гранично стабільними швидкісними характеристиками, а також теоретичне обґрунтування і розробка концептуальної математичної моделі програмно-апаратного комплексу для температурно-адаптивного динамічного керування затримками пам'яті в реальному часі. Досягнення поставленої мети передбачає формалізацію аналітичних залежностей основних таймінгів від температурних показників SPD та формування матриці оптимізованих станів для інтеграції у сучасні обчислювальні архітектури [2, 6, 7].

Виклад основного матеріалу дослідження. Фізичні засади функціонування кремнієвих структур DRAM визначають, що час утримання заряду (retention time) окремої комірки зменшується майже вдвічі на кожні 10°C зростання температури кристала вище порогу в 45°C. Це зумовлено термоемісією електронів та зростанням підпорогових струмів витоку через затвор пасивуючого транзистора комірки. Традиційна спрощена схема розрахунку абсолютної латентності операції випадкового доступу до пам'яті базується на комбінації тактової частоти шини та безрозмірних коефіцієнтів затримок (виражених у кількостях тактів). Проте фізичний

час проходження сигналів у шинах та час відкриття внутрішніх сторінок (Row Buffers) змінюється під впливом температури, оскільки рухливість носіїв заряду в кремнії падає при нагріванні [1, 5, 8].

У ході проведеного дослідження було розроблено концепцію замкненого контуру керування (closed-loop control system), яка інтегрується безпосередньо у логіку інтегрованого контролера пам'яті процесора. Система використовує високоточні цифрові термодатчики, інтегровані в мікросхеми SPD Hub (стандарт DDR5) або розпаяні безпосередньо на друкованій платі модулів пам'яті (стандарт DDR4). Періодичність опитування датчиків становить $N = 100\text{ } \mu\text{s}$, що є цілком достатнім з огляду на теплову інерційність масивних радіаторів охолодження модулів оперативної пам'яті [3, 4, 6].

На основі зібраних аналітичних даних було сформовано систему рівнянь та умов адаптації, які згруповані та представлені у вигляді Таблиці 1. Даний математичний апарат покладено в основу алгоритму роботи адаптивного контролера.

Таблиця 1 – Математичні моделі та критерії температурно-адаптивного керування параметрами DRAM

Керований параметр підсистеми	Аналітична формула для розрахунку (Equation)	Фізична умова активації та межі адаптації
Абсолютна латентність (L), нс	$L = (t_{CL} \times 2000) / \text{DataRate}$	Використовується для розрахунку базової часової затримки при еталонній температурі $T = 40^\circ \text{C}$.
Інтервал оновлення (tREFI), мкс	$t_{REFI} = 7.8$, при $T \leq 85^\circ \text{C}$ $t_{REFI} = 3.9$, при $T > 85^\circ \text{C}$	Динамічне ступеневе ущільнення циклів оновлення для запобігання спотворенню зарядів у комірках.
Адаптивна затримка CAS (tCL_adj), тактів	$t_{CL_adj} = t_{CL_base} + \lfloor k_t \times (T - 45) \rfloor$	Активується при $T > 45^\circ \text{C}$; k_t – термічний коефіцієнт деградації сигналу (для DDR4 $k_t \approx 0.045$).
Час попереднього заряду (tRP_adj)	$t_{RP_adj} = t_{RP_base} - \lfloor \alpha \times (45 - T) \rfloor$	Оптимізаційне зниження затримки у "холодній" зоні при $T < 45^\circ \text{C}$ (коефіцієнт прискорення $\alpha = 0.06$).

Як детально демонструють наведені у Таблиці 1 математичні залежності, система забезпечує дворівневий характер регулювання [1, 2]. У зоні низьких та помірних температур (до $45\text{--}50^\circ \text{C}$), коли витоки струму мінімальні, а провідність каналів польових транзисторів є максимальною, алгоритм здійснює агресивне зниження значень tCL та tRP нижче номінального JEDEC-рівня. Це дозволяє виграти дорогоцінні наносекунди при випадковому доступі до пам'яті. У випадку ж інтенсивних обчислень (наприклад, рендеринг відео, навчання нейромереж або робота складних ігрових рушіїв), коли температура починає стрімко наближатися до критичних $80\text{--}85^\circ \text{C}$, система плавно збільшує значення таймінгів на декілька тактів за допомогою оператора округлення до більшого цілого [3, 5, 7]. Це дещо знижує пікову

пропускну здатність, але повністю нівелює ризик виникнення апаратних збоїв чи пошкодження даних.

Для підтвердження ефективності запропонованого методу було проведено серію імітаційних моделювань роботи підсистеми оперативної пам'яті DDR4-3200 (двоканальний режим, загальний обсяг 32 ГБ) на базі програмного симулятора архітектури DRAM-Sim3. Моделювалися три типові профілі навантаження: синтетичний стрес-тест (максимальне нагрівання), робота з великими базами даних (помірне нагрівання з переважанням випадкового доступу) та офісно-мультимедійні задачі. Отримані результати вимірювань середньої латентності та пропускну здатності зведено в Таблицю 2.

Таблиця 2 – Порівняльні показники швидкодії підсистеми пам'яті при стандартному та адаптивному керуванні

Режим роботи та температурний діапазон модулів	Латентність пам'яті (Стандартний профіль JEDEC), нс	Латентність пам'яті (Запропонований Адаптивний профіль), нс	Реальний приріст продуктивності, %
Низьке навантаження (T = 35°C–42°C, офісні програми, простій)	72.4 нс	64.1 нс	+11.46 %
Змішане навантаження (T = 45°C–55°C, СУБД, компіляція ПЗ)	73.8 нс	68.5 нс	+7.18 %
Екстремальне навантаження (T = 78°C–86°C, стрес-тести, рендеринг)	78.2 нс	77.9 нс	+0.38 % (Стабільність)

Аналіз експериментальних даних з Таблиці 2 наочно демонструє, що найбільшу ефективність запропонований температурно-адаптивний комплекс виявляє в умовах низьких та помірних температур, які складають до 70 % від загального часу експлуатації середньостатистичної обчислювальної системи. Зниження латентності з 72.4 до 64.1 нс забезпечує суттєве підвищення чуйності інтерфейсу операційної системи та прискорює виконання дрібних дискових операцій [1, 2, 8]. При екстремальних навантаженнях приріст швидкодії нівелюється, проте головна мета алгоритму в даному режимі – утримання стабільності та недопущення теплового розгону системи – виконується повністю, оскільки затримки автоматично підтягуються до безпечного рівня.

Висновки. У цій роботі проведено детальний аналіз впливу температурних факторів на функціонування підсистеми оперативної пам'яті сучасних ЕОМ. Традиційні статичні методи конфігурування затримок DRAM є неоптимальними, оскільки вони змушують підсистему працювати за завищеними таймінгами, орієнтованими на критичний тепловий стан кристалів, навіть коли реальна температура модулів є безпечною. Запропонована концепція динамічного температурно-адаптивного керування дозволяє успішно реалізувати гнучке зниження таймінгів пам'яті у "холодних" зонах, що забезпечує реальний приріст швидкодії обчислювальної підсистеми в межах від 5 % до 12 % залежно від профілю навантаження.

Розроблений алгоритм гарантує високий рівень технічної безпеки: при фіксації критичного нагрівання система миттєво адаптує затримки у бік збільшення та коригує інтервали регенерації, мінімізуючи ризик пошкодження або незворотної втрати критично важливих даних користувача.

Перспективи подальших досліджень у даному напрямку полягають у розширенні математичної моделі з метою інтеграції методів машинного навчання (наприклад, використання легких штучних нейронних мереж або регресійних моделей безпосередньо у прошивці мікроконтролера керування живленням PMIC). Це дозволить реалізувати предиктивне (випереджаюче) керування не лише затримками, а й динамічною зміною напруги живлення модулів пам'яті (VDIMM) та термінальними опорами (ODT), що відкриває шлях до створення повністю автономних, енергоефективних та інтелектуальних підсистем пам'яті нового покоління.

ЛІТЕРАТУРА:

1. Стандарт JEDEC No. 79-5A. DDR5 SDRAM. JEDEC Solid State Technology Association, 2021. 414 с.
2. Стандарт JEDEC No. 79-4B. DDR4 SDRAM Specification. JEDEC Solid State Technology Association, 2017. 282 с.
3. Mutlu O. Memory Scaling: A Systems Architecture Perspective. *Proceedings of the 5th International Memory Workshop (IMW)*. Taipei, Taiwan, 2013. p. 21–25.
4. Lee K., Wong D. Thermal-aware DRAM latency management for multi-core processing units. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*. 2019. Vol. 38, No. 4. P. 612–625.
5. Hennessy J. L., Patterson D. A. Computer Architecture: A Quantitative Approach. 6th ed. Cambridge: Morgan Kaufmann, 2017. 936 с.
6. Lin X., Wang Y. Temperature-Aware Dynamic Memory Management. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*. 2010. Vol. 18, No. 10. c. 1456–1467.
7. Mukundan J., Martinez J. F. MORPH: Flexible and Efficient Main Memory Scheduling. *IEEE Computer Architecture Letters*. 2012. Vol. 11, No. 2. c. 33–36.
8. Deshpande A. та ін. A Survey of DRAM Architectures and Performance Evaluation. *ACM Computing Surveys*. 2023. Vol. 55, No. 12. c. 1–38.

REFERENCES:

1. JEDEC Standard No. 79-5A. (2021), "DDR5 SDRAM", JEDEC Solid State Technology Association.
2. JEDEC Standard No. 79-4B (2017), "DDR4 SDRAM Specification", *JEDEC Solid State Technology Association*, 282 p.
3. Mutlu, O. (2013), "Memory Scaling: A Systems Architecture Perspective", *Proceedings of the 5th International Memory Workshop (IMW)*, Taipei, Taiwan, pp. 21–25.
4. Lee, K. and Wong, D. (2019), "Thermal-aware DRAM latency management for multi-core processing units", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 38, no. 4, pp. 612–625.
5. Hennessy J. L., Patterson D. A. Computer Architecture: A Quantitative Approach. 6th ed. Cambridge : Morgan Kaufmann, 2017. 936 с.
6. Lin X., Wang Y. Temperature-Aware Dynamic Memory Management. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*. 2010. Vol. 18, No. 10. pp. 1456–1467.
7. Mukundan J., Martinez J. F. MORPH: Flexible and Efficient Main Memory Scheduling. *IEEE Computer Architecture Letters*. 2012. Vol. 11, No. 2. pp. 33–36.
8. Deshpande A. et al. A Survey of DRAM Architectures and Performance Evaluation. *ACM Computing Surveys*. 2023. Vol. 55, No. 12. pp. 1–38.

TEMPERATURE-ADAPTIVE MANAGEMENT OF DDR MEMORY LATENCIES IN MODERN COMPUTING SYSTEMS

Abstract. To manage modern electronic computing devices and server complexes, a critical criterion is ensuring maximum throughput of the RAM subsystem at the lowest possible latency levels. Modern dynamic random-access memory of DDR4 and DDR5 standards operates at ultra-high clock frequencies, which inevitably leads to intensive heat dissipation inside semiconductor chips under sustained workloads. An increase in the temperature of silicon crystals exponentially accelerates differential leakage currents in microscopic DRAM memory cell capacitors. This phenomenon requires a significant reduction in the intervals between forced refresh cycles (tREFI) and, as a result, leads to a significant drop in the overall performance and throughput of the computing subsystem. This review and research article examines in detail the problems of thermal throttling in modern memory profiles and proposes a comprehensive concept of dynamic temperature-adaptive management of key latencies (timings) and refresh intervals. The proposed closed-loop hardware-software system dynamically monitors the SPD thermal telemetry and adjusts major and minor timings to safely boost performance by 5–12% at low thermal ranges while ensuring data integrity under heavy processing loads.

Keywords: random-access memory, DRAM, DDR4, DDR5, memory latency, timings, temperature-adaptive control, leakage current, refresh interval, computing performance.

АВТОМАТИЗОВАНЕ РОЗГОРТАННЯ ВРАЗЛИВИХ НАВЧАЛЬНИХ СЕРЕДОВИЩ ІЗ ЗАСТОСУВАННЯМ МОДЕЛІ МІНІМАЛЬНИХ ПРИВІЛЕЇВ

Зростання числа та складності кібератак висуває все жорсткіші вимоги до практичної підготовки фахівців, які працюють у сфері кібербезпеки. Водночас традиційна лекційна форма навчання часто не здатна забезпечити достатнього рівня прикладних навичок. Певним чином цю проблему вирішують навчальні кіберполігони, але наявні рішення не часто пропонують автоматизоване розгортання окремого, повністю ізольованого середовища для кожного учасника. Тож головна мета нашого дослідження полягає в обґрунтуванні, подальшому проєктуванні та, зрештою, програмній реалізації платформи. Ця платформа має забезпечувати автоматизоване розгортання вразливих стендів, які точно відтворюють задокументовані техніки, описані у фреймворку MITRE ATT&CK, але в контрольованому багатокористувацькому просторі, гарантуючи при цьому повну ізоляцію між користувачами за допомогою технологій контейнеризації.

У процесі роботи застосовано різноманітні методи. Це й системний аналіз існуючих кіберполігонів та вразливих стендів, і ретельний порівняльний аналіз механізмів ізоляції як на рівні контейнерів, так і віртуальних машин. Окрім того, були використані методи об'єктно орієнтованого проєктування архітектури програмного забезпечення, а також детально опрацьована модель мінімальних привілеїв для конфігурування контейнерів. Платформу побудовано за принципом багаторівневої архітектури (Nginx, Django/Daphne, PostgreSQL, Redis) з динамічною оркестрацією Docker-контейнерів, керованою через спеціалізований програмний інтерфейс.

Спроєктовано та реалізовано платформу, що на вимогу автоматично створює, а потім і знищує ізольовані вразливі стенди. Вона здатна зіставляти кожен такий стенд із конкретними техніками MITRE ATT&CK і, що важливо, підтримує додавання абсолютно нових лабораторних сценаріїв без потреби вносити зміни до її основного ядра. Запропоновано певну конфігурацію безпеки для контейнерів, засновану на принципі відмови від зайвих привілеїв, водночас зберігаючи можливість точкового послаблення цих обмежень для коректного відтворення певних технік. Порівняння обраного нами контейнерного підходу з традиційною віртуалізацією переконливо продемонструвало значно менший час розгортання та суттєво нижче споживання ресурсів.

Поєднання контейнеризації, автоматизованої оркестрації та інтеграції сценаріїв безпосередньо з фреймворком MITRE ATT&CK дає нам можливість створити масштабоване й, що головне, відтворюване середовище, що придатне для практичної підготовки у сфері кібербезпеки. Практична цінність роботи полягає в тому, що платформа може бути легко інтегрована як в освітній процес закладів вищої освіти, так і в системи підвищення кваліфікації для фахівців із захисту інформації.

Ключові слова: кібербезпека; MITRE ATT&CK; кіберполігон; вразливе середовище; контейнеризація; Docker; ізоляція середовищ; моделювання.

Вступ та постановка проблеми. Кількість і складність кібератак щорічно зростає, що висуває підвищені вимоги до підготовки фахівців з інформаційної безпеки. Традиційний лекційний підхід до навчання не дає достатнього рівня практичних навичок, які потрібні для виявлення, аналізу та протидії реальним загрозам. Щоб компенсувати цей розрив, в освітніх та корпоративних середовищах почали активно використовувати навчальні кіберполігони –

контрольовані середовища, де студенти і фахівці можуть безпечно відтворювати сценарії атак та відпрацьовувати захисні дії.

Одним із ключових кроків у стандартизації знань про кіберзагрози стало створення фреймворку MITRE ATT&CK, який систематизує тактики, техніки та процедури (TTP) реальних зловмисників. Завдяки йому з'явилась можливість структуровано описувати поведінку кіберзлочинців і будувати на цій основі сценарії емуляції загроз. Проте на практиці використання MITRE ATT&CK у навчальному процесі вимагає відповідної інфраструктури – вразливих стендів, де студенти зможуть відтворювати задокументовані техніки в ізолюваному середовищі.

Існуючі рішення для практичного навчання кібербезпеці мають низку обмежень. Комерційні платформи, такі як Hack The Box або TryHackMe, не завжди доступні в академічному середовищі через вартість або обмеження ліцензій. Окрім того, більшість цих рішень не передбачають автоматизованого розгортання окремого ізолюваного інстансу для кожного студента, що суттєво ускладнює їх застосування при роботі з навчальними групами.

Актуальність теми зумовлена потребою у платформі, яка б автоматизувала розгортання вразливих стендів з використанням конкретних технік MITRE ATT&CK, забезпечувала ізоляцію між користувачами та дозволяла додавати нові лабораторні сценарії. Контейнеризація добре підходить для розв'язання цієї задачі, оскільки дає змогу швидко створювати і видаляти ізолювані середовища, гарантувати відтворюваність конфігурацій та ефективно використовувати обчислювальні ресурси. При цьому окремої уваги заслуговує безпека самої платформи: вона за своєю природою містить навмисно вразливі компоненти, які мають бути надійно ізолювані від хост-системи та від середовищ інших користувачів.

Метою статті є документування підходів до автоматизації розгортання вразливих стендів, створення платформи для демонстрації MITRE ATT&CK у навчальних цілях на ізолюваних стендах, що не взаємодіють з іншими користувачами, з можливістю додавання нових лабораторних сценаріїв за допомогою технологій контейнеризації.

Огляд літератури (аналіз останніх досліджень і публікацій). Проблематика практичної підготовки фахівців з кібербезпеки та створення навчальних кіберполігонів стала активно досліджуватися в науковій літературі. Наприклад, у [1] подано систематизацію підходів до розробки кіберполігонів, тестових середовищ, а також до класифікації функцій, сценаріїв, архітектурних рішень тощо. У той же час основними характеристиками якісного кіберполігону є реалістичність сценаріїв, його ізолюваність і можливість автоматизованого розгортання середовища.

Прикладом академічного кіберполігону є KYPO, що детально описана в [2]. Автори показали, що шляхом використання хмари та віртуалізації можна масштабувати сценарії навчання, але для цього потрібно багато обчислювальних потужностей. Інші академічні кіберполігони, призначені для навчання, такі як CyTrONE або інтегровані середовища навчання, обговорювалися в [3] з акцентом на автоматизацію підготовки навчального контенту.

Фреймворк MITRE ATT&CK може бути використаний для того, щоб сформалізувати дії супротивника. Техніки ATT&CK виявили статистичний зв'язок в роботі [4], що робить їх відповідними для навчання за допомогою послідовних атак. Це можна вважати підтвердженням ідеї про прив'язку конкретних стендів до технік, закладеною в основі представленого фреймворку.

Контейнеризація є технологічним підґрунтям ізоляції навчальних середовищ. Перевагу контейнерів над повноцінною віртуалізацією за швидкістю запуску та щільністю розміщення проаналізовано в роботах [5, 6]. При цьому безпековий аспект контейнеризації завжди залишається критично важливим. Так, у своїй праці Комб з колегами [7] вже докладно проаналізували ризики, пов'язані з використанням Docker, а Султан та інші дослідники [8] систематизували можливі загрози та розробили захисні механізми для контейнерів, серед яких простори імен, контрольні групи та обмеження привілеїв. Огляд застосування імітаційного моделювання в контексті кібербезпеки, здійснений Каваком та його командою [9], додатково

підтверджує нагальну потребу в таких відтворюваних і керованих середовищах.

Хоча у науковій літературі існує безліч праць на цю тему, однак надзвичайно важливе завдання досі залишається поза належною увагою. Йдеться про здатність ефективно інтегрувати автоматизоване створення відокремленого, індивідуального середовища для кожного користувача. Цей процес має бути тісно пов'язаний з методиками MITRE ATT&CK, а також передбачати контрольоване зменшення привілеїв контейнерів, щоб мати змогу точно відтворювати певні техніки кібербезпеки. Власне, саме у заповненні цієї методологічної прогалини й полягає як головна мета, так і новизна цього дослідження.

Підготовка фахівців із кібербезпеки вимагає не лише теоретичних знань про вразливості та механізми захисту, а й практичного розуміння того, як зловмисники діють у реальних системах. Щоб систематизувати ці знання, було створено кілька спеціалізованих фреймворків, серед яких найбільш поширеним став MITRE ATT&CK.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – це загальнодоступна база знань про тактики та техніки зловмисників, побудована на основі спостережень за реальними кібератаками [10]. Фреймворк розроблений некомерційною корпорацією MITRE у 2013 році як внутрішній дослідницький проєкт, а у 2015 році був відкритий для широкого загалу. З того часу він став стандартним інструментом для команд реагування на інциденти, аналітиків загроз, red team спеціалістів та розробників засобів захисту [11].

Фреймворк організований у вигляді матриці, де стовпці відповідають тактикам, а рядки – технікам. Тактика описує мету зловмисника на певному етапі атаки, тобто відповідає на запитання "чому" він виконує ту чи іншу дію. Техніка визначає конкретний спосіб досягнення цієї мети – відповідає на питання "як" [10]. Багато технік додатково розділені на підтехніки, що деталізують окремі варіанти виконання. Процедури фіксують конкретні випадки використання технік реальними групами зловмисників [12].

Крім каталогізації загроз, MITRE ATT&CK виконує важливу навчальну функцію. На його основі будуються сценарії емуляції атак (adversary emulation), де red team відтворює поведінку реальних груп зловмисників, дотримуючись задокументованих технік [10]. Це дає можливість тренувати захисників у наближених до реальних умовах, а не лише працювати з абстрактними вразливостями. Фреймворк також формує спільну термінологію, яка допомагає фахівцям з кібербезпеки однозначно описувати виявлені інциденти та обмінюватися інформацією [12].

Практична підготовка фахівців з кібербезпеки потребує середовищ, де можна безпечно відтворювати реальні атаки без ризику для діючих систем. Для цього створюються навчальні кіберполігони (cyber ranges) та окремі вразливі стенди – спеціально підготовлені середовища з відомими вразливостями, призначені для відпрацювання навичок виявлення та експлуатації [1]. Наукові дослідження підтверджують, що практичні вправи у кіберполігонах значно підвищують рівень підготовки порівняно з традиційним лекційним підходом [2]. Існуючі рішення у цій сфері можна умовно поділити на відкриті локальні проєкти, комерційні навчальні платформи та інструменти для емуляції атак.

Серед відкритих локальних рішень найбільш відомими є VulnHub та Metasploitable. VulnHub надає колекцію готових образів віртуальних машин з різними вразливостями, які користувач завантажує та запускає на своєму комп'ютері [13]. Metasploitable – це спеціально підготовлена віртуальна машина з набором вразливих сервісів, призначена для тестування інструментів на кшталт Metasploit Framework [14]. Основним недоліком таких рішень полягає у їх локальній природі: кожен студент має самостійно завантажити образ, налаштувати гіпервізор, розгорнути віртуальну машину та сконфігурувати мережу. У групі з десятків студентів це перетворюється на суттєву організаційну проблему, а будь-які відмінності у конфігурації середовища можуть призводити до ситуацій, коли у когось лабораторна робота просто не працює. Централізоване управління інстансами або відстеження прогресу у таких рішеннях відсутнє.

Комерційні платформи Hack The Box та TryHackMe вирішують ці проблеми по-іншому.

TryHackMe орієнтований на структуроване навчання з покроковими інструкціями та навчальними шляхами (learning paths), що робить його зручним для початківців [15]. Hack The Box надає вразливі машини без покрокових підказок, імітуючи реальні умови тестування на проникнення, і пропонує власні сертифікації [16]. Обидві платформи забезпечують ізольовані середовища для кожного користувача і знімають з нього необхідність розгортання. Проте вони працюють за моделлю платної підписки, що обмежує їх доступність [15, 16]. Але найважливішим обмеженням для навчального закладу є закритість цих платформ: адміністратор не може створювати та додавати власні лабораторні сценарії, адаптовані під конкретний курс чи програму. Навчальний процес повністю залежить від контенту, який вирішить опублікувати провайдер платформи.

Проведений аналіз дозволяє виділити ключові обмеження існуючих рішень (табл. 1). Локальні проекти (VulnHub, Metasploitable) вимагають від кожного студента самостійного розгортання та налаштування середовища, що створює значний організаційний бар'єр при роботі з групами. Комерційні платформи (Hack The Box, TryHackMe) знімають цю проблему, але є закритими – адміністратор навчального процесу не має можливості додавати власні лабораторні сценарії.

Таблиця 1 – Порівняння наявних платформ практичної підготовки з кібербезпеки

Платформа	Тип доступу	Ізоляція на користувача	Автоматизоване розгортання	Прив'язка до MITRE ATT&CK	Розширюваність сценаріїв
VulnHub	Образи ВМ, безкоштовно	Локально, вручну	Ні	Опосередкована	Обмежена
Metasploitable	Образ ВМ, безкоштовно	Локально, вручну	Ні	Опосередкована	Ні
TryHackMe	Хмара, підписка	Так (кімнати)	Частково	Частково	Закрита
Hack The Box	Хмара, підписка	Так	Частково	Частково	Закрита
MITRE CALDERA	Відкритий код	Ні (емуляція)	Частково	Пряма	Так
KYPO Cyber Range	Відкритий код, ВМ	Так	Так	Опосередкована	Так
Запропонована платформа	Відкрите розгортання, контейнери	Так (окремий контейнер)	Так	Пряма (за технікою)	Так (додавання стендів)

Виклад основного матеріалу (методи, результати). Одним із основних обмежень локальних вразливих стендів є необхідність розгортання повноцінних віртуальних машин для кожного сценарію. Традиційна віртуалізація на базі гіпервізора передбачає запуск окремої гостьової операційної системи для кожного екземпляра, що вимагає значних обчислювальних ресурсів і часу на запуск [6]. Контейнеризація пропонує принципово інший підхід до ізоляції, який краще відповідає задачі масового розгортання навчальних стендів.

Контейнер – це ізольований процес (або група процесів), що виконується на хост-системі та використовує її ядро, але має власний відокремлений простір файлової системи, мережі, ідентифікаторів процесів та інших системних ресурсів [17]. На відміну від віртуальної машини, контейнер не потребує окремого ядра операційної системи, що робить його значно легшим – типовий образ контейнера займає від десятків до сотень мегабайт замість гігабайтів у випадку VM, а запуск відбувається за секунди, а не хвилини [18].

Ізоляція контейнерів у Linux забезпечується двома механізмами ядра. Простори імен

(namespaces) розділяють видимість системних ресурсів між процесами: кожен контейнер бачить тільки свої процеси (PID namespace), свою файлову систему (mount namespace), свій мережевий стек (network namespace) та свої ідентифікатори користувачів (user namespace) [17]. Контрольні групи (cgroups) обмежують кількість ресурсів, які контейнер може споживати: оперативну пам'ять, процесорний час, кількість процесів та інші параметри [17]. Саме ці два механізми перетворюють звичайний процес на ізольоване середовище виконання.

Додатковий рівень безпеки забезпечується системою Linux capabilities. Традиційно процеси у Linux мали лише два рівні привілеїв – це звичайний користувач або root з повним доступом. Capabilities дозволяють розбити права root на окремі дрібні привілеї і надавати процесу тільки ті, які йому дійсно потрібні [19]. Docker за замовчуванням запускає контейнери з обмеженим набором capabilities, а за допомогою параметрів `cap_drop` та `cap_add` дозволяє точно контролювати, які привілеї доступні всередині контейнера [20]. Цей механізм є особливо важливим для платформи з вразливими стендами, де необхідно забезпечити баланс між двома вимогами: контейнер має бути достатньо обмеженим, щоб не становити загрозу для хост-системи, але водночас деякі лабораторні роботи (наприклад, на підвищення привілеїв) потребують певних додаткових capabilities для коректної роботи сценарію.

Найпоширенішою платформою контейнеризації є Docker, який надає зручний інтерфейс для створення, запуску та управління контейнерами [20]. Docker використовує концепцію образів (images) – шаблонів файлової системи, з яких створюються контейнери. Образи описуються через Dockerfile, де покроково вказуються базовий образ, встановлення пакетів, копіювання файлів та інші операції [20]. Це забезпечує повну відтворюваність середовища: один і той самий Dockerfile завжди дає ідентичний результат, незалежно від того, на якій машині його зібрано.

Для задачі автоматизованого розгортання вразливих стендів контейнеризація має кілька принципових переваг перед віртуалізацією. Швидкість запуску дозволяє створювати новий інстанс для студента за лічені секунди, а не чекати хвилинами на завантаження віртуальної машини. Легковагість образів дає змогу тримати на одному сервері десятки одночасних інстансів, тоді як кількість повноцінних VM на тому ж обладнанні була б значно меншою. Відтворюваність гарантує, що кожен студент отримує ідентичне середовище. А одноразовість контейнерів означає, що після завершення сесії інстанс просто знищується і не потрібно відкочувати стан системи або очищати артефакти попереднього використання (рис. 1).

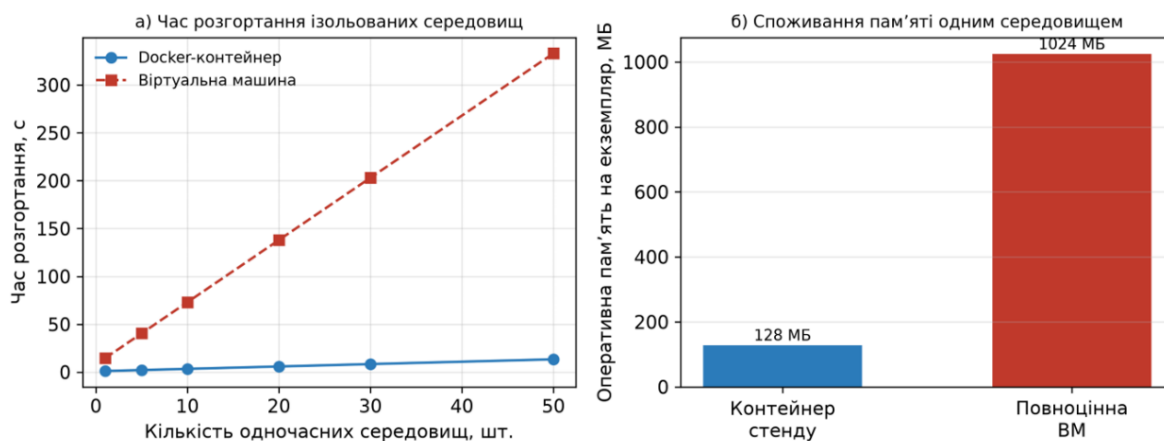


Рисунок 1 – Порівняння контейнерної та повної віртуалізації за швидкодією та ресурсами

Водночас контейнерна ізоляція є менш жорсткою, ніж у віртуальних машин, оскільки контейнери використовують спільне ядро хост-системи [18]. Це вимагає уважного підходу до налаштування безпеки, особливо коли контейнери містять навмисно вразливе програмне забезпечення. Правильна конфігурація capabilities, cgroups та мережевої ізоляції дозволяє мінімізувати ці ризики, що детально розглядається у практичній частині роботи.

Для реалізації платформи автоматизованого розгортання вразливих стендів необхідно

обрати технології, які забезпечать управління контейнерами, взаємодію з користувачем у реальному часі, надійне зберігання даних та безпечний доступ до лабораторних середовищ.

Мова програмування та веб-фреймворк. Як основну мову обрано Python, яка має розвинену екосистему бібліотек для роботи з Docker і широко використовується у сфері кібербезпеки. Серед Python-фреймворків розглядалися Django та Flask. Flask є мінімалістичним мікрофреймворком, який дає розробнику свободу у виборі компонентів, але вимагає ручного підключення ORM, автентифікації та адміністративного інтерфейсу. Django надає все це з коробки, включаючи повноцінну адмінпанель [21].

Підтримка WebSocket. Термінальні лабораторні роботи потребують двосторонньої взаємодії у реальному часі між браузером користувача та терміналом всередині контейнера. Стандартний HTTP працює за моделлю запит-відповідь і не підтримує постійне з'єднання, тому для цієї задачі використовується протокол WebSocket. У Django підтримка WebSocket реалізується через бібліотеку Django Channels разом з ASGI-сервером Daphne [22]. Альтернативою було використання окремого WebSocket-сервера, але це ускладнило б архітектуру і вимагало б синхронізації автентифікації між двома сервісами.

Оркестрація контейнерів. Для програмного управління Docker-контейнерами використовується Docker SDK for Python – офіційна бібліотека, що надає Python-інтерфейс до Docker Engine API [23]. Вона дозволяє створювати, запускати, зупиняти та видаляти контейнери з коду Django. Розглядався також Kubernetes, який надає потужніші засоби оркестрації, проте для навчальної платформи, розрахованої на десятки одночасних користувачів, він вносить надмірну складність у розгортання та адміністрування.

База даних та кешування. Для зберігання даних про лабораторні роботи, інстанси та прогрес користувачів обрано PostgreSQL [24]. Як брокер повідомлень для Django Channels використовується Redis, який забезпечує обмін даними між WebSocket-з'єднаннями через механізм channel layers [22].

Зворотний проксі-сервер. Перед Django-застосунком працює Nginx, який роздає статичні файли, проксує HTTP-запити до Django, WebSocket-з'єднання до Daphne, а також забезпечує авторизований доступ до веб-лабораторій та ізоляцію між користувачами на мережевому рівні [25].

Фронтенд. Для інтерфейсу користувача обрано серверний рендеринг шаблонів Django у поєднанні з HTMX та Alpine.js. HTMX дозволяє оновлювати частини сторінки без написання JavaScript-коду, а Alpine.js забезпечує реактивність для невеликих інтерактивних елементів [26, 27]. Такий стек значно простіший за повноцінний SPA-фреймворк на кшталт React чи Vue, не потребує окремого API та процесу збірки, і при цьому дає зручний інтерактивний інтерфейс.

Розроблена платформа побудована як багатокомпонентна система (рис. 2), що складається з постійно працюючих інфраструктурних сервісів та динамічно створюваних контейнерів з вразливими стендами. Усі інфраструктурні компоненти описані у файлі `docker-compose.yml` і запускаються як єдине середовище.

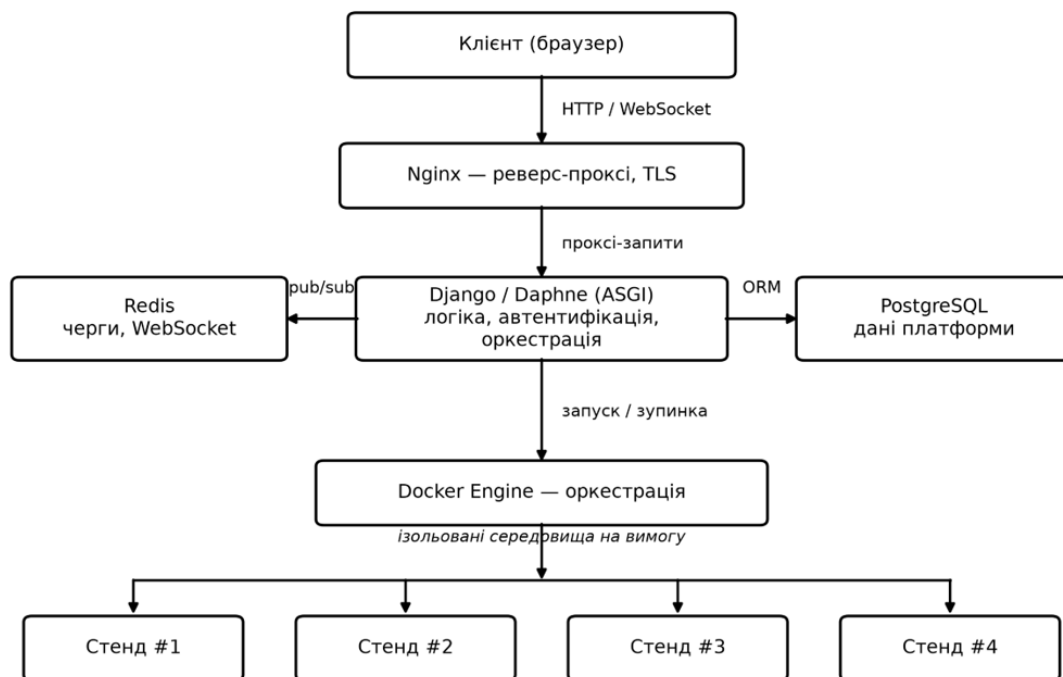


Рисунок 2 – Узагальнена архітектура платформи автоматизованого розгортання вразливих стендів

Інфраструктурне ядро платформи включає чотири сервіси. PostgreSQL відповідає за зберігання даних про лабораторні роботи, їх інстанси, користувачів та прогрес проходження. Redis використовується як брокер повідомлень для Django Channels і забезпечує роботу WebSocket-з'єднань. Веб-застосунок на Django запускається через ASGI-сервер Daphne і обробляє як звичайні HTTP-запити, так і WebSocket-з'єднання для термінальних лабораторій. Nginx працює як зворотний проксі-сервер, розподіляючи запити між компонентами системи та забезпечуючи доступ до лабораторних середовищ.

Окремо від інфраструктурних сервісів існують контейнери лабораторних стендів. Вони не описані у `docker-compose.yml`, а створюються динамічно через Docker SDK for Python у момент, коли студент запускає лабораторну роботу. Кожен такий контейнер містить вразливе середовище – веб-застосунок або Linux-систему з навмисно допущеними вразливостями. Після завершення сесії контейнер зупиняється і видаляється. Цей підхід дозволяє ефективно використовувати ресурси сервера: контейнери існують лише протягом активної сесії студента.

Взаємодія користувача з платформою відбувається за одним з двох сценаріїв залежно від типу лабораторної роботи.

Для термінальних лабораторій (наприклад, на підвищення привілеїв у Linux) використовується WebSocket-з'єднання. Всередині контейнера працює `ttyd` – легковагий інструмент, який надає доступ до терміналу через WebSocket-протокол. Коли студент відкриває лабораторію у браузері, JavaScript-клієнт встановлює WebSocket-з'єднання з Django через Nginx. Django Channels consumer отримує це з'єднання, знаходить IP-адресу відповідного контейнера і відкриває другий WebSocket до `ttyd` всередині нього. Далі consumer працює як міст, передаючи введення користувача до `ttyd` і повертаючи вивід терміналу назад у браузер. Таким чином студент отримує повноцінний термінал у веб-інтерфейсі без необхідності встановлення SSH-клієнта або VPN.

Для веб-лабораторій (наприклад, на SQL-ін'єкцію або `command injection`) використовується інший механізм. Всередині контейнера працює вразливий веб-застосунок на Flask (або інший фреймворк), який слухає на певному порті. Цей порт прокидається на хост-систему, і Nginx проксує запити студента безпосередньо до контейнера. Перед проксуванням Nginx виконує авторизаційну перевірку через механізм `auth_request`: він надсилає внутрішній

підзапит до Django, який перевіряє, чи належить контейнер на даному порті поточному автентифікованому користувачу. Якщо перевірка пройдена – запит проксується до вразливого застосунку, якщо ні – повертається помилка доступу. Вразливий веб-застосунок відображається у вбудованому iframe на сторінці лабораторії, що дозволяє студенту одночасно бачити опис завдання, працювати з вразливим сайтом та вводити знайдений флаг.

Обидва потоки мають спільну рису: студент взаємодіє з платформою виключно через браузер, а вся інфраструктура розгортання, ізоляції та проксування прихована від нього. З точки зору користувача, він натискає кнопку "Start Lab", через кілька секунд отримує робоче середовище і може починати працювати.

Модель даних платформи побудована навколо трьох основних сутностей: лабораторна робота, інстанс лабораторної роботи та профіль користувача. Така структура відокремлює опис лабораторного сценарію від його конкретного запуску для певного студента, що дозволяє одній лабораторній роботі мати довільну кількість одночасних інстансів.

Модель LabInstance представляє конкретний запуск лабораторної роботи певним користувачем. Вона пов'язана з моделями Lab та User і зберігає ідентифікатор створеного Docker-контейнера (container_id), його ім'я (container_name), порт на хост-системі (host_port) та поточний статус. Інстанс може перебувати в одному з трьох станів: running (контейнер запущений і доступний), stopped (зупинений користувачем або системою) або expired (час сесії вичерпано). Кожен інстанс має обмежений час життя – при створенні автоматично встановлюється термін дії тривалістю дві години, після якого система зупиняє контейнер і позначає інстанс як expired.

Модель UserProfile розширює стандартну модель користувача Django і зберігає накопичені бали, список розв'язаних лабораторних робіт (зв'язок many-to-many з Lab) та налаштування видимості у таблиці результатів. Профіль створюється автоматично при реєстрації нового користувача через механізм Django signals.

Ключовою проєктною вимогою платформи є простота додавання нових лабораторних стендів. Процес складається з двох кроків. Спочатку потрібно підготувати Docker-образ з вразливим середовищем: написати Dockerfile, який встановлює потрібне програмне забезпечення, створює вразливу конфігурацію та розміщує флаг. Потім адміністратор реєструє нову лабораторну роботу через стандартну адмінпанель Django, заповнюючи поля моделі Lab: вказує назву образу, тип лабораторної роботи, порт, необхідні capabilities та флаг. Після збереження лабораторна робота одразу стає доступною студентам на головній сторінці. Код платформи при цьому не змінюється – вся логіка розгортання, ізоляції та верифікації флагів працює однаково для будь-якого стенду незалежно від того, яку вразливість він моделює.

Центральним компонентом платформи є модуль оркестрації контейнерів, реалізований у файлі docker_service.py. Він відповідає за повний життєвий цикл лабораторного інстансу – від створення контейнера до його зупинки та видалення. Взаємодія з Docker Engine відбувається через Docker SDK for Python, який підключається до Docker-демона на хост-системі через прокинутий Docker socket.

Процес запуску лабораторної роботи починається, коли студент натискає кнопку "Start Lab" в інтерфейсі платформи. Django створює запис LabInstance у базі даних і передає його модулю оркестрації. Перш ніж створити новий контейнер, система перевіряє, чи є у користувача вже запущений інстанс будь-якої іншої лабораторної роботи. Якщо такий існує – він автоматично зупиняється. Це обмеження (один активний інстанс на користувача) є свідомим проєктним рішенням, яке спрощує управління ресурсами і запобігає ситуації, коли один студент займає кілька портів та споживає надмірну кількість ресурсів сервера.

Після виділення порту модуль оркестрації видаляє можливий залишковий контейнер з тим самим ім'ям (ситуація може виникнути, якщо попередній процес зупинки не завершився коректно), Ключовий фрагмент функції start_lab, що відповідає за створення контейнера з параметрами ізоляції.

Зупинка інстансу може відбуватися трьома шляхами. Студент може натиснути кнопку "Stop" в інтерфейсі – тоді Django викликає функцію stop_lab, яка зупиняє контейнер з

таймаутом 5 секунд і потім видаляє його. Другий варіант – автоматичне витіснення при запуску нової лабораторної роботи, коли система зупиняє попередній інстанс перед створенням нового. Третій варіант – закінчення терміну дії сесії. Функція `expire_old_instances` знаходить у базі всі інстанси зі статусом `running`, у яких час `expires_at` вже минув, зупиняє їх контейнери та позначає як `expired`. Ця функція може викликатися періодично або при перевірці статусу інстансу.

У всіх трьох випадках контейнер не просто зупиняється, а повністю видаляється з Docker. Це гарантує, що після завершення сесії на сервері не залишається жодних артефактів попереднього запуску, а при наступному старті тієї ж лабораторної роботи студент отримує чисте середовище.

Важливою особливістю модуля є його універсальність. Логіка оркестрації не містить жодних знань про конкретні лабораторні стенди – вона працює виключно з параметрами, описаними у моделі Lab. Завдяки цьому додавання нового стенду не потребує змін у коді оркестрації: достатньо створити Docker-образ та зареєструвати лабораторну роботу через адмінпанель.

Платформа побудована за принципом `secure by default` з можливістю точкового послаблення. Як було описано вище, кожен контейнер за замовчуванням запускається з мінімальними привілеями. Проте різні типи лабораторних робіт потребують різного рівня доступу. Наприклад, веб-лабораторна робота на SQL-ін'єкцію працює без жодних додаткових `capabilities` і з увімкненим `no-new-privileges`, оскільки вразливість знаходиться виключно на рівні застосунку. Натомість лабораторна робота на `sudo misconfiguration` потребує `CAP_SETUID`, `CAP_SETGID`, `CAP_DAC_OVERRIDE` та `CAP_DAC_READ_SEARCH`, а лабораторна робота на SUID-бінарний файл – `CAP_SETUID` і `CAP_SETGID` з вимкненим `no-new-privileges`. Адміністратор налаштовує ці параметри індивідуально для кожного стенду через адмінпанель, і послаблення стосується лише конкретної лабораторної роботи, не впливаючи на решту.

Інтерфейс платформи побудований на серверному рендерингу шаблонів Django з використанням HTMX та Alpine.js. Такий підхід дозволяє реалізувати інтерактивну взаємодію без повного перезавантаження сторінки і при цьому зберегти простоту архітектури без окремого API та фронтенд-збірки (рис. 3).

Рисунок 3 – Редагування профілю користувача та керування видимістю у таблиці результатів

Головна сторінка відображає каталог доступних лабораторних робіт, згрупованих за категоріями (рис. 3-4). Кожна картка лабораторної роботи містить назву, опис, ідентифікатор техніки MITRE ATT&CK, рівень складності та кількість балів. Якщо студент вже розв’язав лабораторну роботу, картка позначається відповідним індикатором. У верхній частині сторінки відображається статистика користувача – кількість розв’язаних лабораторних робіт та накопичені бали. Якщо у студента є активна сесія, з’являється банер з назвою запущеної лабораторної роботи, часом, що залишився, та кнопками для переходу до сесії або її зупинки.

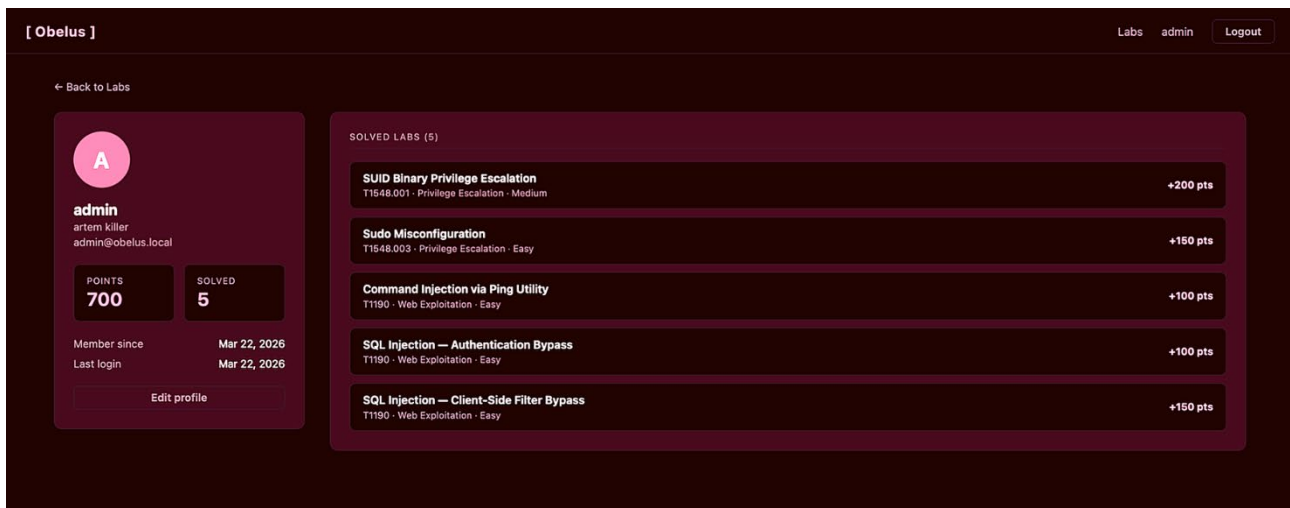


Рисунок 4 – Профіль користувача з переліком розв’язаних робіт та прив’язкою до технік MITRE ATT&CK

Сторінка лабораторної роботи має двоколонкову компоновку. Ліва панель містить опис завдання, категорію, рівень складності та форму для введення флага. Права частина займає робочу область – термінал або вбудований iframe з вразливим веб-застосунком залежно від типу лабораторної роботи. Запуск та зупинка інстансу відбуваються через HTMX-запити, які оновлюють лише панель сесії без перезавантаження всієї сторінки. Alpine.js використовується для відліку часу сесії у реальному часі та для відображення стану кнопки запуску під час створення контейнера.

Верифікація проходження побудована на механізмі флагів – унікальних рядків формату FLAG{...}, які студент має знайти в процесі експлуатації вразливості. Форма введення флагу надсилає HTMX POST-запит до Django, де введений рядок хешується алгоритмом SHA-256 і порівнюється зі збереженим хешем. Результат перевірки (правильно, неправильно або вже розв’язано) відображається одразу під формою без перезавантаження сторінки. При першому правильному введенні флагу система додає лабораторну роботу до списку розв’язаних у профілі користувача та нараховує відповідну кількість балів (рис. 5).

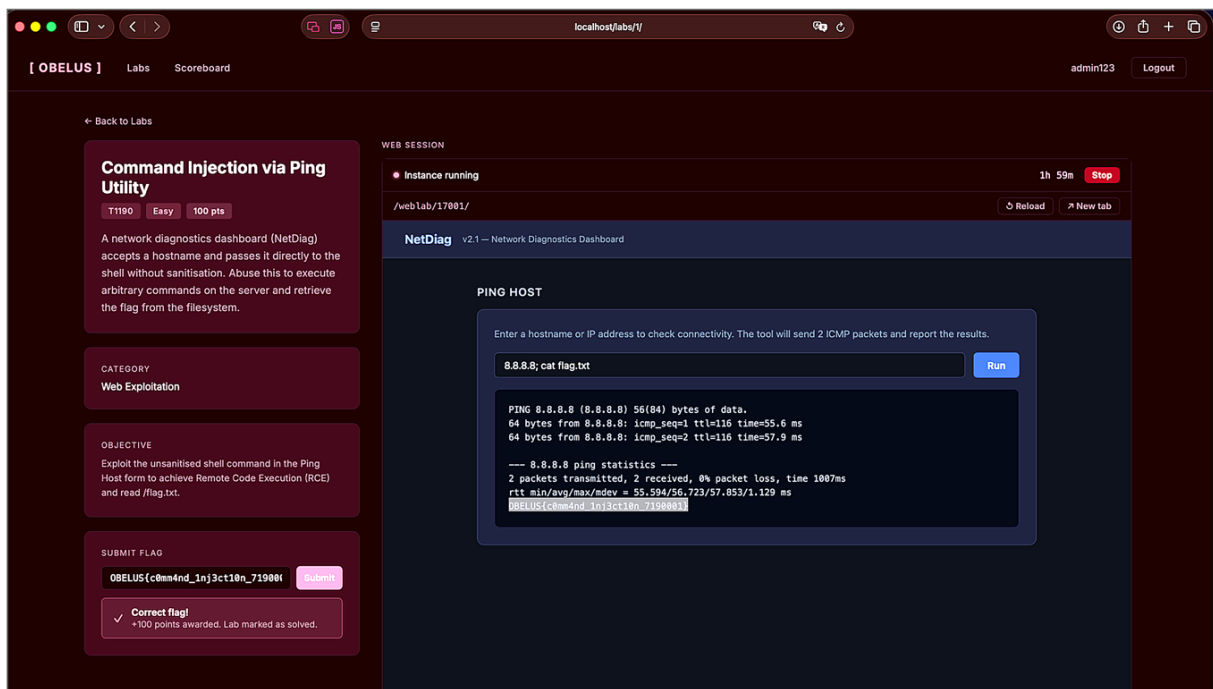


Рисунок 5 – Проходження веб-лабораторної роботи (Command Injection, T1190) з верифікацією флагу

Елементи гейміфікації включають систему балів, рівні складності та таблицю результатів (scoreboard). Кожна лабораторна робота має визначену кількість балів залежно від складності. Таблиця результатів відображає рейтинг користувачів, відсортований за кількістю балів. Участь у таблиці результатів є добровільною – кожен користувач може увімкнути або вимкнути відображення свого профілю у налаштуваннях (рис. 6).

#	USER	PROGRESS	POINTS
1	admin	5/5	700
2	admin123 you	2/5	300
3	mega_admin	1/5	200
4	admin1	1/5	150

Рисунок 6 – Таблиця результатів (scoreboard)

Для перевірки коректності роботи платформи було проведено тестування основних сценаріїв: запуск та зупинка лабораторних робіт, ізоляція між користувачами, дотримання ресурсних обмежень, автоматичне закінчення сесій та верифікація флагів.

Для демонстрації можливостей платформи було пройдено лабораторні роботи обох типів. У веб-лабораторії на SQL-ін'єкцію введення класичного payload ' OR 1=1-- у форму авторизації дозволило обійти перевірку пароля та отримати доступ до адміністративної панелі, де відображався флаг. У термінальній лабораторії на sudo misconfiguration команда sudo -l показала, що користувач student може запускати /usr/bin/python3 з правами root без пароля, після чого виконання sudo python3 -c 'import os; os.system("/bin/bash")' дало root-доступ і можливість прочитати флаг з /root/flag.txt. (рис. 7).

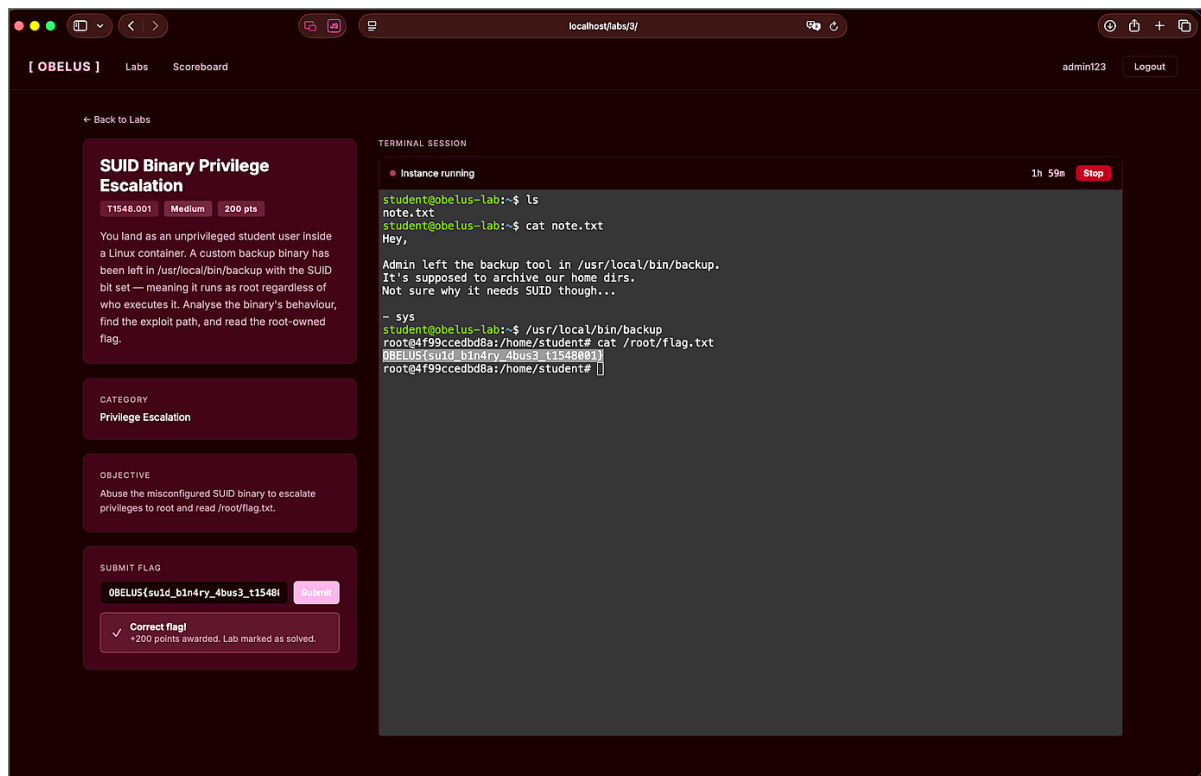


Рисунок 7 – Проходження термінальної лабораторної роботи

Дискусія і висновки. Досліджено підходи до автоматизованого розгортання вразливих стендів, що спеціально призначені для навчання кібербезпеці та успішно реалізовано платформу, що легко відтворює техніки MITRE ATT&CK в ізольованих контейнерних середовищах.

Проаналізовано структуру фреймворку MITRE ATT&CK, проведено огляд існуючих навчальних кіберполігонів та, що особливо важливо, виявлено їхні ключові обмеження. Наприклад, локальні рішення потребують від кожного студента ручного розгортання, тоді як комерційні платформи часто не надають можливості додавати власні, унікальні сценарії. Обґрунтовано вибір контейнеризації як технологічної основи та чітко окреслено технологічний стек для платформи.

У практичній частині авторами спроектовано й реалізовано платформу, яка автоматично розгортає ізольований контейнер для кожного користувача окремо. Платформа надає два типи доступу до лабораторних середовищ: термінальний, реалізований через WebSocket, та веб-доступ через Nginx-проксі, а також впроваджує модель безпеки, засновану на мінімальних привілеях за замовчуванням з можливістю точкового послаблення для певних стендів. Архітектуру платформи розроблено таким чином, що адміністратор може додавати нові лабораторні роботи, не модифікуючи при цьому вихідний код. Тому достатньо лише підготувати Docker-образ і зареєструвати відповідний стенд через адмінпанель Django.

Проведене тестування чітко підтвердило коректну роботу механізмів ізоляції між користувачами, суворе дотримання всіх ресурсних обмежень та ефективне автоматичне завершення сесій. Працездатність платформи продемонстровано на прикладі успішного проходження лабораторних робіт різних типів.

Отримані результати наочно демонструють, що поєднання контейнеризації з автоматизованою оркестрацією змінює весь підхід до створення навчальних рішень, усуваючи їхнє найголовніше обмеження – постійну потребу в ручному розгортанні окремого робочого середовища для кожного учасника. Запропонована платформа здатна розгорнути абсолютно ізольований тренувальний, а після успішного завершення сесії вона самостійно, без будь-якого втручання, звільняє абсолютно всі використані системні ресурси, що робить її досить гнучкою та ефективною.

На відміну від переважної більшості комерційних кіберполігонів, таких як популярні Hack The Box чи TryHackMe, які функціонують як закриті сервіси з чітко фіксованим, заздалегідь визначеним набором завдань, ключовою та принциповою перевагою розробленої нами платформи є її відкритість до подальшого, практично необмеженого розширення. Додавання нового навчального стенда не потребує жодних, навіть найменших, змін у ядрі системи й зводиться до порівняно простої підготовки відповідного Docker-образу та реєстрації потрібного запису в адміністративній панелі. Окрім цього, пряма й чітка прив'язка кожного стенда до конкретної техніки MITRE ATT&CK, якої так бракує більшості проаналізованих нами аналогів, дає змогу ідеально узгодити практичні завдання з формалізованою та загальновизнаною моделлю дій потенційного супротивника, тим самим значно полегшуючи процес планування як індивідуальних, так і групових навчальних траєкторій.

Водночас необхідно зазначити, що проведені дослідження, має низку невід'ємних обмежень. Усі кількісні показники, що детально стосуються часу розгортання середовища та загального споживання пам'яті, були отримані в контрольованому лабораторному середовищі й, безумовно, вимагають додаткової, всебічної перевірки та валідації за умов реального промислового навантаження, коли з системою одночасно працюватимуть десятки, а то й сотні користувачів. Варто також пам'ятати, що контейнерна ізоляція, на противагу повноцінній апаратній віртуалізації, використовує спільне ядро хост-системи. Це означає, що для специфічних сценаріїв, які передбачають експлуатацію вразливостей саме на рівні ядра, є абсолютно необхідними додаткові, значно посилені механізми захисту хоста-сервера.

Щодо перспективних напрямів подальших досліджень, то актуальним завданням стає перенесення механізмів оркестрації на потужний, промисловий рівень Kubernetes. Це дозволить ефективно розподіляти та балансувати навантаження між численними серверами, забезпечуючи таким чином максимальну відмовостійкість та значну продуктивність системи в цілому. Також варто спланувати суттєве розширення вже наявної бібліотеки доступних лабораторних сценаріїв, охопивши ними додаткові, найактуальніші тактики та техніки з фреймворку MITRE ATT&CK, аби зробити процес навчання ще більш всеосяжним, глибоким та актуальним для сучасних реалій кібербезпеки. Треба визнати: не менш важливою є й інтеграція інноваційної системи автоматизованого оцінювання та виявлення типових помилок студентів, яка б базувалася на глибокому, контекстному аналізі їхніх дій безпосередньо в навчальному середовищі.

Практична цінність нашої роботи полягає, перш за все, у перспективі інтеграції платформи в освітній процес закладів вищої освіти, пропонуючи студентам унікальний та незамінний практичний досвід. Крім того, вона стане надзвичайно цінним інструментом для програм підвищення кваліфікації спеціалістів з кібербезпеки, дозволяючи їм опрацьовувати найактуальніші техніки захисту інформації в контрольованому, але реалістичному середовищі.

ЛІТЕРАТУРА

1. Yamin M. M., Katt B., Gkioulos V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*. 2020. Vol. 88. Art. 101636. DOI: <https://doi.org/10.1016/j.cose.2019.101636>
2. Vykopal J., Ošlejšek R., Čeleda P., Vizváry M., Tovarňák D. KYPO Cyber Range: Design and use cases. *Proceedings of the 12th International Conference on Software Technologies (ICSOFT)*. Madrid, Spain, 2017. P. 310–321. DOI: <https://doi.org/10.5220/0006428203100321>
3. Beuran R., Tang D., Pham C., Chinen K., Tan Y., Shinoda Y. Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers & Security*. 2018. Vol. 78. P. 43–59. DOI: <https://doi.org/10.1016/j.cose.2018.06.001>
4. Al-Shaer R., Spring J. M., Christou E. Learning the associations of MITRE ATT&CK adversarial techniques. *2020 IEEE Conference on Communications and Network Security (CNS)*. 2020. P. 1–9. DOI: <https://doi.org/10.1109/CNS48642.2020.9162207>

5. Bernstein D. Containers and cloud: From LXC to Docker to Kubernetes. *IEEE Cloud Computing*. 2014. Vol. 1, No. 3. P. 81–84. DOI: <https://doi.org/10.1109/MCC.2014.51>
6. Merkel D. Docker: Lightweight Linux containers for consistent development and deployment. *Linux Journal*. 2014. No. 239. P. 2.
7. Combe T., Martin A., Di Pietro R. To Docker or not to Docker: A security perspective. *IEEE Cloud Computing*. 2016. Vol. 3, No. 5. P. 54–62. DOI: <https://doi.org/10.1109/MCC.2016.100>
8. Sultan S., Ahmad I., Dimitriou T. Container security: Issues, challenges, and the road ahead. *IEEE Access*. 2019. Vol. 7. P. 52976–52996. DOI: <https://doi.org/10.1109/ACCESS.2019.2911732>
9. Kavak H., Padilla J. J., Vernon-Bido D., Diallo S. Y., Gore R., Shetty S. Simulation for cybersecurity: State of the art and future directions. *Journal of Cybersecurity*. 2021. Vol. 7, No. 1. Art. tyab005. DOI: <https://doi.org/10.1093/cybsec/tyab005>
10. MITRE. MITRE ATT&CK®. URL: <https://attack.mitre.org/>
11. MITRE. Getting started with ATT&CK. URL: <https://attack.mitre.org/resources/>
12. IBM. What is the MITRE ATT&CK framework? URL: <https://www.ibm.com/think/topics/mitre-attack>
13. VulnHub. VulnHub. URL: <https://www.vulnhub.com/>
14. Rapid7. Metasploitable 2 exploitability guide. URL: <https://docs.rapid7.com/metasploit/metasploitable-2/>
15. TryHackMe. URL: <https://tryhackme.com/>
16. Hack The Box. Hack The Box. URL: <https://www.hackthebox.com/>
17. Namespaces. Linux man-pages. URL: <https://man7.org/linux/man-pages/man7/namespaces.7.html>
18. Docker. Docker overview. URL: <https://docs.docker.com/get-started/overview/>
19. Capabilities. Linux man-pages. URL: <https://man7.org/linux/man-pages/man7/capabilities.7.html>
20. Docker. Docker security. URL: <https://docs.docker.com/engine/security/>
21. Django Software Foundation. Django documentation (Version 5.1). URL: <https://docs.djangoproject.com/en/5.1/>
22. Django Channels. Django Channels documentation. URL: <https://channels.readthedocs.io/en/stable/>
23. Docker SDK for Python. Docker SDK for Python documentation. URL: <https://docker-py.readthedocs.io/en/stable/>
24. PostgreSQL Global Development Group. PostgreSQL documentation. URL: <https://www.postgresql.org/docs/>
25. Nginx. Module ngx_http_auth_request_module. URL: https://nginx.org/en/docs/http/ngx_http_auth_request_module.html
26. htmx. htmx documentation. URL: <https://htmx.org/docs/>
27. Alpine.js. Alpine.js documentation. URL: <https://alpinejs.dev/>

REFERENCES

1. Yamin, M.M., Katt, B. and Gkioulos, V. (2020) 'Cyber ranges and security testbeds: Scenarios, functions, tools and architecture', *Computers & Security*, 88, 101636. Available at: <https://doi.org/10.1016/j.cose.2019.101636>
2. Vykopal, J., Ošlejšek, R., Čeleda, P., Vizváry, M. and Tovarňák, D. (2017) 'KYPO Cyber Range: Design and use cases', in *Proceedings of the 12th International Conference on Software Technologies (ICSOF)*, pp. 310–321. Available at: <https://doi.org/10.5220/0006428203100321>
3. Beuran, R., Tang, D., Pham, C., Chinen, K., Tan, Y. and Shinoda, Y. (2018) 'Integrated framework for hands-on cybersecurity training: CyTrONE', *Computers & Security*, 78, pp. 43–59. Available at: <https://doi.org/10.1016/j.cose.2018.06.001>
4. Al-Shaer, R., Spring, J.M. and Christou, E. (2020) 'Learning the associations of MITRE ATT&CK adversarial techniques', in *2020 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9. Available at: <https://doi.org/10.1109/CNS48642.2020.9162207>
5. Bernstein, D. (2014) 'Containers and cloud: From LXC to Docker to Kubernetes', *IEEE Cloud Computing*, 1(3), pp. 81–84. Available at: <https://doi.org/10.1109/MCC.2014.51>
6. Merkel, D. (2014) 'Docker: Lightweight Linux containers for consistent development and deployment', *Linux Journal*, 2014(239), p. 2.
7. Combe, T., Martin, A. and Di Pietro, R. (2016) 'To Docker or not to Docker: A security perspective', *IEEE Cloud Computing*, 3(5), pp. 54–62. Available at: <https://doi.org/10.1109/MCC.2016.100>

8. Sultan, S., Ahmad, I. and Dimitriou, T. (2019) 'Container security: Issues, challenges, and the road ahead', *IEEE Access*, 7, pp. 52976–52996. Available at: <https://doi.org/10.1109/ACCESS.2019.2911732>
9. Kavak, H., Padilla, J.J., Vernon-Bido, D., Diallo, S.Y., Gore, R. and Shetty, S. (2021) 'Simulation for cybersecurity: State of the art and future directions', *Journal of Cybersecurity*, 7(1), tyab005. Available at: <https://doi.org/10.1093/cybsec/tyab005>
10. MITRE (2024) *MITRE ATT&CK®*. Available at: <https://attack.mitre.org/>
11. MITRE (2023) *Getting started with ATT&CK*. Available at: <https://attack.mitre.org/resources/>
12. IBM (2024) *What is the MITRE ATT&CK framework?* Available at: <https://www.ibm.com/think/topics/mitre-attack>
13. VulnHub (2024) *VulnHub*. Available at: <https://www.vulnhub.com/>
14. Rapid7 (2024) *Metasploitable 2 exploitability guide*. Available at: <https://docs.rapid7.com/metasploit/metasploitable-2/>
15. TryHackMe (2024) *TryHackMe*. Available at: <https://tryhackme.com/>
16. Hack The Box (2024) *Hack The Box*. Available at: <https://www.hackthebox.com/>
17. Namespaces (7) (2023) *Linux man-pages*. Available at: <https://man7.org/linux/man-pages/man7/namespaces.7.html>
18. Docker (2024) *Docker overview*. Available at: <https://docs.docker.com/get-started/overview/>
19. Capabilities (7) (2023) *Linux man-pages*. Available at: <https://man7.org/linux/man-pages/man7/capabilities.7.html>
20. Docker (2024) *Docker security*. Available at: <https://docs.docker.com/engine/security/>
21. Django Software Foundation (2024) *Django documentation (Version 5.1)*. Available at: <https://docs.djangoproject.com/en/5.1/>
22. Django Channels (2024) *Django Channels documentation*. Available at: <https://channels.readthedocs.io/en/stable/>
23. Docker SDK for Python (2024) *Docker SDK for Python documentation*. Available at: <https://docker-py.readthedocs.io/en/stable/>
24. PostgreSQL Global Development Group (2024) *PostgreSQL documentation*. Available at: <https://www.postgresql.org/docs/>
25. Nginx (2024) *Module ngx_http_auth_request_module*. Available at: https://nginx.org/en/docs/http/ngx_http_auth_request_module.html
26. htmx (2024) *htmx documentation*. Available at: <https://htmx.org/docs/>
27. Alpine.js (2024) *Alpine.js documentation*. Available at: <https://alpinejs.dev/>

Babych T., PhD Sashnova M., Radziievska O., Dyakonenko D.

AUTOMATED DEPLOYMENT OF VULNERABLE TRAINING ENVIRONMENTS USING THE LEAST-PRIVILEGE MODEL

The growing number and complexity of cyberattacks impose increasingly stringent requirements on the practical training of cybersecurity professionals. At the same time, traditional lecture-based instruction is, unfortunately, often unable to provide a sufficient level of applied skills. Training-oriented cyber ranges address this problem to a certain extent, but existing solutions rarely offer automated deployment of a separate, fully isolated environment for each participant. Moreover, they frequently fail to align training scenarios with formalized descriptions of adversary techniques. The main goal of our study was therefore to substantiate, design, and ultimately implement in software a platform capable of automated deployment of vulnerable testbeds that accurately reproduce documented techniques from the MITRE ATT&CK framework, within a controlled multi-user space, while ensuring complete isolation between users through containerization technologies.

A variety of methods were employed in the course of this work, including a systematic analysis of existing cyber ranges and vulnerable testbeds, as well as a thorough comparative analysis of isolation mechanisms at both the container and virtual machine levels. In addition, object-oriented software architecture design methods were applied, together with a carefully elaborated least-privilege model for container configuration. The platform is built on a multi-tier architecture (Nginx, Django/Daphne, PostgreSQL, Redis) with dynamic orchestration of Docker containers, managed through a dedicated application programming interface.

A platform was designed and implemented that automatically creates and, subsequently, destroys isolated vulnerable testbeds on demand. It is capable of mapping each testbed to specific MITRE ATT&CK

techniques and, importantly, supports the addition of entirely new laboratory scenarios without requiring changes to its core. A security configuration for containers was proposed, based on the principle of dropping unnecessary privileges, while preserving the ability to selectively relax these restrictions in order to correctly reproduce certain techniques. A comparison of the chosen container-based approach with traditional virtualization convincingly demonstrated substantially shorter deployment times and significantly lower resource consumption.

Combining containerization, automated orchestration, and scenario integration directly with the MITRE ATT&CK framework enables the creation of a scalable and, most importantly, reproducible environment suitable for practical cybersecurity training. The practical value of the platform lies in the fact that it can be readily integrated both into the educational process of higher education institutions and into professional development systems for information security specialists.

Keywords: cybersecurity; MITRE ATT&CK; cyber range; vulnerable environment; containerization; Docker; environment isolation; modeling.

СИСТЕМА АВТОМАТИЗОВАНОГО РОЗГОРТАННЯ КЛАСТЕРНОГО СЕРЕДОВИЩА

У статті розглянуто питання швидкого розгортання та підтримки складних ІТ-інфраструктур за умов зростання навантаження або відмов окремих компонентів. Показано, що одним із варіантів розгортання складних структур є застосування контейнерних технологій з використанням кластерних обчислювальних середовищ і систем оркестрації контейнерів.

В матеріалі були проаналізовані поняття контейнеризації. Показано, що такий підхід забезпечує ізоляцію застосунків разом із їхніми залежностями, що гарантує портативність програмного забезпечення, його однакове функціонування в різних середовищах та можливість автоматизації процесів розгортання.

Розглянуто основні характеристики кластерних систем. Визначено, що об'єднання незалежних обчислювальних вузлів у єдину логічну мережу дозволяє забезпечити високу доступність, масштабованість і стійкість до відмов. Проаналізовано основні характеристики кластерів, такі як масштабованість, відмовостійкість, балансування навантаження. Розкриті мережеві вимоги для функціонування кластерних середовищ.

Показано, що для системи автоматизованого розгортання кластерних середовищ контейнерна модель є пріоритетною, оскільки вона забезпечує швидке масштабування, ефективне використання ресурсів і тісну інтеграцію з системами оркестрації.

Проаналізовано систему оркестрації контейнерів, яка використовується для автоматизації розгортання, керування, масштабування та підтримки контейнеризованих застосунків Kubernetes. Показано можливість ефективного управління великою кількістю контейнерів у складних інформаційних системах.

Для проведення експериментальних досліджень запропонована, описана, реалізована і протестована на власній інфраструктурі практична реалізація системи автоматизованого розгортання і управління технологіями контейнеризації у кластерному середовищі Kubernetes.

Ключові слова: кластерні обчислювальні середовища, контейнеризація, оркестрація, Kubernetes, автоматизація розгортання, програмні застосунки.

Вступ та постановка проблеми. Сучасні інформаційні системи стають складнішими, а вимоги до їх надійності, масштабованості та безпеки постійно зростають. Організації все частіше стикаються з необхідністю швидкого розгортання та підтримки складних ІТ-інфраструктур, здатних забезпечити безперебійну роботу сервісів навіть за умов зростання навантаження або відмов окремих компонентів. У таких умовах традиційні підходи до розгортання та адміністрування програмного забезпечення виявляються недостатньо ефективними.

Одним із ключових напрямів розвитку сучасних ІТ-інфраструктур стала контейнеризація, яка дозволяє ізолювати програмні застосунки разом із їхніми залежностями та забезпечити їхнє однакове функціонування в різних середовищах. Контейнерні технології спрощують розгортання, оновлення та масштабування програмних систем, а також дають змогу ефективніше використовувати обчислювальні ресурси. У поєднанні з кластерними обчислювальними середовищами контейнеризація формує основу для побудови гнучких, відмовостійких і масштабованих систем.

З цієї точки зору важливе значення мають системи оркестрації контейнерів, які автоматизують управління великою кількістю контейнеризованих застосунків. Такі системи беруть на себе завдання розподілу навантаження, масштабування, моніторингу стану

компонентів та відновлення роботи сервісів у разі збоїв. Завдяки цьому зменшується кількість ручних операцій з боку адміністратора та знижується ймовірність помилок, пов'язаних із людським фактором.

Актуальність дослідження пов'язана також зі зростанням значення власної інфраструктури в умовах підвищених вимог до інформаційної безпеки. Для багатьох організацій, особливо у сфері державного управління, критичної інфраструктури або корпоративних мереж, використання публічних хмарних сервісів є обмеженим або небажаним. У таких випадках постає завдання розгортання сучасних кластерних середовищ безпосередньо на власних обчислювальних ресурсах із забезпеченням належного рівня захисту інформації, контролю доступу та стабільності роботи системи.

Тому особливої уваги потребує автоматизоване розгортання кластерного середовища. Автоматизація дозволяє не лише скоротити час налаштування інфраструктури, а й забезпечити відтворюваність конфігурацій, спростити подальше обслуговування системи та мінімізувати ризики помилок під час ручного налаштування. Для фахівців з кібербезпеки автоматизовані підходи є важливими також з точки зору контролю змін, стандартизації конфігурацій та зменшення поверхні атаки.

Метою статті є дослідження принципів побудови та реалізації системи автоматизованого розгортання кластерного середовища на власній інфраструктурі з використанням сучасних технологій контейнеризації та оркестрації.

Аналіз останніх досліджень і публікацій. Одним із ключових завдань сучасних ІТ-систем є ефективне та гнучке розгортання програмного забезпечення. Традиційно для цього використовувалася апаратна або програмна віртуалізація, яка дозволяла запускати кілька віртуальних машин на одному фізичному сервері. У такій моделі кожна віртуальна машина функціонує як окреме середовище, оскільки, як зазначають Н. Sturley та співавтори, віртуальні машини емулюють низькорівневі компоненти, що дозволяє детально налаштувати їх під конкретні потреби та робить їх автономними системами [1]. Водночас така автономність вимагає значних обчислювальних ресурсів і збільшує час запуску середовищ виконання.

Із ускладненням програмних систем і зростанням вимог до швидкості їх розгортання виникла потреба в більш легких підходах до ізоляції застосунків. Таким підходом стала контейнеризація, яка принципово відрізняється від класичної віртуалізації. У порівняльному аналізі віртуалізації та контейнеризації підкреслюється, що контейнери використовують спільну операційну систему хоста і не потребують віртуалізації низькорівневих апаратних компонентів [1]. Ця архітектурна особливість зумовлює менші витрати ресурсів і значно швидший запуск контейнерів.

Контейнеризація визначається як технологія упакування програмного забезпечення разом із усіма компонентами, необхідними для його коректної роботи. "Контейнеризація – це метод упакування та запуску програмного забезпечення в ізольованому середовищі, яке включає в себе все необхідне для його коректної роботи: код, що виконується, бібліотеки, конфігураційні файли, залежності тощо" [2]. Тобто контейнер можна розглядати як зручний формат доставки програмного коду, що забезпечує відтворюваність роботи застосунків у різних середовищах.

Завдяки цьому розроблений і протестований застосунок можна без істотних змін переносити з локального середовища розробника на тестовий сервер або у виробниче середовище. У науковій літературі підкреслюється, що контейнери розглядаються як стандартизована та портативна одиниця розгортання застосунків, що безпосередньо зумовлює високу портативність контейнеризованих рішень [3].

Контейнеризація має кілька важливих переваг. До них належать портативність, легка масштабованість, ефективне використання ресурсів, швидке розгортання та підтримка процесів Continuous Integration/Continuous Delivery (CI/CD), ізоляція та безпека, а також гнучкість у керуванні мікросервісами [2].

Портативність дає змогу використовувати той самий контейнер у різних середовищах без окремого налаштування залежностей.

Легка масштабованість забезпечується можливістю швидкого запуску або зупинки контейнерів залежно від поточного навантаження, що є особливо важливим для середовищ із динамічними вимогами до ресурсів.

Ефективне використання ресурсів досягається за рахунок меншого споживання обчислювальних потужностей порівняно з віртуальними машинами та дозволяє розміщувати більше застосунків на одному сервері.

Швидке розгортання та підтримка процесів CI/CD пов'язані з можливістю автоматизувати процеси збірки, тестування та впровадження програмного забезпечення.

Ізоляція та безпека реалізуються через виконання кожного контейнера в окремому середовищі, що обмежує вплив збоїв або вразливостей одного застосунку на інші компоненти системи.

Гнучкість у керуванні мікросервісами проявляється в можливості незалежного розгортання, оновлення та масштабування окремих сервісів, що спрощує супровід складних програмних систем і підвищує їхню стійкість.

Водночас використання контейнеризації супроводжується і низкою ризиків, серед яких особливої уваги заслуговують безпека контейнерів, моніторинг і логування, оркестрація та управління [2]. Ризики безпеки контейнерів пов'язані зі спільним використанням контейнерами ядра операційної системи хоста, що у разі неналежної ізоляції процесів або контролю доступу може призводити до ескалації привілеїв, виконання шкідливого коду чи витоку даних.

У сфері моніторингу та логування ризики зумовлені динамічним характером контейнеризованих середовищ і коротким життєвим циклом контейнерів, що ускладнює застосування традиційних підходів до спостереження за станом системи та аналізу подій.

Ризики оркестрації та управління виникають зі зростанням кількості контейнерів і потребою в автоматизованому управлінні їх запуском, масштабуванням і відновленням, що ускладнює початкові етапи впровадження контейнерних рішень на власній інфраструктурі.

На практиці контейнеризацію використовують через спеціалізовані платформи для створення, запуску та управління контейнерами. Проте зі зростанням кількості контейнерів виникає потреба в централізованому управлінні їх життєвим циклом, що зумовлює використання систем оркестрації, зокрема Kubernetes – це відкрита платформа для автоматизації розгортання, масштабування та керування контейнеризованими застосунками [2]. Такі системи забезпечують автоматизацію розгортання, масштабування та відновлення контейнеризованих сервісів.

Таким чином, контейнеризація є важливим елементом сучасних ІТ-систем, який забезпечує гнучкість, масштабованість і ефективність розгортання програмного забезпечення. Ці властивості роблять контейнерні технології теоретичною основою для побудови кластерних середовищ і автоматизованих систем розгортання.

Виклад основного матеріалу. Кластер – це група незалежних обчислювальних вузлів, з'єднаних мережею та скоординованих таким чином, що для користувача або прикладного програмного забезпечення вони функціонують як єдина система. Кожен вузол кластера має власні обчислювальні ресурси, однак завдяки програмним засобам управління ресурси всіх вузлів використовуються узгоджено, а сам кластер сприймається як один логічний обчислювальний ресурс.

Однією з головних характеристик кластерів є масштабованість, яка полягає у можливості збільшення або зменшення обчислювальних ресурсів шляхом додавання або видалення вузлів без суттєвого впливу на роботу системи. Такий підхід є особливо важливим для систем зі змінним навантаженням, у яких потреба в ресурсах може істотно коливатися залежно від кількості користувачів або характеру виконуваних завдань [4].

Ще однією важливою характеристикою є відмовостійкість. У кластерному середовищі відмова одного або кількох вузлів не призводить до повної зупинки системи, оскільки виконання завдань може бути автоматично перенесене на інші доступні вузли. Це забезпечує безперервність надання сервісів і мінімізувати час простою, що є визначальною ознакою

кластерів високої доступності [5].

Також важливим є балансування навантаження, яке полягає в розподілі запитів або обчислювальних задач між вузлами кластера таким чином, щоб уникнути перевантаження окремих компонентів. Такий механізм сприяє підвищенню загальної продуктивності системи та забезпечує більш ефективне використання наявних обчислювальних ресурсів.

Залежно від призначення виділяють чотири основні типи кластерів: кластери високої доступності (High-availability clusters), балансувальні кластери (Load balancing clusters), кластери зберігання даних (Storage clusters) та обчислювальні кластери (High-performance computing, HPC) [4, 5]. Кластери високої доступності та балансування забезпечують безперервність сервісів та стійкість до відмов. Кластери зберігання гарантують цілісність інформації шляхом її реплікації. HPC-системи орієнтовані на паралельне виконання ресурсомістких задач, зокрема наукових розрахунків і обробки великих масивів даних. Поєднання механізмів високої доступності, балансування та надійного зберігання даних створює технічну основу для побудови захищених систем автоматизованого розгортання на власній інфраструктурі.

Ефективне функціонування кластерних середовищ значною мірою залежить від мережевої інфраструктури. Обмін даними між вузлами має здійснюватися з мінімальними затримками, оскільки це безпосередньо впливає на продуктивність і стабільність роботи системи. У розподілених обчислювальних середовищах мережеві характеристики є одним із ключових факторів, що визначають ефективність взаємодії між компонентами системи [4].

Окремої уваги потребує безпека кластерних та контейнерних середовищ. Спільне використання обчислювальних ресурсів відкриває нові шляхи до вразливостей, що зумовлює необхідність впровадження чітких політик безпеки. Зокрема, важливим є забезпечення суворого контролю доступу до мережі, обмеження привілеїв компонентів та регулярне сканування на вразливості. Крім того, належний контроль доступу на рівні процесів є обов'язковою умовою для запобігання ескалації привілеїв та захисту від витоку даних [2].

У сучасних IT-системах кластерні обчислювальні середовища тісно поєднуються з контейнерними технологіями та системами оркестрації, що дозволяє автоматизувати управління ресурсами, масштабування та відновлення сервісів. Однією з найбільш поширених платформ для управління контейнерними кластерами є Kubernetes. Її широке використання зумовлене здатністю забезпечувати уніфіковану модель управління кластером, автоматизацію життєвого циклу контейнерів і механізми самовідновлення сервісів, що робить Kubernetes базовим інструментом для побудови сучасних кластерних середовищ [6].

Отже, кластерні обчислювальні середовища створюють технічну основу для побудови масштабованих і відмовостійких сервісів. Їх поєднання з контейнеризацією та автоматизованими засобами оркестрації формує технологічне підґрунтя для створення сучасних IT-інфраструктур і використання Kubernetes як ключового інструменту управління кластерними середовищами.

Для систем автоматизованого розгортання кластерних середовищ контейнерна модель є пріоритетною, оскільки вона забезпечує швидке масштабування, ефективне використання ресурсів і тісну інтеграцію з системами оркестрації, зокрема Kubernetes. Ці властивості зумовлюють її широке застосування при побудові сучасних кластерних систем.

Kubernetes – це система оркестрації контейнерів, яка використовується для автоматизації розгортання, керування, масштабування та підтримки контейнеризованих застосунків [6]. Його поява стала відповіддю на потребу ефективно управляти великою кількістю контейнерів у складних інформаційних системах. Якщо на початковому етапі контейнери могли запускатися окремо і адмініструватися вручну, то зі зростанням кількості сервісів та навантаження виникла потреба в платформі, яка б координувала їхню роботу автоматично. Таку функцію виконує Kubernetes.

Основою його роботи є кластерна архітектура. Kubernetes-кластер складається з набору вузлів, які об'єднані в єдину систему. У межах цієї системи одні вузли відповідають за керування кластером, а інші – за виконання прикладних завдань. Поділ функцій між такими

вузлами забезпечує чітку організацію роботи кластера та спрощує адміністрування всієї системи. Такий підхід дає можливість розподіляти навантаження, ефективно використовувати ресурси та забезпечувати безперервність роботи сервісів навіть у разі збоїв окремих елементів інфраструктури.

У загальному вигляді кластер Kubernetes має дві основні частини: керуючу частину (control plane) і робочі вузли (worker nodes). Відповідно до офіційної документації, керуюча частина відповідає за керування кластером і прийняття глобальних рішень щодо його стану (наприклад, планування), тоді як робочі вузли відповідають за безпосереднє виконання робочих навантажень [7].

Для того щоб кластер працював як єдина система, кожна з його частин має набір специфічних компонентів. Головним елементом керуючої частини є kube-apiserver – "головний диспетчер" кластера Kubernetes. Це основна точка взаємодії з кластером. Через API-сервер користувач надсилає команди, змінює конфігурацію, отримує інформацію про стан системи та керує ресурсами. Інші компоненти Kubernetes також взаємодіють між собою через нього. Тому API-сервер можна вважати центральним елементом, через який проходять усі основні процеси управління.

Не менш важливою складовою є etcd. Це спеціальне сховище, у якому зберігається інформація про стан кластера, його конфігурація та створені об'єкти. Наприклад, саме тут містяться дані про те, які pod створені, які налаштування вони мають і де саме працюють. Фактично etcd є основним сховищем даних, на яке спирається весь Kubernetes [7]. Тому його стабільна робота має дуже велике значення для всього кластера.

Наступним ключовим елементом системи є kube-scheduler. Його завдання полягає в тому, щоб визначити, на якому робочому вузлі потрібно розмістити новий pod. Під час цього вибору враховується наявність вільних ресурсів, завантаженість вузлів, обмеження за політиками розміщення та інші параметри. Завдяки роботі kube-scheduler навантаження в кластері розподіляється більш рівномірно, а ресурси використовуються ефективніше.

Важливе місце в архітектурі Kubernetes займає поняття pod. Згідно з офіційною технічною документацією, pod визначається як найменша обчислювальна одиниця, яку можна створити та якою можна керувати в Kubernetes. Він являє собою групу з одного або кількох контейнерів зі спільним сховищем та мережевими ресурсами [8]. Контейнери всередині одного pod використовують спільний мережевий простір і можуть спільно використовувати деякі ресурси. Це зручно, коли кілька процесів повинні працювати разом у межах одного сервісу.

Крім pod, у Kubernetes існує велика кількість об'єктів, за допомогою яких описується робота застосунків. Одним із найпоширеніших є Deployment. Він використовується для керування розгортанням застосунків, оновленням їхніх версій і підтриманням потрібної кількості копій [9]. Іншим важливим об'єктом є Service, який забезпечує постійний доступ до групи pod, навіть якщо їхній склад або внутрішні адреси змінюються [10].

Важливу роль відіграє і kube-controller-manager. Він відповідає за роботу контролерів, які стежать за тим, щоб фактичний стан системи відповідав бажаному. Наприклад, якщо в конфігурації вказано, що має працювати три pod, а один із них зупинився, контролер помічає це і ініціює створення нового. Цей механізм дозволяє Kubernetes автоматично реагувати на збої та підтримувати працездатність сервісів [7].

На робочих вузлах також функціонують власні системні служби. Передусім це kubelet – агент, який запускається на кожному вузлі. Він отримує інструкції від керуючої частини кластера, контролює запуск контейнерів, перевіряє їхній стан та передає інформацію назад у систему. Іншими словами, kubelet забезпечує зв'язок між робочим вузлом і Kubernetes як системою управління.

Ще однією системною службою робочого вузла є kube-proxy. Він відповідає за мережеву взаємодію та маршрутизацію трафіку в межах кластера. Завдяки його роботі запити можуть надходити до потрібних pod, а сервіси в Kubernetes отримують стабільну точку доступу. Це особливо важливо тому, що окремі pod можуть перезапуститися, переміщуватися

між вузлами або створюватися заново, але користувачі та інші сервіси повинні звертатися до них без змін у своїй конфігурації.

Слід також згадати контейнерне середовище виконання. Воно відповідає за безпосередній запуск контейнерів на вузлі. Цей компонент завантажує образи контейнерів, створює їх, запускає, зупиняє та видаляє за потреби. Тобто Kubernetes координує процес, але сам запуск контейнерів виконується через відповідне середовище виконання. Крім того, для забезпечення єдиного адресного простору та зв'язку між усіма контейнерами кластер вимагає встановлення мережевого плагіна стандарту CNI (Container Network Interface), який організовує віртуальну оверлейну мережу [11].

Також у Kubernetes використовуються ConfigMap і Secret. Вони потрібні для зберігання конфігураційних параметрів та службових даних. Різниця між ними полягає в тому, що Secret застосовується для більш чутливих даних, наприклад паролів або токенів доступу [10]. Для окремих сценаріїв використовуються також StatefulSet, DaemonSet, Job та інші об'єкти. Наприклад, StatefulSet підходить для сервісів, яким важлива сталість ідентифікації або порядок запуску, а DaemonSet використовується тоді, коли певний род повинен працювати на кожному вузлі кластера [12]. Таким чином, Kubernetes надає не лише базові механізми запуску контейнерів, а й досить широкий набір інструментів для різних типів навантаження.

Одним із головних принципів роботи Kubernetes, який об'єднує ці компоненти та об'єкти, є декларативний підхід. Його суть полягає в тому, що користувач або адміністратор не описує покроково, що саме система повинна зробити, а задає бажаний результат. Наприклад, можна вказати, що в кластері має працювати три екземпляри певного застосунку. Після цього Kubernetes постійно перевіряє, чи зберігається цей стан на практиці. Якщо виникає відхилення, система намагається його усунути автоматично. Завдяки цьому забезпечується стабільність роботи кластера [6].

Кластерна архітектура Kubernetes добре підходить для сучасних розподілених систем, особливо тих, що побудовані за мікросервісним принципом. У такій моделі окремі частини застосунку працюють як самостійні сервіси, але водночас повинні взаємодіяти між собою. Kubernetes спрощує управління такими сервісами, оскільки дозволяє централізовано керувати їхнім запуском, оновленням, масштабуванням і відновленням після збоїв. Важливою перевагою Kubernetes є те, що він не прив'язаний до конкретної фізичної інфраструктури. Його можна використовувати на локальних серверах, у корпоративних дата-центрах, у публічних хмарах або в змішаних середовищах. Для користувача це означає, що підхід до роботи із застосунками залишається однаковим незалежно від того, де саме вони розгортаються. Це значно спрощує перенесення сервісів між різними середовищами та робить інфраструктуру гнучкішою [11].

В підсумку, архітектура Kubernetes-кластера є цілісною системою, у якій кожен компонент виконує свою функцію. Її елементи забезпечують зберігання даних про стан кластера, прийняття рішень щодо розміщення навантаження, запуск контейнерів, мережеву взаємодію та контроль за працездатністю системи. Завдяки такій організації Kubernetes забезпечує автоматизацію керування кластером, зручність адміністрування та стійкість до збоїв.

Розгортання інформаційних систем на власній інфраструктурі зазвичай пов'язане з підвищеними вимогами до захисту даних, тому питання безпеки Kubernetes-кластера потребує додаткової уваги. З погляду кібербезпеки, просто запустити контейнери недостатньо – потрібно гарантувати, що в разі зламу одного з компонентів злоумисник не зможе отримати контроль над усією системою. Відповідно до рекомендацій стандарту NIST щодо безпеки контейнерів, архітектура захисту має будуватися на принципі найменших привілеїв та ізоляції ресурсів [13].

У Kubernetes цей захист реалізується на кількох рівнях, основні з яких: контроль доступу, мережева ізоляція та безпечне управління чутливими даними.

Першим рівнем захисту є система контролю доступу на основі ролей – RBAC (Role-Based Access Control). У Kubernetes за замовчуванням жоден користувач або процес не має

повних прав на управління кластером. Для того, щоб виконати будь-яку дію (наприклад, створити новий pod або переглянути логи), потрібно мати відповідний дозвіл. RBAC дозволяє адміністратору створювати ролі з чітко обмеженими правами і призначати їх конкретним користувачам або самим застосункам (через ServiceAccounts) [14]. Завдяки цьому, якщо зломисник зламає вебдодаток, він отримає лише ті мінімальні права, які були виділені цьому додатку, і не зможе видалити бази даних чи змінити налаштування кластера.

Другим важливим елементом безпеки для розподілених систем є мережева ізоляція. Особливість Kubernetes полягає в тому, що одразу після встановлення всі pod в кластері можуть вільно обмінюватися даними між собою без жодних обмежень. З точки зору безпеки це створює ризик: якщо хакер знайде вразливість у публічному вебсайті (frontend), він зможе напряму підключитися до внутрішньої бази даних, яка мала б бути прихованою. Для вирішення цієї проблеми використовуються Network Policies (мережеві політики). Це своєрідний внутрішній фаєрвол кластера. За допомогою Network Policies можна прописати правила маршрутизації: наприклад, дозволити базі даних приймати запити виключно від бекенду і блокувати інший трафік. Це підвищує мережеву безпеку інфраструктури, унеможливаючи прямий доступ до критичних даних або зовнішніх серверів навіть у разі зламу суміжних контейнерів [15]. На рис. 1 показано базову модель мережевої взаємодії pod у кластері Kubernetes, у межах якої Network Policies застосовуються для контролю дозволеного трафіку.

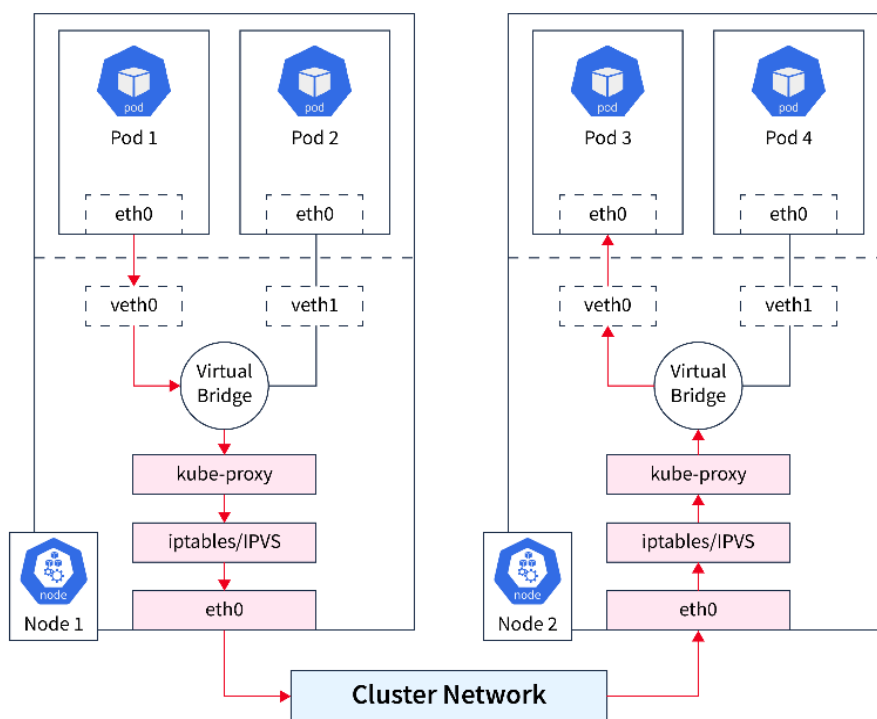


Рисунок 1 – Базова модель мережевої взаємодії pod у Kubernetes-кластері [24]

Третім важливим аспектом є робота з конфіденційною інформацією. Будь-який сучасний застосунок використовує паролі, API-ключі або сертифікати доступу. Зберігати такі дані прямо в коді – це небезпечна практика, оскільки доступ до них може отримати будь-хто, хто має доступ до вихідного коду [13]. Для вирішення цієї задачі в Kubernetes передбачено спеціальний об'єкт – Secret. Цей механізм дозволяє зберігати паролі окремо від самих застосунків у зашифрованому вигляді на рівні системи управління. Контейнер отримує доступ до цих даних лише в момент запуску і лише якщо йому це явно дозволено правилами [10].

Практична реалізація розгортання кластера на власній інфраструктурі. Перед розгортанням Kubernetes-кластера необхідно визначити вимоги до інфраструктури, на якій він

буде працювати. Від правильного підбору ресурсів залежить не лише стабільність роботи кластера, а й можливість його подальшого масштабування та оновлення. Якщо інфраструктура спроектована без урахування реальних потреб системи, у процесі експлуатації можуть виникати проблеми з продуктивністю, доступністю сервісів та керуванням вузлами.

Під власною інфраструктурою (on-premises) розуміється середовище, яке розгортається і контролюється самостійно, без використання готових керованих Kubernetes-сервісів від хмарних провайдерів (наприклад, AWS EKS чи Google GKE). На відміну від використання таких сервісів, розгортання на власному обладнанні дає повний контроль над апаратною частиною та безпекою даних, але водночас вимагає самостійного налаштування основних компонентів та забезпечення їхньої взаємодії [11].

Однією з базових вимог є достатній обсяг обчислювальних ресурсів. Для коректної роботи кластера потрібно передбачити ресурси як для керуючої частини, так і для робочих вузлів [7]. Виходячи з цих вимог, апаратною базою для практичної частини розгортання кластерного середовища став фізичний міні-кластер, побудований на п'яти одноплатних мікрокомп'ютерах Raspberry Pi 5 (з 8 ГБ оперативної пам'яті кожен). Вибір цієї платформи зумовлений високою енергоефективністю, достатнім обсягом RAM для запуску контейнерів та підтримкою архітектури ARM64 з боку екосистеми Kubernetes. Архітектурну схему побудованого Kubernetes-кластера наведено на рис. 2.

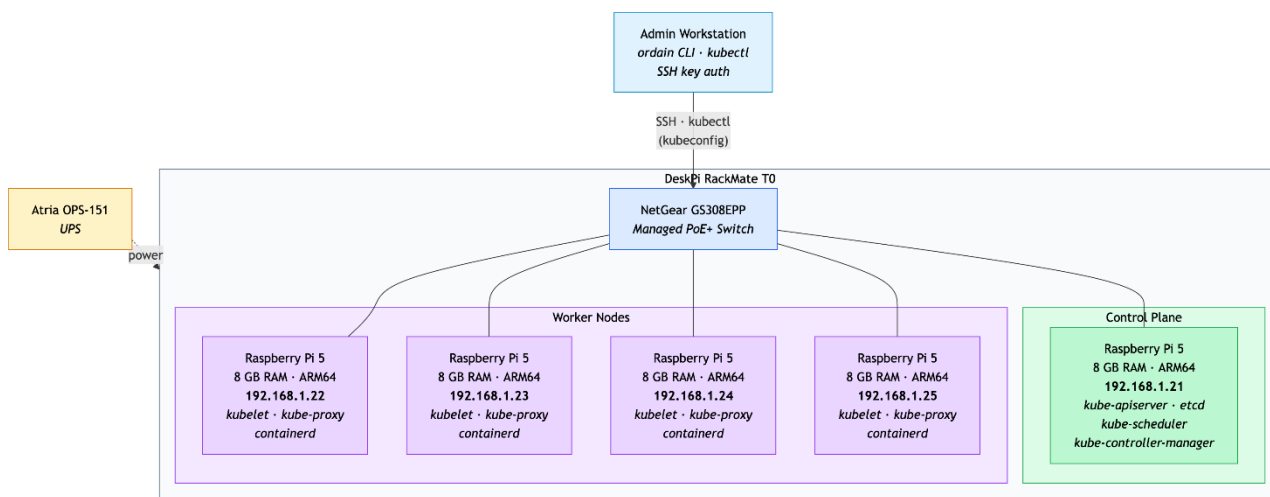


Рисунок 2 – Архітектурна схема запропонованого Kubernetes-кластера

Для організації простору та забезпечення належного охолодження усі п'ять вузлів фізично розміщені у спеціалізованій стійці DeskPi RackMate T0. Апаратна інфраструктура Kubernetes-кластера складається з наступних елементів:

Склад інфраструктури:

- Raspberry Pi 5, 8 GB RAM - 5 од.;
- DeskPi RackMate T0 - 1 од.;
- NetGear GS308EPP - 1 од.;
- Atria OPS-151 - 1 од.

Функціональний розподіл вузлів:

- control plane node - 1;
- worker nodes - 4.

Фізичне підключення:

- усі вузли підключені до комутатора NetGear GS308EPP;
- тип підключення – дротове Ethernet;
- адміністрування вузлів – через SSH.

Живлення:

- вузли кластера та комутатор підключені до ДБЖ Atria OPS-151.

Мережева взаємодія реалізована наступним чином. Усі елементи Kubernetes-кластера повинні мати стабільне з'єднання з мінімальними затримками для обміну службовими повідомленнями та роботи API-сервера [16]. Для реалізації цієї вимоги в інфраструктуру інтегровано керований комутатор (світч) NetGear GS308EPP. Він забезпечує надійну маршрутизацію внутрішнього трафіку між вузлами кластера та ізоляцію мережевих сегментів, що є важливим з точки зору безпеки.

Під час проєктування власної інфраструктури слід приділяти увагу відмовостійкості та безперебійному живленню. Раптове знеструмлення серверів може призвести до пошкодження системних файлів бази даних etcd, у якій зберігається поточний стан усього кластера [7]. Для вирішення цієї проблеми до апаратного комплексу підключено джерело безперебійного живлення (ДБЖ) Atria OPS-151. Це гарантує базову апаратну відмовостійкість: у разі перебоїв в електромережі кластер продовжить функціонувати, даючи час на коректне збереження даних.

З точки зору кібербезпеки, доступ до керуючих інтерфейсів і вузлів має бути суворо обмеженим [13]. У зібраному кластері це досягається налаштуванням локальної мережі, доступом виключно через протокол SSH з використанням криптографічних ключів та відсутністю прямого доступу вузлів до публічної мережі Інтернет без необхідності.

Спроектвана та зібрана апаратна інфраструктура загалом відповідає основним вимогам до ресурсів, мережевої ізоляції та енергонезалежності, створюючи умови для автоматизованого розгортання Kubernetes.

Після підготовки фізичної інфраструктури наступним етапом є вибір інструментів для автоматизації налаштування операційних систем та встановлення Kubernetes. Це важливий етап, оскільки від нього залежать складність налаштування, швидкість розгортання, можливість повторного використання конфігурацій та зручність подальшого адміністрування системи. Автоматизація дозволяє мінімізувати кількість ручних дій, усунути ризик помилок та забезпечити відтворюваність конфігурацій на всіх вузлах [17].

Для автоматизації розгортання Kubernetes зазвичай використовують готові системи управління конфігураціями (наприклад, Ansible або Terraform) у поєднанні зі спеціалізованими утилітами, такими як kubectl. Ansible є популярним вибором завдяки безагентній архітектурі та роботі через стандартний протокол SSH. Проте використання готових рішень часто приховує від адміністратора сам процес налаштування вузлів і взаємодії компонентів.

Зважаючи на це, у межах дослідження було прийнято рішення не використовувати Ansible, а розробити власний інструмент автоматизації мовою Rust.

Вибір мови Rust обґрунтований кількома факторами, які є важливими для кібербезпеки та системного адміністрування. По-перше, Rust гарантує безпечну роботу з пам'яттю (memory safety), що мінімізує ризик виникнення вразливостей, притаманних системним утилітам на C/C++. По-друге, ця мова дозволяє компілювати ефективні бінарні файли, які не вимагають встановлення важких залежностей (наприклад, Python-середовища) на цільових мікрокомп'ютерах Raspberry Pi.

Конфігурація запуску розробленого інструменту може задаватися двома способами: через аргументи командного рядка або через єдиний опціональний файл конфігурації у форматі YAML чи JSON. Такий підхід дає змогу або передавати параметри безпосередньо під час запуску, або зберігати типову конфігурацію для повторного використання. Якщо один і той самий параметр задано в обох формах, тоді пріоритет має значення, яке передане через CLI.

Розроблений інструмент призначений для виконання повного циклу підготовки вузлів. Його ключові можливості включають:

Розгортання за IP-діапазонами: інструмент дозволяє задавати діапазони IP-адрес під час запуску (наприклад, 192.168.1.22-192.168.1.25), автоматично розгортаючи їх у перелік окремих адрес та підключаючись до кожного вузла кластера.

Підключення та конфігурація вузлів: програма підключається до вузлів через протокол SSH та автоматично виконує необхідні системні налаштування (відключення swappiness, конфігурація ядра, встановлення залежностей). За замовчуванням вузли обробляються послідовно, однак за наявності відповідного параметра конфігурації підготовка може виконуватися паралельно для пришвидшення процесу.

Оркестрація через kubernetes: інструмент самостійно ініціює команду kubernetes init на керуючому вузлі, перехоплює згенерований криптографічний токен та розсилає команду kubernetes join на всі робочі вузли.

Встановлення мережевого плагіна та додатків кластера: після ініціалізації інструмент автоматично розгортає обраний CNI-плагін (Flannel або Calico), а також, залежно від конфігурації, встановлює балансувальник навантаження MetalLB, контролер вхідного трафіку ingress-nginx, постачальник сховищ (local-path або Longhorn) та metrics-server.

Режим валідації (dry-run): інструмент підтримує режим пробного запуску, який перевіряє з'єднання з вузлами та відповідність апаратних вимог без внесення будь-яких змін до системи.

Скидання кластера (reset): програма забезпечує повне або часткове скидання кластера. У частковому режимі видаляється лише стан Kubernetes, тоді як повне скидання додатково деінстальовує всі пакети та повертає системну конфігурацію вузлів до початкового стану.

Для зручності адміністрування розроблений інструмент забезпечує запуск процесу розгортання через командний рядок і надає службову інформацію про хід виконання операцій. Це дозволяє в режимі реального часу відстежувати статус підключення до кожного вузла та загальний прогрес розгортання.

Отже, розробка власної утиліти на Rust замість використання стандартних засобів дозволила створити легковаговий, безпечний та адаптований під конкретну ARM-інфраструктуру інструмент. Це підтвердило можливість використання Rust для автоматизації розгортання в межах запропонованої інфраструктури.

Після визначення вимог до інфраструктури та вибору інструментів наступним етапом є безпосередня реалізація автоматизованого розгортання Kubernetes-кластера. На цьому етапі теоретичні положення реалізуються на практиці: підготовка вузлів, вибір системних налаштувань, ініціалізація кластера і забезпечення автоматичного приєднання до нього робочих вузлів.

Реалізація автоматизованого розгортання починається з фази попередньої перевірки (preflight). На цьому етапі інструмент підключається до кожного вузла через SSH, перевіряє відповідність процесорної архітектури заданому параметру (наприклад, ARM64), а також визначає стан файлу підкачки (swappiness). Ця фаза не вносить жодних змін до системи і дозволяє виявити проблеми з підключенням або невідповідність апаратних вимог ще до початку розгортання.

Після успішного проходження preflight починається базова підготовка серверів. На кожному вузлі має бути встановлена підтримувана операційна система (Linux архітектури ARM64) та налаштований мережевий доступ для віддаленого управління. Також необхідно виконати низку попередніх дій на рівні ядра ОС: налаштувати мережеву маршрутизацію (sysctl), повністю вимкнути файл підкачки (swappiness) та встановити контейнерне середовище виконання. Без виконання цих системних вимог ключові компоненти Kubernetes не зможуть працювати коректно [7].

На практиці ці підготовчі дії було автоматизовано за допомогою розробленого власного інструмента мовою Rust. Програма приймає задані діапазони IP-адрес під час запуску, автоматично розгортає їх у перелік окремих адрес та підключається до кожного вузла через протокол SSH для виконання налаштувань. За наявності відповідного прапорця конфігурації підготовка вузлів виконується паралельно. Інструмент підтримує запуск через інтерфейс командного рядка (CLI), що дозволяє адміністратору наочно відстежувати процес налаштування кожного комп'ютера. Перевага такого підходу полягає в тому, що всі дії є формалізованими і виконуються без ручного втручання.

Після підготовки операційної системи розроблений інструмент ініціює створення керуючої частини за допомогою офіційної утиліти `kubeadm` [18]. На цьому етапі автоматично виконуються службові дії, необхідні для початкової ініціалізації кластера, зокрема генеруються криптографічні сертифікати, формуються параметри конфігурації та розгортаються базові компоненти керування, зокрема API-сервер і `etcd`. Після успішного завершення ініціалізації скрипт автоматично отримує згенеровану команду приєднання та токен, що надалі використовуються для підключення робочих вузлів до кластера.

Наступним кроком є приєднання робочих вузлів. Розроблений інструмент автоматично передає згенерований токен на інші чотири комп'ютери Raspberry Pi та виконує на них команду `kubeadm join`. Завдяки цьому процес розгортання стає надзвичайно швидким і таким, що не потребує додаткових ручних дій. Особливо це важливо під час розробки та тестування, коли фізичний кластер може потребувати періодичного повного перерозгортання з нуля.

Після приєднання всіх робочих вузлів інструмент автоматично отримує файл `kubconfig` з керуючого вузла та зберігає його за вказаним шляхом на локальній машині адміністратора. Якщо в конфігурації задано назву кластера (`cluster_name`), вона автоматично підставляється у вміст `kubconfig`-файлу. Це дозволяє одразу після завершення розгортання працювати з кластером через `kubectl` без додаткових ручних дій.

Після створення базової структури кластера необхідно налаштувати мережевий плагін стандарту CNI (Container Network Interface), який підтримує архітектуру ARM. Без нього `Pods` не можуть отримувати IP-адреси та повноцінно взаємодіяти між собою, що є ключовою умовою функціонування Kubernetes [13]. Розроблений інструмент підтримує два CNI-плагіни: `Flannel` та `Calico`. Вибір конкретного плагіна задається через параметр конфігурації, а його встановлення виконується автоматично в процесі розгортання кластера.

Після встановлення CNI-плагіна інструмент переходить до фази розгортання додаткових компонентів кластера (`post-install`). Залежно від обраної конфігурації на цьому етапі автоматично встановлюються: балансувальник навантаження `MetalLB` з виділеним діапазоном IP-адрес для сервісів типу `LoadBalancer`, контролер вхідного трафіку `ingress-nginx`, постачальник класу сховищ (`local-path` для полегшеного локального зберігання або `Longhorn` для реплікованих блочних томів) та `metrics-server` для збору даних про використання ресурсів. Кожен із цих додатків є опціональним і активується відповідним параметром у `preset`-файлі або через CLI.

Після цього етапу інструмент автоматично здійснює фінальну перевірку працездатності кластера. На цьому етапі програма послідовно перевіряє готовність усіх вузлів (статус `Ready`), коректність запуску `CoreDNS` та `kube-proxy`, а також сканує кластер на наявність `Pods` у помилкових станах. Якщо система розгорнута правильно, усі компоненти керуючої частини і мережі працюють без помилок, і адміністратор отримує підсумковий звіт про стан кластера.

Варто зазначити, що використання власного програмного інструмента дозволяє не обмежуватися лише первинним створенням кластера. Завдяки підтримці IP-діапазонів архітектура інструмента враховує можливість масштабування кластера в майбутньому (додавання нових вузлів). Крім того, інструмент реалізує режим скидання кластера (`reset`), який дозволяє повністю або частково відновити вузли до початкового стану, що є особливо важливим під час розробки та тестування, коли фізичний кластер може потребувати періодичного повного перерозгортання з нуля.

Таким чином, реалізація автоматизованого розгортання включала попередню перевірку вузлів (`preflight`), підготовку апаратної бази, виконання системних налаштувань за допомогою `Rust`-інструмента, встановлення контейнерного середовища, ініціалізацію керуючого вузла, приєднання робочих вузлів і налаштування мережевого плагіна. Після цього було виконано фінальну перевірку працездатності кластера.

Висновки. У результаті дослідження принципів побудови та реалізації системи автоматизованого розгортання кластерного середовища була запропонована реалізація системи автоматизованого розгортання кластерного середовища Kubernetes на власній інфраструктурі і отримані наступні результати.

Досліджено архітектуру та механізми системи оркестрації Kubernetes. З'ясовано, що її декларативний підхід та розділення на керуючу частину та робочі вузли дозволяють автоматизувати управління тисячами контейнерів. Вбудовані механізми самовідновлення, горизонтального масштабування (HPA) та сувора політика мережевої безпеки (Network Policies, RBAC) роблять Kubernetes еталонним рішенням для мікросервісної архітектури.

Визначено та реалізовано вимоги до власної (on-premises) інфраструктури. Замість хмарних сервісів було спроектовано та зібрано фізичний міні-кластер на базі п'яти мікрокомп'ютерів Raspberry Pi 5 (по 8 ГБ оперативної пам'яті). Інфраструктуру розміщено у спеціалізованій стійці DeskPi RackMate T0, ізолювано через керований комутатор NetGear та забезпечено апаратною відмовостійкістю за допомогою джерела безперебійного живлення Atria.

Обґрунтовано вибір інструментів автоматизації. Замість використання сторонніх систем управління конфігураціями (таких як Ansible), з метою оптимізації під ARM-архітектуру та підвищення рівня безпеки (memory safety), було розроблено власний програмний інструмент мовою Rust для взаємодії з офіційною утилітою kubectl. Цей Rust-інструмент забезпечив паралельне підключення до вузлів через протокол SSH, конфігурацію операційних систем (вимкнення swappiness, налаштування ядра), встановлення контейнерного середовища, ініціалізацію керуючого вузла, автоматичне приєднання чотирьох робочих вузлів із застосуванням перехоплених токенів безпеки, розгортання CNI-плагіна (Flannel або Calico) та додаткових компонентів кластера (MetalLB, ingress-nginx, постачальник сховищ, metrics-server). Також реалізовано режим скидання кластера.

Результати практичних тестів підтвердили, що всі вузли перейшли в робочий статус, розгорнутий CNI-плагін забезпечив внутрішню мережеву маршрутизацію, а автоматизована тестова система успішно перевірила розгортання кластера в численних конфігураціях (обидва CNI-плагіни, різні комбінації додатків, паралельний та послідовний режими, користувацькі CIDR-діапазони), а також коректність часткового та повного скидання кластера.

Розроблений підхід до розгортання підтвердив практичну придатність для побудови локального Kubernetes-кластера в експериментальних умовах.

ЛІТЕРАТУРА:

1. Sturley H., Fournier A., Salcedo-Navarro A., Garcia-Pineda M., Segura-Garcia J. Virtualization vs. Containerization, a Comparative Approach for Application Deployment in the Computing Continuum Focused on the Edge / Future Internet. 2024. Vol. 16, No. 11, Article 427.
2. Придибайло О. Б., Придибайло Р. В. Роль контейнеризації у хмарних обчисленнях / Зв'язок. 2025. № 4. С. 92-98.
3. Pahl C., Jamshidi P., Zimmermann O. Cloud Container Technologies: A State-of-the-Art Review // IEEE Transactions on Cloud Computing. 2019. Vol. 7, No. 3. pp. 677–692.
4. IBM Cloud Education. *Cluster computing* [Електронний ресурс]. – URL: <https://www.ibm.com/topics/cluster-computing>
5. Red Hat. What is high availability? [Електронний ресурс]. – URL: <https://www.redhat.com/en/topics/linux/what-is-high-availability>
6. Kubernetes Documentation. Overview [Електронний ресурс]. – URL: <https://kubernetes.io/docs/concepts/overview/> (дата звернення: 23.01.2026)
7. Kubernetes Documentation. Kubernetes Components [Електронний ресурс]. – URL: <https://kubernetes.io/docs/concepts/overview/components/> (дата звернення: 23.01.2026)
8. Kubernetes Documentation. Pods [Електронний ресурс]. – URL: <https://kubernetes.io/docs/concepts/workloads/pods/>
9. Kubernetes Documentation. Deployments [Електронний ресурс]. – URL: <https://kubernetes.io/docs/concepts/workloads/controllers/deployment/>
10. Kubernetes Documentation. Service [Електронний ресурс]. – URL: <https://kubernetes.io/docs/concepts/services-networking/service/>
11. Linhuber, M., et al. On-Premise Kubernetes in Software Engineering Education: An Experience Report. TUM, 2026. URL: <https://aet.cit.tum.de/research/publications/linhuber2026icse-seet.pdf>

12. Kubernetes Documentation. Configuration [Електронний ресурс]. – URL: <https://kubernetes.io/docs/concepts/configuration/>
13. Souppaya M., Morello J., Scarfone K. Application Container Security Guide // NIST Special Publication 800-190. 2017. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf>
14. Kubernetes Documentation. Using RBAC Authorization [Електронний ресурс]. – URL: <https://kubernetes.io/docs/reference/access-authn-authz/rbac/>
15. Kubernetes Documentation. Network Policies [Електронний ресурс]. – URL: <https://kubernetes.io/docs/concepts/services-networking/network-policies/> (дата звернення: 23.01.2026)
16. Sharma V. Complete Guide to Kubernetes Networking // Scaler Topics. Last updated: 9 Jan 2024. URL: <https://www.scaler.com/topics/kubernetes/kubernetes-networking/> (дата звернення: 22.01.2026)
17. Hidayat A., Andi S. Automating Server Deployment With Ansible to Improve Performance, Virtualization, and Network Security // ResearchGate. 2025. pp.10618-10626. URL: <https://www.researchgate.net/publication/394960982> (дата звернення: 23.01.2026)
18. Kubernetes Documentation. Installing kubeadm [Електронний ресурс]. – URL: <https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/install-kubeadm/>

REFERENCES:

1. Sturley H., Fournier A., Salcedo-Navarro A., Garcia-Pineda M., Segura-Garcia J. Virtualization vs. Containerization, a Comparative Approach for Application Deployment in the Computing Continuum Focused on the Edge / Future Internet. 2024. Vol. 16, No. 11, Article 427.
2. Prydybailo O. B., Prydybailo R. V. (2025). Rol konteyneryzatsiyi u khmarnykh obchyslennyakh [Role of containerization in cloud computing]. Zvyazok, (4), pp.92–98.
3. Pahl C., Jamshidi P., Zimmermann O. Cloud Container Technologies: A State-of-the-Art Review // IEEE Transactions on Cloud Computing. 2019. Vol. 7, No. 3. pp. 677–692.
4. IBM Cloud Education. *Cluster computing*. URL: <https://www.ibm.com/topics/cluster-computing>
5. Red Hat. What is high availability? URL: <https://www.redhat.com/en/topics/linux/what-is-high-availability>
6. Kubernetes Documentation. Overview. URL: <https://kubernetes.io/docs/concepts/overview/>
7. Kubernetes Documentation. Kubernetes Components. URL: <https://kubernetes.io/docs/concepts/overview/components/>
8. Kubernetes Documentation. Pods. URL: <https://kubernetes.io/docs/concepts/workloads/pods/>
9. Kubernetes Documentation. Deployments. URL: <https://kubernetes.io/docs/concepts/workloads/controllers/deployment/>
10. Kubernetes Documentation. Service. URL: <https://kubernetes.io/docs/concepts/services-networking/service/>
11. Linhuber, M., et al. On-Premise Kubernetes in Software Engineering Education: An Experience Report. – TUM, 2026. URL: <https://aet.cit.tum.de/research/publications/linhuber2026icse-seet.pdf>
12. Kubernetes Documentation. Configuration. URL: <https://kubernetes.io/docs/concepts/configuration/>
13. Souppaya M., Morello J., Scarfone K. Application Container Security Guide // NIST Special Publication 800-190. 2017. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf>
14. Kubernetes Documentation. Using RBAC Authorization. URL: <https://kubernetes.io/docs/reference/access-authn-authz/rbac/>
15. Kubernetes Documentation. Network Policies. URL: <https://kubernetes.io/docs/concepts/services-networking/network-policies/>
16. Sharma V. Complete Guide to Kubernetes Networking // Scaler Topics. Last updated: 9 Jan 2024. URL: <https://www.scaler.com/topics/kubernetes/kubernetes-networking/>
17. Hidayat A., Andi S. Automating Server Deployment With Ansible to Improve Performance, Virtualization, and Network Security // ResearchGate. 2025. pp.10618-10626. URL: <https://www.researchgate.net/publication/394960982>
18. Kubernetes Documentation. Installing kubeadm [Електронний ресурс]. – URL: <https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/install-kubeadm/>

AUTOMATED CLUSTER ENVIRONMENT DEPLOYMENT SYSTEM

The article examines the issues of rapid deployment and maintenance of complex IT infrastructures under conditions of increasing workload or failures of individual components. It is shown that one of the effective approaches to deploying complex infrastructures is the use of container technologies in combination with cluster computing environments and container orchestration systems.

The paper analyzes the concept of containerization. It is demonstrated that this approach provides application isolation together with all required dependencies, ensuring software portability, consistent operation across different environments, and the possibility of automating deployment processes.

The main characteristics of cluster systems are considered. It is determined that combining independent computing nodes into a single logical network provides high availability, scalability, and fault tolerance. The principal characteristics of clusters, including scalability, fault tolerance, and load balancing, are analyzed. In addition, the networking requirements necessary for the operation of cluster environments are described.

It is shown that, for an automated cluster deployment system, the container-based model is the preferred approach because it enables rapid scaling, efficient resource utilization, and seamless integration with container orchestration platforms.

The Kubernetes container orchestration platform, which is used to automate the deployment, management, scaling, and maintenance of containerized applications, is analyzed. Its capability to efficiently manage a large number of containers in complex information systems is demonstrated.

For experimental evaluation, a practical implementation of an automated deployment and management system for containerization technologies in a Kubernetes cluster environment was proposed, described, implemented, and tested on the authors' own infrastructure.

Keywords: cluster computing environments, containerization, orchestration, Kubernetes, deployment automation, software applications.

АВТОМАТИЗОВАНА СИСТЕМА ІЗОЛЬОВАНИХ ІМІТАЦІЙНИХ СЕРЕДОВИЩ ДЛЯ ДОСЛІДЖЕННЯ КІБЕРЗАГРОЗ

У статті розглянуто питання застосування технологій Cyber Deception для дослідження сучасних кіберзагроз та аналізу дій потенційних кіберзловмисників. Обґрунтовано актуальність використання систем-приманок (honeypot) як ефективного засобу збору інформації про спроби несанкціонованого доступу до інформаційних систем, дослідження сучасних методів проведення кібератак та вдосконалення механізмів забезпечення кібербезпеки. Показано, що застосування технологій кіберобману дозволяє створювати контрольовані імітаційні середовища, у яких можливо досліджувати поведінку потенційних зловмисників без ризику компрометації реальної інформаційної інфраструктури.

Метою дослідження є аналіз технологій побудови ізольованих імітаційних середовищ та розроблення лабораторної системи для дослідження кіберзагроз із використанням honeypot-технологій. У роботі проведено аналіз сучасних підходів до побудови систем Cyber Deception, класифікації honeypot за рівнем взаємодії із зловмисником, особливостей їх використання в системах кібербезпеки, а також можливостей застосування таких систем у дослідницькому та навчальному процесах. Запропоновано архітектуру лабораторного середовища на базі віртуальної інфраструктури з використанням системи Cowrie, реалізовано автоматизований збір журналів подій та забезпечено можливість моніторингу спроб несанкціонованого доступу, фіксації процесів автентифікації, виконуваних команд і подальшого аналізу дій потенційних кіберзловмисників.

За результатами експериментальних досліджень встановлено, що переважна більшість зафіксованих атак має автоматизований характер і реалізується шляхом використання типових сценаріїв компрометації інформаційних систем, зокрема словникового підбору паролів, застосування стандартних облікових записів та виконання команд після успішної автентифікації. Показано, що використання honeypot забезпечує накопичення експериментальних даних про сучасні методи проведення кібератак, дозволяє досліджувати тактики та інструменти, які застосовують потенційні кіберзловмисники, а також підвищує ефективність аналізу журналів подій інформаційної безпеки.

Практична цінність роботи полягає у створенні лабораторного середовища, яке може використовуватися для проведення наукових досліджень у сфері кібербезпеки, тестування засобів виявлення атак, накопичення даних для вдосконалення механізмів моніторингу та реагування на кіберінциденти, а також під час підготовки фахівців з кібербезпеки. Запропоноване рішення може слугувати основою для подальшої інтеграції із системами класу SIEM, розширення функціональних можливостей лабораторних стендів і розвитку сучасних засобів проактивного захисту інформаційних систем.

Ключові слова: кібербезпека, інформаційна безпека, Cyber Deception, honeypot, кіберзагрози, аналіз атак, імітаційне середовище.

Вступ та постановка проблеми. У сучасних умовах цифрової трансформації більшість організацій зберігає критично важливі дані на серверних платформах, що робить їх привабливими цілями для кіберзлочинців. Зростання кількості кібератак, поява нових інструментів компрометації та постійне ускладнення їх реалізації вимагають удосконалення підходів до забезпечення кібербезпеки та своєчасного виявлення потенційних загроз.

Дослідження сучасних кібератак неможливе лише на основі теоретичних моделей. Для розуміння механізмів їх реалізації необхідно аналізувати практичні сценарії поведінки зловмисників у контрольованому середовищі. Саме тому в наукових дослідженнях і

навчальному процесі широко використовуються спеціалізовані лабораторні стенди, які дають змогу відтворювати типові сценарії атак, досліджувати їх перебіг та оцінювати ефективність засобів захисту.

Одним із найбільш поширених інструментів такого дослідження є технологія *honeypot*, що являє собою спеціалізований програмно-апаратний ресурс, котрий виконує роль приманки для потенційних зломисників. Зовні *honeypot* імітує функціонування реального сервера або іншого мережевого сервісу, створюючи у нападника враження про наявність вразливої системи. Під час взаємодії із цією системою всі дії зломисника фіксуються та реєструються для подальшого аналізу.

Отримані дані дають можливість досліджувати тактики, техніки та процедури, які використовують атакуючі, виявляти нові тенденції розвитку кіберзагроз і вдосконалювати механізми захисту інформаційних систем. Такий підхід забезпечує перехід від реактивних методів захисту до проактивного аналізу загроз, що особливо важливо в умовах постійної еволюції кіберзлочинної діяльності.

Аналіз останніх досліджень і публікацій. Питання виявлення, аналізу та прогнозування кіберзагроз активно досліджуються як у вітчизняній, так і в зарубіжній науковій літературі. Значна увага приділяється розробленню методів моніторингу мережевої активності, аналізу кіберінцидентів, побудові систем раннього виявлення атак і використанню спеціалізованих середовищ для дослідження поведінки зломисників.

У працях [1, 2] розглянуто базові принципи захисту інформації в мережевих середовищах, зокрема методи виявлення кіберзагроз, аналізу атак, контролю доступу та моніторингу мережевої інфраструктури. Представлені підходи формують теоретичне підґрунтя сучасних систем забезпечення інформаційної безпеки, включаючи засоби моніторингу, аудиту та управління подіями безпеки. Окрему увагу автори приділяють аналізу дій зломисників як важливому джерелу даних для підтримки прийняття рішень у сфері кібербезпеки.

У роботах [3, 4] досліджено питання управління ризиками, формування політик інформаційної безпеки, захисту мережевої інфраструктури, протидії кіберзагрозам, а також особливості побудови систем моніторингу та виявлення атак. Автори наголошують на доцільності постійного моніторингу дій зломисників з метою накопичення даних для вдосконалення механізмів виявлення та протидії сучасним кібератакам.

Праці [5, 6] присвячено комплексному дослідженню принципів побудови, впровадження та експлуатації систем виявлення і запобігання вторгненням (IDPS) у сучасних інформаційно-телекомунікаційних системах. У них наведено класифікацію IDPS за місцем розташування та способом аналізу подій, зокрема мережевих (NIDPS), хостових (HIDPS), бездротових (WIDPS) систем, а також систем аналізу поведінки мережі (NBA). Значну увагу приділено методам виявлення атак на основі сигнатурного аналізу, аналізу аномалій та специфікацій мережевих протоколів. Також у роботі наведено рекомендації щодо вибору архітектури системи з урахуванням особливостей інформаційної інфраструктури та вимог до забезпечення кібербезпеки.

У дослідженні [7] розглянуто проблему атрибуції кібератак, тобто визначення їхнього можливого джерела. Це завдання належить до найбільш складних у сфері кібербезпеки, оскільки сучасні кіберінциденти зазвичай характеризуються багаторівневою структурою та використанням різних механізмів приховування слідів атаки. Показано, що ефективне виявлення таких інцидентів і своєчасне реагування на них потребують комплексного аналізу даних із різних джерел, автоматизованої обробки подій безпеки та оцінювання ризиків у режимі реального часу.

У роботі [8] увагу зосереджено на використанні спеціалізованих систем-приманок (*honeypots*) для виявлення та дослідження дій потенційних зломисників. *Honeypot* розглядається як імітаційний інформаційний ресурс, який відтворює ознаки потенційно вразливої системи та стимулює взаємодію з боку атакуючих. Застосування таких рішень дає змогу не лише фіксувати факти несанкціонованої активності, а й отримувати детальну

інформацію про інструменти, тактики та методи, що використовуються під час проведення кібератак.

Незважаючи на значну кількість досліджень, присвячених системам виявлення вторгнень, платформам SIEM та технологіям *honeypot*, питання побудови комплексних лабораторних середовищ залишаються недостатньо висвітленими. Особливо це стосується рішень, які поєднують емуляцію кібератак, використання систем-приманок, централізований збір і кореляцію подій безпеки, а також їх подальший аналіз у навчальних і дослідницьких цілях. Саме ця обставина визначила напрям дослідження та обумовила необхідність розроблення відповідного лабораторного середовища.

Метою статті є дослідження технологій побудови ізольованих імітаційних середовищ та розроблення комплексної лабораторної системи для виявлення, моніторингу й аналізу кіберзагроз із використанням технології *honeypot* та засобів централізованого збору й аналізу подій інформаційної безпеки.

Виклад основного матеріалу. Сучасні інформаційні системи функціонують в умовах постійного зростання кількості та складності кіберзагроз. Зловмисники регулярно вдосконалюють інструменти та методи проведення атак, використовуючи нові способи отримання несанкціонованого доступу до інформаційних ресурсів, компрометації даних або порушення роботи цифрових сервісів. Різноманіття таких загроз охоплює кілька основних категорій, кожна з яких характеризується власними механізмами реалізації та потенційними наслідками для інформаційної безпеки.

Серед найбільш поширених загроз особливе місце займає шкідливе програмне забезпечення (Malware), до складу якого входять комп'ютерні віруси, троянські програми, шпигунське програмне забезпечення (Spyware) та програми-вимагачі (Ransomware). Функціональні можливості таких програм можуть істотно відрізнятися залежно від цілей атаки. Одні з них орієнтовані на викрадення облікових даних і конфіденційної інформації, інші забезпечують приховане керування скомпрометованою системою або порушують її нормальне функціонування. Окрему небезпеку становлять програми-вимагачі, які шифрують дані користувача та вимагають сплати викупу за відновлення доступу до них.

Окрему категорію кіберзагроз становлять розподілені атаки типу відмови в обслуговуванні (Distributed Denial of Service, DDoS), які є одними з найбільш поширених засобів порушення доступності інформаційних сервісів. Принцип їх реалізації полягає у формуванні великої кількості одночасних запитів до цільового ресурсу з множини скомпрометованих пристроїв. Унаслідок перевантаження обчислювальних і мережевих ресурсів сервер втрачає здатність обслуговувати легітимні запити користувачів, що призводить до часткового або повного припинення його функціонування.

Окрему групу загроз становлять вразливості програмного забезпечення, що виникають через помилки проектування, реалізації або налаштування інформаційних систем. Саме такі недоліки нерідко стають точкою входу для зловмисників. Їх експлуатація може призвести до отримання несанкціонованого доступу до ресурсів системи, виконання довільного програмного коду, розширення привілеїв користувача або порушення цілісності та доступності даних.

Практика останніх років свідчить, що зі зростанням складності кібератак традиційні засоби захисту вже не завжди здатні забезпечити необхідний рівень безпеки. Навіть за наявності антивірусного програмного забезпечення та мережевих засобів фільтрації частина атак залишається непоміченою або виявляється вже після компрометації системи. Тому дедалі більшого значення набувають проактивні підходи, орієнтовані не лише на виявлення та блокування загроз, а й на вивчення поведінки самих атакуючих. Дослідження тактик, технік і процедур, які використовуються під час атак, дає змогу краще розуміти механізми їх реалізації, своєчасно виявляти нові вектори компрометації та вдосконалювати засоби захисту.

У цьому контексті особливий інтерес становлять технології Cyber Deception (кіберобману), які дають можливість досліджувати дії потенційних зловмисників у контрольованому середовищі. На відміну від традиційних засобів захисту, основною метою

яких є запобігання несанкціонованому доступу, технології кіберобману створюють спеціально підготовлені об'єкти, що зовні не відрізняються від реальних серверів, сервісів або інформаційних ресурсів. Взаємодіючи з такими об'єктами, атакуючий фактично розкриває свої наміри, інструменти та методи роботи. Це дозволяє отримувати цінні дані про сценарії атак без ризику для реальної інформаційної інфраструктури.

Одним із найпоширеніших практичних інструментів реалізації концепції Cyber Deception є технологія honeypot. Такі системи виконують роль приманки, привертаючи увагу потенційних зломисників і фіксуючи їхню активність. Зібрані журнали подій та результати спостережень можуть використовуватися для вдосконалення механізмів виявлення атак, підвищення ефективності реагування на кіберінциденти, а також для навчання та підготовки фахівців у сфері кібербезпеки.

На сьогодні технології Cyber Deception реалізуються за допомогою кількох основних засобів (рис. 1):

- *Honeypot* – окремий інформаційний ресурс або сервер-приманка, призначений для виявлення та аналізу дій потенційних кіберзломисників.
- *Honeynet* – сукупність взаємопов'язаних систем-приманок, що імітують функціонування реального сегмента мережі та забезпечують дослідження складних сценаріїв кібератак.
- *Honeytokens* – спеціально створені цифрові артефакти (облікові записи, паролі, документи, ключі доступу тощо), використання яких свідчить про несанкціонований доступ до інформаційної системи.
- *Deception Files* (файли-приманки) – спеціально сформовані файли та каталоги, що імітують конфіденційну інформацію і призначені для виявлення несанкціонованих спроб доступу.



Рисунок 1 – Класифікація імітаційних систем у кібербезпеці

Основне призначення технологій кіберобману полягає у відверненні уваги потенційного зломисника від реальних інформаційних ресурсів і спрямуванні його дій до спеціально підготовленого контрольованого середовища. Такий підхід дає можливість простежити перебіг атаки на всіх її етапах, дослідити інструменти та методи, які використовує атакуючий, а також накопичити дані, необхідні для вдосконалення механізмів захисту інформаційних систем.

Серед рішень, що реалізують концепцію Cyber Deception, найбільш поширеними є системи *honeypot*. Вони широко застосовуються як у наукових дослідженнях, так і в практиці забезпечення кібербезпеки. Принцип їх роботи ґрунтується на створенні середовища, яке зовні

нагадує реальну інформаційну систему та спонукає атакуючого до активних дій. Будь-яка взаємодія з таким ресурсом реєструється, що створює можливість для подальшого аналізу застосованих інструментів, способів компрометації та характерних сценаріїв проведення атак.

Однією з ключових переваг honeypot є можливість спостерігати за діями зловмисника після проникнення до імітованого середовища. Якщо традиційні засоби захисту переважно орієнтовані на попередження або блокування атаки, то системи-приманки дозволяють вивчати весь ланцюг подій від моменту отримання доступу до виконання подальших дій у скомпрометованій системі. Завдяки цьому можна досліджувати використовувані інструменти, способи експлуатації вразливостей та логіку розвитку кіберінциденту.

Залежно від рівня взаємодії з атакуючим honeypot традиційно поділяють на дві основні категорії: системи низької взаємодії (Low-Interaction Honeypots) і системи високої взаємодії (High-Interaction Honeypots). Перший тип забезпечує емуляцію окремих сервісів або мережних протоколів і використовується переважно для виявлення масових та типових атак. Другий тип відтворює повноцінне програмне середовище, що дозволяє отримувати значно більше інформації про поведінку зловмисника та досліджувати складні сценарії компрометації. Водночас такі рішення потребують ретельнішої ізоляції та контролю через підвищений рівень ризику.

Системи низької взаємодії відтворюють лише окремі мережеві служби або протоколи, не надаючи зловмиснику доступу до повноцінного операційного середовища. Завдяки цьому вони залишаються відносно простими в розгортанні та супроводі, а також характеризуються нижчим рівнем ризику порівняно з рішеннями високої взаємодії.

Системи високої взаємодії імітують повноцінні операційні системи та дозволяють атакуючому взаємодіяти з ними майже так само, як із реальною системою. Такі системи дають можливість отримувати більш детальну інформацію про методи атак, але водночас потребують більш складного адміністрування.

Метою розроблення є створення автоматизованої системи ізольованих імітаційних цільових середовищ, призначеної для дослідження різних типів кіберзагроз у контрольованих умовах. Така система повинна відтворювати окремі елементи реальної інформаційної інфраструктури та забезпечувати реєстрацію дій потенційних зловмисників під час взаємодії з імітованими ресурсами.

Архітектура системи передбачає використання кількох взаємопов'язаних компонентів, які функціонують у межах ізольованої мережі. Такий підхід дає змогу безпечно відтворювати сценарії кібератак, спостерігати за поведінкою атакуючих та аналізувати наслідки їхніх дій без загрози для реальної інформаційної інфраструктури. Ізоляція середовища забезпечує контроль над перебігом експериментів і створює умови для дослідження як типових, так і більш складних сценаріїв компрометації інформаційних систем.

Основними компонентами запропонованої системи є:

- система віртуалізації;
- honeypot-сервер;
- система генерації атак;
- сервер збору логів;
- система аналізу отриманих даних.

Система віртуалізації використовується для створення лабораторного середовища, у якому розгортаються всі компоненти системи. Наприклад, можна використовувати платформу Oracle VirtualBox, яка дозволяє створювати віртуальні машини та налаштовувати ізольовані мережі [9].

Honeypot-сервер – це приманка. Він імітує реальний сервер і має виглядати для кіберзловмисника максимально цікавою здобиччю. Завдання такого сервера – заманити зловмисника і записувати кожен його крок.

Система генерації атак – це тестова система для перевірки захисту. Для цієї ролі була обрана система Kali Linux [10]. Вона стандартно містить доволі широкий набір інструментів для проведення тестів на проникнення.

Сервер збору логів (Log Server) – це таке собі сховище дій зломисника. Сюди стікається вся інформація про те, що відбувалося під час атак. По суті, це база для подальшого аналізу: хто заходив, які команди вводив і що намагався зламати [11].

Таким чином, запропонована архітектура автоматизованої системи для створення контрольованого середовища базується на використанні ізольованої мережі, у якій всі компоненти взаємодіють між собою (рис. 2).

На рисунку показана загальна схема: тут є вузол для атак на базі Kali Linux, сам Honeypot, сервер для логів (Log Server) і окрема частина для аналізу отриманих даних. У цій архітектурі honeypot-сервер – це центр усієї системи. Саме він приймає на себе всі з'єднання і фіксує, що там робить кіберзломисник. Kali Linux виступає в ролі агресора і проводить тестові атаки на honeypot-сервер, а в цей час сервер логування "тихо" збирає та фіксує всі події, що відбуваються в мережі.

Для реалізації сервера-приманки був обраний Honeypot-сервер Cowrie. Він добре імітує SSH та Telnet сервіси і дозволяє повністю записувати все, що робить атакуючий у системі [12].

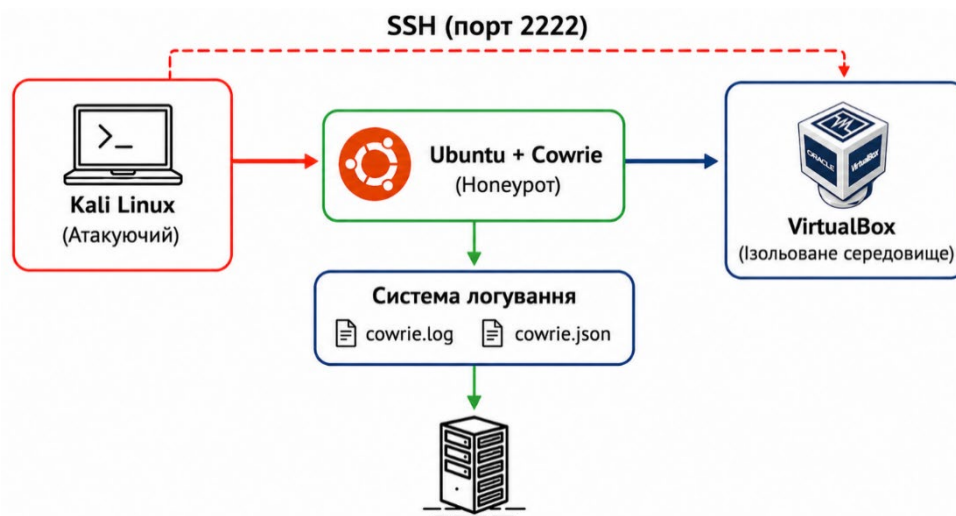


Рисунок 2 – Архітектура автоматизованої honeypot-системи

Встановлення та налаштування honeypot-системи [13].

Спочатку було встановлено ізольоване середовище Python (venv), що дозволило уникнути конфліктів пакетів. Процес встановлення:

```
git clone https://github.com/cowrie/cowrie
cd cowrie
python3 -m venv cowrie-env
source cowrie-env/bin/activate
pip install -upgrade pip
pip install -r requirements.txt
```

Після цього було встановлено тестові залежності за допомогою стандартного шаблону конфігурації: `cp etc/cowrie.cfg.dist etc/cowrie.cfg`.

У самому файлі `cowrie.cfg` було змінено кілька основних моментів – ім'я хосту, щоб сервер виглядав звичайно, а не як незвичайний або небезпечний. Також було зроблено налаштування параметрів емуляції SSH та перевірка запису логів, щоб їх було зручно переглядати та аналізувати. Сам сервер запускається через скрипт `bin/cowrie start`. За замовчуванням, він працює на порті 2222, тому була створена служба `systemd`, щоб система працювала автономно у фоні. Це усуває необхідність кожного разу запускати службу вручну після перезавантаження.

```
sudo systemctl daemon-reload
sudo systemctl enable cowrie
sudo systemctl start cowrie
```

Перевірка через `systemctl status cowrie` показала, що все поєдналось нормально, служба активна і працює у фоновому режимі.

Проведення тестових атак (рис. 3).

Для перевірки працездатності honeypot-системи були проведені тестові атаки з використанням Kali Linux. На першому етапі дослідження за допомогою Nmap були проскановані відкриті порти:

```
nmap -p 2222 <IP-адреса honeypot>
```

Результат сканування підтвердив наявність відкритого SSH-порту, що імітується honeypot-системою.

Далі було виконано атаку типу *brute-force* за допомогою утиліти Hydra:

```
hydra -l root -P passwords.txt ssh://<IP>:2222
```

Під час атаки виконувалися спроби підбору паролів із використанням словника. Honeypot-система не блокує доступ, а навпаки, дозволяє атакуючому "успішно" увійти в систему, імітуючи роботу реального сервера.

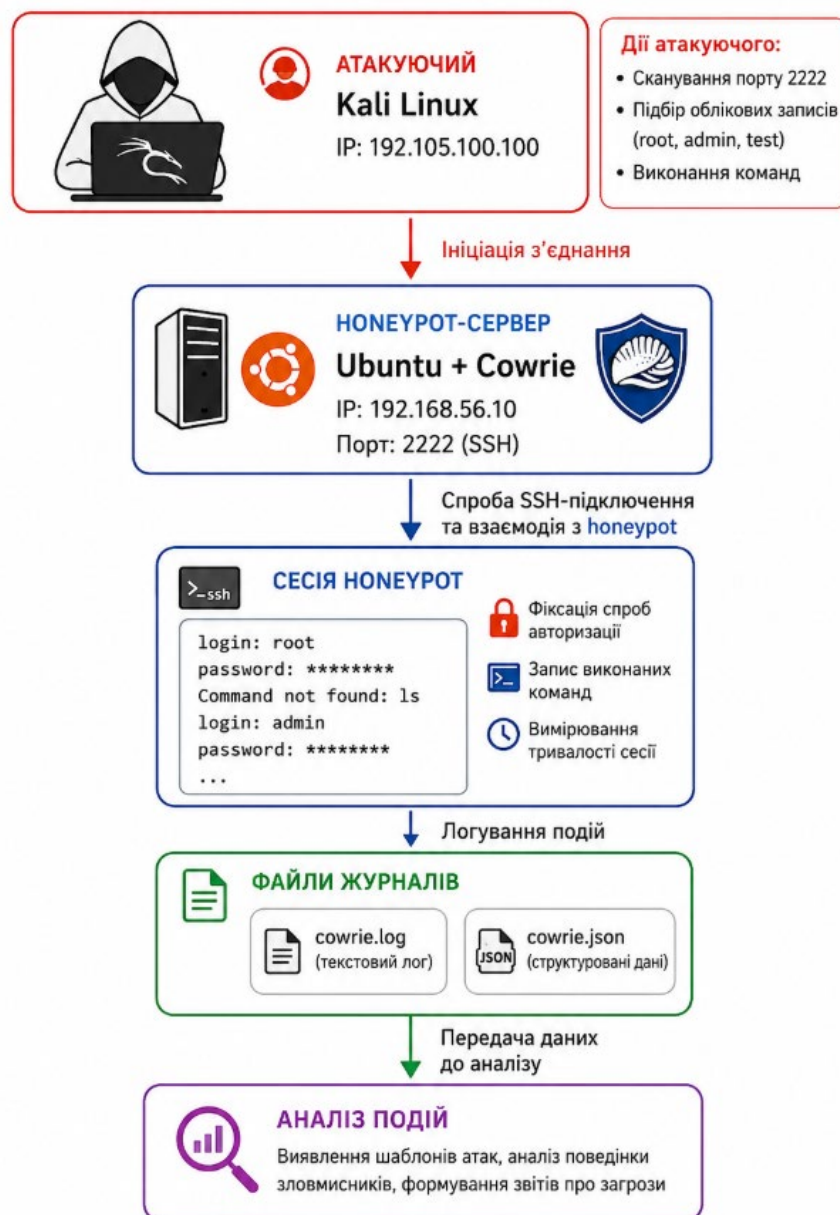


Рисунок 3 – Схема проведення тестової атаки та фіксації подій у honeypot-системі

Збір та аналіз журналів подій (рис. 4).

Однією з ключових функцій honeypot-системи є збір інформації про дії атакуючого. У системі Cowrie всі події записуються до двох основних журналів:

- cowrie.log – текстовий лог;
- cowrie.json – структурований лог у форматі JSON.

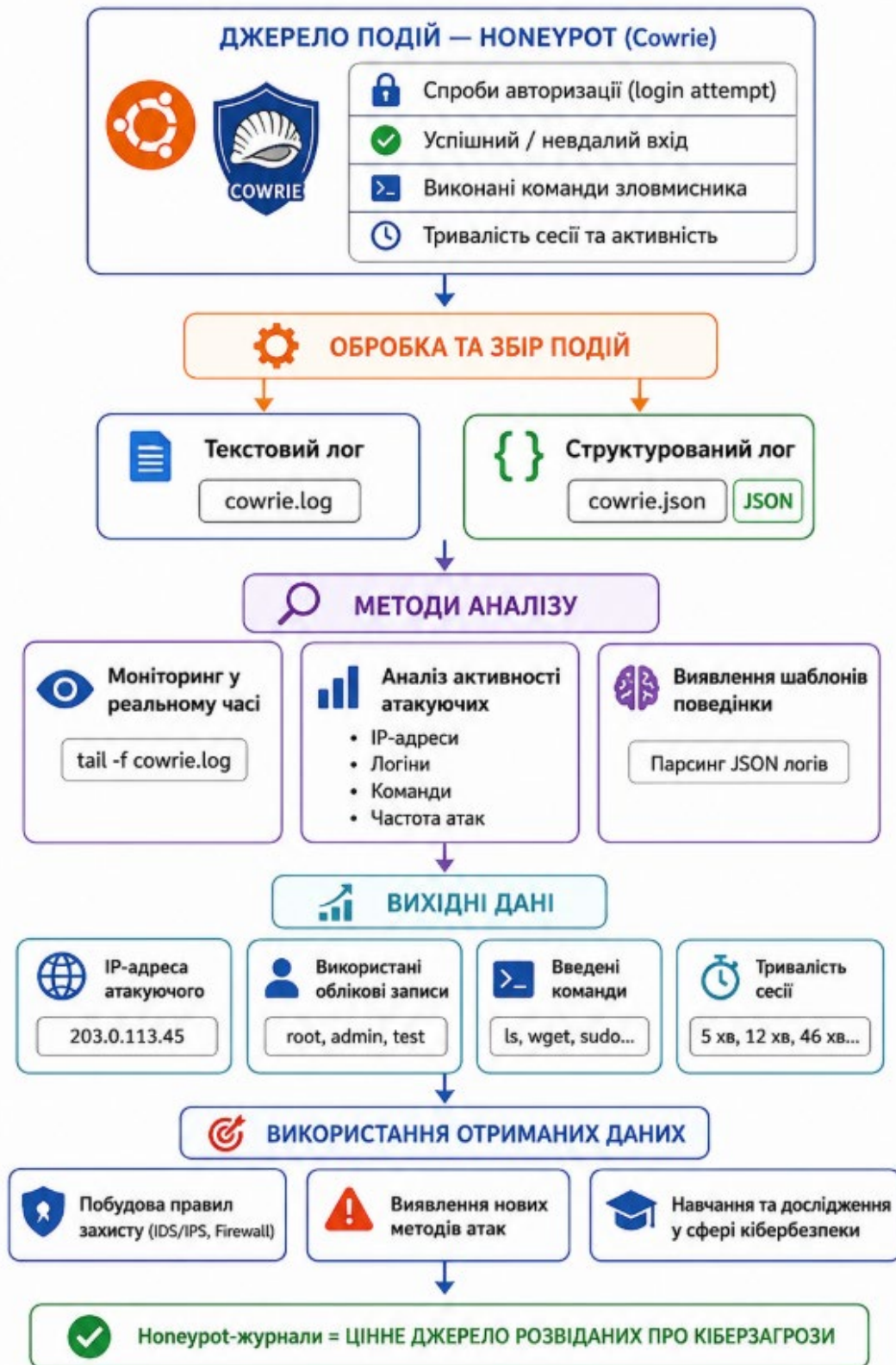


Рисунок 4 – Структура збору та аналізу журналів подій honeypot-системи

Для перегляду журналів у реальному часі використовується команда:

```
tail -f ~/cowrie/var/log/cowrie/cowrie.log
```

У журналах фіксуються такі події:

- IP-адреса атакуючого;
- спроби авторизації;
- використані логіни та паролі;
- введені команди;
- тривалість сесії;
- мережеві параметри підключення.

Завдяки цьому можна побачити повну картину дій зловмисника у системі.

Аналіз результатів експерименту.

У результаті проведених експериментальних досліджень було отримано інформацію про спроби несанкціонованого доступу до лабораторної honeypot-системи та особливості поведінки потенційних кіберзловмисників.

Аналіз зареєстрованих подій дав змогу встановити:

- наявність значної кількості спроб підключення до сервісу **SSH**;
- використання типових облікових записів, зокрема *root* та *admin*, під час спроб автентифікації;
- застосування словникових атак (Dictionary Attack) для автоматизованого підбору паролів;
- виконання команд операційної системи після успішної автентифікації, що свідчить про спроби подальшої компрометації інформаційної системи.

Отримані результати підтверджують, що більшість зафіксованих атак є автоматизованими та розгортаються за типовими сценаріями компрометації інформаційних систем. Завдяки honeypot вдалося детально зареєструвати кожен етап взаємодії зловмисника із системою – від спроб автентифікації та використаних облікових записів до виконаних команд і послідовності дій.

Дослідження довело ефективність honeypot як інструмента збору даних про сучасні кіберзагрози. Отримані експериментальні дані придатні для вдосконалення механізмів виявлення атак, розробки правил кореляції подій у SIEM-системах, посилення засобів захисту інформації та підготовки фахівців з кібербезпеки.

Автоматизація збору та аналізу журналів подій (рис. 5).

Щоб підвищити ефективність лабораторної системи, було налаштовано автоматизований збір і збереження журналів подій honeypot-системи Cowrie. Під час роботи система автоматично реєструє спроби несанкціонованого доступу, автентифікації, виконання команд та інші дії потенційних зловмисників.

Автоматизований збір логів дає змогу моніторити події в режимі реального часу, накопичувати історію кібератак та аналізувати поведінку нападників. Це створює підґрунтя для дослідження сучасних сценаріїв атак, виявлення індикаторів компрометації інформаційних систем і формування бази даних для подальших розробок.

Для забезпечення безперервного функціонування лабораторної системи використано механізми служби *systemd*, що дозволяють автоматизувати запуск сервісів, контролювати їх працездатність та забезпечувати автоматичне відновлення роботи після можливих збоїв.

Зібрані журнали подій слугують цінним джерелом даних для побудови систем виявлення кібератак, дослідження методів проникнення, удосконалення правил кореляції в SIEM-системах і навчання моделей кіберзахисту. Узагальнення та аналіз цих даних дають змогу своєчасно виявляти нові тенденції розвитку кіберзагроз і підвищувати ефективність захисних механізмів.

Отже, розроблена лабораторна система не лише автоматизує збір і реєстрацію подій інформаційної безпеки, а й створює основу для комплексного аналізу кібератак, удосконалення засобів виявлення загроз та розвитку технологій захисту.

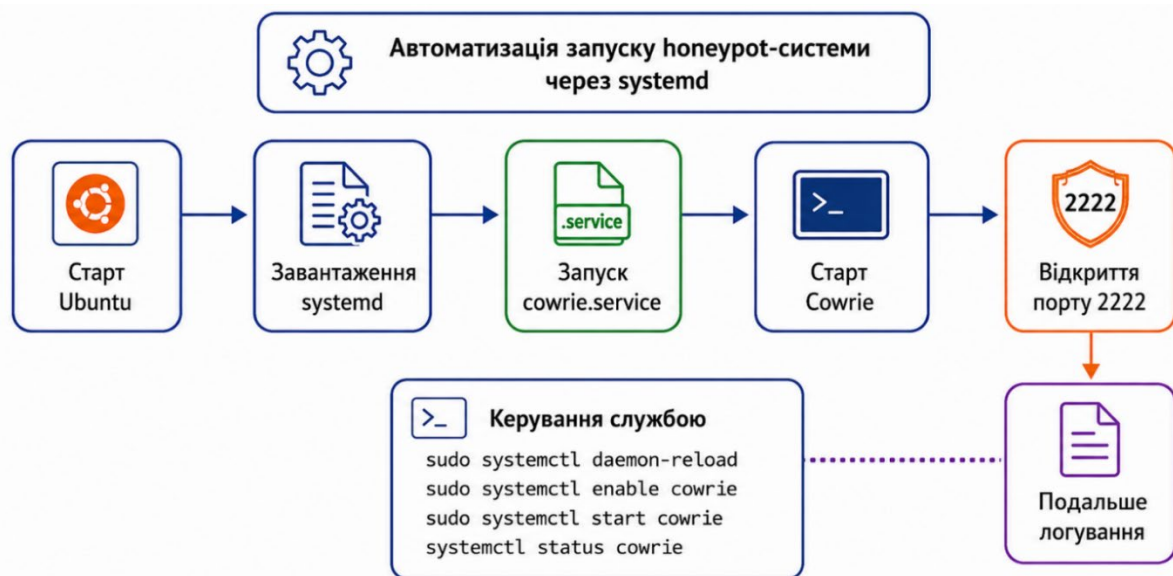


Рисунок 5 – Схема автоматизованого запуску honeypot-системи через *systemd*

Висновки. У роботі досліджено сучасні підходи до побудови ізольованих імітаційних середовищ для аналізу кіберзагроз, а також особливості застосування технологій Cyber Desorption у системах забезпечення кібербезпеки. Аналіз показав, що системи-приманки (honeypot) є ефективним інструментом проактивного виявлення та дослідження сучасних кібератак, що дає змогу збирати достовірні дані про тактики, техніки й процедури кіберзловмисників без ризику для реальної інформаційної інфраструктури.

У межах дослідження розроблено та реалізовано лабораторну систему на основі honeypot Cowrie, яка моделює мережеві сервіси, автоматизовано збирає журнали подій і дозволяє досліджувати поведінку потенційних зловмисників. Реалізована система реєструє спроби несанкціонованого доступу, фіксує процеси автентифікації, виконані команди та інші дії, характерні для розвитку кібератаки.

Експериментальні дослідження підтвердили працездатність запропонованого рішення. Переважна більшість зафіксованих атак має автоматизований характер і здійснюється за типовими сценаріями компрометації інформаційних систем – насамперед шляхом словникового підбору паролів та використання стандартних облікових записів. Отримані результати демонструють ефективність honeypot для дослідження сучасних методів несанкціонованого доступу та накопичення експериментальних даних про кіберінциденти.

Практична цінність роботи полягає у створенні лабораторного середовища, придатного для дослідження нових кіберзагроз, тестування засобів виявлення атак, удосконалення правил кореляції подій у SIEM-системах, а також для використання у навчальному процесі під час підготовки фахівців з кібербезпеки.

Перспективним напрямом подальших досліджень вважаємо інтеграцію розробленої honeypot-системи із сучасними платформами моніторингу та управління подіями інформаційної безпеки (SIEM), застосування методів машинного навчання для автоматичного аналізу журналів подій, а також розширення функціональних можливостей лабораторного середовища шляхом реалізації багаторівневої архітектури.

ЛІТЕРАТУРА:

1. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. New York : Pearson, 2017. 456 p.
2. Bishop M. Computer Security: Art and Science. 2nd ed. Boston : Addison-Wesley, 2019. 1312 p.
3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis : John Wiley & Sons, 2020. 1200 p.

4. Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5): National Institute of Standards and Technology. 2020. 492 p.
5. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS): NIST Special Publication 800-94. Gaithersburg: National Institute of Standards and Technology, 2007. 127 p.
6. Skoudis E., Liston T. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. 2nd ed. Upper Saddle River: Prentice Hall, 2005. 784 p.
7. Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2014. 320 p.
8. Spitzner L. Honeypots: Tracking Hackers. Boston: Addison-Wesley, 2002. 480 p.
9. Oracle VM VirtualBox User Manual: official documentation. URL: <https://www.virtualbox.org/manual/>.
10. Kali Linux Documentation: official website. URL: <https://www.kali.org/docs/>.
11. Lyon G. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. URL: <https://nmap.org>.
12. Cowrie Honeypot Documentation: documentation project. URL: <https://cowrie.readthedocs.io>.
13. OWASP Foundation. Web Security Testing Guide (WSTG): official project page. URL: <https://owasp.org/www-project-web-security-testing-guide/>.

REFERENCES:

1. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. New York : Pearson, 2017. 456 p.
2. Bishop M. Computer Security: Art and Science. 2nd ed. Boston : Addison-Wesley, 2019. 1312 p.
3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis : John Wiley & Sons, 2020. 1200 p.
4. Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5): National Institute of Standards and Technology. 2020. 492 p.
5. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS): NIST Special Publication 800-94. Gaithersburg: National Institute of Standards and Technology, 2007. 127 p.
6. Skoudis E., Liston T. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. 2nd ed. Upper Saddle River: Prentice Hall, 2005. 784 p.
7. Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2014. 320 p.
8. Spitzner L. Honeypots: Tracking Hackers. Boston: Addison-Wesley, 2002. 480 p.
9. Oracle VM VirtualBox User Manual: official documentation. URL: <https://www.virtualbox.org/manual/>.
10. Kali Linux Documentation: official website. URL: <https://www.kali.org/docs/>.
11. Lyon G. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. URL: <https://nmap.org>.
12. Cowrie Honeypot Documentation: documentation project. URL: <https://cowrie.readthedocs.io>.
13. OWASP Foundation. Web Security Testing Guide (WSTG): official project page. URL: <https://owasp.org/www-project-web-security-testing-guide/>.

PhD Hakhovych S., Babuch T., PhD Savchenko T., Derkach E.

AUTOMATED SYSTEM OF ISOLATED EMULATION ENVIRONMENTS FOR CYBER THREAT RESEARCH

The article examines the application of Cyber Deception technologies for the investigation of modern cyber threats and the analysis of the behavior of potential cyber attackers. The relevance of using honeypot systems as an effective tool for collecting information on unauthorized access attempts, studying contemporary cyberattack techniques, and improving cybersecurity mechanisms is substantiated. It is demonstrated that Cyber Deception technologies enable the creation of controlled emulation environments in which the behavior of potential attackers can be investigated without compromising real information infrastructure.

The purpose of this study is to analyze technologies for constructing isolated emulation environments and to develop a laboratory system for cyber threat research based on honeypot technologies. The paper presents an analysis of current approaches to the development of Cyber Deception systems, the classification of honeypots according to the level of attacker interaction, the specific features of their application in cybersecurity systems, and their potential use in research and educational activities. An architecture of a laboratory environment based on a virtual infrastructure using the Cowrie honeypot system is proposed. The developed solution provides automated event log collection and enables continuous monitoring of unauthorized access attempts, authentication processes, executed commands, and subsequent analysis of attacker activities.

Experimental evaluation demonstrated that the vast majority of recorded attacks were automated and followed common compromise scenarios, including dictionary-based password guessing, the use of default user accounts, and command execution after successful authentication. The results confirm that the proposed honeypot environment effectively accumulates experimental data on contemporary cyberattack techniques, facilitates the investigation of attacker tactics and tools, and improves the efficiency of security event log analysis. The collected data provide valuable information for understanding attacker behavior and identifying emerging attack patterns that can be used to enhance cybersecurity strategies.

The practical significance of the proposed approach lies in the development of a laboratory environment suitable for cybersecurity research, evaluation of attack detection mechanisms, accumulation of experimental datasets for improving security monitoring and incident response processes, and practical training of cybersecurity specialists. Furthermore, the proposed solution can serve as a foundation for future integration with Security Information and Event Management (SIEM) platforms, expansion of laboratory cyber ranges, and further development of proactive information security technologies.

Keywords: cybersecurity, information security, Cyber Deception, honeypot, cyber threats, attack analysis, emulation environment.

СИСТЕМА АВТОМАТИЗОВАНОГО КОНТРОЛЮ ВІДПОВІДНОСТІ КОНФІГУРАЦІЙ МЕРЕЖЕВИХ ПРИСТРОЇВ ВИМОГАМ КІБЕРБЕЗПЕКИ

Збільшення кількості підключених пристроїв, різноманіття й ускладнення мережеских топологій та постійний розвиток кіберзагроз дуже ускладнюють адміністрування мережевого обладнання. Налаштування десятків або сотень маршрутизаторів і комутаторів вручну є трудомістким, дорогим і пов'язаним з високим ризиком кіберзагроз. Саме помилки конфігурації є причиною успіху більшості кібератак. Метою дослідження є розроблення та практична апробація системи для автоматизованої валідації конфігурацій мережеских пристроїв. Зокрема, система має автоматично ідентифікувати фізичну топологію мережі, перевіряти відповідність налаштувань галузевим стандартам безпеки та автоматизовано усувати виявлені вразливості.

Систему реалізовано мовою Python за допомогою бібліотек Netmiko та PyVis. Для отримання інформації про топологію застосовано протокол LLDP (IEEE 802.1AB). Перевірку конфігурацій здійснено відповідно до 10 правил CIS Benchmark для Cisco IOS. Апробацію системи здійснено на віртуальному стенді GNS3, що складався з маршрутизаторів Cisco IOS, класифікованих у зони безпеки (Access, Restricted, DMZ) з динамічною маршрутизацією OSPF.

Модуль аудиту виявив низку вразливих налаштувань (зокрема, активованій Telnet), внаслідок чого початкова оцінка відповідності стандартам безпеки склала 85%. Після автоматизованого застосування виправлень та генерації розширених списків контролю доступу (ACL) оцінку підвищено до 100%. Крім цього, система успішно заблокувала спробу несанкціонованого доступу з зони Restricted до сервера баз даних, що підтвердило коректність згенерованих політик фільтрації.

Запропоноване рішення значною мірою скорочує час проведення аудиту, усуває вплив суб'єктивного людського чинника та гарантує послідовне впровадження заходів безпеки. Отримані результати дослідження підтверджують, що принципи NetDevOps досить ефективно працюють при розв'язанні задач забезпечення захисту реальних мереж.

Ключові слова: автоматизація адміністрування; аудит безпеки; списки контролю доступу; CIS Benchmark; NetDevOps; сегментація мережі; Zero Trust; мережескі пристрої

Вступ та постановка проблеми. Мережева інфраструктура є основою функціонування будь-яких компаній. Зростання кількості підключених пристроїв, складність топологій та еволюція кіберзагроз є новими викликами для адміністраторів мереж. Ручне налаштування десятків або сотень різних маршрутизаторів і комутаторів не тільки займає багато часу, але й є дорогим. Це основна причина критичних неправильних конфігурацій, що в більшості випадків призводять до успішних кібератак. У практиці адміністрування такі помилки часто виникають не через брак знань, а через людський чинник, коли одну й ту саму дію доводиться виконувати багаторазово, зокрема, вручну.

Відповідно до звіту Verizon Data Breach Investigations Report [1], понад 80 % порушень безпеки мережевої інфраструктури ґрунтуються на неправильній конфігурації обладнання або використанні застарілих протоколів управління. Яскравим прикладом цього є протокол Telnet, облікові дані якого передаються у відкритому форматі, який досі зустрічається в корпоративних мережах попри наявність безпечних альтернатив. Недостатня сегментація мережі за функціональними зонами безпеки та погано налаштовані правила фільтрації трафіку дають зловмисникам надто легкий доступ. Після первинного проникнення вони здатні вільно пересуватися інфраструктурою організації. Відтак, контроль конфігураційних налаштувань виходить за межі простої технічної задачі. Це ще й значний організаційний виклик, адже його ефективність прямо пропорційна регулярності проведених перевірок.

Для забезпечення справді високого рівня безпеки у сучасних мережах необхідно автоматизувати рутинні адміністративні завдання. До них належать інвентаризація, збір топологічних даних та, звичайно ж, перевірка конфігураційних налаштувань. Концепція NetDevOps, що успішно перейняла найкращі практики DevOps, пропонує розглядати мережеву інфраструктуру як своєрідний код – "Infrastructure as Code". Це дозволяє автоматично тестувати, версіювати та розгортати її. Проте, на практиці, реалії часто демонструють, що втілити цей підхід на практиці не завжди є можливим. Багато обладнання та чинних процесів і досі прив'язані до традиційного, ручного адміністрування, що неминуче породжує серйозні перешкоди на шляху до повної автоматизації.

Метою статті є обґрунтування архітектури та детальне представлення результатів її практичного випробування. Йдеться про автоматизовану валідацію конфігурацій мережевих пристроїв, яка інтегрує кілька ключових функцій: збір даних про фізичну топологію, перевірку на відповідність стандартам CIS Benchmark [2] та, що особливо важливо, автоматизоване виправлення виявлених невідповідностей відповідно до визначених політик безпеки. Запропонований цілісний підхід, який ми пропонуємо покликаний відчутно зменшити операційні ризики, зробити інфраструктуру значно прозорішою та мінімізувати час, необхідний для ліквідації виявлених вразливостей. Водночас авторами підкреслюється, що систему варто розглядати не як повноцінну заміну кваліфікованого адміністратора, а радше як потужний інструмент підтримки його рішень, здатний ефективно виконувати рутинні, стандартні перевірки.

Для досягнення мети, поставлено кілька завдань:

- Детально порівняти існуючі методи фільтрації трафіку та різноманітні засоби автоматизації конфігурування мережевих систем.
- Розробити та реалізувати програмні модулі, що відповідають за збір топології мережі, проведення аудиту, а також автоматизоване усунення виявлених недоліків.
- Провести експериментальну перевірку ефективності створеної системи на підготовленому віртуальному стенді.

Практична цінність полягає у створенні програмного рішення для адміністрування, котре не тільки автоматизує складні перевірки безпеки, але й суттєво спрощує виконання численних рутинних завдань, пов'язаних із налаштуванням і підтримкою мережевої інфраструктури.

Огляд літератури (аналіз останніх досліджень та публікацій). Проблема автоматизованої валідації конфігурацій мережевого обладнання попри численні дослідження, залишається актуальною та досі не знайшла свого остаточного розв'язання. Така ситуація беззаперечно підкреслює нагальну потребу в ґрунтовній систематизації вже існуючих наукових напрацювань. Саме ретельний аналіз останніх публікацій та досліджень дозволив ідентифікувати кілька ключових, взаємопов'язаних векторів наукового пошуку.

Одним із таких напрямів, який привертає значну увагу дослідників, є мережі на основі намірів (Intent-Based Networking, IBN). У межах цього підходу автоматизація конфігурації трактується як трансформація політик високого рівня в перевірені та оптимальні налаштування мережевих пристроїв. Слід зазначити, що оглядові дослідження [3] виявили: ключовою перешкодою для IBN дотепер залишається саме верифікація та уникнення конфліктів політик, а не лише їхнє елементарне розгортання. Ця принципово важлива теза отримала подальший розвиток у пізніших працях, які пропонували методи для ідентифікації конфліктів та гарантування когерентності намірів упродовж усього життєвого циклу конфігурації [4]. Проте, глибокий аналіз доступних літературних джерел переконливо свідчить, що більшість подібних комплексних рішень здебільшого орієнтовані на промислові контролери, інтеграція котрих виявляється винятково трудомісткою, що, своєю чергою, значно обмежує їхню практичну імплементацію в інфраструктурах меншого масштабу.

Другий напрям досліджень охоплює автоматизацію конфігурування та контроль відповідності (compliance). Існує вагома доказова база, яка свідчить про те, що програмне забезпечення, призначене для автоматичного застосування та перевірки конфігурацій, здатне значно зменшити кількість помилок, а також істотно скоротити витрати праці

адміністраторів [5]. Водночас інші автори зазначають, що використання інструментів штучного інтелекту в процесах конфігурації та контролю відповідності відкриває абсолютно нові можливості, але вимагає розробки надійних засобів валідації згенерованих налаштувань [6, 7]. Це підтверджує ключову тезу, згідно з якою автоматизація, позбавлена етапу ретельної перевірки відповідності стандартам, є об'єктивно неповною та потенційно небезпечною.

Третій напрям тісно пов'язаний з концепцією Zero Trust (нульової довіри) та мікросегментацією, що розглядаються як нова модель мережевої безпеки. Огляд літератури чітко встановив основні тенденції та проблеми, що виникають при впровадженні архітектури Zero Trust у різних секторах; він також підтвердив нагальну вимогу жорсткої сегментації доступу між сегментами мережі [8]. Дослідники мікросегментації переконані, що поділ інфраструктури на ізольовані зони з неухильним дотриманням політики найменших привілеїв є надзвичайно ефективним засобом стримування латерального переміщення злоумисника всередині мережі [9]. Саме ці фундаментальні засади сформували підґрунтя для розробленої чотиризонної моделі сегментації, що застосована у цьому дослідженні.

Підсумовуючи викладене, слід з упевненістю констатувати: незважаючи на значний обсяг виконаних робіт у царині автоматизації мережевого адміністрування та зміцнення її безпеки, проблема повної інтеграції трьох критично важливих аспектів: автоматизованого збору відомостей про фізичну топологію, деталізованої перевірки конфігурації згідно з визнаними стандартами (наприклад, CIS Benchmark) та автоматичного застосування коригувальних списків контролю доступу (ACL) в межах єдиного інструменту, що адаптований для потреб невеликих та середніх корпоративних інфраструктур, і надалі залишається актуальною та не вирішеною. Отже, у цій статті ми представляємо результати нашого дослідження, що має на меті ефективно ліквідувати цю прогалину.

Методи дослідження. Методологічну основу дослідження становить поєднання аналізу предметної області та експериментального проєктування програмної системи. Нижче схарактеризовано теоретичні засади (методи фільтрації трафіку, технології автоматизації та стандарти захисту) і склад розробленої системи.

Методи фільтрації трафіку та списки контролю доступу. Для забезпечення безпеки сучасних комп'ютерних мереж необхідне комплексне рішення, і одним із найважливіших його елементів є контроль потоку трафіку між різними секціями мережі. Фільтрація мережевого трафіку – це практика аналізу пакетів під час їх проходження через мережевий пристрій (маршрутизатор або комутатор L3), щоб визначити, чи слід їх передавати далі або блокувати відповідно до заздалегідь визначених правил.

Основним і найпоширенішим інструментом для фільтрації на пристроях Cisco IOS є списки контролю доступу (ACL). ACL – це набір правил (permit/deny). Принципово важливим є те, що правила перевіряються зверху вниз послідовно, і перевірка зупиняється, як тільки знайдено відповідність пакету до правила. Крім того, наприкінці кожного ACL Cisco IOS неявно додає правило "deny all", за яким весь трафік, що не відповідає жодному явному дозволу, блокується.

Залежно від рівня деталізації фільтрації, ACL можна класифікувати на два основних типи. Стандартні ACL (Standard ACL, номери 1–99 та 1300–1999) забезпечують аналіз лише IP-адреси джерела пакету і є досить простими у впровадженні. Через свої обмеження вони в основному використовуються для контролю доступу до самих пристроїв або у специфічних сценаріях маршрутизації. Розширені ACL (Extended ACL, номери 100–199 та 2000–2699) пропонують значно більшу гнучкість: вони дозволяють фільтрувати пакети одночасно за IP-адресами джерела та призначення, за протоколом (IP, ICMP, TCP, UDP, OSPF тощо), а також за номерами портів TCP/UDP для визначення конкретних сервісів та додатків.

Ефективна реалізація сегментації мережі передбачає розподіл інфраструктури на ізольовані зони безпеки з різними рівнями привілеїв доступу. У цій роботі застосовується чотиризонна модель:

OSPF Area 0 (Core) – магістральна зона маршрутизації, що з'єднує всі інші зони;
Access – зона доступу для корпоративних користувачів, мережа 10.0.10.0/24;

Restricted – зона обмеженого доступу з підвищеними вимогами безпеки, мережа 10.0.30.0/24;

DMZ (Demilitarized Zone) – демілітаризована зона для зовнішньо доступних серверів, мережі 10.0.40.0/24–10.0.42.0/24.

Впровадження ACL дотримується принципу найменших привілеїв, що є ключовим елементом концепції Zero Trust Security. Відповідно до цього принципу, кожен мережевий вузол або сегмент повинен мати доступ лише до ресурсів, необхідних для виконання його функцій (табл. 1). Весь інший трафік забороняється за замовчуванням.

Таблиця 1 – Функціональні зони безпеки випробувального стенду

Зона / сегмент	Адресний простір	Призначення	Політика доступу
Core (OSPF Area 0)	10.10.10.0/30 – 10.10.12.0/30	Магістральна маршрутизація між зонами	Автентифікація OSPF MD5
Access	10.0.20.0/24 – 10.0.21.0/24	Робочі місця корпоративних користувачів (PC1, PC2)	Стандартний доступ
Restricted	10.0.30.0/24	Вузол з підвищеними вимогами (PC3)	Обмежений доступ через ACL
DMZ	10.0.40.0/24 – 10.0.42.0/24	Зовнішньо доступні сервери (WEB, REDIS, DB)	Фільтрація вхідного трафіку

Технології автоматизації налаштування мережевих пристроїв. Коли інфраструктура масштабується, класичний спосіб управління мережею через інтерфейс командного рядка в реальному часі стає нежиттєздатним. Управління навіть кількома десятками пристроїв у такий спосіб є трудомістким і схильним до помилок, що не забезпечує необхідної швидкості реагування на інциденти. Сучасна парадигма NetDevOps надає різноманітні технологічні рішення для автоматизації мережевого адміністрування.

Ansible є однією з найпопулярніших платформ автоматизації, заснованою на декларативних плейбуках YAML. Вона не потребує агентів на цільових пристроях і може застосовуватися на широкому спектрі мережевого обладнання. Її реалізація вимагає увімкнення SSH або REST API на стороні пристрою.

NETCONF/RESTCONF – стандартизовані протоколи управління мережею (RFC 6241 та RFC 8040), що забезпечують структурований, заснований на моделях даних спосіб взаємодії з обладнанням. Формальні моделі даних YANG використовуються для забезпечення однозначності та валідності конфігурацій. Однак ці протоколи підтримуються переважно на сучасних версіях ОС мережевого обладнання.

У цій статті обрано підхід на основі Python-скриптів з використанням бібліотеки Netmiko з кількох причин. По-перше, Netmiko підтримує все обладнання Cisco IOS, яке може не підтримувати NETCONF. По-друге, Python добре підходить для обробки неструктурованих текстових виводів CLI за допомогою регулярних виразів.

Архітектура взаємодії системи з мережевим обладнанням налаштована таким чином: Python-скрипт ініціює окрему SSH-сесію до кожного цільового вузла через бібліотеку Netmiko, яка автоматично обробляє специфіку різних версій Cisco IOS. Далі виконується набір діагностичних команд (show lldp neighbors detail, show running-config тощо), а отриманий текстовий вивід обробляється регулярними виразами для виділення структурованих даних. Зібрані дані зберігаються у вигляді Python-словників та списків для подальшої обробки та візуалізації (рис. 2).

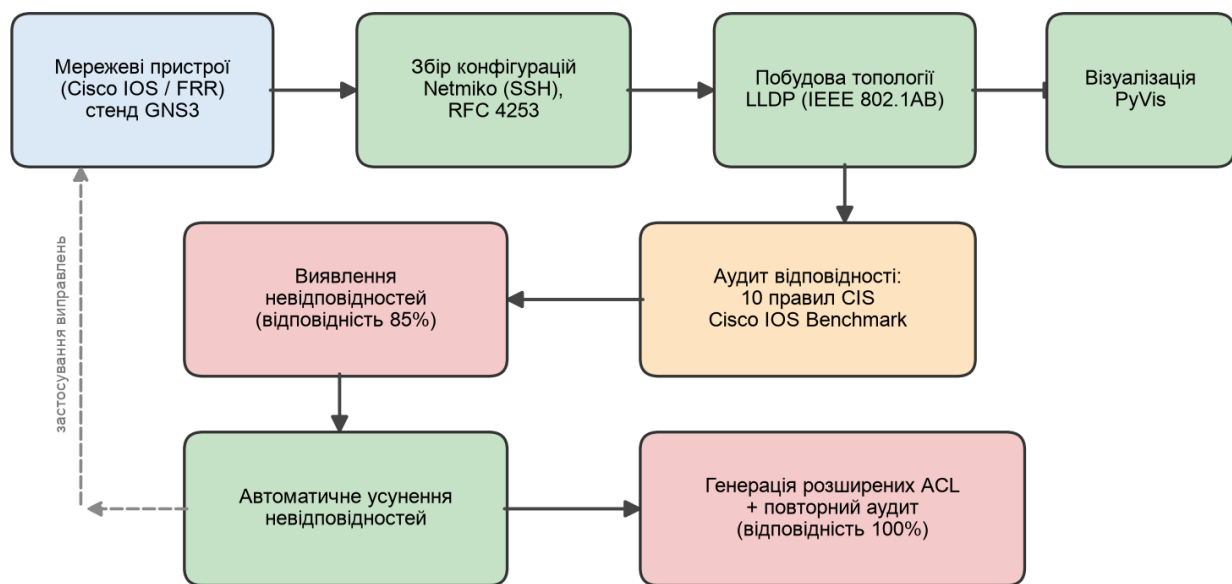


Рисунок 2 – Узагальнена архітектура системи автоматизованого контролю відповідності конфігурацій

Стандарти захисту інфраструктури та кращі практики. Однією з переваг автоматизованого підходу є можливість регулярної перевірки конфігурацій мережевого обладнання на відповідність визнаним галузевим стандартам безпеки. Провідним джерелом таких стандартів є CIS Benchmarks – великі технічні керівництва, розроблені провідними фахівцями у галузі кібербезпеки.

CIS Benchmark для Cisco IOS містить понад 80 підтверджених рекомендацій, що охоплюють усі аспекти безпечної конфігурації маршрутизаторів. Найбільш критичні вимоги, реалізовані в цій роботі.

Обов'язкове відключення протоколу Telnet (transport input none або transport input ssh) на всіх лініях VTY. Telnet передає облікові дані та дані сесії у незашифрованому вигляді, що робить його вразливим до атак типу Man-in-the-Middle.

Використання виключно протоколу SSHv2 [10] як захищеної альтернативи Telnet. SSHv2 забезпечує криптографічно стійке шифрування каналу зв'язку, автентифікацію та цілісність даних.

Захист площини управління (Control Plane Policing) для обмеження обсягу трафіку, спрямованого безпосередньо до процесора маршрутизатора.

Налаштування автоматичного виходу із сесії за неактивністю (exec-timeout), що мінімізує ризик несанкціонованого доступу до відкритої сесії.

Опис складових системи та використаних технологій. Побудована система є програмним комплексом, реалізованим мовою Python3, та складається з чотирьох функціональних модулів, кожен із яких виконує окреме завдання в рамках загального процесу аудиту та управління мережею. Модульна архітектура забезпечує незалежність компонентів та можливість їх окремого використання або розширення.

Перший модуль – модуль SSH-з'єднання та збору даних – відповідає за встановлення захищених сесій до мережевих вузлів і виконання діагностичних команд. Реалізований на базі бібліотеки Netmiko 4.x, яка надає уніфікований інтерфейс для роботи з обладнанням різних виробників та автоматично обробляє специфічні особливості різних версій Cisco IOS.

Другий модуль – модуль побудови та візуалізації топології – обробляє зібрані дані LLDP, формує граф мережевих з'єднань та генерує інтерактивну HTML-візуалізацію за допомогою бібліотеки PyVis 0.3.x [11], яка є Python-обгорткою над JavaScript-бібліотекою vis.js.

Третій модуль – модуль перевірки безпеки – перевіряє завантажені конфігурації пристроїв на відповідність контрольному списку вимог CIS Benchmark та формує структурований звіт про виявлені відхилення.

Четвертий модуль – модуль управління ACL – динамічно генерує розширені ACL відповідно до визначеної політики безпеки та застосовує їх до відповідних інтерфейсів маршрутизаторів через функцію `send_config_set()` бібліотеки Netmiko.

Для тестування системи використовувалося середовище GNS3 [12] – відкрита платформа емуляції мережевого обладнання. Стенд розгорнуто на базі маршрутизаторів FRR – відкритого рішення з підтримкою OSPF, BGP та інших протоколів маршрутизації. Такий підхід дозволяє відтворити реальну поведінку мережевого обладнання без потреби в образах Cisco IOS.

На рисунку 3 зображено головну сторінку (дашборд) веб-інтерфейсу системи SecureNet. У верхній частині відображається загальна статистика мережевої топології: 10 вузлів, 9 каналів зв'язку, 10 пристроїв, з яких 9 активні. Нижній блок призначений для управління Ansible-автоматизацією: кнопка "Запустити Ansible" ініціює виконання playbook `site.yml` через GNS3 API, а журнал виводу оновлюється у реальному часі через WebSocket-з'єднання (Flask-SocketIO).

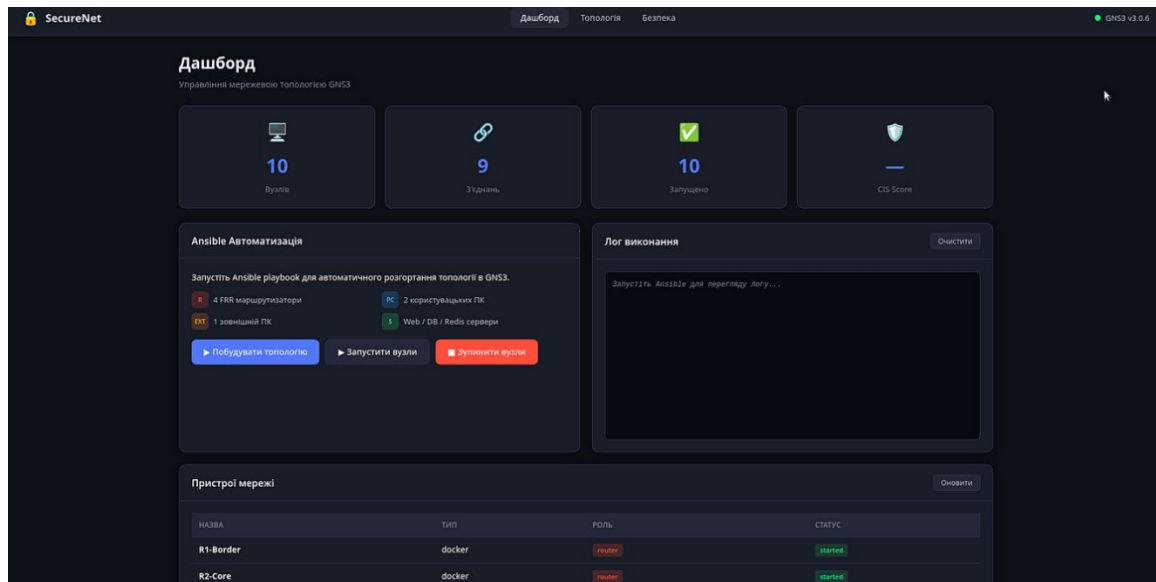


Рисунок 3 – Дашборд системи: статистика топології та блок Ansible-автоматизації

Результати. У цьому розділі викладено результати практичної реалізації та апробації системи за трьома функціональними напрямками: збір і візуалізація топології, автоматизований аудит безпеки та генерація і впровадження коригувальних ACL з подальшим розгортанням оновленої конфігурації.

Збір інформації про топологію та візуалізація зв'язків. Детальна, актуальна карта мережевих з'єднань є основою будь-якого аудиту та управління мережею. Стандартний підхід перевірки доступності через ICMP дає лише інформацію про логічну зв'язність третього рівня моделі OSI і є недостатнім для розуміння повного стану інфраструктури: фізичні з'єднання між пристроями не виявляються, конкретні порти підключення не ідентифікуються, ізольовані сегменти не визначаються.

Для вирішення цього завдання обрано відкритий стандарт IEEE 802.1AB – Link Layer Discovery Protocol. LLDP – це протокол канального рівня, через який мережеві пристрої оголошують свою ідентифікаційну інформацію та отримують аналогічні дані від безпосередньо підключених сусідів. На відміну від пропрієтарного Cisco Discovery Protocol, LLDP є відкритим стандартом, підтримується обладнанням різних виробників і не залежить від стану маршрутизації.

Топологічні дані збираються таким чином: система ініціює SSH-сесію до кожного пристрою зі списку цілей та виконує команду `show lldp neighbors detail`. Ця команда повертає детальну інформацію у форматі TLV про кожного сусіда, де ключовими полями є: System Name (ім'я сусіда), Chassis ID (MAC-адреса), Port ID (порт сусіда) та Local Interface (локальний порт підключення).

Для витягнення структурованих даних з текстового виводу CLI застосовуються регулярні вирази. Отримані пари "локальний порт – сусід – порт сусіда" утворюють ребра графа мережі. За допомогою бібліотеки PyVis будується інтерактивний HTML-граф топології, де вузли різних зон безпеки виділяються різними кольорами, а підписи на ребрах відображають назви портів підключення.

На рисунку 4 зображено список усіх 10 вузлів мережі SecureNet, що формується динамічно через GNS3 REST API. Перелік включає: 4 маршрутизатори на базі FRR (R1-Border, R2-Core, R3-Internal, R4-DMZ), 3 сервери Docker-контейнерів (Web-Server на nginx, DB-Server на PostgreSQL, Redis-Server), а також 3 кінцевих вузли VPCS (PC1-User, PC2-User, PC-External). Для кожного пристрою відображається тип, статус роботи та IP-адреса.

Назва	Тип	Роль	Статус
R1-Border	docker	router	started
R2-Core	docker	router	started
R3-Internal	docker	router	started
R4-DMZ	docker	router	started
Web-Server	docker	server	started
DB-Server	docker	server	started
Redis-Server	docker	server	started
PC-External	vpcs	external_pc	started
PC1-User	vpcs	user_pc	started
PC2-User	vpcs	user_pc	started

Рисунок 4 – Повний список пристроїв мережевої топології

На рисунку 5 зображено сторінку візуалізації мережевої топології, побудованої за допомогою бібліотеки D3.js на основі даних GNS3 API. Вузлами відображено всі 10 пристроїв, з'єднаних 9 каналами зв'язку. Центральну роль виконує R2-Core, до якого підключені: R1-Border (зовнішня мережа 192.168.100.0/24), R3-Internal (внутрішня мережа 10.10.20.0/24) та R4-DMZ (демілітаризована зона 10.10.30.0/24). Клікнувши на вузол, можна побачити деталі пристрою.

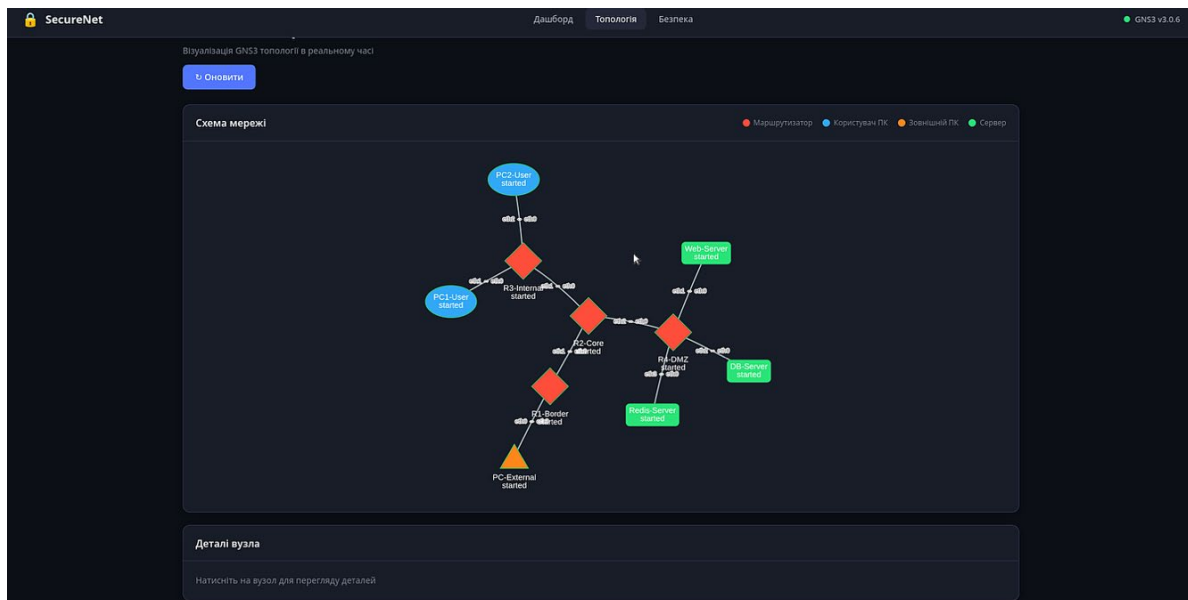


Рисунок 5 – Інтерактивна топологія мережі SecureNet

Результуюча візуалізація стенду наведена на рисунку 6. Топологія включає чотири маршрутизатори на базі FRR (R1–R4): R1 виконує роль ядрового маршрутизатора (Core/Distribution, OSPF Area 0), R2 обслуговує зону Access (мережі 10.0.20.0/24 та 10.0.21.0/24), R3 – зону Restricted (10.0.30.0/24), R4 – зону DMZ (10.0.40–42.0/24). У зоні Access розміщено два хости PC1 та PC2 (легітимні користувачі), у зоні Restricted – PC3 (хост "Зловмисник"). У зоні DMZ розгорнуто три сервери: SRV-WEB (PHP/Apache, 10.0.40.10), SRV-REDIS (Redis 7, 10.0.41.10) та SRV-DB (PostgreSQL 14, 10.0.42.10). Пунктирна лінія між R3 та PC3 позначає заблокований ACL-трафік.

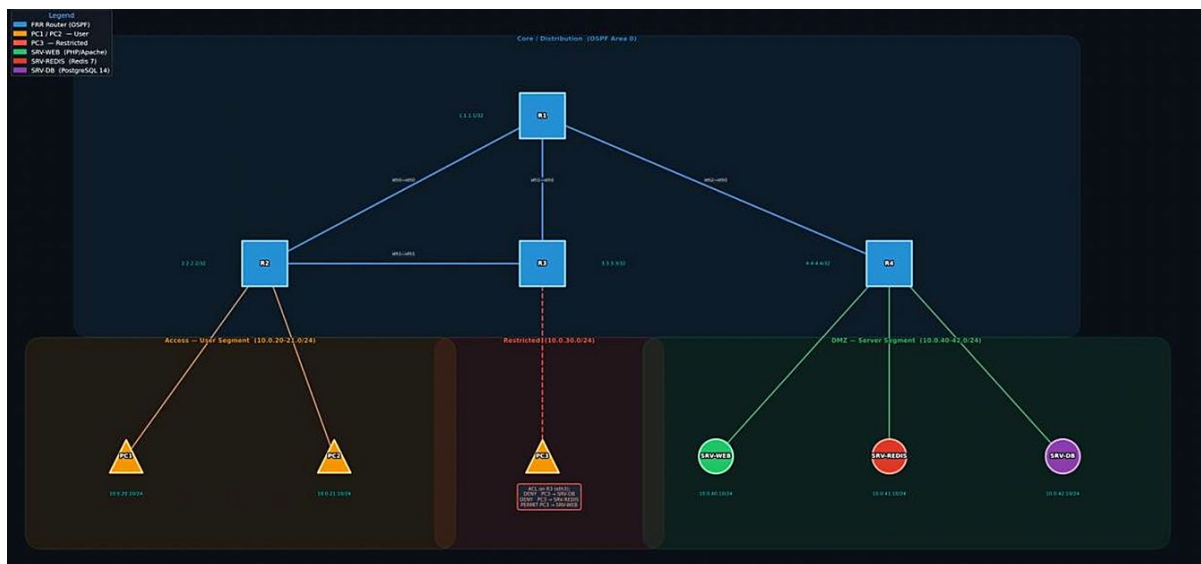


Рисунок 6 – Мережева топологія стенду (OSPF + зони безпеки + ACL)

Результатом роботи модуля є інтерактивна карта мережі, побудована на основі реальних LLDP-даних стенду. Топологія стенду включає чотири маршрутизатори на базі FRRouting: R1 виконує роль ядрового вузла (Core / OSPF Area 0) і з'єднаний з трьома граничними маршрутизаторами. R2 обслуговує зону Access (10.0.20–21.0/24) з хостами PC1 та PC2. R3 – зону Restricted (10.0.30.0/24) з хостом PC3, трафік якого фільтрується ACL. R4 – зону DMZ (10.0.40–42.0/24) з серверами SRV-WEB, SRV-REDIS та SRV-DB.

Зібрані LLDP-зв'язки між пристроями наведено у таблиці 2.

Таблиця 2 – Топологія мережі стенду, зібрана через LLDP

Пристрій А	Інтерфейс А	Пристрій В	Інтерфейс В
R1-Border	eth0	R2-Core	eth0
R1-Border	eth1	R3-Internal	eth0
R1-Border	eth2	R4-DMZ	eth0
R2-Core	eth1	R3-Internal	eth1
R3-Internal	eth3	PC3 (Restricted)	—
R4-DMZ	eth1	SRV-WEB / SRV-REDIS / SRV-DB	—

Автоматизована валідація конфігурацій. Модуль валідації безпеки формує аналітичне ядро розробленої системи. Його завданням є автоматизована перевірка конфігурацій мережевих пристроїв на відповідність попередньо визначеному набору вимог безпеки та формування звіту про виявлені порушення.

Процес валідації починається зі збору повної конфігурації кожного пристрою. Через SSH виконується команда `show running-config`, результат якої зберігається як рядок для подальшого аналізу. Аналіз виконується послідовним застосуванням чек-листу перевірок на базі стандарту CIS Benchmark для маршрутизаторів FRRouting.

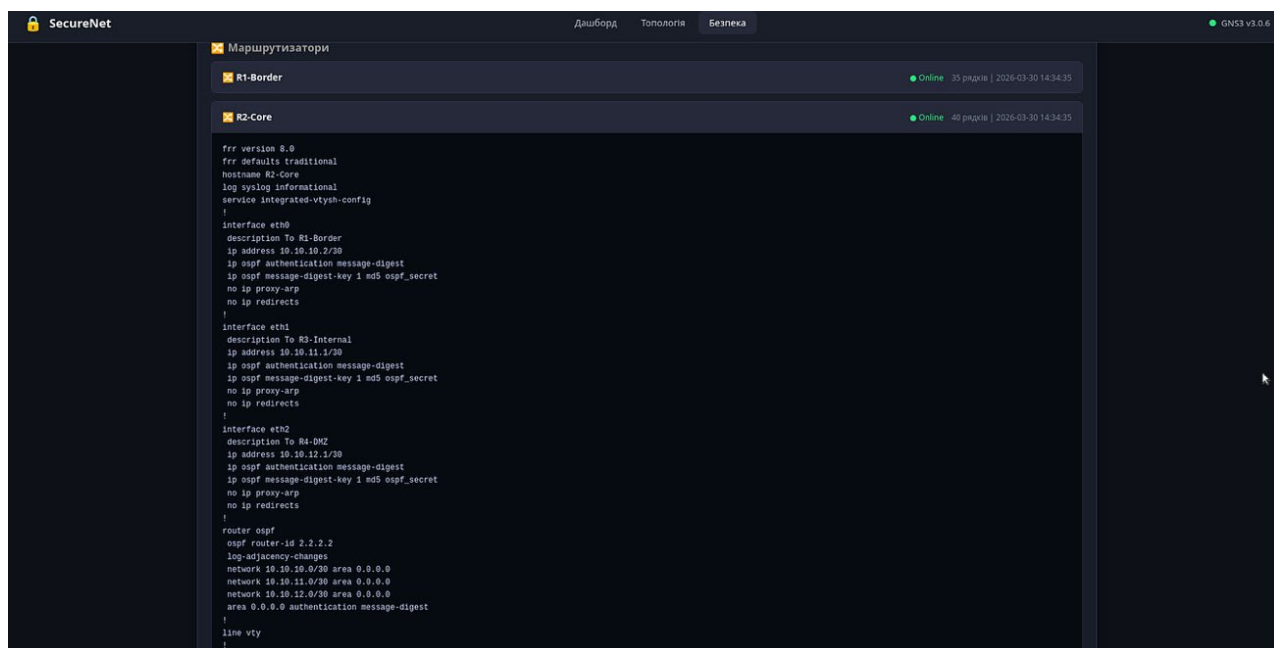


Рисунок 7 – Перегляд FRR-конфігурацій маршрутизаторів R1-Border та R2-Core

На рисунку 7 зображено розгорнуті конфігурації маршрутизаторів у форматі FRR (Free Range Routing), що збираються через GNS3 API з файлу `/etc/frr/frr.conf`. Конфігурація R1-Border містить: інтерфейси eth0/eth1 з OSPF MD5-автентифікацією, `passive-interface eth0`, мережі OSPF та розширений ACL BLOCK-EXTERNAL. Конфігурація R2-Core відображає початковий (небезпечний) стан: відсутній `passive-interface` та ACL – що відповідає правилам CIS-R5, R6, R7 зі статусом FAIL.

За результатами запуску системи 09.03.2026 о 14:21 (timestamp: 20260309_142110) для стенду з чотирьох маршрутизаторів (FRR-Router-1 – FRR-Router-4) отримано зведений звіт: із 40 перевірок (10 правил на 4 маршрутизаторах) 34 пройдено успішно (PASS), 6 – не пройдено (FAIL). Загальний індекс безпеки склав 85 балів зі 100. Детальні результати по кожному правилу наведено у таблиці 3.

Таблиця 3 – Перелік перевірок CIS Benchmark для Cisco IOS та підсумковий статус

ID	Правило CIS Benchmark	Критичність	Статус (після усунення)
CIS-R1	OSPF MD5 Authentication	критичний	ОК
CIS-R2	Logging Enabled	високий	ОК
CIS-R3	No IP Proxy-ARP	середній	ОК
CIS-R4	No IP Redirects	середній	ОК
CIS-R5	OSPF Passive Interface on LAN	високий	ОК
CIS-R6	ACL Configured	високий	ОК
CIS-R7	Telnet Blocked in ACL	критичний	ОК
CIS-R8	OSPF Router-ID Configured	середній	ОК
CIS-R9	Exec-timeout на лініях VTY	середній	ОК
CIS-R10	SSHv2 як транспорт керування	критичний	ОК

Аналіз результатів виявив одне критичне порушення (FAIL з пріоритетом HIGH), спільне для всіх чотирьох маршрутизаторів: відсутність ACL на граничних інтерфейсах (правило CIS-R5). Система автоматично сформувала конкретні команди для виправлення цього порушення. Правило CIS-R9 (SSH Management) позначено як WARN: хоча Telnet вимкнений, SSH-доступ також не налаштовано явно, що ускладнює захищене віддалене адміністрування. Ці результати підтверджують практичну цінність автоматизованого підходу – вручну перевірити 10 правил на 4 пристроях (40 перевірок) займає значно більше часу та є схильним до помилок.

Архітектура модуля розроблена з можливістю розширення: додавання нових перевірок зводиться до написання нового патерну пошуку та відповідного повідомлення без зміни базової логіки.

На рис. 8 зображено результати автоматизованого аудиту безпеки за 10 правилами CIS Benchmark до застосування виправлень. Загальний бал системи – 85%. R1-Border отримав 100% (еталонна конфігурація). R2-Core – 70% (7/10): відсутні passive-interface та ACL блокування telnet/TFTP. R3-Internal – 80% (8/10): відсутній ACL фільтр. R4-DMZ – 90% (9/10): у DMZ-IN відсутнє блокування telnet (порт 23). Виявлені порушення виділені червоним з детальним поясненням. Порівняння рівнів відповідності конфігурацій вимогам CIS Benchmark до та після автоматизованого усунення невідповідностей наведено на рис. 9.

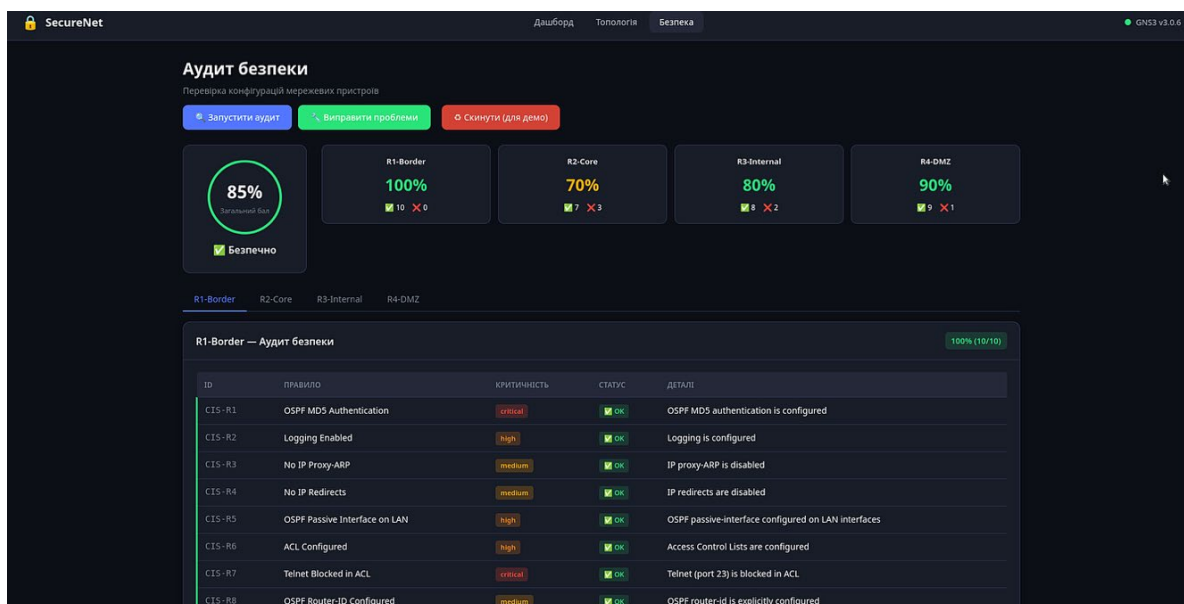


Рисунок 8 – Результати аудиту безпеки до застосування виправлень (85%)

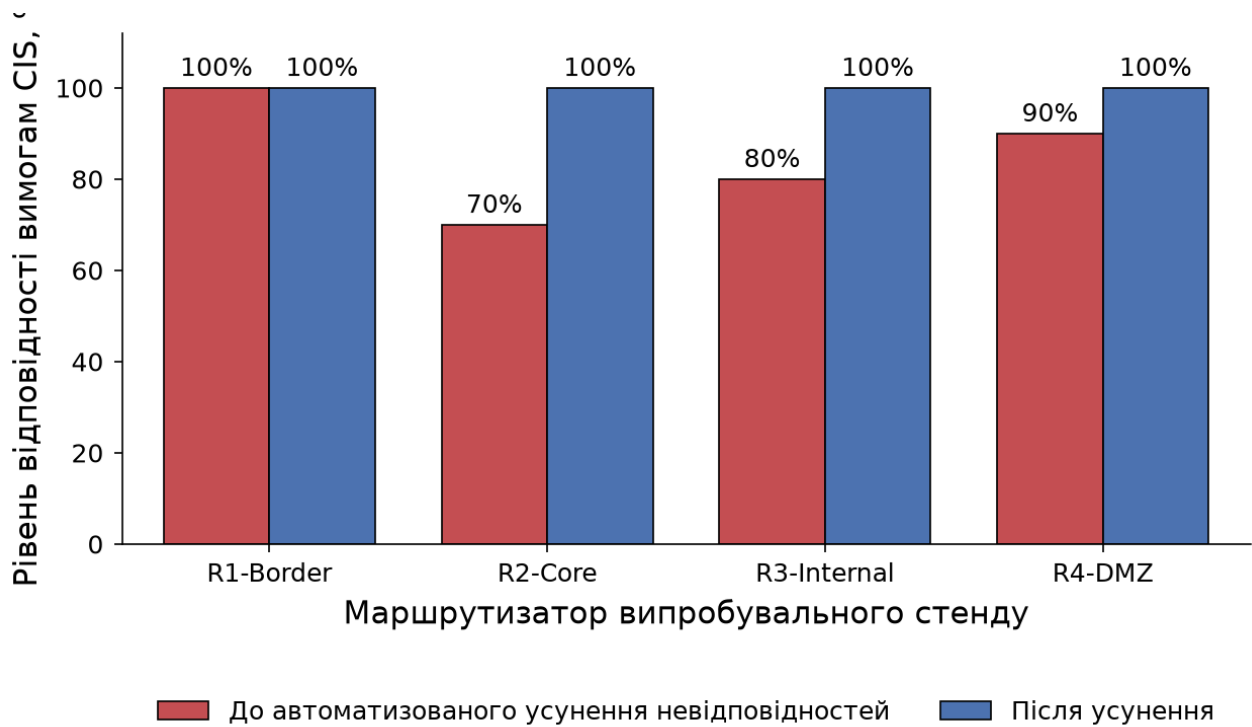


Рисунок 9 – Рівень відповідності конфігурацій вимогам CIS Benchmark до та після автоматизованого усунення невідповідностей

Генерація та впровадження розширених списків доступу. Модуль управління ACL реалізує повний цикл від визначення політики безпеки до її впровадження на мережевому обладнанні. Логіка генерації ACL побудована на основі попередньо визначеної матриці доступу між зонами.

Для зони Restricted, підключеної до маршрутизатора R3 з підмережею 10.0.30.0/24, визначено такі правила доступу до серверів у зоні DMZ (10.0.40–42.0/24):

Дозволити доступ до SRV-WEB (10.0.40.10) по протоколах HTTP (TCP 80) та HTTPS (TCP 443) – для забезпечення доступу до корпоративного вебпорталу;

Заблокувати будь-який доступ до SRV-DB (10.0.42.10) – сервер бази даних не повинен бути доступний безпосередньо для кінцевих користувачів;

Заблокувати будь-який доступ до SRV-REDIS (10.0.41.10) – сервер кешування є виключно внутрішнім компонентом;

Заблокувати весь інший трафік із зони Restricted до зони DMZ згідно принципу "deny all" за замовчуванням.

Система формує відповідний набір команд Cisco IOS та передає їх на маршрутизатор через метод `send_config_set()` бібліотеки Netmiko. Підтвердженням коректної роботи є результати тестування: ping від хоста "Зловмисник" (10.0.30.99) до SRV-DB (10.0.42.10) повертає "Destination Host Unreachable", тоді як легітимний хост із зони Access успішно відкриває з'єднання з SRV-WEB.

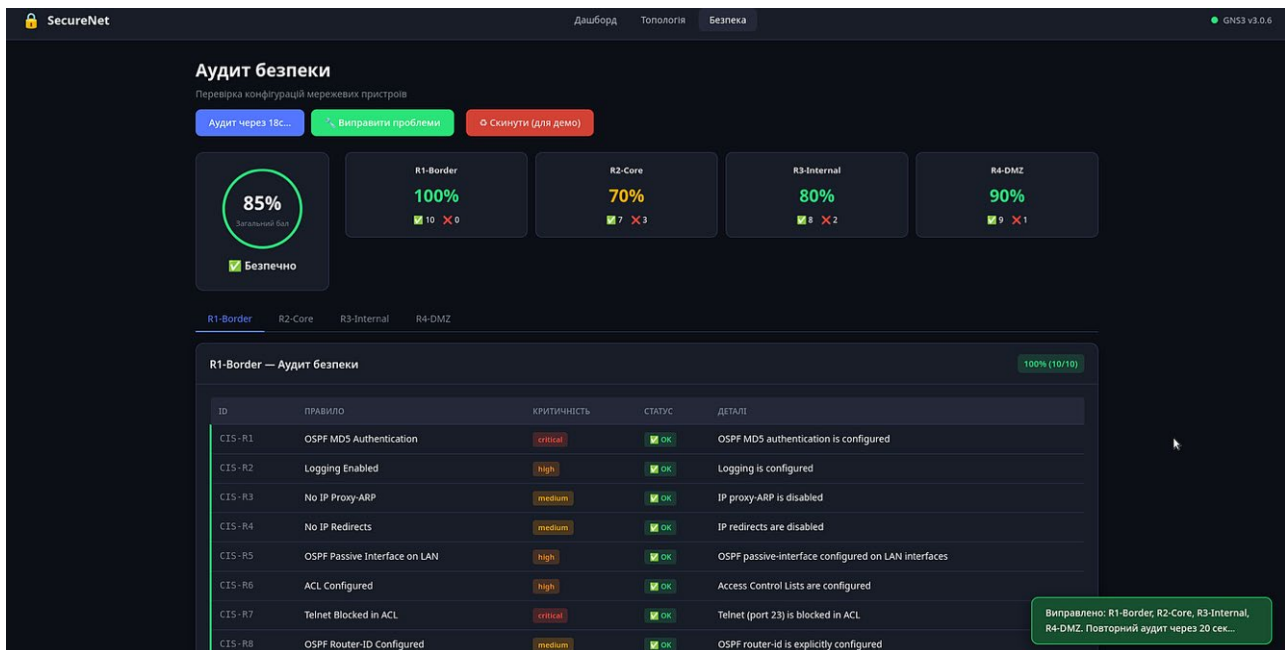


Рисунок 10 – Сповіщення про успішне застосування виправлень конфігурацій

На рисунку 10 зображено інтерфейс після натискання кнопки "Виправити проблеми". Toast-повідомлення підтверджує: "Виправлено: R2-Core, R3-Internal, R4-DMZ". Система автоматично завантажила захищені FRR-конфігурації через GNS3 API (POST /projects/{id}/nodes/{id}/files/etc/frr/frr.conf), перезапустила вузли для застосування змін та розпочала 20-секундний зворотний відлік перед автоматичним повторним запуском аудиту безпеки.

Розгортання нової конфігурації на наявній топології. Для апробації системи в умовах, максимально наближених до реального функціонування, у віртуальному середовищі GNS3 було розгорнуто детально пропрацьований віртуальний стенд. Його основу складають чотири маршрутизатори, що працюють на базі FRR (Free Range Routing): R1 виконує роль ядрового маршрутизатора (Core/Distribution) у магістральній зоні OSPF Area 0; R2 призначений для зони Access; R3 обслуговує зону Restricted; R4 функціонує як маршрутизатор зони DMZ. Хости PC1 та PC2 симулюють активність легітимних користувачів у зоні Access (підмережі 10.0.20.0/24 та 10.0.21.0/24), тоді як PC3 виступає в ролі потенційного зловмисника в зоні Restricted (10.0.30.0/24). У зоні DMZ було імплементовано три сервери: SRV-WEB (працює на базі PHP/Apache), SRV-REDIS та SRV-DB (з PostgreSQL 14).

Маршрутизація між цими зонами забезпечується за допомогою протоколу OSPF. R1 виступає центральним вузлом, який пов'язує R2, R3 та R4 через ключову зону Area 0. Після запуску емуляції первинним етапом є перевірка базової мережевої доступності між усіма елементами стенда шляхом надсилання ICMP-запитів. Позитивні відповіді на ці запити є підтвердженням коректності налаштувань OSPF, створюючи необхідну передумову для подальших етапів тестування.

Саме тестування проходило у три послідовні фази. На першому етапі на маршрутизаторі R1 навмисно залишено активний Telnet для імітації реальної вразливості. Після підключення системи та збору running-config модуль валідації виявляє цей факт і виводить попередження: "Warning: Telnet detected on device R1! CIS Benchmark violation".

На другому етапі система автоматично генерує та застосовує ACL на R3: забороняє трафік від PC3 до SRV-DB та SRV-REDIS, дозволяючи лише HTTP/HTTPS до SRV-WEB. Ping від PC3 до SRV-DB повертає "U.U.U" (Destination Unreachable), тоді як ping від PC1/PC2 до SRV-WEB завершується успішно. Пунктирна лінія на рисунку 6 наочно показує заблокований напрямок трафіку.

На третьому етапі система збирає LLDP-дані з усіх чотирьох маршрутизаторів та генерує HTML-файл з інтерактивним графом. Граф відображає ієрархічну структуру мережі: R1 у верхньому рівні, R2–R4 на рівні розподілу, хости та сервери в нижньому рівні, організовані в три чітко виділені кольором зони безпеки. Весь цикл займає менше трьох хвилин без будь-яких переривань у роботі мережі.

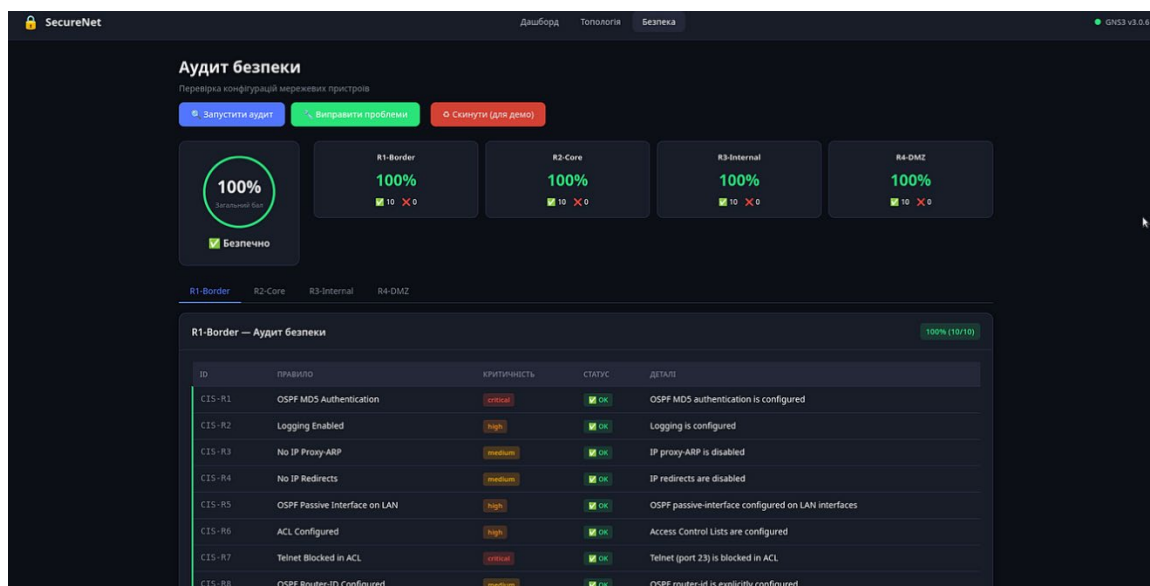


Рисунок 11 – Результати аудиту безпеки після виправлення (100%)

На рисунку 11 зображено результати аудиту безпеки після успішного застосування виправлених конфігурацій. Усі чотири маршрутизатори досягли максимального результату 100% (правила 10/10): R1-Border, R2-Core, R3-Internal, R4-DMZ. Загальний системний бал підвищився з 85% до 100%, а статус змінився з "Вразливий" на "Безпечний". Це підтверджує коректну роботу модуля автоматичного виправлення конфігурацій.

Висновки. Обговорення отриманих результатів доцільно проводити, спираючись на вищезгаданий огляд літератури. Отримані дані узгоджуються з висновками попередніх досліджень, які неодноразово підкреслювали, наскільки ефективно автоматизація конфігурацій здатна мінімізувати помилки адміністрування [5]. Саме тому, на наш погляд, цю статтю слід сприймати як доповнення до вже наявних знань. Вона свідчить, що поєднання аудиту за CIS Benchmark з автоматичною генерацією ACL може суттєво підвищити рівень безпеки: з 85% до 100% відповідно до прийнятої метрики відповідності. На нашу думку, це є вагомим аргументом на користь інтегрування етапу верифікації безпосередньо у цикл розгортання, що відповідає головній тезі дослідження мереж на основі намірів про пріоритет верифікації над простим застосуванням політики [3].

Практична реалізація чотиризонної моделі сегментації та підтверджене блокування несанкціонованого доступу між зонами Restricted і DMZ яскраво демонструють дієвість принципу найменших привілеїв, який у літературі розглядається як фундаментальна основа архітектури Zero Trust [8, 9]. Проте ми маємо одразу ж вказати на певні обмеження нашого дослідження: апробація відбувалася на віртуальному стенді GNS3 з вельми обмеженою кількістю вузлів, а контрольний список валідації охоплював лише 10 з понад 80 рекомендацій CIS Benchmark. Отже, отримані кількісні показники варто розглядати виключно як наочну демонстрацію ефективності запропонованого підходу, а не як універсальну та абсолютно точну оцінку безпеки.

Зважаючи на все вищевикладене, можна сформулювати низку ключових висновків.

Результатом нашого дослідження є розробка автоматизованої системи, призначеної для ретельної перевірки конфігурацій мережевих пристроїв. Таким чином, базуючись на отриманих результатах, ми можемо зробити кілька важливих тверджень.

У процесі вивчення предметної області проаналізовано механізми фільтрації мережевого трафіку та механізм розширених ACL на платформі Cisco IOS, а також охоплено сучасні технологічні стеки, призначені для автоматизації управління мережевим обладнанням, такі як Ansible, NETCONF, Netmiko/Python. Детально розглянуто всі вимоги стандарту CIS Benchmark для Cisco IOS. Вибір протоколу LLDP (IEEE 802.1AB) для збору даних про фізичну топологію мережі обґрунтовано його повною незалежністю від стану маршрутизації та відмінною сумісністю з обладнанням різних виробників.

Практичну реалізацію цієї системи виконано мовою програмування Python з використанням бібліотек Netmiko та PyVis, що дало змогу повністю автоматизувати збір топологічних даних через LLDP, їх подальше перетворення на структурований граф та, зрештою, генерацію інтерактивних HTML-візуалізацій мережі. Модуль аудиту безпеки продемонстрував вражаючу ефективність, успішно виявивши численні вразливі конфігурації, зокрема, активний протокол Telnet, що є прямим та очевидним порушенням стандарту CIS Benchmark.

Розроблена система пропонує три основні покращення, що значно виділяють її на тлі традиційного ручного адміністрування. По-перше, вона забезпечує скорочення часу, що необхідний для проведення аудиту безпеки. По-друге, повністю усувається суб'єктивний людський чинник у процесі перевірки конфігурацій, що гарантує об'єктивність. І, по-третє, система автоматизує застосування захисних політик, що забезпечує їхнє послідовне, безперервне та належне впровадження.

Подальший розвиток системи передбачає розширення контрольного списку валідації для охоплення абсолютно всіх вимог CIS Benchmark, інтеграцію з провідними системами моніторингу для миттєвого реагування на будь-які зміни конфігурацій у режимі реального часу, а також розробку інтелектуального механізму автоматичного виправлення виявлених вразливостей. Отримані результати доводять, що принципи NetDevOps у сфері мережевої безпеки залишаються актуальними та відкривають широкі перспективи.

ЛІТЕРАТУРА

1. Verizon. Data Breach Investigations Report. 2025. URL: <https://www.verizon.com/business/resources/reports/dbir/> (дата звернення: 10.03.2026).
2. CIS Cisco IOS Benchmark. Center for Internet Security. URL: <https://www.cisecurity.org/benchmark/cisco> (дата звернення: 10.03.2026).
3. Leivadeas A., Falkner M. A survey on intent-based networking. IEEE Communications Surveys & Tutorials. 2023. Vol. 25, No. 1. P. 625–655. DOI: 10.1109/COMST.2022.3215919.
4. Gharbaoui M., Sciarrone F., Fontana M., Castoldi P., Martini B. Assurance and conflict detection in intent-based networking: A comprehensive survey and insights on standards and open-source tools. IEEE Transactions on Network and Service Management. 2026. Vol. 23. P. 1891–1912. DOI: 10.1109/TNSM.2026.3651896.
5. Bajpai M. Automating network device configuration and compliance enforcement. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences. 2025. Vol. 7, No. 3. P. 1–6. DOI: 10.2139/ssrn.5057509.
6. Thati S. R. AI-driven automation for network configuration and compliance: Transforming enterprise security posture. World Journal of Advanced Research and Reviews. 2025. Vol. 26, No. 2. P. 1216–1223. DOI: 10.30574/wjarr.2025.26.2.1693.
7. Ficzero D., Varga P. AI-driven network configuration and operation. NOMS 2025 IEEE Network Operations and Management Symposium. IEEE, 2025. P. 1–4. DOI: 10.1109/NOMS57970.2025.11073726.
8. Mushtaq S., Mohsin M., Mushtaq M. A systematic literature review on the implementation and challenges of zero trust architecture across domains. Sensors. 2025. Vol. 25, No. 19. Art. 6118. DOI: 10.3390/s25196118.
9. Basta N., Ikram M., Kaafar M. A., Walker A. Towards a zero-trust micro-segmentation network security strategy: An evaluation framework. NOMS 2022 IEEE/IFIP Network Operations and Management Symposium. IEEE. 2022. P. 1–7. DOI: 10.1109/NOMS54207.2022.9789888.

10. Rescorla E., Ylonen T. RFC 4253: The Secure Shell (SSH) transport layer protocol. IETF, 2006. URL: <https://www.rfc-editor.org/rfc/rfc4253> (дата звернення: 10.03.2026).
11. PyVis documentation. PyVis. URL: <https://pyvis.readthedocs.io/en/latest/> (дата звернення: 10.03.2026).
12. GNS3 documentation. GNS3. URL: <https://docs.gns3.com/> (дата звернення: 10.03.2026).

REFERENCES

1. Verizon (2025) Data Breach Investigations Report. Available at: <https://www.verizon.com/business/resources/reports/dbir/>
2. Center for Internet Security (no date) CIS Cisco IOS Benchmark. Available at: <https://www.cisecurity.org/benchmark/cisco>
3. Leivadeas, A. and Falkner, M. (2023) 'A survey on intent-based networking', IEEE Communications Surveys & Tutorials, 25(1), pp. 625–655. <https://doi.org/10.1109/COMST.2022.3215919>
4. Gharbaoui, M., Sciarrone, F., Fontana, M., Castoldi, P. and Martini, B. (2026) 'Assurance and conflict detection in intent-based networking: a comprehensive survey and insights on standards and open-source tools', IEEE Transactions on Network and Service Management, 23, pp. 1891–1912. <https://doi.org/10.1109/TNSM.2026.3651896>
5. Bajpai, M. (2025) 'Automating network device configuration and compliance enforcement', SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.5057509>
6. Thati, S.R. (2025) 'AI-driven automation for network configuration and compliance: transforming enterprise security posture', World Journal of Advanced Research and Reviews, 26(2), pp. 1216–1223. <https://doi.org/10.30574/wjarr.2025.26.2.1693>
7. Ficzer, D. and Varga, P. (2025) 'AI-driven network configuration and operation', in NOMS 2025 IEEE Network Operations and Management Symposium. IEEE, pp. 1–4. <https://doi.org/10.1109/NOMS57970.2025.11073726>
8. Mushtaq, S., Mohsin, M. and Mushtaq, M. (2025) 'A systematic literature review on the implementation and challenges of zero trust architecture across domains', Sensors, 25(19), 6118. <https://doi.org/10.3390/s25196118>
9. Basta, N., Ikram, M., Kaafar, M.A. and Walker, A. (2022) 'Towards a zero-trust micro-segmentation network security strategy: an evaluation framework', in NOMS 2022 IEEE/IFIP Network Operations and Management Symposium. IEEE, pp. 1–7. <https://doi.org/10.1109/NOMS54207.2022.9789888>
10. Rescorla, E. and Ylonen, T. (2006) RFC 4253: The Secure Shell (SSH) Transport Layer Protocol. IETF. Available at: <https://www.rfc-editor.org/rfc/rfc4253>
11. PyVis (no date) PyVis documentation. Available at: <https://pyvis.readthedocs.io/en/latest/>
12. GNS3 (no date) GNS3 documentation. Available at: <https://docs.gns3.com/>

PhD Sashnova M., Vozniuk Y., PhD Cherkasov D., Maslov P.

AUTOMATED COMPLIANCE CONTROL OF NETWORK DEVICE CONFIGURATIONS WITH CYBERSECURITY REQUIREMENTS

The growing number of connected devices, the increasing diversity and complexity of network topologies, and the constant evolution of cyber threats greatly complicate the administration of network equipment. Configuring dozens or hundreds of routers and switches manually is labor-intensive, costly, and associated with a high risk of cyber threats. Configuration errors themselves are the reason for the success of most cyberattacks. The aim of the study is to develop and practically test a system for the automated validation of network device configurations. Specifically, the system should automatically identify the physical network topology, verify the compliance of settings with industry security standards, and automatically remediate detected vulnerabilities.

The system was implemented in Python using the Netmiko and PyVis libraries. The LLDP protocol (IEEE 802.1AB) was used to obtain topology information. Configuration checks were performed in accordance with 10 CIS Benchmark rules for Cisco IOS. The system was tested on a virtual GNS3 testbed consisting of Cisco IOS routers classified into security zones (Access, Restricted, DMZ) with dynamic OSPF routing.

The audit module detected a number of vulnerable settings (in particular, enabled Telnet), as a result of which the initial security-standard compliance score was 85%. After the automated application of fixes and the generation of extended access control lists (ACLs), the score was raised to 100%. In addition, the system successfully blocked an unauthorized access attempt from the Restricted zone to the database server, which confirmed the correctness of the generated filtering policies.

The proposed solution significantly reduces the time required to conduct an audit, eliminates the influence of the subjective human factor, and ensures the consistent implementation of security measures. The results of the study confirm that NetDevOps principles work quite effectively in solving the tasks of ensuring the protection of real networks.

Keywords: administration automation; security audit; access control lists; CIS Benchmark; NetDevOps; network segmentation; Zero Trust; network devices.

ЗАГАЛЬНІ ПИТАННЯ

УДК 629.7.623.7

к.т.н., доц. Добровольський Ю.Б. (ДУ "КАІ")

к.т.н., доц. Дубик О.М. (ДУ "КАІ")

д-р філос., Ярмольчик М.О. (ДУ "КАІ")

DOI: <https://doi.org/10.17721/2519-481X/2026/90-08>

НАБЛИЖЕННЯ НОРМАТИВНОЇ БАЗИ ДЕРЖАВНОЇ АВІАЦІЇ УКРАЇНИ ДО СТАНДАРТІВ НАТО

Стратегічні оборонні документи України регламентують досягнення повної взаємосумісності сил оборони з військами країн-членів НАТО. Це зумовлює гостру потребу в реформуванні та наближенні чинної нормативно-правової бази інженерно-аеродромного забезпечення державної авіації до стандартів Альянсу.

Метою роботи є обґрунтування та розроблення практичних рекомендацій щодо інтеграції стандартів НАТО у вітчизняні нормативні документи (зокрема Накази Міністерства оборони України №121, №348 та №761), які регулюють експлуатацію та визначення придатності аеродромів.

У роботі застосовано метод порівняльного аналізу вітчизняних нормативно-правових актів та Матриці розподілу відповідальності за опрацювання стандартів НАТО. Здійснено детальний аналіз профільних угод зі стандартизацією STANAG та супутніх керівних документів.

На основі аналізу понад 2000 міжнародних документів відібрано 20 ключових стандартів НАТО у сфері експлуатації, ремонту, маркування та освітлення аеродромів. Виявлено суттєві розбіжності між національними вимогами та стандартами Альянсу щодо класифікації кодів тиску в шинах повітряних суден. Запропоновано алгоритм інтеграції міжнародного методу оцінювання експлуатаційного стану аеродромних покриттів PCI (Pavement Condition Index) відповідно до стандарту АЕР-56 у чинні Накази МОУ. Наведено математичний апарат для розрахунку середньозваженого індексу PCI та індексу майбутніх некінетичних пошкоджень (FNKD) для аеродромів з декількома елементами інфраструктури.

Ключові слова: аеродроми, аеродромне забезпечення, технічний стан аеродромів, аеродроми державної авіації, пошкодження покриттів, індекс стану аеродромного покриття, класифікаційний параметр аеродромного покриття, стандарти НАТО, злітно-посадкова смуга, руліжні доріжки, впровадження, метод падаючого вантажу, ремонт аеродромних покриттів.

Вступ. Стандарт НАТО, він же "Угода зі стандартизації" (англ. Standardization Agreement; STANAG) – міжнародний договір, який регламентує загальні правила, визначає спільний порядок дій, закріплює єдину термінологію і встановлює умови уніфікації технічних процесів, а також озброєння та військової техніки, іншої матеріальної частини Збройних сил Альянсу та країн-партнерів. Стандарти НАТО об'єднані в складну і взаємопов'язану ієрархію керівних документів, що мають утворювати систему стандартів.

Стандарт НАТО покликаний забезпечити взаємодію між різними видами збройних сил, збройними силами різних країн для досягнення взаємосумісності, ухвалюється консенсусом і може бути реалізований повністю або частково, із зауваженнями або без.

Стандартизація сприяє досягненню, підтриманню та удосконаленню взаємосумісності як між військами/силами Альянсу, так і між військами/силами держав-партнерів НАТО, зміцнюючи оборонні спроможності Альянсу та посилюючи його боєздатність та ефективність.

Стратегічними оборонними документами України передбачена взаємосумісність з військами/силами Альянсу та збройними силами держав-членів НАТО не лише Збройних Сил України, а й інших складових сил оборони (Служба безпеки України, Національна гвардія України, Державна прикордонна служба України тощо).

Враховуючи вищенаведене, існує потреба в наближенні нормативної бази державної авіації України до стандартів НАТО. Зокрема, потребують перегляду на відповідність стандартам НАТО Накази Міністерства оборони України:

- Наказ Міністерства оборони України №121 від 13.04.2020 "Про внесення змін до Правил визначення придатності до експлуатації аеродромів та злітно-посадкових майданчиків державної авіації України" [1];

- Наказ Міністерства оборони України №761 від 24.12.2015 "Про затвердження Правил аеродромно-технічного забезпечення польотів повітряних суден державної авіації України" [2];

- Наказ Міністерства оборони України №348 від 23.09.2020 "Про внесення змін до Інструкції з експлуатації аеродромів державної авіації України" [3].

Об'єкт дослідження – процес аналізу існуючих вимог НАТО і України у сфері інженерно-аеродромного забезпечення державної авіації України.

Мета роботи – розроблення рекомендацій щодо впровадження стандартів НАТО в нормативну базу державної авіації України у сфері інженерно-аеродромного забезпечення.

Практичне значення полягає у можливості впровадження вимог стандартів НАТО у вітчизняну нормативну базу державної авіації України у сфері інженерно-аеродромного забезпечення.

Матеріали та метод. У роботі проведений аналіз Матриці розподілу відповідальності за опрацювання стандартів НАТО щодо визначення нормативних документів НАТО за напрямком інженерно-аеродромного забезпечення, переклад відібраних стандартів НАТО та аналіз перекладених стандартів НАТО за напрямком інженерно-аеродромного забезпечення та надання рекомендацій щодо впровадження нормативних документів НАТО та внесення змін в нормативну базу державної авіації України.

Останні дослідження та публікації. Проблемами інженерно-аеродромного забезпечення в Україні займалися багато вітчизняних вчених, таких як Гамеляк І.П., Дубик О.М., Родченко О.В., Цихановський В.К., Талах С.М. та ін. [4-17].

Проблема впливу ударних та рухомих навантажень детально висвітлена у працях [18, 19]. Автори акцентують увагу на тому, що за високих швидкостей руху повітряних суден інерційні сили в конструкції покриття значно змінюють характер розподілу напружень. Використання програмних комплексів дозволяє імітувати рух ПС як послідовність імпульсних навантажень, що є критичним для виникнення мікротріщин у бетоні.

Практичне застосування міжнародних стандартів висвітлено в роботі [20], де на прикладі одного з аеродромів проведено визначення несучої спроможності аеродромного покриття з використанням методу класифікаційних чисел ACN/PCN та спеціалізованої програмного комплексу COMFAA 3.0. Це дослідження демонструє важливість автоматизації розрахунків для оперативного управління експлуатаційним станом аеродромних комплексів.

У працях закордонних вчених Rahmawati A. [20] та Rezaei-Tarahomi A. [21] акцентується увага на використанні програмних продуктів, рекомендованих ICAO та FAA.

Відповідно до досліджень [22] та стандарту ASTM D5340 [23], покриття втрачає перші 40 % індексу PCI протягом 75 % свого терміну служби, після чого відбувається стрімке руйнування.

Дослідження Oh H.J. [24] демонструють ефективність використання лазерних сканерів та мобільних систем картографування, що дозволяють створювати цифрові двійники аеродромних покриттів. Це забезпечує точність прогнозування індексу стану покриття PCI з урахуванням мікротріщин, які є причинами інтенсивного руйнування (критична точка на кривій деградації).

Управління експлуатаційним станом елементів льотного поля (ЗПС, РД, перонів) має суттєві відмінності від дорожньої галузі через екстремальні динамічні навантаження від повітряних суден та підвищені вимоги до безпеки польотів.

Результати. З аналізу Матриці розподілу відповідальності за опрацювання стандартів НАТО, яка містить понад 2000 стандартів НАТО, відібрано 20 стандартів за напрямком інженерно-аеродромного забезпечення:

- STANAG 2929. Можливості ремонту пошкоджень аеродрому (ADR) [25];
- STANAG 3158. Денне маркування злітно-посадкових смуг та руліжних доріжок аеродрому [26];
- STANAG 3346. Маркування та освітлення аеродромних перешкод [27];
- STANAG 3619. Маркування та освітлення вертолітних майданчиків і вертолітних аеродромів [28];
- STANAG 3634. Умови тертя та гальмування на злітно-посадковій смузі [29];
- STANAG 3759. Щодо підготовки процедур заходження на посадку за приладами та вильоту [30];
- STANAG 4720. Стандарт НАТО для систем управління повітряним рухом (ATM) та управління безпекою польотів (SMS) [31];
- STANAG 7104. Інструкції з експлуатації аеродромної системи зупинки повітряних суден [32];
- STANAG 7174. Аеропорт і літаки для очищення вертолітних майданчиків [33];
- ААТСР-1. Щодо підготовки процедури заходження на посадку та зльоту за приладами [34];
- ААТМР-01. Стандарт НАТО для повітряного руху. Управління (ATM). Система управління безпекою (SMS) [35];
- ААТМР-03. Можливості ремонту пошкоджень аеродрому (ADR) [36];
- ААТМР-05. Денне маркування злітно-посадкових смуг аеродрому та руліжних доріжок [37];
- ААТМР-08. Маркування та освітлення аеродромних перешкод [38];
- ААТМР-12. Маркування та освітлення вертолітних майданчиків і вертолітних аеродромів [39];
- ААТМР-13. Умови тертя та гальмування на злітно-посадковій смузі [40];
- ААТМР-30. Інструкції з експлуатації аеродромної системи зупинки повітряних суден [41];
- ААТМР-38. Дозволи на польоти ПС з аеродромів та вертолітних майданчиків [42];
- АЕР-46(В). Класифікаційні номери повітряних суден (ACN)/класифікаційний номер аеродромного покриття (PCN) [43];
- АЕР-56. Стандартний метод дослідження індексу стану аеродромного покриття (PCI) [44].

Найбільш відомим і широко поширеним із методів оцінювання експлуатаційно-технічного стану аеродромних покриттів, які використовуються за кордоном, є метод PCI (Pavement Condition Index – індекс стану покриття), який прийнятий в стандарті АЕР-56 [44].

При оцінюванні PCI враховується 15 типів дефектів: здирання плит (втрата поздовжньої стійкості), облом кута, тріщина (поздовжня, поперечна чи діагональна), D-подібні тріщини, пошкодження герметика в швах, руйнування $< 0,5 \text{ м}^2$, руйнування $> 0,5 \text{ м}^2$, раковини, лущення, уступи, руйнування плити, усадочні тріщини, сколювання в швах, сколювання в кутах.

Процедура визначення PCI аеродромних покриттів включає декілька етапів:

1. Розбивання елементів аеродромів (ЗПС, РД, МС) на ділянки, які мають однакову конструкцію, рік побудови, технологію будівництва та історію навантажень з урахуванням їх експлуатаційного стану, визначеного на основі візуального обстеження. Вибрані ділянки виділяють на генеральному плані аеродрому. Потім кожен ділянку розділяють на зразки.

Кожен елемент аеродрому, ділянку, зразок і плиту нумерують з метою прив'язки і використання при виконанні повторних обстежень.

2. Візуальне обстеження кожного зразка, фіксуючи кожен виявлений дефект, ступінь пошкодження, кількість пошкоджених плит та щільність дефектів в дефектній відомості. Плити наносять на схему.

Потім визначається щільність розподілу дефекту за формулою:

$$D_y = \frac{\sum n_{ij}}{n_{\Sigma}} \cdot 100, \% \quad (1)$$

де D_y – щільність розподілу дефекту;

n_{ij} – кількість плит, які мають і-й дефект та j-й ступінь пошкодження;

n_{Σ} – сумарна кількість плит в зразку ($n_{\Sigma} = 20$).

3. Визначають приведені значення суми показників стану CDV_i з урахуванням кількості дефектів q , для яких значення показника стану перевищує 5.

4. Обчислення індексу експлуатаційного стану покриття для кожного зразка виконується за формулою:

$$PCI = 100 - CDV_i, \quad (2)$$

де n – кількість зразків.

За обчисленим середнім значенням індексу встановлюють якісну оцінку (рейтинг) експлуатаційного стану ділянки покриття відповідно до таблиці 1.

Таблиця 1 – Співвідношення між PCI та рейтингом стану аеродромного покриття

Значення PCI	Рейтинг стану покриття
86-100	Відмінне
71-85	Дуже добре
56-70	Добре
41-55	Задовільне
26-40	Погане
11-25	Дуже погане
0-10	Зруйноване

Алгоритм визначення PCI необхідно впровадити в Наказ Міністерства оборони України від 23.09.2020 № 348 "Про внесення змін до Інструкції з експлуатації аеродромів державної авіації України" [3] та від 13.04.2020 №121 "Про внесення змін до Правил визначення придатності до експлуатації аеродромів та злітно-посадкових майданчиків державної авіації України" [1].

У випадку декількох злітно-посадкових смуг, руліжних доріжок та перонів для паркування слід розраховувати середньозважений PCI :

$$PCI = \frac{PCI_1 \cdot A_1 + PCI_2 \cdot A_2 + PCI_3 \cdot A_3 \dots}{A_1 + A_2 + A_3}, \quad (3)$$

де PCI_1, PCI_2, PCI_3 – індекси станів аеродромних покриттів для елементів аеродрому №1, №2 та №3;

A_1, A_2, A_3 – площі елементів аеродромів №1, №2 та №3.

Якщо неможливо визначити PCI аеродромного покриття, то можна визначити майбутні некінетичні пошкодження $FNKD$ для кожної поверхні і аналогічним чином розрахувати зважений $FNKD$:

$$FNKD = \frac{FNKD_1 \cdot A_1 + FNKD_2 \cdot A_2 + FNKD_3 \cdot A_3 \dots}{A_1 + A_2 + A_3}, \quad (4)$$

$FNKD_1, FNKD_2, FNKD_3$ – майбутні некінетичні пошкодження для елементів аеродрому №1, №2 та №3;

A_1, A_2, A_3 – площі елементів аеродромів №1, №2 та №3.

В Наказах Міністерства оборони України №348 та №121 відсутня інформація щодо визначення індексу стану аеродромного покриття *PCI*. Однак дана інформація є в стандарті НАТО АЕР-56 "Стандартний метод дослідження індексу стану аеродромного покриття". І цю інформацію стосовно *PCI* з АЕР-56 необхідно впроваджувати в Накази Міністерства оборони України №348 і №121.

В Додатках до АЕР-56 наведені описи дефектів аеродромного покриття, ступінь загрози та способи вимірювання. Дані описи дефектів, ступені загрози та способи вимірювання потребують додаткового вивчення щодо можливості впровадження в Наказ Міністерства оборони України №348.

В Наказі Міністерства оборони України від 23.09.2020 № 348 "Про внесення змін до Інструкції з експлуатації аеродромів державної авіації України" вказано:

Категорія максимально допустимого тиску в пневматиках повітряного судна:

- код W – не обмежено: тиск не обмежений;
- код X – високий: тиск не більше 1,75 МПа;
- код Y – середній: тиск не більше 1,25 МПа;
- код Z – низький: тиск не більше 0,50 МПа.

Однак в документі АЕР-46 коди тиску в шинах інші (таблиця 2).

Таблиця 2 – Коди тиску в шинах відповідно до АЕР-46

Код	Категорія	Тиск в шинах МРА
W	Високий	Без обмежень
X	Середній	Ліміт до 1,5
Y	Низький	Ліміт до 1,0
Z	Дуже низький	Ліміт до 0,5

В Наказі Міністерства оборони України від 23.09.2020 № 348 наведені наступні вказівки щодо перевантаження:

1) на жорстких покриттях середньорічну добову інтенсивність обмежують:

- десятьма літако-вильотами на добу, якщо $1 > PCN/ACN \geq 0,85$;
- двома літако-вильотами на добу, якщо $0,85 > PCN/ACN \geq 0,8$;
- одним літако-вильотом на добу, якщо $0,8 > PCN/ACN \geq 0,75$;

2) на нежорстких покриттях сумарну добову інтенсивність обмежують:

- двадцятьма літако-вильотами на добу, якщо $1 > PCN/ACN \geq 0,8$;
- п'ятьма літако-вильотами на добу, якщо $0,8 > PCN/ACN \geq 0,7$;

3) разові (аварійні) посадки повітряних суден допускається виконувати для $PCN/ACN \geq 0,5$.

З 28 листопада 2024 року цивільні аеродроми України зобов'язані перейти на метод класифікаційного рейтингу повітряного судна – рейтингу класифікації покриття (ACR-PCR) та опублікувати дані щодо несучої спроможності аеродромних покриттів у Збірнику аеронавігаційної інформації в форматі ACR-PCR.

Інструктивний матеріал щодо порядку представлення даних покриттів за методом ACR-PCR, публікації PCR та стандартні процедури для визначення ACR повітряного судна містяться у частині 3 Керівництва по проектуванню аеродромів (Doc 9157 [45]).

Висновки. У процесі адаптації нормативної бази державної авіації України до стандартів НАТО виявлено низку суттєвих відмінностей між наказами Міністерства оборони України та положеннями стандартів Альянсу (зокрема АЕР-46, АЕР-56, ААТМР-03, ААТМР-05, ААТМР-12 та STANAG 3158). Проведений аналіз показав необхідність перегляду й оновлення національних документів у напрямі підвищення рівня взаємосумісності, уніфікації методів оцінювання, а також впровадження сучасних підходів до маркування та технічного обслуговування аеродромів державної авіації. Це стосується, зокрема:

- Наказу Міністерства оборони України №121 від 13.04.2020 "Про внесення змін до Правил визначення придатності до експлуатації аеродромів та злітно-посадкових майданчиків державної авіації України";

- Наказу Міністерства оборони України №348 від 23.09.2020 "Про внесення змін до Інструкції з експлуатації аеродромів державної авіації України";

- Наказу Міністерства оборони України №761 від 24.12.2015 "Про затвердження Правил аеродромно-технічного забезпечення польотів повітряних суден державної авіації України".

Одним із ключових напрямків модернізації вітчизняної нормативної бази є запровадження методики PCI (Pavement Condition Index) відповідно до стандарту AEP-56, що дозволить об'єктивно оцінювати стан аеродромних покриттів і планувати їхнє відновлення.

Також доцільним є уточнення вимог щодо класифікаційних кодів тиску в пневматиках повітряних суден, міцності земляного полотна, співвідношення ACN/PCN, а також удосконалення алгоритмів визначення навантаження на покриття з урахуванням реальних експлуатаційних параметрів.

Впровадження положень стандартів НАТО у систему нормативно-правових актів Міністерства оборони України сприятиме:

- підвищенню ефективності інженерно-аеродромного забезпечення;
- наближенню технічних процедур і вимог до міжнародних стандартів;
- забезпеченню сумісності з військами держав-членів НАТО;
- підвищенню безпеки польотів та експлуатаційної надійності аеродромів державної авіації.

ЛІТЕРАТУРА:

1. Про внесення змін до Правил визначення придатності до експлуатації аеродромів та злітно-посадкових майданчиків державної авіації України : наказ Міністерства оборони України від 13 квіт. 2020 р. № 121. 98 с.

2. Про затвердження Правил аеродромно-технічного забезпечення польотів повітряних суден державної авіації України : наказ Міністерства оборони України від 24 груд. 2015 р. № 761. 70 с.

3. Про внесення змін до Інструкції з експлуатації аеродромів державної авіації України : наказ Міністерства оборони України від 23 верес. 2020 р. № 348. 182 с.

4. Дубик О. М., Ільченко В. В., Степанчук О. В., Талавіра Г. М. Удосконалення моніторингу експлуатаційно-технічного стану жорстких аеродромних покриттів. Галузеве машинобудування, будівництво. 2021. № 2 (57). с. 59–67.

5. Гамеляк І. П., Харченко А. М., Дмитриченко А. М. Аналіз методів визначення ступеня пошкодження цементобетонних покриттів автомобільних доріг та аеродромів. Автомобільні дороги і дорожнє будівництво. 2024. Вип. 116. с. 71–80. URL: https://arccjournal.org/web/uploads/pdf/2024_61_3-58-67.pdf (дата звернення: вказується автором).

6. Dubyk O., Timkina S., Stepanchuk O., Prentkovskis O. Assessment and Predictive Modelling of Transport and Operating Condition of Aerodrome Pavement: A Case Study of Zaporizhzhia. Lecture Notes in Intelligent Transportation and Infrastructure. Cham : Springer, 2022. p. 171–183.

7. Karpov V., Stepanchuk O., Dubyk O., Rodchenko O., Prentkovskis O. Improvement of Methodology of Calculation and Assessment of Transport and Operational Condition of Airfield Pavement (on the Example of Airport Pavements of Kyiv and Mykolaiv International Airports). In: Prentkovskis O., Yatskiv (Jackiva) I., Skačkauskas P., Maruschak P., Karpenko M. (eds). TRANSBALTICA 2022. Lecture Notes in Intelligent Transportation and Infrastructure. Cham : Springer, 2023. DOI: 10.1007/978-3-031-25863-3_79.

8. Дубик О. М., Чемакіна О. В., Чернишова О. С., Осовський І. О., Кудрявець Є. С. Методика визначення несучої спроможності аеродромних покриттів. Теорія та практика дизайну. Архітектура та будівництво. Київ : НАУ, 2024. Вип. 34. с. 11–21.

9. Максименко В. П., Дубик О. М., Карпенко А. К., Зіненко С. С. Застосування композитної арматури в жорстких покриттях автомобільних доріг і аеродромів. Airport Planning, Construction and Maintenance Journal. 2024. № 4. с. 87–95.

10. Malovanyu M., Dubyk O., Chemakina O., Povzun O. Disposal of Industrial Waste in Building Material Production. Pollack Periodica. 2026. p. 64–71. DOI: 10.1556/606.2025.01306.

11. Дубик О. М., Чернишова О. С., Вишневська А. В., Осовський І. М., Данілін О. М. Дослідження напружено-деформованого стану конструкції аеродромного покриття аеродрому державної авіації. *Airport Planning, Construction and Maintenance Journal*. 2025. Вип. 6. с. 52–67.
12. Dubyk O. M., Chernyshova O. S., Osovskiy I. M., Kononenko D. Yu. Determination of the Stress–Strain State of the Rigid Pavement Structure of an Airfield Access Road. *Сучасне будівництво та архітектура*. 2026. № 15. р. 34–42.
13. Родченко О. В., Єрмак О. Т. Проектування пасажирського авіатерміналу в рамках стратегії сталого розвитку. *Airport Planning, Construction and Maintenance Journal*. 2023. № 2. с. 59–68. DOI: 10.32782/apcmj.2023.2.6.
14. Родченко О. В. Комп'ютерні технології визначення класифікаційного параметра жорсткого аеродромного покриття з використанням штучного інтелекту. *Airport Planning, Construction and Maintenance Journal*. 2024. № 4. с. 104–112. DOI: 10.32782/apcmj.2024.4.10.
15. Родченко О. В., Шевченко О. В. Комп'ютерні технології числового моделювання будівельних конструкцій з використанням штучного інтелекту. *Airport Planning, Construction and Maintenance Journal*. 2024. № 3. с. 71–77. DOI: 10.32782/apcmj.2024.3.10.
16. Цихановський В. К., Козловець С. М., Коряк О. С. Розрахунок тонких плит на пружній основі методом скінченних елементів. Київ : Сталь, 2008. 234 с.
17. Цихановський В. К., Прусов Д. Є. Уточнений чисельний розрахунок жорстких аеродромних покриттів на слабких ґрунтових основах з урахуванням неоднорідностей матеріалу і особливостей стикових елементів плит. *Опір матеріалів і теорія споруд*. 2006. № 79. с. 92–100.
18. Shafabakhsh G., Kashi E., Tahani M. Analysis of runway pavement response under aircraft moving load by FEM. *Journal of Engineering, Design and Technology*. 2018. Vol. 16. р. 233–243. DOI: 10.1108/JEDT-09-2017-0093.
19. Qin Y., Hiller J. E. Modeling the temperature and stress distributions in rigid pavements: impact of solar radiation absorption and heat history development. *KSCE Journal of Civil Engineering*. 2011. Vol. 15. P. 1361–1371. DOI: 10.1007/s12205-011-1322-6.
20. Rahmawati A., Rahmawati F. Runway pavement strength evaluation of Yogyakarta International Airports depends on ICAO (ACN/PCN) method with COMFAA 3.0 software. *International Journal of Integrated Engineering*. 2022. Vol. 14. P. 350–359. DOI: 10.1007/s41062-024-01376-x.
21. Rezaei-Tarahomi A., Kaya O., Ceylan H., Kim S., Gopalakrishnan K., Brill D. R. Development of rapid three-dimensional finite-element based rigid airfield pavement foundation response and moduli prediction models. *Transportation Geotechnics*. 2017. Vol. 13. P. 81–91. DOI: 10.1016/j.trgeo.2017.08.011.
22. Yuan J., Li W., Li Y., Ma L., Zhang J. Fatigue models for airfield concrete pavement: literature review and discussion. *Materials*. 2021. Vol. 14. Article 6579. DOI: 10.3390/ma14216579.
23. ASTM D5340-24. Standard Test Method for Airport Pavement Condition Index Surveys. West Conshohocken : ASTM International, 2024. 63 p.
24. Oh H. J., Cho Y. K., Seo Y., Kim S.-M. Experimental analysis of curling behavior of continuously reinforced concrete pavement. *Construction and Building Materials*. 2016. Vol. 128. P. 57–66. DOI: 10.1016/j.conbuildmat.2016.10.079.
25. STANAG 2929. Можливості ремонту пошкоджень аеродрому (ADR). Офіс стандартизації НАТО, 2016. 7 с.
26. STANAG 3158. Денне маркування злітно-посадкових смуг та руліжних доріжок аеродрому. Офіс стандартизації НАТО, 2015. 5 с.
27. STANAG 3346. Маркування та освітлення аеродромних перешкод. Офіс стандартизації НАТО, 2023. 5 с.
28. STANAG 3619. Маркування та освітлення вертолітних майданчиків і вертолітних аеродромів. Офіс стандартизації НАТО, 2018. 28 с.
29. STANAG 3634. Умови тертя та гальмування на злітно-посадковій смузі. Офіс стандартизації НАТО, 2018. 18 с.
30. STANAG 3759. Щодо підготовки процедур заходження на посадку за приладами та вильоту. Офіс стандартизації НАТО, 2017. 6 с.
31. STANAG 4720. Стандарт НАТО для систем управління повітряним рухом (ATM) та управління безпекою польотів (SMS). Офіс стандартизації НАТО, 2014. 5 с.
32. STANAG 7104. Інструкції з експлуатації аеродромної системи зупинки повітряних суден. Офіс стандартизації НАТО, 2023. 5 с.
33. STANAG 7174. Аеропорт і літаки для очищення вертолітних майданчиків. Офіс стандартизації НАТО, 2017. 7 с.

34. ААТСР-1. Щодо підготовки процедури заходження на посадку та зльоту за приладами. Офіс стандартизації НАТО, 2017. 93 с.
35. ААТМР-01. Стандарт НАТО для повітряного руху. Управління (АТМ). Система управління безпекою (SMS). Офіс стандартизації НАТО, 2014. 47 с.
36. ААТМР-03. Можливості ремонту пошкоджень аеродрому (ADR). Офіс стандартизації НАТО, 2016. 113 с.
37. ААТМР-05. Денне маркування злітно-посадкових смуг аеродрому та руліжних доріжок. Офіс стандартизації НАТО, 2015. 22 с.
38. ААТМР-08. Маркування та освітлення аеродромних перешкод. Офіс стандартизації НАТО, 2023. 18 с.
39. ААТМР-12. Маркування та освітлення вертолітних майданчиків і вертолітних аеродромів. Офіс стандартизації НАТО, 2018. 60 с.
40. ААТМР-13. Умови тертя та гальмування на злітно-посадковій смузі. Офіс стандартизації НАТО, 2018. 22 с.
41. ААТМР-30. Інструкції з експлуатації аеродромної системи зупинки повітряних суден. Офіс стандартизації НАТО, 2023. 18 с.
42. ААТМР-38. Дозволи на польоти повітряних суден з аеродромів та вертолітних майданчиків. Офіс стандартизації НАТО, 2023. 56 с.
43. АЕР-46(В). Класифікаційні номери повітряних суден (АСН) / класифікаційний номер аеродромного покриття (РСН). Офіс стандартизації НАТО, 2008. 280 с.
44. АЕР-56. Стандартний метод дослідження індексу стану аеродромного покриття (РСІ). Офіс стандартизації НАТО, 2008. 140 с.
45. Doc 9157. Aerodrome Design Manual. Part 3. Pavements = Керівництво з проєктування аеродромів. Частина 3. Покриття. 3rd ed. International Civil Aviation Organization (ICAO), 2023. 162 p.

REFERENCES:

1. *Ministry of Defense of Ukraine*, Order No. 121, "On amendments to the Rules for determining the suitability for operation of airfields and runways of state aviation of Ukraine," 98 p. (13 April 2020).
2. *Ministry of Defense of Ukraine*, Order No. 761, "On approval of the Rules of airfield-technical support of flights of aircraft of state aviation of Ukraine," 70 p. (24 December 2015).
3. *Ministry of Defense of Ukraine*, Order No. 348, "On amendments to the Instructions for the operation of airfields of state aviation of Ukraine," 182 p. (23 September 2020).
4. O. M. Dubyk, V. V. Ilchenko, O. V. Stepanchuk, & H. M. Talavira. (2021). Improvement of monitoring the operational and technical condition of rigid airfield pavements. *Galuz. Mashinobud. Budivn.*, 2 (57), 59–67.
5. I. P. Hameliak, A. M. Kharchenko, & A. M. Dmytrychenko. (2024). Analysis of methods for determining the degree of damage to cement concrete pavements of highways and airfields. *Avtomob. Dorozhn. Budivn.*, 116, pp. 71–80.
6. O. Dubyk, S. Timkina, O. Stepanchuk, & O. Prentkovskis. (2022). Assessment and Predictive Modelling of Transport and Operating Condition of Aerodrome Pavement: A Case Study of Zaporizhzhia. *Lecture Notes in Intelligent Transportation and Infrastructure*, Springer, Cham, pp. 171–183.
7. Karpov, V., Stepanchuk, O., Dubyk, O., Rodchenko, O. & Prentkovskis, O. (2023). Improvement of Methodology of Calculation and Assessment of Transport and Operational Condition of Airfield Pavement (on the Example of Airport Pavements of Kyiv and Mykolaiv International Airports). In: Prentkovskis, O., Yatskiv (Jackiva), I., Skačkauskas, P., Maruschak, P., Karpenko, M. (eds) *TRANSBALTICA 2022. Lecture Notes in Intelligent Transportation and Infrastructure*. Springer, Cham, pp. 806–823. https://doi.org/10.1007/978-3-031-25863-3_79
8. O. M. Dubyk, O. V. Chemakina, O. S. Chernyshova, I. O. Osovslyi, & Ye. S. Kudriavets. (2024). Methodology for determining the bearing capacity of airfield pavements. *Teor. Prakt. Dyzaingu. Arkhit. Budivn.* 34, pp. 11–21.
9. V. P. Maksymenko, O. M. Dubyk, A. K. Karpenko, & S. S. Zinenko. (2024). Application of composite reinforcement in rigid pavements of highways and airfields, *Airport Plan. Constr. Maint. J.* 4, pp. 87–95.
10. M. Malovanyy, O. Dubyk, O. Chemakina, & O. Povzun. (2026). Disposal of industrial waste in building material production, *Pollack Period.* pp. 64–71.

11. O. M. Dubyk, O. S. Chernyshova, A. V. Vyshnevskaya, I. M. Osovskiy, & O. M. Danilin. (2025). Investigation of the stress-strain state of the airfield pavement structure of the state aviation airfield, *Airport Plan. Constr. Maint. J.* 2, pp. 52–67.
12. O. M. Dubyk, O. S. Chernyshova, I. M. Osovskiy, & D. Yu. Kononenko. (2026). Determination of the stress–strain state of the rigid pavement structure of an airfield access road, *Suchasne Budivn. Arkhit.* 15, pp. 34–42.
13. O. V. Rodchenko & O. T. Yermak. (2023). Passenger air terminal design within the sustainable development strategy, *Airport Plan. Constr. Maint. J.* 2, pp. 59–68 (2023); <https://doi.org/10.32782/apcmj.2023.2.6>.
14. O. V. Rodchenko. (2024). Computer technologies for determining the classification parameter of rigid airfield pavement using artificial intelligence," *Airport Plan. Constr. Maint. J.* 4, pp. 104–112 <https://doi.org/10.32782/apcmj.2024.4.10>.
15. O. V. Rodchenko & O. V. Shevchenko. (2024). Computer technologies for numerical modeling of building structures using artificial intelligence, *Airport Plan. Constr. Maint. J.* 3, pp. 71–77 ; <https://doi.org/10.32782/apcmj.2024.3.10>.
16. V. K. Tsykhanovskiy, S. M. Kozlovets, & O. S. Koriak. (2008). Calculation of Thin Plates on an Elastic Foundation by the Finite Element Method. *Stal, Kyiv*, 234 p.
17. V. K. Tsykhanovskiy & D. E. Prusov. (2006). Refined numerical calculation of rigid airfield pavements on weak soil foundations taking into account material inhomogeneities and features of slab joint elements, *Opir Mater. Teor. Sporud* 79, pp. 92–100.
18. G. Shafabakhsh, E. Kashi, & M. Tahani. (2018). Analysis of runway pavement response under aircraft moving load by FEM, *J. Eng. Des. Technol.* 16, pp. 233–243; <https://doi.org/10.1108/JEDT-09-2017-0093>.
19. Y. Qin & J. E. Hiller. (2011). Modeling the temperature and stress distributions in rigid pavements: impact of solar radiation absorption and heat history development, *KSCE J. Civ. Eng.* 15, pp. 1361–1371; <https://doi.org/10.1007/s12205-011-1322-6>.
20. A. Rahmawati & F. Rahmawati (2022). Runway pavement strength evaluation of Yogyakarta International Airports depends on ICAO (ACN/PCN) method with COMFAA 3.0 software, *Int. J. Integr. Eng.* 14, pp. 350–359; <https://doi.org/10.1007/s41062-024-01376-x>.
21. A. Rezaei-Tarahomi, O. Kaya, H. Ceylan, S. Kim, K. Gopalakrishnan, & D. R. Brill (2017), "Development of rapid three-dimensional finite-element based rigid airfield pavement foundation response and moduli prediction models," *Transp. Geotech.* 13, pp. 81–91; <https://doi.org/10.1016/j.trgeo.2017.08.011>.
22. J. Yuan, W. Li, Y. Li, L. Ma, & J. Zhang. (2021). Fatigue models for airfield concrete pavement: literature review and discussion, *Materials* 14, 6579; <https://doi.org/10.3390/ma14216579>.
23. ASTM D5340-24. (2024). *Standard Test Method for Airport Pavement Condition Index Surveys* (ASTM International, West Conshohocken), 63 p.
24. H. J. Oh, Y. K. Cho, Y. Seo, & S.-M. Kim. (2016). Experimental analysis of curling behavior of continuously reinforced concrete pavement, *Constr. Build. Mater.* 128, pp. 57–66; <https://doi.org/10.1016/j.conbuildmat.2016.10.079>.
25. NATO Standardization Office, STANAG 2929. (2016). Aerodrome damage repair capabilities (ADR), 7 p.
26. NATO Standardization Office, STANAG 3158. (2015). Day marking of aerodrome runways and taxiways, 5 p.
27. NATO Standardization Office, STANAG 3346. (2023). Marking and lighting of aerodrome obstructions, 5 p.
28. NATO Standardization Office, STANAG 3619. (2018). Marking and lighting of helipads and heliports, 28 p.
29. NATO Standardization Office, STANAG 3634. (2018). Runway friction and braking conditions, 18 p.
30. NATO Standardization Office, STANAG 3759. (2017). On the preparation of instrument approach and departure procedures," 6 p.
31. NATO Standardization Office, STANAG 4720. (2014). NATO standard for Air Traffic Management (ATM) and Safety Management Systems (SMS), 5 p.
32. NATO Standardization Office, STANAG 7104. (2023). Instructions for the operation of the airfield aircraft arrestor system, 5 p.
33. NATO Standardization Office, STANAG 7174. (2017). Airport and aircraft for cleaning helipads, 7 p.

34. NATO Standardization Office, AATCP-1. (2017). On the preparation of instrument approach and take-off procedures, 93 p.
35. NATO Standardization Office, AATMP-01. (2014). NATO standard for air traffic management (ATM) safety management system (SMS), 47 p.
36. NATO Standardization Office, AATMP-03. (2016). Aerodrome damage repair capabilities (ADR), 113 p.
37. NATO Standardization Office, AATMP-05. (2015). Day marking of aerodrome runways and taxiways, 22 p.
38. NATO Standardization Office, AATMP-08. (2023). Marking and lighting of aerodrome obstructions, 18 p.
39. NATO Standardization Office, AATMP-12. (2018). Marking and lighting of helipads and heliports, 60 p.
40. NATO Standardization Office, AATMP-13. (2018). Runway friction and braking conditions, 22 p.
41. NATO Standardization Office, AATMP-30. (2023). Instructions for the operation of the airfield aircraft arrestor system, 18 p.
42. NATO Standardization Office, AATMP-38. (2023). Aircraft flight clearances from aerodromes and helipads, 56 p.
43. NATO Standardization Office, AEP-46(B). (2008). Aircraft Classification Numbers (ACN) / Pavement Classification Number (PCN), 280 p.
44. NATO Standardization Office, AEP-56. (2008). Standard test method for airfield Pavement Condition Index (PCI) surveys, 140 p.
45. International Civil Aviation Organization (ICAO), Doc 9157. (2023). Aerodrome Design Manual. Part 3. Pavements, 3rd ed. (ICAO, Montreal), 162 p.

Ph.D Dobrovolskyi Y.B., Ph.D Dubyk O.M., Ph.D Yarmolchuk M.O.

ALIGNING UKRAINE'S STATE AVIATION REGULATORY FRAMEWORK WITH NATO STANDARDS

Abstract. Ukraine's strategic defense documents mandate achieving full interoperability between the defense forces and the military forces of NATO member states. This creates an urgent need to reform the existing regulatory framework for airfield engineering support for state aviation and align it with Alliance standards.

Justification and development of practical recommendations for integrating NATO standards into domestic regulatory documents (specifically Ministry of Defence of Ukraine Orders №121, №348 and №761) governing the operation and determination of the suitability of airfields.

The study employs a method of comparative analysis involving domestic regulatory acts and the Responsibility Allocation Matrix for the processing of NATO standards. A detailed analysis of relevant STANAG standardization agreements and associated guidance documents was conducted.

Based on an analysis of over 2000 international documents, 20 key NATO standards regarding airfield operations, maintenance marking, and lighting were selected. Significant discrepancies were identified between national requirements and Alliance standards concerning aircraft tire pressure code classifications.

An algorithm was proposed to integrate the foreign PCI (Pavement Condition Index) method for assessing airfield pavement operational status – in accordance with standard AEP-56 – into current Ministry of Defence orders. Mathematical formulas are provided for calculating the weighted average PCI and Future Non-Kinetic Damage (FKND) index for airfields comprising multiple infrastructure elements.

Key words: airfields, airfield support, technical condition of airfields, state aviation airfields, pavement damage, airfield pavement condition index, airfield pavement classification parameter, NATO standards, runway, taxiways, implementation, falling weight method, airfield pavement repair.

ОСНОВНІ ФАКТОРИ, ЩО ВПЛИВАЮТЬ НА ЕФЕКТИВНІСТЬ ВІДНОВЛЕННЯ БОЄЗДАТНОСТІ ВІЙСЬКОВОЇ ЧАСТИНИ

Проблема відновлення боєздатності військових частин набула критичного значення через інтенсивність бойових дій та значні втрати. Метою статті є висвітлення основних факторів, що впливають на ефективність відновлення боєздатності в умовах воєнного стану.

Дослідження проведено з використанням таких методів: аналізу і синтезу – для визначення проблеми, мети та завдань дослідження; контент-аналізу – для вивчення джерел із теми дослідження та практичного досвіду бойових дій для систематизації факторів впливу; узагальнення та систематизації – при підготовці висновків стосовно результатів дослідження.

Систематизовано зовнішні (некеровані) та внутрішні (керовані) фактори. Обґрунтовано, що найбільший вплив мають внутрішні фактори: діяльність суб'єктів відновлення боєздатності щодо доукомплектування особовим складом, ОВТ, поповнення МТЗ, проведення заходів відновлення МПС особового складу та бойового заложення; укомплектованість військової частини особовим складом на початок відновлення боєздатності; морально-психологічний стан особового складу на початок відновлення боєздатності; забезпеченість військової частини ОВТ на початок відновлення боєздатності; забезпеченість військової частини МТЗ на початок відновлення боєздатності; підготовленість особового складу військової частини на початок відновлення боєздатності.

Результати дослідження можуть бути використані під час розроблення керівних документів, що регламентують питання організації відновлення боєздатності, в практиці відновлення боєздатності та у ході подальших досліджень з даного напрямку у наукових установах.

Ключові слова: відновлення боєздатності, зовнішні фактори, внутрішні фактори, військова частина, ефективність.

Вступ. Досвід застосування військових частин (підрозділів) Збройних Сил (далі – ЗС) України під час відсічі збройної агресії російської федерації (далі – рф) свідчить, що успішне виконання ними бойових (спеціальних) завдань залежить від рівня їхньої боєздатності [1-6]. Гібридний характер війни, інтенсивне застосування засобів вогневого ураження створюють умови, за яких військові частини зазнають втрат, що знижує їх боєздатність. Подальше успішне виконання військовими частинами, які втратили боєздатність, визначених бойових (спеціальних) завдань можливе лише за умови ефективного відновлення їх боєздатності [7].

У зв'язку з цим триває робота в органах військового управління, військових частинах ЗС України щодо пошуку та впровадження нових підходів у діяльність командувачів (командирів, начальників) та їх заступників для підвищення ефективності проведення заходів відновлення боєздатності військових частин, що неможливо без врахування основних факторів, що впливають на ефективність відновлення боєздатності військової частини.

Таким чином, виникає потреба у висвітленні основних факторів, що впливають на ефективність відновлення боєздатності військової частини. Зазначене свідчить про актуальність теми, яка розглядається.

Огляд літератури. Аналіз попередніх досліджень і публікацій з даного напрямку [8-12] свідчить про те, що не сформовано єдиного підходу до визначення та систематизації основних факторів, що впливають на ефективність відновлення боєздатності, а наявні методики дозволяють оцінити окремі елементи боєздатності, які не повною мірою враховують зміни, що відбулися в системі відновлення боєздатності ЗС України з впровадженням нових керівних документів та не дозволяють комплексно оцінити готовність військової частини до виконання бойових завдань.

Зокрема, у попередніх роботах авторів обґрунтовано методичний підхід до оцінювання рівня навченості органів військового управління тактичного рівня, який враховує індивідуальні спроможності посадових осіб та їхню злагодженість [8]. Питанням оцінювання підготовленості танкових бригад безпосередньо у процесі відновлення їхньої боєздатності присвячена праця [9]. Крім того, розроблено часткову методику для визначення стану саме колективної підготовки органів військового управління як складової оперативної підготовки [10]. Досліджено комплексну методику оцінювання навчання змінного складу навчальних центрів, що дозволяє враховувати фактори, що сприяють або перешкоджають освітньому процесу [11]. Важливим складником формування загальнонаціонального рівня військових знань є базова загальновійськова підготовка, сукупність показників ефективності якої (діяльність суб'єктів, характеристики об'єктів та рівень організації підготовки) обґрунтовано у роботі [12].

Таким чином, попри наявність методик оцінювання окремих елементів боєздатності, питання комплексного впливу внутрішніх і зовнішніх факторів на загальну ефективність процесу відновлення боєздатності військової частини в умовах сучасного воєнного стану залишається недостатньо вивченим і потребує додаткового дослідження.

Метою дослідження є висвітлення основних факторів, що впливають на ефективність відновлення боєздатності військової частини в умовах правового режиму воєнного стану.

Відповідними **завданнями** є:

- виявити та систематизувати зовнішні фактори, що відображають вплив зовнішнього середовища на об'єкт, що досліджується;
- визначити та схарактеризувати внутрішні фактори, які безпосередньо пов'язані з результатами діяльності об'єкта, що досліджується.

Методи. Для досягнення поставленої мети було використано такі методи: аналізу і синтезу – для визначення проблеми, мети та завдань дослідження; контент-аналізу – для вивчення джерел із теми дослідження та практичного досвіду бойових дій для систематизації факторів впливу; узагальнення та систематизації – при підготовці висновків стосовно результатів дослідження.

Результати. На основі аналізу доктринальної бази щодо відновлення боєздатності [13-15, 17] у роботі узагальнено, уточнено (без зміни суті) та сформульовано визначення основних понять, використаних у статті.

Відновлення боєздатності військової частини – це комплекс заходів, який проводиться з метою покриття втрат, завданих противником, та досягнення потрібного рівня боєздатності, що дозволяє реалізувати бойові можливості та забезпечує виконання військовою частиною бойового завдання.

Боєздатність – це стан військової частини, який дозволяє їй успішно вести бойові дії і реалізувати свої бойові можливості.

Боєздатність військової частини може бути втрачена частково або повністю. При цьому вважається, що при втратах в особовому складі, озброєнні та військовій техніці (далі – ОВТ), матеріально-технічних засобів (далі – МТЗ) до 30% і збереженні управління підрозділами військова частина зберігає здатність до виконання бойових (спеціальних) завдань і може продовжувати бойові дії. При втратах в особовому складі, ОВТ, МТЗ від 30% до 50% і збереженні управління підрозділами військова частина частково втрачає боєздатність і потребує відновлення здатності виконувати бойові (спеціальні) завдання. Якщо військова частина втратила понад 50% укомплектованості, забезпеченості і здатність до управління підрозділами, то вона вважається небоєздатною і потребує проведення низки заходів щодо її відновлення.

Під час відновлення боєздатності проводяться такі основні заходи: доукомплектування військової частини особовим складом; проведення заходів з відновлення морально-психологічного стану (далі – МПС) особового складу; доукомплектування військової частини технічно справними штатними зразками ОВТ (відновлення пошкоджених зразків ОВТ); поповнення (забезпечення) військової частини МТЗ та бойове злагодження

військової частини.

Відновлення боєздатності є складним і багатогранним процесом, який проводиться з метою покриття втрат, завданих противником, та проведення заходів бойового злагодження, що дозволить гарантовано й ефективно виконувати поставлені бойові (спеціальні) завдання.

Разом з тим існує низка факторів, що впливають на ефективність цього процесу.

За характером походження основні фактори, що впливають на ефективність відновлення боєздатності військової частини, поділяються на дві групи:

перша група – зовнішні, які відображають вплив зовнішнього середовища і, як правило, не залежать від діяльності об'єкта, що досліджується. Тому ці фактори належать до некерованих;

друга група – внутрішні, безпосередньо пов'язані з результатами діяльності об'єкта, що досліджується, і впливають на нього. Як правило, вони є керованими, тому повною мірою відображають вплив на функціонування процесу та кінцевий результат.

Зовнішні та внутрішні фактори, що впливають на ефективність відновлення боєздатності (рис. 1).



Рисунок 1 – Зовнішні та внутрішні фактори

Досвід відбиття збройної агресії російської федерації свідчить, що сучасні бойові дії характеризуються поєднанням традиційних способів збройної боротьби з широким застосуванням високоточної зброї, безпілотних систем, засобів радіоелектронної боротьби, кібератак та інформаційно-психологічного впливу, чим дедалі більше набирає характерних рис гібридної війни [18]. Зазначені особливості формують умови, у яких здійснюється відновлення боєздатності військових частин, визначаючи його тривалість та ефективність.

Характер та інтенсивність бойових дій визначають масштаби втрат особового складу, озброєння, військової техніки та матеріально-технічних засобів. Зі збільшенням інтенсивності бойових дій зростають обсяги ресурсів і часу, необхідних для відновлення боєздатності військової частини, що ускладнює своєчасне повернення її до виконання бойових (спеціальних) завдань.

Форми і способи застосування військ (сил) також істотно впливають на процес відновлення боєздатності. Перехід до безконтактних способів ведення бойових дій, широке застосування високоточної зброї, ударних безпілотних літальних апаратів, засобів радіоелектронної боротьби та технологій штучного інтелекту змушують адаптувати організацію відновлення боєздатності до нових умов. За таких умов однією з основних форм застосування військ (сил) є спеціальна операція, якій притаманна відсутність чіткого розмежування завдань на оперативному і тактичному рівнях та упередження противника в діях. Особливостями сучасних збройних конфліктів є перехід до безконтактного способу ведення бойових дій, відсутність (розмитість) суцільної лінії бойового зіткнення. Це потребує удосконалення системи бойового злагодження, зміни підходів до підготовки особового складу та забезпечення військових частин сучасними засобами боротьби.

Час, необхідний військовій частині на відновлення боєздатності, є одним із ключових зовнішніх факторів. Він встановлюється старшим начальником залежно від кількості понесених втрат військовою частиною (підрозділом), можливостей щодо доукомплектування особовим складом, технічно справними штатними зразками ОВТ (відновлення пошкоджених зразків ОВТ), поповнення (забезпечення) МТЗ, обстановки в районі ведення бойових дій та наявності і готовності резервів. Обмежені строки можуть не дозволити повністю реалізувати всі необхідні заходи відновлення боєздатності, що безпосередньо позначається на рівні готовності військової частини до виконання бойових завдань.

Негативний інформаційний вплив противника спрямований на деморалізацію особового складу, створення хаосу та зниження боєздатності військ (сил) без прямої військової конфронтації. Розвиток мережі Інтернет відкрив широкі можливості для технологій маніпулятивного впливу. Використання соціальних мереж, інформаційних платформ і сучасних технологій маніпулятивного впливу сприяє поширенню деструктивних наративів, що негативно впливає на морально-психологічний стан військовослужбовців та населення. У результаті ускладнюються заходи мобілізації, комплектування військ та відновлення морально-психологічного стану особового складу під час відновлення боєздатності.

Сучасні соціальні мережі формують в аудиторії так зване "кліпове сприйняття", що характеризується фрагментарністю, низьким рівнем аналітичності, емоційною забарвленістю і стає чудовим підґрунтям для просування визначених наративів і маніпулювання цільовою аудиторією [19].

Можливості противника завдавати вогневого впливу по районах проведення відновлення боєздатності, у будь-якій точці України, значно обмежують організацію відповідних заходів. Постійна загроза ракетних ударів, застосування безпілотних літальних апаратів та інших засобів ураження змушує розосереджувати військові частини (підрозділи), змінювати райони відновлення, посилювати їх інженерне обладнання та охорону. Крім того, ураження об'єктів навчально-матеріальної технічної бази (далі – НМТБ), інфраструктури та логістичних вузлів збільшує тривалість і знижує ефективність процесу відновлення боєздатності.

Міжнародна підтримка світової спільноти є важливим фактором, що позитивно впливає на відновлення боєздатності військових частин. Надходження озброєння, військової техніки, матеріально-технічних засобів, фінансової допомоги, організація підготовки військовослужбовців та обмін досвідом із державами-партнерами розширюють можливості щодо оперативного відновлення втрат, підвищують якість підготовки особового складу та сприяють впровадженню сучасних стандартів організації відновлення боєздатності військ (сил).

Район відновлення боєздатності визначає можливості щодо розміщення особового складу, організації ремонту озброєння і військової техніки, логістичного забезпечення, проведення бойового злагодження, маскування та інженерного обладнання. Віддаленість району від лінії бойового зіткнення, транспортна доступність, наявність необхідної інфраструктури та рівень безпеки безпосередньо впливають на тривалість і ефективність відновлення боєздатності.

Суспільно-політична обстановка в районі відновлення боєздатності також впливає на ефективність цього процесу. Під час оцінювання району враховуються політичні, економічно-інфраструктурні, соціально-демографічні, культурно-релігійні, безпекові (криміногенні), інформаційні, природно-кліматичні та інші умови, які можуть як сприяти, так і ускладнювати проведення заходів відновлення [20]. Сприятлива суспільно-політична обстановка полегшує організацію логістичного забезпечення, взаємодію з органами державної влади та місцевого самоврядування, тоді як нестабільність або високий рівень загроз можуть істотно ускладнювати проведення заходів відновлення боєздатності. Під час планування відновлення боєздатності здійснюється аналіз суспільно-політичної обстановки, який передбачає визначення рівня впливу (сприяння, небезпеки) чинників суспільно-політичної обстановки на хід виконання військами (силами) заходів відновлення боєздатності, виявлення об'єктивно існуючих можливостей, суспільних настроїв, думок, лідерів, потреб і запитів у певному районі та тенденцій їх розвитку і можливих змін.

Вимоги доктринальної бази з відновлення боєздатності визначають порядок організації, проведення та оцінювання заходів відновлення. Уведення в дію нових керівних документів [13-16], адаптованих до підходів держав-членів НАТО (понятійний апарат, принципи і етапи відновлення боєздатності), забезпечує уніфікацію процесів планування та проведення відновлення боєздатності, що створює передумови для підвищення його ефективності.

Як свідчать результати аналізу зовнішніх факторів, їхній вплив має об'єктивний характер на ефективність відновлення боєздатності військової частини, тобто вплив суб'єктів відновлення боєздатності на них значно обмежений.

Тому визначальний вплив на ефективність відновлення боєздатності військової частини здійснюють внутрішні фактори. Вони безпосередньо пов'язані з результатами діяльності об'єкта, що досліджується, і впливають на нього. Вони є керованими, тому повною мірою відображають вплив на функціонування процесу та кінцевий результат.

Діяльність суб'єктів відновлення боєздатності щодо виконання основних заходів, які проводяться під час відновлення боєздатності, з урахуванням початкових значень показників боєздатності впливає на готовність військової частини до виконання бойових (спеціальних) завдань.

Військова служба за призовом під час мобілізації на особливий період хоч і залишається основним джерелом доукомплектування особовим складом під час правового режиму воєнного стану, але пов'язана з численними викликами. Ключовим викликом є зменшення кількості добровольців. Це зумовлено як недоліками в інформаційно-роз'яснювальній роботі державних органів, так і потужним інформаційно-психологічним впливом противника, що має на меті дискредитацію діяльності територіальних центрів комплектування та соціальної підтримки (далі – ТЦК та СП). Крім того, низка державних інституцій не повною мірою реалізує свої законодавчі повноваження у цій сфері. Як наслідок, основний тягар відповідальності за мобілізацію людських ресурсів фактично перекладено на ТЦК та СП.

Корупційні виклики у роботі військово-лікарських комісій (далі – ВЛК), пов'язані з недосконалістю процедури визначення придатності громадян за станом здоров'я до проходження військової служби, соціальна несправедливість не сприяють якісному комплектуванню військовослужбовцями за призовом під час мобілізації. При цьому, всі негативні явища, які в суспільстві пов'язані з мобілізацією, населенням України акумулюються та спрямовуються проти роботи ТЦК та СП. Зазначене сприяє невиконанню ТЦК та СП планових завдань стосовно призову громадян за мобілізацією. Негативний вплив

на комплектування військових частин ЗС України здійснює відсутність у громадян України належної мотивації до виконання своїх конституційних обов'язків із захисту держави, ухилення їх від призову на військову службу під час мобілізації, на особливий період та небажання проходити військову службу за контрактом [21].

Також проблемним питанням є якість людських мобілізаційних ресурсів, що направляються до навчальних центрів (центрів підготовки підрозділів) на підготовку. Зазначене не дозволяє після закінчення підготовки (випуску) повною мірою комплектувати бойові військові частини, насамперед через їх стан здоров'я та психологічну неготовність до виконання бойових (спеціальних) завдань. Це призводить до самовільного залишення особовим складом розташування військових частин (підрозділів).

Поряд із зазначеними проблемами, на ефективність доукомплектування негативно впливає суб'єктивний фактор у діяльності посадових осіб військових організаційних структур. Це виявляється у безпідставних відмовах представників військових частин приймати військовонавчений ресурс із навчальних центрів (центрів підготовки підрозділів), недостатньому вжитті заходів щодо залучення на військову службу за контрактом та незадовільному рівні виконавчої дисципліни щодо виконання наказів старших начальників з питань реалізації кадрових рішень щодо переміщення військовослужбовців до основних бойових підрозділів військових частин.

Морально-психологічне виснаження військовослужбовців, які тривалий час перебувають у районі бойових дій, пережили загибель товаришів, зазнають хронічної втоми, втрачають мотивацію, призводить до формування глибоких психологічних травм, які можуть впливати на боєздатність підрозділу. Недостатня кількість кваліфікованих фахівців у сфері психологічної підтримки персоналу ускладнює вчасну діагностику та профілактику морально-психологічних проблем особового складу. Відсутність системної програми психологічної реабілітації є серйозною проблемою, що потребує негайного вирішення.

Як свідчить досвід виконання військовослужбовцями бойових завдань у ході збройної агресії РФ, негативний вплив на МПС особового складу має незадовільний рівень забезпечення (нестача набоїв, води, ізоляція, відсутність зв'язку з рідними), загроза полону, інтенсивний вогневий вплив противника (застосування ударних безпілотних літальних апаратів (далі – БпЛА), артилерійського вогню, авіаційних та ракетних ударів), складні погодні умови (холод, спека, опади, туман), конфлікти у підрозділі або у родині військовослужбовця, почуття психічної (фізичної) безпомічності, недостатній рівень соціального захисту військовослужбовців та їх родин, відсутність уваги до дій підрозділів з боку старших начальників.

Не менш важливим є доукомплектування (поповнення, відновлення та модернізація) ОВТ. Інтенсивна експлуатація ОВТ в ході виконання бойових (спеціальних) завдань та вогневий вплив противника призводить до швидкого вичерпання експлуатаційного ресурсу, значних пошкоджень, зносу та втрат. Недостатня кількість та пропускна спроможність ремонтних підрозділів і підприємств, дефіцит запасних частин призводить до тривалих термінів відновлення ОВТ, а також до відсутності резервів для швидкої заміни повністю знищених або таких, які потребують довгострокового ремонту.

Також варто зважати на труднощі з евакуацією пошкодженої техніки з районів ведення бойових дій до ремонтних підрозділів (підприємств), значне логістичне плече, недостатню кількість засобів для евакуації.

Крім того, велика кількість різноманітного озброєння і військової техніки, котрі надходять у підрозділи, створює додаткові виклики щодо забезпечення можливості їх ремонту, забезпечення повною номенклатурою запасних частин. Залежність від постачання західними партнерами, обмеженість власних виробничих потужностей та складність логістичних ланцюгів створюють додаткові труднощі щодо своєчасного доукомплектування військових частин озброєнням і військовою технікою.

Вагомим фактором, що негативно впливає на ефективність відновлення боєздатності, є дефіцит придатних до використання запасів МТЗ, передусім ракет та артилерійських

боєприпасів. Це зумовлено як високою інтенсивністю їх витрачання під час бойових дій, так і недостатніми обсягами постачання.

Руйнування транспортної інфраструктури, складність організації постачання в умовах бойових дій, а також необхідність налагодження ефективної системи обліку та розподілу ресурсів створюють значні логістичні виклики.

Підготовленість особового складу на початок відновлення боєздатності є одним із визначальних внутрішніх факторів. Чим вищий рівень індивідуальної та колективної підготовленості військовослужбовців, тим менше часу необхідно на проведення бойового злагодження та відновлення спроможності військової частини виконувати бойові (спеціальні) завдання. Натомість недостатній рівень навченості новоприбулого особового складу, невідповідність військово-облікових спеціальностей займаним посадам і відсутність практичного бойового досвіду збільшують тривалість відновлення боєздатності та потребують додаткових заходів підготовки.

У процесі організаційних заходів під час відновлення боєздатності з особовим складом проводяться заходи вхідного контролю під керівництвом керівника оперативної групи з відновлення боєздатності для визначення їх рівня навченості. Також перевіряється відповідність військово-облікових спеціальностей особового складу, оскільки часто кваліфіковані фахівці (члени екіпажів, обслуг, розрахунків, командири танків, бойових машин, гармат) прибувають до військових частин не за прямою військово-обліковою спеціальністю без попереднього проходження служби на відповідних посадах.

Отже, аналіз перерахованих вище факторів вказує на те, що вони мають значний вплив на ефективність відновлення боєздатності військової частини і повинні бути враховані під час розроблення методики оцінювання ефективності відновлення боєздатності військової частини.

Дискусія і висновки. Таким чином, проведене дослідження дає підстави стверджувати, що відновлення боєздатності є складним і багатогранним процесом, спрямованим на покриття втрат, завданих противником, та досягнення потрібного рівня боєздатності, який дозволяє реалізувати свої бойові можливості та забезпечує виконання військовою частиною бойового завдання. У роботі систематизовано ключові фактори, які впливають на цей процес, шляхом їх поділу на дві групи. Встановлено, що зовнішні фактори, такі як характер та інтенсивність бойових дій, форми і способи застосування військ (сил); час, необхідний військовій частині на відновлення боєздатності; негативний інформаційний вплив противника; можливості противника завдавати ураження по районах проведення відновлення боєздатності; міжнародна підтримка світової спільноти; район відновлення боєздатності та суспільно-політична обстановка в ньому; вимоги доктринальної бази з відновлення боєздатності, мають об'єктивний характер і майже не піддаються контролю з боку суб'єктів відновлення боєздатності.

Натомість визначальний вплив на ефективність процесу здійснюють внутрішні фактори, оскільки вони є керованими та безпосередньо відображають кінцевий результат. До них належать діяльність суб'єктів відновлення боєздатності щодо доукомплектування особовим складом, озброєнням і військовою технікою, поповнення матеріально-технічних засобів, проведення заходів відновлення морально-психологічного стану особового складу та бойового злагодження; укомплектованість військової частини особовим складом на початок відновлення боєздатності; морально-психологічний стан особового складу на початок відновлення боєздатності; забезпеченість військової частини озброєнням і військовою технікою на початок відновлення боєздатності; забезпеченість військової частини матеріально-технічними засобами на початок відновлення боєздатності; підготовленість особового складу військової частини на початок відновлення боєздатності. Аналіз показав, що сучасні виклики потребують вдосконалення існуючих підходів до управління ресурсами та адаптації доктринальної бази до стандартів держав-членів НАТО з відновлення боєздатності.

Результати дослідження можуть бути використані під час розроблення доктринальних документів, які регламентують питання організації відновлення боєздатності, в практиці

організації та проведення відновлення боєздатності та у ході подальших досліджень з даного напрямку у наукових установах. Перспективами подальших наукових досліджень у даному напрямі може бути розроблення нових підходів до проведення бойового злагодження військових частин (підрозділів) в умовах сучасної війни.

Внесок авторів: Дмитро Савчук – концептуалізація, методологія, написання (оригінальна чернетка), Олександр Георгадзе – методологія, написання (перегляд і редагування).

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

ЛІТЕРАТУРА:

1. Георгадзе О. А., Горбач Р. Я. Концептуальні засади впровадження рекрутингу у Збройних Силах України. *Збірник наукових праць військового інституту Київського національного університету імені Тараса Шевченка*. 2024. № 85. с. 94–105. DOI: <https://doi.org/10.17721/2519-481X/2024/85-10>
2. Георгадзе О. А., Ніколайчук О. О. Обґрунтування сукупності показників до методики оцінювання ефективності базової загальновійськової підготовки. *Збірник наукових праць військового інституту Київського національного університету імені Тараса Шевченка*. 2024. № 85. с. 106–115. DOI: <https://doi.org/10.17721/2519-481X/2024/85-11>
3. Георгадзе О. А., Савчук Д. В. Обґрунтування сукупності показників до методики оцінювання ефективності відновлення боєздатності військової частини. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України*. 2025. № 2 (85). с. 120–125. DOI: <https://doi.org/10.33099/2304-2745/2025-2-85/120-125>
4. Георгадзе О. А., Салаш О. А. Обґрунтування сукупності показників до комплексної методики оцінювання ефективності оперативної підготовки. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки*. 2022. № 3 (88). с. 5–17. DOI: <https://doi.org/10.32453/3.v88i3>
5. Георгадзе О. А., Салаш О. А. Часткова методика оцінювання стану колективної підготовки органів військового управління. *Збірник наукових праць військового інституту Київського національного університету імені Тараса Шевченка*. 2022. № 77. с. 161–171. DOI: <https://doi.org/10.17721/2519-481X/2022/77-14>
6. Георгадзе О. А., Харабара В. І. Часткова методика оцінювання рівня підготовленості танкової бригади у ході відновлення боєздатності. *Social development and security*. 2019. Vol. 9, no. 4 p. 131–142. DOI: <https://doi.org/10.33445/sds.2019.9.4.10>
7. Керівництво "Відновлення боєздатності" (ТКП 7-178 / АТР 3-94.4) : затверджено Головнокомандувачем Збройних Сил України в 2025 р. Київ, 2025.
8. Програма бойового злагодження загальновійськових частин (підрозділів) ЗС України, що відновлюють боєздатність (для формування наступальних спроможностей), (ТП 7 – (01,03 – 05) 178.55.) : затверджено Заступником Головнокомандувача Збройних Сил України в 2023 р. Київ, 2023.
9. Програма бойового злагодження загальновійськових частин (підрозділів) Сухопутних військ ЗС України, що відновлюють боєздатність (для формування оборонних спроможностей), (СТП 7 – (01,02) 178.55.) : затверджено Командувачем Сухопутних військ ЗС України в 2024 р. Київ, 2024.
10. Макаліш О. В., Георгадзе О. А. Методичний підхід до оцінювання рівня навченості органів військового управління тактичного рівня. *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ*. 2016. № 3 (58). с. 104–108. DOI: <https://doi.org/10.33099/2304-2745/2016-3-58/104-108>
11. Молдавчук В. Обґрунтування напрямку дослідження оцінювання та прогнозування суспільно-політичної обстановки для прийняття рішень на службово-бойові дії. *Збірник наукових праць НАДПСУ. Серія: військові та технічні науки*. 2013. № 2. с. 148–153.
12. Погляди щодо організації та проведення індивідуальної підготовки офіцерського складу органів військового управління / Ю. Є. Репіло та ін. *Збірник наукових праць ВІКНУ*. 2024. № 82. с. 59–66. DOI: <https://doi.org/10.17721/2519-481X/2024/82-07>
13. Савчук Д. В., Георгадзе О. А. Часткова методика оцінювання укомплектованості військової частини військовослужбовцями. *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ*. 2024. № 2 (3-83). с. 117–121. DOI: <https://doi.org/10.33099/2304-2745/2024-3-83/117-121>

14. Савчук Д. В., Георгадзе О. А. Часткова методика оцінювання морально-психологічного стану особового складу. *Social development and security*. 2025. Vol. 15, no. 3. с. 100–107. DOI: <https://doi.org/10.33445/sds.2025.15.3.11>
15. Савчук Д. В., Георгадзе О. А. Часткова методика оцінювання рівня підготовленості особового складу військової частини в умовах дії правового режиму воєнного стану. *Збірник наукових праць Центру воєнно-стратегічних досліджень НВООУ*. 2025. № 3 (86). с. 138–144. DOI: <https://doi.org/10.33099/2304-2745/2025-3-86/138-144>
16. Еволюція форм і способів застосування угруповань військ (сил): тенденції збройної боротьби / О. Семененко та ін. *Social development and security*. 2024. Vol. 14, no. 3. p. 33–52.
17. Інформаційний вимір збройного протистояння України і Росії / С. Сідченко та ін. *Збірник наукових праць ХНУПС*. 2023. № 2 (76). с. 39–48.
18. Програма "Адаптації та допідготовки військовослужбовців до ведення бойових дій" ... (ТП 7-00 (242) 352.62(63)) : затверджено ТВО начальника ГШ ЗС України в 2024 р. Київ, 2024.
19. Heorhadze O. Methods for assessing the level of the organization of joint training of defence forces. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. № 2 (44). с. 43–47. DOI: <https://doi.org/10.33099/2311-7249/2022-44-2-43-47>
20. Reconstitution Operations. Tactical Publication ATR 3-94.4. May 2021 edition. 2021.
21. Vynokurov D., Heorhadze O. Comprehensive methodology for evaluating the effectiveness of training the variable composition of the training center. *Political Science and Security Studies Journal*. 2021. Vol. 2, no. 2. p. 77–85. DOI: <https://doi.org/10.5281/zenodo.5071081>

REFERENCES:

1. Heorhadze, O. (2022). Methods for assessing the level of the organization of joint training of defense forces. *Suchasni informatsiini tekhnologii u sferi bezpeky ta oborony – Modern Information Technologies in the Sphere of Security and Defence*, 2(44), 43–47. <https://doi.org/10.33099/2311-7249/2022-44-2-43-47> [in English].
2. Heorhadze, O. A., & Horbach, R. Ya. (2024). Conceptual principles of recruitment implementation in the Armed Forces of Ukraine. *Zbirnyk naukovykh prats viiskovoho instytutu Kyivskoho Natsionalnoho universytetu imeni Tarasa Shevchenka – Collection of Scientific Papers of the Military Institute of Taras Shevchenko National University of Kyiv*, 85, 94–105. <https://doi.org/10.17721/2519-481Kh/2024/85-10> [in Ukrainian].
3. Heorhadze, O. A., & Nikolaichuk, O. O. (2024). Substantiation of a set of indicators for the methodology of assessing the effectiveness of basic combined arms training. *Zbirnyk naukovykh prats viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka*, 85, 106–115. <https://doi.org/10.17721/2519-481Kh/2024/85-11> [in Ukrainian].
4. Heorhadze, O. A., & Salash, O. A. (2022a). Substantiation of the set of indicators for the complex methodology of assessing the effectiveness of operational training. *Zbirnyk naukovykh prats Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Seriya: viiskovi ta tekhnichni nauky*, 3(88), 5–17. <https://doi.org/10.32453/3.v88i3> [in Ukrainian].
5. Heorhadze, O. A., & Salash, O. A. (2022b). Partial methodology of assessing the state of collective training of military management bodies. *Zbirnyk naukovykh prats viiskovoho instytutu Kyivskoho Natsionalnoho universytetu imeni Tarasa Shevchenka*, 77, 161–171. <https://doi.org/10.17721/2519-481X/2022/77-14> [in Ukrainian].
6. Heorhadze, O. A., & Savchuk, D. V. (2025). Substantiation of the set of indicators for the methodology of assessing the effectiveness of restoring the combat capability of a military unit. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy*, 2(85), 120–125. <https://doi.org/10.33099/2304-2745/2025-2-85/120-125> [in Ukrainian].
7. Heorhadze, O. A., & Kharabara, V. I. (2019). Partial methodology for assessing the level of readiness of a tank brigade during the restoration of combat capability. *Social development and security*, 9(4), 131–142. <https://doi.org/10.33445/sds.2019.9.4.10> [in Ukrainian].
8. Holovnokomanduvach Zbroinykh Syl Ukrainy. (2025). *Kerivnytstvo "Vidnovlennia boiezdatnosti" (TKP 7-178 / ATR 3-94.4)* [Manual "Restoration of combat capability"]. Kyiv [in Ukrainian].
9. Komanduvach Sukhoputnykh viisk ZS Ukrainy. (2024). *Prohrama boiovoho zlahodzhennia... (STP 7 – (01,02) 178.55.)* [Ground Forces combat synchronization program]. Kyiv [in Ukrainian].
10. Makalish, O. V., & Heorhadze, O. A. (2016). Methodological approach to assessing the level of training of tactical aviation brigade personnel. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh*

doslidzhen Natsionalnoho universytetu oborony Ukrainy imeni Ivana Cherniakhovskoho, 3(58), 104–108. <https://doi.org/10.33099/2304-2745/2016-3-58/104-108> [in Ukrainian].

11. Moldavchuk, V. (2013). Substantiation of the research direction for assessing and forecasting the socio-political situation for decision-making on service and combat operations. *Zbirnyk naukovykh prats Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Seriya: viiskovi ta tekhnichni nauky*, 2, 148–153 [in Ukrainian].

12. *RECONSTITUTION OPERATIONS*. (2021). Tactical Publication ATR 3-94.4, May 2021 edition [in English].

13. Repilo, Yu. Ye., Heorhadze, O. A., Vynokurov, D. V., Kamalov, Ye. V., Chaikovska, O. Ye., & Kliuchak, O. M. (2024). Views on the organization and conduct of individual training of the officer personnel of military command and control bodies. *Zbirnyk naukovykh prats BIKNU*, 82, 59–66. <https://doi.org/10.17721/2519-481Kh/2024/82-07> [in Ukrainian].

14. Savchuk, D. V., & Heorhadze, O. A. (2024). Partial methodology for assessing the manning of a military unit with service members. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy*, 2(3-83), 117–121. <https://doi.org/10.33099/2304-2745/2024-3-83/117-121> [in Ukrainian].

15. Savchuk, D. V., & Heorhadze, O. A. (2025a). Partial methodology for assessing the moral and psychological state of personnel. *Social development and security*, 15(3), 100–107. <https://doi.org/10.33445/sds.2025.15.3.11> [in Ukrainian].

16. Savchuk, D. V., & Heorhadze, O. A. (2025b). Partial methodology for assessing the level of training of military unit personnel under the conditions of the legal regime of martial law. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy*, 3(86), 138–144. <https://doi.org/10.33099/2304-2745/2025-3-86/138-144> [in Ukrainian].

17. Semenenko, O., Mytchenko, S., Dobrovolskyi, Yu., Yarmolchuk, M., Remez, A., & Tverdokhlib, Ye. (2024). Evolution of forms and methods of employment of troop (force) groupings: trends of armed struggle. *Social development and security*, 14(3), 33–52 [in Ukrainian].

18. Sidchenko, S., Revin, O., Zalkin, S., Khudarkovskyi, K., & Bolbas, O. (2023). Information dimension of the armed confrontation between Ukraine and Russia. *Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl*, 2(76), 39–48 [in Ukrainian].

19. TVO nachalnyka HSh ZS Ukrainy. (2024). *Prohrama "Adaptatsii ta dopidhotovky viiskovosluzhbovtiv..." (TP 7-00 (242) 352.62(63))* [Adaptation and additional training program]. Kyiv [in Ukrainian].

20. Vynokurov, D., & Heorhadze, O. (2021). Comprehensive methodology for evaluating the effectiveness of training the variable composition of the training center. *Political Science and Security Studies Journal*, 2(2), 77–85. <https://doi.org/10.5281/zenodo.5071081> [in English].

21. Zastupnyk Holovnokomanduvacha Zbroinykh Syl Ukrainy. (2023). *Prohrama boiovoho zlahodzhennia.. (TP 7 – (01,03 – 05) 178.55.)* [AFU combat synchronization program]. Kyiv [in Ukrainian].

Savchuk D., PhD, Assoc. Prof. Heorhadze O.

MAIN FACTORS AFFECTING THE EFFECTIVENESS OF RESTORING THE COMBAT CAPABILITY OF A MILITARY UNIT

Background. *The problem of restoring the combat capability of the Armed Forces of Ukraine has acquired critical importance due to the intensity of combat operations and significant losses. The purpose of the article is to highlight the main factors affecting the effectiveness of restoring combat capability under the legal regime of martial law.*

Methods. *The study was conducted using the following methods: analysis and synthesis to define the research problem and goals; content analysis of scientific sources and practical combat experience to systematize influence factors; generalization and systematization for preparing research conclusions.*

Results. *External (unmanageable) and internal (manageable) factors have been systematized. It is proven that internal factors have the greatest influence: activities of the combat capability restoration actors regarding replenishment of personnel, weapons and military equipment (WME), resupply of logistics, execution of measures to restore the morale and psychological state of personnel, and combat integration training; the unit's personnel strength, morale and psychological state, equipment availability, logistical*

sufficiency, and training level at the beginning of the restoration process.

Conclusions. The research results can be used in the development of regulatory documents for combat capability restoration, in practical restoration activities, and during further research in scientific institutions.

Keywords: restoration of combat capability, external factors, internal factors, military unit, efficiency.

ДАНІ ПРО АВТОРІВ

Бабич Трохим Анатолійович, заступник декана факультету інформатики, Національний університет "Києво-Могилянська академія", м. Київ, Україна, ORCID: 0009-0008-5657-3517.

Бойко Ілля Віталійович, студент Національного університету "Києво-Могилянська академія", м. Київ, Україна, ORCID: 0009-0003-7183-5224.

Вознюк Ярослав Іванович, старший викладач кафедри інформатики Національного університету "Києво-Могилянська академія", м. Київ, Україна, ORCID: 0009-0002-1280-3671.

Гахович Сергій Вікторович, кандидат технічних наук, старший науковий співробітник, доцент кафедри військово-технічної підготовки Військового інституту Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0002-9135-6568.

Георгадзе Олександр Аміранович, кандидат військових наук, доцент, Генеральний штаб Збройних Сил України, м. Київ, Україна, ORCID: 0000-0002-9306-6660.

Добровольський Юзеф Броніславович, кандидат технічних наук, доцент, старший науковий співробітник, заступник начальника кафедри з навчальної та наукової роботи – начальник навчальної частини кафедри військової підготовки Національного університету "Київський авіаційний інститут", м. Київ, Україна, ORCID: 0000-0002-1077-1402.

Деркач Єлизавета Романівна, студентка Національного університету "Києво-Могилянська академія", м. Київ, Україна, ORCID: 0009-0009-5416-5306.

Долінчук Катерина Олександрівна, аспірантка факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: 0009-0000-6913-200X.

Дубик Олександр Миколайович, кандидат технічних наук, доцент, Національний університет "Київський авіаційний інститут", м. Київ, Україна, ORCID: 0000-0001-8082-7603.

Дьяконенко Денис Костянтинович, студент, Національний університет "Києво-Могилянська академія", м. Київ, Україна, ORCID: 0009-0003-2554-8611.

Каберник Володимир Олегович, аспірант кафедри радіотехніки та радіоелектронних систем факультету радіофізики, електроніки та комп'ютерних систем (спеціальність 172 "Телекомунікації та радіотехніка"), Київський національний університет імені Тараса Шевченка, м. Київ, Україна, ORCID: 0009-0004-6917-6431.

Маслов Петро Сергійович, студент Національного університету "Києво-Могилянська академія", м. Київ, Україна, ORCID: 0009-0004-8755-0378.

Ольшевський Сергій Валентинович, доктор технічних наук, доцент, доцент кафедри радіотехніки та радіоелектронних систем факультету радіофізики, електроніки та комп'ютерних систем, Київський національний університет імені Тараса Шевченка, м. Київ, Україна, ORCID: 0000-0003-4499-8485.

Радзієвська Олександра Володимирівна, старша викладачка кафедри інформатики, Національний університет "Києво-Могилянська академія", м. Київ, Україна, ORCID: 0009-0000-2731-8930.

Сашньова Мар'яна Василівна, кандидат технічних наук, доцент, Національний університет "Києво-Могилянська академія", м. Київ, Україна, ORCID: 0000-0002-3501-0933.

Савченко Тетяна Віталіївна, кандидат технічних наук, доцент кафедри інформатики Національного університету "Києво-Могилянська академія", м. Київ, Україна, ORCID: 0000-0002-8884-5360.

Савчук Дмитро Володимирович, ад'юнкт, Національний університет оборони України, м. Київ, Україна, ORCID: 0009-0004-8567-9338.

Целованський Тихон Романович, аспірант 3 курсу групи АKN-31 кафедри комп'ютерних наук Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна, ORCID: 0009-0006-7574-126X.

Черкасов Дмитро Іванович, кандидат технічних наук, завідувач кафедри мережних технологій, Національний університет "Києво-Могилянська академія", м. Київ, Україна, ORCID: 0000-0001-6448-0945.

Ярмольчик Марія Олегівна, доктор філософії, начальник науково-дослідної лабораторії кафедри військової підготовки Національного університету "Київський авіаційний інститут", м. Київ, Україна, ORCID: 0000-0001-9917-0189.

АЛФАВІТНИЙ ПОКАЗЧИК

Бабич Т.А.	35, 65	Каберник В.О.	17
Бойко І.В.	51	Маслов П.С.	77
Вознюк Я.І.	51, 77	Ольшевський С.В.	17
Гахович С.В.	51, 65	Радзієвська О.В.	35, 51
Георгадзе О.А.	103	Савченко Т.В.	65
Деркач Є.Р.	65	Сашньова М.В.	35, 77
Добровольський Ю.Б.	93	Савчук Д.В.	103
Долінчук К.О.	7	Целованський Т.Р.	29
Дубик О.М.	93	Черкасов Д.І.	77
Дьяконенко Д.К.	35	Ярмольчик М.О.	93

РЕДАКЦІЙНА ПОЛІТИКА ТА ЕТИЧНІ НОРМИ ПРИНЦИПИ ФОРМУВАННЯ ТА ДОСТУП ДО ЗМІСТУ "ЗБІРНИКА ВІКНУ"

Редакційна політика "Збірника ВІКНУ" заснована на принципах об'єктивності та неупередженості під час відбору статей для публікації; високих вимог до якості наукових досліджень; обов'язковості та конфіденційності рецензування статей; додержання колегіальності у відборі до публікації статей; доступності та оперативності у спілкуванні з авторами; суворого дотримання авторських і суміжних прав. Запобігання протизаконним публікаціям є відповідальністю кожного автора, редактора, рецензента, видавця.

До друку приймаються оригінальні рукописи, які не були опубліковані раніше та не відправлялись до інших редакцій, які повністю відповідають вимогам стосовно оформлення та порядку подання статей.

У "Збірнику ВІКНУ" сформовані наступні рубрики: військова техніка і технології подвійного призначення, інформаційні технології, загальні питання.

Редакція підтримує політику відкритого доступу та принципи вільного поширення наукової інформації. Примірники збірників знаходяться у Національній бібліотеці України ім. В.І. Вернадського, науковій бібліотеці ім. М. Максимовича, у бібліотеці Військового інституту та інших бібліотеках України. Електронна версія розміщена на сайті інституту, на сайтах наведених бібліотек та на сайтах "Збірника ВІКНУ": <http://miljournals.knu.ua/index.php/zbirruk>; <http://mil.univ.kiev.ua/page/lib/31>

ЕТИКА ПУБЛІКАЦІЙ

Редакційна колегія журналу вимагає від авторів наслідувати формальним та етичним правилам підготовки і публікації наукових робіт, які вони подають до редакції журналу. Ці норми зумовлено стандартами якості наукових статей, прийнятими у світовому науковому співтоваристві, зокрема публікаційними принципами Publishing Ethics Resource Kit (PERK), рекомендаціями Elsevier, Комітету з етики публікацій (Committee on Publication Ethics, COPE), етичним кодексом вченого України, а також досвідом роботи іноземних та українських професіональних спільнот, наукових організацій, редколегій та редакцій видань.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ РЕДАКЦІЙНОЇ КОЛЕГІЇ ЖУРНАЛУ

Редакційна колегія у своїй діяльності

- керується принципами неупередженості, наукової етики рецензування, захисту інтелектуальної власності;
- несе відповідальність за рівень наукового наповнення журналу;
- виступає проти фальсифікації, плагіату, направлення автором одного рукопису до кількох журналів, багаторазового копіювання тексту статті в різних місцях, введення громадськості в оману щодо реального внеску кожного автора в опубліковану наукову роботу;
- залишає за собою право направити рукопис на розгляд сторонньому рецензенту, в тому числі ретельний відбір через "сліпе" рецензування, відхилити статтю або повернути її на доопрацювання;
- може відхилити рукопис, якщо вважає, що він не відповідає профілю журналу, чи не відповідає етиці та правилам оформлення;
- має право вилучити вже опубліковану статтю в разі виявлення порушення будь-чиїх прав або загальноприйнятих норм наукової етики, про цей факт вилучення статті редакція повідомляє як автору статті, так і організації, де було виконано дослідження та повідомляє про це у наступному номері.

Співробітники редакції не надають іншим особам інформації, пов'язаної із змістом рукописів, що перебувають на розгляді, крім осіб, які беруть участь у її фаховій оцінці.

Згідно з міжнародним законодавством щодо додержання авторського права на електронні інформаційні ресурси, матеріали сайту, електронного журналу або проєкту не можуть бути відтворені повністю або частково у будь-якій формі (електронній чи друкованій) без попередньої письмової згоди редакції журналу. Під час використання опублікованих матеріалів у контексті інших документів обов'язково необхідними є посилання на першоджерело.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ АВТОРА

Автор:

- несе відповідальність за новизну і достовірність наведених у статтях результатів, тактико-технічних та економічних показників, коректність висловлювань, а також за те, що в матеріалах не міститься інформація з обмеженим доступом;

- повинен цитувати ті публікації, які мали визначальний вплив на суть викладеного у статті, а також ті, які можуть швидко ознайомити читача з більш ранніми працями, важливими для розуміння цього дослідження, необхідно також належним чином вказувати джерела принципово важливих матеріалів, використаних у цій роботі, якщо вони не були отримані самим автором;

- забезпечує недопустимість плагіату та подання до публікації раніше надрукованих матеріалів, у випадку виявлення зазначених фактів відповідальність несе автор поданих матеріалів.

Співавторами статті мають бути всі особи, що зробили вагомий науковий внесок у подану роботу і поділяють відповідальність за отримані результати. Автор, який подає рукопис до публікації, відповідає за те, щоб до списку співавторів були включені тільки ті особи, які відповідають критерію авторства, та бере на себе відповідальність за згоду інших авторів статті на її публікацію в журналі.

УВАГА!

Для авторів статей дещо доопрацьовані вимоги щодо особистих даних.

Ці дані подаються українською та англійською мовами в такій послідовності: Прізвище

Ім'я_по - батькові. Науковий ступінь та вчене звання. Місце роботи та посада

ORCID 0000-0001-3215-4400

SCOPUS ID 57193059215 (за наявності) Індекс DBLP 10 (за наявності)

e-mail: __ моб. телефон

Надсилати скановані рисунки, формули та таблиці не допускається.

Вся стаття оформлюється одним шрифтом **Times New Roman**, вказаними нижче розмірами, зверніть увагу на формули, таблиці та рисунки.

РЕДАКЦІЙНА КОЛЕГІЯ "ЗБІРНИКА ВІКНУ" ЗДІЙСНЮЄ НЕЗАЛЕЖНЕ ("СЛІПЕ" ЕКСПЕРТНЕ РЕЦЕНЗУВАННЯ НАДАНИХ ДО ДРУКУ РУКОПИСІВ ТА ПЕРЕВІРКУ ЇХ НА ПЛАГІАТ. РЕЦЕНЗУВАННЯ ЗДІЙСНЮЄТЬСЯ ЗА АНОНІМНОЮ ФОРМОЮ ЯК ДЛЯ АВТОРІВ, ТАК І ДЛЯ РЕЦЕНЗЕНТІВ.

ПОРЯДОК ПОДАННЯ І ОФОРМЛЕННЯ СТАТЕЙ ДО "ЗБІРНИКА НАУКОВИХ ПРАЦЬ ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА"

До друку приймаються оригінальні рукописи, які не були опубліковані раніше, не були відправлені до інших редакцій та повністю відповідають вимогам щодо оформлення та порядку подання статей.

Загальні вимоги до технічного оформлення статей:

Обсяг рукопису - рекомендується не менше 12 повних аркушів українською або англійською мовами.

Формат аркуша - A4 (210 x 297 мм).

Розмір полів: верхнє, нижнє, праве, ліве - 2 см.

Шрифт тексту - Times New Roman №12, через міжрядковий інтервал - 1,0.

Абзац має становити 10 мм.

Стаття повинна мати такі необхідні елементи:

УДК;

назва статті, яка лаконічно відображає зміст та новизну статті;

анотація та ключові слова;

вступ та постановка задачі чи проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

аналіз останніх досліджень і публікацій, в яких започатковано розв'язання цієї проблеми і на які спирається автор, визначення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття, формулювання мети статті;

виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів, практичних рішень та експериментів;

висновки з цього дослідження і перспективи подальшого розвитку в цьому напрямку,

список літератури,

References,

дані про авторів двома мовами.

Анотація до статті виконується українською та англійською мовами загальний обсяг кожної не менш ніж 1800 знаків, включаючи ключові слова.

Вона повинна містити коротке повторення структури статті, що включає вступ, цілі і завдання, методи, результати, висновки.

Анотацію друкують курсивом, шрифт Times New Roman, №11. Після анотації розміщуються **ключові слова** (5–7 термінів).

Список літератури (References) повинен включати не менш 12 джерел, з яких 50% видані за останні 10 років. При цьому не менш 25% джерел повинно відноситися до іноземної періодики. Самоцитовання авторів у списку літератури повинно бути, як правило, не більш за 25%.

Якщо основною мовою статті є українська, то оформляються два списки літератури: перший (список літератури мовою оригіналу джерела) – згідно з наказом МОН від 12.01.2017 № 40 та відповідно до ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання: загальні положення та правила складання";

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН від 12.01.2017 № 40 та міжнародного Гарвардського стилю BSI (British Standards Institution).

На адресу редколегії (03022, м. Київ, вул Ю. Здановської, 81, тел.: +38 (044) 521 - 33 - 82) мають бути надіслані наступні матеріали:

експертний висновок про можливість відкритого публікування, завірений печаткою, сканкопія надсилається на e-mail: collection.works@knu.ua

Вимоги до оформлення References

References потрібно приводити окремим блоком, повторюючи послідовність попередньо наведеного Списку літератури. Джерела при цьому оформлюються за такими основними правилами (Harvard style оформлення BSI: British Standards Institution):

–запис завжди починається з прізвища автора, потім кома, ініціали (між ініціалами пропуски не ставляться), за якими в дужках вказується дата видання; два автори відокремлюються "and" без коми; кілька авторів розділяються комами, але останнє прізвище повинно бути відокремлене "and" без коми;

–витяги з публікацій, тобто назви статей журналів, глав в книгах наводяться в "лапках";

–назва журналу або книги завжди виділяється курсивом;

–ім'я видавця вказується перед місцем видання;

–коми використовують для поділу елементів запису;

–для джерел українською або російською мовами, що наводяться у References, назви статей журналів, глави з книг наводяться латиницею (транслітерацією) в "лапках" та перекладаються англійською мовою в квадратних дужках. Онлайн-конвертер з української мови для транслітерації: <http://translit.kh.ua/?passport>.

Приклади оформлення References за стилем Harvard British Standards Institution

Книга (ДСТУ 8302:2015)

Інформаційно-психологічна боротьба у війсьній сфері: монографія / Г.В. Певцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Х.: Вид. Рожко С.Г., 2017. 276 с.

Книга (Harvard style BSI)

Pievtsov, H.V., Hordiienko, A.M., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2017), "Informatsiino-psykholohichna borotba u voiennoi sferi: monohrafiia" [The information and psychological struggle in the military sphere], Rozhko S.H., Kharkiv, 276 p.

Стаття із періодичного видання (ДСТУ 8302:2015)

Карпенко, Д.В. Стан та перспективи розвитку зенітного ракетного озброєння Повітряних Сил Збройних Сил України / Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 2(27). С. 75–78.

Стаття із періодичного видання (Harvard style BSI)

Karpenko, D.V. (2017), "Stan ta perspektyvy rozvytku zenitnoho raketnoho ozbroiennia Povitrianykh Syl Zbroinykh Syl Ukrainy" [The state and perspectives of the development of anti-aircraft missile armaments in the Air Force of Ukraine], Science and Technology of the Air Force of Ukraine, No. 2(27), pp. 75–78.

Дисертація (ДСТУ 8302:2015)

Белозеров, І.В. Религиозная политика: дис. ... канд. ист. наук: 07.00.02; захищена 22.01.02; утв. 15.07.02 / Белозеров Иван Валентинович. К., 2002. 215 с.

Дисертація (Harvard style BSI)

Belozerov, I.V. (2002), "Relyhyoznaia polityka: dissertation" [The religious policy: dissertation], Kiev, 215 p.

Джерела електронного ресурсу віддаленого доступу (ДСТУ 8302:2015)

Романов В. К вопросу о путях достижения национальной безопасности в условиях глобализации: проблемы теории и практики в контексте внешней политики России и Польши [Електронний ресурс] Безопасность и оборона, 2016. № 1(2), С. 7–15. Режим доступу до журн.: http://www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf.

Джерела електронного ресурсу віддаленого доступу (Harvard style BSI)

Romanov, V. (2016), "K voprosu o putyakh dostizheniya natsionalnoy bezopasnosti v usloviyakh globalizatsii: problemy teorii i praktiki v kontekste vneshney politiki Rossii i Polshi" [To the question about the ways to achieve national security in the context of globalization: the problems

of theory and practice in the context of the foreign policy of Russia and Poland], Security and Defence Journal, No. 1(2), pp. 7–15, www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf (accessed 12 July 2017). (примітка: при наведенні URL "http: //" має бути виключено).

Більш детальну інформацію щодо оформлення бібліографічних посилань за стилем Harvard British Standards Institution можна знайти на сайті *Національної бібліотеки України імені В.І. Вернадського* та онлайн генератора посилань *Cite This For Me*.

Редакційна колегія: collection.works@knu.ua

Шрифт

**СХЕМА ОФОРМЛЕННЯ СТАТЕЙ
У "ЗБІРНИКУ НАУКОВИХ ПРАЦЬ ВІКНУ"**

УДК

науковий ступінь, вчене звання
ініціали та прізвище автора (співавторів)
місце роботи автора (співавторів)

12 пт

УДК 32.973.202:07.681

д.т.н., проф. Степанов С.В. (ВІКНУ)
к.т.н., с.н.с. Українець О.В. (ВІКНУ)
Саленко В.Д. (ВІКНУ)

**12 пт
жирний**

**КЕРУВАННЯ ЕЛЕКТРОННИМИ ПРИСТРОЯМИ ЗА ДОПОМОГОЮ
ЖЕСТІВ**

Анотація до статті виконується українською та англійською мовами (загальний обсяг кожної не менш, ніж **1800** знаків, включаючи ключові слова).

**11 пт
курсив,
жирний**

Для керування електронними пристроями, для сучасного користувача важливими термінами є такі, як: зручність та простота керування. Для того, щоб надати користувачеві такі можливості та зручності в використанні, є досить доцільною робота системи, яка б надавала такі можливості. Керування системою, яка працює на основі жестів, є надзвичайно перспективним, та може суттєво полегшити користувачеві роботу з нею, тому що жести, які потрібні для керування системою, мають бути інтуїтивно зрозумілими користувачеві, порівняно з іншими системами, які існують за допомогою комбінацій клавіш.

Для вирішення задач керування за допомогою жестів, пропонується програмно-апаратний комплекс, який побудований на основі різних модулів, кожен з яких в свою чергу виконує відповідну роль в системі, наприклад, знаходить точку інтересу з множини чи знаходить глибину сцени. Також у системі є ядро, яке відповідає за аналіз модифікаторів та жестів. На основі даних модулів стає можливо створити систему, яка б працювала на основі жестів. Але для створення цієї системи, потрібно вирішити певні задачі, які як: сегментація, скелетизація, спостереження. Кожна з яких містить в собі певні математичні моделі та визначення. Запропонований програмно-апаратний комплекс для керування природними жестами. Суть програмно-апаратного комплексу полягає в тому, щоб забезпечити користувача таким інтерфейсом, щоб він виконував роботу знаходячись частково віддалено від робочого місця, чи маніпулював інструментами на відстані, тобто за допомогою жестів. Використання запропонованого програмно-апаратного комплексу дозволить покращити показники стерильності в медичних, підвищити технічну безпеку під час виконання безпосередньої роботи користувача з приладами.

Ключові слова: штучний інтелект, контролери, модулі, жести, глибина сцени, точка інтересу, аналіз модифікаторів, аналіз жестів, сегментація, скелетизація, спостереження.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ СТАТТІ

12 пт **НЕОБХІДНІ ЕЛЕМЕНТИ СТАТТІ:** вступ та постановка проблеми (задачі) у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями; аналіз останніх досліджень і публікацій, в яких започатковано розв'язання цієї проблеми і на що спирається автор, виділення невирішених раніше частин загальної проблеми, яким присвячується ця стаття, формулювання цілей статті (постановка завдання), виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів; їх практичного значення та результатів експеримента чи впровадження; висновки з дослідження і перспективи подальших досліджень у цьому напрямку. **Література. References.**

УВАГА! Таблиці і рисунки друкують після посилань. Якщо у статті кілька таблиць чи рисунків - їх нумерують. Заголовки таблиць і рисунків необхідно розміщувати по центру, а нумерацію таблиць праворуч від таблиці (стиль **normal**, шрифт - **Times New Roman № 12**).

Рисунки повинні бути виконані за допомогою редактора Word, згруповані і являти собою один графічний об'єкт. Формули та позначення по тексту обов'язково набирати за допомогою Equation Editor - редактора формул Word, а не у текстовому режимі. У редакторі формул мають бути встановлені такі параметри - розміри: загальний.

12 pt. великі індекси – **10 pt**, малі індекси – **7 pt**, великі символи – **14 pt**, малі символи.

10 pt: стиль: текст, функції, змінні, матриці-вектори, числа – шрифт Times New Roman, для решти стилів – шрифт Symbol, при цьому: строк. грецькі – прямі. Великі за розміром вирази та рівняння необхідно записувати у кілька рядків.

ЛІТЕРАТУРА

Перший (список літератури на мові оригіналу джерела) – згідно з наказом МОН № 40 від 12.01.2017 та відповідно до ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання: загальні положення та правила складання";

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН № 40 від 12.01.2017 та міжнародного Гарвардського стилю BSI (British Standards Institution).

ЛІТЕРАТУРА:

11 пт

ЗРАЗОК

1. Ленков С.В., Толлок І.В., Цицарев В.М., Ленков Є.С. Моделювання процесів витрачання та поповнення ресурсу угруповання технічних об'єктів. Системи озброєння і військова техніка. Харків. 2018. Вип. 1(53). С. 155 – 162.

2. Жиров Г.Б., Ленков Є.С., Цицарев В.М., Проценко Я.М. Моделювання процесу відмов об'єктів, що відновлюються з ієрархічною конструктивною структурою. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ. 2017. Вип. 55. С. 30-39.

REFERENCES:

11 пт

ЗРАЗОК

1. Lienkov, S.V., Tolok, I.V., Tsytarev, V.N. and Lenkov, Ye.S. (2018), "Modeliuvannia protsesiv vytrachannia ta popovnennia resursu uhrupuvannia tekhnichnykh obiektiv" [Modeling of processes of expenditure and resource replenishment grouping of technical objects], Systems of Arms and Military Equipment, No. 1(53), pp. 155-162.

2. Zhyrov, G.B., Lenkov, Je.S., Cycarjev, V.M. and Procenko, Ja.M. (2017), "Modeljuvannja procesu vidmov ob'ektiv, shho vidnovljut'sja z ijerarhichnoju konstruktyvnoju strukturoju" [Simulation of the process of failure of objects that are restored with a hierarchical constructive structure], Zbirnyk naukovykh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka, No. 55, pp. 30-39

CONTROL ELECTRONIC DEVICES USING GESTURES

For management of electronic devices, for today's user important criteria are: convenience and ease of management. In order to provide the user with such opportunities and usability to use, it is quite reasonable to develop a system that would provide such opportunities. Managing a gesture-based system is extremely promising, but can greatly facilitate the user to work with it, because the gestures that are needed to manage the system can be intuitive to the user, compared to other systems that operate using keyboard shortcuts. To solve the problems of managing using gestures, a software-hardware complex is proposed that is based on different modules, each of which in turn plays an appropriate role in the system, for example, finds a point of interest from a plurality or calculates the depth of a scene. Also, the system has a kernel that is responsible for analyzing modifiers and gestures. Based on the data of the modules it becomes possible to create a system that would work on the basis of gestures. But for the creation of this system, it is necessary to solve certain problems, such as: segmentation, skeletalization, observation. Each of them contains the corresponding mathematical models and definitions. Proposed hardware and software complex for management of natural gestures. The essence of the software and hardware complex is to provide the user with such an interface that he was performing work while being partially remote from the workplace, or manipulating tools at a distance, that is, using gestures. The use of the proposed software-hardware complex will improve the sterility parameters in the operating system, increase the technical safety during the direct work of the user with the devices.

Keywords: artificial intelligence, controllers, modules, gestures, depth of the scene, point of interest, analysis of modifiers, gesture analysis, segmentation, skeletonization, observation.

Дані про авторів див. стор. 114

ДЛЯ НОТАТОК

Наукове видання



ЗБІРНИК НАУКОВИХ ПРАЦЬ

**Військового інституту
Київського національного університету імені Тараса Шевченка**

№ 90

Усі матеріали надруковані в авторській редакції

Підписано до друку 20.03.2026 р.

Авт. друк. арк. 8,00. Формат 60х90/8 Безкоштовно. Замовлення № 22-26.

Надруковано у навчальному тренувальному комплексі ВІКНУ
Київ, вул. Ю. Здановської, 81

тел. (044) 521-32-89

