ISSN 2519-2310 (Online)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені В.Н.КАРАЗІНА
V.N. KARAZIN KHARKIV NATIONAL UNIVERSITY

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА
COMPUTER SCIENCE AND CYBERSECURITY
(CS&CS)

№ 2(28) 2025
Issue 2(28) 2025

Заснований 2015 року

Міжнародний електронний науково-теоретичний журнал
International electronic scientific journal

УДК 004(051)

Засновник і видавець Харківський національний університет імені В.Н. Каразіна Міністерства освіти і науки України. Засновано у 2015 році. Періодичність виходу –2 рази на рік.

В журналі публікуються наукові статті з теоретичних і науково-технічних проблем, що пов'язані зі створенням ефективних засобів комп'ютерних інформаційно-комунікаційних систем та питань захисту інформації, на основі передових математичних методів, інформаційних технологій і технічних засобів.

Схвалено до розміщення в мережі Інтернет Вченою радою Харківського національного університету імені В.Н. Каразіна (22.12.2025 р., Протокол № 32).

DOI (Онлайн): **10.26565/2519-2310-2025-2**.

Редакція: Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 6, офіс 315а, Харків, 61022, Україна (*Північний корпус університету, 3 поверх*)
Електронна пошта: cscsjournal@karazin.ua
Веб-сторінка: http://periodicals.karazin.ua/cscs (Open Journal System)
Ідентифікатор медіа у Реєстрі суб'єктів у сфері медіа: R40-06757 (Рішення № 2804 від 18.12.2025 р Національної ради України з питань телебачення і радіомовлення. Протокол № 28)

UDC 004(051)

Founder and publisher V.N. Karazin Kharkiv National University of the Ministry of Education and Science of Ukraine. Established in 2015. Published 2 times a year.

The journal publishes research articles on theoretical, scientific and technical problems of effective facilities development for computer information-communication systems and information security questions based, on advanced mathematical methods, information technologies and technical means.

Approved for placement on the Internet by Academic Council of the Karazin Kharkiv National University (December 22, 2025, Protocol No.32).

The journal has Digital Object Identifier: **10.26565/2519-2310-2025-2** (Online).

Editorial office: V.N. Karazin Kharkiv National University, Svobody Sq., 6, office 315a, Kharkiv, 61022, Ukraine (*North building of University, 3th floor*)
E-mail: cscsjournal@karazin.ua
Web-page: http://periodicals.karazin.ua/cscs (Open Journal System)
Media identifier in the Register of the field of Media Entities: R40-06757 (Decision № 2804 dated December 18, 2025 of the National Council of Television and Radio Broadcasting of Ukraine, Protocol № 28)

The authors of the published materials are solely responsible for the selection, accuracy of the facts, proper names, etc. Published articles have been internally and externally peer reviewed.

ЗМІСТ

CONTENTS

ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 2 (28)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 2 (28)

https://doi.org/10.26565/2519-2310-2025-2-01
УДК 004.056.55:004.932

ОЦІНКА РЕЗУЛЬТАТІВ ПРОСТОРОВИХ ПЕРЕТВОРЕНЬ ОПОРНИХ БЛОКІВ КОНТЕНТУ ЯК ОКРЕМОГО ЕТАПУ ГІБРИДНОГО СТЕГАНОАЛГОРИТМУ

Микита Гончаров[1], аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій, e-mail: m.honcharov@student.karazin.ua, ORCID: https://orcid.org/0000-0002-9790-7260
Сергій Малахов[1], к.т.н., ст. науковий співробітник, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, e-mail: malakhov@karazin.ua, ORCID: https://orcid.org/0000-0001-8826-1616
[1]*Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна*

Рукопис надійшов 1 вересня 2025 р. Отримано після рецензування 1 жовтня 2025 р. Прийнято 2 листопада 2025 р. Опубліковано 30.12.2025 р.

Анотація: У роботі представлено результати моделювання та аналізу наслідків реалізації процедур зміни просторової орієнтації опорних блоків (ОБ) зображень, вилучених з масиву довжин серій ОБ контенту. Мета роботи полягає у визначенні характеру впливу і наслідків використання різних варіантів просторових перетворень ОБ зображення - контенту на його стійкість до атак та обчислювальну складність. Проведене моделювання продемонструвало, що просторові перетворення ОБ контенту, незважаючи на їх низьку обчислювальну складність та цілковиту оборотність, забезпечують ефективний й незалежний рівень захисту. Інтеграція відповідних процедур, сумісно з іншими рівнями (інструментами) захисту, суттєвим чином підсилює кінцевий ефект, покращуючи стійкість стеганографічного контенту до спроб його несанкціонованого вилучення. Оцінка обчислювальної складності просторових перетворень ОБ контенту, підтвердила можливість забезпечення ресурсного консенсусу при виконанні цих процедур, навіть в умовах дефіциту вільних ресурсів використовуваних апаратних платформ. Зроблено висновок, що широка комбінаторність можливих схем реалізації просторових перетворень ОБ, є ефективним і обчислювально «легким» інструментом з протидії спробам неавторизованого доступу до контенту. Отримані результати підтверджують перспективність застосування механізму змін просторової орієнтації опорних блоків контенту у малоресурсні алгоритми стеганографічного захисту інформації та/або відповідні мобільні додатки. Це відкриває широкі можливості для подальшого вдосконалення розглянутої концепції стегановставки зображень, шляхом розширення комбінаторики структури ключа екстрактора даних, адаптивного вибору параметрів обробки та комбінування варіантів просторових трансформацій опорних блоків зображень контенту.

Ключові слова: *інформаційна безпека, загрози, кібератака, обчислювальна складність, цифрові зображення, інкапсуляція даних, екстракція даних, просторова орієнтація, несанкціонований доступ, стеганографія, кодування довжин серій*

Як цитувати: Гончаров М., Малахов С., Оцінка результатів просторових перетворень опорних блоків контенту як окремого етапу гібридного стеганоалгоритму. *Комп'ютерні науки та кібербезпека.* 2025; № 2(28): С. 6–20. https://doi.org/10.26565/2519-2310- 2025-2-01

In cites: Honcharov M., Malakhov S., (2025). Evaluation of the results of spatial conversions of basic blocks of content as a separate stage of a hybrid steganographic algorithm. *Computer Science and Cybersecurity. 2*(28): 6–20. https://doi.org/10.26565/2519-2310- 2025-2-01 (in Ukrainian)

1. Вступ

Сталий розвиток сучасних інформаційно-комунікаційних систем (ІКС) зумовлює зростання обсягів циркулюючих цифрових даних та постійне розширення застосовуваної комунікаційної інфраструктури. У таких умовах забезпечення конфіденційності, цілісності та прихованості інформації, залишається одним із ключових завдань в галузі сучасної інформаційної безпеки [1-2]. Серед доступних механізмів захисту особливу увагу привертає цифрова стеганографія, оскільки вона дозволяє не лише надійно зберегти зміст повідомлення, а й повністю приховати сам факт передавання чи зберігання важливої інформації, роблячи стеганографічну систему принципово невизначуваною для стороннього спостерігача [3-6]. На відміну від криптографії, що виключає несанкціонований доступ до вмісту умовного повідомлення, але залишає очевидним сам факт захищеної передачі чи зберігання даних, стеганографічні методи використовують статистичні й структурні властивості цифрових контейнерів, забезпечуючи непомітну інтеграцію прихованих даних без порушення цифрового «вигляду» носія – переносника даних [1, 3, 4, 7].

Одним із центральних викликів сучасної стеганографії є поєднання високої надійності приховування з низькою ресурсомісткістю обробки. Це особливо актуально в умовах обмежених обчислювальних можливостей мобільних пристроїв та/чи вбудованих апаратних систем, де продуктивність, енергоефективність і швидкодія алгоритмів є визначними характеристиками, що безпосередньо впливають на реальну застосовність методу [8-9]. У зв’язку з цим зростає потреба у створенні малоресурсних стеганографічних методів, які раціонально використовують статистичні властивості оброблюваних цифрових даних (в контексті даної роботи – зображень), забезпечуючи високу якість приховування при збереженні мінімальних вимог до апаратних ресурсів і часу виконання. Важливою складовою таких досліджень є детальний аналіз обчислювальної складності базових процедур, що визначають структуру та продуктивність розроблюваних гібридних стеганографічних алгоритмів. Саме на цьому етапі формується умовна ресурсна модель системи, яка впливає на умови реалізації стеганографічної вставки даних, загальну швидкодію, енергоспоживання та, в кінцевому підсумку, практичну придатність розроблених методів у реальних умовах експлуатації відповідних систем й алгоритмів. У цьому контексті особливого значення набуває розроблення методів, здатних ефективно поєднувати властивості використовуваних цифрових контейнерів і вбудованого контенту, оскільки від узгодженості їх структурних та статистичних характеристик залежить як якість приховування [1, 3-4], так і стійкість стеганографічної системи до сучасних методів аналізу з боку стеганоаналітика. У межах реалізації таких методів окрему роль відіграють процедури, які впливають на просторову організацію (орієнтацію) блоків вихідних даних перед їх інкапсуляцією до структури контейнера - переносника інформації, створюючи тим самим додатковий рівень захисту контенту на основі геометричних перетворень блоків зображень [10-11]. Так наприклад, в умовах досліджуваної версії тестового гібридного стеганоалгоритму [9] в якості маніпуляцій із просторовою орієнтацією вихідних опорних блоків (ОБ) контенту виступають: - обертання та/чи віддзеркалення окремих ОБ зображення, яке використовується як додатковий механізм посилення стійкості стеганографічної системи [11].

Попри те, що такі геометричні перетворення не змінюють значення пікселів і не впливають на візуальну якість зображення, вони суттєво ускладнюють задачу неавторизованої екстракції контенту, призводячи до повної фрагментації або незворотного спотворення відновленого контенту [10-14], навіть за умови мінімальної помилки у підборі діючих параметрів складеного ключа екстрактора даних [15]. Вочевидь, що детальне оцінювання обчислювальних властивостей цих операцій є необхідним для формування об'єктивного ресурсоорієнтованого профілю відповідного алгоритму і обґрунтування можливостей, щодо його подальшого використання на пристроях з обмеженими ресурсами.

2. Спрощена схема тестового алгоритму та призначення функціональних модулів

В ході циклу досліджень було проведено імітаційне моделювання роботи перших двох етапів дослідного алгоритму [9]. Моделювання включало: - різні варіанти передобробки (або згладжування) вихідних зображень [16–18]; - формування серій ОБ з додатковим критерієм [19], який враховує всі умови перевірки подібності (структурної автентичності); - використання різних схем розгортки ОБ зображень [20]; - а також застосування просторових геометричних перетворень ОБ контенту. Така послідовність моделювання створює потрібні умови для оцінки впливу блоку процедур просторових маніпуляцій, на стійкість стеганографічної системи та обчислювальну складність алгоритму [10-14]. У процесі моделювання варіювалися ключові параметри: - порогові значення різниці яскравості елементів зображень Pz1 та Pz2 (*що відповідають різним етапам алгоритму обробки*); - розмірності ОБ «N»; - різні схеми розгортки ОБ зображення [20]. Такий підхід дозволив комплексно оцінити поведінку алгоритму на різних етапах обробки та визначити ступінь впливу кожного з параметрів на структуру сформованого масиву серій ОБ та характер артефактів (викривлень) у випадку хибного відновлення контенту у разі спроби його неавторизованого вилучення. Статистичний аналіз результатів включав оцінку кількості базових операцій (*арифметичних, логічних та операцій порівняння*), які виконувалися на кожному етапі дослідного алгоритму. Кількісне оцінювання проводилося за кількома критеріями: - час виконання окремих процедур, значення метрики PSNR [3-4] після застосування передобробки, а також різних схем розгортки ОБ [20].

Усі результати, які розглядаються в межах цієї роботи, отримані для тестової групи комп'ютерно-синтезованих (CG) зображень типу «*Портрет* CG» та «*Пейзаж* CG», що характеризуються високою текстурною варіативністю й великими значеннями локальних перепадів яскравості, що дозволило достатньо всебічно оцінити ефективність розглянутих процедур у складних умовах обробки (випадковість і спорадичність вільних ресурсів).

Наступний кроком дослідження стало детальне вивчення процедур просторової орієнтації ОБ, які виступають одним із додаткових параметрів обробки стеганографічного контенту. Впровадження цих процедур дозволяє суттєво ускладнити задачу неавторизованої екстракції даних навіть у разі компрометації основних механізмів мультиплексування [9, 11].

Під просторовою орієнтацією розуміється застосування до вихідного масиву ОБ зображення контенту, процедур геометричних перетворень (*обертання, горизонтальне або вертикальне віддзеркалення, інверсія, зсув ділянок тощо*), вибір та сутність яких декларується відповідним елементом в структурі ключа екстрактора даних [9, 15]. Такі маніпуляції є обчислювально простими, повністю оборотними (при наявності правильного ключа), але призводять до кардинальної зміни порядку зчитування пікселів при помилковому відновленні блоків атакуючою стороною. Внаслідок цього, навіть при правильному визначенні схеми розгортки блоків і розмірності блоків, відновлене зображення-контент зазнає значної фрагментації та втрачає цілісність загальної сцени, яка відображається, що робить неможливим візуальну чи автоматичну ідентифікацію об'єктів спостереження [10-14].

Варто зазначити, що подібні просторові перетворення виконують роль додаткового стеганографічного шару, який ускладнює аналіз структури даних заповненого контейнера-переносника для стороннього спостерігача. Оскільки обертання чи віддзеркалення не змінюють вихідних статистичних властивостей зображення ОБ, вони не погіршують якість даних для легітимного користувача, однак створюють серйозні перешкоди для несанкціонованого вилучення контенту. Будь-яка спроба відновити ОБ без знання їх орієнтації призводить до того, що пікселі опиняються в нетипових позиціях, руйнуючи відхідну структуру зображення. Таким чином, механізм просторової орієнтації забезпечує ефективний захист даних не за рахунок складних обчислень, а завдяки можливості комбінування простих й повністю оборотних трансформацій, критичних до точності інтерпретації відомостей ключа екстрактора даних [9]. На рис. 1 наведено спрощену схему, яка наочно ілюструє основну суть процедур, що виконуються в межах реалізованої концепції комп'ютерного моделювання. Ця схема дозволяє отримати загальне уявлення про структуру й послідовність дій, підкреслюючи ключові особливості підходу без надмірного заглиблення у технічні деталі. Такий спрощений формат сприяє швидкому розумінню логіки роботи системи і взаємозв'язків між окремими етапами процесу. Нижче надано стислий огляд кожного з етапів і його роль у загальному процесі.

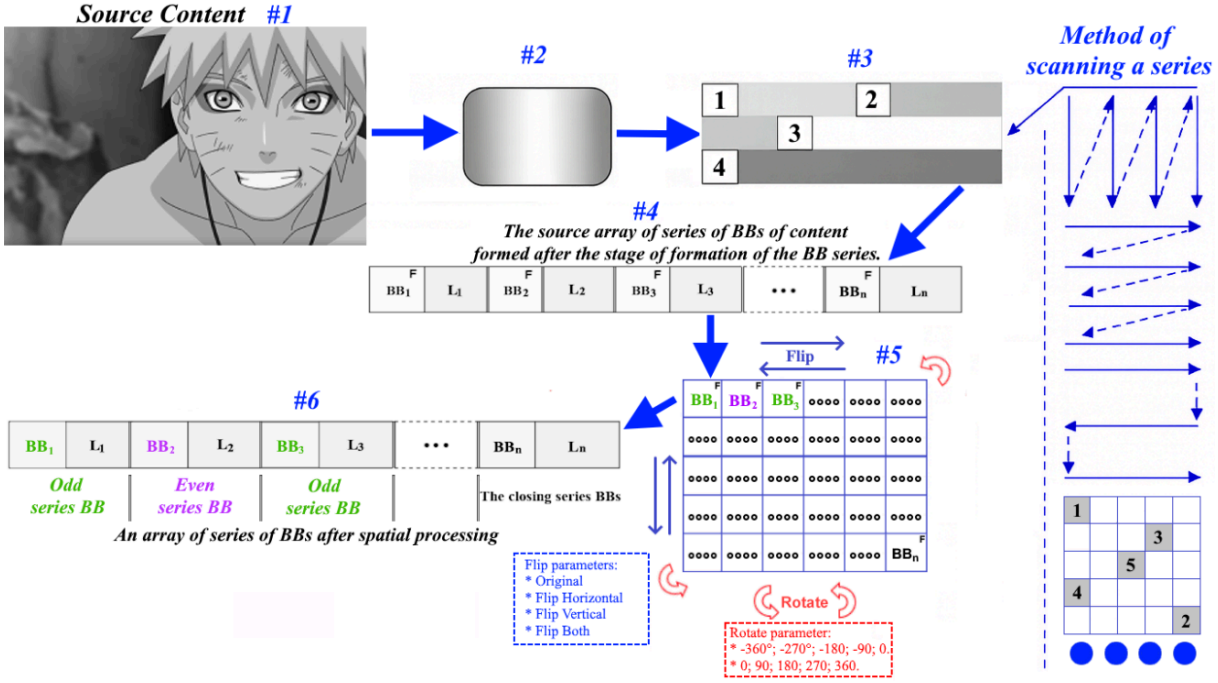

Рис. 1 – Спрощена схема перетворень поточного масиву серій ОБ

Fig. 1 – Simplified scheme of conversion of the current array of BBs series

На першому кроці дослідного алгоритму здійснюється зчитування вихідного тестового зображення (крок 1, на рис. 1). Отримане зображення передається на подальші етапи обробки.

На другому кроці (крок №2, на рис. 1) виконується процедура «згладжування» вихідних даних. З цією метою застосовуються: - один із варіантів [16-18] згладжування; - потрібне значення порога загрублення (P_{Z1}) та розмірність блоків N. Поріг загрублення (P_{Z1}) визначає максимальну допустиму різницю значень яскравості між сусідніми пікселями в межах оброблюваних блоків зображення [19]. Відповідно до обраного варіанту згладжування, алгоритм формує однорідні області на зображенні, що дає змогу суттєво зменшити помітність спотворень та локальних перепадів яскравості [7]. Така обробка сприяє вирівнюванню

розподілу яскравості всередині збережених блоків, зменшує обсяг необхідних обчислень на етапах проведення кодування з перетворенням [7, 9] та знижує ймовірність її (заміни елементів) виявлення статистичними методами.

На 3-му кроці відповідно до обраної користувачем схеми розгортки [20] виконується послідовний обхід елементів зображення (в даному випадку ОБ) за певною схемою розгортки з метою їх подальшого групування у відповідні масиви серій ОБ (з заданою розмірністю ОБ).

На 4-му кроці формується масив серій ОБ (сукупність ОБ й параметрів їх довжини). Отриманий масив можна обробляти повністю або попередньо розділити масив на парні й непарні елементи. Ці дані зберігаються у вигляді лінійного масиву розмірності 1×X (залежно від того, використовується повний масив чи двопрохідна обробка (парний + непарний ОБ)), де X - загальна кількість ОБ та їхніх довжин, задіяних у зображенні. Така структура (ОБ + *довжина*) використовується на наступних етапах дослідного гібридного алгоритму та формується за допомогою методу кодування довжин серій [7], що враховує всі необхідні умови перевірки подібності. Аналіз масиву проводиться за наступним критерієм: - якщо різниця між максимальним і мінімальним значенням яскравості елементів ОБ перевищувала встановлений поріг загрублення (P_{Z2}), це свідчило про наявність важливої інформативної складової в блоці. У випадку, коли зазначена різниця була незначною, блок вважався менш інформативним, характеризувався низькою варіативністю пікселів та малою різницею між максимальним і мінімальним значеннями [19]. Згідно з цим підходом, у першому випадку блок формує окрему (одиничну) серію, а в іншому - масив серій, що дозволяє ефективно групувати схожі між собою блоки. На 4-му кроці більш детально демонструється структура масиву серій. Отриманий масив серій ОБ, використовується для їх подальшої обробки, дозволяючи на наступних етапах дослідного алгоритму реалізувати процедури багаторівневого мультиплексу цих даних.

На 5-му кроці для кожного ОБ, представленого у вигляді лінійного масиву розмірності 1×X, формується новий двовимірний масив оптимальної розмірності A×B = X (A – висота масиву, B – ширина масиву), такий котра відповідає вихідному значенню X [12]. Параметри «A» та «B» обираються відповідно до заданої користувачем стратегії обробки (*зокрема, для повного масиву або для розділених, парного та непарного проходів*). Таке повернення до двовимірної структури значно посилює руйнівні наслідки хибного відновлення взаємного розташування блоків при можливій атаці, а також суттєво ускладнює зловмиснику підбір правильних параметрів кодування (стегановставки).

Слід зазначити, що якщо загальна кількість елементів X, є простим числом, то до масиву додається додатковий нульовий елемент, щоб уникнути утворення масиву розмірності 1xX, оскільки з такою розмірністю геометрична обробка не змінює його вигляду та взаємного розташування ОБ. Унаслідок цього зловмисник не отримує жодних візуальних чи статистичних відмінностей між правильною та хибними орієнтаціями, що повністю нівелює захисний ефект від впровадження механізму перестановки та зміни орієнтації ОБ. Запропоноване рішення цієї проблеми з додаванням нуля, дозволяє сформувати масив оптимального розміру для масиву, необхідного для виконання подальших геометричних перетворень.

Після завершення обробки цей нульовий елемент вилучається, а його позиція (біт) фіксується у відповідному елементі ключа екстрактора даних, що забезпечує коректне зворотне відновлення. На наступному етапі (крок № 5.1) до сформованого масиву серій застосовуються просторові геометричні перетворення: обертання на -360°/0°/360° (*тобто без змін*), 90°, 180° або 270° (за чи проти ходу годинникової стрілки); горизонтальне віддзеркалення, вертикальне віддзеркалення, будь-які їх комбінації (наприклад, обертання на 180° + горизонтальне віддзеркалення) (крок № 5.2), а також селективне застосування серії (наприклад, двопрохідна схема, обертання лише непарних ОБ на 90°, парних на 270°, чергування обертання та віддзеркалення за використаною схемою тощо), включно з варіантом відсутності будь-якого

перетворення (ідентичність). Вибір конкретного перетворення для кожного ОБ визначається поточним станом відповідного елемента ключової послідовності [9, 15], що забезпечує 13–26 варіантів (включно з відсутністю трансформації) на блок і стеганографічну стійкість. Навіть при компрометації основних параметрів мультиплексування, хибно збережена орієнтація ОБ призводить до сильної просторової фрагментації й повної втрати цілісності відновлюваного контенту (рис. 3 в [10]). На 6-му етапі за результатами виконання всіх передбачених процедур обробки та просторових перетворень, формується підсумковий масив серій ОБ. Отриманий масив слугує основою для подальших етапів дослідного алгоритму. У межах цієї роботи здійснюється відновлення результуючого зображення, що відображає сукупний ефект від застосованих методів просторової орієнтації ОБ. На рис. 2- наведено результати виконання всіх вказаних вище етапів обробки, які характеризують формування підсумкового масиву серій ОБ, та відновлення результуючого зображення (в даному разі за схемою «*Змійка-2*» [20]).

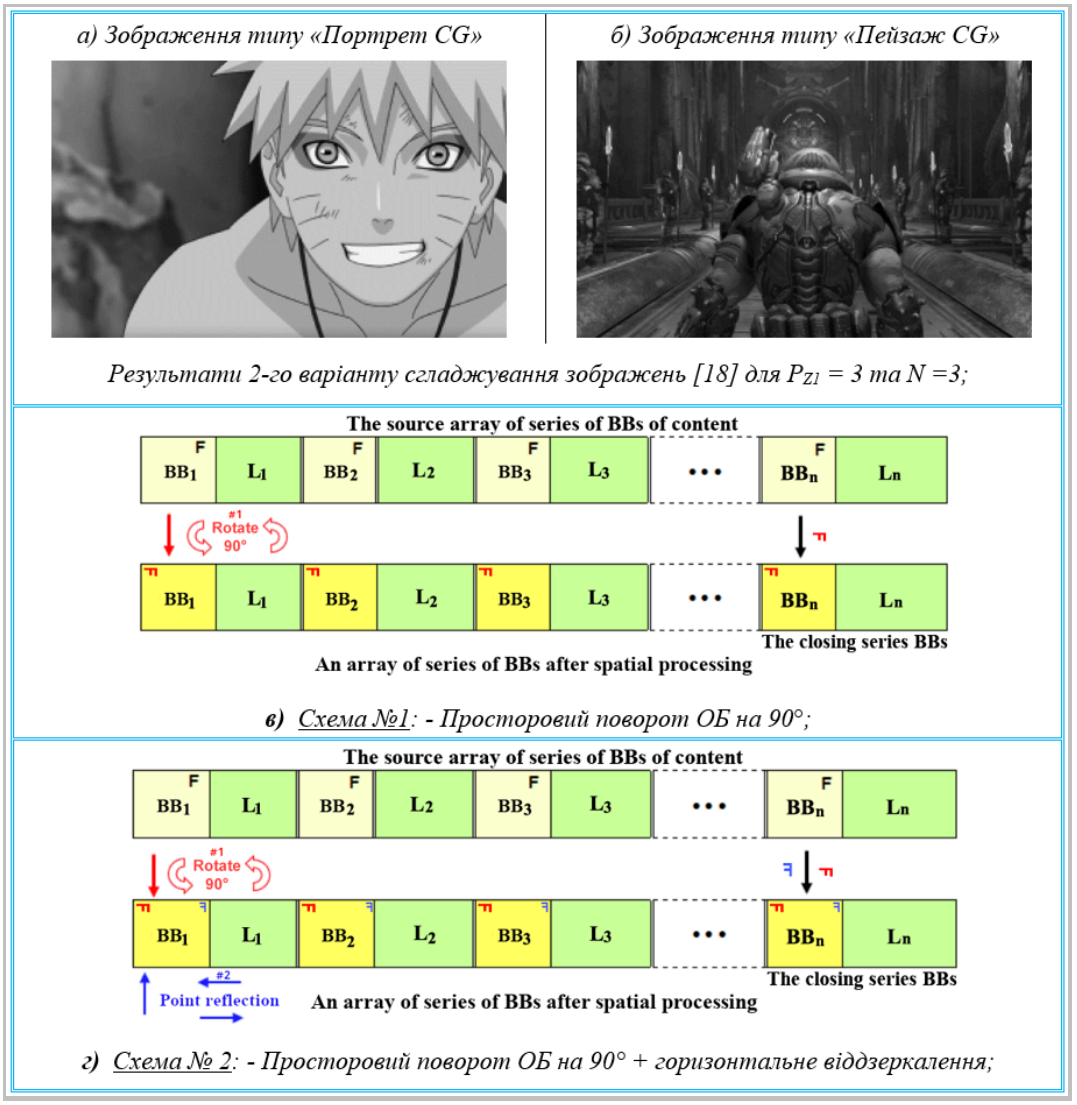

Рис. 2 – Зразки тестових зображень та схеми просторової орієнтації ОБ (а-б)
Fig. 2 – Samples of test images and spatial orientation schemes of BBs (a-b)

3. Обчислювальна складність процедур просторової орієнтації вихідних даних

Обчислювальна складність процедур зміни просторової орієнтації сформованих ОБ, визначається характером застосовуваних перетворень, де кожна така операція обмежується перестановкою координат блоків розмірності N×M та не потребує виконання арифметичних дій над значеннями яскравості складових елементів. Перетворення обертання, що включають варіанти 0°/360°/-360°; 90°/-270°, 180°/-180° та 270°/-90°, реалізуються через просту зміну індексної структури новоствореного масиву ОБ, у відповідності до матричних перестановок (рис. 1 крок 5). Для кожного ОБ такі операції мають лінійну складність O(N×M), оскільки кожен елемент переставляється одноразово (де O - це асимптотична оцінка складності алгоритму, що описує верхню межу кількості операцій). Аналогічно, операції віддзеркалення у межах ОБ горизонтальне, вертикальне, обидва одночасно й варіант відсутності перетворення, виконуються через інверсію відповідних осей та мають порядок складності O(N×M).

Оскільки обидва вказані різновиду перетворень не потребують додаткових перевірок їх меж та/чи умовних переходів, то їх обчислювальна складність визначається лише кількістю елементів в серії ОБ та параметром довжини (тобто повтором). Комбіновані схеми, у межах яких до окремих ОБ застосовуються різні просторові орієнтації, залежно від їхньої парності або позиції у масиві серій ОБ *(див. рис. 2(в-г)),* не змінюють асимптотичного порядку алгоритму, оскільки збільшення кількості варіантів трансформацій впливає лише на логічну вибірку операції для конкретного блока, що є сталою дією O(1). У випадках зміни операцій (*наприклад, обертання непарних блоків на 90° та парних на 270°, або комбінації обертання з віддзеркаленням*), кожен наступний ОБ, як і раніше, проходить рівно одну просторову трансформацію, не змінюючи при цьому, загального порядку обчислень.

Загальна складність просторової орієнтації для масиву розмірністю «X» блоків залишається лінійною і визначається лише загальною кількістю елементів (ОБ), що підлягають перестановці. Хоча подвійні чи комбіновані схеми технічно збільшують час виконання майже вдвічі через обробку двох масивів (масив парних і непарних ОБ), ці додаткові витрати залишаються сталими чи близькими до них. Т.ч. асимптотичний порядок обробки не змінюється та не залежить від кількості доступних варіантів чи ступеня їх комбінування. Попри лінійний характер потрібних обчислювальних витрат, розглянуті процедури помітно посилюють стійкість контенту до спроб його неавторизованого вилучення [10-11, 14].

Поєднання низької складності та широкої варіативності перетворень визначає практичну цінність процедур зміни просторової орієнтації ОБ. У цьому контексті важливо підкреслити, що такі трансформації не лише не обтяжують систему додатковими обчисленнями, але й органічно інтегруються у загальний процес вбудовування. Оскільки вони впливають виключно на просторове впорядкування елементів ОБ та не змінюють значення яскравості пікселів ОБ або інші параметри, що можуть бути модифіковані в процесі вбудовування інформації, ці перетворення фактично не створюють додаткового обчислювального навантаження. Їх внесок у загальну безпеку системи, а також широка різноманітність доступних просторових трансформацій і можливість їх комбінування, дозволяють гнучко налаштувати механізм до різних моделей загроз, широкого спектра застосувань, а також вимог щодо рівня захищеності. Механізм просторової орієнтації ОБ контенту, може бути використаний, як незалежний (окремий) рівень захисту, без впливу на якість стегановставки (це різні етапи) чи пропускну здатність системи. Впровадження такого рівню захисту, посилює загальну комбінаторику елементів ключа екстрактора даних [15], забезпечуючи надійний захист навіть за умови компрометації інших складових [9-10].

Результати експериментальної оцінки обчислювальної складності реалізованих процедур зміни просторового позиціонування ОБ, наведено на прикладі тестових зразків

зображень типу «Портрет» і «Пейзаж» (*обидва зразки є синтетичними зображеннями, які є результатом комп'ютерної графіки, тобто «CG»*). Для обраних зразків використовувався 2-й варіант передобробки [16-18], визначений як оптимальний з урахуванням забезпечуваного співвідношення між одержуваним рівнем згладжування й якістю отриманого зображення. У процесі моделювання досліджувалися часові характеристики виконання просторових операцій і якість відновлення контенту, оцінювана за PSNR (*піковим значенням сигнал/шум*).

Рисунок 3 характеризує вплив різних схем просторової орієнтації ОБ на якість відновленого тестового зображення (рис. 2 (а-б)) та час виконання етапу просторової обробки ОБ. Верхня частина рис.3 відповідає результатам обробки зображення типу «*Портрет CG*», а нижня – «*Пейзаж CG*». Кожна частина містить дві гістограми: - значення PSNR після застосування процедур зміни просторової орієнтації ОБ для одно/двохпрохідної схем; - тривалість часу виконання цих процедур. Червоні діаграми демонструють результати, отримані під час обробки цільного (тобто нерозривного) масиву серій ОБ, тоді як сині елементи характеризують двопрохідну схему (наприклад, поворот парних ОБ на 90° та віддзеркалення непарних). Т.ч., у роботі наведено результати виконання однопрохідних і двопрохідних схем, що відображено у підписах до наданих діаграм.

Аналіз результатів моделювання показує, що всі розглянуті варіанти просторових перетворень ОБ (рис. 2), забезпечують майже однакове значення PSNR: - близько 29 дБ для «*Портрет CG*» та 32 дБ «*Пейзаж CG*». Двопрохідні схеми розгортки [14] демонструють лише незначне зниження PSNR, порівняно з однопрохідними (*див. рис. 1 (а-в,д,і) в роботі* [20]). Збільшення часу виконання у разі застосування просторових перетворень для повного масиву серій ОБ, є мінімальним. Подібне невелике збільшення часу обробки (в середньому на 0.020 секунди, що становить близько 18.4%), можна спостерігати і при переході до двопрохідних схем. При цьому комбінаторна складність ключа екстрактора [9] зростає кратно, що суттєво посилює захищеність стеганоконтенту. Аналіз результатів обробки (див. рис. 2) зображень типу «*Пейзаж CG*», які характеризуються складною структурою (насичені текстури, велика кількість дрібних деталей, висока локальна варіативність), підтверджує тенденцію, до незначного збільшення часу виконання процедур зміни просторової орієнтації ОБ (в середньому на 0.016 секунди, що становить близько 11.3%), що свідчить про стабільність цього показника, навіть за складніших умов. Значення PSNR, також зберігаються на рівні, близькому до базових тестових сцен (тобто у випадку без виконання процедур просторової обробки). Візуальний вигляд відновлених зображень може суттєво відрізнятися. Це пов’язано з тим, що глобальна метрика PSNR має низьку чутливість до локальних неоднорідностей (артефактів), оскільки у складних сценах (насичених дрібними деталями), навіть мінімальні зміни можуть візуально сприйматися як суттєві, хоча їх внесок у середньоквадратичну похибку залишається незначним [3-4].

В цілому, додавання до структури складеного ключа екстрактора даних [9, 15] елементу, який визначає варіант просторової орієнтації ОБ в отриманому масиві серій [14], майже не впливає на обчислювальні витрати, але істотно підвищує стійкість системи, до спроб неавторизованого вилучення контенту (*див. рис. 3 в роботі* [10]). Навіть одноразова помилка в параметрі орієнтації ОБ під час спроби нелегітимної екстракції контенту, призводить до появи виражених артефактів, що унеможливлюють розпізнавання контенту навіть на рівні класифікації типу вихідних зображень (*див. рис. 4 (в-е)*). Це підтверджує початкове припущення про впровадження у структуру гібридного алгоритму етапу просторових маніпуляцій із ОБ зображення-контенту, як в однопрохідної, так й двохпрохідної схемах їх реалізації, що узгоджується з концепцією малоресурсної стеганографії. Використання різних схем просторової обробки ОБ масиву серій контенту, зумовлює ***min*** збільшення обчислювальної складності всього алгоритму при суттєвому посиленні стійкості контенту до спроб його неавторизованого вилучення (Рис. 3 в [10]).

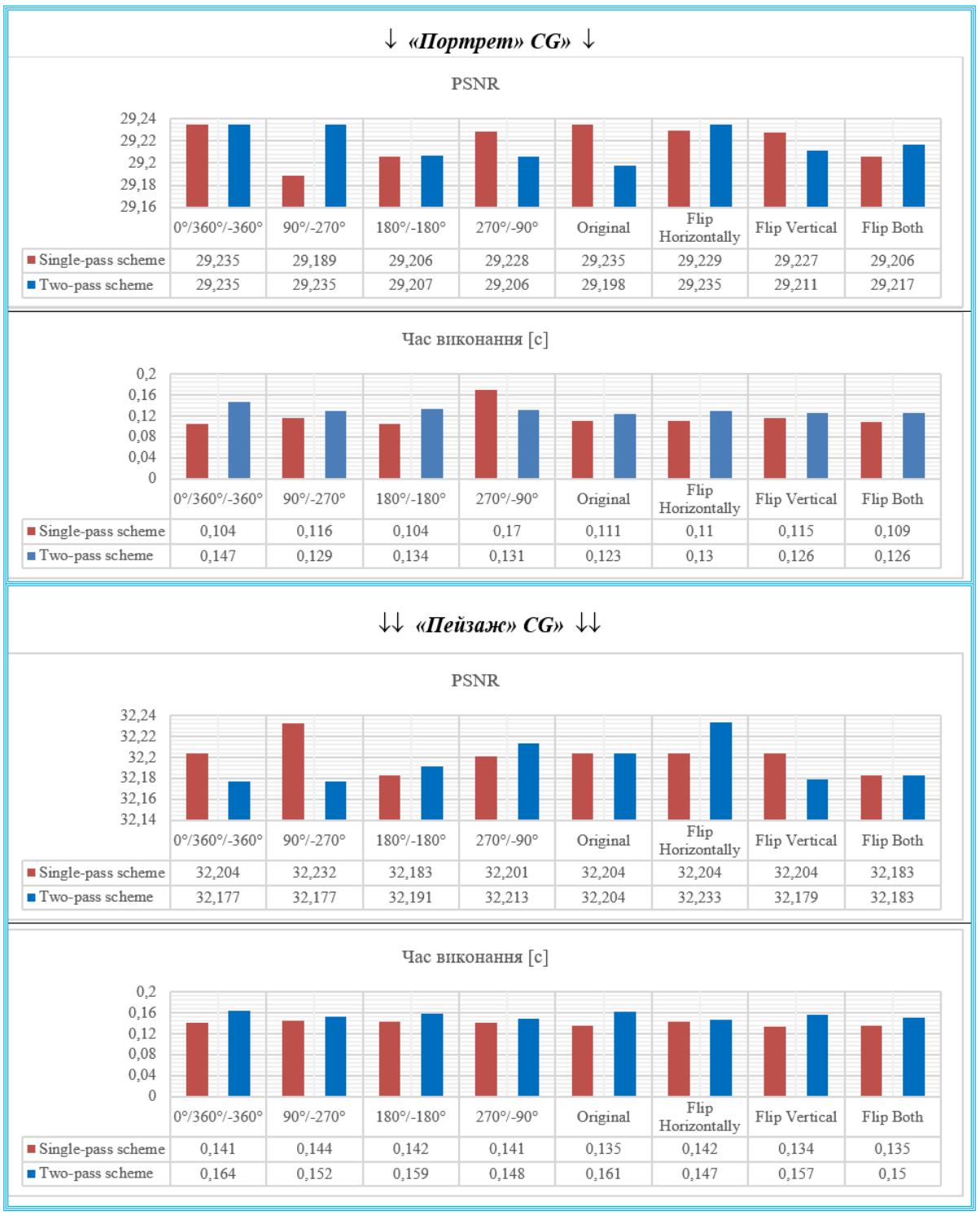

Рис. 3 – Значення PSNR та обчислювальна складність процедур зміни просторової орієнтації ОБ (8×8 ел) без урахування складності інших етапівї

Fig. 3 – PSNR values and computational complexity of procedures for changing the spatial orientation of BBs (8×8 el.) without taking into consideration the complexity of other stages

4. Результати моделювання спроб несанкціонованого вилучення контенту для різних схем просторової обробки ОБ та сценаріїв атак

Нижче, на рис.4 представлені результати спроб несанкціонованого вилучення тестових зображень (рис. 2 (а-б)), за умови їх обробки з використанням розгортки типу «*Подвійна Змійка-2*» (*Рис. 1(е) в роботі* [20]). В ході проведеного моделювання використані схеми просторової обробки ОБ (рис. 2(в-г)), які відповідають наступним параметрам передобробки вихідного контенту [16-18]: − маска згладжування *3×3* ел.; − 2-й варіант передобробки/згладжування; − порогове значення відмінності рівнів яскравості елементів сусідніх блоків вихідного зображення, P_{Z1}=7. Наведені результати відповідають ситуаціям, коли зловмисник: − правильно визначив розмірність блоків ОБ, проте припустився помилки з чинною схемою розгортки ОБ контенту (використавши розгортку типу «Змійка-2»); − вірно визначив тип розгортки, але використав хибну просторову схему формування ОБ. Як слід із рис.4, таки спроби призводять до формування характерних артефактів, що роблять неможливим відновлення початкової структури зображення (рис. 4 (в-е), помилка із просторовою обробкою), навіть за умови правильного підбору частини діючих елементів ключа екстрактору даних (Fig.1, [15]).

За умови помилки параметра просторової обробки ОБ, у всіх розглянутих сценаріях атак, отримані результати демонструють повну втрату пізнаваності (тобто, характерних рис чи ознак) вихідного контенту. Артефакти, що виникають унаслідок помилок у просторовій схемі або розгортці, суб'єктивно мають хаотичний характер і не формують жодних впізнаваних структур. Це підтверджує ефективність застосованих заходів для цілей протидії спробам несанкціонованого відновлення контенту, оскільки часткове порушення параметрів його обробки на будь-якому рівні захисту [9] призводить до суттєвої руйнації структури масиву серій ОБ, і таким чином унеможливлює коректне відновлення вихідного зображення [10, 15].

Аналіз результатів моделювання різних комбінацій атак показав, що структура спотворень «атакованих» зображень не дає змоги ідентифікувати вихідний контент, навіть на рівні класифікації типу вихідних зображень. Це залишається практично неможливим за будь-яких варіантів просторової орієнтації ОБ і тільки посилюється в разі хибної реалізації діючої схеми розгортки (тобто, формування масиву серій ОБ). Крім того, значний діапазон використаних в ході моделювання розмірностей ОБ, дозволив простежити загальні тенденції у зміні інтенсивності викривлень та визначити характерні особливості в структурі артефактів атакованого контенту. Незважаючи на наявність артефактів, що притаманні для деяких комбінацій атак (рис.4(а–б)), котрі дають змогу частково відтворити загальні риси вихідного кадру (контури обличчя, основне розташування об’єктів сцени тощо), ступінь спотворень все одно залишається достатньо високою, щоб ускладнити точну візуальну ідентифікацію об'єктів.

Іншими словами, хоча певна видимість оригіналу й простежується, вона не забезпечує зловмиснику простого і надійного способу визначити зміст прихованого контенту або однозначно відновити вбудовані дані. Як слід із представлених на рис.4 зразків, використання процедур просторової орієнтації усуває зазначені «недоліки» та створює додаткові бар’єри для виключення простих рішень щодо ідентифікації прихованої інформації [10-14, 20]. В цілому, можна стверджувати, що поєднання різних схем розгортки і варіантів просторової орієнтації ОБ, формує найбільш сприятливі умови для max ускладнення процедур неавторизованої зворотної реконструкції вихідного контенту з боку атакуючої сторони. Можливість використання різноманітних комбінацій таких схем (рис. 2), істотно збільшує комбінаторний простір структури ключа екстрактора даних (рис. 1, [15]) та підвищує загальну стійкість контейнера-переносника даних проти спроб його аналізу з боку стеганоаналітика.

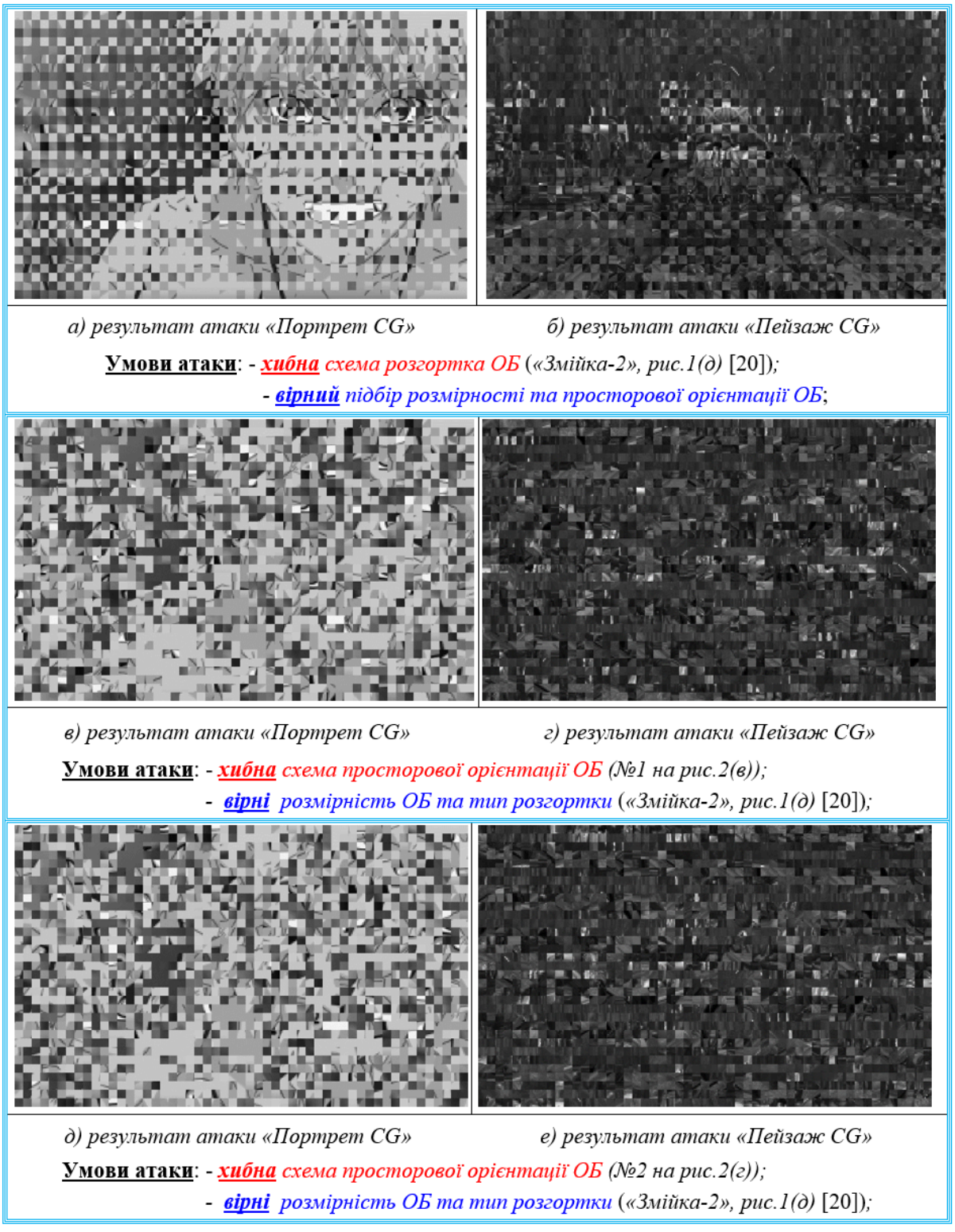

Рис. 4 – Результати атаки контенту для різних комбінацій підбору діючих параметрів обробки (*розгортка «Подвійна Змійка», рис.1(е) [20]; ОБ 16×16 ел.*);

Fig. 4 – Results of content attack for various combinations of selection of current processing parameters (scan «Double Snake», Fig. 1(e) [20]; BBs 16×16 el.)

Узагальнюючи результати, можна стверджувати, що механізм зміни просторової орієнтації ОБ масиву серій, є ефективним інструментом посилення стійкості стеганографічної системи без втрати її продуктивності (у сенсі можливостей підтримки реального масштабу часу обробки), зберігаючи потрібний ресурсний консенсус в межах використовуваної програмно-апаратної платформи. Розглянутий підхід забезпечує можливості для подальшого вдосконалення методів малоресурсної стеганографії та синтезу багатошарових механізмів протидії спробам неавторизованого вилучення стеганографічного контенту, що робить його перспективним рішенням для систем інформаційної безпеки, які функціонують в умовах дефіциту вільних ресурсів ІКС та/чи спорадичного характеру обчислювальних навантажень. В якості прикладу таких випадків можна розглядати апаратуру мобільних мереж стільникового зв'язку в часи їх пікових навантажень (свята, надзвичайні ситуації, масштабні онлайн заходи тощо) або корпоративні обчислювальні мережі в моменти відбиття інтегрованих атак (наприклад, *«Amplification Attacks»*) на їх інформаційну інфраструктуру, що мають на меті комплексне переповнення каналів зв'язку (*Bandwidth*) в ІКС жертви з метою навмисного створення «жорсткого» дефіциту на вільні ресурси в цих системах.

5. Висновки

1. Проведене моделювання процедур зміни просторової орієнтації ОБ зображення-контенту (обертання, горизонтальне/вертикальне віддзеркалення та їх комбінації), наочно підтвердило очікуваний ефект від впровадження відповідного механізму протидії спробам несанкціонованого вилучення даних в умовах компрометації інших рівнів захисту [9, 15] дослідного алгоритму. Оцінка обчислювальної складності етапу просторових перетворень ОБ, продемонструвала їх низьку складність та підтвердила можливість забезпечення ресурсного консенсусу при виконанні цих процедур, навіть в умовах спорадичного дефіциту вільних ресурсів використовуваних програмно-апаратних платформ [8].

2. Дослідження однопрохідних та двопрохідних схем просторової орієнтації ОБ (рис. 2) підтвердило, що широка комбінаторність використовуваних схем просторових перетворень ОБ, є ефективним й обчислювально «легким» інструментом протидії спробам неавторизованого доступу до контенту. В окремих випадках, особливо за умови різкого обмеження вільних обчислювальних ресурсів базової платформи, механізм просторових перетворень ОБ, може використовуватися як автономний (окремий) захисний інструмент. Інтеграція відповідних процедур сумісно з іншими рівнями захисту даних, суттєвим чином підсилює одержуваний ефект (рис.4), покращуючи стійкість контенту до спроб його несанкціонованого вилучення.

3. Однопрохідні схеми просторової орієнтації ОБ є найпростішими в реалізації та мають min обчислювальні витрати. Кратні схеми (наприклад, окрема обробка парних і непарних ОБ) демонструють лише незначне зростання часу виконання та практично не впливають на значення метрики PSNR порівняно з однопрохідними схемами. Водночас застосування двопрохідних схем суттєвим чином підвищує комбінаторність станів відповідного елементу в структурі ключа екстрактора даних [9], що кратне ускладнює задачу неавторизованої екстракції контенту, навіть у разі компрометації (підборі діючих параметрів) інших рівнів захисту. Отримуваний ефект значно перевищує наслідки незначного збільшення обчислювальних витрат, роблячи багатопрохідні схеми просторового перетворення ОБ, особливо ефективними в умовах обмеження ресурсів використовуваних апаратних платформ.

4. Результати тестування механізму просторових перетворень ОБ контенту, свідчать про те що «вдалий» підбір діючих параметрів обробки даних на двох інших рівнях захисту [17-20], не гарантує «успішної» зворотної компіляції вихідного контенту. Це добре підтверджується високим ступенем руйнувань зразків «атакованих» тестових зображень (рис. 4(в-е)).

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

References

1. Fridrich, J. (2010). *Steganography in digital media.* Cambridge University Press
2. Hassaballah, M. (Ed.). (2020). *Digital media steganography: Principles, algorithms, and advances*. Academic Press.
3. Конахович, Г., Прогонов, Д., & Пузиренко, О. (2018). *Комп’ютерна стеганографічна обробка й аналіз мультимедійних даних:* Підручник. Центр навчальної літератури.
4. Кузнецов, О. О., Євсеєв, С. П., & Король, О. Г. (2011). *Стеганографія*: навч. посіб. Харків: Видавництво ХНЕУ.
5. Yahya, A. (2019). *Steganography techniques for digital images*. Springer International Publishing.
6. Shih, F. Y. (2020). *Digital watermarking and steganography*. CRC Press.
7. Pratt, W. K. (1978). *Digital image processing.* New York: John Wiley & Sons.
8. Гончаров, М., & Малахов, С. (2024). Аналіз сучасних мобільних платформ для забезпечення процедур стеганографічної вставки. *Grail of Science,* (52), с. 705–707. URL: https://archive.journal-grail.science/index.php/2710-3056/issue/view/23.05.2025/40
9. Лєсная, Ю., Гончаров, М., & Малахов, С. (2021). Відпрацювання концепту багаторівневого мультиплексу даних гібридного стеганоалгоритму. *Збірник наукових праць SCIENTIA*. URL: https://ojs.ukrlogos.in.ua/index.php/scientia/article/view/17666
10. Гончаров, М., & Малахов, С. (2023). Моделювання спроб несанкціонованого вилучення стеганоконтенту при зміні параметрів просторової орієнтації опорних блоків контенту. *Наука і техніка сьогодні,* 6(20), с. 114-129, URL: DOI: https://doi.org/10.52058/2786-6025-2023-6(20)-114-129
11. Малахов, С., Колованова, Є., & Гончаров, М. (2023). Особливості несанкціонованої екстракції стеганоконтенту при змінах просторового позиціювання опорних блоків контенту. *Збірник наукових праць ЛОГОΣ*, с. 152-157. DOI: https://doi.org/10.36074/logos-26.05.2023.041
12. Гончаров, М., & Малахов, С. (2023). Адаптивна модифікація вихідного масиву серій опорних блоків як механізм протидії неавторизованої екстракції стеганоконтенту. *Наука і техніка сьогодні*, 8(22), с. 336-352. DOI: https://doi.org/10.52058/2786-6025-2023-8(22)-336-352
13. Гончаров, М., & Малахов, С. (2023). Research of procedures for disintegration of the series length array as a mechanism way to confront unauthorized extraction of steganocontent. *Science and Technology Today*, 13(27), с. 701-717, DOI: https://doi.org/10.52058/2786-6025-2023-13(27)-701-717
14. Гончаров, М., Малахов, С., & Колованова, Є. (2024). Результати моделювання різних схем просторової орієнтації та розгортки серій опорних блоків зображень для протидії несанкціонованої екстракції стеганографічних даних. *Комп’ютерні науки та кібербезпека*, (2), 58-70. DOI: https://doi.org/ 10.26565/2519-2310-2023-2-06
15. Honcharov, M., & Malakhov, S. (2024). Modeling attempts of unauthorized extraction of steganocontent under different combinations of data key-extractor. *Débats scientifiques et orientations prospectives du développement scientifique*. pp. 234–245. DOI: https://doi.org/10.36074/logos-01.03.2024.053
16. Honcharov, M., & Malakhov, S. (2025). Analysis of prerequisites for ensuring resource consensus when performing steganographic data insertion procedures. *Modern Information Security*, 63(3), 37–47. DOI: https://doi.org/10.31673/2409-7292.2025.030518
17. Honcharov, M., & Malakhov, S. (2025). Assessment of the complexity of input data preprocessing procedures for implementing steganographic transformations. *Scientific Trends and Trends in The Context of Globalization. Proceedings of the 9th International Scientific and Practical Conference*. Umea, Sweden. 2025. Pp. 275-283. URL: https://archive.interconf.center/index.php/2709-4685/issue/view/19-20.06.2025/262

18. Гончаров, М.О., & Малахов, С.В. (2021). Моделювання процедур підготовки даних стеганоалгоритма з багаторівневим мультиплексуванням контенту. *Комп'ютерне моделювання в наукоємних технологіях* (КНМТ-2021): Матеріали 7-ї міжнар. наук.-техн. конф. (pp. 118–122). ХНУ ім. В. Н. Каразіна.
19. Малахов, С., & Гончаров, М. (2024). Уточнення процедур формування серій опорних блоків зображень на етапі їх передобробки при реалізації процедур стегановставки. *Grail of Science*, (46), 694–700. URL: https://archive.journal-grail.science/index.php/2710-3056/issue/view/29.11.2024/34
20. Гончаров, М., & Малахов, С. (2023). Дослідження способів розгортки вихідних блоків зображення-стеганоконтенту як механізму протидії від несанкціонованої екстракції даних. *Наука і техніка сьогодні,* 4(18), с. 293-308. DOI: https://doi.org/10.52058/2786-6025-2023-4(18)-293-308

EVALUATION OF THE RESULTS OF SPATIAL CONVERSIONS OF BASIC BLOCKS OF CONTENT AS A SEPARATE STAGE OF A HYBRID STEGANOGRAPHIC ALGORITHM

Mykyta Honcharov[1], Postgraduate student of the Department of Cybersecurity of Information Systems, Networks and Technologies; e-mail: m.honcharov@student.karazin.ua;
ORCID: https://orcid.org/0000-0002-9790-7260
Serhii Malakhov[1], Ph.D., Senior Researcher, Associate Professor of the Department of Cybersecurity of Information Systems, Networks and Technologies; e-mail: malakhov@karazin.ua;
ORCID: https://orcid.org/0000-0001-8826-1616
[1] *V. N. Karazin Kharkiv National University, Ukraine*
Manuscript was received September 1, 2025; Received after review October 1, 2025;
Accepted November 2, 2025; Published December 30, 2025

Abstract. The work presents the results of modeling and analyzing the consequences of implementing procedures for changing the spatial orientation of basic blocks (BBs) of images extracted from an array of lengths series of BBs content. The purpose of this work is to determine the character of the influence and consequences of using various variants of spatial conversion of BBs of an image-content on its resistance to attacks and computational complexity. The conducted modeling demonstrated that spatial transformations of BBs of content, despite their low computational complexity and complete reversibility, provide an effective and independent level of protection. Integrating the appropriate procedures, in compatible with other levels (tools) of protection, significantly enhances the final effect, improving the robustness of steganographic content against attempts at unauthorized extraction. The evaluation of the computational complexity of spatial conversions of BBs of content confirmed the possibility of ensuring resource consensus when performing these procedures, even in conditions of a shortage of free resources used by hardware platforms. It was concluded that the wide combinatoriality of possible schemes for implementing spatial transformations of BBs is an effective and computationally «light» tool for countering attempts at unauthorized access to content. The results obtained confirm the prospects for applying the mechanism of changing the spatial orientation of BBs of content in low-resource algorithms for steganographic information protection and/or corresponding mobile applications. This opens up broad opportunities for further improvement of the considered concept of steganographic insertion image by expanding the combinatorics of the structure of the data extractor key, adaptive selection of processing parameters, and combining variants of spatial transformations of BBs of image content.

Keywords: *information security, threats, cyberattack, computational complexity, digital images, data encapsulation, data extraction, spatial orientation, unauthorized access, steganography, run-length encoding*

Conflicts of Interest: the authors declare no conflict of interest.

ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 2 (28)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 2 (28)

https://doi.org/10.26565/2519-2310-2025-2-02
УДК 004.89:004.4

КОНЦЕПЦІЯ ІНТЕЛЕКТУАЛЬНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ ПРОВЕДЕННЯ ПРИЙМАЛЬНОГО ТЕСТУВАННЯ НЕЙРОННИХ МЕРЕЖ ГЛИБОКОГО НАВЧАННЯ

Юрій Галайчук[1], аспірант кафедри комп'ютерних систем та робототехніки ННІ комп'ютерних наук та штучного інтелекту; e-mail: yurii.halaichuk@student.karazin.ua, ORCID: https://orcid.org/0000-0004-1048-9425

Марина Мірошник[1], доктор технічних наук, професор кафедри комп'ютерних систем та робототехніки ННІ комп'ютерних наук та штучного інтелекту; e-mail: m.miroshnyk@karazin.ua, ORCID: https://orcid.org/0000-0002-2231-2529

Ельвіра Кулак[2], доктор філософії, доцент кафедри автоматизації проектування; e-mail: elvira.kulak@nure.ua, ORCID: https://orcid.org/0000-0002-8441-5187

[1]*Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна*

[2]*Харківський національний університет радіоелектроніки, пр. Науки, 14, Харків, 61166, Україна*

Рукопис надійшов 2 вересня 2025 р. Отримано після рецензування 1 жовтня 2025 р. Прийнято 2 листопада 2025 р. Опубліковано 30 грудня 2025 р.

Анотація: У сучасному світі все більше критичних інфраструктур та комерційних систем покладаються у своїй роботі на результати обчислень алгоритмів штучного інтелекту, зокрема нейронних мереж. Паралельно з цим набуває великого значення проведення процесу оцінювання якості роботи таких алгоритмів та належного виконання всіх етапів їх тестування для усунення можливих недоліків та забезпечення здатності отримувати очікувані результати. Дана стаття присвячена проблемі вдосконалення процесу приймального тестування користувачами (User Acceptance Testing, UAT) для предметно-орієнтованого програмного забезпечення, що використовує нейронні мережі глибокого навчання. У роботі розглядаються виклики, пов'язані з обмеженими ресурсами, недостатньою кваліфікацією команд UAT у сфері машинного навчання та складністю тестування систем, які продовжують навчатися після початкової розробки та проведений загальний огляд наявних шляхів вирішення зазначених проблем з вказанням їх переваг та недоліків. Запропоновано концепт інтелектуальної інформаційної системи, що базується на моделі прогнозування для оцінки показників якості нейронних мереж, зокрема точності та функції втрат та дозволяє провести процес оцінювання якості таких мереж використовуючи набір навчальних і валідаційних даних. Описано експериментальну методологію, яка включає алгоритм розробки моделі прогнозування для аналізу трендів якості нейронної мережі та розробку інтелектуальної інформаційної системи для прискорення та спрощення процесу UAT. Представлено схему розгортання компонентів системи, що охоплює взаємодію між клієнтськими додатками, веб-сервером, сервером виконання та базою даних із застосуванням сучасних мережевих протоколів та технологій. Результати дослідження спрямовані на підвищення ефективності проведення процесу UAT шляхом його автоматизації та застосування моделі передбачення для отримання динамічних показників якості алгоритмів нейронних мереж глибокого навчання.

Ключові слова: *глибоке навчання, інтелектуальна інформаційна система, модель передбачення, оцінювання якості, приймальне тестування користувачами*

Як цитувати: Галайчук Ю., Мірошник М., Кулак Е. Концепція інтелектуальної інформаційної системи для проведення приймального тестування нейронних мереж глибокого навчання. *Комп’ютерні науки та кібербезпека.* 2025; № 2(28): С. 21–31. https://doi.org/10.26565/2519-2310-2025-2-02

In cites: Halaichuk Y., Miroshnyk M., Kulak E. (2025). The concept of an intelligent information system for conducting acceptance testing of deep learning neural networks. *Computer Science and Cybersecurity. 2(28)*: 21–31. https://doi.org/10.26565/2519-2310- 2025-2-02 (in Ukrainian)

1. Вступ

Завдяки стрімкому розвитку галузі машинного навчання та зростанню обчислювальних потужностей у сучасному світі ми спостерігаємо стрімке проникнення технологій штучного інтелекту, зокрема нейронних мереж глибокого навчання (Deep Learning), у різноманітні сфери людської діяльності [1]. Від автоматизованого аналізу медичних зображень для ранньої діагностики захворювань та розпізнавання мови в голосових помічниках до виявлення шахрайства та обробки фінансових транзакцій у фінансовому секторі, алгоритми глибокого навчання здатні обробляти складні дані та приймати інтелектуальні рішення. Часто таке програмне забезпечення є предметно-орієнтованим та розробляється по замовленню користувачів, проходячи життєвий цикл розробки від аналізу вимог до приймального тестування (User Acceptance Testing, UAT).

Ключовою відмінністю нейронних мереж глибокого навчання є те, що такі мережі продовжують навчатись після закінчення процесу їх розробки та початкового навчання, що значно ускладнює їх тестування. При цьому у предметно-орієнтованому програмному забезпеченні алгоритм нейронної мережі глибокого навчання може бути лише невеликою частиною відносно загального його обсягу, а UAT проводиться командами, учасники яких є спеціалістами у предметній галузі, але не є спеціалістами у галузі машинного навчання [11].

Через сукупність цих факторів, а також обмеженні ресурси на проведення UAT у порівнянні із загальним процесом розробки та тестування програмного забезпечення, виникає загальна потреба у розробці та впровадженні інноваційних підходів до UAT, які б могли забезпечити більш глибоку та автоматизовану перевірку функціональності складного програмного забезпечення, що використовує алгоритми нейронних мереж глибокого навчання.

2. Постановка проблеми

Приймальне тестування користувачами є фінальним етапом тестування програмного забезпечення перед його введенням в експлуатацію, спрямованим на підтвердження готовності системи до використання реальними користувачами в їхньому наближеному до реального середовищі [2]. Зазвичай процес UAT проводиться окремою незалежною командою з боку замовника (користувача) та включає в себе виконання інших типів тестування програмного забезпечення з метою верифікації на відповідність заявленим вимогам. У контексті програмного забезпечення, що використовує алгоритми нейронних мереж глибокого навчання, проведення ефективного UAT особливо важливо, оскільки неправильна робота або неочікувана поведінка таких систем може призвести не лише до фінансових втрат, але й до серйозних наслідків у сферах, де приймаються критично важливі рішення на основі їх висновків.

Незважаючи на те, що не існує точно зазначених правил, скільки часу відносно загального терміну життєвого циклу програмного забезпечення (SDLC) мають займати різні типи тестування, звернувшись до теорії тестування можна сформувати наступний розподіл [3, 4, 5]:

Таблиця 1 – Порівняння приблизного часу на виконання типів тестування відносно SDLC
Table 1 – Comparison of estimated execution time of test types relative to SDLC

Тип тестування	Час на тестування відносно SDLC	Чи входить до UAT
Модульне тестування	5-10%	Ні
Інтеграційне тестування	10-15%	Так
Функціональне тестування	20-30%	Так
Приймальне тестування користувача	**10-15%**	**-**
Регресійне тестування	5-10%	Ні
Тестування продуктивності	10-15%	Так
Тестування безпеки	10-15%	Так
Тестування зручності та інтерфейсу користувача	5-10%	Так

Значення можуть значно відрізнятися залежно від специфіки та архітектури проекту, проте з Таблиці 1 можна побачити, що на UAT виконується за малий термін відносно загального життєвого циклу програмного забезпечення та включає в себе великий обсяг робіт. Також, додатково процес ускладнюють:

а) відсутність у команд тестування, що проводять UAT з боку замовника, кваліфікацій у машинному навчанні - знайти людей, які одночасно є спеціалістами у предметній галузі та машинному навчанні важко та не завжди фінансово доцільно;

б) відсутність доступу у UAT команди до процесу розробки та навчання нейронної мережі.

Зазвичай, для проведення UAT у таких випадках застосовуються наступні способи [6]:

1. Використання існуючої бізнес-логіки для передачі вхідних даних що використовуються для подальшого навчання алгоритму та використання наявного набору валідаційних даних для верифікації вихідних даних [7]. Цей підхід має певні недоліки, такі як високі витрати часу на введення даних та необхідність мати великий об’єм навчальних даних, що не використовувались при початковому навчанні алгоритму. Частково проблема з введенням даних вирішується застосуванням засобів автоматизації, імпортом даних у базу даних або за допомогою імпорту через файловий формат, проте, такі можливості не завжди наявні у системі без додаткових доопрацювань, а доопрацювання можуть бути не обгрунтовані економічно.

2. Застосування методів пояснення роботи нейронних мереж, таких як SHAP (SHapley Additive exPlanations) [8] та LIME (Local Interpretable Model-agnostic Explanations) [9], заснованих відповідно на теорії ігор та лінійній регресії, для інтерпретації зв’язків у моделі нейронної мережі. Ці методи є класичними методами тестування чорної скрині (black box

testing) нейронних мереж, проте їх недоліками в контексті проведення UAT є відносна математична складність та нездатність моделювати саме процес донавчання моделі.

3. Використання методів імітаційного моделювання (Synthetic Data Generation, Environment Simulation, Adversarial Attack Simulation, Monte Carlo Simulation). Такі методи дозволяють провести тестування із покриттям багатьох нестандартних випадків, проте, потребують створення нових наборів даних для тестування та є більш доцільними до використання протягом розробки та модульного тестування нейронних мереж.

Таким чином, існує потреба у впровадженні методології незалежного тестування нейронних мереж глибокого навчання з урахуванням часових обмежень та кваліфікації команд, що проводять тестування.

3. Концепція інтелектуальної інформаційної системи для проведення UAT нейронних мереж глибокого навчання

У вирішенні зазначених проблем могла б допомогти розробка інтелектуальної інформаційної системи з алгоритмом моделі передбачення, що надасть змогу передбачити тренд показників якості нейронних мереж, зокрема мереж глибокого навчання та провести незалежне тестування використовуючи наявний набір навчальних та валідаційних даних.

Короткий опис дослідження, спрямованого на розробку моделі передбачення для тестування мереж глибокого навчання, може виглядати наступним чином:

1. Програмна реалізація нейронної мережі для збору даних з відповідності показників якості ступеням навчання (Мережа А);
2. Розподіл навчальних даних Мережі А на три частини - навчальну, валідаційну, дані для донавчання.
3. Використання навчального набору даних для навчання Мережі А.
4. Використання валідаційного набору даних для зняття показників точності, значення функції втрат на n епохах (ітераціях) навчання Мережі А при різних конфігураціях навчальних даних.
5. Застосування програмних та математичних методів для розробки та реалізації моделі прогнозування (умовно Мережа В).
6. Навчання Мережі В на отриманих при тестуванні мережі а показниках.
7. Застосування Мережі В для прогнозування показників точності, значення функції втрат при подальшому навчанні Мережі А.
8. Тестування моделі із застосуванням набору даних для донавчання, що емулює подальше навчання Мережі А та порівняння отриманих реальних даних з результатами прогнозування Мережі В.

3.1. Вибір моделі для проведення збору показників якості роботи нейронної мережі.

Для збору показників якості було вирішено використовувати модель класифікації зображень, оскільки класифікація зображень є відносно простою задачею та при цьому широко застосовується у предметно-орієнтованих системах. Оскільки кінцевою метою роботи є розробка системи для широкої аудиторії користувачів, були розглянуті найбільш популярні типи нейронних мереж що використовуються при навчанні та тестуванні для задач класифікації зображень, такі як залишкові (Residual network, ResNet), згорткові (Convolutional networks, зокрема, MobileNet та VGG), зорові трансформери (Vision Transformers, ViT), нейронні мережі прямого поширення (Feedforward neural network, FNN).

Також при виборі типу нейронної мережі крім ступеня її розповсюдженості були враховані наступні критерії:

1. складність та місткість архітектури (Capacity): модель не повинна бути занадто простою або занадто складною задля запобігання швидкого перенавчання або недонавчання;
2. динаміка збіжності (Convergence Dynamics): для отримання достатньої вибірки даних для навчання моделі прогнозування необхідна тривала фаза навчання Мережі А;
3. чутливість до гіперпараметрів: при формуванні набору даних з показників навчання Мережі А необхідні невдалі епохи навчання, яких можна добитись зміною налаштувань мережі;
4. ефективність обчислення: одна епоха навчання не має займати вкрай довгий час.

Стислий аналіз розглянутих типів нейронних мереж наведено у таблиці 2 [10][15][16]. Згідно з проведеним аналізом було прийняте рішення використовувати для збору показників ефективності згорткову модель глибинного навчання MobileNet.

Таблиця 2 – Порівняння архітектур-класифікаторів для генерації метрик
Table 2 – Comparison of classifier architectures for metric generation

Критерій	ResNet	MobileNet	Vision Transformer	VGG	FNN
Складність та місткість	Середня / Висока	Низька	Дуже висока	Висока	Залежить від кількості шарів нейронів
Динаміка збіжності	Стабільна (плавна крива втрат)	Швидка, але нестабільна (є коливання метрик)	Дуже повільна	Повільна	Дуже швидка лише на початку
Чутливість до гіперпарамет рів	Середня	Низька	Дуже висока	Середня / Висока	Дуже висока
Ефективність обчислення	Висока	Найвища	Низька	Низька	Низька для зображень

3.2. Вибір моделі прогнозування.

Вибір моделі для прогнозування результатів навчання базується на аналізі метрик як часових рядів. Оскільки значення точності та втрат на кожній епосі прямо залежать від попередніх кроків, головним критерієм вибору архітектури є її здатність працювати з послідовними даними та «запам'ятовувати» тренди.

Для цієї задачі було розглянуто архітектури, що здатні ефективно виявляти закономірності у зміні градієнта. Рекурентні мережі (наприклад, LSTM) є пріоритетними, оскільки вони спроможні відрізнити випадкові коливання метрик від реального плато. Водночас модель має бути достатньо компактною, щоб не перенавчатися на обмеженій кількості кривих навчання, зібраних під час тестування мережі класифікатора. Таким чином, пріоритетом є баланс між глибиною пам'яті моделі та швидкістю її роботи для оперативного прийняття рішень у процесі UAT.

При виборі моделі було враховано наступні критерії:

1. обробка послідовностей (Sequential Dependency): здатність мережі пам'ятати, що відбувалося на 1-й епосі, коли вона аналізує 10-ту;
2. робота з вхідними даними змінної довжини: можливість дати прогноз як після 5-ї епохи, так і після 50-ї;
3. ризик перенавчання на малих вибірках: оскільки набір даних «кривих навчання» відносно невеликий, модель не повинна бути надто складною;
4. швидкість виведення (Inference Speed): прогноз має бути миттєвим, оскільки система передбачає отримання даних у реальному часі;
5. здатність до екстраполяції: наскільки точно мережа може передбачити значення на 100-й епосі, бачачи лише перші 10.

Стислий аналіз розглянутих типів нейронних мереж наведено у таблиці 3 [17] [18] [19] [20]:

Таблиця 3 – Стислий аналіз розглянутих типів нейронних мереж
Table 3 – Brief analysis of the considered types of neural networks

Критерій	LSTM / GRU (Рекурентні)	1D-CNN (Згорткові 1D)	Трансформери	Multilayered perceptron (MLP)
Обробка послідовностей	Має «внутрішню пам'ять» про минулі епохи	Обмежена розміром вікна згортки	Теоретично необмежена	Відсутня
Тип даних	Спадкові послідовності	Локальні патерни в часі	Глобальні залежності	Статичні вектори
Стійкість до малих наборів даних	Середня	Висока	Низька	Дуже висока
Швидкість	Низька	Висока	Середня / Низька	Найвища
Здатність до екстраполяції	Висока	Висока	Висока	Середня

Після проведеного аналізу найкращим вибором визнана Довга короткочасна пам'ять (Long Short-Term Memory, LSTM) або її спрощена версія Вентильний рекурентний вузол (Gated recurrent units, GRU). Вибір цих моделей зумовлений їх здатністю ефективно опрацьовувати часові послідовності метрик, зберігаючи інформацію про динаміку навчання на довгих інтервалах епох.

Основні переваги застосування LSTM / GRU для поставленої задачі:

1. Точність прогнозування: завдяки механізму «пам’яті», модель здатна екстраполювати значення Accuracy та Loss, ідентифікуючи передчасний вихід на плато або деградацію градієнта.
2. Універсальність: модель демонструє стабільні результати при роботі з вхідними даними від різних класифікаторів (ResNet, MobileNet), що робить її надійним інструментом для етапу UAT.

3.3. Проектування інтелектуальної інформаційної системи.

Для подальшої автоматизації може бути впроваджена інформаційна система, яка дозволяє передавати на вхід дані про залежність показників якості роботи нейронної мережі від конфігурації навчальних даних (наприклад, у файловому вигляді), задавати очікувану конфігурацію реальних даних, які буде обробляти алгоритм нейронної мережі після його впровадження у роботу та у реальному часі отримувати прогноз очікуваних показників якості роботи мережі, що тестується, у процесі її подальшого навчання. Можлива архітектура такої системи представлена на Схемі 1.

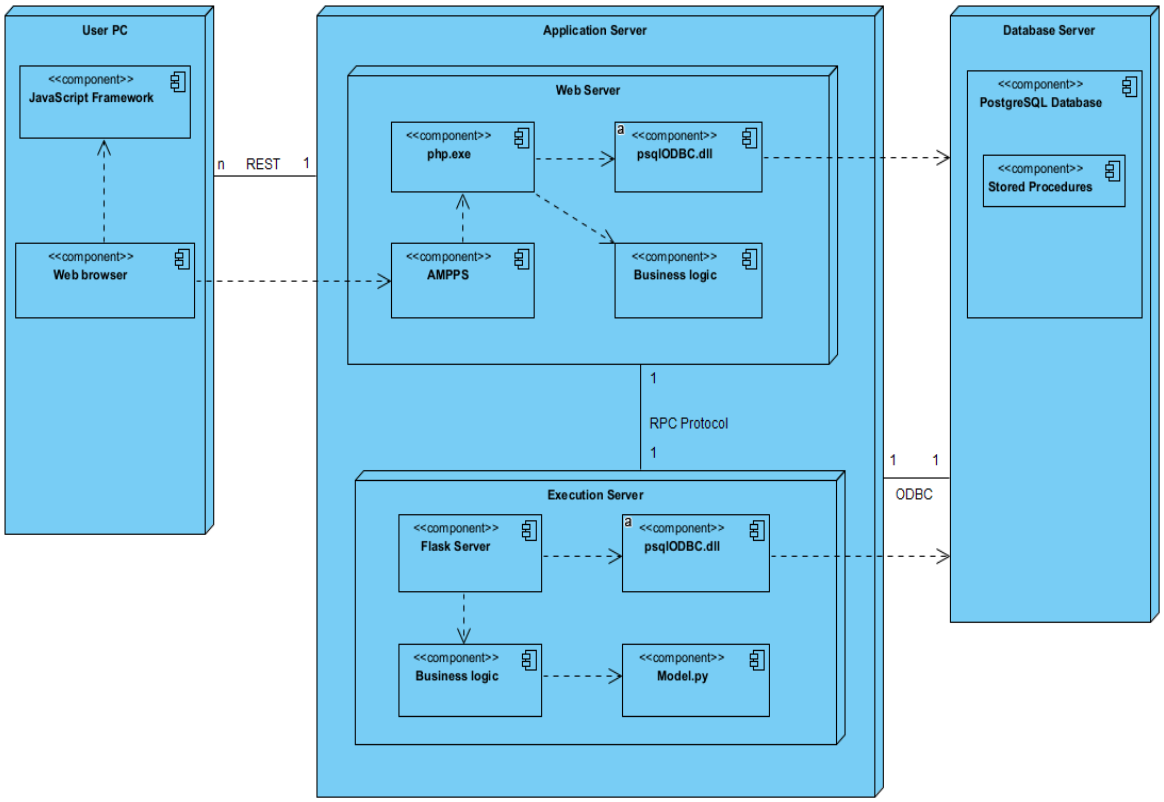

Схема 1 – Діаграма розгортання компонентів [12]

Figure 1 - Component Deployment Diagram[12]

Де:

Вузол User PC:

1) Web Browser - програма веб-браузер, що надає користувачеві доступ до системи;
2) JavaScript Framework - це каркас коду JS, що є необхідним для програмної реалізації певної бізнес-логіки на стороні клієнта.

Вузол Web Server [13]:

1) AMPPS - це каркас для виконання php коду веб-сторінок;
2) php.exe - php інтерпретатор;
3) psqlODBC.dll - PostgreSQL ODBC драйвер;
4) Business logic - програмний код на мові php, що виконує певну частину бізнес логіки (парсинг отриманих від користувача файлів з даними для подальшої обробки)

Вузол Execution Server:

1) Flank Server - це каркас для виконання back end python коду;

2) Business logic - програмний код на мові python, що виконує певну частину бізнес логіки (обробку отриманих від користувача даних);
3) Model.py - це модель передбачення на основі нейронної мережі, що використовується для отримання вихідних даних;
4) psqlODBC.dll - PostgreSQL ODBC драйвер;

Вузол Database Server[14]:

1) PostgreSQL - це БД системи, з якою Web-сервер взаємодіє за допомогою протоколу драйверів ODBC (Open Database Connectivity), а компонент StoredProcedure - це збережені процедури, що містяться у БД системи.

Обмін статичними (збереженими) даними при цьому відбувається через БД, до якої мають доступ компоненти як Web Server, так і Execution Server. Обмін даними між серверами у реальному часі (наприклад, даними про початок / закінчення обробки отриманих даних) відбувається з використанням RPC Protocol (A Remote Procedure Call). Для комунікації вузлів User PC та Web Server використовується REST архітектура мережевих протоколів, оскільки майже не має обмежень щодо формату передачі наборів даних.

Запропонована система має певні переваги та недоліки. Із переваг можна відмітити:

1. універсальність: модель може працювати із різними нейронними мережами спільної архітектури, що усуває необхідність у запровадженні інструментів з автоматизації протягом розробки кожного окремого проекту;

2. швидкість застосування: завдяки автоматизації процесу система дозволяє значно заощадити час на тестування в умовах UAT;

3. низькі вимоги до кваліфікації користувачів у галузі машинного навчання, що робить використання системи доступним для будь-якої команди спеціалістів у предметній галузі;

4. відсутність необхідності у великому обсязі реальних даних для тестування;

5. рішення може бути інтегровано у процес тестування доповнюючи використання інших наявних методів, наприклад, SHAP і LIME для подальшої інтерпретації незадовільних по показникам якості вихідних даних.

Недоліки:

1. модель передбачення не здатна надавати точні значення очікуваних показників якості, а лише значення їх трендів, що можуть бути використані для прийняття рішення про проходження процесу UAT або повернення на доопрацювання;

2. система потребує передачі даних про навчання нейронної мережі, що тестується, від команди розробки до UAT команди, що часто є звичайним процесом передачі тестової документації;

3. модель передбачення вимагає формування очікуваної (estimated) конфігурації даних, що будуть у подальшому використані для здійснення навчання після процесу тестування; ця вимога є типічної вимогою при проведенні процесу тестування та збір очікуваних даних про майбутню роботу програмного забезпечення є невід’ємною частиною таких типів тестування, як тестування продуктивності та тестування сумісності.

4. Висновки

У результаті проведеного аналізу встановлено, що сучасні підходи до приймального тестування користувачами (UAT) програмного забезпечення, яке використовує нейронні мережі глибокого навчання, стикаються з низкою викликів, зокрема через обмежені часові ресурси, недостатню кваліфікацію команд у сфері машинного навчання та складність тестування систем, що продовжують навчатися після початкового етапу розробки. Ці фактори ускладнюють забезпечення надійності та відповідності таких систем заявленим вимогам, особливо в

предметно-орієнтованому програмному забезпеченні, де нейронні мережі є лише частиною загальної архітектури.

Запропонована концепція інтелектуальної інформаційної системи для автоматизації UAT нейронних мереж глибокого навчання базується на використанні моделі передбачення, яка дозволяє прогнозувати показники якості, такі як точність і значення функції втрат, на основі даних, отриманих із тестування базової нейронної мережі. Такий підхід дає змогу моделювати процес донавчання мережі та проводити незалежне тестування з використанням наявних навчальних і валідаційних даних, що зменшує залежність від великих обсягів нових даних і знижує витрати часу на введення даних.

Проведений стислий аналіз існуючих архітектур нейронних мереж, які підходять для задач збору показників навчання для прогнозування з формуванням ключових критеріїв вибору та обґрунтований вибір моделі для кожної из задач.

Розроблена схема розгортання компонентів системи, яка включає вузли User PC, Web Server, Execution Server і Database Server, забезпечує ефективний обмін даними через REST-архітектуру, RPC-протокол і ODBC-драйвери. Це дозволяє реалізувати гнучку та масштабовану систему, здатну обробляти дані в реальному часі та зберігати статичні дані для подальшої обробки.

Запропонована методологія має потенціал для спрощення UAT шляхом автоматизації ключових етапів тестування, зменшення залежності від висококваліфікованих спеціалістів у галузі машинного навчання та підвищення точності оцінки якості нейронних мереж. Подальші дослідження можуть бути спрямовані на вдосконалення моделей прогнозування, розширення їхньої застосовності до складніших архітектур нейронних мереж, а також інтеграцію з іншими методами пояснення роботи нейронних мереж, такими як SHAP і LIME, для забезпечення більшої інтерпретованості результатів.

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

References

1. Directive (Goodfellow I., Bengio Y., Courville A. (2016) *Deep Learning*. Cambridge: MIT Press, 800 c. Deep Learning - Ian Goodfellow, Yoshua Bengio, Aaron Courville https://books.google.com.ua/books/about/Deep_Learning.html?id=Np9SDQAAQBAJ&redir_esc=y
2. Sommerville I. (2015) *Software Engineering*. 10th ed. Boston: Pearson, 816 c.Software Engineering, Global Edition - Ian Sommerville https://books.google.com.ua/books/about/Software_Engineering_Global_Edition.html?id=W_LjCwAAQBAJ&redir_esc=y
3. Myers G.J., Sandler C., Badgett T. (2011) *The Art of Software Testing*, 3rd ed, New York: Wiley, 256 c. The Art of Software Testing - Glenford J. Myers, Corey Sandler, Tom Badgett https://books.google.com.ua/books/about/The_Art_of_Software_Testing.html?id=GjyEFPkMCwcC&redir_esc=y
4. ISO/IEC/IEEE 29119-1:2013. (2013) *Software and Systems Engineering. Software Testing Part 1: Concepts and Definitions.* Geneva: International Organization for Standardization.ISO/IEC/IEEE 29119-1:2013 | IEC https://webstore.iec.ch/en/publication/11972
5. International Software Testing Qualifications Board. (2023). *ISTQB Certified Tester Foundation Level Syllabus (Version 4.0.1)*. URL: https://www.istqb.org/certifications/ certified-tester-foundation-level
6. Russell S., Norvig P. (2020) *Artificial Intelligence: A Modern Approach*,4th ed, Boston:Pearson, 1152 c. Artificial Intelligence: A Modern Approach, 4th US ed. https://aima.cs.berkeley.edu/
7. Tian, Y., Pei, K., Jana, S., & Ray, B. (2018). *DeepTest: Automated Testing of Deep-Neural-Network-Driven Autonomous Cars*. Proceedings of the 40th International Conference on Software Engineering.

DeepTest: Automated Testing of Deep-Neural-Network-driven Autonomous Cars https://arxiv.org/pdf/1708.08559v1

8. Lundberg S.M., Lee S.I. (2017) *A Unified Approach to Interpreting Model Predictions // Advances in Neural Information Processing Systems (NeurIPS)*, Vol. 30, c. 4765-4774. DOI: https://doi.org/10.48550/arXiv.1705.07874
9. Ribeiro M.T., Singh S., Guestrin C. (2016) *"Why Should I Trust You?": Explaining the Predictions of Any Classifier* // Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, c. 1135-1144. DOI: https://doi.org/10.1145/2939672.2939778
10. He K. (2016) *Deep Residual Learning for Image Recognition* / K. He, X. Zhang, S. Ren, J. Sun // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). - P. 770-778.https://doi.org/10.48550/arXiv.1512.03385
11. Zhang J. M., Harman M., Ma L., Liu Y. (2020) *Machine Learning Testing: Survey, Landscapes and Horizons* // IEEE Transactions on Software Engineering. Vol. 48 No. 1, c. 1-36. DOI: https://doi.org/10.1109/TSE.2019.2962027
12. Axel K. (1998) *Using UML for Business Object Based Systems Modeling* / Korthaus Axel // ResearchGate. https://doi.org/10.1007/978-3-642-48673-9_15
13. Nawroze I. (2023) *A Comparative Analysis of PHP and Python Programming Languages for Optimal Software Development* / I. Nawroze, C. Rubel // International Journal of Information Technology 8(1): 1-13, URL: http://dx.doi.org/10.6084/m9.figshare.24885846.v1
14. Faisal Qureshi, Haida Rasheed. (2022) *Comparative Analysis of Modern Database Technologies for Scalable Data Storage in AI-Driven Ecommerce Applications* / Faisal Qureshi, Haida Rasheed // ResearchGate, URL: http://dx.doi.org/10.13140/RG.2.2.14668.83848
15. Howard A.G. (2017) *MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications* / A. G. Howard, M. Zhu, B. Chen [et al.]. - URL: https://arxiv.org/abs/1704.04861
16. Tan M. (2019) *EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks* / M. Tan, Q. V. Le // International Conference on Machine Learning (ICML). https://doi.org/10.48550/arXiv.1905.11946
17. Hochreiter S. (1997) *Long Short-Term Memory* / S. Hochreiter, J. Schmidhuber // Neural Computation. - Vol. 9, Iss. 8. - P. 1735-1780.https://doi.org/10.1162/neco.1997.9.8.1735
18. Vaswani A. (2017) *Attention is All You Need* / A. Vaswani, N. Shazeer, N. Parmar [et al.] // Advances in Neural Information Processing Systems (NIPS). - P. 5998-6008. https://doi.org/10.48550/arXiv.1706.03762
19. Ismail Fawaz H. (2019) *Deep learning for time series classification: a review* / H. Ismail Fawaz, G. Forestier, J. Weber [et al.] // Data Mining and Knowledge Discovery. - Vol. 33. - P. 917-963. https://link.springer.com/article/10.1007/s10618-019-00619-1
20. Domhan T. (2015) *Speeding Up Automatic Hyperparameter Optimization of Deep Neural Networks by Extrapolating Learning Curves* / T. Domhan, J. T. Springenberg, F. Hutter // Proceedings of the 24th International Joint Conference on Artificial Intelligence (IJCAI).- P. 3460-3468.https://dl.acm.org/doi/10.5555/2832581.2832731

THE CONCEPT OF AN INTELLIGENT INFORMATION SYSTEM FOR CONDUCTING ACCEPTANCE TESTING OF DEEP LEARNING NEURAL NETWORKS

Yurii Halaichuk[1], PhD student of Computer Systems and Robotics Department Institute of Computer Science and Artificial Intelligence; e-mail: yurii.halaichuk@student.karazin.ua; ORCID: https://orcid.org/0009-0004-1048-9425
Maryna Miroshnyk[1], Doctor of technical sciences, Professor of Computer Systems and Robotics Department Institute of Computer Science and Artificial Intelligence; e-mail: m.miroshnyk@karazin.ua; ORCID: https://orcid.org/0000-0002-2231-2529
Elvira Kulak[2], PhD, Associate Professor, Associate Professor of Design Automation Department; e-mail: elvira.kulak@nure.ua; ORCID: https://orcid.org/0000-0002-8441-5187
[1] *V. N. Karazin Kharkiv National University, Ukraine*
[2]*Kharkiv National University of Radio Electronics, Nauka Avenue, 14, Kharkiv, Ukraine, 61166*
Manuscript was received September 2, 2025; Received after review October 1, 2025;
Accepted November 2, 2025; Published December 30, 2025

Abstract. In the modern world, an increasing number of critical infrastructures and commercial systems rely on the results of computations by artificial intelligence algorithms, particularly neural networks. In parallel, the process of evaluating the quality of these algorithms and ensuring proper execution of all stages of their testing has become highly significant to eliminate potential flaws and ensure their ability to deliver expected results. The article addresses the issue of improving the User Acceptance Testing (UAT) process for domain-specific software utilizing deep learning neural networks. It examines challenges related to limited resources, insufficient UAT team expertise in machine learning, and the complexity of testing systems that continue learning post-initial development. A general overview of existing solutions is provided, highlighting their advantages and drawbacks. A concept of an intelligent information system based on a predictive model for evaluating neural network quality metrics, specifically accuracy and loss function is proposed, enabling the quality assessment process of such networks using a set of training and validation data. An experimental methodology is described, including the algorithm of development of a predictive model for analyzing network quality trends and the creation of an intelligent information system to streamline and accelerate the UAT process. The system's component deployment architecture is presented, covering interactions between client applications, a web server, an execution server, and a database, leveraging modern network protocols and technologies. The research results aim to enhance UAT efficiency through automation and the application of a predictive model to obtain dynamic quality metrics for deep learning neural network algorithms.

Keywords: *deep learning, intelligent information system, quality assurance, prediction model, user acceptance testing*

Conflicts of Interest: the authors declare no conflict of interest.

ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 2 (28)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 2 (28)

https://doi.org/10.26565/2519-2310-2025-2-03
УДК 621.391:004.7

6G TECHNOLOGY: THE TIME HAS COME

Mhnd Farhan[1], Lecturer at Department of Electrical Engineering, Faculty of Engineering,
e-mail: mhndfarhan@yahoo.com, ORCID: https://orcid.org/0009-0007-0541-6995
[1]*Baghdad University, Iraq*

Manuscript was received September 3, 2025; Received after review October 3, 2025;
Accepted November 2, 2025; Published December 30, 2025

Abstract: The sixth generation of wireless communication technology, or 6G technology, was created to replace 5G. Compared to its predecessors, it promises much faster speeds, more capacity, and reduced latency, opening up new applications and advancing a number of industries. Terabits per second (Tbps) is the target data rate for 6G, which is substantially faster than 5G's gigabits per second (Gbps). In order to facilitate real-time applications and instantaneous data transfer, 6G aims for nearly zero latency, possibly as low as the microsecond level. Compared to 5G's 1 million connected devices per square kilometer, 6G will allow for a potentially 10 million more. With the help of AI and machine learning, 6G will be able to manage resources intelligently, perform better, and add new features. It is anticipated that 6G will facilitate developments in fields such as imaging, location awareness, presence technology, and the Internet of Things (IoT). A review of earlier work is presented in this paper.

Keywords: *6G technology; architecture, applications*

In cites: Mhnd Farhan (2025). 6G Technology: The Time Has Come. *Computer Science and Cybersecurity.* 2(28): 32–39. https://doi.org/10.26565/2519-2310-2025-2-03

1. Introduction

Sixth-generation wireless (6G) is a communication protocol for wireless technologies that may offer lower latency and higher capacity than 5G. It may be able to achieve communication with a latency of one microsecond, which is 1,000 times faster than the estimated latency of 5G cellular technology, which is one millisecond. It is anticipated to be 5G mobile networks' replacement.

6G is currently being researched. Although scientific advances are experimenting with devices capable of operating at higher frequencies, the required high transmission speeds, the energy consumption rates, and the acceptable proportions of the related heat development in the electronic circuits are just some examples of the challenges 6G networks will face in the future. Studies estimate that 6G networks would likely operate in frequencies from 100 GHz to 3 THz due to their wide swaths of the unexplored spectrum (unused frequency waves in the electromagnetic spectrum). An anticipated 1,000-fold speedup over 5G is a communication protocol for wireless communications technologies that facilitate cellular data networks. Consistent connectivity and increased coverage are guaranteed by seamless integration with satellite, Wi-Fi, and fiber optics, particularly in rural regions.

With a potential latency of one microsecond, 6G is a wireless technology communication protocol that could offer higher capacity and lower latency than 5G. This is 1,000 times faster than the estimated 5G cellular technology latency of one millisecond throughput. It is anticipated to be 5G mobile networks' replacement. 6G research is still ongoing. The necessary high transmission speeds, the energy consumption rates, and the acceptable proportions of the related heat development in the electronic circuits are just a few of the difficulties that 6G networks will face in the future, even though scientific advancements are experimenting with devices that can operate at higher frequencies. Due to their extensive coverage of the unexplored spectrum (unused frequency waves in the electromagnetic spectrum), studies predict that 6G networks would most likely function in frequencies between 100 GHz and 3 THz.

The term "wireless cognition," which alludes to wireless networks that might enable free movement of human thoughts over the air, is frequently used by the scientific community to describe 6G. AI applications and remote robots could exchange data at amazing speeds and with excellent coverage in the future thanks to 6G's electromagnetic frequencies. The sub-Terahertz bands would also contain the 6G frequencies. Therefore, based on these many bands, researchers estimate that it could transmit extremely fast calculations across a wide range of frequencies, allowing future mobile devices to have much more amazing capabilities, like human-machine interactions.

2. 6G architecture

The architecture of 6G technology is expected to be extremely intelligent, sustainable, and cyber-resilient, with an emphasis on utilizing new spectrum technologies, AI, and advanced computing. A possible quantum communication backbone, improved edge computing, and a modular design are important features. In addition, the architecture will prioritize digital inclusion, security, and privacy with an eye toward cost reduction and ubiquitous connectivity.

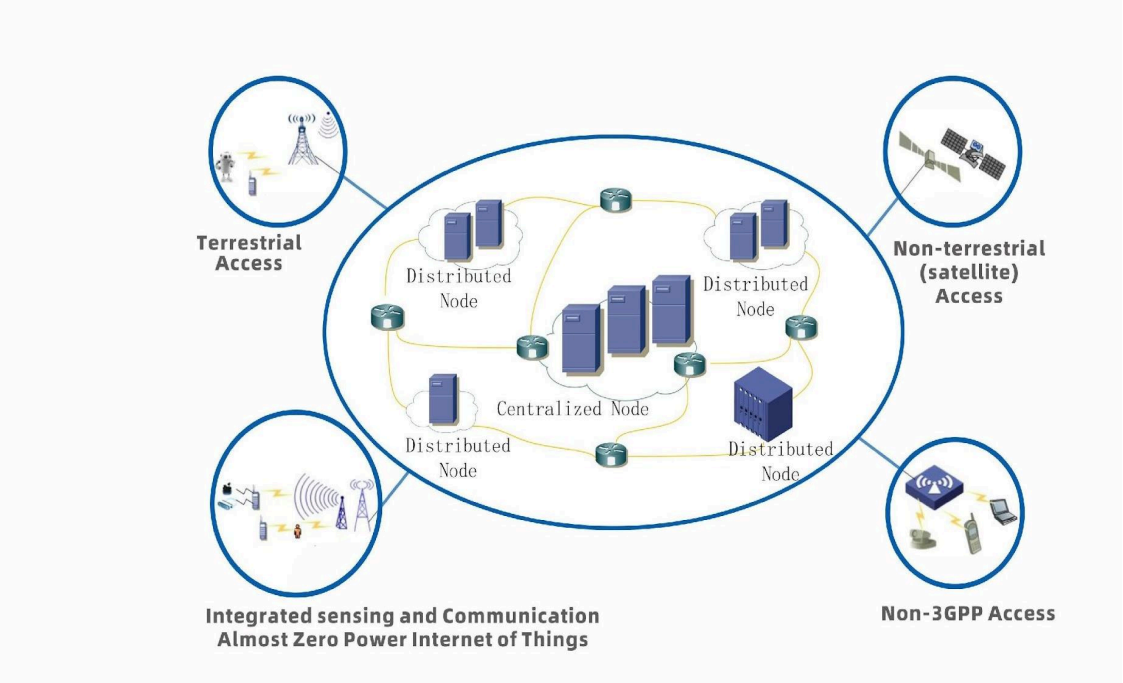

Fig. 1 – 6G architecture

From the standpoint of the air interface, multiple protocol layers may be shared by various planes. Every plane has a different protocol layer configuration, though. Consequently, it is possible to

reuse protocol layers across various planes. Each plane's unique requirements can be satisfied in the interim. According to CN, every plane comprises distinct network functions, each with specific duties as illustrated in Fig. 1. 6G may introduce additional planes based on the control plane and user plane, as well as data planes, depending on the plane and function characteristics. The planes work together to support the essential native traits, such as native security, native intelligence, and native computing. This makes the services available to users. In addition to supporting basic information services like ISAC and converged computing services like integrated Al and communication (IAIAC), it also supports super communication services like 6G NTN and AZP-loT.lt.

3. 6G applications

It is anticipated that 6G applications will transform a number of industries through improvements in computing, sensing, and communication. Improved mobile broadband, fixed wireless access, integrated communication and sensing, and new opportunities for automation and artificial intelligence are a few examples. Additionally, a wide range of services will be made possible by 6G, including remote surgery, smart cities, autonomous cars, holographic communication, and immersive extended reality. A summary of the applications is shown in Fig.2

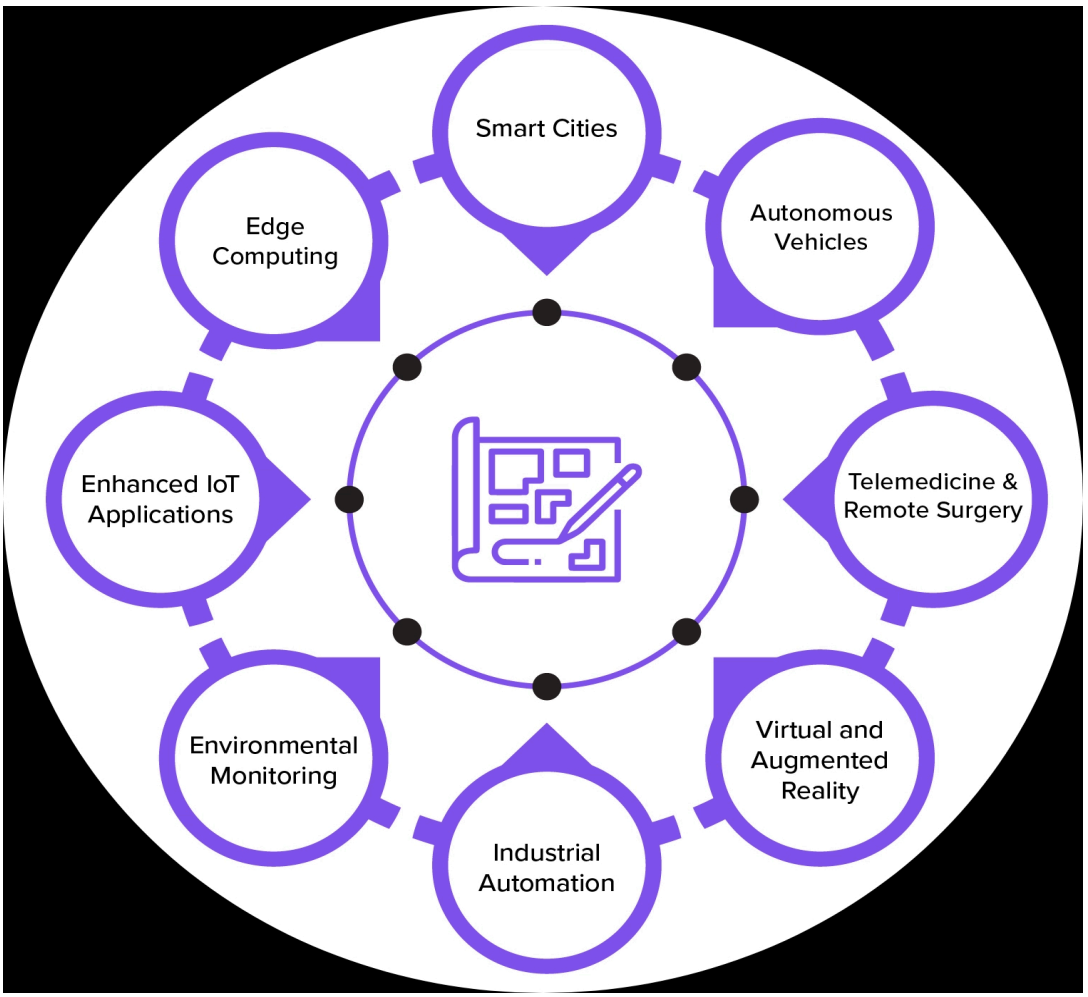

Fig. 2 – Block diagram of 6G applications

4. Literature Survey

The paper in [1] outlines the network architecture and future 6G wireless communication vision. This article discusses new technologies that can help the development of the 6G architecture ensure the quality of service (QoS), including artificial intelligence, terahertz communications, wireless optical technology, free-space optical network, blockchain, three-dimensional networking, quantum communications, unmanned aerial vehicles, cell-free communications, integration of wireless information and energy transfer, integrated sensing and communication, integrated access-backhaul networks, dynamic network slicing, holographic beamforming, backscatter communication, intelligent reflecting surface, proactive caching, and big data analytics. Additionally, potential technologies and anticipated applications with 6G communication requirements are presented. Authors also outline possible obstacles and lines of inquiry to reach this objective.

A groundbreaking study regarding the possible use of 6G to support such extremely demanding applications is presented in [2]. In order to accomplish this, we simulate a 6G system and carry out a case study investigating the use of drone-swarm-based surveillance concepts in a high-definition video monitoring application. Large volumes of video data must be sent over the network in this scenario. The obtained results demonstrate that 6G can handle these high demands on network traffic.

The key technological components required to deploy a 6G communication system are presented in [3]. The creation of an energy-efficient wireless network is the fundamental prerequisite. Intelligent Reflecting Surfaces (IRSs), which are straightforward and reasonably priced structures, are being considered as a replacement for massive MIMO in recent years. The benefits of combining IRSs with other technologies are discussed by the authors of this paper in order to satisfy the demands of next-generation wireless technologies. We go over recent studies on IRS design, IRS multi-cell application, IRS parameter optimization, and the impact of IRS in conjunction with deep learning.

First, the vision and requirements of 6G networks are discussed in [4]. The main enabling technologies that could be used by 6G networks are then discussed. We will pay close attention to index modulation, intelligent surfaces, visible light communications, and terahertz communication technologies. The presentation concludes with a number of issues facing upcoming 6G networks and possible future paths.

The purpose of the paper in [5] is to get a glimpse of the future of wireless communication and related technologies. 6G is anticipated to completely transform the digital world thanks to its higher transmission rate, enhanced spectrum efficiency, larger connection proportions, increased spectrum coherence, and significantly lower latency. The results of a thorough investigation into the development of 6G are presented in this paper. This comprehensive survey's primary focus is on 6G in relation to mobile communication and the major technologies that are anticipated to be deployed on networks enabled by 6G. This paper concludes by outlining current research projects being conducted by different research organizations.

A paper reviewing the state-of-the-art in 6G is found in [6]. With the help of cutting-edge technologies like SC, AI, and ML, authors hope to give readers a foundation in 6G research and an outline of how 6G will be utilized to develop applications. Additionally, the authors conceptualize and identify the role of 6G technology, along with its future challenges and vision. Along with a number of potential future applications for 6G, the authors have also covered the network and user side availability of 6G.

Investigating communication technologies and issues on 6G networks for the internet with the help of the Internet of Things (IOT) is the aim of the article in [7]. Based on a secondary data collection method, the researcher has established a procedure for gathering pertinent data and information about the subject matter. The researcher has used it to guide the study in the right

direction. Likewise, qualitative techniques were employed in the gathered materials to make the data more comprehensible. Additionally, this research will assist readers in comprehending the appropriate efficacy of strategies to alleviate the difficulties in the 6G network system. There are several benefits and challenges associated with implementing a sixth-generation network system, including creating an environmentally friendly, cost-effective network that is compatible with mobile devices and linked to artificial intelligence (AI) technology to increase performance. issues with the next implementation are discussed in this paper.

In order for 6G networks to transition into green networks, research in [8] intends to concentrate on augmenting artificial intelligence in 6G networks.

A thorough review of previous research on the integration of blockchain and artificial intelligence with 6G wireless communications can be found in [9]. More precisely, authors begin with a synopsis of AI and blockchain. The authors then primarily examine the latest developments in the combination of blockchain and artificial intelligence, emphasizing the unavoidable trend of using both technologies in wireless communications. Additionally, the authors thoroughly examine how blockchain and AI can be integrated into wireless communication systems, encompassing secure services and intelligent Internet of Things (IoT) applications. In particular, some of the most talked-about core blockchain and AI-based services are presented, including content caching, spectrum management, computation allocation, security, and privacy. Moreover, authors also focus on some important IoT smart applications supported by blockchain and AI, covering smart healthcare, smart transportation, smart grid, and unmanned aerial vehicles (UAVs). The authors also go into great detail about 6G requirements, visions, and operating frequencies. The authors also examine the unresolved problems and research obstacles related to the integration of blockchain technology and artificial intelligence in 6G wireless communications. Finally, this paper attempts to give a thorough overview of blockchain and AI in 6G networks based on a large number of existing significant works. The survey's creators hope it will provide fresh insight into the study of this recently developed field and act as a guide for future research.

The paper in [10] first gives a thorough overview of the 6G vision, technical specifications, and application scenarios, covering the general consensus on 6G at the moment. The architecture of the 6G network and its main technologies are then critically evaluated. For the first time, advanced 6G verification platforms and testbeds are described in detail. Future research avenues and unresolved issues are also noted in order to further the ongoing international discussion. Lastly, the lessons learned about 6G networks thus far are reviewed.

The 6G WCN framework is presented in [11] along with an example of its main technologies. With the help of a communication scenario demonstration, the various 6G technologies are thoroughly explained, improving key performance indicators with significant variations. The explanation of 6G with the technologies that significantly affect the characteristics of a wireless communication network, including data rate, spectrum efficiency, energy efficiency, connection density, and reliability, is the main contribution of this paper. Each of these technologies has the potential to completely transform the next WCN.

The article in[12] functions as a thorough introduction to 6G by offering a broad overview, a current analysis of the key literature, and an educational tutorial-style presentation format. According to our vision, 6G will be built upon three core components: the Internet of Everything, wireless, and artificial intelligence. 6G can therefore eventually develop into the Intelligent Network of Everything and act as a foundation for mobile intelligence, the next significant development in mobile communication. Mobile intelligence has the potential to make anything intelligent, connected, and aware of its surroundings. This will completely change how systems, apps, and devices are made, how they work and communicate with one another and with people, and how they can be used to benefit individuals, society, and the entire world. The primary details of 6G, such as its essential components,

disruptive applications, and important use cases, are covered after high-level visioning. Particular attention is paid to a wide range of prospective 6G technologies, each of which is presented in a tutorial fashion along with a discussion of the literature, future research directions, opportunities, challenges, history, and future. Lastly, we make some predictions about what will happen after 6G and provide the first high-level overview of 7G. Overall, the goal of this article is to give a comprehensive overview of 6G so that it can be used as a resource and source of inspiration for future research and development projects in industry, academia, and standardization organizations.

With an emphasis on resource management, self-healing, and network security, the paper in [13] suggests an AI-driven framework for 6G networks. It uses machine learning to improve fault recovery, lower latency, and make better decisions in real time. The efficacy of the framework is confirmed by simulations, which also provide scalable solutions for 6G deployment.

The article in [14] reveals how 6G is changing industries, bringing about economic growth, and addressing societal issues. Using contemporary technologies such as terahertz waves and massive MIMO systems, which 6G networks dominate, to achieve data rates, latency, and reliability, the latter provides progressive implementations across various domains. The new idea of human-machine interaction with the new 6G technology is nothing more than a hope for an inventive future. Its applications extend beyond reality to include remote surgery using real-time machines and automated smart factories, as well as communication of autonomous vehicles and immersive experiences. Secondly, a more inclusive society with less economic inequality will result from 6G, which ushers in a new era of growth. 6G networks have the potential to accelerate justice and empower those who were previously marginalized by creating jobs, increasing wealth, and lowering greenhouse gas emissions. Although 6G has many potential risks, particularly in the form of privacy violations, cyberattacks, and network vulnerabilities, the technology itself may also be the cause of these issues. This is supported by the proactive risk management planning, robust security protocols, and the guarantee that 6G networks won't be violated.

The 6G concept is first explained in detail in the study in [15]. The operation of the proposed framework is verified at higher-order modulating plans to achieve higher spectrum efficiencies using performance indicators like error vector size, symbol constellations, and antenna array radiating beams. The performance findings strongly recommend using more data flows per user in order to achieve higher speeds that satisfy $6 \mathbf{G}$ wireless networks' requirements. They also recommend using a particular mMIMO antenna configuration based on the percentage of distinct data flows per user.

The survey article in [16] attempts to clarify the user-centric concept by thoroughly examining all of the different facets of 6G network architecture from a user-centric standpoint.

The study examines the promising features of 6G in [17], such as advanced sensing, accurate localization, and high-quality imaging. Machine learning (ML) and artificial intelligence (AI) will be extensively integrated into 6G technology, particularly in smart cities, where they will play a critical role in raising the standard of living for residents. 6G-enabled apps will support cutting-edge services that improve urban living experiences, tackle environmental issues, and offer more effective solutions across industries by integrating various components for monitoring, analysis, planning, and execution.

5. Conclusions

With much faster speeds, reduced latency, and increased capacity over 5G, 6G technology promises to revolutionize connectivity. Numerous new applications and use cases in a variety of industries, including manufacturing, entertainment, healthcare, and smart cities, will be made possible by this evolution. Although it is still in the early stages of development, 6G is anticipated to be commercially available by the early 2030s, with major improvements anticipated around 2028.

References

1. M.Z. Chowdhury, M. Shahjalal, S. Ahmed and Y.M. Jang, (2020) "6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions," in *IEEE Open Journal of the Communications Society*, vol. 1, pp. 957-975, DOI: https://doi.org/10.1109/OJCOMS.2020.3010270
2. R. Kunst, E. Pignaton, T. Zhou and H. Hu, S., (2020) "Application of future 6G technology to support heavy data traffic in highly mobile networks", *First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, Riyadh, Saudi Arabia, pp. 144-148, https://doi.org/10.1109/SMART-TECH49988.2020.00044
3. A. Vasuki and V. Ponnusamy, (2021) "Latest Wireless Technologies towards 6G," *International Conference on Computer Communication and Informatics (ICCCI)"*, Coimbatore, India, pp.1-4 https://doi.org/10.1109/ICCCI50826.2021.9457010
4. A. Patel, A. Shukla and J. Bhalani., (2021) "A Comprehensive Survey on 6G Networks: Key Technologies and Challenges", *International Conference on Simulation, Automation & Smart Manufacturing (SASM)*, Mathura, India, pp.1-6 https://doi.org/10.1109/SASM51857.2021.9841160
5. Z.A. Bhat, H. Mushtaq, J.A. Mantoo, V.S. Yadav, A.K. Shrivastava and S. Swati, (2021) "Beyond 5G: Reinventing Network Architecture With 6Ge," *2nd International Conference on Intelligent Engineering and Management (ICIEM)*, London, United Kingdom, pp. 316-321, DOI: https://doi.org/10.1109/ICIEM51511.2021.9445274
6. J. Kaur and M. A. Khan, (2022) "Sixth Generation (6G) Wireless Technology: An Overview, Vision, Challenges and Use Cases", *IEEE Region 10 Symposium (TENSYMP),* Mumbai, India, pp. 1-6, https://doi.org/10.1109/TENSYMP54529.2022.9864388
7. K.K. Vaigandla, (2022) "Communication Technologies and Challenges on 6G Networks for the Internet: Internet of Things (IoT) Based Analysis", *2nd International Conference on Innovative Practices in Technology and Management (ICIPTM),* Gautam Buddha Nagar, India, 2022, pp. 27-31 DOI: https://doi.org/10.1109/ICIPTM54933.2022.9753990
8. S. Aneesh and A.N. Shaikh, (2023) "A Survey for 6G Network: Requirements, Technologies and Research Areass," *2nd International Conference on Edge Computing and Applications (ICECAA),* Namakkal, India, pp. 166-171, DOI: https://doi.org/10.1109/ICECAA58104.2023.10212182
9. Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin and X. Li, (2023) "A Survey of Blockchain and Artificial Intelligence for 6G Wireless Communications" in IEEE *Communications Surveys & Tutorials,* vol. 25, no. 4, pp. 2494-2528, Fourth quarter. DOI: https://doi.org/10.1109/COMST.2023.3315374
10. C.-X. Wang et al., (2023) "On the Road to 6G: Visions, Requirements, Key Technologies, and Testbeds," *in IEEE Communications Surveys & Tutorials,* vol. 25, no. 2, pp. 905-974, Secondquarter, DOI: https://doi.org/10.1109/COMST.2023.3249835
11. M. Shafi, R.K. Jha and S. Jain (2024), "6G: Technology Evolution in Future Wireless Networks" *in IEEE Access*, vol. 12, pp. 57548-57573 DOI: https://doi.org/10.1109/ACCESS.2024.3385230
12. H. Pennanen, T. Hänninen, O. Tervo, A. Tölli and M. Latva-Aho, (2025) "6G: The Intelligent Network of Everything," *in IEEE Access*, vol. 13, pp. 1319-1421, DOI: https://doi.org/10.1109/ACCESS.2024.3521579
13. D. Akinwunmi, O. Uche, O. Shokunbi, H. Akinwumi, O. Awodele and C. Ajaegbu, (2024) "Navigating the Horizon Towards 6G Wireless Communication Networks," *IEEE SmartBlock4Africa,* Accra, Ghana, pp. 1-9, DOI: https://doi.org/10.1109/SmartBlock4Africa61928.2024.10779489
14. G.M. Valantina, P. Muneeshwari, D. Lakshmi, R. Suguna and H.A. Jabeen, (2024) "Unraveling the Potential of 6G Wireless Communication Systems in Next-Generation Networks," *International Conference on Recent Advances in Science and Engineering Technology (ICRASET),* B G Nagara,Mandya, India, pp. 1-5, DOI: https://doi.org/10.1109/ICRASET63057.2024.10895776
15. J. Alanya-Beltran, J. Silva-Cueva, L. Velarde-Vela, F. Cardenas-Palominio, F. Alvarez-Huertas and C. Poma-Garcia, (2024) "Sixth Generation (6G) Wireless Networks: Vision, Research, Challenges, and Solution," *7th International Conference on Contemporary Computing and Informatics (IC3I)*, Greater Noida, India, pp. 362-367, DOI: https://doi.org/10.1109/IC3I61595.2024.10829255

16. S.F. Drampalou, D. Uzunidis, A. Vetsos, N.I. Miridakis and P. Karkazis, (2024) "A User-Centric Perspective of 6G Networks: A Survey," *IEEE Access*, vol. 12, pp. 190255-190294, DOI: https://doi.org/10.1109/ACCESS.2024.3516194
17. B. Parmar, R.K. Chaurasiya and M. Choubey, (2025) "Review on 6G Wireless Communication," *IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS),* Bhopal, India, 2025, pp. 1-4, DOI: https://doi.org/10.1109/SCEECS64059.2025.10940493

ТЕХНОЛОГІЯ 6G: ЧАС НАСТАВ

Моханнад Фархан[1], викладач кафедри електротехніки, інженерний факультет;
e-mail: mhndfarhan@yahoo.com; ORCID: https://orcid.org/0009-0007-0541-6995
[1]*Багдадський університет, Ірак*

Рукопис надійшов 3 вересня 2025 р. Отримано після рецензування 3 жовтня 2025 р.
Прийнято 2 листопада 2025 р. Опубліковано 30.12.2025 р.

Анотація: Шосте покоління технології бездротового зв'язку, або технологія 6G, було створено для заміни 5G. Порівняно з попередниками, вона обіцяє набагато вищу швидкість, більшу ємність та зменшену затримку, відкриваючи нові можливості застосування та розвиваючи низку галузей. Терабіти на секунду (Тбіт/с) – це цільова швидкість передачі даних для 6G, яка значно вища за гігабіти на секунду (Гбіт/с) 5G. Для забезпечення роботи програм у режимі реального часу та миттєвої передачі даних, 6G прагне майже нульової затримки, можливо, навіть мікросекундного рівня. Порівняно з 1 мільйоном підключених пристроїв на квадратний кілометр 5G, 6G потенційно дозволить збільшити цей показник до 10 мільйонів. За допомогою штучного інтелекту та машинного навчання 6G зможе інтелектуально керувати ресурсами, працювати краще та додавати нові функції. Очікується, що 6G сприятиме розвитку в таких галузях, як візуалізація, визначення місцезнаходження, технології присутності та Інтернет речей (IoT). У цій статті представлено огляд попередніх робіт.

Ключові слова: *технологія 6G, архітектура, застосунки*

ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 2 (28)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 2 (28)

https://doi.org/10.26565/2519-2310-2025-2-04
УДК 004.056:004.7:004.89

АНАЛІЗ МЕТАДАНИХ ШИФРОВАНОГО ТРАФІКУ ДЛЯ УСУНЕННЯ «СЛІПИХ ЗОН» БЕЗПЕКИ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Максим Горелько[1], студент (бакалаврат, спеціальність F5), кафедра кібербезпеки інформаційних систем, мереж і технологій, e-mail: maksym.horelko@student.karazin.ua,
Сергій Малахов[1], к.т.н., ст. науковий співробітник, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, e-mail: malakhov@karazin.ua,
ORCID: https://orcid.org/0000-0001-8826-1616
[1]*Харківський національний університет імені В.Н. Каразіна, 61022, проспект Свободи, 4, Харків, Україна*

Рукопис надійшов 1 вересня 2025 р. Отримано після рецензування 1 жовтня 2025 р.
Прийнято 2 листопада 2025 р. Опубліковано 30.12.2025 р.

Анотація: Запропоновано огляд останніх напрацювань в межах проблематики комплексного аналізу зашифрованого мережевого трафіку в сучасних інформаційних системах. Основними методами досліджень є: - аналіз, узагальнення та порівняння. Розглянуті питання пошуку можливих шляхів забезпечення компромісу в умовному трикутнику «факторів впливу» при вирішенні завдань оперативного виявлення небезпек в структурі даних зашифрованого трафіку. В якості «факторів впливу» розглянута комбінація наступних чинників: - необхідність забезпечення потрібного рівня інформаційної безпеки (ІБ); - підтримка права користувачів на їх конфіденційність; - ресурсний консенсус впроваджуваних програмно-апаратних рішень. Звернено увагу, що інтеграція технологій штучного інтелекту і машинного навчання (AI/ML) до структури алгоритмів контролю трафіку, є ключовим важелем впливу на кінцевий результат. Підкреслено, що протидіюча сторона, також буде використовувати ці технології для маскування своєї діяльності. Зроблено висновок, що впровадження процедур аналізу метаданих мережевого трафіку, є компромісним рішенням. Реалізація такого підходу дозволяє покращити «прозорість» поточної мережевої активності для завчасного виявлення загроз безпеки, безпосередньо не вдаючись до процедур дешифрування трафіку. Акцентовано увагу, що впровадження парадигми «Cyber Deception» та комплексний аналіз метаданих циркулюючого шифрованого трафіку, є перспективним вектором зусиль для завчасного нівелювання фактору утворення «сліпих зон» безпеки сучасних IT систем.

Ключові слова: *трафік, фільтрація, відбитки трафіку, патерн, інформаційна безпека, VPN, Tor, Cyber Deception*

Як цитувати: Горелько М., Малахов С., Аналіз метаданих шифрованого трафіку для усунення «сліпих зон» безпеки сучасних інформаційних систем. *Комп'ютерні науки та кібербезпека*. 2025; № 2(28): С. 40–50. https://doi.org/10.26565/2519-2310-2025-2-04

In cites: Horelko M., Malakhov S. (2025). Metadata analysis of encrypted traffic to eliminate security «Blind Spots» of modern information systems. *Computer Science and Cybersecurity.* 2(28): 40–50. https://doi.org/ 10.26565/2519- 2310-2025-2-04 (in Ukrainian)

1. Вступ

В сучасному світі телекомунікацій, технології шифрування трафіку VPN та Tor [1-2], де-факто стали стандартом для захисту чутливих даних користувачів в корпоративному та приватному сегментах ринку інформаційних послуг. Однак, на шляху практичної імплементації відповідних рішень існують певні труднощі, що обумовлені «подвійною» природою процесу шифрування. Так, з одного боку, воно є необхідним для забезпечення конфіденційності і цілісності даних, де відмова від процедур шифрування трафіку або його «ослаблення» є неприйнятним (з різних причин). З іншої сторони, впровадження процедур шифрування створює «великий» бар'єр для традиційних систем моніторингу поточного стану інформаційної безпеки (ІБ), які покладаються на перевірку вмісту пакетів даних, що циркулюють в межах умовного периметру безпеки. Така інженерна дилема не є проблемою, яку можна «вирішити» в один крок – «раз і назавжди», що зумовлено неперервною ґенезою ІТ-технологій. Інакше кажучи, така суперпозиція умов роботи сучасних інформаційно-комунікаційних систем (ІКС), є новою реальністю, до якої системи безпеки повинні швидко адаптуватися.

Метою роботи є стислий огляд і узагальнення сучасного досвіду в галузі створення інтелектуальних систем реального часу для цілей аналізу метаданих шифрованого трафіку, що базуються на широкої імплементації можливостей технологій AI/ML.

Ключовими питаннями, що розглядаються є: - передумови утворення «сліпих зон» безпеки в структурі сучасних ІКС, котрі зумовлені присутністю (циркуляцією) шифрованого трафіку; - можливі напрями зусиль для вирішення завдань комплексного аналізу метаданих шифрованого трафіку з метою завчасного виявлення загроз безпеки, без виконання ресурсоємних (умовно «важких») процедур дешифрування.

2. Основна частина

2.1 Технологічний контекст й обмеження «традиційного» моніторингу та вплив новітніх стандартів шифрування

Розглянемо обидва підходи шифрування трафіку, VPN та Tor. Технологія VPN (Virtual Private Network) створює зашифрований «тунель» поверх публічної мережі і виступає, як умовний проксі-сервер, що приховує IP-адресу відправника даних та шифрує трафік [1]. Tor (*The Onion Router*) – це децентралізована мережа, що забезпечує анонімність користувача шляхом маршрутизації його трафіку через ланцюжок випадкових мережевих вузлів [2]. В цьому разі багатошарове шифрування гарантує, що кожен вузол знає лише попередній й наступний елементи ланцюжка, що робить відстеження вихідного джерела надзвичайно складним. Кіберзлочинці активно використовують обидві технології для приховування власної інфраструктури, управління ботнетами, проведення атак, поширення шкідливого програмного забезпечення (ПЗ) та непомітного витоку конфіденційних даних. При цьому традиційні системи безпеки, такі як системи виявлення вторгнень (IDS) чи глибокого аналізу пакетів (DPI), стають менш ефективні, оскільки не можуть аналізувати вміст зашифрованих пакетів.

Окремим викликом для сучасних систем моніторингу трафіку, став перехід мережі Інтернет на протокол TLS 1.3. В минулих версіях протоколу процедура «рукостискання» передавалася у відкритому вигляді, проте в TLS 1.3 шифрується вже більшість параметрів узгодження, включаючи серверний сертифікат. Це робить традиційні методи перевірки валідності сертифікатів без дешифрування (пасивний SSL/TLS аналіз) неможливими. Більш того, впровадження розширення ECH (*Encrypted Client Hello*) [3] закриває останню вразливість в приватності – поле SNI (Server Name Indication), яке раніше дозволяло ідентифікувати доменне ім'я цільового ресурсу. В умовах використання протоколу TLS 1.3 з ECH, пасивний

спостерігач «бачить» лише факт встановлення з'єднання з певною IP-адресою, але не може визначити конкретний сервіс чи хост. Саме це нівелює ефективність сигнатурних методів, таких як JA3/JA3S, змушуючи системи безпеки остаточно змістити фокус зі звичайного/традиційного аналізу заголовків на поведінковий аналіз часових рядів та статистичних характеристик потоку (*Deep Packet Dynamics*).

2.2 Методологія «Traffic Fingerprinting» та її особливості

Як було зазначено вище, в умовах, коли безпосередній аналіз вмісту є неможливий або обтяжливим (*перш за все, з точки зору балансу прикладених зусиль та отримуваного ефекту*), фокус зусиль поступово зміщується на процес аналізу метадані. Цей підхід базується на концепції т.з. «відбитків трафіку» (*Traffic Fingerprinting*), так як будь-яка діяльність в мережі практично завжди залишає унікальний та відтворювальний патерн відповідного мережевого трафіку, навіть якщо його вміст був зашифрован [4]. Ці патерни складаються з таких характеристик, як: - послідовність, розмір пакетів, часові інтервали між ними та напрямок передачі, періодичність й інтенсивність сеансів та ін. При цьому одним з найкращих векторів зусиль для класифікації є послідовність розмірів пакетів. Відомо, що різні програмні застосунки мають різні характерні патерни. Так наприклад, трафік VoIP (Voice over Internet Protocol) складається з великої кількості малих пакетів однакового розміру, що передаються через рівні проміжки часу. Веб-серфінг є асиметричним: - короткі запити від клієнта та значно більші відповіді від сервера. Водночас командно-керуючий (C&C) трафік ботнетів може проявлятися у вигляді дуже малих, періодичних «heartbeat» пакетів. Таким чином, всі ці патерни суттєво відрізняються, як від трафіку звичайного інтернет користувача, так і від передачі великих обсягів даних, що робить їх «помітними» для систем аналізу трафіку (звісно, в разі якщо це не є робота HoneyPot [5]). Часові характеристики трафіку, наприклад інтервали між послідовними пакетами (Inter-Arrival Times), надають цінну інформацію про «природу» даної комунікації. Цей вектор аналізу даних особливо ефективний для відокремлення антропогенної мережевої активності від трафіку породжуваного роботою автоматизованих процесів/систем. Класичним прикладом є аналіз трафіку сесії SSH (*Secure Shell*). Оскільки протокол SSH в інтерактивному режимі відправляє в окремому пакеті відомості про кожне натискання юзером умовних клавіш, то аналіз часових проміжків між цими пакетами дозволяє відтворити ритм набору символів, звичайно за умови якщо це не є наслідком навмисної роботи поведінкового аватару в рамках його сценарного полю [5]. На противагу цьому, технологічна C&C комунікація ботнету, часто відбувається через фіксовані, автоматично генеровані інтервали (тайм-слоти). Також, в межах дослідження «відбитків трафіку», використовується аналіз на рівні мережевих потоків (*Flows*) за допомогою протоколів NetFlow та IPFIX (*Internet Protocol Flow Information Export*) [6-7]. В цілому, ключові метадані Flows, що використовуються для аналізу «відбитків», включають:

- Ідентифікатори потоку: IP-адреси, порти джерела й призначення, протокол (TCP/UDP). Хоча мережі VPN та Tor маскують реальну IP-адресу, ця інформація залишається корисною для аналізу внутрішніх патернів та зв'язків з відомими «шкідливими» серверами;
- Статистика потоку: Тривалість сесії, загальна кількість переданих пакетів та байтів в обох напрямах (як є, тобто без урахування впливу поведінкових аватарів);
- Метадані TLS Handshake: Цінність аналізу TLS-рукостискання полягає в тому, що ще до початку будь-якого шифрування, можливо ідентифікувати ПЗ, що «виходить» в мережу. Те, як програма пропонує шифрувати дані, зумовлює її унікальний «відбиток» (JA3 FingerPrinting). Це дозволяє системам ІБ відрізнити, наприклад легітимний браузер від відомої сигнатури вірусу і заблокувати загрозу ще на етапі підключення [8].

- Сертифікати: Аналіз SSL/TLS сертифікатів (навіть без дешифрування) полягає у швидкій перевірці легітимності сервера. Зловмисники часто економлять на належній інфраструктурі чи цілісності заходів, тому використання ними підозрілих сертифікатів є поширеною практикою. В цьому разі, коли система ІБ «бачить» самопідписаний сертифікат, сертифікат від невідомого центру або з нештатними параметрами (наприклад, невідповідність домену) - це може свідчити, що сервер, ймовірно, є частиною шкідливої інфраструктури, наприклад, фішинговим сайтом, сервером управління ботнетом тощо [9].

2.3 Специфіка аналізу «анонімізуючих» мереж (на прикладі Tor)

Практичні підходи до аналізу трафіку Tor включають заходи на основі парсінгу т.з. «відбитків веб-сайтів» (*Website Fingerprinting, WF*). Відповідні зусилля полягають в спробі ідентифікації відвідуваних сайтів через унікальні патерни розмірів та часу пакетів. Так наприклад, автори роботи [10] свідчать, що хоча в контрольованих «лабораторних» умовах точність висока (95% для 5 сайтів), у реальних сценаріях подій вона стрімко падає (*до 60% при 100 сайтах*). Більш практичний підхід передбачає «онлайн навчання» з використанням справжнього трафіку. У цій парадигмі дій, зловмисник може збирати репрезентативні дані для навчання власної інфраструктури, наприклад, керуючи власним вихідним вузлом (*Exit Relay*) у легітимній мережі «Tor». Це потенційно дозволяє йому отримувати частину справжніх даних з DNS-запитів [11] до моменту встановлення TLS-з'єднання, і постійно оновлювати модель, враховуючи реальну поведінку легітимних користувачів. Проте даний шлях має суттєвий недолік: - результати WF аналізу суттєво залежать від масштабу здійснюваного моніторингу.

Узагальнюючи результати дослідження [12] можна констатувати, що більшою загрозою для Tor є атаки на основі кореляції потоків – «*Stream Correlation Attacks»*. В межах цієї концепції подій, зловмисник, що спостерігає за Tor-трафіком на вході (*R1*) та виході (*R3*) ланцюга, може зіставити відповідні потоки (*див. Рис.1*).

$$Alice \xrightarrow{[M]_{K_{3,2,1}}} R_1 \xrightarrow{[M]_{K_{3,2}}} R_2 \xrightarrow{[M]_{K_3}} R_3 \xrightarrow{M} Bob$$

Рис. 1 – Умовний ланцюг TOR
Fig. 1 – Tor circuit [12]

В цьому разі, атака покладається не на вміст, а на аналіз патернів часу, що зумовлено тим що мережа «Tor» використовує комірки фіксованого розміру в 512 байт (*див. Рис.2*) [12].

В межах цієї концепції, атакуючий може приховано (сніфити) порівнювати затримки між різними комірками «Tor» або штучно створювати часові ряди (задаючи кількість комірок у N-секундному вікні) та, потім, статистично порівнювати параметри векторів R1 та R3 (рис. 1).

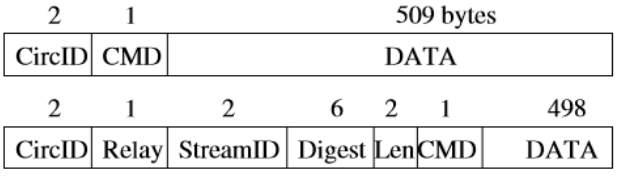

Рис. 2 – Структура комірки TOR
Fig. 2 – Tor cell structure

Відомі і активні атаки: - зловмисник на R1 навмисно вносить зміни в потік (затримка або відкидання комірок), таким чином створюючи власний «водяний знак», який можна ідентифікувати на R3. Такі атаки можуть досягати 99% точності [12]).

2.4 Ідентифікація та аналіз VPN-тунелів

Поряд з цим, VPN трафік, також, має певні вразливості. Оскільки VPN-протоколи, на відміну від Tor, не стандартизують розміри пакетів, вони є потенційно більш вразливими до аналізу. Автори дослідження [13] продемонстрували можливість ідентифікації сеансів OpenVPN з 85% ефективністю. Архітектура відповідної системи (див. Рис.3) передбачає двоетапний підхід. Спочатку мережевий трафік (1) перенаправлявся на відповідний «фільтр» (2), котрий резидентно аналізував весь обсяг даних (зі швидкістю близько 20 Гбіт/с), виявляючи IP-адреси, які поводилися, як VPN-сервери (точка 3, на рис. 3). На 2-му етапі всі «підозрілі» адреси (4) передавалися відповідним «тестувачам» для їх активної перевірки (точка 5 «Пробери»). Якщо за результатами перевірки, сервер підтверджував, що він є OpenVPN, то його додавали до бази даних (6) для подальшого аналізу.

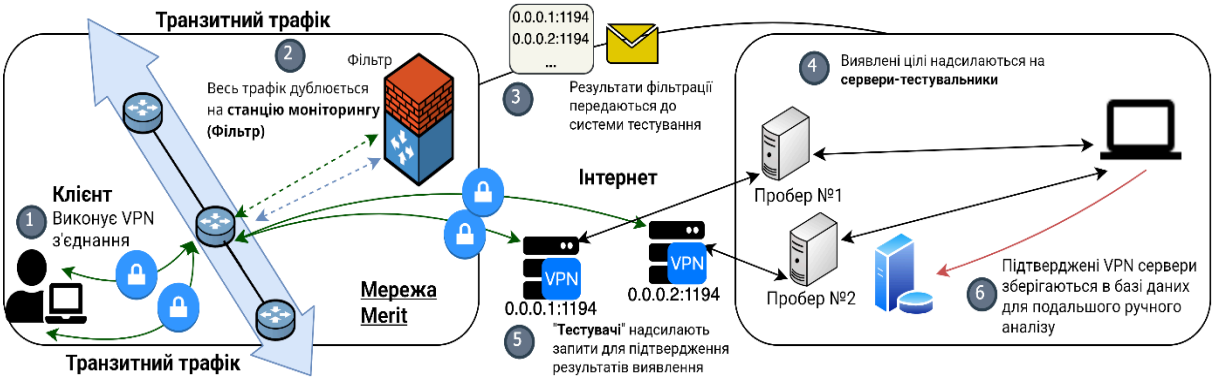

Рис. 3 – Спрощена архітектура системи пасивного моніторингу трафіку для ідентифікації роботи VPN-серверів

Fig. 3 – Simplified architecture of a passive traffic monitoring system for identifying the operation of VPN servers [13]

В цілому, запропонований авторами роботи [14], алгоритм ідентифікації роботи OpenVPN, базується на трьох характеристиках:

По-перше: - аналіз послідовності «*opcode*» (тобто, кодів операцій) у незашифрованих заголовках пакетів «*каналу управління*» під час процедури *TLS Handshake* (*див. Рис.4*) [13];

По-друге: - аналіз «унікальних» розмірів IP пакетів. Інфографіка на Рис.5 свідчить про те, що OpenVPN (*світло-сині стовпці*) демонструє надзвичайно високі «сплески» для певних довжин пакетів-відповідей (*Probe Length*), особливо в діапазоні 1400-1600 байт, на відміну від випадкового трафіку (*стовпці помаранчевого кольору*). Пунктирна темно-синя зростаюча крива (*легенда - OpenVPN CDF, де CDF (Cumulative Distribution Function) - Інтегральна функція розподілу*) стрімко зростає в цих точках, підтверджуючи, що більшість серверів системи OpenVPN відповідають пакетами передбачуваного розміру;

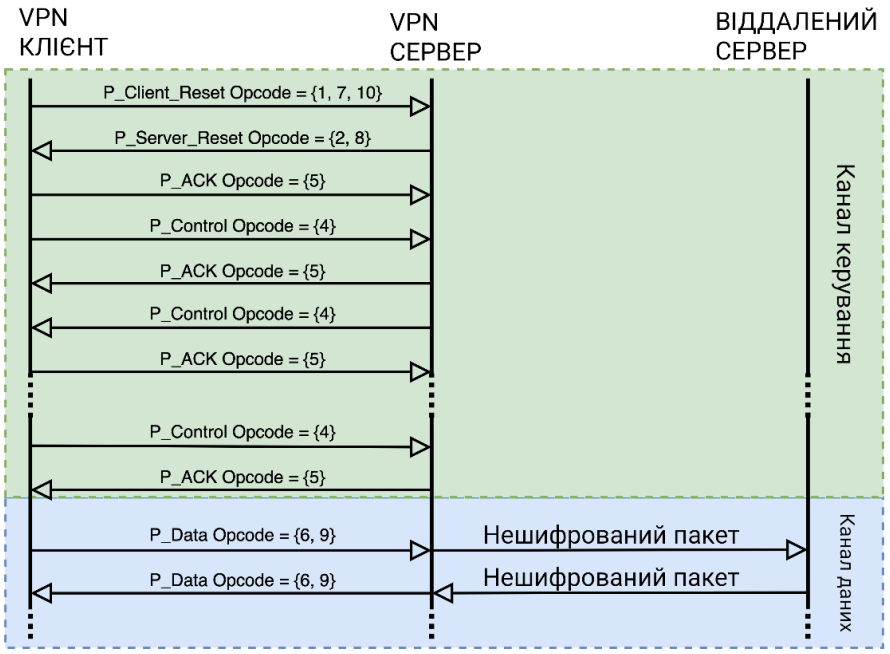

Рис. 4 – Послідовність обміну пакетами та їх «opcode» під час встановлення з'єднання OpenVPN
Fig. 4 – Packet exchange sequence and opcodes during OpenVPN connection establishment [13]

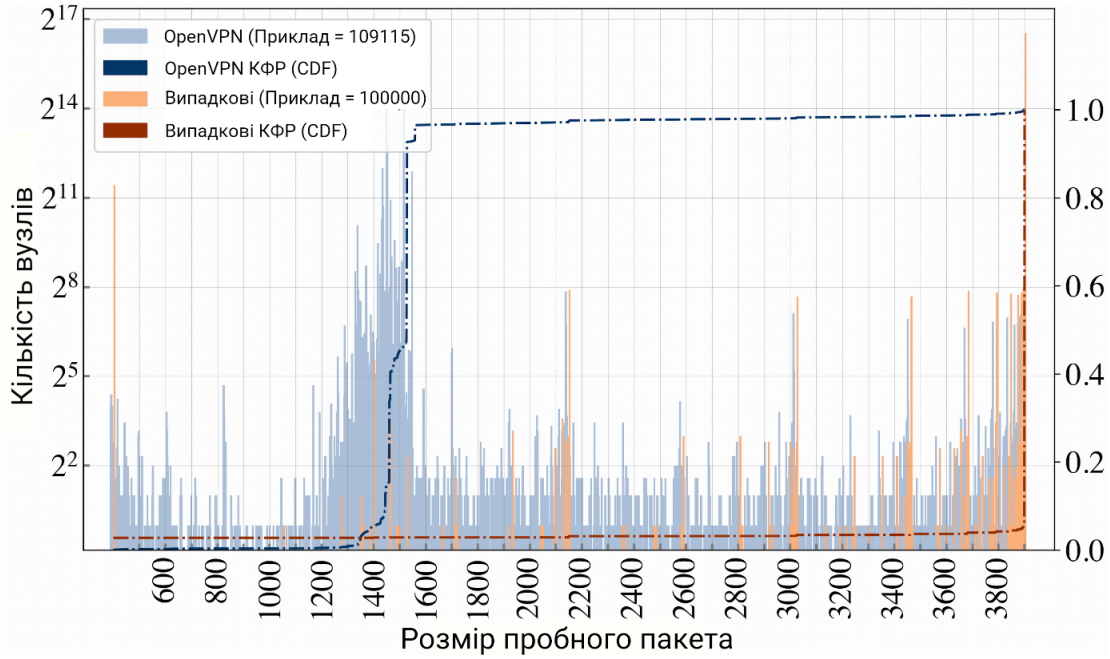

Рис. 5 - Розподіл довжин пакетів-відповідей для серверів OpenVPN, порівняно з іншими випадковими серверами *(згідно з даними [13])*
Fig. 5 - Distribution of response packet lengths for OpenVPN servers, compared to random servers [13]

По-третє: – проведення процедур активної перевірки (див. точка 5 - «*Пробери*», на рис.

3). «Тестувач» надсилає спеціальний запит, на який «справжній» сервер OpenVPN, відповідає характерним RST-пакетом. Однак цей метод має обмеження: - він не працює, якщо на сервері ввімкнено режим «*TLS-Auth*». Як показано на блок-схемі на Рис. 6, пакет тестувача не пройде перевірку «*Valid HMAC?*» та буде відкинутий/ідентифіковано, як «*Invalid HMAC*» (червона стрілка на рис.6) ще до того, як цільовий сервер згенерує відповідь.

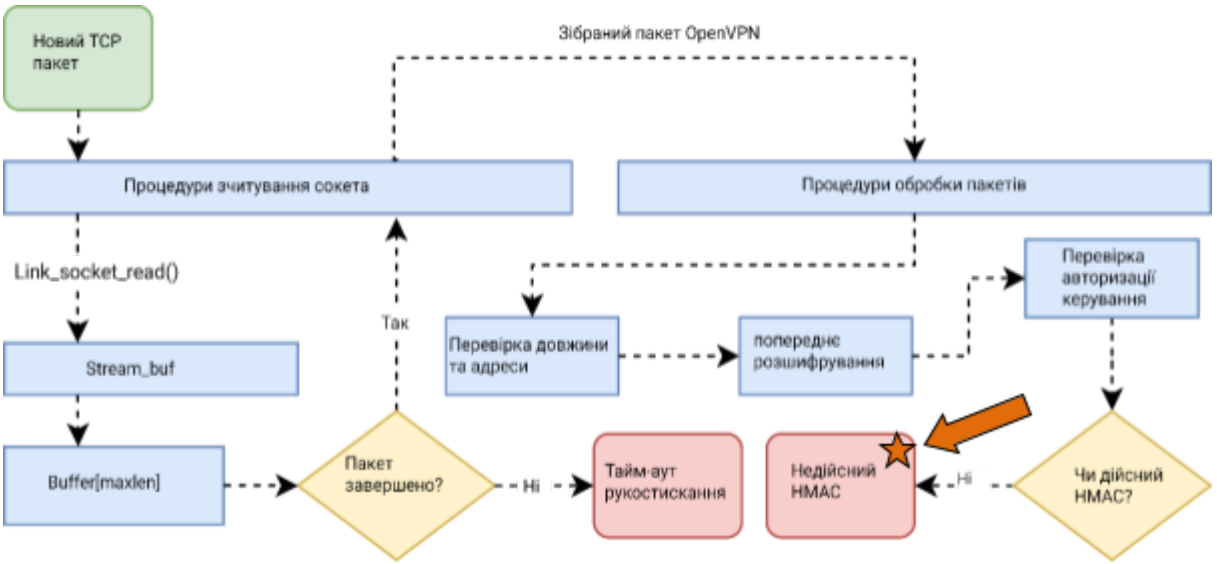

Рис. 6 – Внутрішня логіка обробки пакетів і валідації HMAC сервером OpenVPN [13]
Fig. 6 – Internal logic of packet processing and HMAC validation by the OpenVPN server [13]

Автори дослідження [14] проаналізували вплив «фонового» трафіку всередині VPN, як протидію WF-атакам. Отримані ними результати свідчать, що фоновий трафік дійсно знижує точність (з 95% до 70%). Однак, якщо атакуюча модель попередньо не навчалася на трафіку з «шумом», а потім має справу з ним, то її точність роботи значно погіршується (до 5-30%). При цьому, попередньо навчена система (наприклад, на трафіку Netflix), може «успішно» атакувати користувачів YouTube, підтверджуючи те, що фоновий трафік ускладнює, але не зупиняє атаки.

Виявлення зловмисної активності в зашифрованому трафіку, особливо роботи ботнетів у Tor, є найскладнішим завданням [12]. Зловмисники активно використовують мережу Tor для анонімізації активності C&C серверів, перетворюючи їх на приховані сервіси (.onion).

Концептуально, мережа Tor від самого початку була розроблена, щоб зробити її трафік невизначеним: - IP-адреси анонімні; - порти й протоколи уніфіковані (*все виглядає як звичайний HTTPS*); - вміст зашифрований; - пакети мають фіксований розмір 512 байт (*див. Рис.2*). Однак, незважаючи на це, автори роботи [3] вказують на те, що використання Tor може створювати помітні аномалії. Так, наприклад, сам факт завантаження клієнта Tor на комп'ютер потенційної жертви, опосередковано вже є передумовою, щоб ідентифікувати цей процес, як «підозріла дія». Централізований C&C сервер, навіть гарно прихований, збирає трафік від власної системи ботів, створюючи відповідну мережеву аномалію. В цьому сенсі, відомий приклад ботнету «*Mevade*» показав [15], що одночасне та масове приєднання мільйонів нових клієнтів до мережі «Tor», є сигналом загрози, яка потребує серйозної уваги (*можлива і навмисна імітація*).

Враховуючи все вище зазначене, цілком логічно очікувати, що нові підходи до виявлення зловмисної активності в мережі Tor [16], поступово зміщують увагу з питань контролю вмісту трафіку, на аналіз його поведінкових характеристик та властивостей. Вочевидь, що оскільки IP-адреси, порти та розміри пакетів даних уніфіковані, то очевидними

ознаками для аналізу є: - час (в т.ч., періодичність) та кількість комірок даних, що циркулюють в мережі. Більшість відомих ботнетів для забезпечення власної функціональності, використовують періодичний зв'язок «*heartbeat*». Ця поведінка характерна і для Tor. Хоча періодичність технологічних сеансів зв’язку притаманна і легітимним додаткам (наприклад, IRC), однак їх характеристики відрізняються.

Приклади досліджень реально діючих ботнетів (Win32/Atrax, [17]), підтверджують, що мережа Tor, хоч і приховує місцезнаходження власного «C&C», але при цьому, ніяк не приховує факт його періодичної активності (*збір телеметрії та видача команд управління*). Доречі, дослідники компанії ESETâ змогли ідентифікувати внутрішню .onion адресу ботнету «*Atrax*» [18] та проаналізувати протокол його взаємодії, який виявився звичайними HTTP-запитами. При цьому, хоча локалізувати фізичне місцезнаходження «C&C» ботнетів вкрай важко, проте відомі інструменти й технології аналізу поведінки і протоколів, залишаються актуальними для виявлення такого роду загроз.

3. Застосування методів ML для класифікації зашифрованого трафіку

Розвиток криптографічних протоколів створює умовний бар'єр для традиційних систем моніторингу. Одним із ефективних підходів є використання ансамблевих методів на основі дерев рішень, зокрема алгоритму «Random Forest». Так, згідно дослідження [19], «*TorBot Stalker*» показав себе як дуже результативний інструмент, що здатен легко деанонімізувати ботнети в мережі Tor. Специфіка трафіку Tor вимагає аналізу часових рядів та кількості комірок. *Random Forest* здатний класифікувати таку активність з точністю 99% [19], успішно відокремлюючи трафік ботнетів від легітимних додатків (*наприклад, IRC або Web*) навіть в умовах зашумлених каналів зв'язку (як вже говорилося, зашумлений канал не дуже сильно ускладнює деанонімізацію [12]).

Схема на Рис.7 демонструє етапи обробки даних [19]: - від перехоплення «сирих» комірок до етапу збору та групування за кількістю. Ключовим елементом є «Видобувач інтервалів», який виокремлює регулярні часові шаблони перед передачею їх на вхід «Класифікатора додатків» для верифікації трафіку.

Ключовими ознаками для цього алгоритму виступають інтервали між прибуттям пакетів (*Inter-Arrival Times*) та унікальні підрахунки комірок, що дозволяє ідентифікувати періодичні патерни зв'язку «C&C» серверів. Порівняльний аналіз показав перевагу Random Forest над алгоритмом J48 (C4.5 алгоритм) [20], забезпечуючи нижчий рівень помилкових спрацьовувань. Поряд з цим, для задач виявлення аномалій у шифрованому трафіку високу ефективність демонструє алгоритм XGBoost (*Extreme Gradient Boosting*) [21].

Недоліком ML-моделей залишається проблема існування т.з. «чорного ящика». Для вирішення цих труднощів можна використовувати алгоритми з методами *Explainable AI* (XAI), зокрема SHAP (*SHapley Additive exPlanations*) [22]. Використання SHAP дозволяє розкрити внутрішню логіку моделі, визначаючи вклад кожної ознаки у фінальне рішення блокування.

Впливовими ознаками є загальна кількість переданих пакетів, порт отримувача та початковий розмір вікна (від ініціатора з'єднання до отримувача). Такий підхід робить алгоритм зрозумілим і прозорим, де аналітик SOC (*Security Operations Center*) може бачити конкретні причини класифікації трафіку.

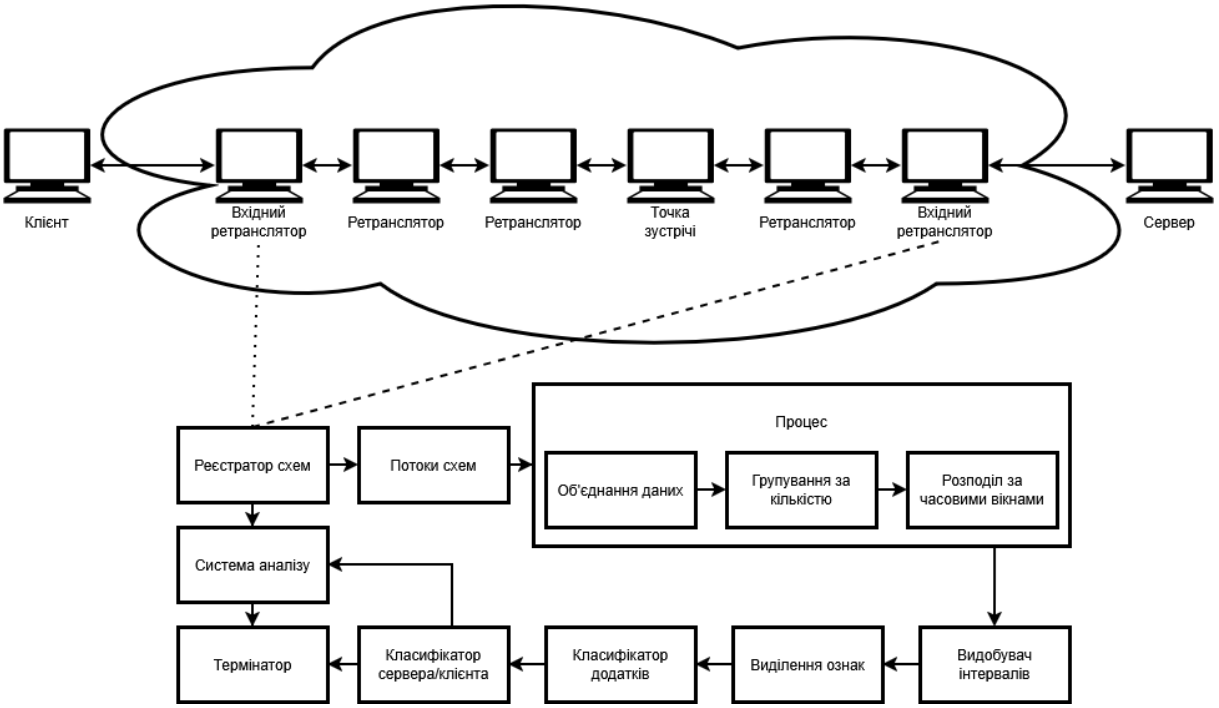

Рис. 7 – Схема роботи TorBot Stalker
Fig. 7 – TorBot Stalker operation scheme [19]

4. Висновки

1. Огляд відомих інцидентів ІБ та останніх напрацювань в галузі активної протидії складним – інтегрованим загрозам ІБ, дозволяє окреслити та конкретизувати можливі підходи до вирішення проблематики існування т.з. «сліпих зон» ІБ. В певному сенсі, процедури шифрування даних (трафіку) формують нову – «мережеву реальність», котра породжує формування відповідних «зон». Як наслідок - діючи системи ІБ вимушені швидко адаптуватися, змінюючи традиційні методики й засоби протидії новим викликам.

2. Аналіз метаданих трафіку є компромісним рішенням, що дозволяє покращити «прозорість» мережевої активності для завчасного виявлення загроз, не вдаючись до процедур дешифрування. Ключова перевага – збереження конфіденційності, оскільки аналізуються лише характеристики процесу передачі (сеансів/сесій), а не вміст пакетів трафіку. На відміну від ресурсномісткого дешифрування (*SSL/TLS*), аналіз метаданих є більш реалістичним сценарієм дій, що забезпечує високу масштабованість (*перш за все за рахунок віртуалізації процесів обробки та організації спеціалізованих хмарних систем*) відповідних реалізацій (рис. 3).

3. Узагальнення результатів сучасних досліджень [10, 12-14, 16, 19, 22] декількох незалежних груп фахівців з ІБ, дозволяє стверджувати, що перспективним напрямом зусиль є синтез інтегрованих систем, що здатні в реальному часі аналізувати метадані зашифрованого трафіку за допомогою широкої імплементації AI/ML. Такі функціональні платформи реалізують проактивний підхід (*Threat Hunting*). Вони базуються на зборі спеціалізованих метаданих (*IPFIX/NetFlow, JA3, дані сертифікатів*), що складає субстантивний фундамент аудиту аномальної мережевої активності. Т.ч. забезпечується еволюційний перехід від реактивної моделі ІБ до концепції проактивного захисту, що базується на розподіленому пошуку та систематизації опосередкованих індикативних ознак існування різного типу загроз.

4. Традиційні методи, що засновані на DPI, поступово втрачають ефективність. Натомість впровадження парадигми технології *Cyber Deception* та комплексний аналіз метаданих циркулюючого трафіку (*інтервалів та розмірів пакетів*) є найбільш перспективним вектором зусиль для цілей детектування і класифікації зашифрованого трафіку [13,19]. Таке поєднання в змозі забезпечити оперативне сепарування застосунків та виявлення непрямих ознак деструктивної дії ботнетів, навіть при роботі на вузлових мережевих шлюзах при гігабітних швидкостях транзитного трафіку (приклад, як в разі «*Merit Network*» на рис.3).

5. За сукупністю отримуваних властивостей зазначена вище стратегія дій, бачиться як практично можливий шлях для підтримки (принаймні на близьку перспективу) бажаного компромісу між: - необхідністю забезпечення потрібного рівня безпеки; - правом користувачів на їх конфіденційність; - можливостями ресурсної підтримки впроваджуваних програмно-апаратних реалізацій. На цьому шляху, глибока інтеграція технологій AI/ML є ключовим фактором впливу на кінцевий результат, оскільки зловмисники, у свою чергу, також будуть використовувати ці технології для маскування своєї діяльності.

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

References

1. Cloudflare. *What is a VPN?* https://www.cloudflare.com/ru-ru/learning/access-management/whatisavpn/
2. Tor Project. *Tor: Overview* https://2019.www.torproject.org/about/overview.html.en
3. Cloudflare. *ECH Protocol* https://developers.cloudflare.com/ssl/edge-certificates/ech/
4. Multilogin. *What is Traffic Fingerprinting?* https://surl.lt/empsdf
5. Kokhanovska, T., Narezhnyi, O., & Diachenko, O. (2020). Exploring the possibilities of Honeypot technology. *Computer Science and Cybersecurity, 1(17)*, 33-42. https://doi.org/10.26565/2519-2310-2020-1-03 [in Ukrainian]
6. Softpiua. *What is NetFlow?* https://surl.li/dqzslu [in Ukrainian]
7. Pitutin V. Softpiua. *What is IP Flow Information Export?* https://surl.lu/cwmkud [in Ukrainian]
8. Peakhour. *What is JA3 Fingerprinting?* https://www.peakhour.io/learning/fingerprinting/what-is-ja3-fingerprinting/
9. Cloudflare. *What is an SSL certificate?* https://www.cloudflare.com/ru-ru/learning/ssl/what-is-an-ssl-certificate/
10. Cherubin, G., Jansen, R., & Troncoso, C. (2022, August 10-12). *Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World* https://www.usenix.org/system/files/sec22-cherubin.pdf
11. Chepel, D., & Malakhov, S. (2024). Summary of DNS traffic filtering trends as a component of modern information systems security. *Computer Science and Cybersecurity, 1(25)*, 6–21. https://doi.org/10.26565/2519-2310-2024-1-01 [in Ukrainian]
12. DeFabbia-Kane, S. (2011, April). *Analyzing the Effectiveness of Passive Correlation Attacks on the Tor Anonymity Network* https://surl.li/zghbyu
13. Xue, D., Ramesh, R., Jain, A., Kallitsis, M., Halderman, J. A., Crandall, J. R., & Ensafi, R. (2024, March 6). *OpenVPN is Open to VPN Fingerprinting* https://arxiv.org/html/2403.03998v1
14. DeFabbia-Kane, S. (2023, June 15). *The Effect Background Traffic in VPNs has on Website Fingerprinting* https://www.diva-portal.org/smash/get/diva2:1779408/FULLTEXT01.pdf
15. Tor Project. *Tor metrics. Directly connecting users* https://metrics.torproject.org/userstats-relay-country.png?start=2013-06-05&end=2013-11-02&country=all&events=off
16. Fajana, O. (2023, October). *Novel Techniques for Detecting Tor Botnets* https://pure.port.ac.uk/ws/portalfiles/portal/91457639/up797388-Oluwatobi-Fajana-Thesis-2023-final.pdf

17. Stormshield Customer Security Lab. (2014, August 20). *Win32/Atrax.A* https://www.stormshield.com/news/win32atrax-a/
18. Matrosov, A. (2013, July 24). *The rise of TOR-based botnets* https://www.welivesecurity.com/2013/07/24/the-rise-of-tor-based-botnets/
19. Fajana, O., Owenson, G., & Cocea, M. *TorBot Stalker: Detecting Tor Botnets through Intelligent Circuit Data Analysis* https://pure.port.ac.uk/ws/portalfiles/portal/12745078/TorBot_Stalker_new.pdf
20. Khanna, N. (2021, August 18). *J48 Classification (C4.5 Algorithm) in a Nutshell* https://medium.com/@nilimakhanna1/j48-classification-c4-5-algorithm-in-a-nutshell-24c50d20658e
21. Pawan Saxena. GeeksforGeeks. (2025, October 24). *XGBoost* https://www.geeksforgeeks.org/machine-learning/xgboost/
22. Sing, K., Kashyap, A., & Cherukuri, A. K. (2025, May). *Interpretable Anomaly Detection in Encrypted Traffic Using SHAP with Machine Learning Models* https://surl.lt/oidsuz

METADATA ANALYSIS OF ENCRYPTED TRAFFIC TO ELIMINATE SECURITY «BLIND SPOTS» OF MODERN INFORMATION SYSTEMS

Maksym Horelko[1], Student (Bachelor's degree, specialty F5) at the Department of Cybersecurity of Information Systems, Networks and Technologies; E-mail: maksym.horelko@student.karazin.ua;
Serhii Malakhov[1], Ph.D., Senior Researcher, Associate Professor of the Department of Cybersecurity of Information Systems, Networks and Technologies; e-mail: malakhov@karazin.ua; ORCID: https://orcid.org/0000-0001-8826-1616
[1]*V. N. Karazin Kharkiv National University, Ukraine*
Manuscript was received September 1, 2025; Received after review October 1, 2025;
Accepted November 2, 2025; Published December 30, 2025

Abstract. A review of recent developments is offered on the issues in the complex analysis of encrypted network traffic in modern information systems. The main research methods are: - analysis, generalization and comparison. The paper considers the issue of finding possible ways to ensure a compromise in the conditional triangle of «influence factors» when solving the tasks of operational detection of dangers in the data structure of encrypted traffic. As «influence factors» a combination of the following factors is considered: - the need to ensure the required level of Information Security (IS); - support for the right of users to their confidentiality; - resource consensus of the implemented software and hardware solutions. Attention is drawn to the fact that the integration of artificial intelligence and machine learning (AI/ML) technologies into the structure of network traffic control algorithms is a key lever for influencing the final result. It is emphasized that the opposing party will also use these technologies to mask its activities. It is concluded that the implementation of procedures for analyzing network traffic metadata is a compromise solution. The implementation of such an approach allows to improve the «transparency» of current network activity for early detection of security threats, without directly resorting to traffic decryption procedures. It is emphasized that the implementation of the «Cyber Deception» paradigm and a comprehensive analysis of the metadata of circulating encrypted traffic are a promising vector of efforts for preventive elimination of the prerequisites of the formation of "blind spots" in the security of modern IT systems.

Keywords: *traffic, Filtering, Traffic Fingerprinting, Pattern, Information Security (IS), VPN, Tor, Cyber Deception*

Conflicts of Interest: the authors declare no conflict of interest.

ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 2 (28)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 2 (28)

https://doi.org/10.26565/2519-2310-2025-2-05
УДК 004.415.2:519.876:656.2

РОЗРОБКА ТА ПРОГРАМНА ІМПЛЕМЕНТАЦІЯ МОДЕЛІ МАРШРУТИЗАЦІЇ НА ЗАЛІЗНИЦІ

Артем Панченко[1], доктор філософії зі спеціальності комп'ютерні науки, доцент кафедри теоретичної і прикладної інформатики, e-mail: artem.panchenko@ karazin.ua,
ORCID: https://orcid.org/0000-0001-5865-6158,
Ірина Зарецька[1], доктор філософії зі спеціальності математика, доцент кафедри теоретичної і прикладної інформатики, e-mail: zaretskaya@ karazin.ua,
ORCID: https://orcid.org/0000-0001-8747-2737
Марина Владимирова[1], кандидат економічних наук за спеціальністю «Математичні методи в економіці», доцент кафедри теоретичної і прикладної інформатики,
e-mail: vladymyrova@karazin.ua, ORCID: https://orcid.org/0009-0000-9868-2617
Аліна Білецька[1], магістр, кафедра теоретичної і прикладної інформатики,
e-mail: aleesha.biletska@gmail.com,
[1]*Харківський національний університет імені В.Н. Каразіна,*
61022, проспект Свободи, 4, Харків, Україна

Рукопис надійшов 1 жовтня 2025 р. Отримано після рецензування 2 листопада 2025 р.
Прийнято 2 грудня 2025 р. Опубліковано 30.12.2025 р.

Анотація: У сучасних умовах функціонування АТ «Укрзалізниця» ключову роль у забезпеченні економічної ефективності вантажних перевезень відіграє стратегія маршрутизації та вибір маршруту відправлення. Наразі маршрут здебільшого обирається за принципом найкоротшого шляху, що забезпечує мінімальні витрати палива на перевезення, а також зменшує амортизацію тягових потужностей та іншого рухомого складу підприємства. Відповідно, замовник перевезення сплачує мінімально можливу вартість доставки вантажу. Однак такі маршрути формуються на визначений період і не передбачають динамічної зміни, що спричиняє низку проблем, зокрема неврахування під час перевезення поточного технічного стану рухомого складу на окремих дільницях та рівня їх завантаженості. Особливо гостро ці проблеми проявилися внаслідок повномасштабного вторгнення Російської Федерації в Україну, яке призвело до руйнування частини залізничної інфраструктури, зокрема колій і мостів, а також до пошкодження або повного виведення з експлуатації частини тягового рухомого складу АТ «Укрзалізниця» та інших операторів залізничних перевезень. Водночас альтернативні підходи до маршрутизації наразі розглядаються обмежено через недостатню кількість досліджень, присвячених стратегічному управлінню процесами перевезень. У роботі описано процес розроблення та імплементації програмної моделі функціонування залізничної системи, основною метою якої є забезпечення можливості проведення експериментальних досліджень різних гіпотез щодо альтернативних підходів до маршрутизації. Це дозволяє розв'язати науково-прикладну задачу оптимізації вантажних залізничних перевезень шляхом формування гнучких стратегій управління. Дослідження базується на синтезі теорії графів (представлення мережі у вигляді зваженого мультиорієнтованого графа), дискретно-подієвого моделювання (DES) для аналізу динаміки процесів та змішаного цілочислового лінійного програмування

(MILP) для формування еталонних показників (бенчмаркінгу). Імплементовано гібридну політику готовності (Threshold Policy), що базується на параметрах мінімального наповнення поїзда та граничного часу очікування і забезпечує баланс між пропускною здатністю вузлів та термінами доставки. Розроблено спеціалізований програмний полігон мовою Python, який інтегрує життєвий цикл подій (Spawn, Form, Depart, Arrive) та дає змогу тестувати інтелектуальні стратегії управління в імітаційному середовищі. Практичне значення дослідження полягає у можливості використання розробленого інструментарію для кількісної оцінки ефективності різних стратегій маршрутизації та формування поїздів на сортувальних станціях. Створений програмний комплекс є фундаментальною основою для подальших досліджень авторів, спрямованих на мінімізацію середнього часу обороту рухомого складу та вузлових простоїв відправлень у реальних логістичних системах, що сприятиме підвищенню економічної ефективності вантажних перевезень.

Ключові слова: *математичне моделювання, лінійне програмування, дискретно – подієве моделювання, імплементація математичних моделей, ефективність перевезень*

Як цитувати: Панченко А., Зарецька І., Владимирова М., Білецька А., (2025) Розробка та програмна імплементація моделі маршрутизації на залізниці. *Комп’ютерні науки та кібербезпека*. 2025; № 2(28): С. 51–68. https://doi.org/10.26565/2519-2310-2025-2-05

In cites: Panchenko A., Zaretska I., Vladimirova M., Biletska A. (2025). Development and software implementation of a railway routing model. *Computer Science and Cybersecurity.* 2(28): 51–68. https://doi.org/10.26565/2519- 2310-2025-2-05 (in Ukrainian)

1. Вступ

Вантажні залізничні перевезення відіграють ключову роль у забезпеченні економічної стабільності України, зокрема в умовах глобальної реорганізації логістичних потоків та інтеграції з європейськими транспортними коридорами. З огляду на масштаби мережі та обсяг перевезень, ефективна маршрутизація вантажних поїздів є важливим елементом логістичного управління, що впливає на транспортні витрати, час доставки і загальну пропускну спроможність залізничної інфраструктури.

Процес визначення маршруту вантажного перевезення передбачає формування послідовності руху поїзда від станції відправлення до станції призначення з урахуванням технічних, експлуатаційних та організаційних обмежень. В умовах поточного стану транспортної системи України, зокрема наслідків бойових дій, які призвели до часткового руйнування інфраструктури, питання оптимальної маршрутизації набувають додаткової складності. На практиці Укрзалізниця застосовує стандартизовані процедурні правила, що не завжди сприяють досягненню оптимального логістичного рішення.

АТ «Укрзалізниця» розробила Правила перевезення вантажів, що визначають порядок організації перевезень, включно з формуванням маршрутів та оформленням документів. Ці правила встановлюють терміни подачі, порядок формування вагонів у маршрутні поїзди та загальні процедури планування перевезень, але не містять формальних критеріїв математичної оптимізації маршруту як такого. Зокрема, розділи Правил перевезення вантажів описують процедури планування перевезень, приймання та оформлення вантажів до перевезення, а також технологічні аспекти формування поїздів на станціях відправлення. У межах цієї нормативної бази також затверджено «Перелік умов щодо організації перевезень вантажів маршрутами», який деталізує технічні вимоги формування маршрутних поїздів та їх масу, довжину і

процедуру узгодження з регіональними філіями. Це важливий офіційний документ, який формує основу для операційної реалізації маршрутизації в Укрзалізниці [1].

У практиці АТ «Укрзалізниця» маршрут вантажного перевезення визначається не складними алгоритмами оптимізації, а через процедури та нормативні умови формування маршрутних поїздів, закріплені у «Переліку умов щодо організації перевезень вантажів маршрутами», затвердженому правлінням компанії. Згідно з цим документом:

1. Формування маршрутного поїзда здійснюється на під'їзних коліях або коліях станції відправлення за наявності відповідного колійного розвитку відправника.
2. Якщо відправник не має достатнього колійного розвитку для збору вагонів у поїзд, але обсяги вантажу дозволяють сформувати маршрутний поїзд у межах технологічного часу (зазвичай до 24 годин), то це узгоджується між регіональною філією та відправником.
3. В договорах про експлуатацію під'їзних колій і перевезення зазначаються параметри маршруту: норми маси та довжини поїзда, порядок подачі вагонів, час формування та повідомлення про завершення формування маршруту.

Це означає, що маршрутного поїзда як «шляху руху» у класичному математичному значенні (оптимальний граф у залізничній мережі) у правилах немає. Натомість Укрзалізниця керується процедурним набором умов, що дозволяють сформувати поїзд у межах технологічних обмежень, без експліцитної логістичної оптимізації шляху (тобто без явного вибору найкращого маршруту між вузлами мережі на основі критеріїв).

Однак, операційно-процедурний підхід, який використовується в Укрзалізниці (тобто накопичення вагонів, погодження формування поїздів із філіями, відправлення за графіком і наявними технічними умовами), не забезпечує:

1. Оптимального вибору шляху з логістичної точки зору: рішення про те, який шлях обрати між вузлами мережі, не ґрунтується на математичній оптимізації часу, капітальних витрат або пропускної спроможності, а на правилах і технічних обмеженнях. Це відрізняється від інтегрованих моделей оптимізації, що описуються у транспортних науках та географії транспорту.
2. Гнучкого реагування на зміни інфраструктури: за значних змін у мережі (наприклад, частковому руйнуванні шляхів через війну) відсутня централізована модель, яка автоматично адаптує маршрути вантажних поїздів.
3. Інформаційної підтримки для стратегічного планування: система побудована більше на процедурній координації, ніж на автоматизованому інтелектуальному виборі маршрутів на основі даних у реальному часі (AI чи аналіз великих даних).

Таким чином, науково-практична проблема з розробки та дослідження альтернативних поточному підходів є актуальною. Слід зазначити що для цього необхідно розробити тестовий програмний полігон для перевірки та тестуванні різноманітних гіпотез алгоритмів маршрутизації з метою практичної оцінки їх ефективності.

В рамках поточного дослідження автори розробили та програмно імплементували таку імітаційну модель залізничних перевезень, що відповідає критеріям модульності (її можна розширювати та модифікувати без значних змін ядра моделі) та адекватності роботи моделі. Поточну роботу слід розуміти як фундаментальну основу та основний імітаційний інструмент для подальших наукових досліджень авторів, спрямованих на розробку алгоритмів, що підвищать економічну ефективніть вантажних перевезень на залізниці.

2. Обгрунтування обраних методів моделювання

Для побудови математичної моделі маршрутизації вантажних перевезень у даній роботі використано апарат теорії графів як базовий інструмент формалізації транспортної мережі.

Такий підхід є загальноприйнятим у світовій практиці моделювання складних транспортно-логістичних систем і широко застосовується у дослідженнях, присвячених оптимізації залізничних перевезень, плануванню руху та управлінню потоками на мережах великої розмірності. Застосування теорії графів дозволяє перейти від описового представлення інфраструктури до строгої математичної моделі, придатної для аналітичного дослідження та алгоритмічної реалізації [3].

У рамках запропонованого підходу залізнична мережа подається у вигляді зваженого мультиорієнтованого графа $G = (V, A)$, де де множина вершин V відповідає станціям і вузлам мережі, а множина дуг A - перегонам між ними. Подібне представлення є стандартним у задачах транспортного моделювання та маршрутизації, оскільки воно забезпечує високий рівень абстракції та універсальність опису, дозволяючи враховувати багатоваріантність маршрутів, наявність паралельних перегонів і напрямленість руху [4]. Формалізація мережі у вигляді графа створює основу для застосування верифікованих алгоритмів комбінаторної оптимізації та методів дослідження операцій.

Елементи графової моделі мають природну інтерпретацію у термінах фізичної інфраструктури залізниці. Вершини графа моделюють станції, сортувальні вузли та інші технологічні пункти, в яких відбуваються операції формування та розформування поїздів, накопичення вагонів і виконання маневрових робіт. Дуги графа відповідають перегонам між станціями. Кожній дузі можуть бути поставлені у відповідність вагові параметри, зокрема довжина L_e , час проходження τ_e , експлуатаційна вартість або пропускна здатність. Це дозволяє формалізувати задачу маршрутизації як задачу пошуку оптимального шляху за заданим критерієм (мінімальний час, мінімальні витрати або багатокритеріальна оптимізація), що є класичною проблемою на графах [3].

Використання графових моделей також відкриває доступ до широкого спектра ефективних алгоритмів, добре досліджених у теорії алгоритмів і транспортних застосуваннях. Для задачі знаходження найкоротших шляхів широко застосовуються алгоритми Дейкстри та його узагальнення, які забезпечують поліноміальний час роботи навіть для мереж великої розмірності [5]. Для аналізу пропускної здатності та розподілу потоків використовуються моделі максимального потоку та мінімального розрізу, що дозволяють досліджувати вузькі місця мережі та оптимізувати використання інфраструктурних ресурсів. У контексті залізничних перевезень графові підходи успішно застосовуються для розв’язання задач планування руху поїздів, розкладів і маршрутизації вантажних потоків [6].

Додатковою перевагою графового підходу є його сумісність із сучасними методами імітаційного моделювання та математичного програмування. Графова структура мережі може бути безпосередньо інтегрована в моделі дискретно-подієвого моделювання або в задачі змішаного цілочислового лінійного програмування для дослідження динаміки транспортних процесів і оптимізації керуючих рішень. Така інтеграція забезпечує узгодженість між структурним описом мережі та алгоритмічними процедурами оптимізації, що є важливим для побудови масштабованих моделей реальних залізничних систем. Отже, використання апарату теорії графів у даній роботі обґрунтовується його математичною строгістю, природною відповідністю фізичній структурі залізничної мережі та наявністю розвиненого інструментарію алгоритмів оптимізації. Це створює надійну теоретичну основу для подальшої розробки моделей маршрутизації та дослідження ефективності управління вантажними перевезеннями.

У якості основного методу моделювання було обрано Дискретно-подієву імітацію (DES). Такий вибір обумовлено тим, що попри високу ефективність методів математичного програмування, зокрема змішаного цілочислового лінійного програмування (MILP) та нелінійної оптимізації, їх застосування в задачах моделювання залізничних транспортних систем має суттєві обмеження при відтворенні оперативної динаміки процесів. Такі методи, як

правило, орієнтовані на пошук стаціонарних або квазістатичних оптимальних рішень і недостатньо адекватно описують часову еволюцію системи в умовах невизначеності. Оскільки метою даної роботи є створення імітаційного полігону для дослідження адаптивних стратегій управління маршрутизацією в стохастичному середовищі, як основний інструмент обрано дискретно-подієве імітаційне моделювання (Discrete-Event Simulation, DES), яке широко застосовується для аналізу складних транспортних і логістичних систем [7].

DES базується на представленні системи як послідовності подій, що відбуваються у дискретні моменти часу та змінюють її стан. Такий підхід є особливо придатним для моделювання залізничних перевезень, де ключові процеси — прибуття та відправлення поїздів, формування составів, обробка вагонів на станціях — природно інтерпретуються як події. У транспортних дослідженнях показано, що DES дозволяє адекватно відтворювати складну взаємодію інфраструктурних ресурсів, рухомого складу та потоків заявок, забезпечуючи високу ступінь реалізму моделі.

Порівняно зі статичними аналітичними моделями, DES має низку принципових переваг. По-перше, цей підхід дозволяє природним чином враховувати стохастичні фактори, зокрема нерівномірність надходження вантажів, варіативність часу руху та технологічні затримки на станціях. У контексті залізничних систем це є критичним для оцінки надійності графіків і стійкості маршрутних стратегій до випадкових збурень. Дослідження у сфері транспортного моделювання підтверджують, що ігнорування стохастичності призводить до систематичного переоцінювання ефективності оптимізаційних рішень.

По-друге, DES забезпечує можливість явного моделювання динаміки накопичення черг $Q_{i \to j}(t)$ на сортувальних станціях і вузлах мережі. Черги є ключовим елементом функціонування залізничних систем, оскільки вони визначають затримки вагонів і впливають на пропускну здатність інфраструктури. У статичних моделях точне відображення черг вимагає складних апроксимацій або лінеаризації, тоді як у DES вони виникають як природний результат взаємодії подій. Це дозволяє досліджувати ефекти перевантаження, каскадні затримки та формування “вузьких місць” у мережі.

По-третє, дискретно-подієва імітація фіксує детальну хронологію взаємодії об’єктів і ресурсів, що створює можливість аналізу мікродинаміки процесів і кількісної оцінки так званої “ціни невизначеності” — різниці між теоретично оптимальними показниками та результатами функціонування системи в реальних умовах. Такий аналіз є особливо важливим для розробки адаптивних стратегій управління, орієнтованих на роботу в умовах неповної інформації та випадкових збурень. DES широко використовується як експериментальна платформа для тестування алгоритмів прийняття рішень і методів штучного інтелекту в транспортних системах.

Окремою перевагою обраного підходу є його сумісність з об’єктно-орієнтованою парадигмою моделювання, що є доцільною для детального опису технологічних процесів залізничних вузлів. У дослідженнях, присвячених імітаційному моделюванню роботи станцій, показано, що традиційні моделі часто характеризуються жорсткою прив’язкою програмної реалізації до конкретної технології, що ускладнює їх повторне використання та масштабування.

Альтернативний підхід полягає у представленні системи як сукупності взаємодіючих об’єктів — технологічних операцій, виконавців і матеріальних елементів інфраструктури. Важливим принципом є відділення формального опису технології від універсального моделюючого ядра. У такій архітектурі вагони, колії та інші об’єкти поєднуються з формалізованими моделями поведінки, які можуть бути представлені у вигляді скінченних автоматів. Це дозволяє створювати бібліотеки типових компонентів і повторно використовувати їх у різних конфігураціях моделі, істотно скорочуючи час розробки та підвищуючи гнучкість імітаційного середовища.

Таким чином, вибір дискретно-подієвого імітаційного моделювання як основного методу дослідження обумовлений його здатністю адекватно відтворювати стохастичну динаміку залізничних процесів, моделювати черги та ресурсні обмеження, а також слугувати експериментальною платформою для тестування інтелектуальних стратегій управління. Поєднання DES з об’єктно-орієнтованим підходом створює масштабовану та модульну основу для подальших досліджень у сфері оптимізації вантажних перевезень.

3. Математична модель залізничних перевезень

Топологія залізничної мережі в межах запропонованої моделі формалізується у вигляді зваженого мультиорієнтованого графа $G(V, A)$, що забезпечує строгий математичний опис структури інфраструктури та створює основу для подальшого алгоритмічного аналізу. Такий підхід дозволяє перейти від фізичного представлення мережі до абстрактної моделі, придатної для застосування методів теорії графів, оптимізації та імітаційного моделювання. Використання мультиорієнтованого графа є обґрунтованим з огляду на складну структуру реальних залізничних мереж, де між одними й тими самими вузлами можуть існувати декілька альтернативних маршрутів з різними технічними характеристиками. У цій структурі множина вершин $V = \{v_1, v_2, \ldots, v_n\}$ відповідає залізничним станціям, сортувальним вузлам та іншим інфраструктурним об’єктам, які виконують функції генерації, обробки або прийому транспортних потоків. Вершини графа інтерпретуються не лише як географічні точки, а як складні технологічні системи з власними ресурсними обмеженнями та операційними процесами. Множина дуг $A = \{a_1, a_2, \ldots, a_m\}$ описує перегони між станціями та визначає можливі напрямки руху поїздів. Орієнтований характер дуг дозволяє враховувати асиметрію параметрів руху в протилежних напрямках, що є характерним для реальних умов експлуатації.

Критично важливою особливістю моделі є реалізація графової структури у вигляді мультиграфа за допомогою класу MultiDiGraph бібліотеки NetworkX. Такий вибір інструментальних засобів забезпечує можливість явного представлення множинних паралельних зв’язків між парами вершин. У реальній залізничній інфраструктурі між станціями i та j часто існує декілька колій або альтернативних маршрутів, які можуть відрізнятися за технічним станом, пропускною здатністю або режимами експлуатації. У моделі ця множина описується як $A_{i\to j} = \{a^1_{i\to j}, \ldots, a^k_{i\to j}\}$, що дозволяє враховувати конкурентні варіанти проходження та підвищує точність відтворення інфраструктурних особливостей.

Кожна дуга $a \in A$ характеризується вектором параметрів $p_a = \langle L_a, C_a, v_a, K_a \rangle$, який відображає ключові фізичні та експлуатаційні характеристики відповідної ділянки. Параметр L_a задає фізичну довжину перегону в кілометрах і використовується як базова метрика просторової відстані. Параметр C_a описує вагову норму або максимально допустиму довжину поїзда, що накладає обмеження на склад і масу рухомого складу. Середня дільнична швидкість v_a визначає часові характеристики руху та дозволяє оцінювати тривалість проходження перегону. Пропускна здатність K_a, виражена у парах поїздів за добу, в імітаційній моделі трансформується у дискретну кількість доступних слотів для одночасного використання ресурсу, що створює механізм урахування конкуренції за інфраструктуру. Таке параметричне описання дуг формує багатовимірний простір характеристик мережі, у якому можуть бути сформульовані різні критерії оптимальності. Воно також забезпечує можливість інтеграції графової моделі з імітаційними процедурами, де кожен перегін розглядається як ресурс з обмеженою пропускною здатністю та часовою динамікою використання.

Базова маршрутизація для кожного вантажного відправлення p, що генерується в системі, визначається статичний маршрут $P_p = (v_{start}, \ldots, v_{end})$, який з’єднує початкову та кінцеву вершини. Задача маршрутизації формулюється як задача пошуку шляху мінімальної вартості у

графі G. У базовій конфігурації функцією вартості виступає довжина дуги L_a, що відповідає критерію мінімізації загальної відстані перевезення. Така постановка створює еталонний маршрут, який використовується як вихідна стратегія для подальшого аналізу.

Для знаходження оптимального шляху P^* застосовується алгоритм Дейкстри, який є ефективним методом пошуку найкоротших шляхів у графах з невід'ємними вагами. Алгоритм гарантує знаходження глобального мінімуму та має поліноміальну обчислювальну складність, що робить його придатним для використання у великих мережах. У контексті запропонованої моделі він забезпечує детерміновану та відтворювану процедуру побудови маршрутів, яка може бути використана як базовий рівень для порівняння з більш складними адаптивними або стохастичними методами маршрутизації.

Функціонування запропонованої моделі залізничної транспортної системи визначається сукупністю фізичних та технологічних обмежень, що відображають реальні інфраструктурні можливості мережі. Урахування цих обмежень є принципово важливим для забезпечення адекватності імітаційних результатів, оскільки вони формують простір допустимих станів системи та безпосередньо впливають на динаміку руху поїздів, формування черг і використання ресурсів. У моделі виділяються чотири основні класи обмежень: часові, місткісні, ресурсні та станційні.

Час проходження поїзда по дузі амоделюється як детермінована базова величина $\tau_a = L_a/v_a$, що визначається відношенням довжини перегону до середньої дільничної швидкості руху. Така формалізація забезпечує узгодженість просторових і часових характеристик мережі та дозволяє безпосередньо інтегрувати їх у календар подій імітаційної моделі. Водночас реальні експлуатаційні умови характеризуються наявністю випадкових збурень, пов'язаних із технічними затримками, обмеженнями сигналізації або операційними факторами. З цією метою у модель вводиться стохастичний компонент δ_t , який модифікує базовий час проходження. Це дозволяє досліджувати чутливість системи до невизначеності та аналізувати вплив варіацій часу руху на загальну стабільність графіка.

Кожен перегін характеризується максимально допустимою місткістю, що інтерпретується як гранична довжина або маса поїзда. Під час формування складу виконується умова $\sum w_i \leq C_a$, де w_i — індивідуальні параметри вагонів. Це обмеження відображає технічні характеристики інфраструктури та тягового рухомого складу, а також гарантує експлуатаційну безпеку. У моделі воно реалізується як жорстке обмеження на допустимі конфігурації поїздів, що впливає на процес консолідації вантажів і може призводити до додаткових затримок у разі перевищення допустимих параметрів. Таким чином, місткісні обмеження формують зв'язок між мікрорівнем (структура поїзда) та макрорівнем (пропускна здатність мережі).

Пропускна здатність кожної ділянки мережі моделюється як обмежений ресурс із дискретною кількістю одночасно доступних слотів. Формально це реалізується у вигляді семафора ємністю K_a, який визначає максимальну кількість поїздів, що можуть одночасно перебувати на перегоні. Поїзд отримує дозвіл на вихід лише за умови наявності вільного ресурсу ($occupied < K_a$). Такий механізм дозволяє явно відобразити конкуренцію між потоками та відтворити ефекти насичення інфраструктури, що проявляються у вигляді заторів і черг. Моделювання пропускної здатності як обмеженого ресурсу є ключовим елементом аналізу вузьких місць і дослідження стратегій управління трафіком.

Станції в моделі розглядаються як складні обслуговуючі системи з обмеженими ресурсами накопичення та переробки. Параметр F_i задає кількість доступних колій для тимчасового розміщення вагонів і поїздів, тоді як R_i визначає максимальну інтенсивність виконання технологічних операцій, виражену в поїздах за годину. Ці обмеження формують локальні черги та впливають на синхронізацію процесів прибуття і відправлення. У поєднанні з обмеженнями перегонів вони створюють складну мережеву взаємодію, де станції виступають

вузловими центрами перерозподілу потоків. Сукупна дія зазначених обмежень формує багаторівневу систему взаємопов’язаних ресурсів, у якій поведінка окремих елементів впливає на глобальну динаміку мережі. Їх формалізація в межах єдиної моделі забезпечує можливість комплексного аналізу ефективності маршрутизації, оцінки стійкості до перевантажень та дослідження альтернативних стратегій управління перевезеннями.

Центральним елементом запропонованої системи управління є політика готовності до відправлення, яка визначає момент завершення процесу накопичення поїзда на станції та ініціює його відправлення на наступну ділянку маршруту. Цей механізм відіграє ключову роль у формуванні балансу між ефективністю використання рухомого складу та якістю транспортного обслуговування. Фактично політика готовності задає правило прийняття рішень у точці конфлікту між прагненням до максимального завантаження поїзда та необхідністю обмежувати час очікування вантажів.

У роботі реалізовано гібридну стратегію, що поєднує критерії завантаження та часу. Такий підхід дозволяє враховувати як ресурсну ефективність, так і сервісні вимоги, формуючи адаптивний механізм керування. Формально склад поїзда w, що перебуває у процесі накопичення на станції, вважається готовим до відправлення у момент часу $\hat{t}$, якщо предикат готовності $\Gamma_w(\hat{t})$ набуває значення

$$\Gamma_w(\hat{t}) = \left(y_w(\hat{t}) = C_e\right) \text{ - Умова 1: Повне заповнення,}$$
$$\vee \left(y_w(\hat{t}) \geq \theta C_e \wedge \left(\hat{t} - t_w^{last} \geq T_{hold}\right)\right) \text{ - Умова 2: Часовий тайм-аут}$$

де $y_w(\hat{t})$ — поточна заповненість складу, C_e — його максимальна місткість, $\theta \in (0,1]$ — коефіцієнт мінімального заповнення, T_{hold} — граничний час очікування після прибуття останнього вагона, а t_w^{last} — момент цього прибуття.

Перша умова відповідає ситуації повного заповнення складу і реалізує стратегію максимізації використання тягових і вагонних ресурсів. У цьому випадку поїзд негайно вважається готовим до відправлення, що мінімізує втрати пропускної здатності та забезпечує високу продуктивність мережі. Друга умова вводить часовий запобіжник, який активується за недостатньої інтенсивності надходження вагонів. Якщо рівень завантаження перевищує порогове значення θC_e, але протягом інтервалу T_{hold} не відбувається подальшого поповнення, система ініціює відправлення частково заповненого поїзда. Це дозволяє обмежити надмірні простої та зменшити середній час доставки.

Запропонована політика може бути інтерпретована як параметризований компроміс між двома конкуруючими цілями: мінімізацією експлуатаційних витрат і мінімізацією часових затримок. Параметр θ виступає регулятором ресурсної ефективності: його збільшення стимулює формування більш повних поїздів, але потенційно підвищує час очікування. Натомість параметр T_{hold} визначає допустимий рівень сервісної затримки та впливає на регулярність відправлень. Варіювання цих параметрів у межах імітаційної моделі дозволяє досліджувати різні режими роботи системи та будувати криві компромісу між продуктивністю і якістю обслуговування.

З точки зору теорії керування, описана політика є локальним правилом прийняття рішень, яке формує глобальну динаміку потоків у мережі. Її застосування призводить до виникнення складних нелінійних ефектів, зокрема синхронізації відправлень, формування хвиль навантаження та появи вузьких місць. Саме тому формалізація політики готовності у вигляді чітко визначеного предиката є необхідною умовою для подальшого аналізу стабільності системи та оптимізації параметрів управління.

4. Програмна імплементація моделі за допомогою Python

Програмна реалізація імітаційної моделі виконана мовою Python із систематичним використанням принципів об’єктно-орієнтованого програмування, що забезпечує модульність, розширюваність та керованість архітектури симулятора. Вибір Python зумовлений поєднанням високого рівня абстракції, наявністю розвиненої екосистеми наукових бібліотек та зручністю швидкого прототипування складних алгоритмічних систем. При цьому було свідомо обрано кастомну архітектуру симулятора замість використання готових спеціалізованих середовищ імітаційного моделювання (таких як AnyLogic або SimPy), що пов’язано з необхідністю глибокої кастомізації логіки взаємодії об’єктів і точного контролю над внутрішніми механізмами обробки подій.

Залізнична станція в моделі розглядається як сукупність взаємодіючих технологічних елементів, кожен з яких характеризується власним станом і правилами поведінки. Ефективне відтворення такої структури потребує представлення інфраструктурних об’єктів — станцій, перегонів, поїздів і вагонів — у вигляді окремих програмних сутностей із чітко визначеними інтерфейсами. Об’єктно-орієнтований підхід дозволяє інкапсулювати внутрішній стан об’єкта разом із методами його зміни в межах єдиного класу. Це забезпечує локалізацію логіки, зменшує зв’язність між компонентами системи та спрощує подальше масштабування моделі. Зокрема, додавання нових типів ресурсів або правил управління не потребує радикальної перебудови існуючої архітектури.

Архітектура симулятора побудована за принципом подієво-орієнтованої системи, у якій еволюція моделі описується послідовністю дискретних подій. Кожна подія інтерпретується як атомарна зміна стану системи, наприклад прибуття поїзда, завершення формування складу або звільнення ресурсу. Центральним елементом ядра симулятора є структура даних PriorityQueue, реалізована за допомогою модуля heapq, яка забезпечує ефективне хронологічне впорядкування подій. Використання пріоритетної черги дозволяє підтримувати календар подій у відсортованому стані та гарантує, що на кожному кроці моделювання обробляється найближча за часом подія.

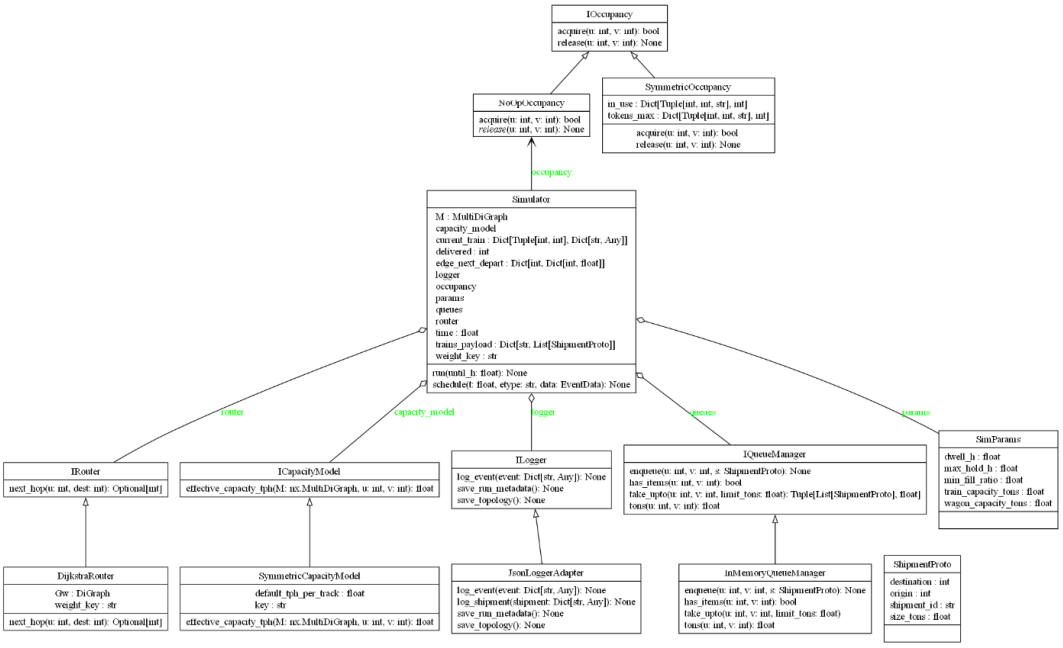

Рис. 1 – Діаграма класів імплементованої моделі залізниці
Fig. 1 – Class diagram of the implemented railway model

Такий механізм організації обчислювального процесу забезпечує часову узгодженість симуляції та дозволяє моделювати складні причинно-наслідкові залежності між подіями. Крім того, пріоритетна черга має логарифмічну складність операцій вставки та вилучення, що є критично важливим для ефективної роботи моделі при великій кількості одночасно запланованих подій. У поєднанні з об’єктно-орієнтованою структурою це формує гнучку програмну платформу, придатну для реалізації експериментальних стратегій управління та інтеграції з алгоритмами оптимізації або машинного навчання.

Динаміка імітаційної моделі реалізується у вигляді подієво-орієнтованого процесу, в якому еволюція системи описується послідовною обробкою скінченної множини атомарних подій. Ці події формують замкнений операційний цикл, що відтворює повний життєвий цикл вантажу в мережі — від моменту його генерації до завершення перевезення. Така декомпозиція дозволяє формалізувати складні технологічні процеси у вигляді чітко визначених переходів стану, забезпечуючи прозорість логіки моделювання та можливість детального аналізу часової структури системи. У моделі виділяються чотири базові типи подій, які взаємодіють між собою та утворюють причинно-наслідковий ланцюг.

Spawn (генерація) - відповідає за ініціалізацію нового транспортного запиту та створення об’єкта вантажу в системі. На даному етапі фіксується час входу t_{in}, який використовується надалі для оцінки тривалості перевезення та показників якості обслуговування. Для згенерованого вантажу обчислюється оптимальний маршрут P^*y графі мережі, після чого визначається перша станція обробки. Вагон додається до відповідної черги накопичення $Q_{src \to dst}$, що представляє собою буфер для формування поїздів за напрямками. Таким чином, подія генерації інтегрує процес маршрутизації з локальною логікою станційного накопичення.

Try Form (спроба формування) - періодична керуюча подія, що виконує моніторинг стану черг накопичення на станціях. Її основною функцією є перевірка виконання предикату готовності Γ_w для потенційних складів. Алгоритм аналізує поточне завантаження, час очікування та доступність ресурсів інфраструктури. У разі виконання умов формується новий об’єкт типу Train, який агрегує вибрану групу вагонів. Після цього планується подія Depart. Якщо ресурси тимчасово недоступні, система зберігає стан очікування та повторно ініціює перевірку через визначений інтервал часу. Такий механізм реалізує адаптивну стратегію керування процесом консолідації вантажів.

Depart (відправлення) - моделює процес захоплення інфраструктурних ресурсів і початок руху поїзда. Симулятор намагається зменшити лічильник доступних слотів K_e на відповідному перегоні, що відповідає резервуванню пропускної здатності. Якщо $K_e = 0$, поїзд переводиться у стан очікування та розміщується в черзі доступу до ресурсу. У разі успішного захоплення перегону обчислюється прогнозований час прибуття $t_{arr} = t_{now} + \tau_e$, де τ_e — час проходження ділянки. Після цього в календар подій додається подія Arrive. Таким чином, відправлення поєднує управління ресурсами з часовим плануванням руху.

Arrive (прибуття) - завершує цикл використання перегону та ініціює наступну фазу обробки вантажів. Після прибуття поїзда ресурс звільняється ($K_e \leftarrow K_e + 1$), що робить його доступним для інших запитів. Далі виконується розформування складу: вагони, що досягли кінцевого пункту призначення, фіксують час виходу t_{out} і видаляються з системи, що дозволяє обчислити повний час доставки. Транзитні вагони сортуються за напрямками та додаються до відповідних черг накопичення, ініціюючи нові події Try Form. Цей етап забезпечує безперервність потоку та замикання циклу моделювання.

Сукупність описаних подій формує замкнену дискретно-подієву систему, в якій глобальна поведінка мережі виникає як результат локальних взаємодій. Така структура дозволяє

детально відтворювати часову динаміку транспортних процесів, аналізувати виникнення черг і досліджувати ефективність різних стратегій управління в умовах обмежених ресурсів.

З метою забезпечення керованої складності та підвищення модульності програмної архітектури модель побудована на принципі розділення відповідальностей між логікою інфраструктури та логікою агентів. Такий підхід дозволяє декомпозувати систему на відносно незалежні підсистеми, кожна з яких відповідає за окремий аспект функціонування транспортної мережі. Зокрема, в архітектурі реалізовано чітку сегрегацію «залізничного» сегмента, що описує рух поїздів як агрегованих транспортних одиниць, та «вантажного» сегмента, який моделює поведінку окремих вагонів як елементарних агентів.

Інфраструктурний рівень відповідає за управління ресурсами мережі — перегонами, станційними коліями та пропускною здатністю. Агентний рівень, у свою чергу, описує життєвий цикл вантажних одиниць і процеси їх агрегування в поїзди. Таке розділення дозволяє незалежно модифікувати правила руху поїздів і логіку обробки вантажів, що є важливим для проведення експериментів із різними стратегіями керування. Крім того, воно спрощує масштабування моделі, оскільки зміни в одному сегменті не потребують суттєвого перепроєктування іншого.

Взаємодія між цими сегментами реалізується через спеціальні точки синхронізації на станціях, які виконують роль інтерфейсів між мікро- та макрорівнем моделі. На нижньому рівні вагони розглядаються як автономні агенти, що перебувають у чергах накопичення та тимчасово блокуються до моменту формування поїзда. Створення об’єкта типу \texttt{Train}, який є агентом верхнього рівня, означає агрегацію групи вагонів у єдину транспортну сутність. У цей момент індивідуальна динаміка вагонів підпорядковується колективному стану поїзда.

Під час руху по перегону вагони делегують представлення свого стану об’єкту поїзда, який виступає проксі-агентом для всієї групи. Це дозволяє зменшити обчислювальну складність, оскільки операції управління ресурсами виконуються на рівні поїздів, а не окремих вагонів. По прибуттю на станцію призначення поїзд як агрегована сутність ліквідується, після чого вагони повертаються в активний стан індивідуальних агентів і знову беруть участь у процесах сортування та накопичення. Такий цикл агрегації та деагрегації забезпечує узгодження детального опису вантажних потоків із ефективним моделюванням руху поїздів.

Для розв’язання конфліктів за інфраструктурні ресурси в моделі реалізовано механізм зворотного зв’язку, що імітує диспетчерське регулювання руху. Якщо подія Depart не може негайно отримати доступ до необхідного ресурсу, вона не скасовується, а перепланується на майбутній момент часу. Інтервал повторної спроби визначається за експоненційним законом розподілу, що моделює стохастичний характер затримок і рішень диспетчера. Такий підхід запобігає втраті подій, підтримує стабільність симуляції та дозволяє досліджувати вплив перевантаження мережі на часові характеристики перевезень.

У сукупності описана архітектура формує багаторівневу агентно-інфраструктурну систему, в якій локальні правила взаємодії породжують глобальну динаміку транспортних потоків. Це створює гнучку платформу для аналізу стратегій управління, дослідження конфліктів ресурсів і оцінки ефективності різних організаційних рішень у складних логістичних мережах.

Однією з суттєвих методологічних проблем класичних дискретно-подієвих моделей транспортних систем є жорстка статичність опису інфраструктури. У традиційних реалізаціях кожен інфраструктурний елемент — зокрема окрема колія або ресурс станції — часто представляється як окремий програмний блок або іменована змінна. Такий підхід призводить до сильної зв’язаності коду з конкретною конфігурацією об’єкта моделювання, ускладнює повторне використання компонентів і практично унеможливлює динамічне масштабування моделі. Будь-яка зміна топології станції або кількості ресурсів у такій архітектурі потребує

ручного втручання в програмний код, що підвищує ризик помилок і знижує відтворюваність експериментів.

У запропонованій роботі для подолання цієї проблеми застосовано підхід, заснований на використанні динамічних колекцій ресурсів, який дозволяє відокремити опис інфраструктурної конфігурації від алгоритмічної логіки симулятора. Основна ідея полягає в представленні однорідних інфраструктурних елементів не як фіксованого набору змінних, а як елементів параметризованих контейнерів, розмір і склад яких можуть змінюватися під час ініціалізації моделі. Це створює узагальнену абстракцію ресурсу, придатну для автоматизованої генерації різних конфігурацій без модифікації вихідного коду.

На рівні програмної реалізації станція описується як об’єкт, що містить колекцію однотипних ресурсів у вигляді списку або іншої динамічної структури даних, наприклад self.tracks = [Track(), …]. Кожен елемент такої колекції є екземпляром класу Track, який інкапсулює стан конкретної колії та методи взаємодії з нею. На відміну від підходу з жорстко закодованими змінними типу track_1, track_2, використання списків дозволяє оперувати ресурсами через уніфіковані ітеративні процедури та узагальнені алгоритми розподілу.

Ключовою перевагою цього підходу є можливість конфігурації інфраструктури на основі зовнішніх описів, зокрема через вхідні JSON-файли. Параметри станції — кількість колій, їх типи та характеристики — зчитуються під час ініціалізації та автоматично трансформуються у відповідні об’єкти моделі. Таким чином, зміна структури станції або масштабування мережі зводиться до редагування конфігураційних даних без необхідності втручання в програмний код. Це підвищує гнучкість моделі, спрощує проведення серій експериментів із різними сценаріями та забезпечує відтворюваність результатів.

З архітектурної точки зору використання динамічних колекцій формує декларативний стиль опису інфраструктури, в якому структура системи визначається даними, а не жорстко зафіксованою логікою програми. Такий підхід сприяє кращій масштабованості, полегшує тестування альтернативних конфігурацій і створює передумови для автоматизованої генерації великих синтетичних мереж. У результаті модель набуває властивостей універсальної платформи, придатної для дослідження широкого спектра задач управління залізничними транспортними системами.

З метою підвищення реалістичності моделювання експлуатаційних процесів у системі передбачено стохастичний механізм розподілу інфраструктурних ресурсів. У реальних умовах диспетчеризація руху рідко зводиться до жорстко детермінованого правила типу «перший вільний ресурс». На практиці вибір колії або локомотива залежить від багатьох факторів — оперативної ситуації, локальних рішень персоналу та випадкових флуктуацій у завантаженні. Тому використання суто детермінованої схеми в імітаційній моделі може призводити до систематичних перекосів у навантаженні ресурсів і нереалістичного розподілу зносу інфраструктури.

У запропонованій моделі реалізовано стохастичну процедуру вибору ресурсу, яка імітує природну варіативність диспетчерських рішень і забезпечує більш рівномірне використання інфраструктури. Основна ідея полягає у випадковому виборі елемента з множини доступних ресурсів після попередньої фільтрації за умовами придатності. Такий підхід дозволяє зберегти технологічні обмеження (доступність, сумісність, стан ресурсу), одночасно уникаючи жорсткої пріоритетності окремих елементів.

5. Визначення еталонної маршрутизації

Оцінка ефективності розробленого симуляційного полігону здійснюється на основі системи ключових показників ефективності, що комплексно характеризують як якість

логістичного сервісу, так і ступінь використання інфраструктурних і рухомих ресурсів. Вибір відповідних метрик зумовлений необхідністю багатокритеріального аналізу, оскільки оптимальне функціонування транспортної системи передбачає одночасне врахування часових, пропускних і ресурсних характеристик. Запропонований набір показників дозволяє здійснювати кількісне порівняння різних стратегій управління та оцінювати їхній вплив на глобальну динаміку мережі.

Середній повний час перебування вагонів ($\bar{S}$). Цей показник є базовою інтегральною метрикою якості транспортного обслуговування та відображає середню тривалість перебування вантажу в системі. Він вимірюється як різниця між моментом генерації вагона t_p^{in} та моментом його прибуття у кінцевий пункт призначення t_p^{out}, усереднена за всіма перевезеннями:

$$\bar{S} = \frac{1}{N}\sum_{p=1}^{N}\left(t_p^{out} - t_p^{in}\right)$$

Показник $\bar{S}$ інтегрує в собі як час руху по мережі, так і всі проміжні затримки на станціях, тому він є чутливим індикатором загальної ефективності логістичного процесу. Зменшення цього значення свідчить про підвищення швидкості доставки та покращення якості сервісу.

Сумарний вузловий простій ($\bar{W}$). Даний показник характеризує середній час очікування вагонів у чергах накопичення $Q_{i\to j}(t)$ на сортувальних станціях. Він відображає ефективність роботи вузлових елементів мережі та ступінь узгодженості процесів формування поїздів. Високі значення $\bar{W}$ свідчать про перевантаження станцій або неефективну організацію потоків. Мінімізація цього показника є важливою умовою підвищення пропускної здатності та зменшення затримок у системі.

Пропускна спроможність потоків ($\Phi_{s,t}$). Цей показник визначається як кількість вагонів, успішно доставлених між конкретною парою станцій «відправлення–призначення» (t) за фіксований часовий інтервал T. Він є прямою мірою продуктивності транспортної системи та дозволяє аналізувати ефективність обслуговування окремих напрямків. Порівняння значень $\Phi_{s,t}$ для різних сценаріїв дає можливість виявляти вузькі місця та оцінювати вплив управлінських рішень на структуру потоків.

Використання локомотивів (U_e). Показник U_e характеризує ступінь завантаження тягового рухомого складу на окремих ділянках мережі. Він визначається як відношення сумарного часу активного руху локомотивів до їхнього загального часу перебування в системі. Це дозволяє оцінити ефективність використання ресурсів і виявити як недовантажені, так і перевантажені ділянки. Аналіз U_e є важливим для оптимізації розподілу тяги та підвищення економічної ефективності експлуатації.

Сукупне використання зазначених показників формує багатовимірну систему оцінювання, що дозволяє всебічно аналізувати результати імітаційних експериментів. Такий підхід створює основу для обґрунтованого вибору стратегій управління та подальшої оптимізації функціонування транспортної мережі.

Для дослідження адаптивних стратегій управління та формування теоретичного еталону ефективності ключові керуючі змінні моделі інтерпретуються як параметри Політики готовності до відправлення (T_{hold}). Ці параметри визначають компроміс між швидкістю доставки та ефективністю використання ресурсів і, відповідно, виступають основними регуляторами поведінки системи. З метою стратегічного аналізу та отримання базового орієнтира оптимальності формується аналітична оптимізаційна модель у вигляді задачі змішаного цілочислового лінійного програмування.

Запропонована MILP-модель описує статичне, детерміноване та агреговане представлення транспортної системи, що контрастує з подієво-орієнтованою динамікою імітаційної DES-моделі. Її призначення полягає у визначенні стратегічно оптимального розподілу потоків і частоти формування поїздів за фіксований плановий горизонт. Така постановка дозволяє отримати нижню оцінку витрат та використовується як еталон для порівняння з результатами імітаційних експериментів.

Метою оптимізації є мінімізація сукупних системних витрат, що включають транспортну роботу та штрафи за простої вантажів на сортувальних станціях. Транспортна складова пропорційна часу руху по дузі та зважується коефіцієнтом , тоді як вузлові затримки враховуються через штрафний коефіцієнт β:

$$\text{Мінімізувати } Z = \sum_{k\in K}\sum_{a\in A}\left(\alpha\cdot\frac{L_a}{v_a}\cdot x_a^k\right) + \sum_{k\in K}\sum_{i\in V_{sort}}\left(\beta\cdot w_i^k\right)$$

Тут змінна x_a^k описує обсяг потоку вагонів типу k по дузі a, а w_i^k моделює агрегований штраф за накопичення або простій відповідного вантажу на станції i. Така структура цільової функції забезпечує баланс між мінімізацією часу транспортування та зменшенням перевантаження вузлів мережі. Для коректного функціонування моделі необхідно імплементувати наступні системи обмежень.

Обмеження балансу потоків. Для кожної станції i і кожного типу вантажу k виконується умова збереження потоку, що гарантує узгодженість розподілу перевезень у мережі:

$$\sum_{a=(i,j)\in A} x_a^k - \sum_{a=(j,i)\in A} x_a^k = B_i^k$$

Параметр B_i^k визначає попит: додатне значення відповідає джерелу генерації потоку, а від’ємне - пункту призначення.

Обмеження місткості поїздів. Сумарний потік по кожній дузі не може перевищувати транспортну спроможність сформованих поїздів:

$$\sum_{k\in K} x_a^k \le y_a \cdot C_{max}, \quad \forall a \in A$$

Тут y_a — кількість поїздів, призначених для руху по дузі a, а C_{max} — максимальна місткість одного складу.

Обмеження інтенсивності відправлень. Кількість поїздів, що формуються на сортувальній станції i протягом планового періоду T, обмежується її технологічною спроможністю:

$$y_{(i,j)} \le R_i \cdot T, \quad \forall a = (i,j) \in A, i \in V_{sort}$$

Параметр R_i відображає максимальну інтенсивність обробки поїздів на станції.

Стратегічне обмеження мінімального розміру складу. Це обмеження є агрегованим аналогом динамічної політики формування поїздів і вимагає, щоб середній рівень завантаження не був нижчим за встановлений поріг:

$$y_{(i,j)}\cdot\theta C_{max} \le \sum_k x_{(i,j)}^k, \quad \forall a = (i,j) \in A$$

Параметр θ задає мінімальну допустиму частку заповнення складу та відображає стратегічну політику ефективного використання рухомого складу.

Умови цілочисловості. Змінні, що описують кількість поїздів, повинні бути невід’ємними цілими числами.

Запропонована MILP-постановка формує узагальнену стратегічну модель оптимального розподілу потоків і формування поїздів. Вона дозволяє дослідити вплив параметрів політики (T_{hold}) на системні витрати та слугує теоретичною базою для валідації результатів детальної дискретно-подієвої симуляції.

Як відомо, кладність комбінаторної задачі узгодження пасажиропотоку та провізної здатності у великих мережах ускладнює пошук оптимального рішення традиційними методами. Для вирішення цієї проблеми пропонується застосування мультиагентних систем (MAS), де оптимізація досягається через динамічну взаємодію автономних сутностей. Цей підхід дозволяє трансформувати багатокритеріальну задачу оптимізації у процес переговорів (negotiation-based mechanism) між попитом та пропозицією. На відміну від централізованих моделей управління, у яких процес прийняття рішень зосереджений у єдиному керуючому алгоритмі, агентно-орієнтований підхід передбачає декомпозицію транспортної системи на множину автономних взаємодіючих сутностей. Кожна з таких сутностей інтерпретується як агент із власною локальною цільовою функцією, інформаційними обмеженнями та правилами поведінки. Подібна декомпозиція дозволяє відобразити децентралізований характер реальних транспортних процесів, у яких глобальна динаміка системи виникає як результат локальних рішень окремих учасників. У запропонованій моделі виділено шість типів гетерогенних агентів, що представляють різні функціональні рівні залізничної системи.

Агент-відправка (Shipping Agent) моделює сторону попиту на перевезення. Його основною функцією є вибір маршруту та часу відправлення на основі функції корисності, що враховує очікуваний час доставки, рівень завантаженості мережі та доступність ресурсів. Прийняття рішень здійснюється в умовах обмеженої раціональності: агент оперує неповною інформацією та використовує евристичні правила оцінювання альтернатив, що наближує модель до реальної поведінки логістичних суб'єктів.

Агент-поїзд (Train Agent) представляє сторону пропозиції транспортних послуг. Він відповідає за формування складу, планування руху та оптимізацію власного завантаження з урахуванням інфраструктурних обмежень. Цільова функція цього агента спрямована на максимізацію використання місткості поїзда та мінімізацію простоїв, що забезпечує ефективне використання рухомого складу.

Агент-маршрут (Route Agent) виконує аналітичну функцію генерації множини ефективних альтернативних маршрутів для кожної пари «джерело–призначення». Він формує обмежений набір недомінованих шляхів за критеріями довжини, часу руху та навантаження, який використовується іншими агентами під час прийняття рішень. Таким чином забезпечується багатоваріантність маршрутизації та адаптивність системи до змін стану мережі.

Агент-колія (Track Agent) репрезентує інфраструктурний рівень і відповідає за контроль доступу до ресурсів перегонів. Він реалізує обмеження пропускної здатності, правила безпеки руху та механізми розподілу слотів між конкуруючими поїздами. Через взаємодію з цим агентом моделюються ефекти перевантаження та черг.

Агент-станція (Station Agent) функціонує як локальний координаційний вузол. На цьому рівні відбувається накопичення вагонів, формування поїздів і перерозподіл потоків між напрямками. Станційний агент приймає рішення щодо черговості обробки та ініціює взаємодію між агентами попиту й пропозиції.

Агент-мережа (Network Agent) виконує роль глобального спостерігача та координатора. Він контролює часову синхронізацію подій, керує ітераційними циклами симуляції та збирає статистичні показники. При цьому він не втручається безпосередньо в локальні рішення агентів, а забезпечує узгодженість функціонування всієї системи.

Запропонована багаторівнева агентна архітектура дозволяє розглядати транспортну систему як замкнений контур зворотних зв'язків, у якому зміни в пропозиції транспортних

ресурсів безпосередньо впливають на поведінку агентів попиту, а адаптація попиту, у свою чергу, модифікує навантаження на інфраструктуру. Такий підхід створює передумови для дослідження самоорганізаційних ефектів, виникнення вузьких місць та адаптивних режимів роботи мережі.

6. Висновки

У дослідженні розв’язано актуальну науково-прикладну задачу розробки математичної моделі та програмного забезпечення для оптимізації процесів маршрутизації та формування поїздів у вантажних залізничних перевезеннях. Отримані результати формують цілісну методологічну та інструментальну основу для створення імітаційного полігону, придатного для дослідження складних динамічних процесів у транспортних мережах та тестування адаптивних стратегій управління.

Обґрунтовано використання теорії графів як фундаментальної математичної бази для формалізації топології залізничної мережі та задач маршрутизації. Доведено доцільність застосування дискретно-подієвого імітаційного моделювання для відображення стохастичної природи транспортних процесів, що забезпечує переваги порівняно зі статичними аналітичними підходами. Розроблено формальний опис мережі у вигляді зваженого мультиорієнтованого графа з урахуванням інфраструктурних і технологічних обмежень, включно з параметризованою політикою готовності до відправлення поїздів. На цій основі реалізовано кастомний DES-симулятор мовою Python з подієвою архітектурою, що детально відтворює життєвий цикл вантажів і поїздів. Запропоновано систему ключових показників ефективності для комплексної оцінки якості функціонування моделі та сформульовано задачу змішаного цілочислового лінійного програмування як стратегічний еталон для порівняльного аналізу.

Основні наукові результати полягають у створенні комплексної математичної моделі залізничної мережі, яка інтегрує стратегічний MILP-підхід і динамічну DES-модель в єдину дослідницьку рамку. Такий гібридний підхід дозволяє кількісно оцінювати вплив невизначеності на ефективність перевезень і досліджувати розрив між теоретично оптимальними та практично досяжними рішеннями. Розроблена програмна реалізація демонструє високу гнучкість і масштабованість, забезпечуючи можливість моделювання складних сценаріїв та інтеграції з інструментами аналізу даних.

Експериментальні дослідження підтвердили суттєвий вплив стохастичних факторів на показники роботи транспортної системи та дозволили кількісно оцінити «ціну невизначеності». Показано, що використання адаптивних стратегій управління здатне значно зменшити затримки доставки та підвищити ефективність використання ресурсів. Практична цінність роботи полягає у створенні прототипу цифрового двійника транспортного полігону, який може застосовуватися для аналізу пропускної здатності, тестування нових організаційних рішень і проведення сценарного аналізу без втручання в реальний перевізний процес.

Перспективи подальших досліджень пов’язані з розширенням моделі засобами прогнозування попиту на основі методів машинного навчання, а також з інтеграцією імітаційного комплексу з реальними інформаційними системами залізничних операторів для підтримки прийняття рішень у режимі реального часу.

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

References

1. Cargo transportation rules :JSC "Ukrzaliznytsia". [in Ukranian] https://www.uz.gov.ua/cargo_transportation/legal_documents/terms_of_freight/
2. Cargo transportation rules. Chapter 17 Rules for the carriage of goods by the sender's routes: JSC "Ukrzaliznytsia". [in Ukranian] https://www.uz.gov.ua/cargo_transportation/legal_documents/terms_of_freight/264782/
3. Ahuja, R., Magnanti, T. and Orlin, J. (1993) *Network Flows: Theory, Algorithms, and Applications.* Prentice-Hall, Upper Saddle River. https://books.google.com.ua/books/about/Network_Flows.html?id=WnZRAAAAMAAJ&redir_esc=y
4. Kurant, M., & Thiran, P. (2006). Extraction and analysis of traffic and topologies of transportation networks. *Physical Review E*, 74(3).https://doi.org/10.1103/PhysRevE.74.036114
5. Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). *Introduction to Algorithms* (3rd ed.). MIT Press. https://www.cs.mcgill.ca/~akroit/math/compsci/Cormen%20Introduction%20to%20Algorithms.pdf
6. Gallo, G., Longo, G., Pallottino, S., & Nguyen, S. (1993). Directed hypergraphs and applications. *Discrete Applied Mathematics*, 42(2–3), 177–201.https://doi.org/10.1016/0166-218X(93)90045-P
7. Luteberget, B., Claessen, K., Johansen, C. et al. SAT modulo discrete event simulation applied to railway design capacity analysis. Form Methods Syst Des 57, 211–245 (2021). https://doi.org/10.1007/s10703-021-00368-2

DEVELOPMENT AND SOFTWARE IMPLEMENTATION OF A RAILWAY ROUTING MODEL

Artem Panchenko[1], PhD in Computer Sciences, Department of Theoretical and Applied Informatics
e-mail: artem.panchenko@ karazin.ua, ORCID: https://orcid.org/0000-0001-5865-6158;
Iryna Zaretska[1], PhD in Mathematics, Department of Theoretical and Applied Informatics,
e-mail: zaretskaya@ karazin.ua, ORCID: https://orcid.org/0000-0001-8747-2737;
Maryna Vladimirova[1], PhD in Economics specialized in Mathematical Methods in Economics, Department of Theoretical and Applied Informatics
e-mail: vladymyrova@karazin.ua, ORCID: https://orcid.org/0009-0000-9868-2617
Alina Biletska[1], Master, Department of Theoretical and Applied Informatics, e-mail: aleesha.biletska@gmail.com,
[1]*V. N. Karazin Kharkiv National University, Ukraine*
Manuscript was received October 1, 2025; Received after review November 2, 2025;
Accepted December 2, 2025; Published December 30, 2025

Abstract: Under current operating conditions of Ukrzaliznytsia, routing strategy and route selection play a key role in ensuring the economic efficiency of freight transportation. At present, routes are predominantly selected according to the shortest-path principle, which minimizes fuel consumption for transportation and reduces the wear of traction units and other rolling stock. Consequently, customers pay the lowest possible delivery cost. However, such routes are typically fixed for a predefined period and do not support dynamic adjustment, which leads to several issues, including the failure to account for the current technical condition of rolling stock on specific sections and their actual congestion levels during transportation. These problems have become particularly acute as a result of the full-scale invasion of Ukraine by the Russian Federation, which caused the destruction of parts of the railway infrastructure, including tracks and bridges, as well as damage to or complete loss of part of the traction rolling stock of Ukrzaliznytsia and other railway operators. At the

same time, alternative routing approaches remain insufficiently explored due to the limited number of studies devoted to strategic management of transportation processes.

This paper describes the development and implementation of a software model of railway system operations aimed at enabling experimental investigation of various hypotheses regarding alternative routing approaches. This provides a basis for solving a scientific and applied problem of optimizing freight rail transportation through the design of flexible management strategies. The study is based on a synthesis of graph theory (representation of the network as a weighted multidigraph), discrete-event simulation (DES) for analyzing process dynamics, and mixed-integer linear programming (MILP) for generating benchmark performance indicators. A hybrid threshold-based dispatching policy is implemented, relying on parameters of minimum train fill level and maximum waiting time, thereby balancing node capacity utilization and delivery times. A specialized simulation framework has been developed in Python that integrates the event lifecycle (Spawn, Form, Depart, Arrive) and enables testing of intelligent control strategies in a simulated environment. The practical significance of the research lies in the possibility of using the developed toolkit for quantitative evaluation of different routing and train formation strategies at classification yards. The created software complex serves as a fundamental platform for further research aimed at minimizing average rolling stock turnaround time and node-related dispatch delays in real logistics systems, thereby improving the economic efficiency of freight transportation.

Keywords: *mathematical modeling, linear programming, discrete-event simulation, implementation of mathematical models, transportation efficiency*

Conflicts of Interest: the authors declare no conflict of interest.

Електронне наукове видання

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА
№ 2(28) 2025

Міжнародний електронний науково-теоретичний журнал

Українською та англійською мовами

Комп'ютерне верстання – Єсіна М.В., Власова В.В.

Підписано до розміщення 30.12.2025. Гарнітура Times New Roman.
Ум. друк. арк. 3,7. Обсяг 4,63 Мб. Зам. № 56/25.

Харківський національний університет імені В. Н. Каразіна,
61022, м. Харків, майдан Свободи, 4.
Свідоцтво суб'єкта видавничої справи ДК № 3367 від 13.01.2009