КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.898
УДК 004.8:004.056:004.94:004.77

**Савченко Тетяна Віталіївна**
Кандидат технічних наук, доцент, доцент кафедри інформатики
Національний університет «Києво-Могилянська академія», Київ, Україна
ORCID ID: 0000-0002-8884-5360
*tsavchenko@ukma.edu.ua*

**Луцька Наталія Миколаївна**
Доктор технічних наук, професор, професор кафедри автоматизації
та комп'ютерних технологій систем управління ім. проф. А.П. Ладанюка
Національний університет харчових технологій, Київ, Україна
ORCID ID: 0000-0001-8593-0431
*lutskanm2017@gmail.com*

**Власенко Лідія Олександрівна**
Кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0000-0002-2003-6313
*vlasenko.lidia1@gmail.com*

**Томенко Наталя Дмитрівна**
Студентка спеціальності «Комп'ютерні науки»
Національний університет «Києво-Могилянська академія», Київ, Україна
*natalia.tomenko@ukma.edu.ua*

# АНАЛІЗ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ АНОМАЛІЙ МЕЖЕВОГО ТРАФІКУ НА ОСНОВІ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ

**Анотація.** У статті представлено підхід до побудови моделі виявлення аномалій в реальному часі в мережевому трафіку типу DoS (Denial of Service) та її інтеграцію в систему моніторингу. Це відкриває нові можливості для візуалізації, дослідження та розробки систем виявлення вторгнень (IDS) та побудови їх цифрових двійників, забезпечуючи гнучку платформу для моделювання кіберфізичних загроз і реагування на них. У роботі синтезовано низку моделей з різними архітектурами нейронних мереж, зокрема, різновиди CNN (Convolutional Neural Networks), LSTM (Long Short-Term Memory) та Autoencoder, проведено порівняння та вибір ефективної моделі для задачі прогнозування аномалій у мережевому трафіку за різнотипними метриками. Обрана модель обмінюється даними з середовищем Node-RED, що реалізує систему моніторингу трафіку та забезпечує графічне представлення результатів виявлення вторгнень, автоматичну реакцію, а також додаткову симуляцію мережевого трафіку. Модель слугує цифровим двійником для системи автоматичного виявлення аномалій. Такий підхід дозволяє розробити прототип системи, який може бути швидко розгорнутий без необхідності у складних обчислювальних ресурсах чи кластерних системах. Важливою особливістю застосованого підходу є поєднання використання сучасних моделей нейронних мереж з логікою автоматичного реагування, що дозволяє наблизити її поведінку до автономної системи захисту, здатної оперативно реагувати на кіберфізичні загрози у реальному часі. Це значно розширює можливості цифрових двійників у сфері навчання, тестування і розвитку сучасних систем кібербезпеки, а також підвищує ефективність досліджень і практичних розробок у галузі захисту інформації. Завдяки представленому рішенню відкриваються перспективи подальшої інтеграції складних моделей глибокого навчання, гібридних архітектур та систем автоматичного моніторингу мережевого трафіку.

**Ключові слова:** виявлення аномалій; нейронні мережі; мережевий трафік; машинне навчання; цифровий двійник; атаки типу DoS; модель; Node-RED.

## ВСТУП

У сучасному кіберпросторі ефективне виявлення аномалій у мережевому трафіку набуває ключового значення з огляду на широкий спектр загроз — від DoS-атак до складних кіберпроникнень [1]. Традиційні сигнатурно-статистичні методи втрачають ефективність у середовищах з великими обсягами даних і новими, раніше невідомими типами атак [2]. Це спричиняє підвищений інтерес до інтелектуальних моделей виявлення, зокрема, нейронних мереж, що здатні виявляти нетипові просторово-часові патерни в трафіку [3].

У межах сучасних досліджень дедалі більша увага приділяється застосуванню глибоких нейронних мереж для виявлення відхилень від нормального функціонування системи. Зокрема, рекурентні архітектури (LSTM, GRU) демонструють високу ефективність при обробці послідовних часових даних, характерних для мережевого трафіку. Згорткові нейронні мережі, в свою чергу, дозволяють ефективно витягати локальні просторові патерни, особливо корисні при обробці агрегаційних характеристик трафіку.

Особливу нішу займають автоенкодери, що використовуються для моделювання нормальної поведінки системи із подальшою детекцією аномалій на основі відновлювальної помилки. Такий підхід активно вивчається і довів свою ефективність на широкому спектрі задач, включно з аналізом індустріального трафіку.

Паралельно із розвитком моделей, концепція цифрового двійника (Digital Twin) набула значної популярності як платформа для моделювання, симуляції та тестування поведінки складних об’єктів у безпечному середовищі. В контексті кібербезпеки цифрові двійники дозволяють емулювати атаки, аналізувати реакцію системи та перевіряти ефективність алгоритмів виявлення аномалій [4]. Окремі дослідження розглядають інтеграцію цифрових двійників у системи виявлення вторгнень (IDS).

Також варто відзначити дослідження у сфері гібридних моделей, які поєднують CNN і LSTM для виявлення як просторових, так і часових залежностей. Такі підходи підтвердили свою ефективність в умовах високої складності трафіку та необхідності моделювання динамічних змін.

Підхід, що використовується в даному дослідженні, також спирається на принцип контекстуального виявлення аномалій, коли оцінка відхилення здійснюється з урахуванням часових вікон і попереднього контексту поведінки системи.

Усі ці концепти поєднано у підході, де цифровий двійник слугує інтерактивною платформою, а нейромережева модель забезпечує інтелектуальний аналіз даних з метою виявлення відхилень. Такий симбіоз дозволяє проводити імітаційне моделювання атак, оцінку реакції системи та перевірку алгоритмів у контрольованому середовищі.

**Постановка проблеми.** Зростання складності та масштабованості інформаційно-комунікаційних систем, а також розширення поверхні атак в умовах цифрової трансформації створюють критично важливі потреби у своєчасному та точному виявленні аномальної активності. Традиційні системи вторгнень (IDS), що базуються на сигнатурному аналізі, не здатні виявляти нові або модифіковані атаки, які не мають заздалегідь визначених шаблонів. У цьому контексті моделі на основі глибокого навчання, зокрема, нейронні мережі типу CNN, LSTM, GRU та Autoencoder, демонструють значні переваги у виявленні складних аномальних патернів. Крім того, перспективним напрямом є інтеграція Digital Twins з нейромережевими моделями, що дозволяє в режимі реального часу симулювати поведінку систем, ідентифікувати потенційні відхилення та оцінювати ризики.

В науковій літературі спостерігається активний розвиток досліджень на перетині глибокого навчання, кібербезпеки та цифрових двійників. Проте, комплексні рішення, що поєднують ці підходи у єдину платформу моніторингу та виявлення аномалій, залишаються недостатньо реалізованими, зокрема, з позиції обчислювальної ефективності та адаптації до нових середовищ [5] – [7].

**Аналіз останніх досліджень і публікацій.** Сучасні мережі генерують великі обсяги різнорідних даних у режимі реального часу, що вимагає адаптивних та інтелектуальних методів аналізу. Нейронні мережі (включаючи архітектури CNN, LSTM, автокодувальники) демонструють високий потенціал у виявленні складних закономірностей і нетипові поведінки в мережевому трафіку [8]. Наприклад, у роботі [9] запропонований contractive autoencoder для виявлення DDoS-атак з точністю до 97 % на датасеті CIC-DDoS та до 96 % на NSL-KDD.

А модель CNN-LSTM для IDS [10] показала 95 % точності та виявилася ефективнішою за чисті LSTM чи GRU. У статті [11] представлено модель MHA-Res-PDC, яка об’єднує паралельні згортки з розширеним полем огляду із залишковим навчанням та механізмом multi-head attention, що забезпечує ефективне виокремлення ознак на різних рівнях узагальнення та підвищує точність виявлення аномалій мережевого трафіку.

Одночасно зростає інтерес до цифрових двійників (Digital Twins) як інструменту симуляції та моделювання поведінки мереж або кіберфізичних систем. Наприклад, в роботі [12] описано Snitch Digital Twin, мережу взаємопов’язаних DT для виявлення аномалій на прикладі системи охолодження генератора із кращими результатами, ніж KPCA або OCSVM. У численних дослідженнях, таких як [13], DT застосовується для моніторингу стану інструментів у виробничому процесі в реальному часі, забезпечуючи детекцію зносу та аномального зносу за допомогою вібраційних сигналів.

В роботі [14] розроблено мультиагентське DT-рішення для виявлення аномалій у промислових процесах. У дослідженні, проведеному на криогенно-складському середовищі, було зафіксовано зростання продуктивності на 30 % завдяки ранньому реагуванню на аномальні події. Аналіз LSTM-підходів для технічних систем, що підсилює загальну модель DT-нейронних інтеграцій розглянуто в [15].

На основі проведеного аналізу останніх досліджень та публікацій можна зробити наступні узагальнення та висновки:

- моделі CNN, LSTM, автокодувальники успішно детектують аномалії із точністю 95–97 %, особливо у складних мережевих та критичних середовищах;
- цифрові двійники забезпечують симуляцію, яка дозволяє генерацію тренувальних даних, раннє виявлення аномалій і порівняння моделей з традиційними методами;
- гібридні моделі (DT + нейронна мережа) демонструють пріоритетну точність над методами KPCA, OCSVM та класичними ML-підходами;
- онлайн-моніторинг у реальному часі можливий за допомогою DT-систем з адаптивною самонавчальною здатністю (наприклад, TWIN-ADAPT).

У межах даного дослідження теоретичним підґрунтям слугує концепція виявлення аномалій як методу ідентифікації відхилень від нормальної поведінки системи, що не відповідають її типовим шаблонам або розподілу даних. У сфері кібербезпеки, зокрема, в аналізі мережевого трафіку, аномалії можуть сигналізувати про несанкціоновану активність, вторгнення або збої у роботі системи. Центральною ідеєю інтегрованого підходу є синтез нейронних мережевих архітектур із концепцією цифрового двійника з метою побудови інтелектуальної системи виявлення аномалій у мережевому трафіку.

Загалом, комплексна інтеграція цифрового двійника та нейронної мережі дозволяє реалізувати підхід, що забезпечує безперервне спостереження, аналіз та реагування на аномальні явища в мережевому середовищі. Така система може динамічно адаптуватися до нових загроз, тестувати оновлені моделі в ізольованому середовищі та підвищувати надійність і точність виявлення порушень.

**Мета статті.** Метою даної статті є дослідження ефективності архітектур нейронних мереж у контексті виявлення аномалій в умовах цифрового моделювання (Digital Twin), а також інтеграція таких моделей у прототип системи виявлення вторгнень у середовищі Node-RED. Для досягнення цієї мети вирішуються наступні завдання: аналіз сучасних підходів до виявлення аномалій на основі глибокого навчання та дослідження ефективності різних архітектур нейромереж; реалізація цифрового двійника симульованої мережі з генератором трафіку та умовною атакою типу DoS; впровадження нейромережевого механізму прогнозування аномалій у середовищі Node-RED та розробка автоматичної реакції на виявлення аномалії.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Методичний підхід у даному дослідженні передбачає багаторівневу експериментальну процедуру побудови моделі виявлення аномалій в середовищі програмування Python, а потім випробовування та перевірку моделі у реальному часі у середовищі Node-RED. Основною метою є оцінка здатності різних моделей глибокого навчання виявляти аномалії у мережевому трафіку в умовах, наближених до реальних.

Кінцеву систему виявлення аномалій у мережевому трафіку реалізовано у-середовищі Node-RED, яке використано як візуальну платформу для створення цифрового двійника мережевого середовища. Node-RED дозволяє інтегрувати обробку даних, імітацію трафіку, візуалізацію на Dashboard, а також запуск моделі машинного навчання через спеціалізовані функціональні вузли. Такий підхід відповідає сучасним рекомендаціям щодо побудови експериментальних цифрових копій для тестування безпеки.

Для розробки моделей використовувалися Python-модулі для машинного навчання. Після навчання, ці моделі були розгорнуті як REST API-сервіси за допомогою таких фреймворків, як TensorFlow Serving або TorchServe. Це дозволило інтегрувати їх у середовище моніторингу Node-RED, де вони використовуються для аналізу трафіку, представленого у вигляді часових рядів. Крім того, для тестування та симуляції були розроблені вбудовані JavaScript-симулятори, які імітують поведінку навченої нейромережі, дозволяючи моделювати як нормальний, так і аномальний трафік.

### 1. Розробка моделі машинного навчання

Нейронні мережі у контексті виявлення аномалій розглядаються як адаптивні нелінійні моделі, здатні до автоматичного вилучення та узагальнення ознак з високорозмірних і гетерогенних даних. Вони характеризуються здатністю моделювати складні залежності, що не піддаються класичним статистичним методам, та адаптуватися до змін у структурі вхідних потоків.

Ключовими перевагами нейронних мереж у цій сфері є: висока чутливість до прихованих патернів у даних, що знижує рівень пропущених аномалій; стійкість до шуму у вхідних потоках, особливо при використанні регуляризаційних технік та ансамблевих підходів; можливість масштабування на великі обсяги даних у режимі реального часу за рахунок оптимізованих алгоритмів обчислення; інтеграція з цифровими двійниками, що дозволяє проводити симуляційне тестування сценаріїв аномальної поведінки без ризику

для продуктивного середовища. Завдяки цим характеристикам нейронні мережі стають фундаментальним інструментом у сучасних системах кіберзахисту, дозволяючи реалізувати як превентивні, так і реактивні механізми виявлення загроз.

Для дослідження обрано три класи архітектур: GRU Autoencoder — для виявлення відхилень від нормальної поведінки через відновлювальну помилку; Deep CNN — для вилучення просторових ознак на фіксованому вікні трафіку; Bidirectional LSTM — для глибокого захоплення часових залежностей в обох напрямках. Ці архітектури демонструють високу точність у попередніх дослідженнях, що обґрунтовує їх вибір як базових для експериментального порівняння.

В рамках дослідження створено імітаційну модель генерації трафіку з двома станами: нормальний режим (випадкові значення в діапазоні 50–150) та режим атаки (DoS) (пікові значення 500–1000). Ці дані нормалізувалися до [0, 1] та подавалися на вхід моделі. Для оцінювання використовувались часові вікна розміром 10 секунд, що забезпечує достатній контекст для аналізу. У тестах використано попередньо оброблені дані з наборів NSL-KDD та UNSW-NB15, які широко застосовуються у дослідженнях мережевої безпеки.

Для вимірювання ефективності виявлення аномалій застосовано наступні метрики: F1 Score; ROC AUC; Precision / Recall; Latency прогнозу (ms) — для оцінки реального часу виявлення мережевих загроз.

Для перевірки адаптивності моделей використовувалося трансферне навчання — моделі, натреновані на NSL-KDD, були протестовані на UNSW-NB15 без або з мінімальним донавчанням. UNSW-NB15 містить сучасніші та складніші типи атак, а також більш реалістичні характеристики трафіку порівняно з NSL-KDD. Такий підхід з використанням трансферного навчання дозволив оцінити здатність моделей узагальнювати знання, отримані на одному наборі даних, на абсолютно новий та динамічний мережевий ландшафт без або з мінімальним донавчанням.

## 2. Результати розробки та тестування моделі

У межах дослідження проведено оцінку ефективності розроблених моделей виявлення аномалій у мережевому трафіку. Детальний аналіз отриманих даних дозволяє ідентифікувати найбільш продуктивні архітектури для поставленої задачі, проаналізувати їхні характерні особливості та зробити висновки щодо їхньої адаптивності та здатності до узагальнення на нові, невидимі дані.

### 2.1. Навчання та перевірка початкової моделі на даних NSL-KDD

Навчання розглянутих архітектур здійснювалося виключно на наборі даних NSL-KDD. Цей етап навчання дозволив моделям сформувати базові уявлення про патерни мережевого трафіку та різноманітні аномалії, присутні в даних. Моделі вивчали особливості нормального функціонування мережі та різних типів атак, закладаючи основу для подальшої перевірки їхньої здатності до узагальнення.

Таблиця 1 демонструє порівняльні показники ефективності різних архітектур моделей на тестовому наборі даних NSL-KDD. GRU Autoencoder показав виняткову продуктивність, значно перевершуючи всі інші архітектури за основними метриками. Він досяг найвищого F1-score (98,5%), Precision (97,3%), Recall (99,8%) та ROC AUC (99,1%). Це підтверджує його найкращу загальну дискримінаційну здатність та ефективність у виявленні аномалій з мінімальною кількістю хибних спрацьовувань.

Серед інших моделей, автоенкодери загалом продемонстрували найвищу ефективність. Dense Autoencoder (F1-score 91,8%, Recall 95,3%) та CNN Autoencoder (F1-score 91,1%, Recall 97,0%) також показали високі результати, поступаючись лише GRU

Autoencoder. Їхня здатність навчатися на нормальних даних робить їх особливо цінними для виявлення невідомих типів аномалій.

CNN-архітектури, зокрема Deep CNN (F1-score 90,9%), виявилися ефективними у виявленні локальних патернів та демонстрували високу Precision (Residual CNN — 89,2%, Deep CNN — 89,1%), що важливо для мінімізації хибних спрацьовувань. Однак за загальними показниками вони поступаються передовим автоенкодерам.

LSTM-архітектури показали нижчу загальну ефективність порівняно з CNN та автоенкодерами, з F1-score в діапазоні 87,0–88,4%. Серед них Bidirectional LSTM (F1-score 88,4%) виявився кращим, підкреслюючи переваги двонаправленого контексту. Примітно, що стандартна GRU модель, незважаючи на високий Recall (91,7%), мала значно нижчу Precision (85,1%) порівняно з GRU Autoencoder.

*Таблиця 1*

**Порівняння результатів CNN моделей на тестовій вибірці NSL-KDD**

| Архітектура нейронної мережі | Optimal Threshold | Precision | Recall | F1 | ROC AUC |
|---|---|---|---|---|---|
| Базова CNN | 0,004 | 88,7% | 91,9% | 90,2% | 93,0% |
| Deep CNN | 0,035 | 89,1% | 92,9% | 90,9% | 93,1% |
| Residual CNN | 0,003 | 89,2% | 90,0% | 89,6% | 92,4% |
| Basic LSTM | 0,0006 | 87,9% | 87,4% | 87,7% | 89,6% |
| Bidirectional LSTM | 0,0024 | 87,4% | 89,5% | 88,4% | 92,4% |
| GRU | 0,0003 | 85,1% | 91,7% | 88,3% | 91,4% |
| LSTM with Attention | 0,0039 | 86,3% | 87,8% | 87,0% | 89,4% |
| Dense Autoencoder | 0,1190 | 88,5% | 95,3% | 91,8% | 93,4% |
| CNN AE Autoencoder | 0,0055 | 85,9% | 97,0% | 91,1% | 95,3% |
| GRU Autoencoder | 0.4386 | 97,3% | 99,8% | 98,5% | 99,1% |

Оптимальні пороги класифікації суттєво варіюються між моделями, наприклад, 0,0003 для стандартної GRU та 0,4386 для GRU Autoencoder. Це вказує на важливість адаптивного вибору порогу для кожної архітектури та потенційно свідчить про різний характер розподілу помилок реконструкції, що робить автоенкодери більш стабільними.

### 2.2. Дослідження узагальнення розробленої моделі

На наступному кроці моделі були протестовані на наборі даних UNSW-NB15, що представляє сучасніші та реалістичніші сценарії мережевих атак. Це тестування виконувалося або без додаткового донавчання на UNSW-NB15, або з мінімальним донавчанням, що дозволило оцінити здатність попередньо навчених моделей узагальнювати набуті знання та ефективно виявляти аномалії в абсолютно новому домені без значних адаптацій.

Для експерименту були обрані ті моделі з кожної архітектури, що показали найкращі F1 Score та ROC AUC при тестуванні на наборі NSL-KDD (табл. 1) — Deep CNN, Bidirectional LSTM, CNN Autoencoder та GRU Autoencoder. Для вирішення

проблеми різної розмірності вхідних даних між NSL-KDD та UNSW-NB15, для кожної архітектури були розроблені спеціальні адаптаційні шари або модифіковані структури, що дозволило моделям працювати з 183 ознаками замість 122, зберігаючи їхню функціональність та семантичну цілісність.

Експеримент з прямим перенесенням моделей (табл. 2), навчених на NSL-KDD, на набір даних UNSW-NB15 без донавчання показав помірну загальну ефективність: F1-score для всіх моделей коливався в діапазоні 0,71-0,72, що значно нижче їхньої продуктивності на оригінальному датасеті. Серед протестованих моделей Bidirectional LSTM продемонструвала найкращу здатність до прямого перенесення з ROC AUC 0,733, що свідчить про її кращу узагальнюючу здатність. При цьому вона показала найбільш збалансовані показники Precision (0,742) та Recall (0,681).

На противагу цьому, моделі CNN та автоенкодери, включаючи Deep CNN, CNN Autoencoder та GRU Autoencoder, виявили тенденцію до дуже високого Recall (понад 0,98), але за рахунок значно нижчої Precision (0,55-0,57). Зокрема, Deep CNN, яка була високоефективною на NSL-KDD, показала найнижчий ROC AUC (0,429) при прямому перенесенні, що вказує на її сильну спеціалізацію на характеристиках навчального датасету. Це свідчить про обмежену ефективність прямого перенесення моделей між різними мережевими середовищами, де рекурентні моделі можуть мати перевагу завдяки здатності моделювати універсальніші часові залежності.

*Таблиця 2*

**Результати тестування моделей на наборі UNSW-NB15 без донавчання**

| Модель | F1 Score | ROC AUC | Precision | Recall | Поріг |
|---|---|---|---|---|---|
| Deep CNN | 0,710 | 0,429 | 0,550 | 1,000 | 0,001 |
| Bidirectional LSTM | 0,710 | 0,733 | 0,742 | 0,681 | 0,473 |
| CNN Autoencoder | 0,719 | 0,522 | 0,565 | 0,988 | 0,057 |
| GRU Autoencoder | 0,710 | 0,594 | 0,551 | 0,999 | 0,069 |

З метою дослідження впливу донавчання та визначення оптимального обсягу даних, було проведено серію експериментів з чотирма найкращими моделями, попередньо навченими на NSL-KDD. Для донавчання використовувалися випадкові вибірки з UNSW-NB15 розміром 1%, 5%, 10%, 25% та 50% від загального обсягу, при цьому застосовувалися однакові гіперпараметри (10 епох, розмір батчу 64, оптимізатор Adam) та адаптаційні шари, розроблені раніше для сумісності з UNSW-NB15.

У рамках експерименту з донавчанням на UNSW-NB15 спостерігається чітка залежність ефективності моделей від обсягу наданих даних (рис. 1). Deep CNN продемонструвала найбільш виражену адаптацію: її F1-score зріс з 0,710 до 0,845 при збільшенні даних для донавчання з 1 % до 5 %, досягаючи максимуму F1-score 0,878 та ROC AUC 0,952 при 20 % даних. Це вказує на значний потенціал моделі при оптимальній кількості даних, однак подальше збільшення обсягу донавчання (понад 20%) призводило до нелінійного погіршення метрик, що може свідчити про перенавчання.

Bidirectional LSTM виявилася найбільш ефективною та стабільною архітектурою, демонструючи високу базову трансферність навіть з 1 % даних (F1-score 0,96, ROC AUC 0,989) та поступове зростання F1-score до максимуму 0,981 при 20 % даних. Її висока Precision та Recall (>0,94) для всіх обсягів донавчання підтверджує ефективне виявлення

ISSN 2663 - 4023

аномалій зі збалансованими показниками. На противагу цьому, CNN Autoencoder та GRU Autoencoder показали обмежене покращення метрик при збільшенні обсягу даних та зберегли характерну високу повноту (Recall > 0.93) при низькій точності (Precision ~0,55–0,62), що вказує на їхню схильність до хибних спрацьовувань та обмежену адаптацію через донавчання.

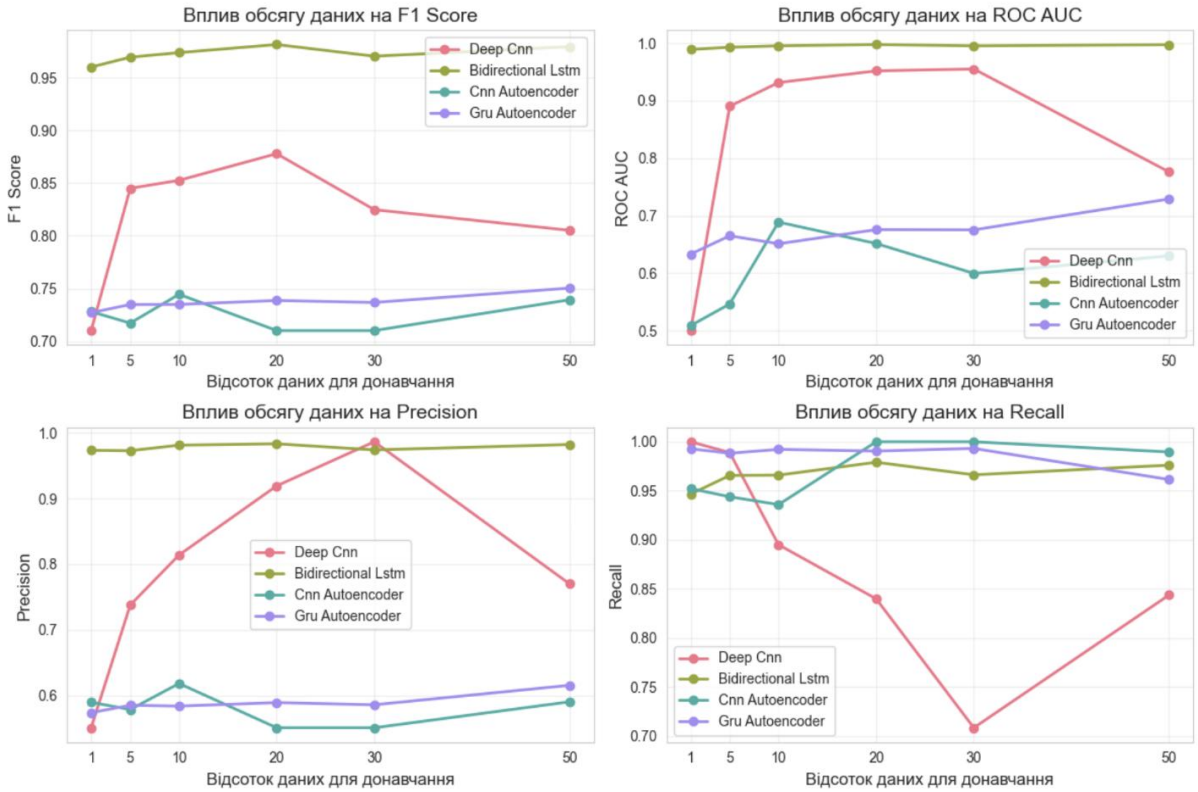


*Рис. 1. Результати експерименту з донавчанням моделей на різних обсягах даних*

### 2.3. Оцінка обчислювальної ефективності моделей

Оцінка обчислювальної ефективності є критично важливою для вибору архітектури нейронної мережі у системах виявлення аномалій, особливо для застосувань у реальному часі. Для всебічного аналізу було проведено експеримент, що включав визначення параметричної складності моделей (кількість параметрів, розмір), вимірювання швидкості інференсу (час обробки одиничного зразка та пакету, ефективність розпаралелювання) та оцінку швидкості навчання (час донавчання на обмеженій вибірці, середній час на епоху).

З аналізу обчислювальної ефективності (рис. 2) та продуктивності (рис. 1) виявлено, що найбільш збалансованою архітектурою є Bidirectional LSTM, яка демонструє високу точність виявлення аномалій та середню швидкість інференсу на одиничний зразок, незважаючи на найбільший розмір моделі та найдовший час навчання. CNN Autoencoder є найефективнішою за розміром (0,07 МБ) та швидкістю інференсу, включаючи пакетну обробку, проте її результати виявлення аномалій є посередніми. Для обробки в реальному часі оптимальною вважається Deep CNN, що забезпечує найкращий час пакетної обробки та має хорошу адаптаційну здатність через донавчання, хоча є повільнішою при обробці одиничних зразків. GRU Autoencoder виявився найефективнішим для частого донавчання завдяки найшвидшому часу навчання (0,735 сек/епоха) та компактному розміру (0,13 МБ),

проте його попередня обмежена здатність до адаптації через донавчання ставить під сумнів доцільність такого підходу.

Проведене дослідження трансферності нейромережевих моделей виявлення аномалій виявило, що рекурентні архітектури на основі LSTM, зокрема, Bidirectional LSTM, демонструють виняткову здатність до трансферу як без донавчання (F1-score 71,05%), так і з мінімальним донавчанням (F1-score 95,99% з 1% даних), що свідчить про їхню ефективність у моделюванні універсальних часових залежностей. Натомість, згорткові архітектури (CNN) потребують суттєвого донавчання (близько 20% даних) для ефективної адаптації, тоді як автоенкодери (CNN та GRU варіанти) виявляють обмежену здатність до трансферу, що вказує на їхню сильну залежність від розподілу нормальних даних у навчальній вибірці. Загалом, трансферність архітектури не корелює безпосередньо з її початковою ефективністю на оригінальному датасеті; рекурентні моделі забезпечують оптимальний баланс між точністю та обчислювальною складністю для одиничних зразків, тоді як CNN краще підходять для пакетної обробки, а автоенкодери, попри компактність та швидкість навчання (особливо GRU Autoencoder), показали гірші показники точності при трансфері.

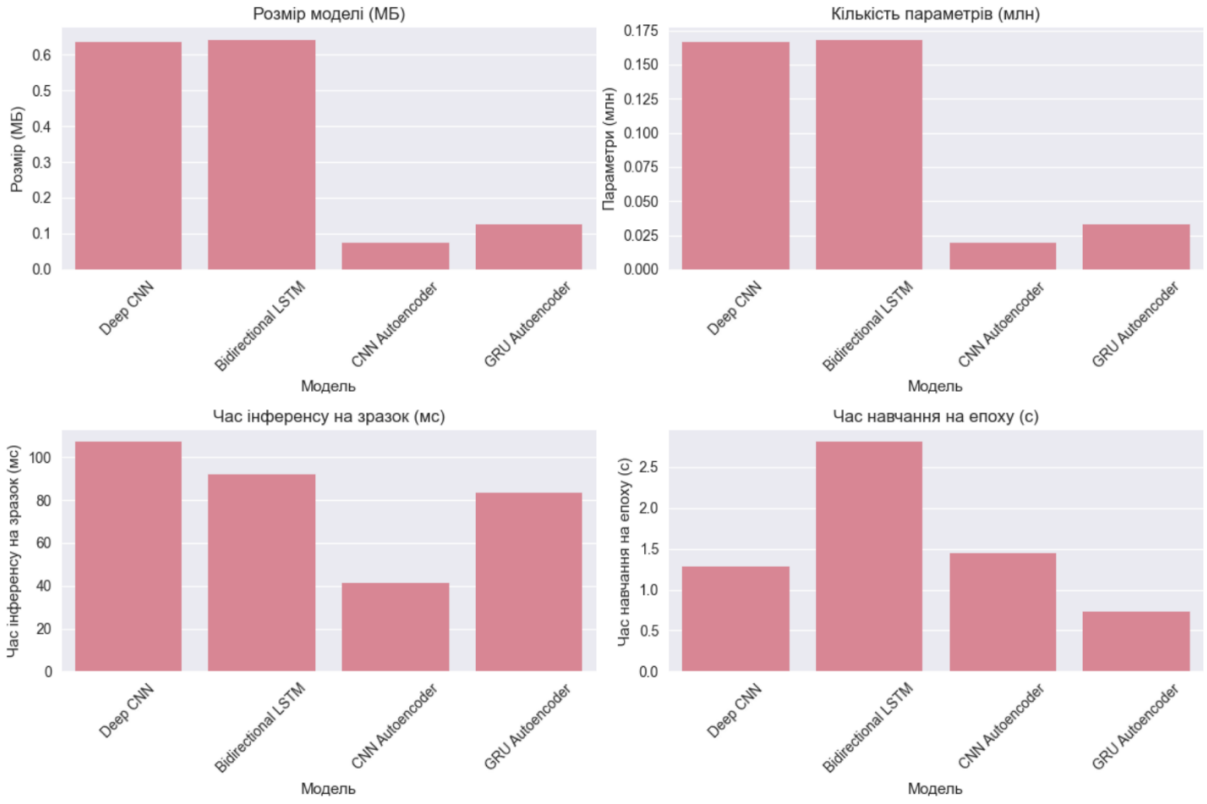


*Рис. 2. Результати експерименту з обчислювальної ефективності моделей*

### 3. Побудова системи виявлення аномалій

На етапі фінальної перевірки ефективності розробленої моделі виявлення аномалій було використано середовище Node-RED як інтеграційну платформу для моделювання реального мережевого трафіку, візуалізації результатів та автоматичної реакції на виявлені загрози. Node-RED — це інструмент візуального програмування, орієнтований на обробку потоків даних (flow-based programming), який дозволяє швидко реалізовувати сценарії взаємодії між різними джерелами даних, сервісами та пристроями.

Тренована модель нейронної мережі для виявлення аномалій була підключена до Node-RED через REST API-інтерфейс. Потоки трафіку, що надходили з тестового середовища, в реальному часі оброблялися моделлю та повертали прогноз ймовірності аномалії.

Для імітації мережевого навантаження використовувалися генератори даних, що відтворювали як звичайний трафік, так і різні типи атак (DoS, Probe, R2L, U2R). Це дозволяло перевірити стабільність роботи моделі в умовах змінного та потенційно зашумленого потоку даних.

У симуляційному середовищі реалізовано повний цикл: генерація трафіку; попередня обробка (нормалізація, агрегування); подавання на вхід моделі; отримання прогнозу (імовірність аномалії); автоматична реакція системи (візуальна індикація, тривога, логування); побудова графіків для моніторингу.

Реалізація реактивної частини дозволяє протестувати **елементи автономної безпеки**, що відповідає концепції *self-healing systems.*

Для представлення результатів валідації використовувалися графічні віджети Node-RED Dashboard:

- лінійні графіки для відображення зміни ймовірності аномалії у часі;
- інтерактивні Gauge-індикатори для демонстрації поточного рівня ризику;
- таблиці для фіксації подій та типів виявлених аномалій.
- У разі перевищення встановленого порогового значення ймовірності аномалії (<0,85) Node-RED автоматично виконував одну або кілька реакцій:
- надсилання повідомлення оператору безпеки;
- генерація події в системі SIEM для подальшого аналізу;
- ініціація блокування підозрілої IP-адреси на рівні брандмауера.

У процесі тестування було зібрано статистику роботи моделі, а саме метрики продуктивності в умовах потокової обробки даних. Порівняння цих показників із результатами офлайн-тестування підтверджує стабільність та відтворюваність моделі.

При виборі оптимальної нейромережевої архітектури для системи виявлення мережевих аномалій, що реалізується на платформі Node-RED, слід враховувати низку специфічних вимог та обмежень. Серед ключових факторів — характер аномалій та типів даних, оскільки точкові аномалії ефективніше виявляються автоенкодерами, тоді як контекстуальні потребують рекурентних мереж. Важливою є стабільність мережевого середовища: для динамічних умов, де часто змінюються характеристики трафіку, потрібна висока адаптивність моделі. Доступність розмічених даних впливає на вибір підходу: за їх відсутності або обмеженої кількості перевага надається автоенкодерам, тоді як великий обсяг даних дозволяє застосовувати класифікаційні моделі. Крім того, співвідношення важливості хибних спрацювань та пропущених аномалій диктує вибір моделі з високим Recall (автоенкодери) або Precision (CNN). Нарешті, обчислювальні ресурси та вимоги до швидкодії є критичними для Node-RED, де можуть бути обмежені ресурси та потреба у високій пропускній здатності для систем реального часу.

На основі проведених досліджень та з урахуванням специфіки Node-RED, рекомендується використовувати архітектуру Bidirectional LSTM для центрального модуля виявлення аномалій. Ця модель продемонструвала найкращі показники трансферності та адаптації навіть за умови мінімального донавчання (1–5% даних), що є критично важливим для динамічних мережевих середовищ та може компенсувати потенційні обмеження Node-RED щодо масованої пакетної обробки. Bidirectional LSTM ефективно виявляє контекстуальні аномалії завдяки своїй здатності моделювати часові залежності в обох напрямках. Незважаючи на більший час навчання порівняно з деякими іншими архітектурами, її висока точність та збалансований Recall і Precision роблять її

ISSN 2663 - 4023

надійним вибором, особливо з урахуванням можливості періодичного донавчання. Для інтеграції в Node-RED необхідно розробити адаптаційні шари (наприклад, TimeDistributed Dense) для узгодження розмірності вхідних даних, а також розглянути стратегії асинхронної обробки або використання окремих мікросервісів для керування інференсом моделі, щоб не перевантажувати основний потік Node-RED.

Таким чином, використання **Node-RED** дозволяє провести **операційну валідацію** моделі в умовах, максимально наближених до реальної експлуатації, забезпечивши комплексну перевірку її роботи, швидку інтеграцію з інфраструктурою та можливість автоматизованого реагування на виявлені аномалії.

**4. Реалізація та перевірка системи**

В рамках дослідження було створено функціональну імітаційну систему виявлення аномалій, що відтворює поведінку мережевого трафіку у цифровому середовищі. Основною метою було моделювання поведінки нейромережевого детектора аномалій у системі реального часу із візуалізацією на інтерактивній панелі.

Реалізація моделі Bidirectional LSTM для виявлення аномалій на Node-RED вимагає кількох ключових кроків, оскільки Node-RED сам по собі не є середовищем для прямого розгортання моделей глибокого навчання, навчених у фреймворках на кшталт TensorFlow або PyTorch. Замість цього, Node-RED виступає як платформа для інтеграції, Orchestration та взаємодії з такими моделями, що працюють як зовнішні сервіси. Загальний підхід до реалізації та розгортання моделі LSTM зображено на рис. 3.

У процесі розроблення та впровадження системи виявлення аномалій на основі моделі Bidirectional LSTM, інтегрованої у середовище Node-RED, особливу увагу необхідно приділити низці технічних аспектів, що безпосередньо впливають на ефективність та надійність її функціонування. Для забезпечення роботи в умовах реального часу критично важливо оптимізувати API-сервіс для швидкого інференсу, що передбачає розгортання на високопродуктивному апаратному забезпеченні та використання спеціалізованих оптимізованих фреймворків, таких як TensorFlow Serving або TorchServe, що забезпечують мінімальну затримку обробки запитів.


*Рис. 3. Процес розгортання моделі LSTM*

Система стабільно моделює дві події: нормальний трафік та DoS-атаку (рис. 4). Коли відбувається перехід за поріг значення > 0,7 (умовна ймовірність), відбувається автоматична реакція: виводиться попередження: «Виявлено аномалію!»; змінюється колір індикатора; зростає значення на графіку Gauge; записується час події. Це відповідає базовим вимогам до системи виявлення аномалій: виявлення, інформування, реакція.

Завдяки оновленню кожні 5 секунд та відображенню на графіку в реальному часі, система дозволяє відслідковувати динаміку трафіку та зміну ймовірності аномалії, що є важливим критерієм для сценаріїв живого моніторингу. Сценарій багаторазово протестовано з різними типами вхідного трафіку. Результати повторювані, логіка реакції зберігається. Це свідчить про стійкість моделі до базових варіацій вхідних даних.

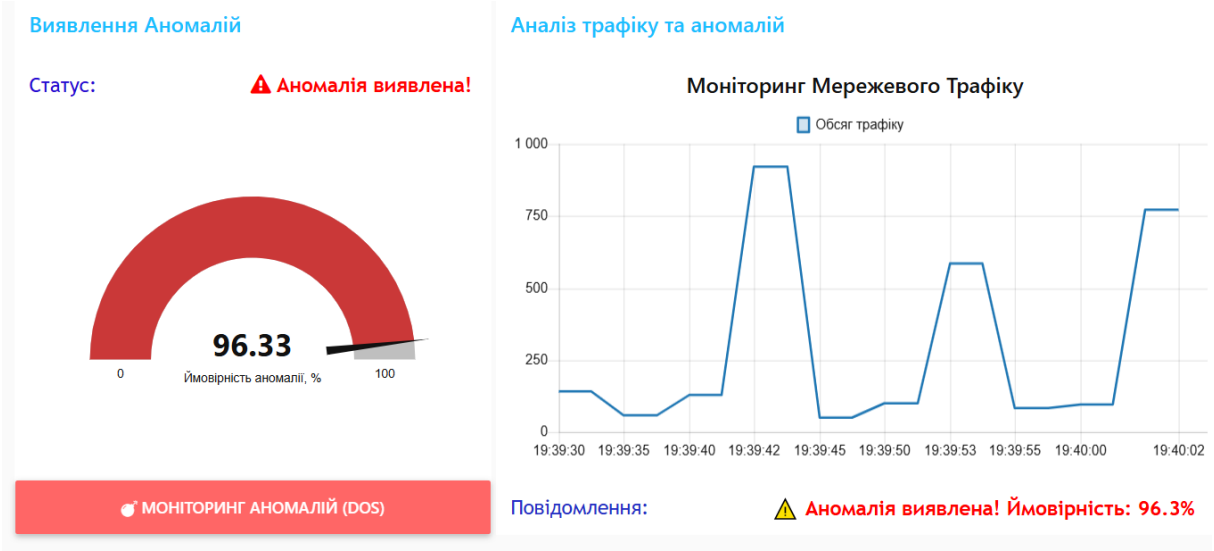


*Рис. 4. Екран моніторингу системи виявлення аномалій (**Node-RED**)*

У випадках очікуваного високого навантаження доцільно застосовувати технології контейнеризації (*Docker*) та оркестрації (*Kubernetes*) для підтримки горизонтального та вертикального масштабування системи, підвищення її відмовостійкості та безперервності функціонування.

API-сервіс, що забезпечує взаємодію моделі з користувацькими або проміжними системами, має бути захищений шляхом впровадження автентифікаційних механізмів (наприклад, API-ключів, токенів доступу), з метою запобігання несанкціонованому доступу та потенційним кіберзагрозам.

Необхідно впровадити систему моніторингу як для середовища Node-RED, так і для API-сервісу з метою безперервного контролю за станом компонентів, аналізу показників продуктивності та своєчасного виявлення можливих відхилень або збоїв.

Застосування зазначених підходів дозволяє інтегрувати модель Bidirectional LSTM у візуально орієнтовану архітектуру Node-RED з високим рівнем адаптивності, забезпечуючи при цьому стабільність, масштабованість та захист системи в умовах реального часу.

Отримані результати демонструють ефективність застосування цифрового двійника мережевого трафіку як платформи для моделювання системи виявлення аномалій на основі нейронних мереж. Імітаційна модель, реалізована у середовищі Node-RED, успішно відтворює ключові функції системи — генерацію даних, їх обробку, прогноз аномалій та автоматичну реакцію, наприклад, відправку сповіщення

адміністратору або блокування підозрілого IP-адресу. Важливо відзначити, що реалізація на Node-RED робить систему гнучкою та простою для інтеграції з реальними даними та зовнішніми ML-сервісами, що відкриває перспективи подальшої автоматизації та оптимізації процесів виявлення аномалій.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У межах даного дослідження здійснено комплексну оцінку систем виявлення аномалій на основі нейронних мереж з фокусом на мережевий трафік. Теоретичний аналіз дозволив систематизувати підходи до класифікації аномалій, вивчити архітектури CNN, RNN, Autoencoder та GRU Autoencoder, а також дослідити їх застосування до задач виявлення відхилень у поведінці мережі.

У практичній частині дослідження реалізовано цифровий двійник системи виявлення аномалій у середовищі Node-RED. Модель демонструє автоматичну реакцію на виявлені аномалії, побудову графіків, зміну індикаторів та повідомлень, а також відображає процес ухвалення рішень на основі ймовірнісного прогнозу, що забезпечує візуалізацію складних процесів виявлення аномалій у простій, інтерактивній формі.

Розроблений симулятор відображає ключові результати теоретичного аналізу та демонструє їхню застосовність у побудові інтелектуальних систем. Отримані експериментальні результати підтверджують високу ефективність GRU Autoencoder і Deep CNN у задачах виявлення аномалій, що співвідноситься з точністю системи, змодельованої у Node-RED.

Таким чином, робота підтверджує доцільність застосування цифрових двійників у сучасних задачах кібербезпеки, поєднуючи симуляцію, машинне навчання та автоматизовані реакції в єдину інтегровану платформу, що сприяє підвищенню якості навчання, досліджень і практичних розробок у галузі захисту інформаційних систем.

Перспективами подальших досліджень передбачається: інтеграція реальних моделей нейронних мереж (CNN, LSTM, Autoencoder) у цифровий двійник з автоматичним навчанням і оновленням; тестування цифрового двійника на реальних потоках мережевого трафіку із широким спектром атак; використання цифрових двійників для побудови комплексних систем кіберзахисту з прогнозуванням і попередженням аномалій.

## ПОДЯКА

This work was supported by a grant from the Simons Foundation (SFI-PD-Ukraine-00014577; T.S.).

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Skladannyi, P., Kostiuk, Y., Rzaeva, S., Samoilenko, Y., & Savchenko, T. (2025). Development of modular neural networks for detecting different classes of network attacks. *Cybersecurity: Education, Science, Technique*, *3*(27), 534–548. https://doi.org/10.28925/2663-4023.2025.27.772
2. Bondarchuk, A. P., & Zhebka, V. V. (2023). Protection of a heterogeneous telecommunication network from the influence of destabilizing factors. *Telecommunication and Information Technologies*, *78*(1). https://doi.org/10.31673/2412-4338.2023.010416

3. Haidur, H. I., Gakhov, S. O., & Bryhynets, A. A. (2023). Detection of network anomalies with neural networks algorithms. *Telecommunication and Information Technologies*, *78*(1). https://doi.org/10.31673/2412-4338.2023.016173
4. Savchenko, T., Lutska, N., Vlasenko, L., Sashnova, M., Zahorulko, A., Minenko, S., Ibaiev, E., & Tytarenko, N. (2025). Risk analysis and cybersecurity enhancement of Digital Twins in dairy production. *Technology audit and production reserves*, *2(2(82))*, 37–49. https://doi.org/10.15587/2706-5448.2025.325422
5. da Silva Ruffo, V. G., Brandão Lent, D. M., Komarchesqui, M., Schiavon, V. F., de Assis, M. V. O., Carvalho, L. F., & Proença, M. L. (2024). Anomaly and intrusion detection using deep learning for software-defined networks: A survey. *Expert Systems With Applications*, *256*, 124982. https://doi.org/10.1016/j.eswa.2024.124982
6. Yin, F., He, B. (2021). Cascaded fault detection system of error back-propagation network based on node association degree. *Computer Communications*, *175*, 142–149. https://doi.org/10.1016/j.comcom.2021.04.011
7. Ullah, W., Hussain, T., Khan, Z. A., Haroon, U., & Baik, S. W. (2022). Intelligent dual stream CNN and echo state network for anomaly detection. *Knowledge-Based Systems*, 109456. https://doi.org/10.1016/j.knosys.2022.109456
8. Dong, S., Su, H., & Liu, Y. (2022). A-CAVE: Network abnormal traffic detection algorithm based on variational autoencoder. *ICT Express*. https://doi.org/10.1016/j.icte.2022.11.006
9. Aktar, S., & Yasin Nur, A. (2023). Towards DDoS Attack Detection using Deep Learning Approach. *Computers & Security*, 103251. https://doi.org/10.1016/j.cose.2023.103251
10. Bamber, S. S., Katkuri, A. V. R., Sharma, S., & Angurala, M. (2024). A Hybrid CNN-LSTM Approach for Intelligent Cyber Intrusion Detection System. *Computers & Security*, 104146. https://doi.org/10.1016/j.cose.2024.104146
11. Qi, G., Mao, J., Huang, K., You, Z., & Lin, J. (2024). Multi-Head attention enhanced parallel dilated convolution and residual learning for network traffic anomaly detection. *Computers, Materials & Continua*, 1–10. https://doi.org/10.32604/cmc.2024.058396
12. Calvo-Bascones, P., Voisin, A., Do, P., & Sanz-Bobi, M. A. (2023). A collaborative network of digital twins for anomaly detection applications of complex systems. snitch digital twin concept. *Computers in Industry*, *144*, 103767. https://doi.org/10.1016/j.compind.2022.103767
13. Liu, Z., Lang, Z.-Q., Gui, Y., Zhu, Y.-P., & Laalej, H. (2024). Digital twin-based anomaly detection for real-time tool condition monitoring in machining. *Journal of Manufacturing Systems*, *75*, 163–173. https://doi.org/10.1016/j.jmsy.2024.06.004
14. Latsou, C., Farsi, M., & Erkoyuncu, J. A. (2023). Digital twin-enabled automated anomaly detection and bottleneck identification in complex manufacturing systems using a multi-agent approach. *Journal of Manufacturing Systems*, *67*, 242–264. https://doi.org/10.1016/j.jmsy.2023.02.008
15. Lindemann, B., Maschler, B., Sahlab, N., & Weyrich, M. (2021). A survey on anomaly detection for technical systems using LSTM networks. *Computers in Industry*, *131*, 103498. https://doi.org/10.1016/j.compind.2021.103498

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

**Tetiana Savchenko**
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Informatics
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine
ORCID ID: 0000-0002-8884-5360
*tsavchenko@ukma.edu.ua*

**Nataliia Lutska**
Doctor of Science, Professor,
Professor of the Department of automation and computer technologies
management system named after Prof. A.P. Ladanyuka
National University of Food Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-8593-0431
*lutskanm2017@gmail.com*

**Lidiia Vlasenko**
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-2003-6313
*vlasenko.lidia1@gmail.com*

**Natalia Tomenko**
Student majoring in «Computer Science»
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine
*natalia.tomenko@ukma.edu.ua*

# ANALYSIS OF THE EFFECTIVENESS OF BORDER TRAFFIC ANOMALY DETECTION BASED ON MACHINE LEARNING MODELS

**Abstract.** The article presents an approach to constructing a real-time anomaly detection model for DoS (Denial of Service) network traffic and its integration into a monitoring system. This opens new opportunities for visualization, investigation, and development of intrusion detection systems (IDS) and their digital twins, providing a flexible platform for modeling cyber-physical threats and responding to them. The study synthesizes a range of models with various neural network architectures, including CNN (Convolutional Neural Networks), LSTM (Long Short-Term Memory), and Autoencoder variants, performs a comparative analysis, and selects an effective model for predicting anomalies in network traffic using diverse metrics. The chosen model exchanges data with the Node-RED environment, which implements the traffic monitoring system and provides graphical representation of intrusion detection results, automated responses, and additional network traffic simulation. The model functions as a digital twin of the anomaly detection system. This approach enables the development of a prototype system that can be rapidly deployed without the need for complex computational resources or cluster systems. A key feature of the applied approach is the combination of modern neural network models with automated response logic, which allows its behavior to approximate that of an autonomous protection system capable of responding promptly to cyber-physical threats in real time. This significantly expands the capabilities of digital twins in education, testing, and development of modern cybersecurity systems, while also enhancing the effectiveness of research and practical implementations in the field of information security. The presented solution opens prospects for further integration of complex deep learning models, hybrid architectures, and automated network traffic monitoring systems.

**Keywords:** anomaly detection; neural networks; network traffic; machine learning; digital twin; DoS attacks; model; Node-RED.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Skladannyi, P., Kostiuk, Y., Rzaeva, S., Samoilenko, Y., & Savchenko, T. (2025). Development of modular neural networks for detecting different classes of network attacks. *Cybersecurity: Education, Science, Technique*, *3*(27), 534–548. https://doi.org/10.28925/2663-4023.2025.27.772
2. Bondarchuk, A. P., & Zhebka, V. V. (2023). Protection of a heterogeneous telecommunication network from the influence of destabilizing factors. *Telecommunication and Information Technologies*, *78*(1). https://doi.org/10.31673/2412-4338.2023.010416
3. Haidur, H. I., Gakhov, S. O., & Bryhynets, A. A. (2023). Detection of network anomalies with neural networks algorithms. *Telecommunication and Information Technologies*, *78*(1). https://doi.org/10.31673/2412-4338.2023.016173
4. Savchenko, T., Lutska, N., Vlasenko, L., Sashnova, M., Zahorulko, A., Minenko, S., Ibaiev, E., & Tytarenko, N. (2025). Risk analysis and cybersecurity enhancement of Digital Twins in dairy production. *Technology audit and production reserves*, *2(2(82))*, 37–49. https://doi.org/10.15587/2706-5448.2025.325422
5. da Silva Ruffo, V. G., Brandão Lent, D. M., Komarchesqui, M., Schiavon, V. F., de Assis, M. V. O., Carvalho, L. F., & Proença, M. L. (2024). Anomaly and intrusion detection using deep learning for software-defined networks: A survey. *Expert Systems With Applications*, *256*, 124982. https://doi.org/10.1016/j.eswa.2024.124982
6. Yin, F., He, B. (2021). Cascaded fault detection system of error back-propagation network based on node association degree. *Computer Communications*, *175*, 142–149. https://doi.org/10.1016/j.comcom.2021.04.011
7. Ullah, W., Hussain, T., Khan, Z. A., Haroon, U., & Baik, S. W. (2022). Intelligent dual stream CNN and echo state network for anomaly detection. *Knowledge-Based Systems*, 109456. https://doi.org/10.1016/j.knosys.2022.109456
8. Dong, S., Su, H., & Liu, Y. (2022). A-CAVE: Network abnormal traffic detection algorithm based on variational autoencoder. *ICT Express*. https://doi.org/10.1016/j.icte.2022.11.006
9. Aktar, S., & Yasin Nur, A. (2023). Towards DDoS Attack Detection using Deep Learning Approach. *Computers & Security*, 103251. https://doi.org/10.1016/j.cose.2023.103251
10. Bamber, S. S., Katkuri, A. V. R., Sharma, S., & Angurala, M. (2024). A Hybrid CNN-LSTM Approach for Intelligent Cyber Intrusion Detection System. *Computers & Security*, 104146. https://doi.org/10.1016/j.cose.2024.104146
11. Qi, G., Mao, J., Huang, K., You, Z., & Lin, J. (2024). Multi-Head attention enhanced parallel dilated convolution and residual learning for network traffic anomaly detection. *Computers, Materials & Continua*, 1–10. https://doi.org/10.32604/cmc.2024.058396
12. Calvo-Bascones, P., Voisin, A., Do, P., & Sanz-Bobi, M. A. (2023). A collaborative network of digital twins for anomaly detection applications of complex systems. snitch digital twin concept. *Computers in Industry*, *144*, 103767. https://doi.org/10.1016/j.compind.2022.103767
13. Liu, Z., Lang, Z.-Q., Gui, Y., Zhu, Y.-P., & Laalej, H. (2024). Digital twin-based anomaly detection for real-time tool condition monitoring in machining. *Journal of Manufacturing Systems*, *75*, 163–173. https://doi.org/10.1016/j.jmsy.2024.06.004
14. Latsou, C., Farsi, M., & Erkoyuncu, J. A. (2023). Digital twin-enabled automated anomaly detection and bottleneck identification in complex manufacturing systems using a multi-agent approach. *Journal of Manufacturing Systems*, *67*, 242–264. https://doi.org/10.1016/j.jmsy.2023.02.008
15. Lindemann, B., Maschler, B., Sahlab, N., & Weyrich, M. (2021). A survey on anomaly detection for technical systems using LSTM networks. *Computers in Industry*, *131*, 103498. https://doi.org/10.1016/j.compind.2021.103498