КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1115
УДК 004.056.53:004.8

Рихва Володимир Ігорович
аспірант кафедри кібербезпеки та інформаційних технологій
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна
ORCID: 0009-0008-2711-547X
volodymyr.rykhva@hneu.net

Солодовник Ганна Валеріївна
к.т.н., доцент кафедри кібербезпеки та інформаційних технологій
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна
ORCID: 0000-0001-6323-5083
ganna.solodovnyk@hneu.net

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ГЛИБОКОГО ТА МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ

Анотація. У статті представлено результати комплексного порівняльного дослідження шести методів машинного та глибокого навчання для задачі багатокласової класифікації мережевих атак. Досліджено ефективність згорткової нейронної мережі (CNN-IDS), мережі довгої короткочасної пам'яті (LSTM-IDS), градієнтного бустингу LightGBM та CatBoost, архітектури Transformer-IDS на основі механізму самоуваги, а також моделі Mamba-IDS на базі селективних просторів станів (Selective State Space Model, S6). Експерименти проведено на чотирьох еталонних наборах даних мережевого трафіку: CIC-IDS2017, CIC-IDS2018, UNSW-NB15 та CICIoT2023. Для забезпечення відтворюваності результатів застосовано єдиний протокол попередньої обробки даних із стандартизацією ознак, стратифікованим розділенням 70/15/15 та зваженою функцією втрат для подолання дисбалансу класів. Оцінювання проведено за метриками Accuracy, Macro F1-score, MCC (коефіцієнт кореляції Метьюза) та Weighted F1-score. Результати показали, що градієнтний бустинг LightGBM забезпечує найвищу точність на всіх чотирьох наборах даних. Моделі глибокого навчання (CNN, LSTM, Transformer, Mamba) продемонстрували кращу здатність до узагальнення на незбалансованих наборах даних, зокрема вищий Macro Recall для рідкісних класів атак. Модель Mamba-IDS показала конкурентоспроможні результати порівняно з Transformer-IDS за лінійної обчислювальної складності $O(n)$ замість квадратичної $O(n^2)$, що робить її перспективною для обробки довгих послідовностей мережевого трафіку в реальному часі. Аналіз per-class F1-score виявив суттєві відмінності у здатності моделей розпізнавати рідкісні класи атак, що підкреслює необхідність багатокласового оцінювання замість загальної точності.
Дослідження робить внесок у розуміння переваг та обмежень сучасних архітектур нейронних мереж для систем виявлення вторгнень, а також надає практичні рекомендації щодо вибору оптимального методу залежно від характеристик набору даних та вимог до часу обробки.

Ключові слова: система виявлення вторгнень; глибоке навчання; машинне навчання; CNN; LSTM; LightGBM; Transformer; Mamba; класифікація мережевого трафіку.

ВСТУП

Постановка проблеми. Зростання кількості та складності кібератак створює нові виклики для забезпечення безпеки комп'ютерних мереж. Системи виявлення вторгнень (Intrusion Detection Systems, IDS) стали невід'ємною частиною архітектури безпеки більшості організацій [1]. Традиційні IDS на основі сигнатурного аналізу не здатні ефективно протидіяти новим, раніше невідомим типам атак, що обумовлює необхідність застосування методів машинного та глибокого навчання для автоматичного розпізнавання аномальної мережевої активності [2].

Сучасні дослідження пропонують різноманітні архітектури нейронних мереж для задачі класифікації мережевого трафіку: від класичних згорткових (Convolutional Neural

Network, CNN) та рекурентних (Long Short-Term Memory, LSTM) мереж до новітніх архітектур на основі механізму уваги (Transformer) та просторів станів (Mamba). Водночас, методи градієнтного бустингу, зокрема LightGBM та CatBoost, демонструють високу ефективність на табличних даних мережевого трафіку. Проте більшість існуючих досліджень обмежуються порівнянням кількох методів на одному наборі даних, що не дозволяє оцінити стійкість результатів до зміни характеристик мережевого середовища [3].

Актуальність дослідження полягає у необхідності проведення комплексного порівняльного аналізу шести сучасних методів на множині еталонних наборів даних із різними характеристиками: кількістю класів (від 6 до 10), обсягом вибірки (від 1 до 6,5 млн зразків), ступенем дисбалансу класів та типами представлених атак. Таке дослідження дозволить сформулювати обґрунтовані рекомендації щодо вибору оптимального методу для конкретних умов функціонування IDS.

Аналіз останніх досліджень і публікацій. Гібридні архітектури CNN-LSTM, запропоновані у роботі [4], демонструють високу ефективність у класифікації мережевого трафіку завдяки поєднанню просторової екстракції ознак згортковими шарами та моделювання часових залежностей LSTM-шарами. Водночас такі архітектури мають суттєві обмеження: рекурентна природа LSTM призводить до значних обчислювальних витрат при обробці довгих послідовностей, а стійкість моделей на різних наборах даних потребує додаткового дослідження.

Методи градієнтного бустингу показали значні успіхи в задачах IDS. Алгоритм LightGBM [5] досягає високої точності класифікації завдяки ефективному алгоритму побудови дерев на основі гістограм. CatBoost [6] застосовує ordered boosting для зменшення зсуву передбачень та демонструє стабільну ефективність. Проте ці методи базуються на ручному конструюванні ознак і не здатні автоматично виявляти ієрархічні патерни у вхідних даних, що обмежує їх застосування для складних атак.

Архітектура Transformer адаптована для аналізу мережевого трафіку у роботах [7, 8, 9]. FlowTransformer використовує механізм самоуваги для потокових IDS, а ET-BERT досягає покращення на 6,2% для аналізу зашифрованого трафіку. Однак квадратична обчислювальна складність $O(n^2)$ механізму самоуваги суттєво обмежує застосування для довгих послідовностей мережевого трафіку.

Модель Mamba [10], заснована на селективних просторах станів (S6), забезпечує лінійну складність $O(n)$ завдяки адаптивній фільтрації вхідної інформації. Попередні дослідження S4 [11] підтвердили перспективність цього підходу для моделювання довгих послідовностей. Водночас застосування Mamba для задач виявлення мережевих вторгнень залишається малодослідженим, а питання поєднання просторової екстракції ознак CNN із часовим моделюванням SSM не розглядалося.

Таким чином, існуючі підходи або мають високу обчислювальну складність (Transformer, LSTM), або не забезпечують автоматичну екстракцію ознак (градієнтний бустинг). Це обґрунтовує актуальність розроблення гібридної архітектури CNN-Mamba, яка поєднує ефективну просторову екстракцію ознак із лінійною складністю моделювання послідовностей.

Аналіз літератури виявив декілька суттєвих прогалин: відсутність порівняння всіх шести зазначених архітектур в єдиних експериментальних умовах, обмежене дослідження ефективності моделі Mamba для задач IDS, недостатня увага до аналізу per-class метрик на множині наборів даних із різними характеристиками дисбалансу.

Мета статті. Провести комплексний порівняльний аналіз шести методів машинного та глибокого навчання (CNN-IDS, LSTM-IDS, LightGBM, CatBoost, Transformer-IDS,

Mamba-IDS) для задачі багатокласової класифікації мережевих атак на чотирьох еталонних наборах даних (CIC-IDS2017, CIC-IDS2018, UNSW-NB15, CICIoT2023) з використанням єдиного протоколу попередньої обробки та оцінити стійкість результатів до зміни характеристик даних.

МЕТОДИКА ДОСЛІДЖЕННЯ

Дослідження побудовано на єдиному експериментальному протоколі, який забезпечує коректність порівняння шести методів класифікації мережевого трафіку. Нижче описано набори даних, архітектури моделей та методологію оцінювання.

Набори даних. Для проведення експериментів обрано чотири еталонні набори даних мережевого трафіку, які відрізняються між собою кількістю класів, обсягом вибірки та типами представлених атак (табл. 1).

Таблиця 1

Характеристики наборів даних для експериментів

Набір даних	Класів	Зразків (тис.)	Ознак	Рік
CIC-IDS2017	7	2 830	78	2017
CIC-IDS2018	6	6 500	78	2018
UNSW-NB15	10	2 540	42	2015
CICIoT2023	8	~1 000	46	2023

Датасет CIC-IDS2017 [12] – це набір даних, створений Канадським інститутом кібербезпеки (Canadian Institute for Cybersecurity), що містить мережевий трафік п’яти днів із такими типами атак: Brute Force, DoS/DDoS, Web Attack, Infiltration, PortScan та Bot. Дані представлені у вигляді 78 ознак мережевих потоків, розрахованих за допомогою CICFlowMeter.

Датасет CIC-IDS2018 – це розширена версія попереднього набору даних із додатковими типами атак та більшим обсягом трафіку (понад 6,5 млн записів). Набір містить 6 класів: Benign, Bot, DDoS, DoS, Infiltration та WebAttack.

Датасет UNSW-NB15 – це набір даних, створений Австралійським центром кібербезпеки (ACCS), що містить 10 категорій трафіку (Normal, Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms) та 42 ознаки. Цей набір характеризується значним дисбалансом класів, де рідкісні категорії (Worms, Shellcode) становлять менше 0,5% вибірки.

Датасет CICIoT2023 [13] – це найновіший набір даних, спеціально створений для дослідження безпеки IoT-пристроїв. Містить трафік від 105 реальних IoT-пристроїв із 8 категоріями атак, включаючи Mirai botnet, DDoS та DoS різних типів.

Архітектури моделей. У дослідженні використано шість моделей, які представляють різні парадигми машинного навчання. Параметри архітектур наведено у таблиці 2.

Таблиця 2

Архітектури досліджуваних моделей

Модель	Тип	Ключові параметри
CNN-IDS	Згорткова НМ	Conv1D(128)→Conv1D(64)→Dense(128)
LSTM-IDS	Рекурентна НМ	LSTM(128)→LSTM(64)→Dense(128)
LightGBM	Градієнтний бустинг	n_est=500, lr=0.05, leaves=63
CatBoost	Градієнтний бустинг	iterations=500, lr=0.05, depth=8
Transformer-IDS	Self-Attention	d=128, heads=4, layers=2
Mamba-IDS	Простори станів (S6)	d=128, d_state=16, layers=2

Модель CNN-IDS використовує два шари одновимірної згортки (Conv1D) з 128 та 64 фільтрами відповідно, за якими слідує глобальна агрегація та повнозв'язний шар із 128 нейронами. Як функцію активації обрано ReLU, а для запобігання перенавчанню застосовано Dropout з імовірністю відключення 0,3. Модель навчається протягом 50 епох з ранньою зупинкою (patience=15) та оптимізатором Adam (lr=0.001).

Модель LSTM-IDS складається з двох шарів LSTM із 128 та 64 нейронами. Вхідні ознаки перетворюються у послідовність для обробки рекурентними шарами. Використовується та сама стратегія навчання, що й для моделі CNN-IDS, із зваженою крос-ентропією для врахування дисбалансу класів.

Модель LightGBM [5] – це алгоритм градієнтного бустингу на основі гістограм, який забезпечує високу швидкість навчання та ефективне використання пам'яті. Налаштовано 500 дерев із learning rate, який дорівнює 0,05, кількістю листів, яка дорівнює 63 та максимальною глибиною -1 (без обмеження). В моделі використовується функція втрат multiclass softmax.

Модель CatBoost [6] – це алгоритм градієнтного бустингу з ordered boosting, який зменшує зсув передбачень при послідовній побудові дерев. Модель має наступні параметри: кількість ітерацій дорівнює 500, learning rate дорівнює 0,05, глибина дерева дорівнює 8.

Модель Transformer-IDS адаптує архітектуру Transformer [7] для класифікації табличних даних. Вхідні ознаки проєктуються у простір розмірністю d=128 через лінійний шар, після чого обробляються двома шарами Multi-Head Self-Attention із 4 головами. Позиційне кодування не використовується, оскільки ознаки мережевого трафіку не мають природного порядку.

Модель Mamba-IDS [10] використовує архітектуру селективних просторів станів (S6). Модель складається з двох блоків Mamba із розмірністю стану d_state=16 та розмірністю моделі d=128. Кожен блок включає лінійну проєкцію, селективне сканування (selective scan) та вихідну проєкцію. На відміну від Transformer, Mamba забезпечує лінійну складність O(n) завдяки рекурентному обчисленню без матриці уваги.

Протокол експерименту. Для забезпечення коректності порівняння всі моделі оцінюються за єдиним протоколом:

1. Попередня обробка, яка полягає у видаленні дублікатів та нескінченних значень, заповненні пропусків нулями, стандартизації ознак (StandardScaler) з навчанням лише на тренувальній вибірці.
2. Розділення даних передбачає стратифіковане розділення 70% / 15% / 15% (навчання / валідація / тест) із фіксованим зерном random_state=42 для відтворюваності.
3. Врахування дисбалансу використовується для моделей глибокого навчання за зважених втрат (weighted cross-entropy) з вагами, обернено пропорційними частоті класів. Для LightGBM та CatBoost аналогічно застосовуються параметри class_weight.
4. Якість моделей оцінено за метриками: Accuracy – для загальної точності; Macro Precision, Macro Recall, Macro F1-score – для рівноважного врахування класів; Weighted F1-score – для врахування частоти класів; MCC – для комплексної оцінки на незбалансованих даних [14].

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Результати порівняння шести моделей на чотирьох наборах даних представлено у таблицях 3-6 та на рисунках 1-2.

Таблиця 3

Результати класифікації на CIC-IDS2017 (7 класів)

Модель	Accuracy	Macro F1	Weighted F1	MCC
CNN-IDS	0.9910	0.9570	0.9914	0.9886
LSTM-IDS	0.9920	0.9640	0.9923	0.9899
LightGBM	0.9995	0.9977	0.9995	0.9994
CatBoost	0.9994	0.9967	0.9994	0.9992
Transformer-IDS	0.9876	0.9486	0.9880	0.9843
Mamba-IDS	0.9927	0.9675	0.9928	0.9907

На наборі даних CIC-IDS2017 (табл. 3) всі шість моделей демонструють високу загальну точність (Accuracy > 0,987). Найкращий результат показав LightGBM із Macro F1 = 0,9977, що свідчить про практично ідеальне розпізнавання всіх семи класів. CatBoost посідає друге місце (Macro F1 = 0,9967). Серед моделей глибокого навчання Mamba-IDS (Macro F1 = 0,9675) перевершує Transformer-IDS (Macro F1 = 0,9486), демонструючи перевагу архітектури просторів станів для цього набору даних.

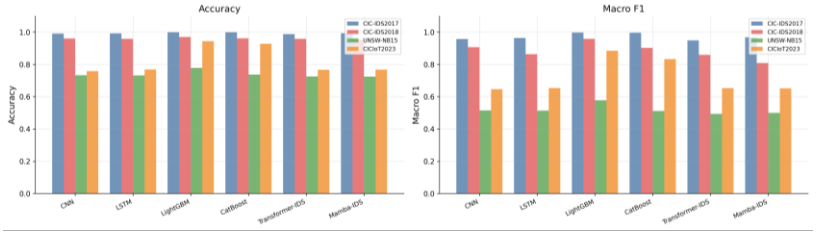

Рис. 1. Порівняння Accuracy та Macro F1 шести моделей на чотирьох наборах даних

Таблиця 4

Результати класифікації на CIC-IDS2018 (6 класів)

Модель	Accuracy	Macro F1	Weighted F1	MCC
CNN-IDS	0.9607	0.9065	0.9610	0.9509
LSTM-IDS	0.9579	0.8638	0.9583	0.9478
LightGBM	0.9704	0.9583	0.9706	0.9636
CatBoost	0.9612	0.9020	0.9615	0.9515
Transformer-IDS	0.9581	0.8595	0.9585	0.9479
Mamba-IDS	0.9529	0.8090	0.9560	0.9413

На CIC-IDS2018 (табл. 4) спостерігається значно більший розкид між моделями. LightGBM зберігає лідерство із Macro F1 = 0,9583, тоді як Mamba-IDS демонструє найнижчий Macro F1 = 0,8090. Це зниження пов’язане зі складністю класифікації рідкісного класу WebAttack, який становить лише 1,2% вибірки. CNN-IDS показує другий результат (Macro F1 = 0,9065), перевершуючи CatBoost (0,9020) та LSTM-IDS (0,8638).

Таблиця 5

Результати класифікації на UNSW-NB15 (10 класів)

Модель	Accuracy	Macro F1	Weighted F1	MCC
CNN-IDS	0.7331	0.5152	0.7628	0.6839
LSTM-IDS	0.7322	0.5136	0.7601	0.6834
LightGBM	0.7785	0.5778	0.8074	0.7258
CatBoost	0.7375	0.5112	0.7713	0.6858
Transformer-IDS	0.7259	0.4939	0.7564	0.6754
Mamba-IDS	0.7241	0.4994	0.7573	0.6729

Набір даних UNSW-NB15 (табл. 5) є найскладнішим для всіх моделей через наявність десяти класів із суттєвим дисбалансом (клас Worms складає менше 0,1% вибірки). Найкращий Macro F1 = 0,5778 (LightGBM) свідчить про значні труднощі у розпізнаванні рідкісних класів. Розрив між значеннями Accuracy (0,7785) та Macro F1 (0,5778) підтверджує, що загальна точність є не найкращою метрикою для незбалансованих даних, адже модель може правильно класифікувати домінуючі класи, ігноруючи рідкісні. Моделі глибокого навчання демонструють Macro F1 у діапазоні 0,49-0,52, при цьому CNN-IDS та LSTM-IDS показують дещо кращі результати, ніж Transformer-IDS та Mamba-IDS.

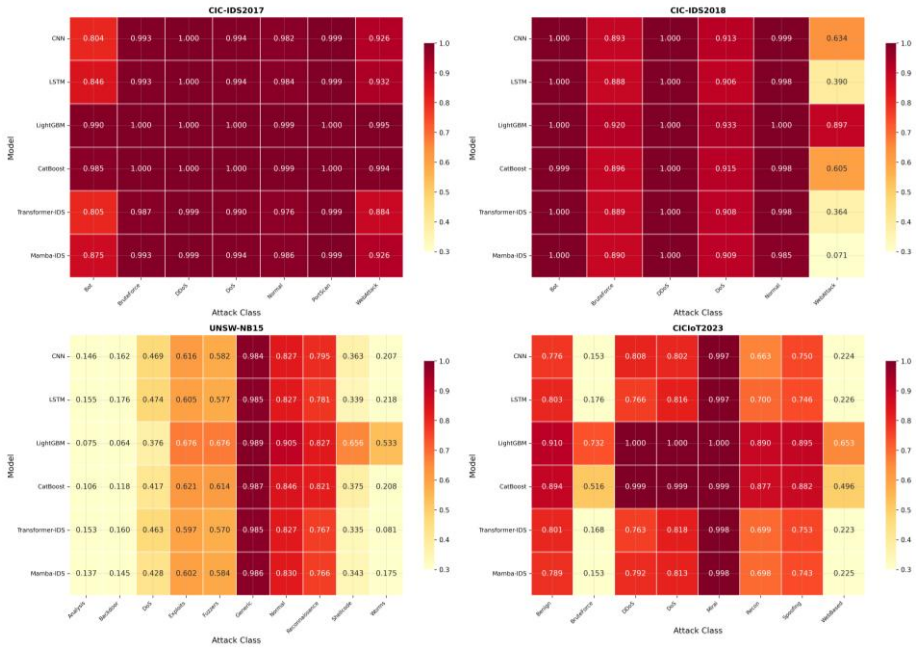

Рис. 2. Теплова карта Per-class F1-score для шести моделей на чотирьох наборах даних

Таблиця 6

Результати класифікації на CICIoT2023 (8 класів)

Модель	Accuracy	Macro F1	Weighted F1	MCC
CNN-IDS	0.7579	0.6467	0.7872	0.7235
LSTM-IDS	0.7682	0.6536	0.7924	0.7354
LightGBM	0.9436	0.8850	0.9436	0.9329
CatBoost	0.9275	0.8326	0.9327	0.9148
Transformer-IDS	0.7662	0.6528	0.7929	0.7338
Mamba-IDS	0.7672	0.6513	0.7931	0.7331

На CICIoT2023 (табл. 6) спостерігається чітке розділення моделей на дві групи: градієнтний бустинг (LightGBM – Macro F1 = 0,8850, CatBoost – 0,8326) значно перевершує моделі глибокого навчання (Macro F1 у діапазоні 0,647-0,654). Це може бути пов’язано з табличною природою ознак мережевого трафіку, де деревоподібні моделі ефективніше використовують дискретні та категоріальні залежності між ознаками [15].

Аналіз результатів. Узагальнені результати порівняння моделей на всіх чотирьох наборах даних представлено на рисунках 1-2 та у зведеній таблиці 7.

Таблиця 7

Зведені результати: найкращі моделі за Macro F1 на кожному наборі даних

Набір даних	Найкраща модель	Macro F1	Друга модель	Macro F1
CIC-IDS2017	LightGBM	0.9977	CatBoost	0.9967
CIC-IDS2018	LightGBM	0.9583	CNN-IDS	0.9065
UNSW-NB15	LightGBM	0.5778	CNN-IDS	0.5152
CICIoT2023	LightGBM	0.8850	CatBoost	0.8326

Аналіз результатів дозволяє сформулювати такі ключові спостереження:

5. Наявність домінування градієнтного бустингу, тобто LightGBM є найкращою моделлю за Macro F1 на всіх чотирьох наборах даних. Це підтверджує результати досліджень [5, 15], які демонструють перевагу деревоподібних методів на табличних даних.

6. Порівняння моделей Mamba-IDS та Transformer-IDS свідчить, що на трьох із чотирьох наборів даних Mamba-IDS перевершує або показує схожі результати з Transformer-IDS: CIC-IDS2017 (+1,89 п.п.), UNSW-NB15 (+0,55 п.п.), CICIoT2023 (–0,15 п.п., різниця несуттєва). Виняток складає набір даних CIC-IDS2018, за якого Mamba-IDS відстає (0,8090 порівняно з 0,8595). Загалом модель Mamba-IDS демонструє конкурентоспроможність при нижчій обчислювальній складності.

7. Вплив дисбалансу класів. На найбільш збалансованому наборі даних CIC-IDS2017 розрив між моделями є мінімальним. На наборі даних UNSW-NB15 із найбільшим дисбалансом розрив зростає до 8,39 п.п. Це підкреслює необхідність використання Macro F1 замість Accuracy в якості основної метрики для оцінювання IDS.

Аналіз часу навчання та інференсу. Час навчання моделей суттєво відрізняється (рис. 3, 4). Модель LightGBM є найшвидшою для навчання (час навчання складає 19-63 с залежно від набору даних), тоді як модель CNN-IDS потребує найбільше часу (час навчання складає 370-485 с). Модель Mamba-IDS навчається на 15-19% повільніше за модель Transformer-IDS, що пояснюється додатковими обчисленнями для селективного сканування. Час інференсу для всіх моделей глибокого навчання не перевищує 0,65 с на тестовій вибірці, що підтверджує їх придатність для обробки в реальному часі.

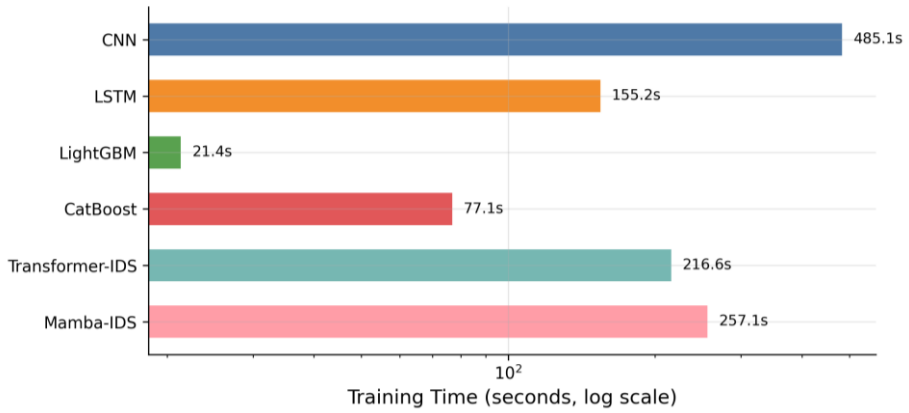

Рис. 3. Порівняння часу навчання (с) шести моделей (CIC-IDS2017)

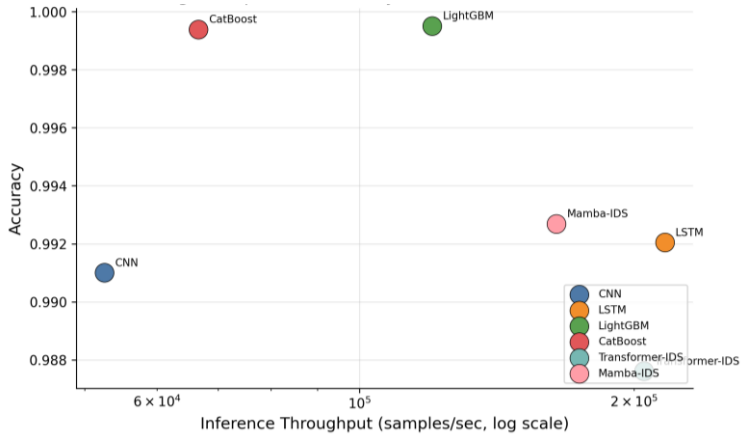

Рис. 4. Компроміс між швидкістю інференсу та точністю моделей (CIC-IDS2017)

Обговорення результатів. Домінування моделі LightGBM на всіх наборах даних пояснюється декількома факторами. По-перше, ознаки мережевого трафіку є табличними, а деревоподібні моделі ефективніше моделюють нелінійні залежності між окремими ознаками без потреби в перетворенні даних у послідовності. По-друге, модель LightGBM використовує гістограмний підхід до побудови дерев, що забезпечує автоматичну дискретизацію неперервних ознак та ефективну обробку пропусків.

Водночас, моделі глибокого навчання мають потенціал для покращення через ансамблювання. Зокрема, їхні ймовірнісні прогнози можуть бути використані як мета-ознаки для стекінг-ансамблю, де мета-класифікатор навчається оптимально комбінувати сильні сторони різних архітектур. Такий підхід може покращити розпізнавання рідкісних класів атак, за яких різні моделі мають комплементарні помилки.

Архітектура Mamba-IDS заслуговує на окрему увагу як перспективний напрям для IDS. Незважаючи на те, що на поточних наборах даних модель Mamba-IDS не перевершує градієнтний бустинг, її лінійна складність робить її придатною для обробки довгих часових рядів мережевого трафіку, за яких модель Transformer стикається з квадратичним зростанням витрат пам’яті. Крім того, модель Mamba може бути інтегрована у потокові системи обробки трафіку завдяки рекурентній природі обчислень.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В ході дослідження було проведено комплексний порівняльний аналіз шести методів машинного та глибокого навчання для задачі багатокласової класифікації мережевих атак на чотирьох еталонних наборах даних. Отримано такі основні результати:

1. Градієнтний бустинг LightGBM забезпечує найвищу точність класифікації на всіх чотирьох наборах даних (Macro F1 від 0,5778 до 0,9977), що підтверджує ефективність деревоподібних методів для табличних даних мережевого трафіку.

2. Модель Mamba-IDS на основі селективних просторів станів демонструє конкурентоспроможні результати порівняно з моделю Transformer-IDS на трьох із чотирьох наборів даних при забезпеченні лінійної обчислювальної складності O(n), що є перспективним для систем реального часу.

3. Аналіз per-class F1-score виявив суттєві відмінності у здатності моделей розпізнавати рідкісні класи атак. На UNSW-NB15 розрив між Accuracy (0,78) та Macro

F1 (0,58) для найкращої моделі підтверджує неадекватність загальної точності як метрики для IDS.

4. Час навчання моделей варіюється від 19 с (для моделі LightGBM) до 485 с (для моделі CNN-IDS), при цьому всі моделі забезпечують час інференсу менше 0,65 с, що підтверджує їх придатність для обробки в реальному часі.

Перспективи подальших досліджень включають: застосування методів відбору ознак (SHAP) для зменшення розмірності вхідного простору, побудову стекінг-ансамблів, що комбінують прогнози різних моделей та дослідження адаптивного навчання для виявлення нових, раніше невідомих типів атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Momand, A., Jan, S. U., & Ramzan, N. (2023). A systematic and comprehensive survey of recent advances in intrusion detection systems using machine learning: Deep learning, datasets, and attack taxonomy. *Journal of Sensors, 2023*, Article 6048087. https://doi.org/10.1155/2023/6048087
2. Lansky, J., et al. (2021). Deep learning-based intrusion detection systems: A systematic review. *IEEE Access, 9*, 112054–112072. https://doi.org/10.1109/ACCESS.2021.3097247
3. Ahmad, Z., et al. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(12), e4150. https://doi.org/10.1002/ett.4150
4. Halbouni, A., et al. (2022). CNN-LSTM: Hybrid deep neural network for network intrusion detection system. *IEEE Access, 10*, 99855–99873. https://doi.org/10.1109/ACCESS.2022.3206425
5. Liu, G., Zhao, W., & Wang, Q. (2021). A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM. *Computers & Security, 102*, Article 102289. https://doi.org/10.1016/j.cose.2021.102289
6. Douiba, M., Benber, S., Idri, S., & Nassih, B. (2023). An improved anomaly detection model for IoT security using decision tree and gradient boosting. *The Journal of Supercomputing, 79*, 16261–16285. https://doi.org/10.1007/s11227-022-04783-y
7. Manocchio, L., et al. (2024). FlowTransformer: A transformer framework for flow-based network intrusion detection systems. *Expert Systems with Applications, 237*, Article 122564. https://doi.org/10.1016/j.eswa.2023.122564
8. Lin, X., et al. (2022). ET-BERT: A contextualized datagram representation with pre-training transformers for encrypted traffic classification. In *Proceedings of the ACM Web Conference 2022* (pp. 2230–2240). https://doi.org/10.1145/3485447.3512217
9. Ferrag, M. A., et al. (2022). Edge-IIoTset: A new comprehensive realistic cybersecurity dataset of IoT and IIoT applications for centralized and federated learning. *IEEE Access, 10*, 40281–40306. https://doi.org/10.1109/ACCESS.2022.3165809
10. Gu, A., & Dao, T. (2023). Mamba: Linear-time sequence modeling with selective state spaces. *arXiv*. https://doi.org/10.48550/arXiv.2312.00752
11. Gu, A., Goel, K., & Ré, C. (2022). Efficiently modeling long sequences with structured state spaces. In *International Conference on Learning Representations (ICLR 2022)*. https://openreview.net/forum?id=uYLFoz1vlAC
12. Engelen, G., Rimmer, V., & Joosen, W. (2021). Troubleshooting an intrusion detection dataset: The CICIDS2017 case study. In *IEEE Security and Privacy Workshops (SPW 2021)* (pp. 96–102). https://doi.org/10.1109/SPW53761.2021.00009
13. Neto, E. C. P., et al. (2023). CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment. *Sensors, 23*(13), Article 5941. https://doi.org/10.3390/s23135941
14. Chicco, D., Tötsch, N., & Jurman, G. (2021). The Matthews correlation coefficient (MCC) is more reliable than balanced accuracy, bookmaker informedness, and markedness in two-class confusion matrix evaluation. *BioData Mining, 14*, Article 13. https://doi.org/10.1186/s13040-021-00244-z
15. Grinsztajn, L., Oyallon, E., & Varoquaux, G. (2022). Why do tree-based models still outperform deep learning on typical tabular data? In *Advances in Neural Information Processing Systems (NeurIPS 2022)*. https://proceedings.neurips.cc/paper_files/paper/2022/hash/0378c7692da36807bdec87ab043cdadc-Abstract-Datasets_and_Benchmarks.html

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Volodymyr Rykhva
Postgraduate student, Department of Cybersecurity and Information Technologies
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: 0009-0008-2711-547X
volodymyr.rykhva@hneu.net

Ganna Solodovnyk
PhD in Technical Sciences, Associate Professor, Department of Cybersecurity and Information Technologies
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: 0000-0001-6323-5083
ganna.solodovnyk@hneu.net

COMPARATIVE ANALYSIS OF DEEP AND MACHINE LEARNING METHODS FOR NETWORK INTRUSION DETECTION

Abstract. This paper presents the results of a comprehensive comparative study of six machine learning and deep learning methods for the task of multi-class network attack classification. We evaluate the effectiveness of a convolutional neural network (CNN-IDS), long short-term memory network (LSTM-IDS), LightGBM and CatBoost gradient boosting, Transformer-IDS based on the self-attention mechanism, and Mamba-IDS based on Selective State Space Models (S6). Experiments are conducted on four benchmark network traffic datasets: CIC-IDS2017, CIC-IDS2018, UNSW-NB15 and CICIoT2023. To ensure reproducibility, we apply a unified preprocessing protocol with feature standardization, stratified 70/15/15 splitting, and weighted loss functions to address class imbalance. Evaluation is performed using Accuracy, Macro F1-score, MCC (Matthews Correlation Coefficient), and Weighted F1-score. Results show that LightGBM gradient boosting achieves the highest accuracy across all four datasets. Deep learning models (CNN, LSTM, Transformer, Mamba) demonstrate better generalization on imbalanced datasets, particularly higher Macro Recall for rare attack classes. Mamba-IDS shows competitive results compared to Transformer-IDS with linear O(n) computational complexity instead of quadratic $O(n^2)$, making it promising for real-time processing of long network traffic sequences. Per-class F1-score analysis reveals significant differences in models' ability to recognize rare attack classes, emphasizing the need for multi-class evaluation beyond overall accuracy. The study contributes to understanding the strengths and limitations of modern neural network architectures for intrusion detection systems and provides practical recommendations for selecting the optimal method depending on dataset characteristics and processing time requirements.

Keywords: intrusion detection system; deep learning; machine learning; CNN; LSTM; LightGBM; Transformer; Mamba; network traffic classification.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Momand, A., Jan, S. U., & Ramzan, N. (2023). A systematic and comprehensive survey of recent advances in intrusion detection systems using machine learning: Deep learning, datasets, and attack taxonomy. *Journal of Sensors, 2023*, Article 6048087. https://doi.org/10.1155/2023/6048087
2. Lansky, J., et al. (2021). Deep learning-based intrusion detection systems: A systematic review. *IEEE Access, 9*, 112054–112072. https://doi.org/10.1109/ACCESS.2021.3097247
3. Ahmad, Z., et al. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(12), e4150. https://doi.org/10.1002/ett.4150
4. Halbouni, A., et al. (2022). CNN-LSTM: Hybrid deep neural network for network intrusion detection system. *IEEE Access, 10*, 99855–99873. https://doi.org/10.1109/ACCESS.2022.3206425
5. Liu, G., Zhao, W., & Wang, Q. (2021). A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM. *Computers & Security, 102*, Article 102289. https://doi.org/10.1016/j.cose.2021.102289

6. Douiba, M., Benber, S., Idri, S., & Nassih, B. (2023). An improved anomaly detection model for IoT security using decision tree and gradient boosting. *The Journal of Supercomputing, 79*, 16261–16285. https://doi.org/10.1007/s11227-022-04783-y
7. Manocchio, L., et al. (2024). FlowTransformer: A transformer framework for flow-based network intrusion detection systems. *Expert Systems with Applications, 237*, Article 122564. https://doi.org/10.1016/j.eswa.2023.122564
8. Lin, X., et al. (2022). ET-BERT: A contextualized datagram representation with pre-training transformers for encrypted traffic classification. In *Proceedings of the ACM Web Conference 2022* (pp. 2230–2240). https://doi.org/10.1145/3485447.3512217
9. Ferrag, M. A., et al. (2022). Edge-IIoTset: A new comprehensive realistic cybersecurity dataset of IoT and IIoT applications for centralized and federated learning. *IEEE Access, 10*, 40281–40306. https://doi.org/10.1109/ACCESS.2022.3165809
10. Gu, A., & Dao, T. (2023). Mamba: Linear-time sequence modeling with selective state spaces. *arXiv*. https://doi.org/10.48550/arXiv.2312.00752
11. Gu, A., Goel, K., & Ré, C. (2022). Efficiently modeling long sequences with structured state spaces. In *International Conference on Learning Representations (ICLR 2022).* https://openreview.net/forum?id=uYLFoz1vlAC
12. Engelen, G., Rimmer, V., & Joosen, W. (2021). Troubleshooting an intrusion detection dataset: The CICIDS2017 case study. In *IEEE Security and Privacy Workshops (SPW 2021)* (pp. 96–102). https://doi.org/10.1109/SPW53761.2021.00009
13. Neto, E. C. P., et al. (2023). CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment. *Sensors, 23*(13), Article 5941. https://doi.org/10.3390/s23135941
14. Chicco, D., Tötsch, N., & Jurman, G. (2021). The Matthews correlation coefficient (MCC) is more reliable than balanced accuracy, bookmaker informedness, and markedness in two-class confusion matrix evaluation. *BioData Mining, 14*, Article 13. https://doi.org/10.1186/s13040-021-00244-z
15. Grinsztajn, L., Oyallon, E., & Varoquaux, G. (2022). Why do tree-based models still outperform deep learning on typical tabular data? In *Advances in Neural Information Processing Systems (NeurIPS 2022).* https://proceedings.neurips.cc/paper_files/paper/2022/hash/0378c7692da36807bdec87ab043cdadc-Abstract-Datasets_and_Benchmarks.html

Отримано редакцією журналу / Received: 25.01.26
Прорецензовано / Revised: 15.02.26
Схвалено до друку / Accepted: 26.03.26