УДК 004.056.53:004.89 DOI https://doi.org/10.35546/kntu2078-4481.2026.1.51

І. О. ШАКЛЕЇНА
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційних систем та мереж
Національний університет «Львівська політехніка»
ORCID: 0000-0003-0809-1480

А. Т. САВШАК
магістр кафедри фізики та інформаційних систем
Дрогобицький державний університет імені Івана Франка
ORCID: 0009-0007-5769-3898

О. Т. ШАКЛЕЇН
магістр кафедри інформаційних систем та мереж
Національний університет «Львівська політехніка»
ORCID: 0009-0001-0025-2166

МЕТОД ЗНИЖЕННЯ ХИБНИХ СПРАЦЮВАНЬ У СИСТЕМАХ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ ПОРОГОВОЇ ФІЛЬТРАЦІЇ ТА GRADIENT BOOSTING

Зростання кількості та складності кіберзагроз зумовлює необхідність підвищення ефективності систем виявлення вторгнень. Практичне використання таких систем суттєво ускладнюється високим рівнем хибних спрацювань, який призводить до перевантаження фахівців з безпеки. Метою роботи є розробка методу зниження хибних спрацювань у системах виявлення мережевих вторгнень, що забезпечує оптимальний баланс між точністю класифікації, обчислювальною ефективністю та практичною придатністю для розгортання у реальних мережевих середовищах. Запропонований метод базується на поєднанні алгоритму градієнтного бустингу LightGBM із механізмом адаптивної порогової фільтрації з fallback-класом. В роботі розроблено мікросервісну архітектуру системи на базі контейнеризації Docker, яка включає п'ять основних компонентів: CICFlowMeter для формування потоків, Converter для конвертації форматів, Agent для батчування подій, API Server для класифікації та Dashboard для візуалізації результатів. Ключовою науковою новизною є алгоритм адаптивної порогової фільтрації, що використовує індивідуальні порогові значення для кожного класу атак та механізм автоматичного повернення до класу BENIGN у разі недостатньої впевненості моделі.

Експериментальні дослідження, виконані на публічному датасеті CIC-IDS2017, показали що запропонований метод забезпечує точність класифікації на рівні F1-score = 0.949 при рівні хибних спрацювань 2.1 %, що становить зниження на 74 % порівняно з базовою моделлю LightGBM без постобробки. У порівнянні з багатошаровою нейронною мережею MLP запропоноване рішення забезпечує вищу точність при чотириразовому скороченні часу навчання та майже вдвічі швидшому інференсі. Також досліджено внесок кожного компонента запропонованої системи у точність виявлення кібератак. Результати тестування на різних типах атак показали найкращу ефективність виявлення для DDoS, PortScan та DoS-атак. Практична значущість роботи полягає у можливості застосування запропонованого методу в реальних системах виявлення вторгнень без потреби у графічних прискорювачах, що робить його придатним для організацій з обмеженими обчислювальними ресурсами.

Ключові слова: *виявлення вторгнень, машинне навчання, кібератаки, мережева безпека, хибні спрацювання, порогова фільтрація.*

I. O. SHAKLEINA
Ph.D. (Physical and Mathematical Sciences), Associate Professor,
Associate Professor at the Information Systems and Networks Department
Lviv Polytechnic National University
ORCID: 0000-0003-0809-1480

A. T. SAVSHAK
Master's Student at the Department of Physics and Information Systems
Drohobych Ivan Franko State Pedagogical University
ORCID: 0009-0007-5769-3898

© І. О. Шаклеїна, А. Т. Савшак, О. Т. Шаклеїн, 2026
Стаття поширюється на умовах відкритої ліцензії CC BY 4.0

O. T. SHAKLEIN
Master's Student at the Department of Information Systems and Networks
Lviv Polytechnic National University
ORCID: 0009-0001-0025-2166

METHOD FOR REDUCING FALSE ACCOUNTS IN INTRUDER DETECTION SYSTEMS BASED ON THRESHOLD FILTERING AND GRADIENT BOOSTING

The increasing number and complexity of cyber threats necessitates the need to improve the efficiency of intrusion detection systems. The practical use of such systems is significantly complicated by the high level of false positives, which leads to an overload of security professionals. The aim of the work is to develop a method for reducing false positives in network intrusion detection systems that provides an optimal balance among classification accuracy, computational efficiency, and practical suitability for deployment in real network environments. The proposed method combines the LightGBM gradient boosting algorithm with an adaptive threshold filtering mechanism and a fallback class. A microservice architecture for the system based on Docker containerization has been developed, comprising five main components: CICFlowMeter for flow generation, Converter for format conversion, Agent for event batching, API Server for classification, and Dashboard for results visualization. The key scientific novelty is the adaptive threshold filtering algorithm, which uses individual threshold values for each attack class and a mechanism for automatically returning to the BENIGN class when model confidence is insufficient.

Experimental studies on the public CIC-IDS2017 dataset showed that the proposed method achieves an F1-score = 0.949 and a false positive rate of 2.1 %, a 74 % reduction compared to the basic LightGBM model without post-processing. Compared to the MLP multilayer neural network, the proposed solution achieves higher accuracy with a fourfold reduction in training time and inference that is almost twice as fast. The contribution of each component of the proposed system to the accuracy of cyberattack detection was also investigated. Testing across different attack types showed the best detection efficiency for DDoS, PortScan, and DoS attacks. The practical significance of the work lies in the ability to apply the proposed method in real intrusion detection systems without the need for graphics accelerators, making it suitable for organizations with limited computing resources.

Key words: *intrusion detection, machine learning, cyberattacks, network security, false positives, threshold filtering.*

Постановка проблеми

В умовах зростання кількості та складності кіберзагроз важливим є вдосконалення методів захисту інформаційних систем. За даними аналітичних звітів з кібербезпеки, у 2024 році кількість кібератак на одну організацію зросла більш ніж на 70 % у порівнянні з попереднім роком, при цьому середня кількість атак сягала понад 1 800 інцидентів на тиждень [1]. У 2025 році ця тенденція зберігається, що підтверджується зростанням кількості складних багатовекторних атак, зокрема ransomware та атак нульового дня.

У таких умовах системи виявлення вторгнень (Intrusion Detection Systems, IDS) залишаються одним із ключових інструментів забезпечення кібербезпеки корпоративних мереж [2]. Водночас їх практичне використання суттєво ускладнюється високим рівнем хибних спрацювань (False Positive Rate, FPR) [3]. Особливо гостро ця проблема проявляється у високонавантажених мережах, де навіть незначне зростання FPR суттєво впливає на ефективність моніторингу безпеки.

У сучасних умовах зростання кіберзагроз існує два основних підходи до побудови систем виявлення вторгнень: використання складних моделей глибинного навчання, які демонструють високу точність, але потребують значних обчислювальних ресурсів [4], та практичні рішення на основі класичних методів машинного навчання, здатні працювати в режимі реального часу на обмежених апаратних ресурсах.

Deep learning підходи забезпечують високу точність виявлення атак, однак мають низку суттєвих обмежень, зокрема потребу у GPU для інференсу, складність інтерпретації результатів, підвищений рівень хибних спрацювань без додаткової пост-обробки та відсутність готових production-рішень для високонавантажених мереж. У зв'язку з цим актуальним є використання класичних моделей машинного навчання з додатковими механізмами зниження FPR.

Аналіз останніх досліджень і публікацій

Традиційні сигнатурні системи виявлення вторгнень, такі як Snort, забезпечують високу швидкодію та низький рівень хибних спрацювань для відомих типів атак. Однак, попри свою зрілість та велику базу правил, Snort демонструє обмежену ефективність при роботі з високонавантаженим трафіком через однопотокову архітектуру [5]. Останніми роками значного поширення набули підходи на основі глибинного навчання (Deep Learning). У роботі В. В. Бандури, М. В. Крихівського та В. І. Чудик [4] запропоновано комплексну модель прогнозування кібератак на основі алгоритмів штучного інтелекту для виявлення аномалій, орієнтовану на аналіз великих обсягів мережевих даних. Запропонована модель поєднує рекурентні нейронні мережі (RNN), двонаправлені рекурентні мережі (Bi-RNN), згорткові нейронні мережі (CNN), механізм уваги та трансформерні архітектури, що дозволяє ефективно аналізувати як часові, так і просторові залежності у мережевому трафіку.

Подібний підхід із використанням гібридної моделі CapsNet + BiLSTM описано у роботі [6], де автори досягли точності 99 % на датасеті CIC-IDS2017. Проблема зниження FPR активно досліджується у науковій літературі. В роботі [7] описано застосання адаптивних алгоритмів машинного навчання з online learning для динамічного налаштування порогів виявлення, що дало змогу знизити FPR на 30–40 % порівняно зі статичними моделями. Дослідження показують, що методи порогової фільтрації є ефективним інструментом для зниження кількості хибних спрацювань без суттєвого погіршення показників виявлення справжніх атак [8].

Deep learning підходи залишаються обмежено придатними для практичного використання через високі вимоги до ресурсів та складність інтерпретації [9]. Таким чином, актуальною є необхідність пошуку менш ресурсомістких і більш інтерпретованих рішень, здатних забезпечити подібну ефективність.

Для побудови IDS на стандартних наборах даних широко застосовуються класичні методи машинного навчання. Дослідження [10] показують, що ці методи забезпечують прийнятну точність і зручність інтерпретації при роботі з датасетом CIC-IDS2017 [11], досягаючи F1-score на рівні 0.94–0.96, однак часто супроводжуються підвищеним рівнем FPR (6–9 %), що негативно впливає на їх практичну ефективність. У роботі [12] проведено комплексне порівняння різних алгоритмів машинного навчання на датасеті CIC-IDS2017, де показано, що вибір методу значною мірою залежить від специфіки мережевого середовища та вимог до балансу між точністю та продуктивністю.

Перспективним напрямом є використання методів градієнтного бустингу, зокрема LightGBM. Порівняльні дослідження демонструють, що ці моделі забезпечують кращий баланс між точністю класифікації та обчислювальною складністю, а також перевершують класичні ML-алгоритми за показниками якості виявлення атак. У роботі [13] запропоновано AutoML-підхід на основі gradient boosting для виявлення мережевих вторгнень, який показав високу ефективність на датасеті CIC-IDS2017 з F1-score 0.95–0.97 та часом інференсу 3–5 мс на подію. Разом із тим, навіть для Gradient Boosting-моделей проблема зниження рівня хибних спрацювань залишається актуальною, що особливо критично для багатокласових моделей у високонавантажених мережах.

Формулювання мети дослідження

Метою даної роботи є розробка методу зниження хибних спрацювань у системах виявлення мережевих вторгнень, що забезпечує оптимальний баланс між точністю класифікації, обчислювальною ефективністю та практичною придатністю для розгортання у реальних мережевих середовищах шляхом поєднання gradient boosting моделі LightGBM із механізмом адаптивної порогової фільтрації з fallback-класом.

Викладення основного матеріалу дослідження

В роботі запропоновано метод зниження хибних спрацювань у системах виявлення мережевих вторгнень. Метод реалізовано у вигляді мікросервісної архітектури на базі контейнеризації Docker, що забезпечує модульність, масштабованість та простоту розгортання. Система охоплює повний цикл обробки мережевого трафіку – від захоплення пакетів до формування сповіщень про виявлені загрози та включає п’ять основних компонентів:

- CICFlowMeter – сервіс перетворення PCAP-файлів у CSV-формат потоків із 83 статистичними ознаками;
- Converter – модуль конвертації CSV-потоків у формат NDJSON із фільтрацією за напрямком трафіку (локальний/вхідний);
- Agent – файловий агент, що формує батчі подій і надсилає їх на сервіс інференсу через HTTP API;
- API (FastAPI) – центральний сервіс, що виконує препроцесинг, класифікацію за допомогою LightGBM, порогову фільтрацію результатів та журналювання детекцій у форматі Parquet;
- Dashboard – веб-інтерфейс для візуалізації статистики виявлених загроз, перегляду останніх алертів та моніторингу стану системи.

Взаємодія між компонентами здійснюється через HTTP-запити та спільні директорії для проміжних даних, що забезпечує слабку зв’язаність компонентів і можливість незалежного масштабування. Центральний сервіс API забезпечує повний цикл обробки подій: отримання даних, передобробка ознак (імпутація та масштабування), інференс моделі LightGBM, застосування порогової фільтрації з fallback-механізмом та формування відповіді у форматі JSON.

На рис. 1 наведено діаграму послідовностей, що ілюструє процес взаємодії основних компонентів системи виявлення вторгнень під час обробки мережевого трафіку. Для збору первинних даних використано інструмент Dumpcap, який і забезпечує високопродуктивне захоплення мережевих пакетів у режимі реального часу з мінімальними накладними витратами на систему. Отримані дампи трафіку зберігаються у форматі PCAP та використовуються як вхідні дані для подальшої обробки. Використання CICFlowMeter дозволяє отримати стандартизований набір ознак, що широко застосовується у сучасних дослідженнях IDS і забезпечує порівнюваність результатів з іншими роботами.

На етапі препроцесингу виконано усунення пропущених значень та нормалізацію ознак. Етап попередньої обробки включає два послідовні кроки:

а) імп’ютація відсутніх значень (SimpleImputer з медіанною стратегією). Використання медіанної стратегії забезпечує стійкість до викидів та зберігає статистичні властивості розподілу даних.

б) стандартизація ознак (StandardScaler). Оскільки ознаки мають різні діапазони значень (від бінарних прапорців до великих цілих чисел), стандартизація забезпечує однакову вагу всіх ознак при навчанні моделі та

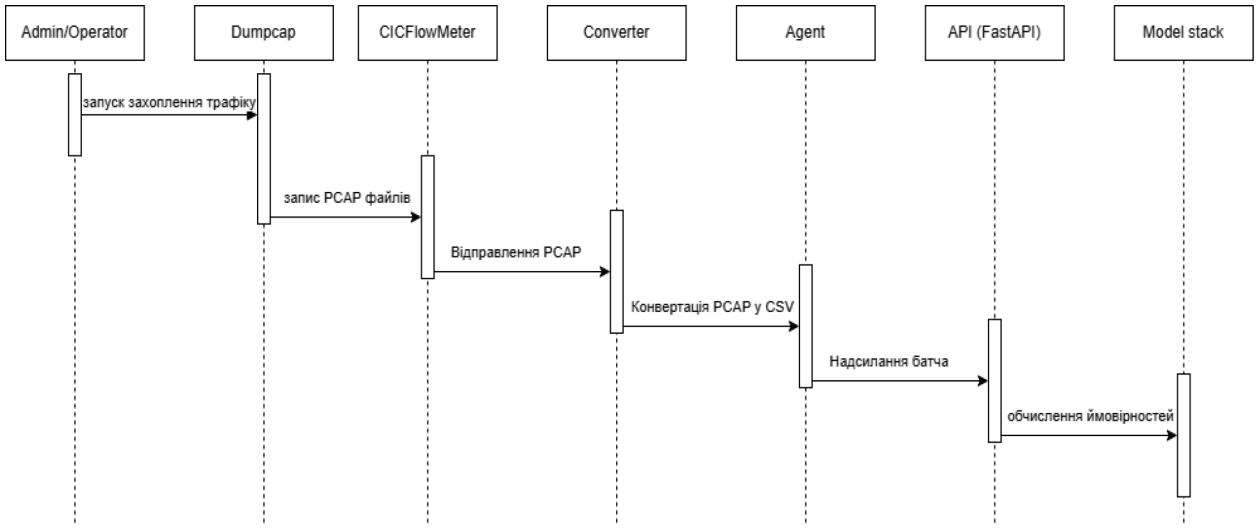

Рис. 1. Процес обробки мережевого трафіку в системі виявлення вторгнень

прискорює збіжність алгоритму градієнтного бустингу. Такий підхід покращує збіжність моделей машинного навчання та підвищує стабільність результатів класифікації.

Для класифікації мережевих потоків використано модель Light Gradient Boosting Machine (LightGBM) з наступними параметрами:

- num_leaves: 31 (кількість листків у дереві)
- max_depth: -1 (необмежена глибина дерева)
- learning_rate: 0.1 (швидкість навчання)
- n_estimators: 100 (кількість дерев)
- objective: ‘multiclass’ (багатокласова класифікація)

Ключовою інновацією запропонованого методу є алгоритм адаптивної порогової фільтрації результатів багатокласової класифікації, що застосовується на виході моделі LightGBM. На першому етапі для кожного мережевого потоку модель LightGBM формує вектор ймовірностей $P = \{p_1, p_2, \ldots, p_n\}$, де p_i відповідає ймовірності належності потоку до i-го класу атак або класу BENIGN. На відміну від традиційного підходу, де фінальний клас визначається як $arg\ max(P)$, у запропонованому методі використовується набір індивідуальних порогових значень $T = \{t_1, t_2, \ldots, t_n\}$, які задають мінімальний рівень впевненості для кожного класу атак.

Алгоритм порогової фільтрації побудований за наступною логікою:

1. Для кожного класу перевіряється умова $p_i \geq t_i$.
2. Формується множина кандидатів, що задовольняють свої порогові значення.
3. Якщо множина кандидатів порожня, потік класифікується як BENIGN (fallback-механізм).
4. Якщо кандидатів декілька, фінальний клас визначається як той, що має максимальну ймовірність серед кандидатів.

Додатково застосовується фільтрація за напрямком трафіку, що дозволяє виключити зовнішній трафік, який не становить безпосередньої загрози внутрішній мережі, та суттєво зменшити кількість хибних спрацювань.

Запропонований алгоритм дозволяє отримати зниження FPR через fallback-механізм; адаптивно налаштовувати чутливість IDS без перенавчання моделі; зберегти високу точність виявлення атак при мінімальних обчислювальних витратах. Зміна порогового значення дозволяє суттєво зменшити кількість хибнопозитивних спрацьовувань, не погіршуючи при цьому здатність системи виявляти реальні атаки. Таким чином, порогова фільтрація виконує роль механізму пост-обробки, який підвищує практичну придатність IDS.

Для навчання та тестування системи використано публічний датасет CIC-IDS2017, розроблений Канадським інститутом кібербезпеки (Canadian Institute for Cybersecurity) [11, 13]. Дані розподілено у співвідношенні 80:20 для навчання та тестування відповідно. Для забезпечення репрезентативності обох вибірок використано стратифікований розподіл (stratified split), що зберігає пропорції класів у навчальній та тестовій вибірках.

Для оцінки ефективності запропонованого підходу виконано порівняльний аналіз моделі LightGBM з багатошаровою нейронною мережею MLP (Multi-Layer Perceptron) за наступними метриками: Precision, Recall, F1-Score; False Positive Rate (FPR); час навчання, час інференсу. Порівняльні характеристики моделей наведено в таблиці 1.

Час навчання та інференсу вимірювався на робочій станції з процесором Intel Core i7-10700 (8 cores, 2.9 GHz), 16 GB RAM, без використання GPU.

Результати показують, що LightGBM перевершує MLP за всіма метриками при значно нижчих обчислювальних витратах. Час навчання LightGBM у 4 рази менший, а час інференсу майже вдвічі швидший порівняно з MLP. Таким

Таблиця 1

Порівняльні характеристики моделей

Модель	Precision	Recall	F1-Score	FPR	час навчання	час інференсу
MLP	0.930	0.912	0.921	9.1 %	180 хв	5.2 мс
LightGBM	0.958	0.941	0.949	2.1 %	45 хв	3.1 мс

Таблиця 2

Вплив компонентів системи на точність виявлення кібератак

Конфігурація	Precision	Recall	F1-Score	FPR
Базова LightGBM	0.89	0.87	0.88	12.3 %
+ SimpleImputer	0.92	0.9	0.91	9.5 %
+ StandardScaler	0.94	0.92	0.93	8.2 %
+ Порогова фільтрація (0.7)	0.96	0.94	0.95	2.1 %

чином, LightGBM забезпечує порівнянну або вищу точність класифікації при значно нижчих обчислювальних витратах.

MLP-модель продемонструвала чутливість до параметрів навчання та більшу схильність до хибних спрацювань, особливо за умов дисбалансу класів. Натомість LightGBM у поєднанні з пороговою фільтрацією забезпечив стабільніше зниження FPR, що є критично важливим для реальних систем виявлення вторгнень. Вплив компонентів системи на точність виявлення наведено в таблиці 2.

Проведений аналіз показав, що кожен компонент запропонованої системи робить внесок у загальну якість класифікації. Формування потоків за допомогою CICFlowMeter забезпечує інформативний набір ознак, препроцесинг підвищує стабільність навчання моделей, а використання LightGBM дозволяє ефективно моделювати складні залежності у даних. Використання імп'ютації знижує FPR (з 12.3 % до 9.5 %), що підтверджує важливість коректної обробки відсутніх значень. Додавання масштабування дає додаткове зниження FPR та покращує F1-score.

Найбільший ефект досягається при застосуванні порогової фільтрації яка дозволяє адаптувати поведінку системи до вимог конкретного середовища експлуатації та значно підвищує практичну ефективність IDS. FPR знижується з 8.2 % до 2.1 %, при цьому F1-score зростає з 0.932 до 0.949 за рахунок підвищення точності (precision).

Також, в роботі було проведено тестування запропонованого методу для різних типів атак Результати показують, що атаки DDoS виявляються найкраще (F1 = 0.978) завдяки чітким патернам великого обсягу трафіку. Атаки PortScan та DoS також добре розпізнаються (F1 ≈ 0.94–0.95). Складніші атаки (Bot, Web Attack, Infiltration) мають нижчі показники (F1 ≈ 0.85–0.90) через менш виражені статистичні патерни та малу кількість прикладів у навчальній вибірці.

Висновки

У статті запропоновано метод зниження хибних спрацювань у системах виявлення вторгнень на основі поєднання алгоритму LightGBM з механізмом адаптивної порогової фільтрації. У ході дослідження розроблено архітектуру IDS, яка охоплює повний цикл обробки мережевого трафіку: захоплення пакетів за допомогою Dumpcap, формування потоків і статистичних ознак із використанням CICFlowMeter, препроцесинг даних та багатокласову класифікацію на основі алгоритму LightGBM. Застосування стандартних методів препроцесингу дозволило підвищити стабільність навчання моделі та покращити узагальнюючу здатність класифікатора.

Ключовою новизною є алгоритм адаптивної порогової фільтрації з індивідуальними пороговими значеннями для кожного класу атак, механізмом fallback до класу BENIGN та фільтрацією за напрямком трафіку. Експериментальне тестування на датасеті CIC-IDS2017 (2.8 млн записів, 9 класів атак) показало зниження FPR з 8.2 % до 2.1 % (на 74 %) при F1-score = 0.949. Досліджено внесок кожного компонента: імпутація знижує FPR на 2.8 в.п., масштабування – на 1.3 в.п., порогова фільтрація – на 6.1 в.п. Порівняння з багатошаровою нейронною мережею MLP продемонструвало перевагу запропонованого методу: LightGBM з фільтрацією забезпечує вищу точність (F1 = 0.949 проти 0.921) при чотириразовому скороченні часу навчання (45 хв проти 180 хв) та майже вдвічі швидшому інференсі (3.1 мс проти 5.2 мс). Отримані результати свідчать, що поєднання класичних моделей машинного навчання з ефективними механізмами пост-обробки є перспективним напрямом побудови практичних IDS, здатних працювати в режимі реального часу. Подальші дослідження можуть бути спрямовані на автоматичну оптимізацію порогових значень, адаптацію методу до нових типів атак та інтеграцію запропонованого підходу у промислові системи кібербезпеки.

Список використаної літератури

1. Keepnet Labs. Cybersecurity Statistics 2024: Updated Trends and Data. URL: https://keepnetlabs.com/blog/171-cyber-security-statistics-2024-s-updated-trends-and-data

2. Ferrag M. A., Maglaras L. A (2024) Comprehensive Review of Intrusion Detection Systems Using Machine Learning. *SN Computer Science*. Vol. 5, № 6. https://doi.org/10.1007/s42979-024-03369-0

3. Corelight. Reducing IDS False Positives. 2025. URL: https://corelight.com/resources/glossary/ids-false-positives

4. Бандура В. В., Крихівський М. В., Чудик В. І. (2025) Прогнозування кібератак за допомогою алгоритмів штучного інтелекту виявлення аномалій. *Вісник Херсонського національного технічного університету*. Т. 1 (92), № 2. https://doi.org/10.35546/kntu2078-4481.2025.1.2.2

5. Ahmad W. et al. (2024) Comparative Analysis of Architectural Differences: Snort vs. Suricata. *Iraqi Journal for Computer Science and Mathematics*. Vol. 7, Issue 2. URL: https://www.ijict.edu.iq/index.php/ijict/article/download/290/122

6. Khan Z. et al. (2025) Improving Intrusion Detection with Hybrid Deep Learning Models: A Study on CIC-IDS2017, UNSW-NB15, and KDD CUP 99. *Journal of Information Systems Engineering and Management*. URL: https://www.researchgate.net/publication/389144460

7. Reducing False Positives in Intrusion Detection Systems with Adaptive Machine Learning Algorithms. ResearchGate. 2025. URL: https://www.researchgate.net/publication/390747122

8. Gupta N., Jain A. (2016) Reducing False Positive in Intrusion Detection System: A Survey. *International Journal of Computer Science and Information Technologies*. Vol. 7, No. 3. P. 1600–1603.

9. Yakub Reddy K., ShankarLingam G. (2024) Artificial Intelligence in Intrusion Detection Systems: Trends, Frameworks, and Future Directions for Cybersecurity. *International Journal of Intelligent Systems and Applications in Engineering*. Vol. 12, No. 21. URL: https://ijisae.org/index.php/IJISAE/article/view/7689

10. Almiani M. et al. (2024) Comparative Performance Evaluation of Machine Learning Algorithms for Cyber Intrusion Detection. *Preprints*. https://doi.org/10.20944/preprints202412.0497.v1

11. Canadian Institute for Cybersecurity. Intrusion Detection Evaluation Dataset (CIC-IDS2017). University of New Brunswick. 2017. URL: https://www.unb.ca/cic/datasets/ids-2017.html

12. Khan Z. I. et al. (2024) A Comprehensive Study on CIC-IDS2017 Dataset for Intrusion Detection Systems. ResearchGate. URL: https://www.researchgate.net/publication/378709289

13. Maseer Z. K. et al. (2021) Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset. IEEE Access. Vol. 9. P. 22351–22370. DOI: 10.1109/ACCESS.2021.3056614

References

1. Keepnet Labs. Cybersecurity Statistics 2024: Updated Trends and Data. URL: https://keepnetlabs.com/blog/171-cyber-security-statistics-2024-s-updated-trends-and-data

2. Ferrag M. A., Maglaras L. A (2024) Comprehensive Review of Intrusion Detection Systems Using Machine Learning. *SN Computer Science*. Vol. 5, № 6. https://doi.org/10.1007/s42979-024-03369-0

3. Corelight. Reducing IDS False Positives. 2025. URL: https://corelight.com/resources/glossary/ids-false-positives

4. Bandura V. V., Krykhivskyi M. V., Chudyk V. I. (2025) Prohnozuvannia kiberatak za dopomohoiu alhorytmiv shtuchnoho intelektu vyiavlennia anomalii. [Forecasting cyberattacks using artificial intelligence algorithms for anomaly detection.] *Visnyk Khmelnytskoho natsionalnoho universytetu*. Vol. 1 (92), № 2. https://doi.org/10.35546/kntu2078-4481.2025.1.2.2 [in Ukrainian].

5. Ahmad W. et al. (2024) Comparative Analysis of Architectural Differences: Snort vs. Suricata. *Iraqi Journal for Computer Science and Mathematics*. Vol. 7, Issue 2. URL: https://www.ijict.edu.iq/index.php/ijict/article/download/290/122

6. Khan Z. et al. (2025) Improving Intrusion Detection with Hybrid Deep Learning Models: A Study on CIC-IDS2017, UNSW-NB15, and KDD CUP 99. *Journal of Information Systems Engineering and Management*. URL: https://www.researchgate.net/publication/389144460

7. Reducing False Positives in Intrusion Detection Systems with Adaptive Machine Learning Algorithms. ResearchGate. 2025. URL: https://www.researchgate.net/publication/390747122

8. Gupta N., Jain A. (2016) Reducing False Positive in Intrusion Detection System: A Survey. *International Journal of Computer Science and Information Technologies*. Vol. 7, No. 3. P. 1600–1603.

9. Yakub Reddy K., ShankarLingam G. (2024) Artificial Intelligence in Intrusion Detection Systems: Trends, Frameworks, and Future Directions for Cybersecurity. *International Journal of Intelligent Systems and Applications in Engineering*. Vol. 12, No. 21. URL: https://ijisae.org/index.php/IJISAE/article/view/7689

10. Almiani M. et al. (2024)Comparative Performance Evaluation of Machine Learning Algorithms for Cyber Intrusion Detection. *Preprints*. https://doi.org/10.20944/preprints202412.0497.v1

11. Canadian Institute for Cybersecurity. Intrusion Detection Evaluation Dataset (CIC-IDS2017). University of New Brunswick. 2017. URL: https://www.unb.ca/cic/datasets/ids-2017.html

12. Khan Z. I. et al. (2024) A Comprehensive Study on CIC-IDS2017 Dataset for Intrusion Detection Systems. ResearchGate. URL: https://www.researchgate.net/publication/378709289

13. Maseer Z. K. et al. (2021) Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset. IEEE Access. Vol. 9. P. 22351–22370. DOI: 10.1109/ACCESS.2021.3056614

Дата першого надходження статті до видання: 18.01.2026
Дата прийняття статті до друку після рецензування: 20.02.2026
Дата публікації (оприлюднення) статті: 30.04.2026