https://doi.org/10.31891/2219-9365-2026-85-31
УДК 004.056:004.852:004.75

СЕМЕНЮК Богдан
Хмельницький національний університет
https://orcid.org/0009-0001-8831-8835
e-mail: bohdan.semenuik@khmnu.edu.ua
КОРЕЦЬКА Людмила
Хмельницький національний університет
https://orcid.org/0000-0002-4284-4936
e-mail: koretskal@khmnu.edu.ua

ОСОБЛИВОСТІ ПРОЄКТУВАННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ СОНІФІКАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ

У роботі досліджено особливості проєктування системи виявлення вторгнень (IDS) на основі частотно-часового представлення мережевого трафіку. Актуальність дослідження зумовлена зростанням складності комп'ютерних атак та обмеженнями традиційних векторних підходів до представлення ознак, що ускладнюють виявлення складних аномалій і призводять до підвищеного рівня помилкових рішень.

Запропоновано підхід до перетворення багатовимірного вектора мережевих ознак у дискретний PCM-сигнал із подальшим застосуванням короткочасного перетворення Фур'є для формування спектрограм, які аналізуються за допомогою двовимірної згорткової нейронної мережі. Такий підхід забезпечує структуроване 2D-подання трафіку та підвищує інформативність вхідних даних для задачі класифікації атак.

З метою зменшення впливу дисбалансу класів розроблено сигнатурозбережний адаптивний метод балансування навчальної вибірки, що враховує помилки базової моделі під час формування розширеної множини даних. Додатково формалізовано т-інтервал невизначеності прогнозу та реалізовано каскадний механізм прийняття рішень із використанням допоміжного класифікатора для перевизначення результатів у критичній зоні. Окрему увагу приділено забезпеченню принципу незалежності тестової вибірки з метою запобігання витоку даних та коректної оцінки узагальнювальної здатності моделі.

Експериментальне дослідження підтвердило доцільність використання частотно-часового представлення трафіку та запропонованих механізмів підвищення точності, що дозволило зменшити рівень хибнонегативних рішень та підвищити стабільність класифікації в умовах дисбалансу класів.

Ключові слова: система виявлення вторгнень, соніфікація мережевого трафіку, PCM-кодування, спектрограма, 2D-CNN, дисбаланс класів, зона невизначеності, каскадна класифікація, витік даних, корпоративні мережі.

SEMENUIK Bohdan, KORETSKA Lyudmyla
Khmelnytskyi National University

FEATURES OF DESIGN AND INVESTIGATION OF AN INTRUSION DETECTION SYSTEM BASED ON NETWORK TRAFFIC SONIFICATION

This paper investigates the design and research features of an intrusion detection system (IDS) based on the time–frequency representation of network traffic. The relevance of the study is obusловed by the increasing complexity of cyberattacks and the limitations of traditional vector-based feature representations, which often lead to insufficient detection of complex anomalies and elevated false decision rates. A method for transforming multidimensional network feature vectors into discrete PCM signals followed by short-time Fourier transform (STFT) is proposed to generate spectrograms analyzed using a two-dimensional convolutional neural network (2D-CNN). The proposed approach provides a structured two-dimensional representation of network traffic and enhances the informativeness of input data for attack classification tasks.

To mitigate the impact of class imbalance, a signature-preserving adaptive balancing method is developed, which considers the misclassification patterns of the baseline model during the formation of the extended training set. Additionally, a т-based uncertainty interval is formalized, and a cascade decision-making mechanism is introduced using an auxiliary classifier to refine predictions within the uncertainty zone. Particular attention is paid to maintaining strict independence between training and test datasets in order to prevent data leakage and ensure reliable generalization performance evaluation.

Experimental evaluation confirms the effectiveness of the proposed time–frequency representation and accuracy enhancement mechanisms, demonstrating a reduction in the false negative rate and improved classification stability under class imbalance conditions.

Keywords: intrusion detection system, network traffic sonification, PCM encoding, spectrogram, 2D-CNN, class imbalance, uncertainty zone, cascade classification, data leakage prevention, corporate networks.

Стаття надійшла до редакції / Received 06.01.2026
Прийнята до друку / Accepted 04.02.2026
Опубліковано / Published 05.03.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Стрімкий розвиток інформаційних технологій і масштабування корпоративних мереж зумовлюють постійне зростання кількості та складності комп'ютерних атак. Сучасні мережеві середовища

характеризуються високою інтенсивністю обміну даними, різноманітністю протоколів і сервісів, а також появою нових типів загроз, включаючи багатоступеневі та модифіковані атаки. У таких умовах системи виявлення вторгнень (Intrusion Detection Systems, IDS) залишаються одним із ключових компонентів забезпечення інформаційної безпеки корпоративних мереж.

Аналіз сучасних досліджень свідчить про активне впровадження методів машинного та глибинного навчання у задачах виявлення вторгнень [1, 8, 12]. Застосування згорткових і рекурентних нейронних мереж, автоенкодерів та генеративних моделей дозволяє підвищувати точність детекції, зокрема для складних або раніше невідомих атак [4], [15, 18]. Водночас низка проблем залишається невирішеною.

По-перше, більшість існуючих IDS використовують векторне представлення мережевих ознак, що не враховує потенційні частотно-часові закономірності у структурі трафіку. Такий підхід обмежує можливості виявлення складних аномалій, які проявляються не лише у значеннях окремих параметрів, а й у їх просторово-структурній взаємодії. По-друге, характерною особливістю реальних мережевих даних є суттєвий дисбаланс класів, коли кількість нормальних з'єднань значно перевищує кількість атак. Це призводить до зниження повноти виявлення міноритарних класів і збільшення рівня хибнонегативних рішень (False Negative Rate), що становить особливу небезпеку для корпоративних систем [9, 16].

Крім того, у практиці побудови та оцінювання IDS часто виникає проблема витоку даних (data leakage), яка пов'язана з некоректним використанням тестової вибірки під час налаштування моделі або балансування даних. Порушення принципу незалежності тестового набору призводить до завищених оцінок точності та спотворення реальної узагальнювальної здатності моделі, що є критичним у задачах інформаційної безпеки.

Одним із перспективних напрямів підвищення ефективності IDS є використання методів соніфікації мережевого трафіку. Соніфікація передбачає перетворення багатовимірного вектора ознак мережевого з'єднання у звуковий сигнал із подальшим аналізом його спектральних характеристик. Такий підхід дозволяє перейти від одномірного векторного подання до структурованого частотно-часового представлення, що відкриває можливість застосування методів комп'ютерного зору, зокрема двовимірних згорткових нейронних мереж, для класифікації спектрограм. Попри наявність окремих досліджень у сфері аналізу часових рядів [13], комплексне обґрунтування особливостей проєктування IDS на основі соніфікації мережевого трафіку залишається недостатньо висвітленим.

У зв'язку з цим актуальною є задача дослідження особливостей проєктування системи виявлення вторгнень, що поєднує частотно-часове представлення мережевого трафіку, механізми адаптивного балансування навчальної вибірки та каскадну обробку рішень у зоні невизначеності прогнозу із забезпеченням незалежності тестової вибірки.

Метою роботи є дослідження особливостей проєктування та експериментальне обґрунтування ефективності системи виявлення вторгнень на основі соніфікації мережевого трафіку, а також розроблення механізмів підвищення точності класифікації в умовах дисбалансу класів і зони невизначеності прогнозу.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– формалізувати процес перетворення мережевого трафіку у частотно-часове представлення;

– розробити механізм сигнатурозбережного адаптивного балансування навчальної вибірки;

– формалізувати τ-інтервал невизначеності та реалізувати каскадний механізм прийняття рішень;

– забезпечити коректну методологію розділення навчальної та тестової вибірок із запобіганням витоку даних;

– провести експериментальне дослідження та порівняльний аналіз запропонованих підходів.

Аналіз сучасних підходів до виявлення вторгнень

Сучасні системи виявлення вторгнень базуються на широкому спектрі методів аналізу мережевого трафіку, серед яких домінують підходи машинного та глибинного навчання. Активний розвиток ML/DL-технологій зумовив значне підвищення точності класифікації атак, однак одночасно виявив низку методологічних і прикладних проблем, пов'язаних із представленням даних, дисбалансом класів і стабільністю моделей.

Методи машинного та глибинного навчання в IDS

Ранні ML-підходи до побудови IDS ґрунтувалися на класичних алгоритмах класифікації, таких як SVM, k-NN, Decision Tree та Random Forest. Застосування таких методів до стандартних датасетів (KDD, NSL-KDD, UNSW-NB15) дозволило досягти високих показників точності за умов коректного відбору ознак [12]. Однак ефективність класичних алгоритмів значною мірою залежить від якості інженерії ознак і не завжди забезпечує достатню узагальнювальну здатність.

Подальший розвиток отримали глибинні нейронні мережі, зокрема згорткові (CNN), рекурентні (RNN, LSTM) та гібридні архітектури [1, 7, 10]. CNN ефективно застосовуються для автоматичного вилучення локальних структурних патернів у даних, тоді як RNN дозволяють враховувати часові залежності в потоках

або сесіях. Дослідження демонструють покращення показників Precision та Recall у порівнянні з класичними ML-алгоритмами, особливо для складних або багатокласових задач.

Окремий напрям пов'язаний із використанням генеративних моделей та adversarial learning [15, 18], що дозволяє розширювати навчальні вибірки або підвищувати стійкість систем до модифікованих атак. Водночас складність таких моделей і потреба у значних обчислювальних ресурсах обмежують їх практичне впровадження у режимі реального часу.

Проблема дисбалансу класів у задачах IDS

Характерною особливістю задачі виявлення вторгнень є суттєвий дисбаланс між кількістю нормальних з'єднань та атак. У більшості реальних сценаріїв нормальний трафік становить переважну частку даних, тоді як окремі типи атак представлені незначною кількістю прикладів. Це призводить до зміщення функції ризику моделі в бік домінуючого класу та зниження повноти виявлення міноритарних класів.

Для компенсації дисбалансу застосовуються методи надсемплінгу (SMOTE, ADASYN), підвибірки або гібридні стратегії [9]. Такі підходи дозволяють вирівняти розподіл класів у навчальній множині, однак можуть призводити до втрати структурних характеристик даних або до формування синтетичних зразків, які не повністю відображають реальні властивості атак. Крім того, некоректне застосування балансування без чіткого розділення навчальної та тестової вибірок може спричинити витік даних та завищення оцінок точності.

У ряді досліджень особлива увага приділяється зменшенню рівня хибнонегативних рішень (FNR), оскільки пропущена атака становить значно більшу загрозу, ніж хибнопозитивне спрацювання [16]. Проте більшість робіт зосереджена переважно на показнику Accuracy, що не завжди адекватно відображає ефективність IDS у разі дисбалансу класів.

Представлення мережевого трафіку та його обмеження

Більшість сучасних IDS використовують векторне представлення мережевого з'єднання у вигляді набору числових ознак:

$$x_i = (x_{i1}, x_{i2}, \dots, x_{id}) \in R^d, \quad (1)$$

де d– кількість параметрів, що описують з'єднання.

Такий підхід є зручним для застосування стандартних алгоритмів класифікації, однак не враховує потенційні структурні взаємозв'язки між ознаками. Багатовимірний простір параметрів розглядається як набір незалежних координат, що може обмежувати здатність моделі виявляти складні закономірності, які проявляються у взаємодії ознак або у їх частотно-часовій структурі.

Окремі дослідження у сфері аналізу часових рядів і багатовимірних сигналів [13] демонструють, що перехід до частотно-часового представлення дозволяє виявляти додаткові закономірності, недоступні при традиційному векторному аналізі. Проте комплексне застосування такого підходу до задачі IDS із формалізацією механізмів підвищення точності та обґрунтуванням методології оцінювання залишається недостатньо дослідженим.

Методологічні аспекти оцінювання IDS

Коректність оцінювання ефективності IDS є критично важливою для практичного застосування. Однією з ключових вимог є забезпечення незалежності тестової вибірки від процесу навчання та налаштування моделі. Порушення цього принципу, зокрема через використання тестових даних під час балансування або підбору гіперпараметрів, призводить до витоку даних (data leakage) та завищених показників точності.

У задачах із дисбалансом класів доцільним є використання комплексних метрик оцінювання, таких як Precision, Recall, F1-score та FNR, поряд із загальною точністю. Особливо важливим є контроль FNR, оскільки пропущена атака може мати критичні наслідки для корпоративної мережі.

Таким чином, аналіз сучасних підходів дозволяє сформулювати такі основні проблеми:

– обмеженість традиційного векторного представлення мережевого трафіку;

– зниження ефективності класифікації в умовах дисбалансу класів;

– підвищений рівень хибнонегативних рішень;

– ризик витоку даних при некоректному розділенні вибірок.

Вирішення зазначених проблем потребує комплексного підходу, що поєднує альтернативне представлення мережевого трафіку, адаптивні механізми балансування та каскадну обробку рішень у зоні невизначеності прогнозу із суворим дотриманням принципу незалежності тестової вибірки.

Формальна модель системи виявлення вторгнень

У цьому розділі формалізовано структуру системи виявлення вторгнень на основі соніфікації мережевого трафіку, яка поєднує частотно-часове представлення даних, глибинну класифікацію спектрограм та каскадний механізм прийняття рішень.

Формалізація множини мережевих з'єднань

Нехай задано множину мережевих з'єднань

$$X = \{x_i\}_{i=1}^{N}, \tag{2}$$

де N – кількість з'єднань у вибірці, $x_i \in \mathrm{R}^d$ – вектор ознак і-го з'єднання, d – кількість параметрів, що описують з'єднання (тривалість, кількість пакетів, байтів, службові поля тощо).

Кожному з'єднанню відповідає мітка класу

$$y_i \in \{0,1\}, \tag{3}$$

де 0 – нормальний трафік, 1 – атака (у випадку бінарної класифікації).

Метою системи є побудова відображення

$$F: R^d \to \{0,1\}, \tag{3}$$

$$\tag{4}$$

яке мінімізує функцію ризику на генеральній сукупності з'єднань.

На відміну від традиційних підходів, у запропонованій моделі вектор ознак не подається безпосередньо до класифікатора, а проходить етап частотно-часового перетворення.

Перетворення вектора ознак у PCM-сигнал

Для кожного вектора x_iвиконується нормалізація:

$$\tilde{x}_{ij} = \frac{x_{ij} - \min\limits_{j}}{\max\limits_{j} - \min\limits_{j}}, \tag{5}$$

де $\min_j$, $\max_j$ – мінімальне та максимальне значення j-ї ознаки у навчальній вибірці.

Після нормалізації формується дискретний сигнал

$$s_i(n) = g(\tilde{x}_i), \tag{6}$$

де $n = 1, \dots, d$, $g(\cdot)$ – відображення нормалізованого вектора в амплітуду сигналу.

Таким чином, багатовимірний вектор ознак інтерпретується як дискретна амплітудна послідовність, що може розглядатися як PCM-сигнал. Такий підхід дозволяє перейти від абстрактного простору ознак до сигналу, придатного для спектрального аналізу.

Частотно-часове представлення за допомогою STFT

Для отримання спектральної структури сигналу застосовується короткочасне перетворення Фур'є (STFT):

$$S_i(f,t) = \left| \sum_{n} s_i\,(n) w(n-t) e^{-j2\pi f n} \right|, \tag{7}$$

де $w(n-t)$ – віконна функція, f – частота, t – часовий зсув, $S_i(f,t)$ – амплітудний спектр сигналу.

Результатом є спектрограма

$$\mathcal{S}_i \in \mathbb{R}^{F \times T}, \tag{8}$$

де F – кількість частотних компонент, T – кількість часових сегментів.

Таким чином, кожне мережеве з'єднання подається у вигляді двовимірної структури, що містить частотно-часову інформацію про взаємозв'язки між ознаками.

Класифікація спектрограм за допомогою 2D-CNN

Спектрограма $\mathcal{S}_i$подається на вхід двовимірної згорткової нейронної мережі:

$$\hat{y}_i = F_\theta(\mathcal{S}_i), \tag{9}$$

де F_θ– параметризована 2D-CNN, θ – множина вагових коефіцієнтів мережі, $\hat{y}_i$– прогнозована ймовірність належності до класу атаки.

Базове рішення приймається за пороговим правилом:

$$\hat{y}_i = \begin{cases} 1, & P(y = 1 \mid \mathcal{S}_i) \geq 0.5, \\ 0, & \text{інакше.} \end{cases} \tag{10}$$

Однак таке жорстке порогове правило не враховує невизначеність прогнозу, що є критичним у задачах IDS.

Каскадний механізм прийняття рішень

Для врахування невизначеності вводиться τ-інтервал:

$$\tau_L \leq P(y = 1 \mid \mathcal{S}_i) \leq \tau_U, \tag{11}$$

де τ_L, τ_U – нижня та верхня межі зони невизначеності.

Якщо прогноз потрапляє в цей інтервал, рішення передається допоміжному класифікатору:

$$\hat{y}_i^{final} = G_\phi(\mathcal{S}_i), \tag{12}$$

де G_ϕ – допоміжна модель, навчена на прикладах, що були помилково класифіковані базовою мережею.

Таким чином, система набуває каскадної структури:

$$F_{cascade} = \begin{cases} F_\theta, & \text{поза зоною невизначеності,} \\ G_\phi, & \text{у межах } [\tau_L, \tau_U]. \end{cases} \tag{13}$$

Розділення навчальної та тестової вибірок

Нехай множина даних

$$D = D_{train} \cup D_{test}, \tag{14}$$

при цьому

$$D_{train} \cap D_{test} = \emptyset. \tag{15}$$

Усі процедури:

– нормалізація,

– балансування,

– налаштування гіперпараметрів,

– визначення меж τ_L, τ_U, виконуються виключно на D_{train}.

Тестова вибірка використовується лише для фінальної оцінки моделі, що забезпечує відсутність витоку даних та коректну оцінку узагальнювальної здатності системи.

Таким чином, формальна модель IDS включає:

1. перетворення багатовимірного вектора ознак у PCM-сигнал;
2. частотно-часове представлення за допомогою STFT;
3. класифікацію спектрограм 2D-CNN;
4. каскадний механізм обробки зони невизначеності;
5. суворе дотримання принципу незалежності тестової вибірки.

Запропонована структура створює основу для підвищення точності виявлення атак у складних умовах дисбалансу класів та невизначеності прогнозу.

Методи підвищення точності системи

Побудова IDS на основі частотно-часового представлення мережевого трафіку дозволяє підвищити інформативність вхідних даних, однак сама по собі не гарантує мінімізації хибнонегативних рішень та стабільності класифікації в умовах дисбалансу класів. У цьому розділі розглянуто комплекс методів, спрямованих на підвищення точності системи, зокрема сигнатурозбережне адаптивне балансування та каскадну обробку прогнозів у зоні невизначеності.

Сигнатурозбережне адаптивне балансування навчальної вибірки

Нехай навчальна множина має вигляд

$$D_{train} = \{(x_i, y_i)\}_{i=1}^{N_{train}}, \tag{16}$$

де кількість об’єктів класу атаки значно менша за кількість об’єктів нормального класу:

$$N_{attack} \ll N_{normal}. \tag{17}$$

У такому випадку функція ризику моделі зміщується в бік домінуючого класу, що призводить до зниження показника Recall для атак і збільшення FNR.

Традиційні методи балансування (наприклад, SMOTE) формують синтетичні зразки міноритарного класу шляхом інтерполяції у просторі ознак [9]. Проте у випадку складної частотно-часової структури трафіку така інтерполяція може спотворювати внутрішню сигнатуру атак.

У запропонованому підході балансування здійснюється з урахуванням помилок базової моделі. Нехай після початкового навчання 2D-CNN визначено множину помилково класифікованих прикладів:

$$E = \{x_i \in D_{train} \mid \hat{y}_i \neq y_i\}. \tag{18}$$

Формується підмножина міноритарних об'єктів із найбільшим внеском у помилки:

$$E_{attack} = \{x_i \in E \mid y_i = 1\}. \tag{19}$$

Розширення навчальної вибірки здійснюється шляхом підвищення ваг або дублювання елементів із E_{attack}, що дозволяє зосередити процес навчання на складних прикладах без порушення їх структурної цілісності.

Формально модифікована функція втрат набуває вигляду

$$L = -\sum_{i=1}^{N_{train}} w_i \,[y_i \log \hat{y}_i + (1 - y_i)\log(1 - \hat{y}_i)], \tag{20}$$

де $w_i > 1$ для елементів із E_{attack}, $w_i = 1$для інших об'єктів.

Такий підхід дозволяє зменшити вплив дисбалансу на процес оптимізації без формування штучних спотворених зразків і зберігає сигнатурні характеристики атак у спектрограмах.

Формалізація зони невизначеності прогнозу

У класичному підході рішення приймається за фіксованим порогом (0.5). Проте значна частина помилок виникає у випадках, коли прогнозована ймовірність близька до порогового значення.

Вводиться τ-інтервал невизначеності:

$$\tau_L \leq P(y = 1 \mid \mathcal{S}_i) \leq \tau_U, \tag{21}$$

де $0 < \tau_L < 0.5 < \tau_U < 1$.

Множина об'єктів невизначеності визначається як

$$U = \{x_i \mid P(y = 1 \mid \mathcal{S}_i) \in [\tau_L, \tau_U]\}. \tag{22}$$

Емпіричний аналіз показує, що саме в цій області зосереджена значна частка хибнонегативних рішень. Таким чином, замість жорсткого порогового відсікання застосовується селективне перевизначення рішення.

Каскадний механізм перевизначення рішень

Для об'єктів із множини Uвикористовується допоміжний класифікатор

$$\hat{y}_i^{aux} = G_\phi(\mathcal{S}_i), \tag{23}$$

де G_ϕ– модель, навчена на підмножині складних або помилкових прикладів.

Фінальне рішення приймається за правилом

$$\hat{y}_i^{final} = \begin{cases} \hat{y}_i, & x_i \notin U, \\ \hat{y}_i^{aux}, & x_i \in U. \end{cases} \tag{24}$$

Таким чином, система реалізує каскадну структуру прийняття рішень, у якій базова модель забезпечує основну класифікацію, а допоміжна модель виконує уточнення прогнозу у критичній області.

Такий підхід дозволяє: зменшити кількість хибнонегативних рішень, підвищити Recall для міноритарного класу, зберегти загальну стабільність Accuracy.

Забезпечення відсутності витоку даних

Усі процедури балансування, визначення ваг w_i, налаштування меж τ_L, τ_Uта навчання допоміжної моделі виконуються виключно на навчальній вибірці. Формально:

$$\theta, \phi, \tau_L, \tau_U = f(D_{train}), \tag{25}$$

де D_{test} не використовується на жодному етапі оптимізації.

Такий підхід забезпечує коректну оцінку узагальнювальної здатності системи та запобігає завищенню показників точності внаслідок витоку інформації.

Отже, запропонований комплекс методів підвищення точності включає: сигнатурозбережне адаптивне балансування, формалізацію τ-зони невизначеності, каскадний механізм перевизначення рішень, суворе дотримання принципу незалежності тестової вибірки.

Застосування цих механізмів дозволяє мінімізувати FNR та підвищити стабільність IDS у складних умовах дисбалансу класів.

Експериментальне дослідження

Метою експериментального дослідження є оцінювання впливу частотно-часового представлення мережевого трафіку, адаптивного балансування та каскадного механізму обробки зони невизначеності на точність системи виявлення вторгнень.

Експеримент проведено на стандартному наборі мережевих даних, що містить розмічені приклади нормального трафіку та атак. Дані розділено на навчальну та тестову вибірки з дотриманням умови

$$D_{train} \cap D_{test} = \emptyset, \tag{26}$$

при цьому всі процедури нормалізації, балансування та налаштування гіперпараметрів виконувалися виключно на D_{train}.

Для оцінювання ефективності моделей використовувалася метрика Accuracy:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \tag{27}$$

де TP – кількість правильно виявлених атак, TN – кількість правильно визначених нормальних з'єднань, FP – кількість хибнопозитивних рішень, FN – кількість хибнонегативних рішень.

Порівнювалися чотири конфігурації системи, отримані результати наведено у таблиці 1.

Таблиця 1

Кількість варіантів централізації в архітектурі систем

Модель	Accuracy
Векторна модель	76%
Соніфікована модель	76–77%
Соніфікована + балансування	82–83%
Соніфікована + балансування + τ-зона	84–85%

З таблиці видно, що без додаткових механізмів підвищення точності перехід до частотно-часового представлення сам по собі не забезпечує суттєвого приросту Accuracy. Соніфікована модель демонструє близькі до базової моделі результати, що свідчить про коректність перетворення без втрати інформації.

Водночас застосування сигнатурозбережного адаптивного балансування дозволило підвищити точність до 82–83%. Це пояснюється зменшенням впливу дисбалансу класів на функцію втрат і покращенням виявлення міноритарного класу атак.

Додаткове введення τ-зони невизначеності та каскадного механізму перевизначення рішень забезпечило подальше зростання точності до 84–85%. Основний внесок у покращення показників пов'язаний зі зменшенням кількості хибнонегативних рішень у прикордонних випадках, коли прогноз базової моделі був близьким до порогового значення.

Аналіз отриманих результатів дозволяє зробити такі висновки:

1. Частотно-часове представлення мережевого трафіку забезпечує еквівалентну або незначно кращу якість класифікації порівняно з традиційним векторним підходом без погіршення показників точності.

2. Основний приріст ефективності досягається за рахунок адаптивного балансування навчальної вибірки, що дозволяє зменшити вплив дисбалансу класів.

3. Формалізація τ-інтервалу невизначеності та застосування допоміжного класифікатора дозволяють додатково зменшити частку прикордонних помилок і підвищити стабільність системи.

Таким чином, експериментально підтверджено, що комплексне застосування частотно-часового представлення, сигнатурозбережного балансування та каскадної обробки рішень забезпечує покращення точності системи виявлення вторгнень приблизно на 8–9 відсоткових пунктів порівняно з базовою векторною моделлю.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У роботі досліджено особливості проєктування системи виявлення вторгнень на основі соніфікації мережевого трафіку та частотно-часового представлення даних. Показано, що традиційне векторне подання ознак обмежує можливості виявлення складних закономірностей і є чутливим до дисбалансу класів.

Формалізовано модель перетворення багатовимірного вектора мережевих параметрів у PCM-сигнал із подальшим застосуванням короткочасного перетворення Фур'є для формування спектрограм, що

аналізуються 2D-CNN. Запропоновано сигнатурозбережний адаптивний метод балансування навчальної вибірки та формалізовано τ-інтервал невизначеності прогнозу з реалізацією каскадного механізму перевизначення рішень.

Забезпечено принцип незалежності тестової вибірки для запобігання витоку даних та коректної оцінки узагальнювальної здатності моделі. Експериментальні результати підтвердили, що комплексне застосування запропонованих підходів дозволяє підвищити точність системи до 84–85% порівняно з 76% для базової векторної моделі.

Отримані результати можуть бути використані при розробленні інтелектуальних IDS для корпоративних мереж та є основою для подальших досліджень у напрямі розширення мультикласових моделей і оптимізації обчислювальної складності.

Література

1. Ahmad Z., Khan A.S., Shiang C.W., Abdullah J., Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Emerging Telecommunications Technologies. 2021. Vol. 32(1). e4150. https://doi.org/10.1002/ett.4150

2. Alladi T., Chamola V., Sikdar B., Choo K.-K.R. Consumer IoT: Security vulnerability case studies and solutions. IEEE Consumer Electronics Magazine. 2020. Vol. 9(2). P. 17–25. https://doi.org/10.1109/MCE.2019.2953740

3. Baich M., Sael N. Enhancing machine learning model prediction with feature selection for botnet intrusion detection. Engineering Proceedings. 2025. Vol. 112(1). P. 55. https://doi.org/10.3390/engproc2025112055

4. Cai Z., Du H., Wang H., Zhang J., Si Y., Li P. One-dimensional convolutional Wasserstein generative adversarial network based intrusion detection method for industrial control systems. Electronics. 2023. Vol. 12(22). P. 4653. https://doi.org/10.3390/electronics12224653

5. Dalou' J., Al-Duwairi B., Al-Jarrah M. Adaptive entropy-based detection and mitigation of DDoS attacks in SDN networks. International Journal of Computing. 2020. Vol. 19(3). P. 399–410. https://doi.org/10.47839/ijc.19.3.1889

6. Denysiuk D., Savenko O., Lysenko S., Savenko B., Kashtalian A. Method for detecting steganographic changes in images using machine learning. In: Proceedings of the 13th International Conference on Dependable Systems, Services and Technologies (DESSERT 2023). Athens: IEEE, 2023. P. 1–6. https://doi.org/10.1109/DESSERT61349.2023.10416453

7. Farooq M., Ahmad F. Improved intrusion detection in IoT using multi-layered neural architectures. International Journal of Computing. 2024. Vol. 23(2). P. 268–273. https://doi.org/10.47839/ijc.23.2.3546

8. Hussain A., Sharif H., Rehman F. et al. A systematic review of intrusion detection systems in Internet of Things using ML and DL. In: 2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). Sukkur: IEEE, 2023. https://doi.org/10.1109/iCoMET57998.2023.10099142

9. Joloudari J.H., Marefat A., Nematollahi M.A., Oyelere S.S., Hussain S. Effective class-imbalance learning based on SMOTE and convolutional neural networks. Applied Sciences. 2023. Vol. 13(6). P. 4006. https://doi.org/10.3390/app13064006

10. Joseph J.E., Aleke N.T., Onyeanisi O.P. Deep learning based intrusion detection system for network security in IoT system. International Journal of Education, Management, and Technology. 2025. Vol. 3(1). P. 119–138. https://doi.org/10.58578/ijemt.v3i1.4539

11. Kashtalian A., Lysenko S., Sachenko A., Savenko B., Savenko O., Nicheporuk A. Evaluation criteria of centralization options in the architecture of multicomputer systems with traps and baits. Radioelectronic and Computer Systems. 2025. Vol. 1. P. 264–297. https://doi.org/10.32620/reks.2025.1.18

12. Kilincer I.F., Ertam F., Sengur A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks. 2021. Vol. 188. P. 107840. https://doi.org/10.1016/j.comnet.2021.107840

13. Li G., Jung J.J. Deep learning for anomaly detection in multivariate time series: Approaches, applications, and challenges. Information Fusion. 2023. Vol. 91. P. 93–102. https://doi.org/10.1016/j.inffus.2022.10.008

14. Maniriho P., Niyigaba E., Bizimana Z. et al. Anomaly-based intrusion detection approach for IoT networks using machine learning. In: 2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM). Surabaya: IEEE, 2020. P. 303–308. https://doi.org/10.1109/CENIM51130.2020.9297958

15. Mari A.-G., Zinca D., Dobrota V. Development of a machine-learning intrusion detection system and testing of its performance using a generative adversarial network. Sensors. 2023. Vol. 23(3). P. 1315. https://doi.org/10.3390/s23031315

16. Mijalkovic J., Spognardi A. Reducing the false negative rate in deep learning based network intrusion detection systems. Algorithms. 2022. Vol. 15(8). P. 258. https://doi.org/10.3390/a15080258

17. Sathaporn P., Krungseanmuang W., Chaowalittawin V. et al. DDoS detection using a hybrid CNN-RNN model enhanced with multi-head attention for cloud infrastructure. Applied Sciences. 2025. Vol. 15(21). P. 11567.

https://doi.org/10.3390/app152111567

18. Shahriar M.H., Haque N.I., Rahman M.A., Alonso M. G-IDS: Generative adversarial networks assisted intrusion detection system. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). Madrid: IEEE, 2020. P. 376–385. https://doi.org/10.1109/COMPSAC48688.2020.000218

19. Sheibani M., Konur S., Awan I., Qureshi A. A multi-layered defence strategy against DDoS attacks in SDN/NFV-based 5G mobile networks. Electronics. 2024. Vol. 13(8). P. 1515. https://doi.org/10.3390/electronics13081515

20. Sheikh M.S., Peng Y. Procedures, criteria, and machine learning techniques for network traffic classification: A survey. IEEE Access. 2022. Vol. 10. P. 64806–64829. https://doi.org/10.1109/ACCESS.2022.3181135

References

1. Ahmad Z., Khan A.S., Shiang C.W., Abdullah J., Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Emerging Telecommunications Technologies. 2021. Vol. 32(1). e4150. https://doi.org/10.1002/ett.4150

2. Alladi T., Chamola V., Sikdar B., Choo K.-K.R. Consumer IoT: Security vulnerability case studies and solutions. IEEE Consumer Electronics Magazine. 2020. Vol. 9(2). P. 17–25. https://doi.org/10.1109/MCE.2019.2953740

3. Baich M., Sael N. Enhancing machine learning model prediction with feature selection for botnet intrusion detection. Engineering Proceedings. 2025. Vol. 112(1). P. 55. https://doi.org/10.3390/engproc2025112055

4. Cai Z., Du H., Wang H., Zhang J., Si Y., Li P. One-dimensional convolutional Wasserstein generative adversarial network based intrusion detection method for industrial control systems. Electronics. 2023. Vol. 12(22). P. 4653. https://doi.org/10.3390/electronics12224653

5. Dalou' J., Al-Duwairi B., Al-Jarrah M. Adaptive entropy-based detection and mitigation of DDoS attacks in SDN networks. International Journal of Computing. 2020. Vol. 19(3). P. 399–410. https://doi.org/10.47839/ijc.19.3.1889

6. Denysiuk D., Savenko O., Lysenko S., Savenko B., Kashtalian A. Method for detecting steganographic changes in images using machine learning. In: Proceedings of the 13th International Conference on Dependable Systems, Services and Technologies (DESSERT 2023). Athens: IEEE, 2023. P. 1–6. https://doi.org/10.1109/DESSERT61349.2023.10416453

7. Farooq M., Ahmad F. Improved intrusion detection in IoT using multi-layered neural architectures. International Journal of Computing. 2024. Vol. 23(2). P. 268–273. https://doi.org/10.47839/ijc.23.2.3546

8. Hussain A., Sharif H., Rehman F. et al. A systematic review of intrusion detection systems in Internet of Things using ML and DL. In: 2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). Sukkur: IEEE, 2023. https://doi.org/10.1109/iCoMET57998.2023.10099142

9. Joloudari J.H., Marefat A., Nematollahi M.A., Oyelere S.S., Hussain S. Effective class-imbalance learning based on SMOTE and convolutional neural networks. Applied Sciences. 2023. Vol. 13(6). P. 4006. https://doi.org/10.3390/app13064006

10. Joseph J.E., Aleke N.T., Onyeanisi O.P. Deep learning based intrusion detection system for network security in IoT system. International Journal of Education, Management, and Technology. 2025. Vol. 3(1). P. 119–138. https://doi.org/10.58578/ijemt.v3i1.4539

11. Kashtalian A., Lysenko S., Sachenko A., Savenko B., Savenko O., Nicheporuk A. Evaluation criteria of centralization options in the architecture of multicomputer systems with traps and baits. Radioelectronic and Computer Systems. 2025. Vol. 1. P. 264–297. https://doi.org/10.32620/reks.2025.1.18

12. Kilincer I.F., Ertam F., Sengur A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks. 2021. Vol. 188. P. 107840. https://doi.org/10.1016/j.comnet.2021.107840

13. Li G., Jung J.J. Deep learning for anomaly detection in multivariate time series: Approaches, applications, and challenges. Information Fusion. 2023. Vol. 91. P. 93–102. https://doi.org/10.1016/j.inffus.2022.10.008

14. Maniriho P., Niyigaba E., Bizimana Z. et al. Anomaly-based intrusion detection approach for IoT networks using machine learning. In: 2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM). Surabaya: IEEE, 2020. P. 303–308. https://doi.org/10.1109/CENIM51130.2020.9297958

15. Mari A.-G., Zinca D., Dobrota V. Development of a machine-learning intrusion detection system and testing of its performance using a generative adversarial network. Sensors. 2023. Vol. 23(3). P. 1315. https://doi.org/10.3390/s23031315

16. Mijalkovic J., Spognardi A. Reducing the false negative rate in deep learning based network intrusion detection systems. Algorithms. 2022. Vol. 15(8). P. 258. https://doi.org/10.3390/a15080258

17. Sathaporn P., Krungseanmuang W., Chaowalittawin V. et al. DDoS detection using a hybrid CNN-RNN model enhanced with multi-head attention for cloud infrastructure. Applied Sciences. 2025. Vol. 15(21). P. 11567. https://doi.org/10.3390/app152111567

18. Shahriar M.H., Haque N.I., Rahman M.A., Alonso M. G-IDS: Generative adversarial networks assisted intrusion detection system. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). Madrid: IEEE, 2020. P. 376–385. https://doi.org/10.1109/COMPSAC48688.2020.000218

19. Sheibani M., Konur S., Awan I., Qureshi A. A multi-layered defence strategy against DDoS attacks in SDN/NFV-based 5G mobile networks. Electronics. 2024. Vol. 13(8). P. 1515. https://doi.org/10.3390/electronics13081515

20. Sheikh M.S., Peng Y. Procedures, criteria, and machine learning techniques for network traffic classification: A survey. IEEE Access. 2022. Vol. 10. P. 64806–64829. https://doi.org/10.1109/ACCESS.2022.3181135