https://doi.org/10.31891/2219-9365-2026-86-48
УДК 004.75:004.49:004.3

СЕМЕНЮК Богдан
Хмельницький національний університет
e-mail: bohdan.semenuik@khmnu.edu.ua
https://orcid.org/0009-0001-8831-8835
СТЕЦЮК Юрій
Хмельнитцький національнитй університет
e-mail: yuriy.stetsuk@khmnu.edu.ua
https://orcid.org/0000-0003-0312-2276

ДОСЛІДЖЕННЯ ВПЛИВУ СИНТЕТИЧНОГО БАЛАНСУВАННЯ НАВЧАЛЬНОЇ ВИБІРКИ НА ТОЧНІСТЬ ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК

У статті досліджено вплив синтетичного балансування навчальної вибірки на точність виявлення комп'ютерних атак у задачах побудови систем виявлення вторгнень. Актуальність дослідження зумовлена тим, що реальні набори мережевого трафіку характеризуються суттєвим дисбалансом класів, унаслідок чого моделі машинного навчання демонструють знижену здатність до розпізнавання рідкісних і складних типів атак. Метою роботи є порівняльне оцінювання впливу різних підходів до синтетичного балансування навчальних даних на якість класифікації мережевого трафіку. У роботі розглянуто базовий підхід без балансування, класичний метод SMOTENC та сигнатурозбережний адаптивний метод синтетичного балансування, орієнтований на збереження статистичних і структурних властивостей зразків атак. Експериментальне дослідження виконано на даних задачі виявлення атак із використанням показників якості класифікації, зокрема F1-score. Отримані результати показали, що застосування синтетичного балансування забезпечує підвищення якості виявлення атак порівняно з базовим варіантом, тоді як сигнатурозбережний адаптивний підхід демонструє кращі результати порівняно з класичним методом SMOTENC. Практичне значення роботи полягає в обґрунтуванні доцільності використання адаптивного синтетичного балансування для підвищення точності систем виявлення комп'ютерних атак в умовах дисбалансних навчальних вибірок.

Ключові слова: система виявлення вторгнень; комп'ютерні атаки; мережевий трафік; дисбаланс класів; навчальна вибірка; синтетичне балансування.

SEMENUIK Bohdan, STETSYUK Yuriy
Khmelnytskyi National University

RESEARCH ON THE IMPACT OF SYNTHETIC TRAINING SAMPLE BALANCING ON THE ACCURACY OF DETECTING COMPUTER ATTACKS

The article investigates the influence of synthetic balancing of the training set on the accuracy of computer attack detection in intrusion detection system tasks. The relevance of the study is determined by the fact that real network traffic datasets are characterized by a significant class imbalance, due to which machine learning models demonstrate a reduced ability to detect rare and complex attack types. The purpose of the paper is to comparatively evaluate the influence of different approaches to synthetic balancing of training data on the quality of network traffic classification. The study considers a baseline approach without balancing, the classical SMOTENC method, and a signature-preserving adaptive synthetic balancing method aimed at preserving the statistical and structural properties of attack samples. The experimental study was carried out on attack detection data using classification quality metrics, in particular F1-score. The obtained results showed that the use of synthetic balancing improves attack detection quality compared with the baseline variant, while the signature-preserving adaptive approach demonstrates better results than the classical SMOTENC method. The practical significance of the study lies in substantiating the feasibility of using adaptive synthetic balancing to improve the accuracy of computer attack detection systems under conditions of imbalanced training datasets.

Keywords: intrusion detection system; computer attacks; network traffic; class imbalance; training set; synthetic balancing.

Стаття надійшла до редакції / Received 31.03.2026
Прийнята до друку / Accepted 17.04.2026
Опубліковано / Published 31.05.2026

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

Сучасний розвиток інформаційно-комунікаційних технологій, поширення корпоративних мереж, хмарних сервісів, IoT-середовищ і розподілених обчислювальних систем супроводжується зростанням кількості та складності комп'ютерних атак. За таких умов системи виявлення вторгнень набувають важливого значення як один із базових засобів забезпечення кібербезпеки, оскільки дають змогу своєчасно ідентифікувати аномальну або шкідливу активність у мережевому трафіку та зменшувати ризик порушення конфіденційності, цілісності й доступності інформаційних ресурсів [1, 2].

У сучасних дослідженнях задача виявлення атак дедалі частіше розглядається як задача інтелектуальної класифікації мережевого трафіку із застосуванням методів машинного та глибокого навчання. Такий підхід забезпечує вищу гнучкість порівняно з класичними сигнатурними засобами, однак його ефективність істотно залежить від якості навчальних даних, структури ознакового простору та

збалансованості класового складу вибірки. Особливо гостро ця проблема проявляється в середовищах, де нормальний трафік суттєво переважає над шкідливим, а окремі типи атак представлені малою кількістю зразків, що ускладнює їх коректне розпізнавання моделлю [7, 14].

Однією з ключових проблем побудови високоточних систем виявлення комп'ютерних атак є дисбаланс навчальної вибірки. За наявності суттєвого переважання одних класів над іншими модель у процесі навчання орієнтується насамперед на домінантні шаблони, унаслідок чого знижується якість розпізнавання рідкісних і складних атак. Це призводить до збільшення кількості пропущених загроз, погіршення узагальнювальної здатності моделі та зменшення практичної цінності системи виявлення вторгнень у реальних умовах експлуатації.

Одним із поширених підходів до подолання зазначеної проблеми є синтетичне балансування навчальних даних, яке передбачає формування додаткових зразків для недостатньо представлених класів. Однак ефективність такого підходу суттєво залежить від способу генерації нових прикладів. Якщо синтетичні зразки не відтворюють характерні статистичні та структурні властивості атак, це може не лише не покращити результати класифікації, а й призвести до додаткового викривлення меж між класами. У зв'язку з цим актуальним є дослідження впливу синтетичного балансування навчальної вибірки на точність виявлення комп'ютерних атак, а також порівняння класичних і адаптивних підходів до формування синтетичних зразків.

Отже, науково-практична проблема полягає в необхідності визначення того, наскільки застосування синтетичного балансування дає змогу підвищити якість виявлення комп'ютерних атак у дисбалансних наборах мережевого трафіку та який із підходів до балансування є більш доцільним для використання в системах виявлення вторгнень. Саме це зумовлює актуальність дослідження, присвяченого аналізу впливу синтетичного балансування навчальної вибірки на точність класифікації мережевого трафіку в задачі виявлення атак.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У сучасних дослідженнях систем виявлення вторгнень значна увага приділяється застосуванню методів машинного та глибокого навчання для аналізу мережевого трафіку, оскільки такі підходи дають змогу автоматизувати процес виявлення аномалій і складних типів атак, які важко описати жорсткими сигнатурними правилами. У наукових оглядах відзначається, що ефективність IDS дедалі більше визначається не лише вибором архітектури класифікатора, а й якістю використаних даних, способом формування ознакового простору та коректністю процедури навчання моделі [8, 12].

Окремий напрям досліджень пов'язаний із використанням глибоких нейронних мереж для виявлення вторгнень у мережах IoT та інших динамічних інформаційних середовищах. Такі підходи дають можливість виявляти приховані нелінійні залежності у мережевому трафіку та підвищувати точність класифікації порівняно з традиційними алгоритмами. Водночас у роботах підкреслюється, що навіть за використання сучасних deep learning-моделей результати виявлення атак істотно залежать від збалансованості навчальної вибірки та здатності моделі коректно розпізнавати аномальні, але малопредставлені шаблони поведінки [10, 13].

Поряд із класичними архітектурами багатошарових нейронних мереж у задачах intrusion detection активно досліджуються спеціалізовані моделі, орієнтовані на покращення інформативності ознак і точності класифікації. Зокрема, розглядаються підходи, засновані на попередньому відборі найбільш значущих ознак, а також моделі, що поєднують глибоке навчання з генеративними механізмами формування репрезентативних даних. Такі рішення демонструють перспективність у задачах виявлення ботнет-активності, аномалій та вторгнень, однак не усувають повною мірою проблему нерівномірного представлення класів у навчальних наборах [3, 4].

Важливе місце в сучасних дослідженнях займають методи подолання дисбалансу класів, оскільки саме ця властивість даних часто знижує якість розпізнавання рідкісних атак. Одним із найпоширеніших підходів є використання синтетичного oversampling, зокрема методів родини SMOTE, які передбачають генерацію нових зразків для недостатньо представлених класів. У роботах, присвячених поєднанню SMOTE з нейромережевими моделями, показано, що синтетичне балансування здатне покращувати показники класифікації, особливо в умовах значної нерівномірності розподілу даних [9, 15].

Разом із тим наукові публікації свідчать, що покращення інтегральних метрик не завжди означає однаково якісне виявлення всіх типів загроз. Для систем виявлення вторгнень критично важливим є зменшення кількості пропущених атак, тобто зниження помилок другого роду, оскільки саме вони безпосередньо впливають на безпеку мережевого середовища. У зв'язку з цим дослідники наголошують на необхідності розроблення таких методів навчання та балансування, які не лише підвищують загальну точність, а й сприяють кращому розпізнаванню проблемних і рідкісних класів атак [16].

Незважаючи на значну кількість праць у галузі інтелектуального виявлення вторгнень, питання вибору ефективного підходу до синтетичного балансування навчальної вибірки залишається відкритим. Існуючі методи часто орієнтовані на загальне вирівнювання кількості зразків, проте недостатньо враховують структурні та статистичні особливості конкретних типів атак. Це обмежує їх ефективність у задачах, де

важливо не просто збільшити кількість прикладів міноритарного класу, а зберегти характерні властивості атакувального трафіку. Саме тому доцільним є проведення окремого дослідження впливу синтетичного балансування навчальної вибірки на точність виявлення комп'ютерних атак із порівнянням класичного та адаптивного підходів до формування синтетичних зразків.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є дослідження впливу синтетичного балансування навчальної вибірки на точність виявлення комп'ютерних атак, а також порівняльне оцінювання ефективності базового підходу без балансування, класичного методу SMOTENC і сигнатурозбережного адаптивного методу синтетичного балансування за показниками якості класифікації мережевого трафіку.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Вихідні дані та постановка експерименту.

Експериментальне дослідження виконано на наборі даних NSL-KDD, який є одним із найбільш поширених тестових наборів у задачах виявлення комп'ютерних атак і містить як зразки нормального мережевого трафіку, так і записи, що відповідають різним типам атак. Використання цього набору даних зумовлене його придатністю для порівняльного аналізу методів класифікації, наявністю структурованих ознак мережних з'єднань та вираженим дисбалансом між окремими підкласами атак, що робить його доцільним для дослідження впливу синтетичного балансування навчальної вибірки на якість виявлення вторгнень.

У роботі використано стандартний поділ NSL-KDD на навчальну та тестову вибірки. Навчальна вибірка містить 125973 записи, тестова – 22544 записи. Для забезпечення коректності експерименту балансування застосовувалося лише до навчальної частини даних, тоді як тестова вибірка залишалася незмінною та використовувалася виключно для підсумкового оцінювання якості моделі. Такий підхід унеможливлює витік інформації з тестових даних у процес навчання та забезпечує об'єктивність порівняння досліджуваних режимів.

У межах експерименту задачу сформульовано як задачу бінарної класифікації мережевого трафіку з поділом записів на два класи: normal та attack. Така постановка дає змогу зосередити увагу на загальному впливі балансування на здатність моделі розпізнавати атакувальний трафік і є доцільною для порівняння різних підходів до формування навчальної вибірки. Разом із тим усередині класу attack у наборі NSL-KDD спостерігається суттєва нерівномірність представлення окремих типів атак: частина з них містить десятки тисяч прикладів, тоді як інші представлені лише сотнями або навіть одиничними записами. Саме ця обставина формує практичну потребу в застосуванні спеціальних засобів балансування.

Для дослідження впливу синтетичного балансування на точність виявлення комп'ютерних атак розглянуто три режими навчання моделі. Перший режим є базовим і передбачає використання оригінальної навчальної вибірки без будь-якого балансування. Другий режим ґрунтується на застосуванні класичного методу SMOTENC, який формує синтетичні зразки для недостатньо представлених підкласів із урахуванням наявності категоріальних ознак. Третій режим реалізує запропонований сигнатурозбережний адаптивний метод синтетичного балансування, орієнтований на генерацію нових зразків у межах статистично допустимих профілів атак.

Для забезпечення коректності порівняння в усіх трьох режимах використовувався однаковий конвеєр обробки даних, однакова архітектура моделі та однакові параметри навчання. Таким чином, відмінності в отриманих результатах зумовлені саме способом формування навчальної вибірки, а не зміною моделі чи режиму її навчання. Оцінювання виконувалося на спільній тестовій множині за основними метриками якості класифікації, серед яких особливу увагу приділено показнику F1-score як узагальненій характеристиці точності та повноти розпізнавання атакувального трафіку.

Методи синтетичного балансування навчальної вибірки у задачі виявлення атак.

Однією з основних причин зниження точності систем виявлення комп'ютерних атак є нерівномірний розподіл прикладів між класами у навчальній вибірці. У таких умовах модель у процесі навчання переважно орієнтується на найбільш представлені шаблони, тоді як рідкісні та складні типи атак мають недостатній вплив на формування роздільної поверхні. Наслідком цього є погіршення якості виявлення саме тих атак, які становлять найбільший практичний інтерес з погляду кіберзахисту. Одним із поширених способів подолання цієї проблеми є синтетичне балансування навчальної вибірки, за якого кількість прикладів міноритарних класів збільшується не шляхом простого дублювання наявних записів, а шляхом формування нових штучних зразків на основі вже існуючих [9, 15].

У загальному випадку синтетичне балансування спрямоване на те, щоб зробити представлення міноритарних класів більш достатнім для навчання моделі, зменшити її зміщення в бік домінантних класів і підвищити здатність розпізнавати недостатньо представлені шаблони атак. Для задач виявлення вторгнень це особливо важливо, оскільки навіть невелика кількість пропущених аномальних зразків може призводити до зростання помилок другого роду та погіршення практичної ефективності IDS [16]. Водночас результативність

балансування залежить не лише від кількості згенерованих прикладів, а й від того, наскільки коректно нові зразки відтворюють статистичну й структурну організацію реальних атакувальних даних.

У межах даного дослідження розглянуто два підходи до синтетичного балансування навчальної вибірки: класичний метод SMOTENC і сигнатурозбережний адаптивний метод синтетичного балансування. Перший із них використано як базовий референтний інструмент, широко представлений у задачах роботи з дисбалансними даними, тоді як другий орієнтований на більш коректне відтворення внутрішньої структури атакувального трафіку.

Метод SMOTENC є розширенням класичної ідеї SMOTE для випадку, коли вибірка містить одночасно числові та категоріальні ознаки. Його сутність полягає у формуванні нових синтетичних прикладів для недостатньо представлених класів на основі локального оточення наявних зразків. Для числових ознак нові значення формуються шляхом інтерполяції між сусідніми прикладами, а для категоріальних ознак використовується вибір значень із найближчого околу. Завдяки цьому досягається збільшення кількості записів міноритарного класу без простого копіювання вихідних спостережень, що в багатьох випадках позитивно впливає на якість класифікації [9].

Разом із тим застосування SMOTENC у задачах виявлення атак має певні обмеження. По-перше, генерація нових зразків виконується переважно на основі локальної близькості між об'єктами та не враховує повною мірою глобальну структуру розподілу підкласу атаки. По-друге, для складних і неоднорідних класів атаки синтетично згенеровані точки можуть потрапляти в області простору ознак, які слабо відповідають реальним профілям атакувального трафіку. По-третє, у разі значної нерівномірності внутрішньої структури міноритарного класу класичне інтерполяційне породження зразків може призводити до розмивання характерних сигнатурних ознак. Саме тому застосування SMOTENC не завжди забезпечує максимально можливе покращення якості виявлення атак, навіть якщо інтегральні метрики класифікації зростають.

З метою подолання зазначених обмежень у роботі використано сигнатурозбережний адаптивний метод синтетичного балансування навчальної вибірки. Його основна ідея полягає в тому, що нові зразки для недостатньо представлених підкласів атак формуються не лише на основі локальної близькості між об'єктами, а й з урахуванням статистично допустимих меж варіації ознак, характерних для відповідного типу атак. Такий підхід дає змогу зменшити ризик утворення нефізичних або слабо репрезентативних синтетичних точок і забезпечує краще збереження характерного профілю атакувального трафіку.

На відміну від класичного синтетичного oversampling, сигнатурозбережний адаптивний метод орієнтований не на механічне вирівнювання кількості прикладів, а на контрольоване поповнення навчальної множини такими зразками, які не руйнують внутрішню структуру підкласу атаки. У процесі генерації враховуються статистичні характеристики вихідних даних, локальна конфігурація об'єктів і допустимий діапазон змін ознак. У результаті синтетичні записи залишаються ближчими до реальних профілів мережевого трафіку, ніж у разі використання суто інтерполяційних методів.

Метод реалізується як послідовність кількох етапів. На першому етапі визначаються підкласи атак, для яких спостерігається недостатнє представлення у навчальній вибірці. На другому етапі для кожного такого підкласу оцінюються локальні та глобальні статистичні характеристики, що описують характерний профіль класу. На третьому етапі формується план синтетичного поповнення, який визначає кількість нових зразків для кожного підкласу та межі допустимих змін ознак. На завершальному етапі генеруються синтетичні записи, які додаються до навчальної вибірки та використовуються для подальшого навчання моделі класифікації.

У межах даного дослідження запропонований метод формалізовано як сигнатурозбережний адаптивний метод синтетичного балансування навчальної вибірки (*Signature-Preserving Adaptive Sampling, SPAS*). Його призначення полягає у формуванні синтетичних зразків для недостатньо представлених підкласів атак із збереженням статистично допустимих меж зміни ознак і характерного профілю атакувального трафіку.

Нехай навчальна вибірка задається множиною

$$D_{train} = \{(x_i, y_i)\}_{i=1}^{N}, \quad (1)$$

де $x_i \in R^m$ – вектор ознак i-го мережевого з'єднання, $y_i \in C$ – мітка класу, $C = \{c_1, c_2, \dots, c_K\}$ – множина підкласів, що в бінарній постановці узагальнюються до класів $normal$та $attack$.

Для кожного підкласу c_kвизначимо кількість його зразків у навчальній вибірці:

$$n_k = |\{x_i \in D_{train} : y_i = c_k\}|. \quad (2)$$

Підкласи, які потребують синтетичного поповнення, формуються у вигляді множини

$$C^* = \{c_k \in C : n_k < T_{bal}\}, \quad (3)$$

де T_{bal} – цільовий поріг балансування. Для кожного підкласу $c_k \in C^*$ обчислюється дефіцит кількості зразків

$$\Delta_k = T_{bal} - n_k, \Delta_k > 0. \quad (4)$$

На відміну від класичного інтерполяційного oversampling, у методі SPAS новий зразок формується з урахуванням локального сусідства та статистично допустимих меж варіації ознак. Для числової ознаки j у межах підкласу c_kвизначається робастний інтервал допустимих значень

$$I_{k,j} = \left[Q_1^{(k,j)} - \alpha \cdot IQR_{k,j},\ Q_3^{(k,j)} + \alpha \cdot IQR_{k,j}\right], \quad (5)$$

де $Q_1^{(k,j)}$ і $Q_3^{(k,j)}$ – перший і третій квартилі ознаки j, $IQR_{k,j} = Q_3^{(k,j)} - Q_1^{(k,j)}$ – міжквартильний розмах, α – коефіцієнт допустимого розширення інтервалу.

Для пари близьких зразків $x_a, x_b \in c_k$ синтетичний кандидат для числових ознак формується як

$$\tilde{x}_j = x_{a,j} + \lambda_j\left(x_{b,j} - x_{a,j}\right), \lambda_j \in [0,1]. \quad (6)$$

Щоб згенерований зразок не виходив за межі характерного профілю підкласу атаки, отримане значення коригується оператором обмеження

$$\tilde{x}_j^* = \min\left(\max\left(\tilde{x}_j,\ I_{k,j}^{\min}\right), I_{k,j}^{\max}\right), \quad (7)$$

де $I_{k,j}^{\min}$ та $I_{k,j}^{\max}$ – нижня та верхня межі інтервалу $I_{k,j}$.

Для категоріальних ознак синтетичне значення визначається на основі моди в локальному околі підкласу:

$$\tilde{x}_j^{cat} = \mathrm{mode}\left(\mathcal{N}_{k,j}(x_a)\right), \quad (8)$$

де $\mathcal{N}_{k,j}(x_a)$ – множина значень категоріальної ознаки j у локальному околі зразка x_a всередині підкласу c_k.

Тоді збалансована навчальна вибірка формується як об'єднання початкової множини та синтетично згенерованих зразків:

$$D_{train}^{bal} = D_{train} \cup \tilde{D}_{syn}, |\ \tilde{D}_{syn}^{(k)}\ | = \Delta_k,\ c_k \in C^*. \quad (9)$$

Запропонована формалізація відображає принципову відмінність методу SPAS від SMOTENC: якщо класичний підхід формує нові записи переважно на основі локальної інтерполяції, то сигнатурозбережний адаптивний метод додатково контролює статистично допустимі межі ознак і тим самим зменшує ймовірність утворення нефізичних або слабо репрезентативних синтетичних точок. Саме це забезпечує краще збереження внутрішньої структури атакувального трафіку та підвищує придатність сформованої вибірки для навчання моделі виявлення атак.

Перевага такого підходу полягає в тому, що він краще узгоджується зі специфікою задачі виявлення комп'ютерних атак, де важливо не просто збільшити чисельність міноритарного класу, а зберегти інформативні особливості атакувального трафіку. Це особливо суттєво для рідкісних і складних типів атак, для яких навіть незначне викривлення простору ознак може призвести до помітного зниження точності розпізнавання. Саме тому сигнатурозбережне адаптивне балансування розглядається в даній роботі як перспективніший підхід порівняно з класичним SMOTENC.

Отже, у межах дослідження порівнюються два способи синтетичного балансування навчальної вибірки: класичний метод SMOTENC, який використовується як поширений базовий підхід, і сигнатурозбережний адаптивний метод, орієнтований на збереження статистичних та структурних властивостей атакувальних зразків. Їх порівняння в однакових умовах навчання дає змогу оцінити, якою мірою якість синтетично сформованої навчальної вибірки впливає на точність виявлення комп'ютерних атак.

Експерименти

Експериментальне дослідження виконано для трьох режимів навчання моделі виявлення атак: без балансування навчальної вибірки, із застосуванням класичного методу SMOTENC та із використанням сигнатурозбережного адаптивного підходу SPAS. Оцінювання здійснювалося на спільній тестовій множині, що дало змогу порівняти вплив саме способу формування навчальних даних на підсумкову якість класифікації.

Отримані результати показали, що базовий режим без балансування демонструє найгіршу здатність до виявлення атакувального трафіку, оскільки модель у такому випадку істотно зміщується в бік домінантних шаблонів навчальної вибірки. Застосування синтетичного балансування дало змогу покращити основні показники якості класифікації, причому найбільший ефект було досягнуто при використанні сигнатурозбережного адаптивного підходу SPAS.

Як видно з рис. 1, використання SMOTENC забезпечує покращення показників якості порівняно з навчанням на незбалансованій вибірці, однак найкращі результати за інтегральними метриками досягаються при використанні SPAS. Особливо помітною є перевага SPAS за показниками повноти розпізнавання атак та F1-score, що свідчить про кращу здатність моделі виявляти атакувальний трафік без істотної втрати узгодженості класифікації.

Для задач виявлення комп'ютерних атак особливе значення має не лише загальна точність, а й співвідношення між пропущеними атаками та хибними спрацьовуваннями. У цьому аспекті базовий режим характеризується найбільшою кількістю хибнонегативних рішень, тобто пропущених атак, тоді як застосування балансування дозволяє суттєво зменшити цей недолік.

ISSN 2219-9365

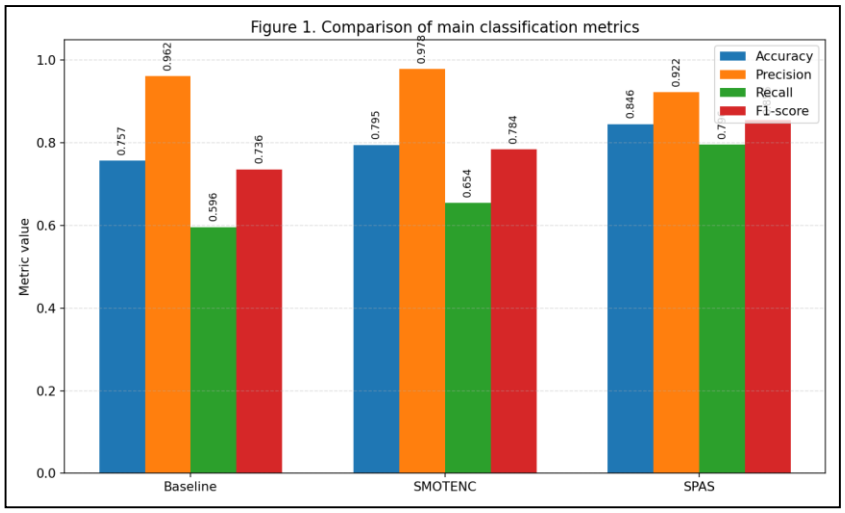

Рис. 1. Порівняння основних метрик класифікації для базового режиму, SMOTENC та SPAS

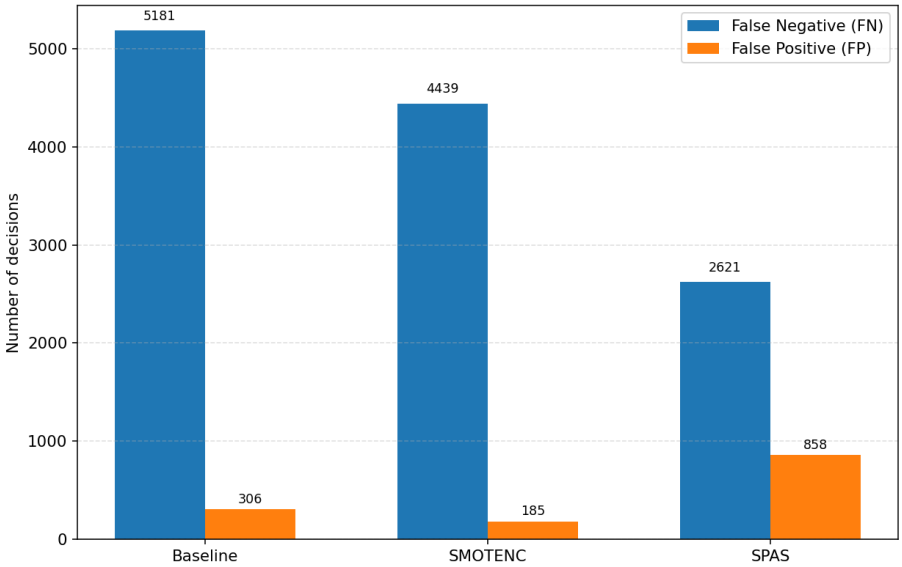

Рис. 2. Порівняння кількості хибнонегативних та хибнопозитивних рішень у досліджуваних режимах

Дані, наведені на рис. 2, показують, що метод SPAS забезпечує найменшу кількість пропущених атак, хоча це супроводжується зростанням кількості хибнопозитивних спрацьовувань порівняно з іншими режимами. Для систем виявлення вторгнень така зміна є виправданою, оскільки пропуск реальної атаки зазвичай є критичнішим, ніж додаткове спрацювання системи безпеки.

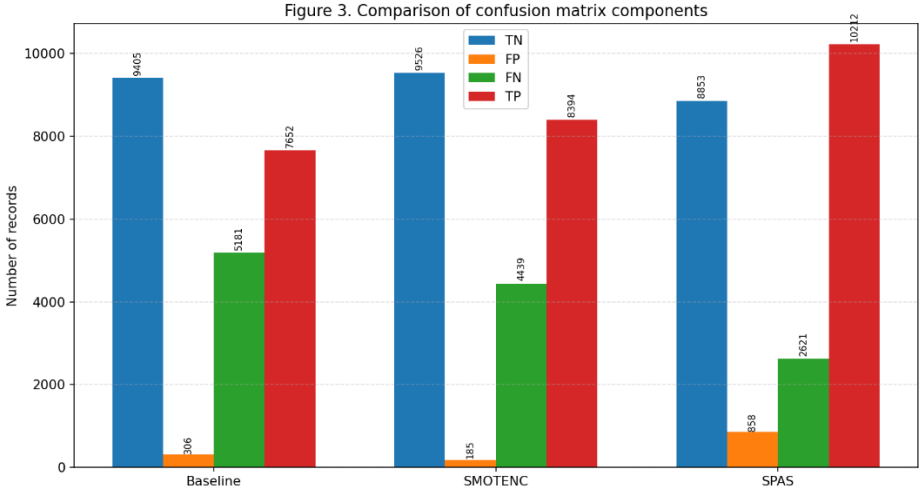

Рис. 3. Порівняння елементів матриці невідповідностей для базового режиму, SMOTENC та SPAS

Більш детальний аналіз помилок класифікації підтверджує, що застосування синтетичного балансування змінює структуру прийнятих рішень моделі. При використанні SPAS спостерігається найбільша кількість правильно виявлених атак, що свідчить про краще відтворення особливостей міноритарних підкласів у навчальній вибірці та ефективніше формування роздільної поверхні між нормальним і атакувальним трафіком.

З погляду практичного застосування важливим є також відносний приріст якості порівняно з базовим режимом. Проведене порівняння показало, що класичне синтетичне балансування покращує результати класифікації, але найбільший приріст забезпечує саме сигнатурозбережний адаптивний підхід. Це підтверджує, що ефективність балансування визначається не лише кількістю згенерованих зразків, а й ступенем збереження статистичних і структурних властивостей атакувального трафіку.

Figure 4. Relative gain of metrics compared to baseline

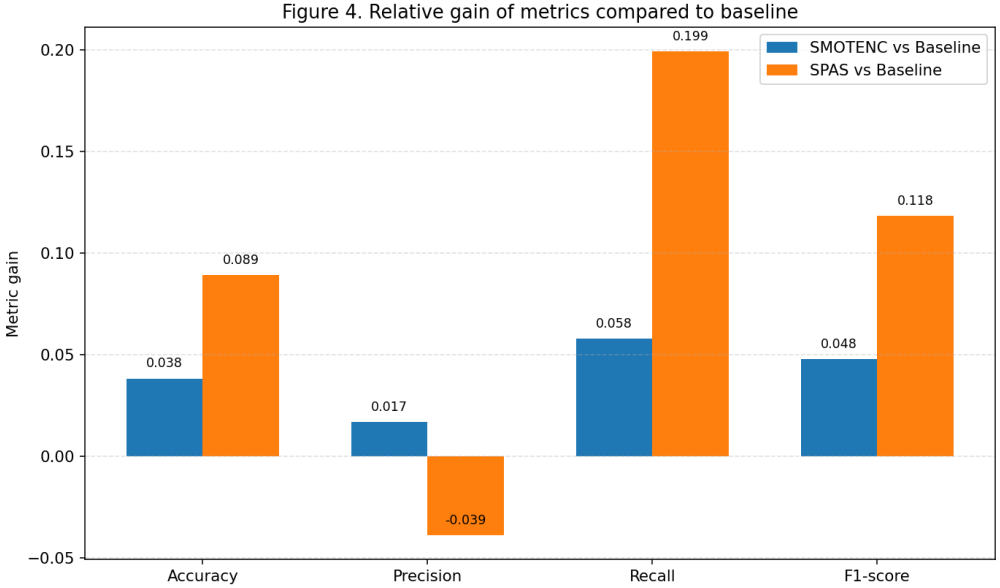

Рис. 4. Приріст основних метрик відносно базового режиму при використанні SMOTENC та SPAS

Отже, результати експерименту підтверджують, що синтетичне балансування навчальної вибірки позитивно впливає на точність виявлення комп'ютерних атак. При цьому найкращий ефект досягається у разі використання сигнатурозбережного адаптивного підходу SPAS, який забезпечує найбільше покращення повноти виявлення атак і F1-score, а також найменшу кількість пропущених загроз.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті досліджено вплив синтетичного балансування навчальної вибірки на точність виявлення комп'ютерних атак у задачі побудови систем виявлення вторгнень. Показано, що однією з ключових причин зниження якості класифікації мережевого трафіку є дисбаланс класів, за якого модель у процесі навчання переважно орієнтується на домінантні шаблони та гірше розпізнає рідкісні й складні типи атак.

У межах дослідження виконано порівняння трьох режимів формування навчальної вибірки: без балансування, із застосуванням класичного методу SMOTENC та із використанням сигнатурозбережного адаптивного підходу SPAS. Отримані результати підтвердили, що синтетичне балансування загалом позитивно впливає на якість виявлення атак, оскільки дає змогу підвищити повноту розпізнавання атакувального трафіку та зменшити кількість пропущених загроз.

Встановлено, що базовий підхід без балансування характеризується найнижчими показниками recall і F1-score, що свідчить про недостатню здатність моделі виявляти атакувальний трафік в умовах дисбалансної навчальної вибірки. Застосування методу SMOTENC забезпечило покращення основних метрик класифікації, однак найбільшого ефекту досягнуто при використанні сигнатурозбережного адаптивного методу SPAS, який продемонстрував найвище значення F1-score та найменшу кількість хибнонегативних рішень.

Отримані результати підтверджують, що ефективність синтетичного балансування визначається не лише фактом збільшення кількості прикладів міноритарного класу, а й якістю сформованих синтетичних зразків. Використання підходу, який враховує статистичні та структурні властивості атакувального трафіку, дає змогу підвищити точність виявлення комп'ютерних атак порівняно з класичними інтерполяційними методами балансування.

Практичне значення роботи полягає в обґрунтуванні доцільності застосування адаптивного синтетичного балансування навчальних даних у системах виявлення вторгнень, орієнтованих на роботу з дисбалансними наборами мережевого трафіку. Перспективою подальших досліджень є розширення

експериментальної перевірки запропонованого підходу на інших наборах даних, а також аналіз його ефективності в багатокласовій постановці задачі виявлення комп'ютерних атак.

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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi:10.3390/a15080258