УДК 004.4
DOI https://doi.org/10.32782/IT/2025-1-26

Богдан СЕМЕНЮК
аспірант, Хмельницький національний університет, 11, вул. Інститутська, м. Хмельницький, Україна, 29016
ORCID: *0009-0001-8831-8835*

Антоніна КАШТАЛЬЯН
кандидат технічних наук, докторанка, доцент кафедри фізики та електротехніки, Хмельницький національний університет, 11, вул. Інститутська, м. Хмельницький, Україна, 29016
ORCID: *0000-0002-4925-9713*
Scopus Author ID: *57218242499*

Бібліографічний опис статті: Семенюк, Б., Каштальян, А. (2025). Виявлення комп'ютерних атак із використанням 2D-CNN та соніфікації мережевого трафіку. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 193–201, doi: https://doi.org/10.32782/IT/2025-1-26

ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК ІЗ ВИКОРИСТАННЯМ 2D-CNN ТА СОНІФІКАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ

У сучасних комп'ютерних мережах обсяги та різноманітність трафіку постійно зростають, що ускладнює завдання виявлення атак (IDS, Intrusion Detection System). Традиційні підходи – сигнатурні, евристичні та статистичні – часто не справляються з динамічними загрозами та призводять до великої кількості хибних спрацювань. Використання приманок та машинного навчання та глибинних нейронних мереж уже продемонструвало покращення точності розпізнавання, проте залишається відкритим питання ефективної презентації даних і виявлення складних закономірностей у високовимірних просторах.

Метою статті *є обґрунтування та експериментальна перевірка підходу «соніфікації» мережевого трафіку для потреб систем виявлення атак. Поставлене завдання – продемонструвати, що перетворення векторів ознак у псевдозвуковий сигнал (PCM) з подальшим застосуванням короткого перетворення Фур'є (STFT) дає двовимірне (час × частота) представлення даних, сумісне з 2D-згортковими нейронними мережами (2D-CNN). Порівнюються результати з традиційними 1D-підходами, а також аналізується можливість «підсилення» вибраних атрибутів шляхом керованої зміни частот і амплітуд.*

Методологія *полягає у застосуванні класичних аудіо-аналітичних методів (перетворення PCM, STFT) для формування двовимірних спектрограм, на яких далі навчається 2D-CNN. Для порівняння з традиційним підходом використовуються аналогічні дані NSL-KDD, оброблені 1D-CNN. Критеріями оцінювання є точність, повнота (recall), обчислювальна складність.*

Наукова новизна *полягає в адаптації методів аудіообробки (зокрема, спектрального аналізу та 2D-конволюцій) до завдання IDS. Показано, що «соніфікація» відкриває нові можливості для візуалізації та подальшого застосування розвинених аудіо-/мовленнєвих технологій у кібербезпеці.*

Висновки. *Експерименти свідчать, що точність виявлення атак із застосуванням соніфікації та 2D-CNN може бути порівнянною з 1D-підходами (~75–80 %), однак перевагою є покращена інтерпретація та спектральна візуалізація. Водночас збільшується обчислювальне навантаження, тож подальші дослідження можуть бути зосереджені на прискоренні процедури STFT, балансуванні класів та використанні додаткових рекурентних блоків (CRNN).*

Ключові слова: *виявлення вторгнень, нейронні мережі, PCM, STFT, соніфікація мережевого трафіку, 2D-CNN, IDS, приманки.*

Bohdan SEMENIUK
Postgraduate Student, Khmelnytskyi National University, 11, Instytutska Str., Khmelnitsky, Ukraine, 29016, faludore@mail.com
ORCID: *0009-0001-8831-8835*

Antonina KASHTALIAN
Candidate of Technical Sciences, PhD Candidate, Associate Professor at the Department of Physics and Electrical Engineering, Khmelnytskyi National University, 11, Instytutska Str., Khmelnytskyi, Ukraine, 29016, yantonina@ukr.net
ORCID: *0000-0002-4925-9713*
Scopus Author ID: *57218242499*

To cite this article: Semeniuk, B., Kashtalian, A. (2025). Vyiavlennia kompiuternykh atak iz vykorystanniam 2D-CNN ta sonifikatsii merezhevoho trafiku [Detection of computer attacks using 2D-CNN and traffic sonification]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 193–201, doi: https://doi.org/10.32782/IT/2025-1-26

DETECTION OF COMPUTER ATTACKS USING 2D-CNN AND TRAFFIC SONIFICATION

In modern computer networks, the ever-growing volume and diversity of traffic complicate the task of detecting attacks (IDS, Intrusion Detection System). Traditional approaches – signature-based, heuristic, and statistical – often fail to handle dynamic threats and result in numerous false positives. Although honeypots and machine learning and deep neural networks have demonstrated improved recognition accuracy, the question of effective data representation and the identification of complex patterns in high-dimensional spaces remains open.

***The purpose of the article** is to substantiate and experimentally validate a «sonification» approach for network traffic in intrusion detection systems. The objective is to demonstrate that converting feature vectors into a pseudo-audio signal (PCM), followed by applying the Short-Time Fourier Transform (STFT), yields a two-dimensional (time × frequency) representation compatible with 2D convolutional neural networks (2D-CNN). This article compares the results with traditional 1D-based methods and examines the possibility of «enhancing» certain attributes through controlled adjustments of frequencies and amplitudes.*

***The methodology** involves employing classical audio-analytical techniques (PCM transformation, STFT) to form two-dimensional spectrograms, which are then used to train a 2D-CNN. For comparison with the traditional approach, the same NSL-KDD dataset is processed by a 1D-CNN. The evaluation criteria include accuracy, recall, and computational complexity.*

***The scientific novelty** lies in adapting audio-processing methods (specifically spectral analysis and 2D convolutions) to the IDS context. It is shown that «sonification» opens up new opportunities for visualization and further application of advanced audio/speech technologies in cybersecurity.*

***Conclusions.** Experiments indicate that the detection accuracy of attacks using sonification and 2D-CNN can be comparable to 1D approaches (~75–80 %), while offering improved interpretability and spectral visualization. However, the computational overhead grows accordingly, which suggests that future research might concentrate on speeding up the STFT procedure, balancing classes, and incorporating additional recurrent blocks (CRNN).*

***Key words:** intrusion detection, neural networks, PCM, STFT, network traffic sonification, 2D-CNN, IDS, honeypots.*

Вступ. При розробленні систем виявлення та протидії зловмисному програмному забезпеченню (ЗПЗ) і комп'ютерним атакам (КА) в умовах постійно зростаючого обсягу та різноманітності мережевого трафіку (R. Bace at al., 2001), важливо забезпечити методи аналізу даних, здатні вчасно та ефективно ідентифікувати нові типи загроз. Традиційні засоби захисту (антивірусне ПЗ, файрволи, класичні IDS) у багатьох випадках не встигають адаптуватися до динамічних сценаріїв атак, часто генерують надмірну кількість хибних спрацювань та потребують регулярного оновлення сигнатур. Крім того, обмеженою лишається здатність цих систем виявляти складні або невідомі атаки, що вимагають гнучкіших підходів.

Застосування приманок та методів машинного навчання та глибинних нейронних мереж дає змогу суттєво підвищити результативність виявлення КА завдяки автоматичному формуванню ознак із великих обсягів мережевого трафіку та виявленню аномалій. Приманки та методи виявлення аномалій пропонують компроміс між точністю виявлення атак та їх кількістю. Вдосконаленим підходом до виявлення атак, в тому числі атак нульового дня, є використання тіньових приманок, які дублюють роботу робочих сервісі, однак є захищеними та розробленими для виявлення потенційних атак. Такі приманки дозволяють аналізувати трафік в режимі реального часу, не впливаючи на роботу основного сервісу. Разом із тим постає проблема ефективного представлення даних для глибинних моделей, яка зводиться не лише до попередньої обробки й нормалізації атрибутів, а й до визначення способу відображення складних багатовимірних патернів (зокрема часових і просторових) у формі, придатній для розпізнавання (R. Bace at al., 2001). Одним із перспективних напрямків у цьому контексті є «соніфікація» мережевого трафіку, яка передбачає перетворення векторів ознак у псевдозвуковий сигнал (PCM) з наступним застосуванням віконного перетворення Фур'є (STFT) та двовимірних згорткових мереж (2D-CNN). Такий підхід розвиває ідеї аудіоаналітики, перевірені в галузі розпізнавання мовлення та музики, адаптуючи їх до завдань виявлення аномалій у трафіку.

Таким чином, **метою** даної роботи є обґрунтування та експериментальне дослідження підходу «PCM + STFT + 2D-CNN» для виявлення комп'ютерних атак, який покликаний надати альтернативний спосіб представлення

мережевих даних і потенційно підвищити рівень детектування. У роботі викладено аналіз існуючих рішень, описано модель «соніфікації» мережевого трафіку та наведено результати експериментальних досліджень на базі датасету NSL-KDD. Наостанок сформульовано висновки та визначено напрями подальших досліджень, зокрема щодо оптимізації обчислювального навантаження, балансування класів і застосування додаткових рекурентних елементів (CRNN).

Аналіз останніх досліджень і публікацій. Сучасні системи виявлення вторгнень (IDS) дедалі частіше ґрунтуються на інструментах машинного навчання (ML), що істотно підвищує здатність обробляти великі обсяги різнорідних даних і знаходити неочевидні закономірності. Як відомо, характеристики джерел даних (пакети, потоки, сесії, логи) відображають специфіку певних типів атак, і вибір відповідного джерела суттєво впливає на показники точності виявлення.

Окремий напрям досліджень – виявлення атак на основі пакетів, коли аналізуються бінарні дані заголовків і корисного навантаження. Пакети містять IP-адреси, порти та часові мітки, що дозволяє доволі точно встановлювати джерело та послідовність подій. У роботі (R. Velea et al., 2017) для захоплення пакетів з корпоративної мережі запропоновано застосовувати інструменти, які дозволяють поділяти трафік за типами протоколів і формувати кластери подібних пакетів за допомогою K-means. Моделі SVM на базі таких кластерів досягали точності 99,6 % для HTTP та понад 90 % для інших протоколів. Некеровані методи (fuzzy C-means) також демонструють зниження хибних спрацювань і пропущених атак (Y. Hu et al., 2024). Водночас обмеження пакетного підходу полягає в тому, що поодинокий пакет може не відображати контекст сесії чи складні DDoS-сценарії.

Виявлення атак на основі аналізу корисного навантаження зорієнтоване переважно на вміст пакетів прикладного рівня, і за відсутності шифрування це відкриває можливості для глибокого аналізу (E. Min et al., 2018; Y Zeng et al., 2019). Складність полягає в тому, що вихідні дані часто потребують значної попередньої обробки, аби сформувати вектори або «токени» для CNN чи LSTM. Впровадження глибоких автоенкодерів (Y. Yu et al., 2017) дозволило досягти на деяких наборах даних (CTU-UNB) точності понад 98 %. Однак такі методи чутливі до зашифрованого трафіку й можуть виявлятися обчислювально витратними.

Ще одним популярним джерелом є потокові дані, в яких агрегуються пакети за певний інтервал часу. Потоки дають ширший огляд мережевої активності, що корисно для виявлення масованих атак типу DoS/Probe (S. Potluri et al., 2016). Методи на основі інженерії ознак включають розрахунки середньої довжини пакета, співвідношення TCP/UDP, частки певних TCP-флагів тощо (K. Goeschel, 2016). У більш сучасних підходах (Belkacem, 2024) застосовують некеровані моделі глибокого навчання (напр., автоенкодери) з подальшим класифікуванням через XGBoost, що суттєво покращує результативність, особливо за умови незбалансованих класів (GAN для синтетичного розширення даних). Основне обмеження полягає в тому, що потокові дані не містять повного змісту пакетів, тож атаки на рівні R2L/U2R можуть лишатися нерозкритими.

У працях, присвячених виявленню атак на основі сесій, увага зосереджена на п’ятикомпонентному кортежі (IP клієнта, порт клієнта, IP сервера, порт сервера, протокол), який фіксує високорівневу семантику комунікації. Такі дані особливо корисні для детального аналізу тривалих з’єднань (S. Teng et al., 2017). Перевага – у можливості відстежувати конкретні пари IP і виявляти тунельні чи троянські атаки, тоді як динаміка подій у межах однієї сесії може точно вказувати на джерело загрози. Проте змінна тривалість сесій ускладнює обробку, оскільки потребує кешування великого обсягу пакетів. Застосування RNN (LSTM, GRU) до послідовностей пакетів чи ознак (B. J. Radford et al., 2018; W. Wang et al., 2017) дало змогу підвищити точність до 95–99 %, але за умови якісної обробки змішаних типів трафіку й тонкого налаштування моделей.

Аналіз логів (журналів системної чи прикладної активності) також набув поширення для виявлення складних загроз, таких як SQL-ін’єкції (S. O. Uwagbole et al., 2017) або внутрішні загрози. Виявлення на основі логів передбачає кореляцію подій, указаних в логах системи чи застосунків, з мережею, що дозволяє деталізувати дії користувачів і збільшувати рівень довіри до рішень (W. Meng et al., 2015; S. McElwee et al., 2017). Гібридні методи (правила + ML) або текстовий аналіз (n-грам, частотні словники, TF-IDF) демонструють точність понад 95 %, але потребують суттєвого налаштування під конкретну систему та врахування різних форматів логів. Для боротьби з дисбалансом (аномальних записів зазвичай мало) часто застосовують аугментацію мінорних класів SMOTE та автоенкодери (A. M. Vartouni et al., 2018).

В роботах (А. Каштальян, 2023; A. Kashtalian et al., 2024) запропоновано модель та архітектуру системи з приманками, яка може збирати та опрацьовувати трафік в мережі за принципом тіньової приманки. В роботі (A. Nicheporuk et al., 2020) запропоновано метод виявлення зловмисних програм на основі моделі змішаних даних CNN. А в роботах (S. Lysenko et al., 2022; B. Savenko et al., 2023) аналіз трафіку за підтримки систем в корпоративних мережах та мережі з IoT.

Таким чином, проведений аналіз підтверджує, що незалежно від типу вхідних даних (пакети, потоки, сесії, логи) системи IDS інтенсивно використовують інструменти машинного навчання та глибинних моделей (CNN, LSTM, автоенкодери). Ключовим завданням лишається обрання представлення даних, яке полегшуватиме виявлення різноманітних видів атак. У цьому контексті поява нових підходів, орієнтованих на нетипові форми подання (наприклад, перетворення в «звуковий простір»), має практичну цінність. Саме тому у даній роботі зосереджено увагу на «соніфікації» мережевого трафіку, що поєднує методи аудіоаналітики із завданнями кібербезпеки.

Методологія дослідження. При розробленні систем виявлення комп'ютерних атак (IDS), зокрема на базі глибинного навчання, важливим аспектом є обрання та підготовка даних, а також спосіб подання векторів ознак. У цій роботі пропонується методика «соніфікації» мережевого трафіку, що поєднує традиційні алгоритми аудіообробки (PCM, STFT) із механізмами двовимірної згорткової нейронної мережі (2D-CNN). Такий підхід розвиває ідеї, котрі в суміжних дослідженнях використовуються для розпізнавання мовлення або музичних сигналів (E. Min et al., 2018; Y. Zeng et al., 2019).

Першим етапом обробки є соніфікація мережевого трафіку. Одним із альтернативних підходів до вирішення задачі виявлення загроз є «соніфікація» – перетворення вектору ознак на псевдозвуковий сигнал (PCM). Ідея базується на тому, що з аудіосигналами накопичено багато напрацювань у галузі розпізнавання мовлення, музики тощо, які можуть бути корисними і для мережевого аналізу.

Загальна схема така:

1. Нормалізація та підготовка вектора $x \in [-1, 1]^F$.

2. Формування PCM-сигналу довжиною N зразків (наприклад, 0.4 с при 8000 Гц → 3200 відліків). Кожен атрибут x_i відображається у певний часовий відрізок Δt, де формується синусоїдальний фрагмент із частотою

$$f_i = f_{\min} + x_i \cdot (f_{\max} - f_{\min})$$

та амплітудою $A_i = x_i$ (або $|x_i|$).

3. Отриманий PCM надалі обробляється методами аналізу аудіосигналів, зокрема віконним перетворенням Фур'є (STFT), щоб у результаті мати двовимірне представлення «час × частота».

Наступний етапом після соніфікації є порівняння 1D-CNN та «PCM + STFT» (2D-CNN). У класичному підході для глибинного навчання з векторами ознак застосовують 1D-CNN. Розглянемо вектор $x \in \mathbb{R}^F$: 1) x інтерпретується як одновимірна послідовність довжини F; 2) на кожному кроці 1D-CNN виконує згортку з фільтрами розміром $k \times 1$; 3) після кількох згорток і пулінгів мережа переходить або до повнозв'язного шару, або до глобального пулінгу, а потім виконує класифікацію із функцією активації sigmoid/softmax.

Натомість для 2D-CNN потрібно двовимірний тензор $\mathbb{R}^{H \times W}$. Якщо застосовувати соніфікацію, отримуємо псевдозвукову хвилю, далі за допомогою STFT отримується матриця $S(f, t)$, де f відповідає частоті (наближення $0..f_{nyquist}$) t – часові «вікна» (кадри). Таким чином, S стає «зображенням» (H, W). 2D-CNN здатна з достатньою точністю виявляти локальні «плями» у цьому 2D-просторі, подібно до аналізу зображень.

Математична основа перетворення PCM. Нехай $x \in [-1, 1]^F$. Позначимо N = sample rate × duration sec. Для i-го атрибуту x відводиться

$$\Delta n_i = \left\lfloor \frac{N}{F} \right\rfloor,$$

а якщо $\sum_i \Delta n_i < N$, то залишок зразків $R = N - \sum_i \Delta n_i$ можна заповнити нулями (або повторювати останній атрибут).

У відрізку Δn_i для Δn_i для k = 0, 1, …, Δn_i – 1 обчислюємо:

$$f_i = f_{\min} + x_i \cdot (f_{\max} - f_{\min}), \quad A_i = x_i.$$

Наступним етапом є віконне перетворення Фур'є (STFT). Отриманий PCM-сигнал $w[n]$, $n = 0, \ldots, N - 1$ ділимо вікном розміром L (наприклад, 256 зразків) зі зсувом $\Delta < L$. Виконуємо перетворення Фур'є (наприклад, швидке перетворення Фур'є FFT):

$$Zxx_m(\omega) = \sum_{k=0}^{L-1} \tilde{W}_m[k] e^{-j 2\pi \omega k / L}.$$

Надалі обчислюємо амплітуду $|Zxx_m(\omega)|$, а для візуалізації або подачі в 2D-CNN беремо лог-амплітуду:

$$S[m, \omega] = \log(1 + |Zxx_m(\omega)|).$$

Отримана матриця S розмірності (частоти × вікна часу), що є вхідним шаром 2D-CNN.

Було розроблено графічне представлення перетворень описаних вище (PCM та STFT). Формуються хвилі для двох умовних записів A та B (Рис. 1). Кожен із них має 41 атрибут, які знаходяться у діапазоні [–1..1]. Після перетворення на PCM-сигнал довжиною ~3200 відліків (0.4 с при 8 кГц) застосовується STFT з параметрами nperseg=256 та noverlap=128. Таким чином, отримуємо 2D-матриці розміром 129 × 25. На рис. 2 зображені спектрограми $S(A)$ та $S(B)$.

Переваги розглянутого підходу є можливість використання готових аудіо-методик (CNN з 2D-фільтрами, CRNN, спектральні ознаки тощо), інтуїтивна візуалізація (рисунки зі спектрограмою), можливість виявлення закономірностей за наявності складної часової структури, недоступних 1D-аналізу.

Водночас наявні недоліки, зокрема: штучна «часова» вісь у випадку відсутності природної послідовності реальних атрибутів вектору надає мало нової інформації; значні обчислювальні витрати, а саме обробка 100k+ записів (кожен 0.4 с → STFT); простий 1D-CNN чи MLP

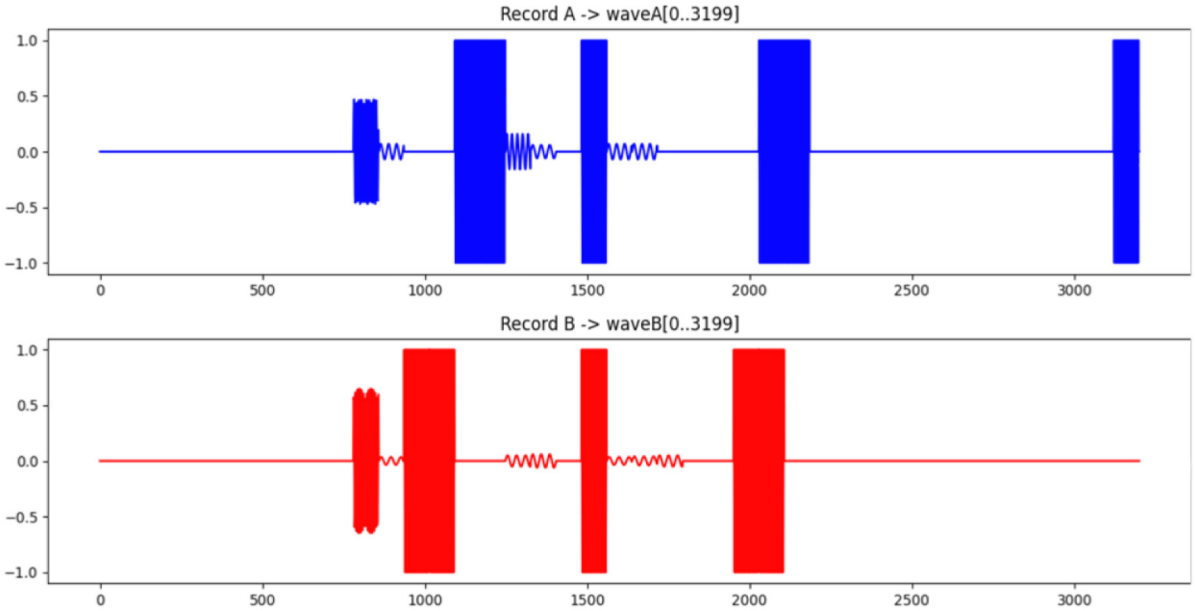

Рис. 1. Графік сигналу для запису A і B після перетворення PCM

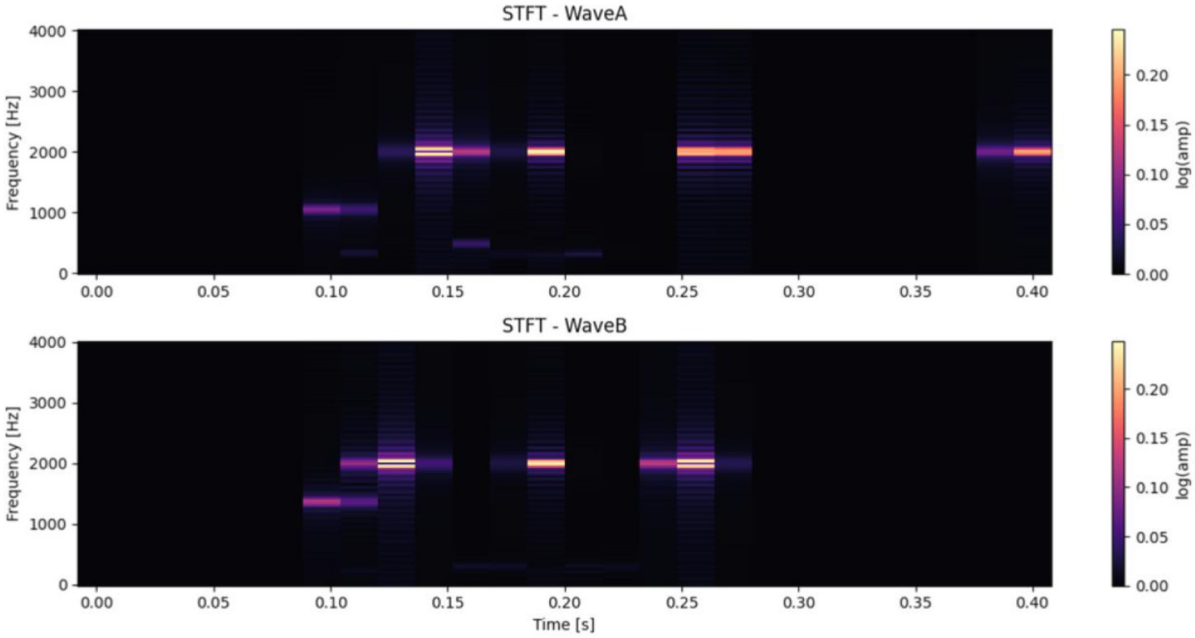

Рис. 2. STFT-спектрограми двох різних записів

на вихідних ознаках може дати схожу точність при меншому навантаженні.

Виходячи з вище наведених переваг та недоліків соніфікації трафіку із подальшою обробкою 2D-CNN, такий підхід може бути доцільним у таких випадках: 1) якщо реально існують часові кореляції між атрибутами (наприклад, якщо кожен атрибут – це «шматок потоку» в різні моменти), то перетворення STFT може виявити закономірності в частотному просторі; 2) соніфікація використовується як метод візуалізації, що дає можливість системному адміністратору «програвати» (чи принаймні переглядати спектр) і оперативно визначати аномальні патерни.

Напрямками вдосконалення цього підходу може бути розвиток цього підходу через Mel-спектри замість сирої STFT, застосування додаткового підсилення певних «частот» (атрибутів), поєднання 2D-CNN з рекурентною складовою (CRNN), якщо потрібен аналіз довгих часових інтервалів.

Отже, в роботі детально описано процес перетворення вектору ознак у псевдозвуковий сигнал, застосування віконного перетворення Фур'є для одержання спектрограми та побудову 2D-CNN, наведено математичні основи формування PCM-сигналу і приклад, що ілюструє трансформацію для двох різних записів із NSL-KDD. Показано, що цей підхід реалізується досить прозоро, проте створює додаткове обчислювальне навантаження й не завжди суттєво перевершує традиційні методи.

Дослідження ефективності. Показниками ефективності є точність, поведінка при виявленні атак та час обчислень. На навчальному наборі даних Train (125973 зразки) модель досягала 96 % точності; на валідаційному наборі Val ~96,7 %, та на тестовому наборі Test (22544 зразки) точність ~76–77 %, що узгоджується з даними інших досліджень (E. Min et al., 2018; Y. Zeng et al., 2019) за подібних налаштувань. Поведінка для класу "attack". Приблизне значення повноти для атак ~62 %, тоді як влучності ~96 %. Модель краще розпізнає нормальний трафік, а деякі патерни "attack" плутаються з нормальними. Формування PCM і спектрограм для 125 тис. зразків є відчутним навантаженням. У середньому генерація одного PCM займає ~1,2 мс (на CPU), а STFT ~0,8 мс, що в масштабі великого датасету потребує паралельної оптимізації чи GPU-прискорення.

Порівняння з 1D-підходом. Для зіставлення була навчається звичайна 1D-CNN (Conv1D) із тими ж 122 атрибутами, без перетворення у двовимір. За схожих налаштувань точність сягала 78–80 % на тестовому наборі, що іноді перевершувало «2D + STFT»-варіант. Таким чином, соніфікація не завжди гарантує більшу точність, особливо якщо атрибути не мають виразної часової структури. Однак спектрограма може давати додатковий простір для дослідження патернів і кращу візуалізацію.

Обговорення та перспективи вдосконалення. У випадку складних даних, зокрема якщо вектор ознак містить атрибути, що справді відображають послідовні стани (наприклад, фрагменти трафіку в різні моменти), тоді перехід до STFT може виявитися ефективним. Низька повнота для атаки свідчить про бажаність застосування oversampling-методів (SMOTE, GAN) або внесення коригувань у функцію втрат. Застосування методу потребує оптимізації обчислень. За великої кількості зразків формування PCM + STFT стає «вузьким місцем». Можливе використання GPU або прискорених бібліотек

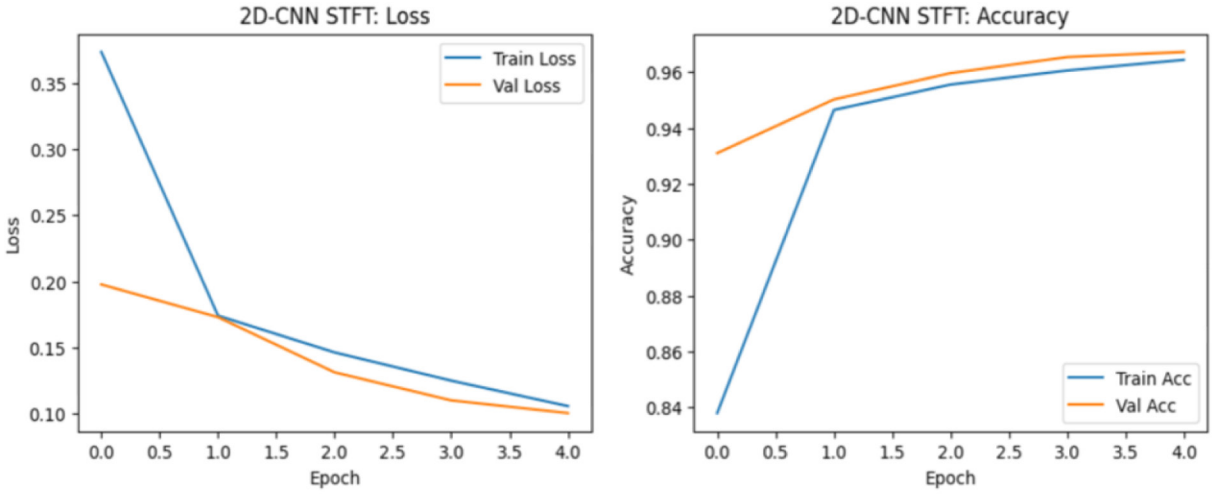

Рис. 3. Результати дослідження ефективності

аудіообробки. У перспективі можна використовувати CRNN (Con + RNN) чи застосувати Mel-спектрограми та інші ознаки, що використовуються для аудіо сигналу.

Отже, дослідження ефективності дає змогу зробити висновок, що метод «PCM + STFT + 2D-CNN» є працездатним та пропонує альтернативне представлення даних, але вимагає ретельного налаштування параметрів аудіоаналітики й балансування класів.

Висновки. Здійснено детальний опис методології «соніфікації» мережевого трафіку для задачі виявлення атак, а також проаналізовано ефективність цього підходу на прикладі датасету NSL-KDD. Результати підтверджують, що: 1) соніфікація (PCM + STFT) та подальша обробка 2D-CNN можуть забезпечити точність, порівнянну з традиційним 1D-підходом (~75–80 %), одночасно відкриваючи можливості візуалізації спектрограм і використання різноманітних аудіоаналітичних методів; 2) обчислювальні витрати помітно зростають через формування PCM-сигналів і обчислення STFT на великому обсязі даних. Без оптимізацій це може бути перешкодою для промислових застосувань у реальному часі; 3) балансування класів (oversampling, GAN) та оптимізація архітектури (Mel-спектр, CRNN-блоки, налаштування кількості фільтрів і шарів) лишаються ключовими факторами для поліпшення результатів, особливо за умов різноманіття атак і великої кількості «нормального» трафіку.

Таким чином, запропонований підхід є перспективним у розробці систем IDS, які покликані розпізнавати небезпеки на основі нетрадиційних форм представлення даних. Майбутні дослідження доцільно зосередити на: впровадженні автоматичного «підсилення» або вагових коефіцієнтів у PCM-перетворенні для критичних атрибутів; розширенні архітектур 2D-CNN за допомогою рекурентних компонент (CRNN) для кращого урахування послідовних патернів у спектрограмі; детальному аналізі впливу різних діапазонів частот та типів отримання вікна в STFT на якість детектування; перевірці підходу на більш сучасних та складних наборах даних (UNSW-NB15, CICIDS2017, MAWILab), а також на зашифрованому трафіку й потоках у реальному часі.

Загалом, метод «PCM + STFT + 2D-CNN» не лише сприяє дослідженню нових підходів у сфері кібербезпеки, але й актуалізує застосування інструментарію аудіоаналізу в задачах IDS, де інформативність та інтерпретованість результатів відіграють особливо важливу роль.

ЛІТЕРАТУРА:

1. Bace R., Mell P. Intrusion Detection Systems. *Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD*, USA, 2001.

2. Velea R, Ciobanu C., Margarit L., Bica I. Network Traffic Anomaly Detection Using Shallow Packet Inspection and Parallel K-means Data Clustering. *Studies in Informatics and Control*, 2017, 26, P. 387–398. https://doi.org/10.24846/v26i4y201702

3. Hu Y., Tu B. Security Situation Assessment Model of DDoS Attack Based on Progressive Fuzzy C Clustering Algorithm. *2024 International Conference on Data Science and Network Security (ICDSNS), Tiptur, India*, 2024, P. 1–4. doi: https://doi.org/10.1109/ICDSNS62112.2024.10691183

4. Min E., Long J., Liu Q., Cui J., Chen W. TR-IDS: Anomaly-based intrusion detection through text-convolutional neural network and random forest. *Secur. Commun. Netw.*, 2018, 4943509. https://doi.org/10.1155/2018/4943509

5. Zeng Y., Gu H., Wei W., Guo Y. Deep-Full-Range: A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework. *IEEE Access*, 2019, 7, P. 45182–45190. https://doi.org/10.1109/ACCESS.2019.2908225.

6. Yu Y., Long J., Cai Z. Network intrusion detection through stacking dilated convolutional autoencoders. *Secur. Commun. Netw*. 2017, 4184196. https://doi.org/10.1155/2017/4184196.

7. Potluri S., Diedrich C. Accelerated deep neural networks for enhanced Intrusion Detection System. *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, Germany*, 2016, P. 1–8. doi: https://doi.org/10.1109/ETFA.2016.7733515

8. Goeschel K. Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis. *SoutheastCon 2016, Norfolk, VA, USA*, 2016, P. 1–6. doi: https://doi.org/10.1109/SECON.2016.7506774

9. Belkacem S. Simultaneous Botnet Attack Detection Using Long Short Term Memory-Based Autoencoder and XGBoost Classifier. *International Journal of Safety and Security Engineering*, 2024, 14, P. 155–163. https://doi.org/10.18280/ijsse.140115

10. Teng S., Wu N., Zhu H., Teng L., Zhang W. SVM-DT-based adaptive and collaborative intrusion detection. *IEEE/CAA J. Autom. Sin*., 2017, 5, P. 108–118. https://doi.org/10.1109/JAS.2017.7510730

11. Radford B. J., Apolonio L. M., Trias A. J., Simpson, J. A. Network traffic anomaly detection using recurrent neural networks. 2018. https://arxiv.org/abs/1803.10769

12. Wang W., Sheng Y., Wang J., Zeng X., Ye X., Huang Y., Zhu M. HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE Access*, 2017, 6, P. 1792–1806. https://doi.org/10.1109/ACCESS.2017.2780250

13. Uwagbole S. O., Buchanan W. J., Fan L. Applied machine learning predictive analytics to SQL injection attack detection and prevention. *Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May*, 2017. P. 1087–1090.

14. Meng W., Li W., Kwok L. F. Design of intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection. *Secur. Commun. Netw*., 2015, 8, P. 3883–3895. https://doi.org/10.1002/sec.1307

15. McElwee S., Heaton J., Fraley J., Cannady J. Deep learning for prioritizing and responding to intrusion detection alerts. *Proceedings of the MILCOM 2017–2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD*, USA, 23–25 October, 2017. P. 1–5.

16. Vartouni A. M., Kashi S. S., Teshnehlab M. An anomaly detection method to detect web attacks using Stacked Auto-Encoder. *Proceedings of the 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS)*, Kerman, Iran, 28 February–2 March, 2018. P. 131–134.

17. Каштальян А. С. Концептуальна модель архітектури мульти-комп'ютерних систем із приманками та пастками для виявлення та протидії зловмисному програмному забезпеченню та комп'ютерним атакам. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2023, № 3, С. 22–31. https://doi.org/10.32782/IT/2023-3-3

18. Kashtalian A., Lysenko S., Savenko O., Nicheporuk A., Sochor T., Avsiyevych V. Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems*, 2024. 1, P. 152–175. doi: https://doi.org/10.32620/reks.2024.1.13

19. Nicheporuk, A., Savenko, O.,A. Nicheporuk, and Y. Nicheporuk. An android malware detection method based on CNN mixed-data model. *CEUR Workshop Proceedings*, Kharkiv, Ukraine, 2020, 2732, P. 198–213.

20. Lysenko S., Bobrovnikova K., Kharchenko V., Savenko O. IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. *Algorithms*, 2022. 15(7), 239. https://doi.org/10.3390/a15070239

21. Savenko B., Kashtalian A., Lysenko S., Savenko O., Malware Detection by Distributed Systems with Partial Centralization. *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Dortmund, Germany, 2023. P. 265–270. doi: https://doi.org/10.1109/IDAACS58523.2023.10348773

REFERENCES:

1. Bace, R., Mell, P. (2001). Intrusion Detection Systems. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, USA.

2. Velea, R, Ciobanu, C., Margarit, L., Bica, I. (2017). Network Traffic Anomaly Detection Using Shallow Packet Inspection and Parallel K-means Data Clustering. *Studies in Informatics and Control*, 26, P. 387–398. doi: https://doi.org/10.24846/v26i4y201702

3. Hu, Y., Tu, B. (2024). Security Situation Assessment Model of DDoS Attack Based on Progressive Fuzzy C Clustering Algorithm. *2024 International Conference on Data Science and Network Security (ICDSNS), Tiptur, India*, P. 1–4. doi: https://doi.org/10.1109/ICDSNS62112.2024.10691183

4. Min, E., Long, J., Liu, Q., Cui, J., Chen, W. (2018). TR-IDS: Anomaly-based intrusion detection through text-convolutional neural network and random forest. *Secur. Commun. Netw*. 4943509. https://doi.org/10.1155/2018/4943509

5. Zeng, Y., Gu, H., Wei, W., Guo, Y. (2019). Deep-Full-Range: A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework. *IEEE Access*, 7, P. 45182–45190. https://doi.org/10.1109/ACCESS.2019.2908225

6. Yu, Y., Long, J., Cai, Z. (2017). Network intrusion detection through stacking dilated convolutional autoencoders. *Secur. Commun. Netw*. 4184196. https://doi.org/10.1155/2017/4184196

7. Potluri, S., Diedrich, C. (2016). Accelerated deep neural networks for enhanced Intrusion Detection System. *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, Germany*, P. 1–8. doi: https://doi.org/10.1109/ETFA.2016.7733515

8. Goeschel, K. (2016). Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis. *SoutheastCon 2016, Norfolk, VA, USA*, P. 1–6. doi: https://doi.org/10.1109/SECON.2016.7506774

9. Belkacem, S. (2024). Simultaneous Botnet Attack Detection Using Long Short Term Memory-Based Autoencoder and XGBoost Classifier. *International Journal of Safety and Security Engineering*, 14, P. 155–163. https://doi.org/10.18280/ijsse.140115

10. Teng, S., Wu, N., Zhu, H., Teng, L., Zhang, W. (2017). SVM-DT-based adaptive and collaborative intrusion detection. *IEEE/CAA J. Autom. Sin*., 5, P. 108–118. https://doi.org/10.1109/JAS.2017.7510730

11. Radford, B. J., Apolonio, L. M., Trias, A. J., Simpson, J. A. (2018). Network traffic anomaly detection using recurrent neural networks. https://arxiv.org/abs/1803.10769

12. Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., Zhu, M. (2017). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE Access*, 6, P. 1792–1806. https://doi.org/10.1109/ACCESS.2017.2780250

13. Uwagbole, S. O., Buchanan, W. J., Fan, L. (2017). Applied machine learning predictive analytics to SQL injection attack detection and prevention. *Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May*, P. 1087–1090.

14. Meng, W., Li, W., Kwok, L. F. (2015). Design of intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection. *Secur. Commun. Netw*. 8, P. 3883–3895. https://doi.org/10.1002/sec.1307

15. McElwee, S., Heaton, J., Fraley, J., Cannady, J. (2017). Deep learning for prioritizing and responding to intrusion detection alerts. *Proceedings of the MILCOM 2017–2017 IEEE Military Communications Conference (MILCOM)*, Baltimore, MD, USA, 23–25 October, P. 1–5.

16. Vartouni, A. M., Kashi, S. S., Teshnehlab, M. (2018). An anomaly detection method to detect web attacks using Stacked Auto-Encoder. *Proceedings of the 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS)*, Kerman, Iran, 28 February–2 March, P. 131–134.

17. Kashtalian, A. (2023). Kontseptualna model arkhitektury multy-kompiuternykh system iz prymankamy ta pastkamy dlia vyiavlennia ta protydii zlovmysnomu prohramnomu zabezpechenniu ta kompiuternym atakam [Conceptual model of multi-computer architecture with baits and traps to detect and counteract malicious software and computer attacks]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, P. 22–31. https://doi.org/10.32782/IT/2023-3-3 [in Ukrainian].

18. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., Avsiyevych, V. (2024). Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems*, 1, P. 152–175. doi: https://doi.org/10.32620/reks.2024.1.13

19. Nicheporuk, A., Savenko, O., A. Nicheporuk, and Y. Nicheporuk. (2020). An android malware detection method based on CNN mixed-data model. *CEUR Workshop Proceedings*, Kharkiv, Ukraine, 2732, P. 198–213.

20. Lysenko, S, Bobrovnikova, K, Kharchenko, V, Savenko, O. (2022). IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. *Algorithms*, 15(7), 239. https://doi.org/10.3390/a15070239

21. Savenko, B., Kashtalian, A., Lysenko, S., Savenko, O. (2023). Malware Detection by Distributed Systems with Partial Centralization. *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany*, P. 265–270. doi: https://doi.org/10.1109/IDAACS58523.2023.10348773