https://doi.org/10.31891/2219-9365-2024-77-41
УДК 004.896.8:004.932.2

МАЙОР Євген
Хмельницький національний університет
https://orcid.org/0009-0004-1867-6241
e-mail: evmaior@khmnu.edu.ua

# ВИЯВЛЕННЯ ШКІДЛИВИХ ПАКЕТІВ ТА DDOS-АТАК У МЕРЕЖЕВОМУ ТРАФІКУ ЗА ДОПОМОГОЮ ГЛИБОКИХ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ

*Робота присвячена аналізу мережевого трафіку за допомогою глибоких згорткових нейронних мереж для виявлення шкідливих пакетів та DDoS-атак. Процес аналізу трафіку включає попередню обробку даних, розробку оптимальних алгоритмів аналізу, та оцінку моделей за допомогою різних метрик ефективності. У роботі досліджено ефективність моделей глибокого навчання, зокрема CNN та LSTM, у виявленні DDoS-атак. Основний набір даних KDD Cup 99 використовується для аналізу трафіку та оцінки ефективності моделей.*

*Ключові слова: виявлення шкідливих пакетів, кібербезпека мережевого середовища, захист від кібератак, машинне навчання у кібербезпеці, медоти виявлення атак, аналіз мережевого трафіку, шлибокі згорткові нейронні мережі.*

MAIOR Yevhen
Khmelnytsky National University

# DETECTING MALICIOUS PACKAGES AND DDOS ATTACKS IN NETWORK TRAFFICE USING DEEP CONVOLUTIONAL NEURAL NETWORKS

*Deep convolutional neural networks (CNNs) have become a powerful tool in the network security arsenal, proving adept at detecting malicious packets and countering distributed denial of service (DDoS) attacks. The synergy between CNN and machine learning methodologies has ushered in a new era of effectiveness in threat detection.*

*The traffic analysis process involves a complex interplay of techniques for preprocessing incoming network traffic data, converting it into patterns that can be recognized by a neural network, algorithmic optimization, and rigorous model evaluation, often using large datasets such as KDD Cup 99, to create robust detection models. This approach is a key step towards strengthening network infrastructure against an increasingly diverse range of cyber threats and with the ability to expand and further train the model.*

*The proposed system embodies adaptability, characterized by a continuous learning system that improves models over time with new input data. Its well-thought-out design gives users the flexibility to choose network adapters and fine-tune learning parameters, providing a responsive and customizable operating environment. By integrating a user-friendly WinForms interface and comprehensive reporting mechanisms, the system strikes a harmonious balance between usability and reliability.*

*To confirm its effectiveness, additional software was developed to simulate various traffic scenarios and stress test the model's performance. The results not only confirmed the effectiveness of the model, but also highlighted the need for continuous improvement of the model to maintain resilience in the face of emerging threats. This research highlights the enormous potential of deep convolutional neural networks in network traffic analysis, signaling a continued evolution toward higher standards of network security.*

*Keywords: detection of malicious packets, cybersecurity of network environments, protection against cyber-attacks, machine learning in cybersecurity, attack detection methods, analysis of network traffic, deep convolutational networks.*

## Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

У зв'язку із стрімким та масштабним зростанням мережевих атак у сучасному світі виявлення шкідливих пакетів та DDoS-атак стає проблемою для будь-якої організації. Це стає не лише ключовим аспектом забезпечення безпеки мережі, а й визначальним чинником для збереження репутації підприємства, захисту конфіденційної інформації та забезпечення надійності та доступності сервісів для користувачів.

Через низку наступних причин важливе передчасне виявлення шкідливих пакетів для швидкої реакції на загрозу, що може виникнути, якщо атаку не буде вчасно припинено:

– зменшення втрат часу та ресурсів шляхом ефективного виявлення та припинення атак, що дозволяє підприємствам уникнути перерв у роботі та зберегти продуктивність;

– забезпечення високої доступності сервісів для користувачів шляхом швидкої реакції на потенційні загрози, що дозволяє підтримувати високу репутацію компанії та задоволеність клієнтів;

– зменшення ризику втрати даних або порушення конфіденційності через швидке виявлення та блокування шкідливих пакетів, що забезпечує захист важливої інформації;

– покращення здатності мережевих інфраструктур адаптуватися до змін у загрозах шляхом навчання на основі аналізу даних про попередні атаки, що дозволяє підвищити ефективність заходів захисту у майбутньому.

Поява нових, інноваційних методів DDoS-атак створює серйозні труднощі для існуючих методів протидії. У цьому контексті використання різних методів машинного навчання виявляє перспективи в

боротьбі з DDoS-атаками. Ці методи дозволяють виявляти атаки з високою точністю і низьким рівнем помилкових спрацьовувань. Розробка та вдосконалення таких систем машинного навчання стає важливим кроком у напрямку забезпечення надійності та безпеки комп'ютерних мереж у умовах постійно зростаючого рівня загрози DDoS-атак.

**Аналіз досліджень та публікацій**

Дослідження актуальних кіберзагроз виявляє важливість вчасного виявлення шкідливих пакетів та атак DDoS у мережах. Ця проблема створює серйозні виклики для забезпечення безпеки мережі та збереження конфіденційності, цілісності та доступності даних. Для ефективного виявлення та протидії таким загрозам потрібно провести комплексне дослідження, розробити адаптовані підходи та впровадити інноваційні технологічні рішення. Вирішення цього завдання має вирішальне значення для забезпечення безпеки мереж і підвищення їх стійкості перед сучасними кіберзагрозами [1].

Атака DoS (Denial of Service – «відмова в обслуговуванні») полягає у спробі призвести систему до непрацездатності, ускладнюючи або блокуючи доступ звичайних користувачів до конкретних сервісів [1,2].

DDoS (Distributed Denial of Service) — це більш складна форма атаки, де напади відбуваються з різних пристроїв, можливо, заражених ботнетами. Основна мета полягає у спричиненні недоступності послуг шляхом зруйнування роботи системи [3,4].

Атаки з використанням протоколу є одним з найбільш поширених методів атак на сервери та мережеві інфраструктури. Вони базуються на експлуатації вразливостей у роботі мережевих протоколів, таких як TCP/IP, HTTP, або DNS, для затримки або переривання нормальної обробки запитів на сервері. Атаки цього типу можуть призвести до перевантаження сервера, витрати його ресурсів, а також зниження продуктивності або повного відмови у обслуговуванні. [5].

Атаки на основі відображення є одним з найбільш складних та ефективних методів DDoS. У таких атаках зловмисник використовує різні вразливості в мережевих протоколах, щоб перенаправити трафік через безпечні вузли мережі, які відправляють свої відповіді на адресу жертви. Це дозволяє зловмиснику приховати свою справжню IP-адресу та уникнути виявлення. Більше того, в атаках на основі відображення застосовується концепція ампліфікації, де короткі запити спричиняють генерацію значно більших відповідей. Це дозволяє зловмиснику підсилювати обсяг трафіку, що надходить до жертви, порівняно з тим, що він сам надсилає, рис. 1 ілюструє процес атаки, під час якого відбивачі спрямовують більш інтенсивний трафік до жертви порівняно з трафіком, що надсилається від зловмисника до відбивача. Такий підвищений обсяг трафіку робить атаки на основі відображення особливо небезпечними та складними для виявлення та протидії [6].

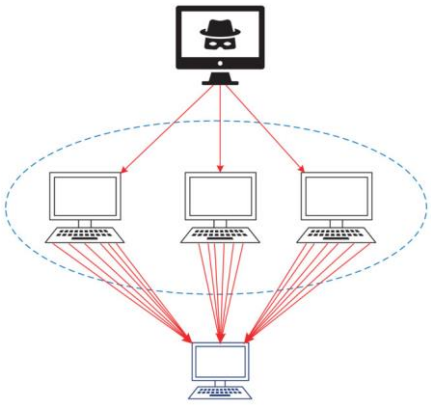

**Рис. 1. Атака розподіленої відмови в обслуговуванні (DDoS)**

Стаття [7] присвячена інноваційному методу виявлення різноманітних атак App-DDoS, використовуючи поєднання генетичного алгоритму (GA) і випадкового лісу (RF), а також комплексного механізму вибору ознак. Дослідження демонструє виняткову ефективність та адаптивність запропонованого методу виявлення атак, яка робить його перспективним рішенням для забезпечення кібербезпеки в критичних інфраструктурах. Застосування GA-RF дозволяє не лише забезпечити надійність виявлення атак, але й підвищити продуктивність системи захисту. Враховуючи постійно зростаючі загрози кібербезпеки, ця робота відкриває нові перспективи у сфері захисту критичних мережевих систем.

Стаття [8] представляє нову систему виявлення вторгнень, що ґрунтується на моделях глибокого навчання для розпізнавання DDoS-атак. Для дослідження використали набір даних CIC-DDoS 2019, що включає 12 класів, у тому числі безпечний клас. Провели експерименти з різними моделями глибокого навчання, такими як DNN, CNN та LSTM, розглядаючи різні конфігурації їхніх шарів. Крім того, була покращена ефективність системи шляхом використання методів попередньої обробки даних, таких як елімінація та вибір ознак, у результаті чого було обрано 40 найбільш важливих ознак з загальної кількості

88. Дослідження дозволили створити новий однорідний набір даних, який враховує оптимальну комбінацію ознак для підвищення точності та ефективності системи виявлення вторгнень.

Стаття [9] описується новий підхід до виявлення DDoS-атак з використанням технології SDN (Software-Defined Networking), що є перспективним рішенням для підвищення безпеки в мережах Інтернету речей. Пропонується новий алгоритм під назвою DALCNN, який реалізований на платформі OpenDayLight. Цей алгоритм дозволяє класифікувати типи DDoS-атак, використовуючи нову функцію активації Tanh2 та використовуючи рекурентні нейронні мережі. Для навчання моделі використовувався навчальний набір даних NSL-KDD, протягом якого модель RNN була навчена протягом 100 епох. Цей алгоритм відкриває нові перспективи для ефективного виявлення та управління DDoS-атаками в мережах Інтернету речей.

Мережі з використанням конволюційних нейронних мереж (CNN) навчаються за допомогою різноманітних наборів даних, які включають як законні, так і потенційно шкідливі пакети. Ці дані дозволяють мережі вивчати візуальні особливості, які характеризують шкідливі пакети від законних. Після завершення навчання мережа може використовуватися для реального часу виявлення шкідливих пакетів. Шляхом аналізу трафіку та використання знань про характеристики шкідливих пакетів, мережа визначає, чи може певний пакет вважатися шкідливим.

CNN володіють численними перевагами в порівнянні з іншими методами виявлення шкідливих пакетів та атак DDoS. Вони відзначаються високою точністю та здатністю розпізнавати різноманітні шкідливі атаки, що робить їх більш привабливими порівняно зі статистичними методами. Крім того, CNN є більш масштабованими, здатними обробляти великі обсяги трафіку, і застосовуються для виявлення шкідливих пакетів у великому масштабі. Це робить їх ефективними та надійними інструментами у боротьбі з кіберзагрозами, забезпечуючи високий рівень безпеки мережі [11, 12].

Методи виявлення DDoS, що базуються на машинному навчанні (ML), можна узагальнити до трьох основних груп: контрольовані, неконтрольовані та гібридні, кожна з яких містить кілька підкатегорій. Систематика цих методів представлена на рис. 2.

Структура методу включає три ключові компоненти: попередню обробку даних, вилучення ознак та класифікацію. Під час попередньої обробки даних виконується видалення зайвих та нерелевантних функцій мережевого трафіку. Модель CNN використовується для виділення просторових ознак з оброблених даних, тоді як модель LSTM відповідає за класифікацію часових ознак, отриманих з CNN. LSTM забезпечує захоплення послідовних залежностей у даних та ідентифікацію шаблонів DDoS-атак [13, 14]..

Ефективність запропонованого методу була оцінена на реальному наборі даних мережевого трафіку, що був зібраний з програмно визначеного тестового стенда IIoT.

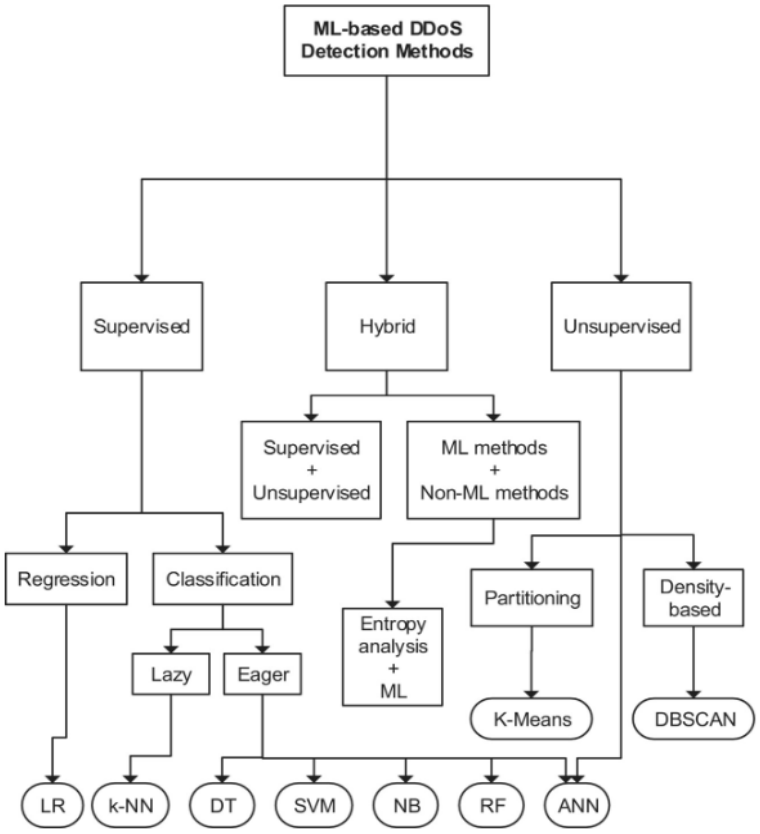


**Рис. 2. Система розподілених методів виявлення відмови в обслуговуванні на основі машинного навчання**

Розробка методів виявлення DDoS-атак на основі глибокого навчання включає кілька підходів. Використання глибоких нейронних мереж дозволяє розділити мережевий трафік на дві категорії: DDoS та не-DDoS. Інший підхід передбачає використання згорткових нейронних мереж (CNN) для виявлення аномалій у трафіку, які можуть свідчити про можливу DDoS-атаку.

**Виклад основного матеріалу**

Попередня обробка є критичним етапом для використання згорткових нейронних мереж (CNN) у аналізі мережевого трафіку. Дані зазвичай надходять у вигляді пакетів, які містять різні заголовки та корисні деталі. Для того щоб вони могли бути використані у моделі CNN, необхідна попередня обробка.

Процес обробки пакетів зазвичай складається з кількох етапів. Перш ніж пакети будуть аналізовані, вони отримуються, сортуються, та скануються. Потім вони реєструються в центральному місці і направляються до відповідного місця призначення, де маркуються відповідно. Після досягнення місця призначення пакети знову сортуються, скануються та вивантажуються для забезпечення точності. Нарешті, вони доставляються адресатам.

Для забезпечення узгодженості важливо стандартизувати формат та розмір пакетів. Такі методи, як стиснення трафіку або одноразове кодування, можуть бути використані для перетворення даних у числовий формат, який підходить для подальшої обробки CNN. Характеристики, такі як довжина пакета, IP-адреси джерела та призначення, а також номери портів, є важливими для аналізу пакетних даних.

Нормалізація - це метод попередньої обробки, який включає помноження даних на скаляр таким чином, щоб середнє значення було близьким до 0, а стандартне відхилення - до 1. Це допомагає забезпечити однаковий масштаб даних і полегшує навчання моделей.

Архітектура згорткової нейронної мережі (CNN) містить кілька згорткових шарів, за якими слідують повністю зв'язані шари. Згорткові шари відділяють високорівневі характеристики з вхідних даних, тоді як повністю зв'язані шари комбінують ці характеристики для прогнозування типу трафіку.

Навчання моделі CNN передбачає подання їй великої кількості позначених даних трафіку та налаштування її параметрів для мінімізації помилки класифікації. Гіперпараметрична оптимізація включає вибір оптимальних значень параметрів, таких як кількість згорткових шарів, кількість фільтрів у кожному шарі та функції активації.

Архітектура згорткової нейронної мережі для аналізу мережевого трафіку представлена на діаграмі на рис. 3. Першим кроком є обробка вхідних даних - серії пакетів з різними заголовками та корисною інформацією. Нормалізація пакетів грає ключову роль у забезпеченні консистентності та однорідності даних, а подальший аналіз полегшується шляхом перетворення пакетів у стандартний формат та зведення їх розмірів.

Для досягнення оптимальних результатів аналізу мережевого трафіку важливо переконатися, що пакети готові для глибокої згорткової обробки нейронною мережею. Уважне спостереження за їхнім розміром та форматуванням допомагає максимізувати ефективність мережі та отримати точні та оперативні результати.

Перетворення пакетних даних у числовий формат, що ефективно обробляється згортковими нейронними мережами (CNN), є важливим етапом обробки. Для забезпечення їхньої придатності для подальшого аналізу та використання у моделях машинного навчання необхідно використовувати методи одноразового кодування або стиснення трафіку.

Вилучення ключових функцій з пакетних даних, таких як IP-адреси джерела та призначення, номери портів та інші параметри, які мають високу інформативність, є важливим етапом обробки. Цей процес дозволяє значно зменшити обсяг даних, зберігаючи важливу інформацію для подальшого аналізу та виявлення аномалій у мережевому трафіку.

Використання кількох згорткових шарів у нейронних мережах виявляється ключовим для ефективного виділення високорівневих характеристик з вхідних даних мережевого трафіку. Ці шари відповідають за виявлення абстрактних особливостей та взаємозв'язків у пакетах, допомагаючи автоматично витягувати та узагальнювати важливі ознаки. Це сприяє зменшенню розмірності даних та підготовці їх для подальшого аналізу.

Після виділення характеристик використовуються повністю зв’язані шари для об’єднання цих характеристик та роботи з ними для прогнозування типу трафіку. Ці шари дозволяють створювати зв'язки між отриманими характеристиками та визначати тип трафіку з високою точністю, використовуючи узагальнені ознаки, отримані на попередніх етапах обробки.

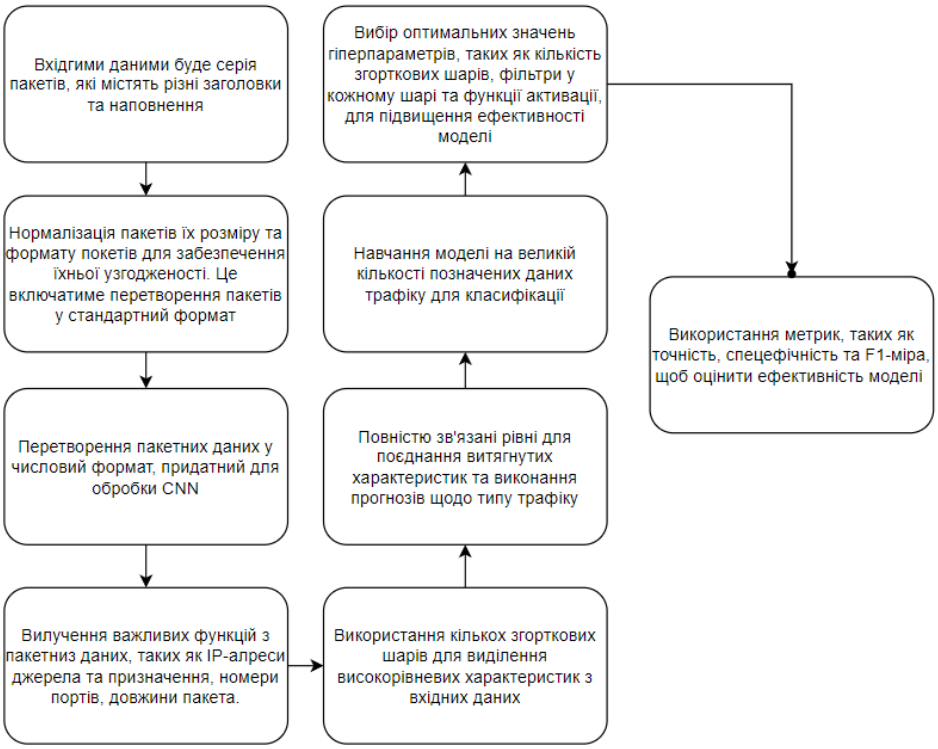


**Рис. 3. Життєвий цикл роботи нейронної мережі**

Навчання моделі на великій кількості позначених даних мережевого трафіку є ключовим для досягнення високої точності класифікації. Чим більше різноманітних даних має модель на вході, тим краще вона може вивчати та розрізняти різні типи трафіку, що покращує її здатність виявляти аномальну активність та шкідливі пакети.

Оптимізація нейронної мережі включає вибір оптимальних значень гіперпараметрів, таких як кількість згорткових шарів, фільтрів у кожному шарі та функцій активації. Цей процес вимагає систематичних експериментів та оцінки результатів для вибору найкращих параметрів, що допомагає підвищити ефективність та точність моделі.

Використання метрик для оцінки моделі на тестових даних є важливим етапом у визначенні точності та ефективності алгоритму класифікації мережевого трафіку. Метрики, такі як точність (accuracy), відгук (recall), специфічність (specificity) та F1-мера, надають різноманітний огляд того, наскільки добре модель справляється з класифікацією.

KDD Cup є важливим інструментом для дослідження та розвитку систем виявлення атак у комп'ютерних мережах. Для вашої роботи, пов'язаної з методами виявлення DDoS-атак та аналізу мережевого трафіку, використання цього набору даних може бути дуже корисним. Ви можете використовувати його для навчання моделей машинного навчання та тестування різних алгоритмів, що дозволить вам отримати більше інсайтів і покращити ефективність вашої системи виявлення атак.

Під час порівняння моделей для виявлення DDoS-атак використовуються різні метрики та стратегії оцінки, які допомагають визначити, яка модель є найбільш ефективною для даного завдання.

Однією з таких метрик є точність (Precision), яка вимірює, яка частина позитивних випадків, ідентифікованих моделлю, є дійсно позитивними [15]. Формула для обчислення точності [1]:

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

TP (True Positives) вказує на кількість правильно виявлених позитивних випадків, тобто кількість виявлених атак. FP (False Positives) вказує на кількість помилково ідентифікованих позитивних випадків, коли звичайний трафік помилково класифікується як атака.

Зменшення втрат під час тренування свідчить про те, що модель стає кращою у передбаченні. Чим менші втрати, тим більше модель відповідає даним тренувального набору, тобто її прогнози стають ближчими до фактичних значень. Процес тренування спрямований на оптимізацію моделі з метою мінімізації втрат і підвищення її точності та надійності у передбаченні.

Recall або Sensitivity, визначається як відношення кількості правильно визначених позитивних випадків до загальної кількості існуючих позитивних випадків. Це означає, що Recall - це кількість True Positives (TP) поділена на суму True Positives та False Negatives (FN). Формула обчислення чутливості [2]:

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

False Negatives (FN) - це кількість позитивних випадків, які були неправильно не визначені моделлю, і які представляють собою атаки, що були помилково визнані як нормальний трафік.

F1-міра об'єднує точність (Precision) та чутливість (Recall) у єдину метрику, яка є гармонічним середнім між ними. Формула для F1-міри [3]:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{3}$$

F1-міра дозволяє оцінити модель з точки зору як правильно класифікованих позитивних випадків, так і здатності уникнути пропусків атак (чутливість), що робить її важливим критерієм оцінки моделі в контексті виявлення DDoS-атак [16].

Специфічність - це важлива метрика, особливо коли ми маємо справу з незбалансованими даними, де кількість від'ємних випадків (нормальний трафік) може бути значно більшою за кількість позитивних випадків (атаки). Вона допомагає оцінити, наскільки ефективно модель відрізняє нормальний трафік від атак, забезпечуючи додатковий контроль над прогнозами моделі щодо від'ємних випадків [17].

Формула для обчислення специфічності виглядає наступним чином [4]:

$$Specificity = \frac{TP}{TP + FP} \tag{4}$$

True Negatives (TN) - кількість правильно визначених від'ємних випадків, тобто нормальний трафік, який був правильно визнаний як нормальний.

False Positives (FP) - кількість неправильно визначених позитивних випадків, які були помилково визнані як нормальний трафік.

Недостатня навченість може бути виявлена, якщо як на навчальній, так і на валідаційній кривих точність занадто низька, що може свідчити про те, що модель недостатньо складна або потребує більше епох тренування.

Перенавченість може виникнути, якщо на навчальній кривій точність висока, але на валідаційній низька. Це може вказувати на те, що модель перенавчилася на навчальних даних і потребує більше даних або регуляризації.

Оптимальний момент для завершення тренування може бути визначений тим, коли криві для навчального та валідаційного наборів даних збігаються або залишаються стабільними. Це може бути момент, коли модель навчилася.

Здатність моделі узагальнювати нові дані та потреба в повторному навчанні можуть бути оцінені, спостерігаючи за змінами в показниках ефективності на кривій навчання при збільшенні обсягу даних для навчання та перевірки.

Система виявлення атак аналізує вхідні дані, які можуть бути фізичним, логічним або протокольним мережевим трафіком. Вона отримує мережевий трафік з різних джерел, таких як фізичні та логічні мережеві пристрої, інші системи безпеки. Після збору дані обробляються для видалення шуму та непотрібних деталей, а потім фільтруються для виявлення незначних атак. Далі система виявлення атак аналізує мережевий трафік, щоб виявити ознаки атак.

Якщо система виявлення атак виявляє атаку, вона генерує результати, які включають тип атаки, деталі та рекомендації щодо реагування. Ці результати зберігаються для подальшого аналізу та аудиту.

Діаграма потоку даних системи виявлення DDoS-атак буде мати наступний вигляд, представлений на рис. 4.


**Рис. 4 Діаграма потоку даних системи для виявлення шкідливих пакетів**

Проведемо завантаження тестових даних, які будуть використовуватися для тренування моделі. Наступним кроком буде навчання глибокої згорткової нейронної мережі та оцінка якості навченої моделі. Результати навчання можна побачити на рис. 5, де представлений графік та звіт про якість моделі за метриками F1-міри, специфічності та точності. Детальний опис результатів представлений у таблиці 1, яка містить значення кожної метрики, отримані моделлю, та визначає ефективність запропонованого методу. У випадку високої ефективності моделі, значення метрик будуть наближені до 1.00: для F1-міри - 0.9, для специфічності - 0.95, а для точності - 1.00.

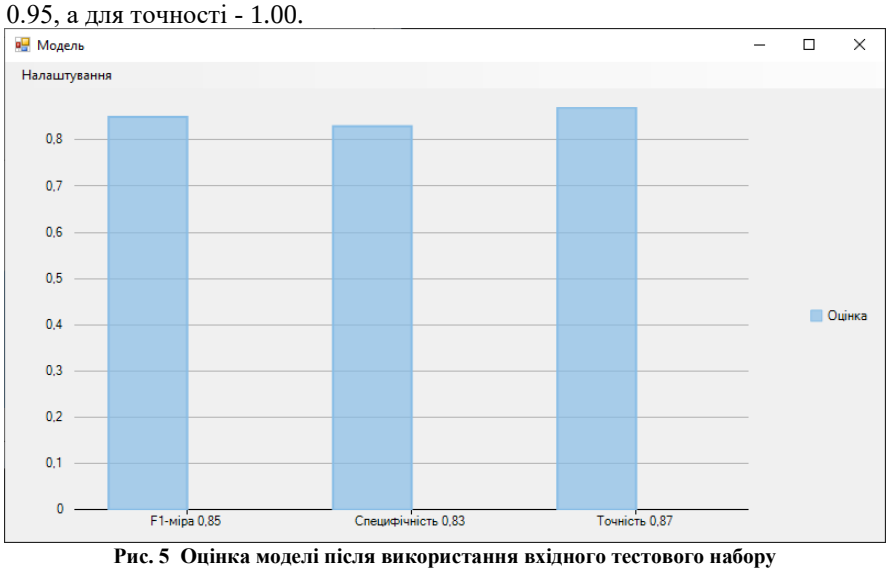


**Рис. 5 Оцінка моделі після використання вхідного тестового набору**

Таблиця 1

**Результати оцінки моделі на тестових даних**

| Метрика | Оцінка | Опис |
|---|---|---|
| F1-міра | 0.85 | Значення 0.85 свідчить про те, що модель добре працює як у точності передбачень, так і в покритті справжніх позитивних випадків. |
| Специфічність | 0.83 | Значення 0.83 також є досить хорошим показником, свідчить про те, що модель правильно ідентифікує нешкідливі пакети. Здатності моделі визначати негативні класи можна оцінити, як високу. |
| Точність | 0.87 | Значення 0.87 є досить високим і може свідчити про те, що модель правильно класифікує обидва класи (шкідливі та нешкідливі пакети) з високою точністю. |

В результаті оцінки моделі на тестових даних було отримано наступні результати, які відображені у таблиці 1:

1. F1-міра: 0.85. Це значення свідчить про те, що модель добре працює як у точності передбачень, так і в покритті справжніх позитивних випадків.
2. Специфічність: 0.83. Цей показник також є досить хорошим, що свідчить про те, що модель правильно ідентифікує нешкідливі пакети. Здатність моделі визначати негативні класи можна оцінити як високу.
3. Точність: 0.87. Це високе значення може свідчити про те, що модель правильно класифікує обидва класи (шкідливі та нешкідливі пакети) з високою точністю.

Отримані результати свідчать про те, що модель показала дуже прийнятні результати після навчання. Точність на рівні 0.87 може бути показником того, що модель добре навчилася і показує високу правильність передбачень.

**Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі**

Запропонований метод виявлення DDoS-атак у мережах з використанням глибоких згорткових нейронних мереж використовує для аналізу трафіку завчасно навчену модель нейронної мережі, засновану на наборі даних, який описує значну кількість можливих атак на мережу.

Досліджено сучасний стан аналізу DDoS-атак, визначено, що використання CNN є ефективним інструментом для виявлення цих загроз. Мережі можна навчити розпізнавати особливості, що відрізняють шкідливі пакети від дозволених, що дозволяє виявляти їх з високою точністю. Досліджено моделі CNN та LSTM, визначено їхню ефективність серед існуючих методів виявлення DDoS-атак. Зокрема, метод DDoS-Detector на базі глибоких згорткових мереж показав високу ефективність у порівнянні із іншими типами виявлення.

Архітектура згорткових нейронних мереж використовує кілька згорткових та повністю зв’язаних шарів для виділення важливих характеристик та зроблення прогнозів щодо типу трафіку. Оптимальна архітектура моделі сприяє підвищенню точності та ефективності виявлення шкідливих пакетів.

Підготовка даних перед навчанням моделі є вирішальним етапом для досягнення високої точності класифікації. Оптимізація гіперпараметрів також впливає на ефективність моделі, допомагаючи досягти оптимальних результатів.

Використання наборів даних, таких як KDD Cup 99, є важливим для аналізу кібербезпеки. Ці дані надають можливість розробити моделі, здатні виявляти складні загрози та аналізувати різноманітні аспекти мережевого трафіку. Остаточна оцінка моделі на тестових даних здійснюється за допомогою різноманітних метрик, таких як точність, відгук, специфічність та F1-мера. Ці метрики дозволяють оцінити ефективність та точність алгоритму виявлення DDoS-атак.

Таким чином, згорткові нейронні мережі разом із попередньою обробкою даних виявляються потужним інструментом для аналізу мережевого трафіку та виявлення шкідливих.

## References

1. Li, Q.; Meng, L.; Zhang, Y.; Yan, J. DDoS attacks detection using machine learning algorithms. In *International Forum on Digital TV and Wireless Multimedia Communications*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 205–216.
2. Mohammad Najafimehr, Sajjad Zarifzadeh, Seyedakbar Mostafavi (2023). DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. [URL] - https://onlinelibrary.wiley.com/doi/full/10.1002/eng2.12697.
3. Nick Barney, Ben Lutkevich. Network Security. [URL] - https://www.techtarget.com/searchnetworking/definition/network-security.
4. What is network security? [URL] - https://www.cloudflare.com/learning/network-layer/network-security.
5. "DDoS, Machine Learning, Measures". // "Understanding Denial-of-Service Attacks". / , 2016. – (Taylor & Francis Group). – (ISBN:13: 978-1-4987-2965-9). – С. 12–34.
6. M. Tayyab, B. Belaton, and M. Anbar, ‘‘ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review,’’ IEEE Access, vol. 8, pp. 170529–170547, 2020.
7. Dyari Mohammed Sharif, Hakem Beitollahi. A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Computers & Security: Volume 135, December 2023, 103511. URL: https://doi.org/10.1016/j.cose.2023.103511.
8. Devrim Akgun, Selman Hizal, Unal Cavusoglu. A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Computers & Security: Volume 118, July 2023, 102748. URL: https://doi.org/10.1016/j.cose.2022.102748.
9. Omerah Yousuf, Roohie Naaz Mir. DDoS attack detection in Internet of Things using recurrent neural network. Computers and Electrical Engineering: Volume 101, July 2022, 108034. URL: https://doi.org/10.1016/j.compeleceng.2022.108034
10. Ali Mustapha, Rida Khatoun, Sherali Zeadally, Fadlallah Chbib, Ahmad Fadlallah, Walid Fahs, Ali El Attar. Computers & Security: Volume 127, April 2023, 103117. URL: https://doi.org/10.1016/j.cose.2023.103117.
11. Pew Research Center. Artificial Intelligence and the Future of Humans. URL: https://www.pewresearch.org/internet/2018/12/10/artificial-intelligence-and-the-future-of-humans.
12. Freecodecamp. Deep Learning Neural Networks Explained in Plain Englishhttps://www.freecodecamp.org/news/deep-learning-neural-networks-explained-in-plain-english.
13. Zainudin A, Ahakonye LAC, Akter R, Kim D-S, Lee J-M. An efficient hybrid-DNN for DDoS detection and classification in software-defined IIoT networks. IEEE Internet Things J. 2023; 10(10):8491-8504. doi:10.1109/JIOT.2022.3196942.

14. Hoang L.-H. TRe-Map: Towards Reducing the Overheads of Fault-Aware Retraining of Deep Neural Networks by Merging Fault Maps / Le-Ha Hoang, Muhammad Abdullah Hanif, Muhammad Shafique // 2021 24th Euromicro Conference on Digital System Design (DSD), Palermo, Italy, 1–3 September 2021. – 2021. – DOI: https://doi.org/10.1109/dsd53832.2021.00072.

15. Zhang L. Self-Distillation: Towards Efficient and Compact Neural Networks / Linfeng Zhang, Chenglong Bao, Kaisheng Ma // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2021. – Vol. 44, no. 8. – P. 4388-4403. – DOI: https://doi.org/10.1109/tpami.2021.306710.

16. A taxonomy and survey of attacks against machine learning / Nikolaos Pitropakis [et al.] // Computer Science Review. – 2019. – Vol. 34. – DOI: https://doi.org/10.1016/j.cosrev.2019.100199.

17. Detection and recovery against deep neural network fault injection attacks based on contrastive learning / Wang C. [et al.] // Proceedings of the 3rd Workshop on Adversarial Learning Methods for Machine Learning and Data Mining at KDD, Singapore, 14 Aug. 2021. – 2021.