УДК 004.8:004.9 **doi: 10.26906/SUNZ.2025.2.125-131**

О. Ю. Заковоротний, А. В. Хулап

Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна

АНАЛІЗ МОДЕЛЕЙ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ НЕЙРОМЕРЕЖ У СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Анотація. Стрімкий ріст популярності систем інтернету речей робить проблему підвищення безпеки все більш значущою. Але через те, що більшість сенсорів та виконавчих пристроїв базуються на енергоефективних мікроконтролерах, використання популярних моделей виявлення вторгнень на основі нейромереж практично неможливе для таких пристроїв. **Мета** даної роботи полягає в аналізі існуючих систем виявлення вторгнень на основі мережевої інформації з точки зору використання в енергоефективних мікроконтролерах з обмеженими обчислювальними можливостями. **Отримані наступні результати:** переважна більшість досліджень пропонують масштабні моделі нейромереж, які неможливо використати у малих мікроконтролерах. Проводяться тільки дослідження ефективності, але не швидкодії або споживання ресурсів. Але у декількох роботах запропоновано зниження кількості параметрів мережевих протоколів, на основі яких проводиться розпізнавання, та проведено аналіз впливу цього зниження на ефективність розпізнавання. Також визначені найпопулярніші загальнодоступні набори даних, які можна використовувати для порівняння ефективності виявлення вторгнень. **Висновки:** моделі нейромереж, які використовують скорочений набір мережевих параметрів для розпізнавання, в поєднанні з оптимізацією обчислень нейромереж є перспективним напрямом подальших досліджень. При використанні загальнодоступних наборів даних можна проводити порівняння з рішеннями, які вже існують.

Ключові слова: нейромережа, розпізнавання втручань, мережевий трафік, набори даних, аналіз.

Вступ

Інтернет речей (IoT) швидко розвивається, охоплюючи різноманітні аспекти нашого життя. Завдяки технологіям 4G, 5G і покращенню стандартів зв`язку, IoT стає дедалі доступнішим. У 2020 році кількість IoT-пристроїв складала 15,1 мільярда, а до 2030 року прогнозується зростання до 29 мільярдів [1]. Основними напрямками розвитку є промислове застосування, медичні пристрої та розумні будинки. У 2023 році понад 57% організацій у Європі та Північній Америці вже впровадили IoT [2]. Очікується, що до 2025 року в середньому в домогосподарствах США буде 20 підключених пристроїв [3].

Розумні будинки включають пристрої, такі як системи безпеки, термостати та освітлення, якими можна керувати дистанційно або автоматично. У промисловості IoT використовується для моніторингу обладнання, покращення ефективності і оптимізації виробничих процесів. У медичній сфері IoT допомагає в моніторингу стану пацієнтів, управлінні хронічними захворюваннями та наданні своєчасної медичної допомоги.

Таким чином, інтернет речей (IoT) відкриває нові можливості для автоматизації та підвищення ефективності, однак також створює нові загрози для безпеки. У дослідженнях [4..9] наведені основні типи атак на IoT через мережу. Ці атаки можуть дозволити зловмисникам проникнути до внутрішньої мережі та отримати доступ до конфіденційної інформації або засобів управління пристроями. Також хакери можуть використовувати спеціально створені експлойти для несанкціонованого доступу, запуску шкідливих команд або повного порушення роботи системи.

Системи виявлення вторгнень (Intrusion Detection System, IDS) можна загалом поділити на два основні типи: виявлення вторгнень на основі хосту та мережеве виявлення вторгнень. Виявлення на основі хосту відстежує специфічні дії на хості, такі як доступ до системних файлів або запуск програм. Мережеве виявлення вторгнень зосереджується на моніторингу потоку даних між комп'ютерами та виявленні аномального мережевого трафіку між різними комп'ютерами в мережі.

У мережі існують дві основні категорії поведінки: нормальна та аномальна. Нормальна поведінка відповідає певним стандартам щодо обсягу трафіку, використовуваних програм та типів даних, якими обмінюється мережа. Аномалії мережі можна поділити на дві основні групи: мережеві збої, такі як перевантаження мережі або поламка файлових серверів, а також атаки на безпеку мережі, зокрема DDoS-атаки та інші шкідливі дії, що здійснюються зловмисниками.

Машинне навчання (Machine Learning, ML) має важливу роль у сучасних системах виявлення мережевих вторгнень (IDS), оскільки дозволяє ефективно аналізувати великі обсяги мережевих даних і виявляти аномалії, які можуть бути ознаками кібератак. До традиційних належать дерева рішень, наївний баєсівський класифікатор та метод опорних векторів (SVM). Ці алгоритми дозволяють класифікувати трафік на нормальний і підозрілий, ґрунтуючись на аналізі характеристик даних. Наприклад, дерева рішень забезпечують високу точність і добре масштабуються на великі обсяги інформації. Глибоке навчання, зокрема конволюційні (CNN) та рекурентні нейронні мережі (RNN), демонструє високу ефективність у виявленні атак завдяки здатності виявляти складні просторові та часові залежності в даних. Це дозволяє моделювати поведінкові шаблони, характерні для різних типів вторгнень. Генеративні змагальні мережі (GAN) використовуються для вирішення проблеми дисбалансу даних, що є актуальним у випадках рідкісних атак. Штучно згенеровані зразки підвищують ефективність навчання IDS-моделей. Гібридні підходи поєднують переваги кількох методів, наприклад, CNN та RNN, що дозволяє враховувати як просторову, так і часову структуру трафіку. Крім того, застосування методів обробки природної мови (NLP) дає

змогу аналізувати текстові компоненти мережевих даних, такі як лог-файли чи заголовки повідомлень. Таким чином, використання машинного навчання у виявленні вторгнень дозволяє значно підвищити точність та адаптивність систем кіберзахисту в умовах постійно змінюваного середовища загроз.

Попри значні досягнення, використання машинного навчання в IDS стикається з певними викликами. Одним з основних є необхідність у великих обсягах даних для навчання моделей. Крім того, моделі машинного навчання можуть бути вразливими до атак, таких як отруєння даних, коли зловмисники вводять шкідливі дані для навчання моделі. Важливо також забезпечити інтерпретацію та візуалізацію результатів, щоб користувачі могли розуміти, чому модель приймає певні рішення.

Однак найбільша проблема полягає в необхідності великих ресурсів, таких як обчислювальна потужність і великий обсяг пам'яті, що є недоступними для більшості пристроїв Інтернету речей. У цій статті проводиться аналіз рішень IDS, які вже існують, їх відповідність обчислювальним можливостям IoT та можливості подальшої оптимізації цих IDS.

Постановка проблеми

Сучасні кіберзагрози стають дедалі складнішими, що ставить нові вимоги до систем виявлення мережевих вторгнень (NIDS). Для забезпечення ефективності цих систем необхідні актуальні й реалістичні набори даних мережевого трафіку, здатні відображати реальні умови. Основною проблемою є те, що існуючі стандартні набори даних не завжди відповідають вимогам реального світу; вони можуть не містити необхідних характеристик або містити зайві й непотрібні дані.

У статтях [10..13] розглядаються важливі аспекти збору даних для побудови систем виявлення мережевих вторгнень, зокрема для застосування методів машинного навчання. Автори підкреслюють необхідність створення стандартного набору важливих характеристик для мережевого трафіку, що дозволяє ефективно застосовувати машинне навчання у реальних умовах. Дослідження вказують на важливість мінімізації обсягу даних, що збираються, для досягнення високої ефективності в реальному часі. Встановлення оптимального набору характеристик і мінімального обсягу даних дозволяє значно знизити витрати на збір та обробку даних, забезпечуючи при цьому точність і ефективність моделей виявлення вторгнень.

Окрім основних проблем і підходів, пов’язаних із використанням машинного навчання для виявлення вторгнень, у дослідженнях цієї галузі акцентується увага на низці важливих аспектів, що визначають ефективність практичних рішень. Одним із таких аспектів є використання даних на основі потоків (flow-based), таких як NetFlow, IPFIX або sFlow. Потокові дані дозволяють зменшити обсяг інформації для обробки та забезпечують ефективний аналіз у високошвидкісних мережах, що є критично важливим для виявлення вторгнень у реальному часі.

Значною проблемою є постійно змінюваний ландшафт кіберзагроз. Нові типи атак швидко з’являються, роблячи застарілими як існуючі набори даних, так і моделі виявлення, що вимагає розробки адаптивних систем, здатних працювати з новими, ще невідомими загрозами. Також підкреслюється необхідність оптимізації процесу збору даних, адже надмірний обсяг навчальної інформації призводить до зростання витрат ресурсів. Завдання полягає у мінімізації обсягу вхідних даних без втрати ефективності побудованої моделі.

Одним із критичних етапів моделювання є вибір характеристик (feature selection). Коректне визначення інформативних ознак дозволяє зменшити складність моделі та підвищити її точність. При цьому надмірна кількість непотрібних або корельованих ознак може призвести до погіршення якості класифікації та зниження швидкодії. Окремо розглядається проблема недостатньої доступності маркованих даних. У більшості реальних мереж важко отримати чітко класифікований трафік, що значно ускладнює навчання алгоритмів у контрольованому режимі. У таких умовах зростає роль методів напівконтрольованого та безконтрольного навчання.

Важливим викликом є перенесення теоретичних рішень у реальні умови. Моделі, розроблені у лабораторних середовищах, не завжди ефективно працюють у продуктивних мережах, де додатковими обмеженнями є питання конфіденційності, точності збору та затримки в обробці даних. Крім того, визначення мінімально необхідного обсягу навчальних даних для побудови ефективної моделі дозволяє оптимізувати процеси збору та знизити ресурсоємність впровадження IDS у практичні мережі. Нарешті, важливою задачею є стандартизація наборів ознак для виявлення атак. Визначення загального підходу до формування ефективних характеристик дозволяє спростити інтеграцію рішень та забезпечити можливість використання технік перенесення навчання, що зменшує потребу у створенні окремих моделей для кожного нового випадку.

Ці теми підкреслюють важливі аспекти, пов'язані з практичним застосуванням машинного навчання у кібербезпеці, а також необхідність оптимізації процесів збору та обробки даних для досягнення ефективних результатів.

Основна частина роботи

У галузі виявлення мережевих вторгнень (NIDS) вирішальну роль відіграють відкриті набори даних, що використовуються для навчання та тестування різноманітних моделей та алгоритмів. Наявність якісних та різноманітних даних дозволяє ефективно перевіряти нові системи в реальних умовах. У цьому контексті порівняння найпоширеніших публічних наборів даних для NIDS є важливим етапом у виборі найбільш підходящих для подальших досліджень. У аналізі [14.. 16] розглядаються найбільш вживані набори даних, їхні особливості та недоліки, а також висновки щодо їхньої ефективності для порівняння нових систем виявлення вторгнень.

Серед усіх наборів слід відзначити наступні:

- KDD Cup 1999: Один з найвідоміших наборів даних для IDS, створений на основі DARPA 1998 року. Він містить 41 ознаку та понад 4.8 млн рядків даних, що описують атаки в чотирьох категоріях:

DoS, R2L, U2R та probing. Однак він має деякі недоліки, такі як дублювання між навчальним та тестовим набором, відсутність важливих ознак (наприклад, IP-адрес), застарілість даних, що було зібрано понад 20 років тому, і синтетичність даних.

- NSL-KDD 2009: Поліпшений набір даних для виправлення недоліків KDD Cup 1999, що зменшив кількість дублюючих записів, зберігаючи більшу частину важливих даних. Незважаючи на це, він все одно містить дані, зібрані ще в 1998 році, що обмежує його актуальність та застосування до сучасних атак.
- UNSW NB15 IDS: Зібраний за допомогою генератора трафіку IXIA, цей набір містить дані у форматах pcap, BRO, Argus і CSV. Він є оновленим набором, що включає нові типи атак. Однак дані згенеровані синтетично, що знижує їхню реалістичність порівняно з реальним трафіком.
- UGR'16: Зібраний з кількох колекторів netflow v9 в мережі іспанського інтернет-провайдера, цей набір має поділ на калібрувальні та навчальні набори. Більшість трафіку позначено як "фоновий", що може бути як аномальним, так і безпечним. Суміш синтетичних атак і реального трафіку також впливає на якість даних.
- CIDDS-001: Цей набір даних зібраний для оцінки аномалій в IDS та містить обмежену кількість атак (DoS, Brute Force, Port Scanning). Недостатня різноманітність атак обмежує можливості для оцінки ефективності систем у широкому спектрі атак.
- CICIDS'17: Набір даних включає різні типи атак, що відбувалися протягом п'яти днів, із зазначенням конкретних атак на кожен день. Трафік на основі реального використання, хоча й містить певні застарілі дані, але цей набір більш актуальний порівняно з попередніми.
- CSE-CIC-IDS2018: Набір включає 50 машин у мережі, де присутні атаки різних типів з використанням B-профілю для моделювання поведінки. Однак використання штучно створених профілів може знизити точність даних.
- LITNET-2020: Зібраний в Литві, цей набір містить реальні мережеві атаки в національній мережі. Оскільки дані зібрані в специфічному регіоні, вони можуть бути менш застосовними для досліджень в інших країнах або на глобальніших мережах.
- MAWILab: Набір даних містить мережевий трафік між Японією та США, охоплюючи кілька років і включаючи різноманітні аномалії. Однак він може бути менш актуальним для сучасних мереж, оскільки використовуються старі мережеві лінії.

Аналізуючи наведені набори даних, можна зробити висновок, що найбільш придатними для подальших досліджень є наступні набори. CICIDS'17 та CSE-CIC-IDS2018: Обидва набори містять більш актуальні дані про атаки, що відбуваються в сучасних мережах. Вони охоплюють широкий спектр атак, що дозволяє проводити різноманітні дослідження ефективності систем в реальних умовах. NSL-KDD 2009: Попри застарілість, цей набір все ж може бути корисним для порівняння нових методів з давно відомими базами, оскільки він надає структуровані й очищені дані. Для порівняння ефективності нових систем, що використовують машинне навчання, необхідно враховувати не лише актуальність даних, а й специфічні характеристики трафіку в мережах. Зокрема, використання реальних даних (наприклад, у CICIDS'17 та LITNET-2020) буде значно кориснішим для тестування нових IDS на сучасних реальних атаках.

З огляду на наведене, для подальших досліджень найдоцільніше зосередитися на CICIDS'17, CSE-CIC-IDS2018 та NSL-KDD 2009, оскільки вони дозволяють порівняти різні методи на актуальних даних та проводити ефективне тестування нових підходів до виявлення вторгнень.

Попри високий потенціал нейронних мереж, особливо моделей глибинного навчання, їхнє застосування у системах виявлення вторгнень супроводжується низкою обмежень, які необхідно враховувати при розробці та впровадженні таких рішень.

Однією з головних проблем є значні обчислювальні вимоги. Глибокі моделі потребують високопродуктивного апаратного забезпечення, зокрема графічних (GPU) або тензорних процесорів (TPU), що робить їх навчання ресурсомістким та дорогим процесом [17]. Паралельно з цим, великі обсяги моделі призводять до підвищеного споживання пам'яті [18], що особливо критично в умовах обмежених ресурсів, як-от на периферійних пристроях або в реальному середовищі мережевого моніторингу.

Ще одним важливим обмеженням є тривалий час навчання. Моделі глибинного навчання вимагають значного часу для обробки великих обсягів даних, що ускладнює оперативне оновлення моделей при появі нових типів атак. Цей фактор також знижує здатність систем до швидкої адаптації. Важливою вимогою до мережевих IDS-систем є здатність працювати в режимі реального часу. Проте висока складність моделей може спричиняти затримки в обробці трафіку, що обмежує їхню ефективність у виявленні загроз у момент їх виникнення.

Окрему увагу слід приділити проблемі перенавчання. У випадку навчання на незбалансованих наборах даних, де частка атак є незначною, нейронні мережі можуть демонструвати хороші результати на навчальному наборі, але погано узагальнювати знання на нові або раніше невідомі загрози. Зі збільшенням масштабів мереж також ускладнюється завдання масштабованості та адаптації. У таких умовах підтримка високої точності потребує регулярного оновлення моделей або їхнього часткового перенавчання, що додатково збільшує навантаження на систему та її ресурси [19].

Системи виявлення мережевих вторгнень (NIDS), що базуються на нейронних мережах, надають розширені можливості для виявлення складних та еволюціонуючих загроз. Однак їх використання часто супроводжується численними проблемами, пов'язаними з використанням ресурсів, продуктивністю та ефективністю. Зокрема, високі обчислювальні вимоги, значне споживання пам'яті, тривалі часи навчання моделей та затримки при обробці даних у реальному часі ускладнюють їхнє впровадження. Крім того, проблеми перенавчання, складність у масштабуванні та потреба в регулярному перенавчанні моделей знижують загальну

ефективність систем. Ці фактори підкреслюють важливість оптимізації процесів збору та обробки даних для досягнення ефективних результатів у реальному часі, що залишається суттєвим викликом у використанні NIDS, заснованих на нейронних мережах. Виявлення вторгнень у комп'ютерних мережах є важливою складовою забезпечення кібербезпеки. Останні десятиліття для вирішення цієї проблеми активно використовуються алгоритми машинного навчання. Зокрема, методи, такі як опорні вектори (SVM), дерева рішень (DT), глибинне навчання демонструють високу ефективність у задачах класифікації та виявлення атак. Однак ефективність цих методів може значно знижуватися в умовах ворожого середовища, що створює нові виклики для розвитку систем виявлення вторгнень. Стаття [15] розглядає основні підходи до виявлення вторгнень, зокрема алгоритми машинного навчання та їх застосування в умовах реальних атак.

Для оцінки ефективності системи використовуються п'ять ключових метрик: точність, прецизійність, відгук, помилковий тривога та F-оцінка. Ці метрики дозволяють оцінити здатність системи виявляти атаки та розрізняти нормальний і шкідливий мережевий трафік. Застосування таких методів у контексті мережевої безпеки підтверджено у кількох роботах, таких як [15, 20, 21].

Точність (accuracy) вимірює загальну частку правильних класифікацій. Висока точність є бажаною, але вона може не відображати якість класифікації в умовах нерівномірних даних. Прецизійність (precision) показує частку правильно виявлених атак серед усіх виявлених атак. Ця метрика є критично важливою для мінімізації помилкових тривог. Відгук (recall) відображає частку правильно виявлених атак серед усіх реальних атак. Високий відгук свідчить про те, що система виявляє значну частину атак, але не враховує помилкові позитиви. Рівень помилкової тривоги (false alarm) вимірює кількість нормальних мережевих подій, які були помилково класифіковані як атаки. Низький рівень помилкових тривог є важливим для забезпечення точності системи. F-оцінка (f-score) комбінує прецизійність та відгук, дозволяючи знайти оптимальний баланс між ними. Вона є корисною при роботі з нерівномірними наборами даних.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}; \quad (1)$$

$$Precision = \frac{TP}{TP + FP}; \quad (2)$$

$$Recall = \frac{TP}{TP + FN}; \quad (3)$$

$$Falsealarm = \frac{FP}{FP + TN}; \quad (4)$$

$$F - score = \frac{2 * Precision * Recall}{Precision + Recall}, \quad (5)$$

де TP – кількість істинно позитивних результатів (true positives), TN – істинно негативних результатів (true negatives), FP – помилкових позитивів (false positives), FN – помилкових негативів (false negatives).

Використання цих п'яти метрик — точності, прецизійності, відгуку, помилкових тривог та F-оцінки — дає змогу детально оцінити ефективність системи виявлення мережевих вторгнень на основі глибоких згорткових нейронних мереж. Кожна метрика підкреслює різні аспекти роботи системи, забезпечуючи всебічну оцінку ефективності методу.

Далі буде розглянуто декілька наукових праць, які пропонують різні варіанти моделей нейромереж для виконання задач розпізнавання мережевих атак. Всі вони мають різні підходи та використовують загальнодоступні набори даних, які були розглянуті вище.

У дослідженні [22] було розроблено глибоку нейронну мережу яка проводила розпізнавання на основі 41 параметра, які були або напряму взяті з мережевих даних, або сформовані на основі цих даних. Точність розпізнавання склала більше 98%, окрім класу атак U2R (User to Root attack). Але це може бути спричинено відносно невеликою кількістю записів типу U2R у використаних наборах даних. Для експерименту використовувався ПК з процесором Intel Core i-7-5820k, 16 GB RAM та відеокартою Geforce GTX1060. Результати представлені у табл. 1 та 2.

Таблиця 1 – **Ефективність на наборі KDD99**

Тип вторгнення	Accuracy	Recall	F-score
PROBE	0.9818	0.9896	0.9909
DOS	0.999	0.9997	0.9998
U2R	0.8182	0.9091	0.8333
R2L	0.9706	0.9804	0.9756
NORMAL	0.9997	0.9995	0.9997

Таблиця 2 – **Ефективність на наборі NSL-KDD**

Тип вторгнення	Accuracy	Recall	F-score
PROBE	0.9773	0.9935	0.9927
DOS	0.9867	0.994	0.9959
U2R	0.8182	0.9091	0.6452
R2L	0.9694	0.9796	0.9412
NORMAL	0.9984	0.9935	0.9959

У статті [23] проведено три експерименти використовуючи набори даних CICIDS2017 та CTU. У першому експерименті були використані тільки просторові параметри наборів даних. У другому — тільки часові параметри. А у третьому — і просторові, і часові параметри. Результати експерименту приведені у табл. 3 та 4. Точність розпізнавання — більше 99% для усіх типів атак. Для експерименту був використаний ПК з Intel(R) Xeon(R) CPU E5-2620б 32 GB RAM та відеоадаптером Geforce GTX1080ti 11GB.

Таблиця 3 – **Ефективність на наборі CICIDS2017**

Тип н. мережі	Accuracy	Precision	Recall	F-score
CNN2	0.9985	0.9976	0.9985	0.9980
LSTM2	0.9942	0.9944	0.9903	0.9923
CNN+ LSTM2	0.9991	0.9985	0.9993	0.9989
CNN11	0.9978	0.9994	0.9995	0.9995
LSTM11	0.9927	0.9972	0.9971	0.9972
CNN+ LSTM11	0.9981	0.9985	0.9998	0.9992

Таблиця 4 – **Ефективність на наборі NSL-KDD**

Тип н. мережі	Accuracy	Precision	Recall	F-score
CNN2	0.9982	0.9985	0.9989	0.9987
LSTM2	0.9942	0.9984	0.9932	0.9957
CNN+ LSTM2	0.9982	0.9991	0.9984	0.9988
CNN11	0.9701	0.9984	0.9921	0.9952
LSTM11	0.9639	0.9975	0.9916	0.9945
CNN+ LSTM11	0.9877	0.9984	0.9981	0.9983

У експерименті, описаному у [24], використовується набір даних NSL-KDD CUP. Він містить 2 підмножини: KDDTest+ та KDDTest-21. Результати експерименту приведені у табл. 5. Точність визначення — від 79 до 95% в залежності від моделі. Найнижчі результати були отримані для рекурсивної нейронної мережі (RNN). Для експерименту використовувався ПК з наступною конфігурацією: Intel Core i7-7700, 16 GB RAM, Geforce GTX1050.

Таблиця 5 – **Ефективність на наборі KDDTest**

Набір даних	Модель	Accuracy	Recall	False alarm
KDD Test+	IBWNIDM	0.9536	0.9555	0.0076
	LeNet-5	0.8454	0.9131	0.0203
	DBN	0.9245	0.9568	0.0085
	RNN	0.9308	0.9439	0.0092
KDD Test^{-21}	IBWNIDM	0.9091	0.9242	0.0396
	LeNet-5	0.8236	0.8793	0.0324
	DBN	0.8869	0.8948	0.0446
	RNN	0.7947	0.8058	0.0175

Дослідження, яке описане у [25], пропонує декілька моделей нейромереж та використовує набори даних NSL-KDD та UNSW-NB15. На наборі даних NSL-KDD запропоновані моделі показали точність вище 99.5%. Але на наборі даних UNSW-NB15, точність розпізнавання була дещо нижчою — 93%, але, все одно, це дуже гарний результат. Результати цього дослідження наведені у таблицях 6 та 7.

Таблиця 6 – **Ефективність на наборі NSL-KDD**

Модель	Accuracy	Precision	Recall	F-score
MDNN	0.995	0.9953	0.995	0.9951
MCNN	0.995	0.995	0.995	0.995
MCNN-DFS	0.997	0.995	0.998	0.996
NDAE	0.8542	1.00	0.8542	0.8737

Таблиця 7 – **Ефективність на наборі UNSW-NB15**

Модель	Accuracy	Precision	Recall	F-score
BDNN	0.9321	0.94	0.93	0.93
BCNN	0.9442	0.95	0.94	0.94
BCNN-DFS	0.9571	0.96	0.96	0.96

Дослідники, які проводили огляд моделей розпізнавання, які базуються на згорткових нейронних мережах [26], також провели і свій експеримент, запропонувавши декілька своїх моделей розпізнавання. На наборах даних CIC-IDS2017 та NSL-KDD була досягнута точність розпізнавання у 97% та 82% відсотки відповідно. Результати експерименту наведені у табл. 8 та 9.

Всі моделі нейромереж, наведені вище, мають дуже високу точність розпізнавання, але, на жаль, вимагають значних обчислювальних ресурсів.

Таблиця 8 – **Ефективність на наборі CIC-IDS2017**

Модель	К-ть шарів CNN	Accuracy	Precision	Recall	F-score	False alarm
Basic 1D-CNN	1	0.9799	0.9854	0.9975	0.9437	0.0237
	2	0.9808	0.9248	0.9651	0.9445	0.016
	3	0.9766	0.8838	0.992	0.9348	0.0265
Basic 2D-CNN	1	0.981	0.913	0.9809	0.9458	0.019
	2	0.9761	0.9192	0.9414	0.9301	0.0168
	3	0.9774	0.8864	0.9937	0.937	0.0259
Hybrid LTSM with 1D-CNN	2	0.9802	0.9038	0.9881	0.9441	0.0214
Hybrid LTSM with 2D-CNN	2	0.9755	0.8765	0.9954	0.9321	0.0285
Hybrid Autoencoder with CNN	2	0.9524	0.9076	0.7997	0.8502	0.0166

Таблиця 9 – **Ефективність на наборі NSL-KDD**

Модель	К-ть шарів CNN	Accuracy	Precision	Recall	F-score	False alarm
Basic 1D-CNN	1	0.8267	0.9262	0.7558	0.8323	0.0796
	2	0.849	0.9334	0.7913	0.8565	0.0747
	3	0.8887	0.9493	0.8498	0.8968	0.0599
Basic 2D-CNN	1	0.8522	0.9335	0.7971	0.8599	0.0751
	2	0.8559	0.9718	0.7692	0.8587	0.0295
	3	0.8443	0.9348	0.7809	0.8509	0.072
Hybrid LTSM with 1D-CNN	2	0.8993	0.9547	0.8642	0.9072	0.0542
Hybrid LTSM with 2D-CNN	2	0.8205	0.9302	0.7403	0.8244	0.0734
Hybrid Autoencoder with CNN	2	0.8439	0.9335	0.7813	0.8507	0.0735

І тому взагалі не підходять до інтернету речей, де потрібно розпізнавання у реальному часі при дуже обмежених ресурсах. Наприклад, обчислення нейромережі, запропонованої у [25], займало від 3.59 с до 4.17 с. Це дуже великий час для аналізу одного пакета. Через це було проведено дослідження [27] по визначенню мінімально достатнього набору параметрів мережевих протоколів для забезпечення якісного розпізнавання вторгнень. Експерименти показали, що на всіх наборах даних є спільні найбільш інформативні ознаки. Кількість обраних ознак, які не призводять до зниження здатності моделі машинного

навчання до розпізнавання, коливається навколо 10 із 33 доступних ознак у наборах. Остаточний список ознак був складений на основі результатів відбору ознак і порівняний з результатами коефіцієнта кореляції між ознаками, після чого ознаки, які були сильно корельовані між собою, були видалені. Цей список приведений у табл. 10.

Таблиця 10 – **Зменшений перелік мережевих параметрів**

Назва параметру	Значення параметру
FLOW_DURATION_MILLISECONDS	Тривалість потоку даних в мілісекундах
TCP_WIN_MAX_IN	Максимальне TCP вікно (src-dst)
DURATION_OUT	Тривалість потоку від клієнта до сервера (мсек)
MAX_TTL	Максимальний TTL (Time To Live) потоку
L7_PROTO	Протокол 7-го рівня (числ. код)
SRC_TO_DST_AVG_THROUGHPUT	Байт в секунду від джерела до призначення
SHORTEST_FLOW_PKT	Найкоротший пакет потоку (байт)
MIN_IP_PKT_LEN	Довжина min IP-пакету потоку
TCP_WIN_MAX_OUT	Максимальне TCP вікно (dst-src)
OUT_BYTES	Кількість вихідних байтів

Висновки та перспективи подальших досліджень

Моделі нейронних мереж, що використовують повний набір параметрів мережевих протоколів, стикаються з суттєвими обмеженнями при впровадженні в інтернеті речей (IoT) через незначні обчислювальні ресурси та обсяги пам’яті кінцевих пристроїв. Такі моделі вимагають значних обчислювальних потужностей для обробки даних у реальному часі, що ускладнює їх використання в умовах IoT, де час виконання є критичним. Крім того, зберігання великої кількості параметрів та проміжних результатів потребує великих обсягів оперативної пам'яті, що часто є неприпустимим для малих і середніх пристроїв з обмеженими ресурсами.

Натомість моделі нейронних мереж, що використовують скорочений набір ключових мережевих параметрів (10 параметрів), здатні значно зменшити вимоги до ресурсів при збереженні високої ефективності у завданнях класифікації та виявлення аномалій. Поєднання таких моделей із методами оптимізації обчислювальних процесів [28] може сприяти значному покращенню їх продуктивності та масштабованості в реальному часі. Подібні підходи відкривають перспективи для більш ефективного застосування нейронних мереж в умовах IoT, де обмеження з боку ресурсів є ключовим фактором.

Використання загальнодоступних наборів даних, таких як KDD Cup або NSL-KDD 2009, дозволяє проводити порівняння з існуючими методами та алгоритмами, що вже довели свою ефективність в області виявлення вторгнень та аномалій. Це дає змогу систематично оцінювати нові підходи, аналізувати їх точність та швидкодію, а також вдосконалювати методи машинного навчання для забезпечення більш стабільного та надійного захисту мереж в умовах обмежених ресурсів. Подальші дослідження у цьому напрямку є важливими для оптимізації існуючих моделей та їх адаптації до специфічних вимог IoT-систем.

СПИСОК ЛІТЕРАТУРИ

1. Khanna, A., Kaur, S. (2020), “Internet of Things (IoT), Applications and Challenges: A Comprehensive Review”, Wireless Pers Commun 114, 1687–1762, doi: https://doi.org/10.1007/s11277-020-07446-4
2. Kumar, S., Tiwari, P. & Zymbler, M. (2019), “Internet of Things is a revolutionary approach for future technology enhancement: a review”, J Big Data 6, 111, doi: https://doi.org/10.1186/s40537-019-0268-2
3. Choudhary, A. (2024), “Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions”, Discov Internet Things 4, 31, doi: https://doi.org/10.1007/s43926-024-00084-3
4. (2023), “IoT Security: 15 Types of Attacks with Real-World Examples”, Inovasense, url: https://www.inovasense.com/15-types-of-attacks-with-real-world-examples/
5. Chakraborty, S., Pandey, S.K., Maity, S. (2024), “Detection and Classification of Novel Attacks and Anomaly in IoT Network using Rule based Deep Learning Model”, SN COMPUT. SCI. 5, 1056, doi: https://doi.org/10.1007/s42979-024-03429-5
6. Bensaoud, A., Kalita, J. (2025), “Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models”, Ad Hoc Networks 170: 103770, doi: https://doi.org/10.48550/arXiv.2502.11470
7. Almohaimeed, M.; Albalwy, F. (2024), “Enhancing IoT Network Security Using Feature Selection for Intrusion Detection Systems”, Appl. Sci., 14, 11966, doi: https://doi.org/10.3390/app142411966
8. Newman, R.C. (2009), “Computer Security: Protecting Digital Resources”, Jones & Bartlett Learning, url: https://www.jblearning.com/catalog/productdetails/9780763759940?srsltid=AfmBOop8BLj-VJGp7IKaVkbLmnhpqhMjpdoF-8hPzKwlAPy-fAaoVcuUQ
9. Thottan M., Chuanyi Ji. (2003), "Anomaly detection in IP networks", IEEE Transactions on Signal Processing, vol. 51, no. 8, pp. 2191-2204, doi: https://doi.org/10.1109/TSP.2003.814797
10. Dong, H., Kotenko, I. (2025), “Cybersecurity in the AI era: analyzing the impact of machine learning on intrusion detection”, Knowl Inf Syst, doi: https://doi.org/10.1007/s10115-025-02366-w
11. Ajagbe, S.A., Awotunde, J.B. & Florez, H. (2024), “Intrusion Detection: A Comparison Study of Machine Learning Models Using Unbalanced Dataset”, SN COMPUT. SCI. 5, 1028, doi: https://doi.org/10.1007/s42979-024-03369-0
12. Hussein Ali, A., Charfeddine, M., Ammar, B. et al. (2024), “Unveiling machine learning strategies and considerations in intrusion detection systems: a comprehensive survey”, Frontiers in Computer Science, doi: https://doi.org/10.3389/fcomp.2024.1387354
13. Ring, M., Wunderlich, S., Grüdl, D. et al. (2017), “Flow-based benchmark data sets for intrusion detection”, ECCWS 2017 16th European Conference on Cyber Warfare and Security. Academic Conferences and publishing limited, url: https://books.google.com.ua/books?hl=uk&lr=&id=uFA8DwAAQBAJ&oi=fnd&pg=PA361&dq=intrusion+detection+based+on+network+data&ots=YUq_mFVm5C&sig=J12NbOfJq4fMxm7JXE-JWvFkmgM&redir_esc=y#v=onepage&q=intrusion%20detection%20based%20on%20network%20data&f=false

14. Mohammadpour, L., Ling, T. C., Liew, C. S., & Aryanfar, A. (2022), “A Survey of CNN-Based Network Intrusion Detection”, Applied Sciences, 12(16), 8162, doi: https://doi.org/10.3390/app12168162
15. Zhen Yang, Xiaodong Liu, Tong Li, Di Wu, Jinjiang Wang, Yunwei Zhao, Han Han. (2022), “A systematic literature review of methods and datasets for anomaly-based network intrusion detection”, Computers & Security, Volume 116, doi: https://doi.org/10.1016/j.cose.2022.102675
16. Chou D., Jiang, M. (2021), “A Survey on Data-driven Network Intrusion Detection”, ACM Computing Surveys (CSUR), Volume 54, Issue 9, doi: https://doi.org/10.1145/3472753
17. Abdi, M., Razzak, M. I., & Zaib, A. (2020), "Neural Networks for Network Intrusion Detection Systems: A Survey", Computers, Materials & Continua, 63(3), 1401-1420, doi: https://doi.org/10.32604/cmc.2020.011216
18. Zhang, Y., Wang, S., & Jin, X. (2019), "Deep Learning for Network Intrusion Detection Systems: A Survey." Future Generation Computer Systems, 101, 755-763, doi: https://doi.org/10.1016/j.future.2019.07.046
19. Siddiqui, M. K., Khan, M. A., & Zhang, L. (2020), "Challenges in the Real-Time Application of Neural Network-Based Intrusion Detection Systems.", International Journal of Computer Science and Network Security, 20(9), 56-63, doi: https://doi.org/10.22937/IJCSNS.2020.20.9.56
20. L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng and Y. Li (2020), "Data-Driven Intrusion Detection for Intelligent Internet of Vehicles: A Deep Convolutional Neural Network-Based Method", IEEE Transactions on Network Science and Engineering, vol. 7, no. 4, pp. 2219-2230, 1 Oct.-Dec. 2020, doi: https://doi.org/10.1109/TNSE.2020.2990984
21. Muneer, S., Farooq, U., Athar, A., Ahsan Raza, M., Ghazal, T.M., & Sakib, S. (2024), “A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis”, Journal of Engineering, doi: https://doi.org/10.1155/2024/3909173
22. Jia, Y., Wang, M. and Wang, Y. (2019), “Network intrusion detection algorithm based on deep neural network”, IET Inf. Secur., 2019, Vol. 13 Iss. 1, pp. 48-53, doi: https://doi.org/10.1049/iet-ifs.2018.5258
23. Zhang Y., Chen X., Jin L., Wang X., Guo D. (2019), "Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data", IEEE Access, vol. 7, pp. 37004-37016, doi: https://doi.org/10.1109/ACCESS.2019.2905041
24. Yang H., Wang F. (2019), "Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network", IEEE Access, vol. 7, pp. 64366-64374, 2019, doi: https://doi.org/10.1109/ACCESS.2019.2917299
25. Al-Turaiki, I., Altwaijry, N. (2021), “A Convolutional Neural Network for Improved Anomaly-Based Network Intrusion Detection”, Big Data, 2021, Vol. 9, No. 3, pp. 233-252. doi: https://doi.org/10.1089/big.2020.0263
26. Mohammadpour, L., Ling, T.C., Liew, C.S., Aryanfar, A. A (2022), “Survey of CNN-Based Network Intrusion Detection”, Appl. Sci. 2022, 12, 8162, doi: https://doi.org/10.3390/app12168162
27. Komisarek, M., Pawlicki, M., Kozik, R., Hołubowicz, W., & Choraś, M. (2021), “How to Effectively Collect and Process Network Data for Intrusion Detection?”, Entropy, 23(11), 1532, doi: https://doi.org/10.3390/e23111532
28. Заковоротний, О.Ю., Хулап, А.В. (2024), “Оптимізація обчислення нейромереж за допомогою використання цілочисельної арифметики”, Системи управління, навігації та зв’язку, Том 2 № 76, doi: https://doi.org/10.26906/SUNZ.2024.2.090

Received (Надійшла) 20.02.2025
Accepted for publication (Прийнята до друку) 23.04.2025

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Заковоротний Олександр Юрійович - доктор технічних наук, професор, завідувач кафедри комп’ютерної інженерії та програмування, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Oleksandr Zakovorotnyi - Doctor of Technical Sciences, Professor, Head of Department of Computer Engineering and Programming, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine;
e-mail: oleksandr.zakovorotnyi@khpi.edu.ua; ORCID Author ID: http://orcid.org/0000-0003-4415-838X;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57201613700.

Хулап Андрій Валерійович - аспірант кафедри комп’ютерної інженерії та програмування, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Andrii Khulap - PhD student, Department of Computer Engineering and Programming, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine;
e-mail: Andrii.Khulap@cs.khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0002-4103-7972.

Optimization of neural network computation using integer arithmetic

Oleksandr Zakovorotnyi, Andrii Khulap

Abstract. The rapid growth in the popularity of Internet of Things (IoT) systems makes the issue of improving security increasingly important. However, since most sensors and actuators are based on energy-efficient microcontrollers, the use of popular neural network-based intrusion detection models is practically infeasible for such devices. **The aim of this work** is to analyze existing intrusion detection systems based on network information in terms of their applicability to energy-efficient microcontrollers with limited computational capabilities. **The following results were obtained:** the vast majority of studies propose large-scale neural network models that cannot be used on small microcontrollers. Most research focuses solely on detection accuracy, without considering performance or resource consumption. However, several studies propose reducing the number of network protocol parameters used for detection, and analyze the impact of this reduction on detection effectiveness.
The most popular publicly available datasets suitable for evaluating and comparing intrusion detection efficiency were also identified. **Conclusions:** neural network models that use a reduced set of network parameters for recognition, combined with neural network computation optimization, represent a promising direction for future research. Publicly available datasets enable comparison with existing solutions.

Keywords: neural network, intrusion detection, network traffic, datasets, analysis.