КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.772
УДК 004.852:004.056.5

Складанний Павло Миколайович
кандидат технічних наук, доцент
завідувач кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Костюк Юлія Володимирівна
PhD in Computer Science
доцент кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Рзаєва Світлана Леонідівна
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-7589-2045
s.rzaieva@kubg.edu.ua

Самойленко Юлія Олександрівна
кандидат технічних наук, доцент
доцент кафедри автоматизації та комп'ютерних
технологій систем управління ім. професора А.П. Ладанюка
Національний університет харчових технологій, Київ, Україна
ORCID ID: 0000-0003-3787-1435
samoilenkouo@nuft.edu.ua

Савченко Тетяна Віталіївна
кандидат технічних наук, доцент, доцент кафедри інформатики
Національний університет «Києво-Могилянська академія», Київ, Україна
ORCID ID: 0000-0002-8884-5360
sv_t@ukr.net

РОЗРОБКА МОДУЛЬНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ РІЗНИХ КЛАСІВ МЕРЕЖЕВИХ АТАК

Анотація. У статті розглянуто розробку модульних нейронних мереж для виявлення різних класів мережевих атак, що є важливим кроком у напрямку удосконалення систем виявлення вторгнень. Сучасні системи виявлення атак стикаються з численними обмеженнями, серед яких основними є низька ефективність при аналізі великих обсягів даних, високі вимоги до часу навчання моделей, а також проблеми з адаптацією до нових типів загроз. Ці недоліки обумовлені використанням монолітних підходів, при яких усі параметри мережевої взаємодії обробляються в рамках однієї нейронної мережі, що значно знижує гнучкість та ефективність системи. Пропонований у статті модульний підхід передбачає використання окремих нейронних мереж для обробки груп однотипних параметрів мережевої взаємодії, що дозволяє підвищити ефективність виявлення атак, зменшити час навчання моделей, а також здійснювати динамічне відключення або перепідготовку окремих модулів без необхідності зупиняти роботу всієї системи. Така архітектура дозволяє більш ефективно класифікувати атаки, а також покращити здатність системи до адаптації до нових загроз. У статті також детально аналізуються переваги модульного підходу порівняно з традиційними монолітними системами, що забезпечують значно більшу гнучкість і точність у виявленні та класифікації різних класів атак.

Ключові слова: кібербезпека; кіберзагроза; модульні нейронні мережі; кібератака; мережеві атаки; аналіз трафіку; машинне навчання; класифікація загроз; градієнтний спуск; система виявлення вторгнень.

ВСТУП

Забезпечення належного захисту комп'ютерних мереж від вторгнень та кіберзагроз є одним з основних завдань сучасних інформаційних технологій. В умовах постійного збільшення складності атак та появи нових типів загроз традиційні системи виявлення вторгнень, які використовують сигнатурний метод, стають менш ефективними. Це пов'язано з їх здатністю виявляти лише відомі атаки за допомогою формальних ознак, таких як параметри заголовків або передані дані, що обмежує їх здатність протидіяти новим, невідомим загрозам. Для вирішення цієї проблеми пропонується використання модульного підходу, який полягає у використанні окремих нейронних мереж для аналізу різних груп параметрів мережевої взаємодії. Такий підхід дозволяє підвищити ефективність виявлення атак та забезпечує гнучкість при адаптації системи до нових умов. Завдяки модульній архітектурі можна більш точно аналізувати специфічні типи мережевих атак, обробляючи лише відповідні параметри, що зменшує кількість помилкових спрацьовувань та підвищує точність класифікації. Окрім того, кожен модуль може бути оптимізований для конкретних параметрів, що дозволяє адаптувати систему до різних типів мережевих загроз. Модульний підхід також дає змогу здійснювати динамічне оновлення або перепідготовку частин системи, що дозволяє системі швидко реагувати на нові загрози без необхідності перепідготовки всієї мережі. Це знижує навантаження на систему та скорочує час реагування на зміни в мережевому середовищі. Більш того, модульний підхід забезпечує зручність у масштабуванні системи, оскільки нові модулі можна додавати для аналізу нових параметрів або типів атак без значних змін в основній архітектурі. В цілому, модульний підхід надає можливість створити більш адаптивні та ефективні системи виявлення вторгнень, здатні забезпечити високий рівень захисту в умовах постійно змінюваних кіберзагроз.

Постановка проблеми. Однією з основних проблем сучасних систем виявлення вторгнень є обмеження, пов'язані з використанням монолітного підходу, при якому всі параметри мережевого взаємодії подаються на вхід однієї нейронної мережі. Це призводить до зниження ефективності аналізу, збільшення часу навчання та ускладнення перепідготовки системи при зміні топології мережі. Крім того, неможливість класифікації атак, зокрема нових або невідомих, ускладнює подальшу обробку результатів та усунення загроз. Модульний підхід, що передбачає використання окремих нейронних мереж для обробки груп однотипних параметрів, дозволяє усунути ці недоліки та значно підвищити ефективність виявлення та класифікації атак. Задача полягає в розробці такої архітектури, що забезпечить покращену класифікацію атак та дозволить адаптувати систему до нових типів загроз.

Аналіз останніх досліджень і публікацій. Аналіз літературних джерел показує, що сучасні дослідження в області нейронних мереж для виявлення мережевих атак намагаються удосконалити існуючі підходи, підвищуючи їх ефективність і точність. І. Шпінарева розглядає застосування глибоких нейронних мереж для виявлення атак на основі мережевого трафіку, зокрема для класифікації різних класів мережевих атак, таких як DoS та Shellcode. Вона акцентує увагу на важливості використання модульних нейронних мереж для покращення точності виявлення та зменшення помилкових спрацьовувань [1]. Проте

зазначений підхід не враховує проблему інтеграції з уже існуючими системами безпеки, що є важливим для розгортання таких мереж в реальних умовах.

T. Tang пропонує модульну архітектуру нейронних мереж для класифікації аномалій в мережевому трафіку, зокрема для таких атак, як Fuzzers та Worms. Її дослідження акцентує на значенні динамічної адаптації до нових типів атак, що дозволяє підвищити ефективність існуючих систем захисту [2]. Однак запропонований підхід потребує подальших удосконалень у напрямку автоматичного навчання та оновлення моделей без залучення спеціалістів.

М. Максімов аналізує застосування багаторівневих нейронних мереж для забезпечення безпеки мережевого трафіку, зокрема для виявлення складних атак, таких як Backdoors та Reconnaissance. Вона зазначає, що модульний підхід дозволяє знижувати навантаження на систему та оптимізувати час обробки даних [3]. Однак її робота не враховує питання захисту від помилкових спрацьовувань, що може призвести до ненавмисного блокування легітимного трафіку.

R. Markus розглядає підхід, при якому для класифікації мережевих атак використовуються окремі нейронні мережі для кожного типу атаки, що дозволяє знижувати ймовірність помилок і підвищити точність виявлення. Автор також досліджує можливість використання таких моделей для інтеграції з іншими системами захисту, що забезпечує гнучкість при їх адаптації до нових загроз [4]. Проте робота не містить досліджень щодо можливих обмежень у масштабуванні таких систем при великих обсягах даних.

Y. Liu та S. Lee проводять порівняльний аналіз традиційних та модульних нейронних мереж для виявлення мережевих атак, пропонуючи підхід, який інтегрує механізми глибокого навчання та штучного інтелекту для створення систем виявлення вторгнень [5]. Основною перевагою їхнього дослідження є можливість швидкої адаптації до нових загроз, однак це потребує високих обчислювальних потужностей, що може стати суттєвим обмеженням для деяких організацій.

Мета статті. Метою статті є розробка та аналіз ефективних підходів до виявлення мережевих атак за допомогою модульних нейронних мереж, що дозволяє подолати обмеження традиційних систем виявлення вторгнень, орієнтованих на сигнатурні методи, шляхом використання окремих нейронних мереж для аналізу різних груп параметрів мережевої взаємодії, що підвищує точність класифікації атак, скорочує час навчання та забезпечує гнучкість при адаптації до нових загроз.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У теорії інформаційної безпеки важливим аспектом є розгляд основних понять, причин виникнення атак, їх різноманітних типів, а також методів захисту від мережевих атак, що обумовлює необхідність впровадження сучасних технологій для забезпечення надійності інформаційних систем. Важливе місце у забезпеченні безпеки мереж займають мережеві системи виявлення вторгнень (СВВ), використання яких виправдане для захисту окремих мережевих сегментів, де розглядаються різноманітні типи СВВ, їх принципи роботи, а також аналізуються комерційні та вільно доступні рішення, що знаходять широке застосування для забезпечення цілісності та конфіденційності даних у мережах [1]. Водночас, у контексті нейронних мереж (НС) розглядаються основи їх теорії, зокрема алгоритми навчання багатошарових перцептронів, які є ефективними інструментами для виявлення загроз у мережах, оскільки вони здатні обробляти великі

обсяги даних і виявляти як відомі, так і невідомі атаки [2], [3]. З метою кращого розуміння напрямків розвитку технології, вивчаються існуючі дослідження, що застосовують НС для виявлення атак у мережевих СВВ, що сприяє подальшому вдосконаленню механізмів захисту.

Існують два основні методи виявлення вторгнень у систему: пошук аномалій та пошук зловживань, і хоча вони обидва використовуються для захисту, вони мають принципові відмінності, що полягають у підходах до виявлення загроз: метод пошуку аномалій орієнтований на виявлення відхилень від нормального функціонування системи, що дозволяє виявляти невідомі атаки, тоді як метод пошуку зловживань зосереджений на виявленні вже відомих атак за допомогою сигнатур [4]. Однак метод пошуку аномалій стикається з проблемою складності побудови профілю нормальної активності користувача, оскільки, по-перше, немає гарантії, що в системі не були зафіксовані атаки на етапі формування цього профілю, а по-друге, стиль роботи користувача може змінюватися з часом, що знижує точність виявлення. Натомість метод пошуку зловживань є більш ефективним для виявлення відомих атак, проте він не здатен реагувати на нові, раніше невідомі загрози, що суттєво обмежує його застосування.

Водночас одним з основних переваг використання НС у обробці інформації є їх здатність до узагальнення, що дозволяє ефективно виявляти навіть раніше невідомі атаки, що є важливим аспектом при створенні систем для виявлення зловживань [7]. У роботі обґрунтовано доцільність використання НС як аналізаторів для пошуку зловживань, оскільки, по-перше, це дозволяє уникнути методів пошуку аномалій, а по-друге, забезпечує більш ефективну обробку інформації та усуває суттєві недоліки традиційних методів пошуку зловживань, що підвищує надійність системи захисту [8]. Проте, аналіз сучасних досліджень показує, що більшість існуючих робіт мають суттєву недосконалість: аналіз параметрів проводиться в рамках однієї нейронної мережі, що обмежує їх здатність масштабуватися та ефективно справлятися з великими обсягами даних, що створює потребу у пошуку нових підходів.

Для подолання обмежень монолітного підходу в роботах пропонується використання кількох нейронних мереж для аналізу параметрів, що створює модульну архітектуру (рис. 1) [10].

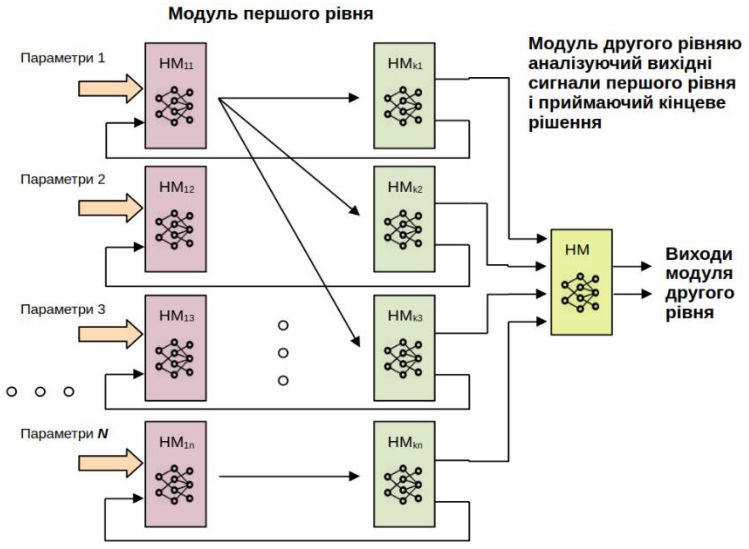

Рис. 1. Модульний підхід до виявлення мережевих атак
Джерело: розроблено автором в середовищі Libre Office (знімок з екрану)

Модульний підхід передбачає використання ієрархічно організованих модулів, кожен з яких містить нейронну мережу різного типу та підсистему обробки вхідних даних, що дозволяє підвищити ефективність аналізу, скоротити час реакції та забезпечити інтеграцію з іншими системами захисту, створюючи таким чином більш гнучку та потужну систему для виявлення та запобігання мережевим атакам.

Модульний підхід до виявлення мережевих атак полягає в використанні ієрархічної структури, де кожен модуль виконує конкретні функції в рамках загальної СВВ. Цей підхід передбачає інтеграцію кількох нейронних мереж різного типу, що дозволяє ефективно обробляти мережевий трафік і виявляти різноманітні класи атак, включаючи нові, невідомі загрози. Важливою перевагою модульної архітектури є здатність кожного модуля адаптуватися до змінюваних умов і специфічних вимог системи, що дозволяє значно підвищити точність виявлення атак, зменшити кількість помилкових спрацьовувань і забезпечити високу продуктивність при обробці великих обсягів даних.

Завдяки такому підходу можна значно знизити навантаження на окремі компоненти системи, оскільки кожен модуль працює з обмеженим набором задач, що дозволяє більш ефективно використовувати ресурси обчислювальних потужностей. Крім того, модульна система має гнучкість у масштабуванні, що робить її адаптованою до різних умов роботи та дозволяє ефективно реагувати на нові типи атак, що з’являються в процесі розвитку технологій.

Застосування нейронних мереж в такій модульній архітектурі дозволяє розв’язувати складні проблеми, такі як виявлення аномалій у мережевому трафіку, автоматичне навчання на основі великих обсягів даних і інтеграцію з іншими системами безпеки [4]. Така система може бути використана для виявлення не тільки традиційних атак, але й складних загроз, таких як атаки типу «zero-day», що робить її важливим інструментом у сучасних умовах кібербезпеки.

Крім того, нейронні мережі в такій архітектурі здатні адаптуватися до нових загроз шляхом безперервного навчання на основі отриманих даних. Вони можуть аналізувати поведінкові характеристики трафіку та виявляти відхилення від нормальної активності. Це дозволяє ефективно реагувати на потенційні загрози ще до того, як вони завдадуть шкоди системі. Завдяки глибокому навчанню та аналізу великих масивів даних, нейронні мережі можуть ідентифікувати навіть малопомітні аномалії. Інтеграція з іншими інструментами безпеки забезпечує багаторівневий захист і підвищує загальну ефективність системи. Така модульна архітектура дає змогу масштабувати рішення відповідно до потреб конкретної організації. Вона також сприяє зниженню рівня помилкових спрацьовувань, що є важливим для оптимізації роботи аналітиків з кібербезпеки. Використання нейромереж дозволяє зменшити час реагування на інциденти завдяки автоматизованому аналізу загроз. Крім того, їх можна навчати на різних наборах даних, що забезпечує гнучкість у виявленні нових типів атак. Таким чином, застосування нейронних мереж у такій архітектурі значно покращує ефективність і надійність систем кібербезпеки.

Розробка модульних нейронних мереж для виявлення різних класів мережевих атак передбачає створення ефективної архітектури системи виявлення вторгнень (СВВ), що враховує специфіку різноманітних мережевих загроз. Для цього було розроблено методику навчання, тестування та застосування СВВ, яка дозволяє ефективно реагувати на атакувальні вектори, що використовуються в сучасних кіберзагрозах. У процесі досліджень були виділені та описані основні типи мережевих атак, які використовувались для навчання та тестування моделі, а також проведена їх класифікація, що сприяло точному визначенню параметрів міжмережевої взаємодії,

ISSN 2663 - 4023

необхідних для обробки в СВВ [8]. На основі аналізу атак, що мали місце, були обрані відповідні групи параметрів, що підлягають обробці у системі виявлення вторгнень, що значно підвищує точність виявлення нових загроз [9]. Крім того, розроблено методи обробки та підготовки значень цих параметрів для подачі їх на вхід системи, що забезпечує належну ефективність при обробці великих обсягів даних. У дослідженні також обґрунтовано необхідність реалізації генератора мережевого шуму, що дозволяє імітувати реальні умови мережевого середовища і підвищує надійність тестування системи [11]. Проведені дослідження вказують на те, що найбільш оптимальним рішенням для цієї задачі є архітектура, представлена на рис. 2, яка враховує всі основні аспекти виявлення та класифікації мережевих атак у реальному часі.

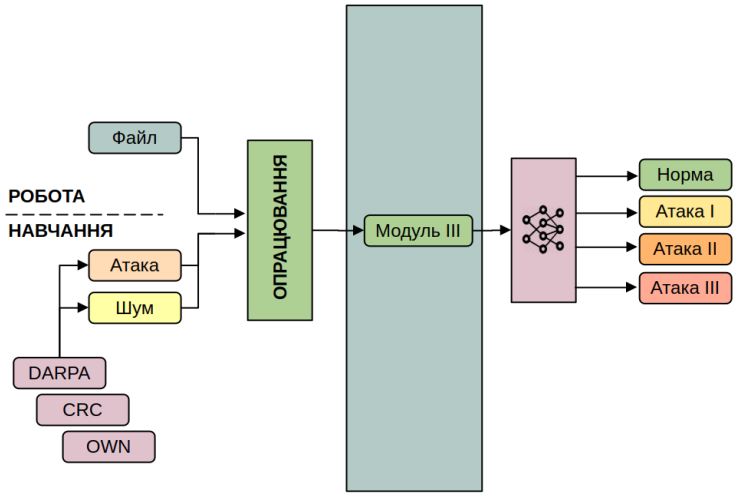

Рис. 2. Архітектура модульної СВВ
Джерело: розроблено автором в середовищі Libre Office (знімок з екрану)

У розробці модульних нейронних мереж для виявлення різних класів мережевих атак важливу роль відіграє підготовка даних для навчання, яка включає використання підготовлених баз атак і генератора мережевого шуму. Обробка даних здійснюється через усереднення за допомогою методу «ковзаючого вікна», нормалізацію, додавання шуму та видалення нульових векторів. Такий підхід дозволяє забезпечити стабільність і точність системи. Модулі першого рівня являють собою ієрархічно розташовані дві нейронні мережі, де друга мережа включається тільки в разі, коли перша не може однозначно визначити наявність аномалії або її відсутність. Завдяки механізму зворотного зв'язку, який використовується в другій мережі, система може динамічно коригувати параметри для глибшого аналізу, що дозволяє значно знизити кількість хибних спрацьовувань.

Виходи модулів першого рівня, що сигналізують про аномалії в певних параметрах, подаються на вхід модуля другого рівня. Тут відбувається остаточне рішення щодо наявності атаки, і при необхідності проводиться додаткова класифікація типу атаки [6], [9]. Така організація дозволяє системі ефективно розпізнавати і класифікувати загрози.

Для навчання нейронних мереж використовуються різноманітні бази атак, що містять приклади реальних загроз. Це дозволяє системі адаптуватися до різних типів атак і умов, забезпечуючи ширший спектр даних для тренування. Застосування різноманітних джерел даних покращує здатність мережі виявляти нові та невідомі методи атак, що підвищує її точність і надійність у реальних умовах.

Розроблена таксономія атак базується на відомій таксономії Ховарда і включає кілька основних класів атак: атаки на аутентифікацію (наприклад, підбір паролів та імен користувачів), методи приховування атак, що використовують специфічні особливості стека TCP/IP, сканування, атаки на доступність (відмова в обслуговуванні), атаки на протокол Telnet, уразливості протоколів TCP/IP та FTP, атаки на різні поштові протоколи (POP3, IMAP, SMTP) та атаки на протокол HTTP [11]. Кожен з цих класів атак містить конкретну кількість прикладів для аналізу, що дозволяє створити точну картину можливих загроз.

Результати аналізу цих атак дозволили обґрунтувати вибір 132 параметрів міжмережевої взаємодії, які використовуються в системах виявлення вторгнень для ідентифікації наявності атак. Крім того, у роботі обґрунтовано застосування методу пошуку зловживань, що вимагало створення генератора мережевого шуму [9], [13]. Це дозволяє забезпечити більш ефективне навчання модулів нейронних мереж і вдосконалити систему виявлення атак [14]. Як основу для побудови генератора шуму була використана база DARPA, що включає як атаки, так і мережеві дані без атак, що робить модель більш стійкою до різноманітних варіантів загроз.

Для усереднення параметрів міжмережевої взаємодії в роботі застосовано метод «ковзаючого вікна». У цьому методі ліва межа тимчасового інтервалу зміщується на величину, меншу за сам розмір інтервалу, що дозволяє ефективно враховувати дані попередніх періодів і адаптувати систему до змін у мережевій активності.

В розробці модульних нейронних мереж для виявлення різних класів мережевих атак важливою частиною є обробка даних, що подаються на вхід нейронних мереж [6]. Одним з основних кроків є оцінка математичного сподівання для дискретного рівномірного розподілу, де ймовірність появи кожного значення, позначеного як $P(X = x_i)$, дорівнює $\frac{1}{n}$, де $i = 1,2 \dots, n$, а n — кількість елементів у множині. Математичне сподівання для таких даних є середнім арифметичним значенням, яке обчислюється за формулою:

$$E(X) = \frac{1}{n}\sum_{i=1}^{n} x_i \quad (1)$$

де x_i — елементи множини X, $X = \{x_1, x_2, \dots, x_n\}$. У випадку, якщо ми аналізуємо часовий ряд, n — це кількість тимчасових інтервалів у середньому наборі X.

Практичний інтерес для задачі виявлення атак представляє вивчення ряду таких множин, кожна з яких є елементом одного вектора, що подається на вхід НС. Нехай V — множина середніх значень вивченого параметра, $V = \{V_1, V_2, \dots, V_n\}$, де N — кількість інтервалів усереднення. При застосуванні методу «ковзаючого вікна» середнє значення параметра обчислюється за формулою:

$$\hat{E}(X) = \frac{1}{n_w}\sum_{i=1}^{n_w} x_i \quad (2)$$

де n_w — кількість тимчасових інтервалів вікна, x_i — елементи вибірки з тимчасового вікна, що ковзає. Кожне вікно представляє собою певний період часу, і значення цього вікна враховує інформацію з попередніх періодів, що дозволяє більш точно врахувати динамічні зміни в мережевій активності.

У рамках розробки нейронних мереж для виявлення атак було проведено дослідження, в якому було проаналізовано 10 різних типів нейронних мереж, 7 функцій активації та 11 алгоритмів навчання. Як показали результати, найбільш ефективними для задачі виявлення мережевих атак виявилися такі нейронні мережі: багатошаровий

персептрон з автономним алгоритмом навчання на основі градієнтного спуску, самоорганізуюча мережа Кохонена, яка використовує шар Гросберга для ефективного навчання на основі спостережень і патернів вхідних даних. Ці методи продемонстрували високу ефективність у виявленні аномалій та класифікації атак завдяки своїй здатності адаптуватися до змінних умов і різноманітних мережевих атак [2], [5]. Результати дослідження показали, що використання багатошарових персептронів з алгоритмами, що використовують градієнтний спуск, дозволяє знизити помилки першого та другого роду, що є критичними для забезпечення високої точності виявлення загроз у реальних умовах. Самоорганізуючі мережі, в свою чергу, продемонстрували здатність до ефективного кластеризації даних без необхідності в попередньому маркуванні, що значно підвищує їх універсальність для задач, де дані можуть бути неповними або шумними.

Оцінка ефективності алгоритмів навчання показала, що алгоритми, засновані на адаптивних методах оптимізації, таких як адаптивний градієнтний спуск (Adam), значно покращують швидкість навчання та точність класифікації в порівнянні з традиційними методами. Градієнтний спуск для оновлення ваг багатошарового персептрона:

$$w_{ij}^{(t+1)} = w_{ij}^{(t)} - \eta \frac{\partial E}{\partial w_{ij}} \quad (3)$$

де w_{ij} — вагові коефіцієнти, η — швидкість навчання, E — функція помилки. Наведена формула визначає процес коригування ваг у персептроні для зменшення помилки. Це також підтверджує високу здатність моделі до обробки великих обсягів даних із збереженням стабільності роботи в умовах змінного мережевого середовища. Загалом, результати дослідження підтверджують, що обрані нейронні мережі і алгоритми навчання можуть бути ефективно використані для виявлення та класифікації мережевих атак, підвищуючи рівень безпеки інформаційних систем. Використання таких технологій дозволяє знижувати ризики, пов’язані з кіберзагрозами, та покращувати адаптивність систем до нових типів атак, що постійно еволюціонують.

Розглянувши різні типи нейронних мереж і алгоритмів навчання, важливо також звернути увагу на вибір активаційної функції, оскільки саме вона значною мірою визначає ефективність навчання та здатність моделі адаптуватися до різноманітних умов. Активаційна функція є критично важливою для нейронних мереж, оскільки вона визначає, як саме нейрон буде активуватися в залежності від вхідних даних.

У випадку багатошарових персептронів (MLP) однією з найбільш поширених активаційних функцій є сигмоїда. Вибір цієї функції обумовлений її здатністю ефективно моделювати нелінійні залежності між вхідними та вихідними даними, що є важливим для розпізнавання складних патернів, таких як мережеві атаки. Сигмоїда має форму S-подібної кривої, що дозволяє трансформувати вихід нейрона в значення в межах від 0 до 1, що зручно для задач класифікації, де результат можна інтерпретувати як ймовірність належності до певного класу. Завдяки своїй властивості згладжувати вихідні значення, сигмоїда також допомагає нейронним мережам стабільно конвертувати інформацію, що важливо при обробці великих обсягів даних з шумом або з багатьма аномаліями. Однак важливо зазначити, що функція сигмоїди має свої обмеження, такі як проблема «втрати градієнта», коли значення градієнта для великих або малих вхідних значень стають дуже малими, що ускладнює навчання нейронної мережі.

У дослідженні вибір сигмоїди для багатошарових персептронів був обґрунтований її здатністю забезпечувати хорошу рівновагу між ефективністю навчання та здатністю до класифікації атак у складних мережевих середовищах. У поєднанні з ефективними алгоритмами навчання, такими як градієнтний спуск, активаційна функція сигмоїда дозволила досягти стабільних результатів у виявленні аномалій, зокрема в складних і

змінних умовах мережевого трафіку. Активаційна функція сигмоїда, яка використовується в MLP:

$$f(x) = \frac{1}{1 + e^{-x}} \quad (4)$$

Дана функція вводить нелінійність у модель і дозволяє мережі краще розпізнавати складні патерни.

Після того як ми розглянули роль активаційних функцій, важливо звернутися до методів, які дозволяють нейронним мережам ефективно класифікувати й обробляти інформацію. Одним з таких методів є використання самоорганізуючої мережі Кохонена (SOM), яка особливо корисна для задач класифікації та виявлення патернів вхідних даних без необхідності наявності попередніх міток. У мережах Кохонена нейрони не тільки отримують інформацію з вхідних даних, а й самоорганізуються, знаходячи найбільш схожі патерни серед різних варіантів. Однак для того, щоб визначити, який нейрон має найбільшу схожість з поточним вхідним вектором, необхідно застосувати метод обчислення відстані між точками у вхідному просторі [12]. Одним із найпоширеніших способів є обчислення евклідової відстані.

Евклідова відстань між двома точками в багатовимірному просторі є простою і інтуїтивно зрозумілою метрикою для порівняння подібності між векторами. Вона обчислюється як квадратний корінь з суми квадратів різниць між відповідними координатами точок. У контексті мережі Кохонена, ця відстань дозволяє оцінити, наскільки близьким є вхідний вектор до нейрона в простору ознак. Чим менша евклідова відстань, тим більша схожість між вхідними даними і поточним нейроном, що дозволяє цьому нейрону «перемогти» в процесі самоорганізації і стати відповідальним за класифікацію конкретного патерну. Цей процес має важливе значення для нашого дослідження, оскільки допомагає точно і швидко виявляти найбільш релевантні нейрони для конкретних мережевих атак. Обчислюючи евклідову відстань між вхідними даними і нейронами мережі Кохонена, ми можемо ефективно класифікувати атаки, а також забезпечити адаптацію системи до змінних умов мережевого середовища, що є необхідним для підтримки високої ефективності в реальних умовах кібербезпеки. Обчислення евклідової відстані для визначення найближчого нейрона у мережі Кохонена:

$$d_i = \sqrt{\sum_{j=1}^{n} \left(x_j - w_{ij}\right)^2} \quad (5)$$

де x_j — координати вхідного вектора, w_{ij} — ваги нейрона. Даний вираз використовується для знаходження найкращого відповідного нейрона в процесі навчання. Наведені математичні вирази відображають ключові аспекти розробки нейронних мереж, що застосовуються для виявлення мережевих атак.

Розробка модульних нейронних мереж для виявлення різних класів мережевих атак є актуальним напрямом у сфері кібербезпеки. Основною метою такої системи є точне розпізнавання загроз з мінімальним рівнем хибних спрацювань. Для цього в роботі обґрунтовано вибір багатошарового персептрона (MLP), навчання якого здійснюється за допомогою алгоритму зворотного поширення помилки.

Обчислення зваженої суми вхідних сигналів для нейрона в MLP:

$$S_j = \sum_{i=1}^{n} w_{ij} x_i + b_j \quad (6)$$

де S_j — сумарний зважений сигнал нейрона, w_{ij} — вага зв'язку між входом x_iі нейроном j, b_j — зміщення (bias). Ця формула визначає активацію нейрона перед передачею його через функцію активації.

Функція активації (наприклад, ReLU або сигмоїда):

$$f(S_j) = \max(0, S_j) \text{ або } f(S_j) = \frac{1}{1+e^{-S_j}}, \quad (7)$$

У першому випадку (ReLU) значення негативних входів обнуляється, що прискорює навчання, а у другому випадку (сигмоїда) отримується значення в діапазоні $(0,1)$, що підходить для ймовірнісної інтерпретації.

Функція помилки MSE (середньоквадратична похибка):

$$E = \frac{1}{N}\sum_{k=1}^{N}(y_k - \hat{y}_k)^2 \quad (8)$$

де y_k — очікуване значення, $\hat{y}_k$ — передбачене значення, N — кількість зразків у навчальному наборі. Ця функція дозволяє оцінити, наскільки точні передбачення мережі порівняно з реальними значеннями.

Процес навчання нейронної мережі складається з кількох основних етапів. Спочатку на вхід подається один із можливих вхідних векторів у режимі прямого поширення сигналу. Для кожного шару мережі розраховується сума зважених входів за формулою:

$$S_j^{(n)} = \sum_{i=1}^{M} y_i^{(n-1)} w_{ij}^{(n)} \quad (9)$$

де M — кількість нейронів у попередньому шарі, $y_i^{(n-1)}$ — вихідні значення нейронів попереднього шару, $w_{ij}^{(n)}$ — вагові коефіцієнти. Отримане значення передається через функцію активації, що дозволяє враховувати нелінійність процесу. Далі обчислюється помилка вихідного шару шляхом порівняння отриманого результату з очікуваним значенням. На основі цієї похибки коригуються вагові коефіцієнти нейронів за допомогою алгоритму зворотного поширення помилки. Градієнтний спуск або його модифікації використовуються для оновлення вагових коефіцієнтів з метою мінімізації функції втрат. Процес навчання повторюється багаторазово, поки мережа не досягне прийнятного рівня точності. Для покращення якості навчання можуть використовуватися методи регуляризації, такі як dropout або L2-нормалізація. Також важливим етапом є вибір оптимальної функції активації, яка визначає здатність мережі до узагальнення. Після завершення навчання нейронна мережа може ефективно класифікувати нові вхідні дані. Таким чином, процес навчання забезпечує адаптацію мережі до розв'язання конкретних задач.

Наступним етапом є оцінка помилки вихідного шару, яка обчислюється за формулою:

$$\delta_j^{(N)} = (y_j^{(N)} - d_j)\frac{df(S_j^{(N)})}{ds_j} \quad (10)$$

де $y_j^{(N)}$ — отриманий вихід мережі, d_j — очікуване значення, $\frac{df(S_j^{(N)})}{ds_j}$ — похідна функції активації. Потім для всіх прихованих шарів визначається похибка нейронів та виконується коригування ваг:

$$\Delta w_{ij}^{(n)} = -\eta \delta_j^{(n)} y_i^{(n-1)} \quad (11)$$

де η — коефіцієнт навчання. Вагові коефіцієнти оновлюються за правилом:

$$w_{ij}^{(n)}(t) = w_{ij}^{(n)}(t-1) + \Delta w_{ij}^{(n)} \quad (12)$$

Цикл повторюється доти, доки похибка не стане меншою за встановлений поріг.

Для забезпечення високої ефективності роботи системи розроблено методику побудови та навчання нейронної мережі, що включає кілька основних етапів. Перш за все, аналізується топологія мережі з урахуванням актуальних класів атак. Вибираються параметри міжмережевої взаємодії, які є найбільш інформативними для розпізнавання загроз. Після цього здійснюється групування цих параметрів для подальшої подачі на вхід модулів першого рівня, які виконують первинну обробку вхідних даних. Наступним етапом є оптимізація вагових коефіцієнтів нейронної мережі шляхом застосування ефективних алгоритмів навчання, таких як градієнтний спуск або його варіації [5]. Після первинного навчання проводиться тестування модулів на контрольному наборі даних для оцінки точності виявлення атак. У разі виявлення значних похибок здійснюється повторне навчання із коригуванням параметрів моделі. Завершальним етапом є інтеграція нейромережевої системи у реальне середовище та її адаптація до змінюваних умов мережевого трафіку.

Наступним кроком є побудова модуля другого рівня, який здійснює остаточне прийняття рішення щодо виявленої аномалії [8]. Для підвищення точності системи проводиться підготовка навчальних даних, що включає нормалізацію, очищення та введення штучного шуму, що підвищує стійкість моделі до варіацій у вхідних даних. Після цього здійснюється навчання модулів нейронних мереж та тестування системи для оцінки її ефективності.

Оцінка якості роботи нейромережевої системи базується на розрахунку ймовірностей помилок першого та другого роду. Помилка першого роду характеризує хибні спрацювання системи (виявлення атаки там, де її немає), тоді як помилка другого роду означає випадки, коли атака залишилася непоміченою. Мінімізація цих похибок дозволяє досягти високої точності виявлення загроз і підвищити ефективність нейронної мережі в реальних умовах. Розроблений підхід до побудови модульних нейронних мереж дозволяє системі адаптуватися до нових типів атак, що робить її ефективним інструментом у сучасних системах кібербезпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Розробка модульних нейронних мереж для виявлення мережевих атак є важливим напрямом у сфері кібербезпеки, який дозволяє підвищити ефективність виявлення загроз. Використання модульного підходу забезпечує більш точне розпізнавання атак завдяки розподілу процесу аналізу між різними рівнями нейронної мережі. Запропонована система складається з модулів першого рівня, які здійснюють первинну обробку параметрів мережевого трафіку, та модуля другого рівня, що приймає остаточне рішення щодо виявленої аномалії.

На відміну від монолітних нейромереж, що аналізують усі параметри одразу, модульний підхід дозволяє спеціалізованим моделям зосереджуватися на конкретних групах параметрів. Це значно знижує навантаження на систему та підвищує її продуктивність. Однією з основних переваг запропонованого підходу є можливість гнучкого налаштування модулів відповідно до нових типів атак.

Система дозволяє адаптивно додавати нові модулі для обробки ще не відомих загроз без необхідності зміни всієї архітектури. Завдяки використанню методів

машинного навчання та нейронних мереж різного типу, вдалося досягти високої точності класифікації атак. Особлива увага була приділена підготовці навчальних даних, що включає нормалізацію, фільтрацію та введення штучного шуму для покращення узагальнюючої здатності моделі. Проведені експерименти показали, що модульний підхід дозволяє суттєво зменшити рівень хибних спрацювань порівняно з традиційними сигнатурними методами. Помилки першого роду (хибні спрацювання) та другого роду (пропущені атаки) були знижені завдяки оптимізації процесів навчання мережі. Використання сучасних алгоритмів активації та навчання, таких як градієнтний спуск, дозволило підвищити швидкість і точність роботи системи.

Двохрівнева архітектура забезпечує можливість глибшого аналізу даних, що значно покращує здатність системи до виявлення складних загроз. Важливою особливістю є можливість поступового оновлення модулів без необхідності зупинки всієї системи. Це дозволяє забезпечити безперервний моніторинг мережевого трафіку та вчасно реагувати на нові виклики.

На практиці такий підхід може бути інтегрований у сучасні системи виявлення вторгнень для підвищення їхньої ефективності. Запропонована архітектура підходить як для централізованих, так і для розподілених систем безпеки, що робить її універсальним рішенням. Впровадження модульних нейромереж також сприяє зниженню витрат на обчислювальні ресурси, оскільки кожен модуль працює незалежно від інших. Система може бути використана для аналізу різних типів атак, включаючи DDoS, сканування портів, спроби експлуатації вразливостей тощо. Вона дозволяє не тільки виявляти атаки, а й класифікувати їх за типами та рівнем небезпеки. Це значно спрощує процес реагування та усунення загроз.

Динамічне оновлення та можливість автоматичного навчання на нових даних роблять систему стійкою до змін у природі атак. Завдяки цьому запропонована модель здатна ефективно працювати в умовах постійно зростаючої складності мережевих загроз. Модульний підхід до аналізу кібербезпеки дозволяє поєднувати переваги різних нейронних мереж та використовувати їх у відповідних контекстах. Загалом, розроблена система є ефективним рішенням для сучасних викликів у сфері інформаційної безпеки. Вона забезпечує гнучкість, високу точність та можливість адаптації до нових загроз. Враховуючи швидку еволюцію атак, модульна архітектура є найбільш перспективним підходом до побудови систем захисту мережевої інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shpinareva, I. M., Yakushina, A. A., Voloshchuk, L. A., & Rudnichenko, N. D. (2021). Detection and classification of network attacks using the deep neural network cascade. *Herald of Modern Information Technologies, 4(3),* 244–254.
2. Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R. & Ghogho, M. (2016). Deep learning approach for network intrusion detection in software defined networking. *Proceedings of International Conference on Wireless Networks and Mobile Communications (WINCOM),* 258–263.
3. Maksimov, M. & Shpinareva, I. (2018). Attack Detection System on Local Computer Network. *Proceedings of the International Scientific Young Scientists Conference CSYSC,* 102–105.
4. Markus, R., et al. (2019). A survey of network-based intrusion detection data sets. *Computers & security, 8(6),* 147–167.
5. Liu, Y., & Lee, S. (2019). Comparison of Traditional and Modular Neural Networks for Intrusion Detection. *Journal of Cyber Security, 15(2),* 200–212.
6. Pereira, M., & Stewart, S. (2021). Network Interaction in Cloud Protocols. *Cloud Infrastructure Journal, 13(4),* 200–215.

7. Kostiuk, Y., Skladannyi, P., Korshun, N., Bebeshko, B., & Khorolska, K. (2024). Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network. *Information Technology, 4(6),* 14–33.
8. Zhang, M., Xu, B., Bai, S., Lu, S. & Lin, Z. (2017). A deep learning method to detect web attacks using a specially designed CNN. *Proceedings of 24th International Conference on Neural Information Processing,* 828–836.
9. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H. & Korshun, N. (2025). Models and algorithms for analyzing information risks during the security audit of personal data information system. *Cyber Hygiene & Conflict Management in Global Information Networks, 3925*, 155–171.
10. Wang, W., Zhu, M., Zeng, X., Ye, X. & Sheng, Y. (2017). Malware traffic classification using convolutional neural network for representation learning. *Proceedings of International Conference on Information Networking*. https://doi.org/10.1109/ ICOIN.2017.7899588
11. Liu, H. Y., Xiangdong, C. & Lakkaraju, S. (2017). Understanding modern intrusion detection systems. *College of Technology, Eastern Michigan University,* 1–3.
12. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. *Cyber Hygiene & Conflict Management in Global Information Networks, 3925,* 249–264.
13. Harsh, P. & Purvi P. (2018). Study and Analysis of Decision Tree Based Classification Algorithms. *International Journal of Computer Sciences and Engineering, 6(10),* 74–78.
14. Panigrahi, R. (2018). A detailed analysis of dataset for designing Intrusion Detection Systems. *IJET, 7(24),* 479–482.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Pavlo Skladannyi
PhD, Associate Professor, Head of the Department of Information and
Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Yuliia Kostiuk
PhD in Computer Science,
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Rzaeva Svitlana
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7589-2045
s.rzaieva@kubg.edu.ua

Yuliia Samoilenko
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department Automation and Computer
Technologies of Control Systems named after Professor Anatoliy Ladanyuk
National University of Food Technologies, Kyiv, Ukraine
ORCID ID: 0000-0003-3787-1435
samoilenkouo@nuft.edu.ua

Tetiana Savchenko
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Informatics
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine
ORCID ID: 0000-0002-8884-5360
sv_t@ukr.net

DEVELOPMENT OF MODULAR NEURAL NETWORKS FOR DETECTING DIFFERENT CLASSES OF NETWORK ATTACKS

Abstract. The article discusses the development of modular neural networks for detecting different classes of network attacks, which is an important step towards improving intrusion detection systems. Modern attack detection systems face numerous limitations, including low efficiency when analyzing large volumes of data, high training time requirements, and challenges in adapting to new types of threats. These shortcomings are due to the use of monolithic approaches, where all network interaction parameters are processed within a single neural network, significantly reducing the system's flexibility and effectiveness. The modular approach proposed in the article involves using separate neural networks to process groups of similar network interaction parameters, which increases attack detection efficiency, reduces model training time, and enables dynamic disabling or retraining of individual modules without stopping the entire system. This architecture allows for more effective attack classification and enhances the system's ability to adapt to new threats. The article also thoroughly analyzes the advantages of the modular approach compared to traditional monolithic systems, providing significantly greater flexibility and accuracy in detecting and classifying various types of attacks.

Keywords: cybersecurity; cyber threat; modular neural networks; cyberattack; network attacks; traffic analysis; machine learning; threat classification; gradient descent; intrusion detection system.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Shpinareva, I. M., Yakushina, A. A., Voloshchuk, L. A., & Rudnichenko, N. D. (2021). Detection and classification of network attacks using the deep neural network cascade. *Herald of Modern Information Technologies, 4(3),* 244–254.
2. Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R. & Ghogho, M. (2016). Deep learning approach for network intrusion detection in software defined networking. *Proceedings of International Conference on Wireless Networks and Mobile Communications (WINCOM),* 258–263.
3. Maksimov, M. & Shpinareva, I. (2018). Attack Detection System on Local Computer Network. *Proceedings of the International Scientific Young Scientists Conference CSYSC,* 102–105.
4. Markus, R., et al. (2019). A survey of network-based intrusion detection data sets. *Computers & security, 8(6),* 147–167.
5. Liu, Y., & Lee, S. (2019). Comparison of Traditional and Modular Neural Networks for Intrusion Detection. *Journal of Cyber Security, 15(2),* 200–212.
6. Pereira, M., & Stewart, S. (2021). Network Interaction in Cloud Protocols. *Cloud Infrastructure Journal, 13(4),* 200–215.
7. Kostiuk, Y., Skladannyi, P., Korshun, N., Bebeshko, B., & Khorolska, K. (2024). Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network. *Information Technology, 4(6),* 14–33.
8. Zhang, M., Xu, B., Bai, S., Lu, S. & Lin, Z. (2017). A deep learning method to detect web attacks using a specially designed CNN. *Proceedings of 24th International Conference on Neural Information Processing,* 828–836.
9. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H. & Korshun, N. (2025). Models and algorithms for analyzing information risks during the security audit of personal data information system. *Cyber Hygiene & Conflict Management in Global Information Networks, 3925,* 155–171.
10. Wang, W., Zhu, M., Zeng, X., Ye, X. & Sheng, Y. (2017). Malware traffic classification using convolutional neural network for representation learning. *Proceedings of International Conference on Information Networking*. https://doi.org/10.1109/ ICOIN.2017.7899588
11. Liu, H. Y., Xiangdong, C. & Lakkaraju, S. (2017). Understanding modern intrusion detection systems. *College of Technology, Eastern Michigan University,* 1–3.
12. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. *Cyber Hygiene & Conflict Management in Global Information Networks, 3925,* 249–264.
13. Harsh, P. & Purvi P. (2018). Study and Analysis of Decision Tree Based Classification Algorithms. *International Journal of Computer Sciences and Engineering, 6(10),* 74–78.
14. Panigrahi, R. (2018). A detailed analysis of dataset for designing Intrusion Detection Systems. *IJET, 7(24),* 479–482.