УДК 004.032.26:004.056

СТРУКТУРА НЕЙРОННОЇ МЕРЕЖІ ДЛЯ ПОПЕРЕДЖЕННЯ ТА ВИЯВЛЕННЯ КІБЕРАТАК ТИПУ *USER TO ROOT* ТА *REMOTE TO LOCAL* НА ПІДПРИЄМСТВА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

А. І. Юкальчук, Л. В. Загоруйко

Анотація. У роботі досліджується структура нейронної мережі для попередження і виявлення кібератак типу *UsertoRoot (U2R)* та *RemotetoLocal (R2L)* на підприємства критичної інфраструктури, а також її реалізація мовою програмування *Python*.

Ключові слова: нейронна мережа, кібератака, U2R, R2L, KDD99.

Вступ. Сьогодні комп'ютерні мережі відіграють важливу роль у повсякденному житті людини, адже вони використовуються майже у всіх сферах її діяльності. Яке б не було підприємство – комерційне, державне, муніципальне чи бюджетне, – але у всіх випадках його функціонування так чи інакше забезпечується комп'ютерною мережею. Тож зрозуміло, що забезпечення безпеки є необхідним, оскільки наслідки недостатньої захищеності найрізноманітніші – крадіжка, знищення або поширення конфіденційної інформації (комерційної таємниці), персональних даних, підміна інформації, блокування доступу до неї, обмеження функціональності або повна зупинка діяльності комп'ютерної мережі. А останнє навіть призводить до фактичної зупинки бізнес-процесів, що може завдати великих збитків. Одним зі способів вирішення такої проблеми є побудова інтелектуальних систем виявлення вторгнень. Але їх результативність можлива лише за наявності ефективного набору даних.

У цих умовах особливо важливими є питання оцінки ефективності систем безпеки значущих об'єктів критичної інфраструктури. Тому під час проєктування системи безпеки значущого об'єкта критичної інфраструктури з метою тестування рекомендовано її макетування або створення тестового середовища з використанням засобів та методів моделювання виявлення кібервторгнень різних класів та типів.

Аналіз сучасних моделей нейронних мереж для попередження та виявлення кібератак

У літературі існує низка робіт, пов'язаних із виявленням вторгнень [1–6]. Деякі з цих робіт стосуються загальної класифікації пакетів на нормальні або атакуючі категорії, водночас інші стосуються виявлення конкретних категорій атак, як-от атаки типу *RemotetoLocalUser* та *UsertoRoot*.

Kuang та ін. запропонували новий підхід, заснований на опорних векторах *(SVM)*, який поєднує аналіз головних компонент ядра *(KPCA)* та генетичний алгоритм *(GA)* для виявлення вторгнень [1]. Модель реалізує багатошаровий *SVM*-класифікатор для прогнозування того, чи є дія атакою. В експериментах запропонований *SVM*-класифікатор досягає кращої точності та продуктивності під час виявлення вторгнень.

У роботі M. H. Kamarudin, C. Maple, T. Watson та H. Sofian була проведена розробка і аналіз алгоритму для виявлення атак на мережевий трафік із використанням пакетних заголовків [2]. Автори використали LbAD-модель, яка виявилася дуже перспективною для використання в системах виявлення аномалій. Ця модель використовує статистичний аналіз значень полів пакетних заголовків на трьох рівнях OSI: 7 шарів (рівень з'єднання даних, мережевий рівень, транспортний рівень). Був використаний алгоритм бінарної логістичної регресії для виявлення кореляції між різними шарами пакетних заголовків. Це допомогло виявити, які саме шари є найбільш важливими для виявлення двох типів атак – R2L та U2R. Виявлено, що для атак типу R2L найбільш важливими є шари 3 та 4, тоді як для атак типу U2R – шари 2 та 4. Це дало змогу авторам розробити модель, яка враховує лише найбільш важливі шари, що скорочує час обробки. Проведені експерименти показали високу ефективність запропонованого підходу. Виявлено, що модель досягла дуже високого рівня виявлення обох типів атак: 84 % для R2L та 93,5 % для U2R. Порівняно з наявними алгоритмами, цей підхід показав значні покращення виявлення атак.

У статті Kumar і Yadav запропоновано систему виявлення вторгнень на основі штучної нейронної мережі, яка використовує для навчання алгоритм градієнтного спуску з імпульсним поширенням [3]. Хоча для навчання обрано випадкові патерни, запропонована нейронна мережа протестована на повному «випробувальному» наборі даних KDD cup 99. Результати показують, що точність запропонованої IDS на основі нейронної мережі для бінарної класифікації (атака або нормальний стан) є високою, а рівень виявлення атак зондування, R2L та U2R є високим, порівняно з іншими методами.

У статті M. S. Elsayed надається детальний і систематичний аналіз наявних підходів машинного навчання (ML), які можуть протистояти більшості цих атак. До того ж пропонується фреймворк на основі глибокого навчання (DL) з використанням автокодувальника довгострокової короткочасної пам'яті (LSTM), який може точно виявляти зловмисний трафік у мережевому трафіку. Проведено експерименти в загальнодоступному наборі даних систем виявлення вторгнень (IDS). Отримується значне покращення у виявленні атак, порівняно з іншими методами порівняльного аналізу [4].

У статті Y. F. Sallam представлено модель IDS на основі глибокого навчання (DL) з гіпотезою згорткової нейронної мережі (CNN). Модель було оцінено на наборі даних NSLKDD. Він був навчений Kddtrain+ і перевірений двічі, один раз за допомогою kddtrain+, а другий – за допомогою kddtest+. Досягнута точність тесту становить 99,7 % і 98,43 % з частотою помилкових сповіщень 0,002 і 0,02 для двох сценаріїв тестування відповідно [5].

У роботі U. Shrivastavaand N. Sharma пропонується модель із двох рівнів для підвищення рівня виявлення атак меншості. Вибір функцій для незначних атак виконується за допомогою статистичного аналізу, а штучна нейронна мережа з декількома класифікаторами навчається з окремим набором даних, щоб покращити швидкість виявлення атак меншості. Для виявлення незначних атак зафіксовано точність 99,34 % [6].

Вибір структури нейронної мережі

Під час вибору структури нейронної мережі перевагу отримав клас нейронних мереж, як-от багатошарові мережі прямого поширення, які зазвичай називають багатошаровими персептронами і які є окремим випадком персептрона Розенблата.

Нейронні мережі прямого поширення мають вхідний сигнал, який передається від прошарку до прошарку (від одних нейронів до інших). Саме такою мережею і є багатошаровий персептрон, який складається зі вхідного прошарку, прихованих обчислювальних прошарків всередині системи і вихідного прошарку нейронів. Багатошаровий персептрон – це односпрямована мережа сигмоїдального типу [7].

Багатошарові персептрони часто застосовуються для контрольованих завдань навчання: вони навчаються на безлічі пар вхідних та вихідних даних і моделюють кореляцію (або залежності) між цими входами і виходами. Навчання включає в себе налаштування параметрів або ваг і зсувів моделі з метою мінімізації помилок.

У нашому випадку вхідний прошарок складається з 41 нейрона(параметри мережевого з'єднання), трьох прихованих прошарків з експериментально підібраною кількістю нейронів та трьох вихідних прошарків, які виявляють факт атаки типів*U2R,L2R* або нормальне мережеве з'єднання.

Запропонована структура являє собою нейронну мережу з трьома прихованими прошарками та функцією активації *ReLU (RectifiedLinearUnit)* – функція активації, яка широко використовується в нейронних мережах. Для будь-якого вхідного значення *x,* якщо воно менше або дорівнює нулю, вихід буде нульовим. Якщо ж вхід більше нуля, вихід буде рівний вхідному значенню на кожному з них, а також вихідним прошарком з активацією *Sigmoid*.

Розглянемо детальний опис структури нейромережі.

1. *Вхідний прошарок.* Вхідний прошарок має розмірність *dataset_inputs,* що визначається кількістю функцій (ознак) у вхідних даних. У цьому випадку використовуються дані *train_X* та *test_X*.

2. *Прихований прошарок № 1.* Перший прихований прошарок має 46 нейронів. Активація цього прошарку виконується за допомогою функції активації *ReLU*.

3. *Прихований прошарок № 2.* Другий прихований прошарок має 32 нейрони. Активація також виконується за допомогою *ReLU*.

4. *Прихований прошарок № 3.* Третій прихований прошарок має 12 нейронів, активація – *ReLU*.

5. *Вихідний прошарок.* Вихідний прошарок має розмірність *dataset_outputs*, який визначається кількістю класів (або кількістю вихідних значень). У цьому випадку використовується активація *Sigmoid*, яка призначена для задач класифікації бінарних даних.

Запропонована структура нейромережі навчається за допомогою оптимізатора *Adam* з коефіцієнтом навчання *lr*=0.00456789. Для оцінки втрат використовується середньоквадратична помилка *(MSE)*. Навчання проводиться протягом 500 циклів з пакетами розміру *batch_size*=300. На кожному циклі вимірюється середньоквадратична помилка на тестовому наборі. Якщо поточне значення *MSE* на тесті є кращим, ніж попереднє краще значення *MSE*, то модель оновлюється. У цьому випадку краща модель зберігається.

Вибір мови програмування

Для розробки програмного забезпечення використовувалась мова програмування *Python3*.

Python – об'єктно-орієнтована мова програмування, яка набула надзвичайної популярності у сфері машинного навчання та штучного інтелекту завдяки великій системі бібліотек і фреймворків та можливості легкої інтеграції між наявними компонентами. Перевагами *Python* перед іншими мовами програмування для роботи зі штучними інтелектом і, зокрема, нейронними мережами можна вважати:

- широкий вибір бібліотек та фреймворків;
- кросплатформеність;
- адаптивність та гнучкість у стилях використання;
- простий та зрозумілий синтаксис;
- вбудовані засоби візуалізації даних.

Використання датасетуKDD99 для проведення експериментальних досліджень розробленого програмного забезпечення виявлення атак типів U2R та R2L

Для навчання нейронної мережі використовувалась база даних атак *KDD99*, яка містить стандартний набір даних, який включає в себе широкий спектр вторгнень. Загалом така база містить приблизно 5 000 000 записів про мережеві з'єднання. Кожен запис являє собою образ мережевого з'єднання та включає 41 параметр мережевого трафіка (табл. 1) і позначається як «атака» або «не атака» [8].

Таблиця 1

Частина параметрів мережевого трафіка

№ з/п	Параметр	Опис
1	duration	Тривалість (у секундах) з'єднання
2	protocol_type	Тип протоколу (TCP, UDP, etc.)
3	service	Атакований сервіс
4	src_bytes	Кількість байтів від джерела до призначення
5	dst_bytes	Кількість байтів відповіді клієнту
6	flag	Прапорці з'єднання
7	land	1, якщо з'єднання від/до того самого хоста /порта
8	wrong_fragment	Кількість «хибних» фрагментів
9	urgent	Кількість термінових пакетів
10	hot	Кількість «гарячих» індикаторів
11	num_failed_logins	Кількість невдалих спроб реєстрації
12	logged_in	1, якщо успішний вхід в систему; 0 – якщо неуспішний
13	num_compromised	Кількість «компроментуючих» умов
14	root_shell	1, якщо rootshell отриманий; інакше 0
15	su_attempted	1, якщо виконувалась «suroot»; інакше 0
16	num_root	Кількість «root»-доступів
17	num_file_creations	Кількість операцій створення файлів

У базі представлені 22 типи атак. Атаки поділяються на 4 основні категорії: *DoS, U2R, R2L* і *Probe*. Серед цих атак найбільш цікавими для розробки програмного забезпечення стали атаки типу *U2R* і *R2L*.

U2R-атаки передбачають отримання зареєстрованим користувачем привілеїв локального суперкористувача (мережевого адміністратора). Виділяють чотири типи *U2R*-атак: *buffer_overflow, loadmodule, perl, rootkit.*

R2L-атаки характеризуються отриманням доступу незареєстрованого користувача до комп'ютера з боку віддаленого комп'ютера. Виділяють вісім типів *R2L*-атак: *ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster.*

Зовнішній вигляд бази *KDD99* – текстовий файл, у якому у вигляді матриць представлено набір параметрів певного типу атаки або нормального з'єднання (рис. 1).

```
0,tcp,http,SF,181,5450,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,8,8,0.00,0.00,0.00,0.00,1.00,0.00,0.00,9,9,1
.00,0.00,0.11,0.00,0.00,0.00,0.00,0.00,normal.
0,tcp,ftp,SF,36,197,0,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,1,0.
00,0.05,0.00,0.00,0.39,0.00,0.05,0.00,warezmaster.
```

Рис. 1. Зовнішній вигляд бази KDD99

Результати експериментальних досліджень

Побудована нейронна мережа була навчена з отриманою найкращою середньоквадратичною помилкою *MSE*=0.003573242574930191 (рис. 2, 3).

Середньоквадратична помилка *(MSE)* обчислюється як квадрат відхилення між прогнозованими значеннями моделі та реальними значеннями цільової змінної, і потім осереднюється за всіма прикладами в тестовому наборі даних.

```
Epoch 499: 100%|██████████| 500/500 [00:36<00:00, 14.12it/s, Best MSE=0.003573242574930191]
Out[3]: <All keys matched successfully>
```

Рис. 2. Скриншот результату навчання

У роботі була застосована функція, яка обраховує статистику на тестовому наборі даних. Функція виконує проходження через кожну точку тестового набору, обчислює різницю між фактичними та передбаченими значеннями і виводить статистичні результати у вигляді списку.

Статистика розподілу результатів виконання програми на тестовому наборі даних така:

– Загальна кількість даних (записів про нормальні мережеві з'єднання та атаки у датасеті): 11 178;

– Кількість даних у тренувальному наборі: 8 383;

– Кількість даних у тестовому наборі: 2 795;

– Кількість даних, в яких нейромережа впевнена у правильності передбачень *(confident):* 2 778;

– Кількість сумнівних даних *(doubtful):* 2;

– Кількість неправильно передбачених даних *(wrong):* 15.

```
MSE: 0.010719727963306619
RMSE: 0.10353611912422939
total: 11178, train: 8383, test: 2795, confident: 2778, doubtful: 2, wrong: 15
```

Рис. 3. Скриншот статистичних результатів

На рис. 4 представлені результати перевірки навчання запропонованої структури мережі.

```
Кількість виявлених атак кожного типу та нормальних даних:
normal    10062
r2l        1093
u2r          23
Name: count, dtype: int64
```

Рис. 4. Результат перевірки навчання запропонованої структури мережі

Із результатів перевірки роботи запропонованої структури нейронної мережі видно, що з 1 126 атак типу *R2L*модель виявляє 1 093, а з 52 атак типу *U2R*виявляє 23. На рис. 5 представлено діаграму виявлених атак обох типів.

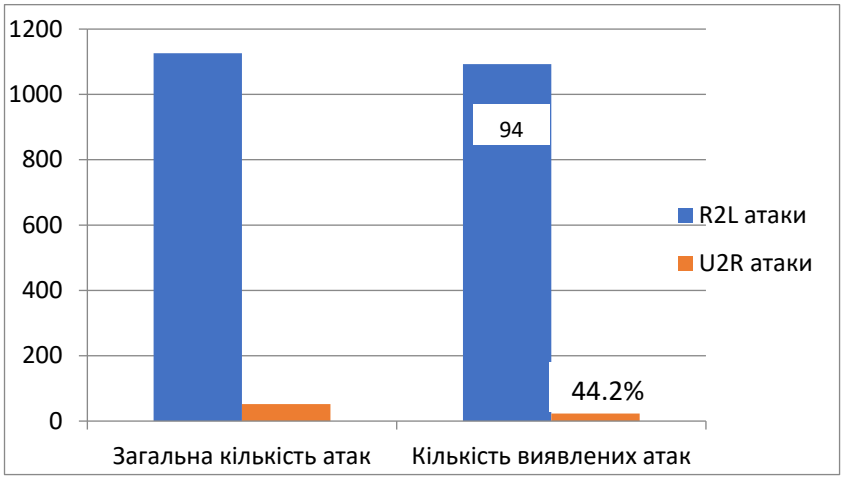

Рис. 5. Діаграма виявлених кібератак

Abstract. The paper investigates the structure of a neural network for predicting and detecting User to Root (U2R) and Remote to Local (R2L) cyberattacks on a critical infrastructure enterprise, as well as its implementation based on Python software.

Keywords: neural network, cyber attack, U2R, R2L, KDD99, multilayer perceptron, neural network learning.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kuang F., Xu W., Zhang S. A novel hybrid KPCA and SVM with GA model for intrusion detection. *Applied Soft Computing.* 2014. Vol. 18. P. 178–184.

2. Packet Header Intrusion Detection with Binary Logistic Regression Approach in Detecting R2L and U2R Attacks / M. H. Kamarudin, C. Maple, T. Watson, H. Sofian. *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)* (Jakarta, Indonesia, 2015). P. 101–106. DOI: 10.1109/CyberSec.2015.28.

3. Kumar S., Yadav A. Increasing performance Of intrusion detection system using neural network. *2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies* (Ramanathapuram, India, 2014). P. 546–550. DOI: 10.1109/ICACCCT.2014.7019145.

4. Detecting Abnormal Traffic in Large-Scale Networks / M. S. Elsayed, N.-A. Le-Khac, S. Dev, A. D. Jurcut. *2020 International Symposium on Networks, Computers and Communications (ISNCC)* (Montreal, QC, Canada, 2020). P. 1–7. DOI: 10.1109/ISNCC49221.2020.9297358.

5. Implementation of Network Attack Detection using Convolutional Neural Network / Y. F. Sallam, H. E.-d. H. Ahmed, A. Saleeb, N. A. El-Bahnasawy, F. E. A. El-Samie. *2021 International Conference on Electronic Engineering (ICEEM)* (Menouf, Egypt, 2021). P. 1–6. DOI: 10.1109/ICEEM52022.2021.9480645.

6. Shrivastava U., Sharma N. Artificial Neural Network based Dual Layered Predictive Model for Rare Attack Detection. *2020 International Conference on Computational Performance Evaluation (ComPE)* (Shillong, India, 2020). P. 146–152. DOI: 10.1109/ComPE49325.2020.9200134.

7. Swingler K. Lecture 4: Multi-Layer Perceptrons. URL: http://www.cs.stir.ac.uk/courses/ITNP4B/lectures/kms/4-MLP.pdf

8. KDD Cup 1999 Data. URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

УДК 004:005:51

МЕТОД ДИХОТОМІЇ ПРИ ЗНАХОДЖЕННІ КОРЕНІВ АПРОКСИМОВАНОЇ ФУНКЦІЇ ПРИЧИННО-НАСЛІДКОВОГО ЗВ'ЯЗКУ МЕТРИК ІНВЕСТИЦІЙНИХ ПРОЦЕСІВ У ВИРОБНИЦТВІ ЕЛЕКТРОННОЇ ПРОДУКЦІЇ

Б. М. Ярошенко, Н. А. Потапова

Анотація. Стаття присвячена дослідженню використання методу дихотомії для знаходження коренів апроксимованої функції, що описує зв'язок між доданою вартістю суб'єктів господарювання України та капітальними інвестиціями у виробництво комп'ютерів, електронної та оптичної продукції. На основі статистичних даних за 2014–2023 рр. проведено апроксимацію залежності. Для знаходження кореня використано метод дихотомії, що дало змогу ітераційним способом уточнити значення точки переходу. Побудовано графічну інтерпретацію отриманих результатів та проведено оцінку похибки. За результатами дослідження підтверджено ефективність застосування методу дихотомії для аналізу подібних залежностей.

Ключові слова: методи обчислень, метод дихотомії, апроксимація, корінь рівняння, похибка.