DOI: 10.59647/978-617-520-936-3/1

Застосування глибоких нейронних мереж для вдосконалення систем виявлення загроз

Сергій Долгополов, асистент кафедри інформаційних технологій [1] (ORCID: 0000-0001-9418-0943), **Лі Тао,** аспірант кафедри IT[1] (ORCID: 0000-0001-8104-5208)

[1] *Київський національний університет будівництва і архітектури, 03037, м. Київ, проспект Повітряних Сил, 31, Україна*

АНОТАЦІЯ

Це дослідження представляє комплексне вивчення розробки ефективної системи виявлення загроз на основі нейронних мереж, спрямованої на ідентифікацію та запобігання витоку даних. Використовуючи різноманітні методи машинного навчання, включаючи K найближчих сусідів, логістичну регресію, дерева рішень, випадковий ліс та різні моделі градієнтного підсилення, ця наукова робота заглиблюється в оптимізацію заходів кібербезпеки через передові аналітичні та моделюючі техніки. Центральним у нашому підході є розгортання глибокої багатошарової перцептронної нейронної мережі, розробленої для точного виявлення широкого спектру кіберзагроз, які потенційно можуть призвести до витоку даних. Методологія дослідження охоплює аналіз та синтез, систематизацію, класифікацію та детальний порівняльний аналіз для оцінки ефективності кожної моделі. Результатом цього дослідження є складне програмне рішення, здатне не лише виявляти складні патерни загроз, але й дозволяти експорт результатів у форматі CSV для подальшого вивчення.

Ключові слова: системи виявлення вторгнень, нейронні мережі, глибоке навчання, машинне навчання, витік даних.

1. ВСТУП

У сучасному цифровому ландшафті інформація постає як першорядний актив у різних сферах, включаючи державне управління, корпоративні сектори та особисту конфіденційність. Експоненціальне зростання генерації та обміну даними підкреслює нагальну потребу в передових механізмах безпеки для запобігання несанкціонованому доступу та витоку даних.

Традиційні заходи кібербезпеки часто не відповідають складності та динамічності сучасних кіберзагроз, стимулюючи дослідження інноваційних рішень. Системи виявлення загроз на основі нейронних мереж є одним з найпріоритетніших напрямів дослідження у галузі кібербезпеки, відкриваючи нові перспективи для захисту інформації від витоків.

Мотивація проведення цього дослідження випливає зі зростаючої кількості випадків витоку даних, які не лише компрометують конфіденційність, але й тягнуть за собою значні фінансові та репутаційні збитки. Звіт IBM Security 2023 [1] підкреслює зростаючі витрати, пов'язані з витоками даних, наголошуючи на необхідності більш ефективних рішень у сфері кібербезпеки.

2. МЕТА РОБОТИ

Метою цього дослідження є розробка та оцінка ефективної системи виявлення загроз на основі нейронних мереж для захисту від витоку даних. Дослідження спрямоване на аналіз та порівняння різних методів машинного навчання для виявлення аномалій у мережевому трафіку. Важливим аспектом є розробка глибокої багатошарової перцептронної нейронної мережі для точного виявлення широкого спектру кіберзагроз. Робота також передбачає оцінку ефективності розробленої системи за допомогою набору даних NSL-KDD та порівняння її з іншими класичними методами машинного навчання.

3. ОСНОВНА ЧАСТИНА

У дослідженні використовується набір даних NSL-KDD, який містить дані про мережевий трафік, включаючи нормальну активність та різні типи атак. Цей набір даних є вдосконаленою версією оригінального набору даних KDD-99, що вирішив проблеми незбалансованості класів та надмірності записів [2].

Рисунок 1 показує співвідношення нормальних та аномальних даних, які використовуються для навчання та тестування нейронної мережі та інших класифікаторів. Більше половини записів є нормальним трафіком, а розподіл атак типу U2R та R2L є надзвичайно низьким.

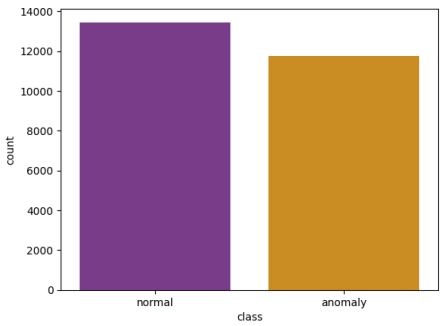

Рисунок 1. Співвідношення нормального та аномального трафіку у наборі даних

Архітектура розробленої нейронної мережі представляє собою повнозв'язну пряму нейронну мережу, як показано на Рисунку 2. Набір даних NSL-KDD містить 43 атрибути, 41 з яких характеризують особливості вхідного трафіку, а два використовуються для маркування: перший вказує, чи є трафік нормальним чи атакою, а другий оцінює серйозність та потенційну шкоду цього трафіку.

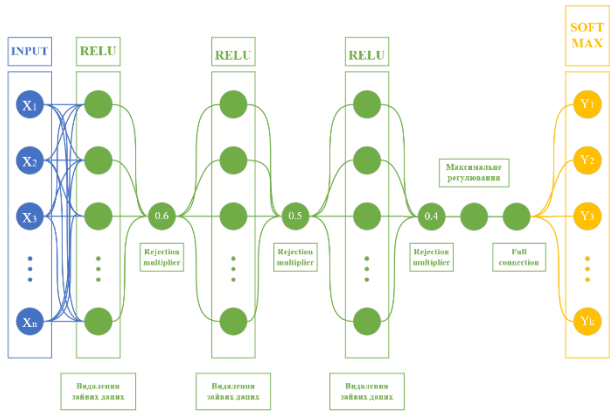

Рисунок 2. Архітектура повнозв'язної нейронної мережі прямого поширення

Типи атак у наборі даних KDD поділяються на чотири основні категорії. Перша – це відмова в обслуговуванні (DoS), яка спрямована на перевантаження системи запитами. Друга категорія – зондування (сканування), що передбачає пошук вразливостей у мережі. Третя – атаки типу «користувач до адміністратора» (U2R), коли зловмисник намагається отримати права адміністратора. Четверта категорія – «віддалений до локального» (R2L), де атакуючий намагається отримати локальний доступ до системи віддалено. Для оцінки ефективності системи виявлення вторгнень використовувались кілька критеріїв. Точність (Accuracy) вимірює співвідношення правильно класифікованих прикладів до загальної кількості прикладів у тестовому наборі даних. F1-Score комбінує точність та повноту в єдину метрику, що особливо корисно при дисбалансі класів. Матриця помилок (Confusion Matrix) надає детальну інформацію про класифікацію даних, включаючи істинно позитивні, хибно позитивні, істинно негативні та хибно негативні результати.

У дослідженні були проаналізовані та використані різні моделі машинного навчання, включаючи: K-найближчих сусідів (KNN), Логістична регресія, Дерева рішень, Випадковий ліс, Градієнтний бустинг (SKLearn, XGBoost, Light), AdaBoost, CatBoost, Наївний байєсівський класифікатор Бернуллі, Ансамблеве голосування, Метод опорних векторів (SVC), Глибока багатошарова перцептронна нейронна мережа (DMLPNN) [3–6]

Результати показали, що ансамблеві м.етоди, зокрема Light Gradient Boosting, XGBoost, Voting та RandomForest, продемонстрували високу ефективність і виявилися найбільш збалансованими з точки зору точності, повноти та F1-міри.

4. ВИСНОВКИ

Таким чином, у дослідженні було проаналізовано та використано різні моделі машинного навчання, включаючи KNN, логістичну регресію, дерева рішень, випадковий ліс, різні варіанти градієнтного підсилення, AdaBoost, CatBoost, наївний байєсівський класифікатор, ансамблеве голосування, SVC, а також розроблену глибоку нейронну мережу DMLPNN.

Ансамблеві методи, зокрема Light Gradient Boosting, XGBoost, Voting та RandomForest, продемонстрували найвищу ефективність та збалансованість щодо точності, повноти та F1-міри. Light Gradient Boosting показав особливо вражаючі результати з точністю та повнотою 0,997 та F1-мірою 0,997, що свідчить про його здатність ефективно розрізняти класи та уникати помилок обох типів.

Розроблена глибока нейронна мережа (DMLPNN) також показала високу ефективність з точністю 0,987, повнотою 0,985 та F1-мірою 0,986, що підкреслює потенціал глибокого навчання у вирішенні складних задач класифікації в галузі кібербезпеки.

Наукова новизна цього дослідження полягає в розробці ефективної системи виявлення загроз на основі нейронних мереж, яка використовує різноманітні методи машинного навчання для оптимізації заходів кібербезпеки. Практичне значення роботи демонструється створенням складного програмного рішення, здатного не лише виявляти складні патерни загроз, але й полегшувати експорт результатів для подальшого аналізу.

Результати дослідження мають важливе значення для подальшого розвитку систем кібербезпеки, демонструючи, що використання передових методів машинного навчання може значно підвищити ефективність виявлення та запобігання кіберзагрозам.

Майбутні дослідження можуть бути спрямовані на подальше вдосконалення архітектури нейронних мереж, розробку гібридних моделей, а також на адаптацію систем до виявлення нових типів атак. Важливим напрямком є також розробка методів, які дозволять системам працювати в режимі реального часу.

Список літератури

[1] "Cost of a Data Breach Report 2023," IBM Security. 2023. URL: https://www.ibm.com/downloads/cas/E3G5JMBP.

[2] S. Sonawane, "Rule Based Learning Intrusion Detection System Using KDD and NSL KDD Dataset," Prestige International Journal of Management & IT-Sanchayan, 4(2), pp. 135–145, 2015, DOI: https://cutt.ly/VwODmoea.

[3] S. Dolhopolov, T. Honcharenko, S. Dolhopolova, O. Riabchun and M. Delembovskyi, "Use of Artificial Intelligence Systems for Determining the Career Guidance of Future University Student," Proceeding of the SIST 2022, 2022 International Conference on Smart Information Systems and Technologies, Nur-Sultan Kazakhstan, 28-30 April 2022, DOI: https://doi.org/10.1109/SIST54437.2022.9945752.

[4] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. A. Khan, "Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review," Procedia Computer Science, 171, pp. 1251–1260, 2020. DOI: https://doi.org/10.1016/j.procs.2020.04.133.

[5] M. H. Al-Mashagbeh, W. Salameh, A. Alamareen, and S. A. Asal, "Intrusion Detection System Employing Neural Network MLP and Detection Trees Using Different Techniques," International Journal of Statistics Applications & Probability, 13(1), pp. 169–180, 2024. DOI: https://doi.org/10.18576/jsap%2F130112.

[6] C. Tian, F. Zhang, Z. Li, R. Wang, X. Huang, L. Xi, and Y. Zhang, "Intrusion Detection Method Based on Deep Learning," Wireless Communications and Mobile Computing 2022, pp. 1–8, 2022. URL: https://cutt.ly/ywODhmCs.