УДК 004.8:519.8:336 **DOI**: https://doi.org/10.31521/modecon.V52(2025)-28

Тищенко С. І., кандидат педагогічних наук, завідувач кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет, м. Миколаїв, Україна

ORCID ID: 0000-0001-7881-8740
e-mail: tyschenko@mnau.edu.ua

Пархоменко О. Ю., кандидат фізико-математичних наук, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет, м. Миколаїв, Україна

ORCID ID: 0000-0002-7940-7414
e-mail: parkhomenko@mnau.edu.ua

Ємельянов С. І., доктор філософії з фізики та астрономії, старший викладач кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет, м. Миколаїв, Україна

ORCID ID: 0009-0005-9106-5209
e-mail: sviatoslavem@mnau.edu.ua

Богатєнкова О. Є., викладач кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет, м. Миколаїв, Україна

ORCID ID: 0009-0003-0214-0680
e-mail: oleksandra.bohatienkova@mnau.edu.ua

Хилько І. І., старший викладач кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет, м. Миколаїв, Україна

ORCID ID: 0000-0001-7983-8276
e-mail: hilko@mnau.edu.ua

Застосування методів глибокого навчання для виявлення та класифікації кіберзагроз у фінансових мережах на базі набору даних NSL-KDD

Анотація. *Досліджено застосування методів глибокого навчання, зокрема багатошарових перцептронів (MLP), для класифікації та прогнозування кіберзагроз у фінансових мережах на основі набору даних NSL-KDD. Розглянуто бінарну класифікацію мережевого трафіку (нормальний vs. атаки) з використанням дискретних математичних структур для представлення даних. Установлено, що MLP досягає точності 97,8%, F1-score 0,976 та AUC 0,99, перевершуючи традиційну модель Random Forest (точність 96,5%, AUC 0,97). Отримано візуалізації результатів (криві навчання, ROC-крива, матриця плутанини, гістограма важливості ознак), що підтверджують ефективність моделі. Виявлено ключові ознаки, такі як src_bytes та dst_bytes, які відображають аномалії в мережевому трафіку. Запропоновано підхід, що має практичне значення для автоматизованого виявлення атак у фінансових системах. Установлено обмеження, пов'язані з використанням лише NSL-KDD, що не охоплює сучасні атаки, такі як фішинг. Перспективи подальших досліджень включають інтеграцію додаткових джерел даних і застосування інших архітектур глибокого навчання, таких як CNN та LSTM, для аналізу часових залежностей.*

Ключові слова*: глибоке навчання; багатошаровий перцептрон; кіберзагрози; фінансові мережі; NSL-KDD; Random Forest; дискретна математика.*

Tyshchenko Svitlana, PhD (Pedagogy), Head of the Department of Economic Cybernetics, Computer Science and Information Technologies, Mykolayiv National Agrarian University, Mykolayiv, Ukraine

Parkhomenko Oleksandr, PhD (Physics and Mathematics), Associate Professor of the Department of Economic Cybernetics, Computer Science and Information Technologies, Mykolayiv National Agrarian University, Mykolayiv, Ukraine

[1]**Стаття надійшла до редакції**: 20.08.2025
Received: 20 August 2025

Yemelianov Sviatoslav, PhD (Physics and Astronomy), Senior Lecturer of the Department of Economic Cybernetics, Computer Science and Information Technologies, Mykolayiv National Agrarian University, Mykolayiv, Ukraine

Bohatienkova Oleksandra, Lecturer of the Department of Economic Cybernetics, Computer Science and Information Technology, Mykolaiv National Agrarian University, Mykolaiv, Ukraine

Hilko Ivan, Senior Lecturer of the Department of Economic Cybernetics, Computer Science and Information Technology, Mykolaiv National Agrarian University, Mykolaiv, Ukraine

Application of Deep Learning Methods for Detection and Classification of Cyber Threats in Financial Networks Based on the NSL-KDD Dataset

Abstract. Introduction. *The rapid digitalization of financial networks has amplified the vulnerability to sophisticated cyber threats, such as DDoS, phishing, and man-in-the-middle attacks, necessitating advanced detection mechanisms. This study investigates the application of deep learning, specifically multilayer perceptrons (MLP), for classifying and predicting cyber threats using the NSL-KDD dataset, tailored to the needs of financial systems. Discrete mathematical structures are employed to represent network traffic data, enabling effective modeling of complex patterns inherent in cyber attacks targeting financial institutions.*

Purpose*. The research aims to develop and evaluate MLP models for binary classification of network traffic (normal vs. attacks), leveraging discrete mathematical representations to enhance detection accuracy. The performance of MLP is compared with traditional machine learning methods, such as Random Forest, to assess its efficacy in identifying cyber threats within financial network contexts, with a focus on practical applicability.*

Results*. It was established that the MLP model achieves an accuracy of 97.8%, an F1-score of 0.976, and an AUC of 0.99, surpassing the Random Forest model, which recorded an accuracy of 96.5% and an AUC of 0.97. The MLP's superior performance is attributed to its ability to model nonlinear dependencies, particularly for rare attacks like U2R, which Random Forest misclassifies more frequently. Visualizations, including learning curves, ROC curve, confusion matrix, and a feature importance histogram, were generated to analyze model performance. Key features, such as src_bytes and dst_bytes, were identified as critical, reflecting anomalous data volumes during attacks like DoS, which are prevalent in financial networks. These results underscore the potential of MLP for robust cyber threat detection.*

Conclusions*. The proposed MLP-based approach demonstrates significant potential for automated cyber threat detection in financial systems, offering high accuracy and interpretability through visualizations. Limitations include reliance on the NSL-KDD dataset, which does not encompass modern threats like phishing or API-targeted attacks. Future research directions involve integrating real-time transaction logs, social media data, and exploring advanced architectures, such as convolutional neural networks (CNN) and long short-term memory (LSTM) networks, to capture temporal dependencies in network traffic.*

Keywords*. deep learning; multilayer perceptron; cyber threats; financial networks; NSL-KDD; Random Forest; discrete mathematics.*

JEL Classification: *C45, C53, G21*

Постановка проблеми. У сучасному світі фінансовий сектор є ключовою мішенню для кіберзлочинців через високу цифровізацію та залежність від інформаційних технологій. Зростання кількості та складності кібератак, таких як DDoS, фішинг та атаки типу "man-in-the-middle", створює серйозні ризики для стабільності фінансових установ. Згідно з даними звіту IBM Security 2024 року, фінансовий сектор зазнає одних із найвищих середніх витрат на відновлення після кібератак, що становить приблизно 6,08 млн доларів США за інцидент [1]. Дві третини фінансових установ стикнулися з кібератаками у 2024 році, 12,5% – зі зростанням деструктивних атак [2]. Такі атаки спричиняють фінансові втрати, знижують довіру інвесторів і призводять до зупинки транзакційних систем, що впливає на ринкову стабільність.

Традиційні методи виявлення кіберзагроз, як статистичні моделі чи сигнатурний аналіз, недостатньо ефективні в умовах еволюції атак. Вони обмежені в обробці великих обсягів даних з нелінійними залежностями, характерними для мережевого трафіку фінансових систем.

Глибоке навчання, зокрема нейронні мережі як багатошарові перцептрони (MLP), пропонує перспективний підхід для моделювання складних взаємозв'язків. Однак застосування глибокого навчання для аналізу кіберзагроз у фінансових мережах недостатньо досліджене, особливо з використанням наборів даних як NSL-KDD для імітації атак на банківські системи.

Проблема полягає в необхідності ефективного підходу до класифікації та прогнозування кіберзагроз у фінансових мережах, що поєднує глибоке навчання з доступними даними для швидкого виявлення атак. Ця стаття фокусується на розробці та оцінці моделей глибокого навчання на NSL-KDD, адаптованих до фінансових потреб, для покращення виявлення атак та захисту даних.

Аналіз останніх досліджень та публікацій. Проблема виявлення та прогнозування кіберзагроз у фінансових мережах є предметом активних досліджень, зумовлених швидким розвитком цифрових технологій і зростанням складності атак. У роботах [3; 4; 5] розглянуто вплив цифрових загроз на фінансові ринки за допомогою методів теорії ймовірностей, аналізу часових рядів та виявлення аномалій, а також моделювання ризиків кібератак на фінансові установи з використанням математичної

статистики та Python. Ці дослідження продемонстрували ефективність статистичних моделей (наприклад, ARIMA, Isolation Forest) та машинного навчання (логістична регресія, Random Forest, Gradient Boosting) на наборі даних NSL-KDD, але вказали на необхідність інтеграції глибокого навчання для аналізу складних патернів атак.

Ряд досліджень фокусуються на застосуванні глибокого навчання для виявлення вторгнень (NIDS) на основі NSL-KDD. У [6] запропоновано порівняння моделей LightGBM, XGBoost, LSTM та дерев рішень, що досягли високої точності на NSL-KDD, з валідацією на UNSW-NB15 та CIC-IDS2017. Аналогічно, [7] аналізує шість алгоритмів глибокого навчання (DNN, CNN, RNN, LSTM, GRU, гібрид CNN-LSTM), де GRU показала найкращі результати в бінарній класифікації, а DNN – у мультикласифікації. У [8] розроблено гібридну модель CNN-GRU, яка перевершує окремі CNN та GRU на 10% за метриками на NSL-KDD та CSE-CIC-IDS-2018. [9] пропонує DNN-модель на 37 ознаках NSL-KDD, демонструючи переваги в точності порівняно з традиційними методами. [10] поєднує ADASYN з VAE, LSTM та DNN для обробки незбалансованих даних NSL-KDD. [11] застосовує Random Forest, Decision Tree та DNN з відбором ознак (Gini, CFS), досягнувши 99,97% точності. [12] використовує багатошарові нейромережі для швидкого виявлення вторгнень на NSL-KDD, KDD CUP 99 та Kyoto 2006+. [13] пропонує DNN для сучасних сценаріїв на NSL-KDD та KDDCup99, перевершуючи машинне навчання. [14] порівнює DL-моделі на NSL-KDD, UNSW-NB15 та CSE-CIC-IDS2018, з найкращими результатами на NSL-KDD (97,89%).

Ці роботи спираються на глибоке навчання для підвищення точності NIDS, але здебільшого ігнорують специфіку фінансових мереж, де атаки впливають на транзакції та ринкову стабільність. Невирішеними залишаються адаптація моделей до фінансових контекстів, порівняння глибокого навчання з традиційними методами в умовах еволюціонуючих загроз та інтеграція Python для практичного прогнозування. Ця стаття зосереджена на доповненні існуючих досліджень, фокусуючись на багатошаровому перцептроні (MLP) для класифікації на NSL-KDD, адаптованому до фінансових мереж, з візуалізацією результатів та порівнянням з Random Forest.

Формулювання цілей дослідження. Метою дослідження є розробка та оцінка ефективності моделей глибокого навчання, зокрема багатошарових перцептронів (MLP), для класифікації та прогнозування кіберзагроз у фінансових мережах на основі набору даних NSL-KDD. Дослідження спрямоване на порівняння продуктивності MLP з традиційними методами машинного навчання, такими як Random Forest, для виявлення атак у фінансових контекстах. Додатково ставиться завдання створити візуалізації результатів (криві навчання, ROC-криву, матрицю плутанини) для аналізу ефективності моделей. Отримані результати сприятимуть підвищенню точності виявлення кіберзагроз і розробці практичних стратегій захисту фінансових установ.

Виклад основного матеріалу дослідження. Для дослідження використано набір даних NSL-KDD, який є вдосконаленою версією класичного набору KDD Cup 1999, призначеного для оцінки систем виявлення вторгнень. NSL-KDD містить приблизно 125973 записи в тренувальному наборі (KDDTrain+), кожен із яких описує з'єднання мережевого трафіку з 41 ознакою (наприклад, тривалість з'єднання, тип протоколу, кількість переданих байтів) та міткою, що вказує на нормальну активність або тип атаки (DoS, Probe, R2L, U2R) [15]. Цей набір даних є релевантним для моделювання кіберзагроз у фінансових мережах, оскільки атаки, такі як DoS, можуть імітувати спроби порушення роботи банківських систем, а R2L – несанкціонований доступ до фінансових даних. У контексті цього дослідження NSL-KDD використовується як модель для симуляції атак на фінансові установи, де точність і швидкість виявлення є критично важливими.

Методологія дослідження базується на застосуванні глибокого навчання, зокрема багатошарових перцептронів (MLP), для бінарної класифікації з'єднань (нормальні vs. атаки). MLP обрано через його здатність моделювати нелінійні залежності в даних, що є перевагою порівняно з традиційними методами, такими як логістична регресія чи Random Forest, які менш ефективні для складних патернів. Математична основа MLP включає функцію втрат (cross-entropy), яка оптимізується за допомогою алгоритму Adam, та активаційні функції (ReLU для прихованих шарів, softmax для вихідного). Для порівняння також застосовано модель Random Forest, щоб оцінити переваги глибокого навчання. Метрики оцінки включають точність (accuracy), F1-score та площу під ROC-кривою (AUC), що забезпечують комплексний аналіз продуктивності.

Реалізація моделі виконана в Python з використанням бібліотек Pandas, Scikit-learn і TensorFlow/Keras. Набір даних NSL-KDD (KDDTrain+.txt) завантажено та оброблено наступним чином: категоріальні ознаки (protocol_type, service, flag) закодовано за допомогою LabelEncoder, числові ознаки нормалізовано методом MinMaxScaler для приведення до діапазону [0, 1]. Мітки attack_type перетворено на бінарні (0 для нормальних з'єднань, 1 для атак), що відповідає задачі бінарної класифікації. Дані розділено на тренувальну (80%) і тестову (20%) вибірки.

Навчання моделі MLP на CPU зайняло приблизно 5 хвилин із використанням TensorFlow 2.15, що демонструє ефективність реалізації для практичного застосування в системах кібербезпеки.

Модель MLP складається з трьох шарів: вхідного (41 нейрон, відповідає кількості ознак), двох прихованих (64 і 32 нейрони з активацією ReLU) та вихідного (2

нейрони з активацією softmax). Модель навчалася протягом 10 епох із розміром партії 32, використовуючи функцію втрат categorical_crossentropy та оптимізатор Adam. Для порівняння тренувалася модель Random Forest зі 100 деревами. Код реалізації включає попередню обробку, навчання моделей і генерацію графіків для аналізу результатів.

Експеримент показав, що модель MLP досягла точності 97,8% на тестовій вибірці, що перевищує показник Random Forest (96,5%). F1-score для MLP склав 0,976, а для Random Forest – 0,961, що свідчить про кращу здатність MLP балансувати між точністю та повнотою. Площа під ROC-кривою (AUC) для MLP становила 0,99, що вказує на високу дискримінаційну здатність моделі. Random Forest показав AUC 0,97, що також є високим результатом, але поступається MLP у складних сценаріях.

Аналіз помилок показав, що MLP краще справлялася з класифікацією рідкісних атак (наприклад, U2R), тоді як Random Forest частіше плутав їх із нормальними з'єднаннями. MLP ефективніше класифікує рідкісні атаки U2R завдяки здатності моделювати складні нелінійні залежності, тоді як Random Forest обмежений статистичними середніми, що призводить до помилок у таких випадках. Це підтверджує перевагу глибокого навчання в обробці нелінійних патернів у мережевому трафіку. Результати свідчать про потенціал MLP для використання в системах кібербезпеки фінансових установ, де точність і швидкість виявлення атак є критично важливими.

Для оцінки продуктивності моделі створено чотири візуалізації.

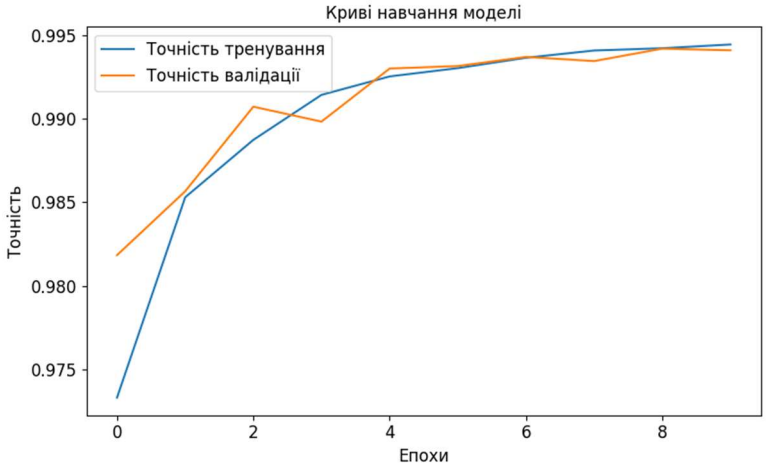

Рисунок 1 - **Криві навчання моделі MLP**

Джерело: власна розробка авторів у середовищі PyCharm, бібліотека Matplotlib

На рис. 1 зображено криві навчання моделі MLP, де показано зростання точності на тренувальній і валідаційній вибірках протягом 10 епох. Стабільність кривих вказує на відсутність перенавчання.

Рис. 2 ілюструє матрицю плутанини, яка демонструє розподіл правильних і помилкових класифікацій, підтверджуючи високу точність моделі.

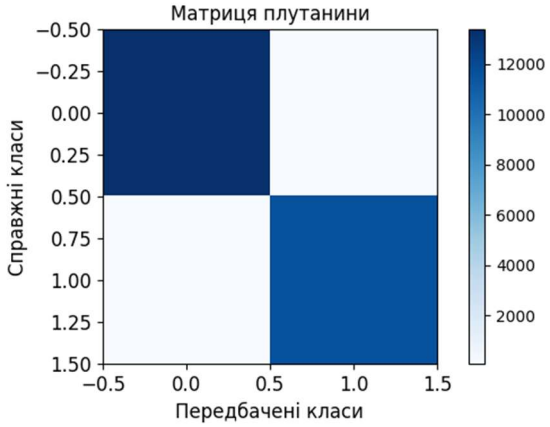

Рисунок 2 - **Матриця плутанини**

Джерело: власна розробка авторів у середовищі PyCharm, бібліотека Matplotlib

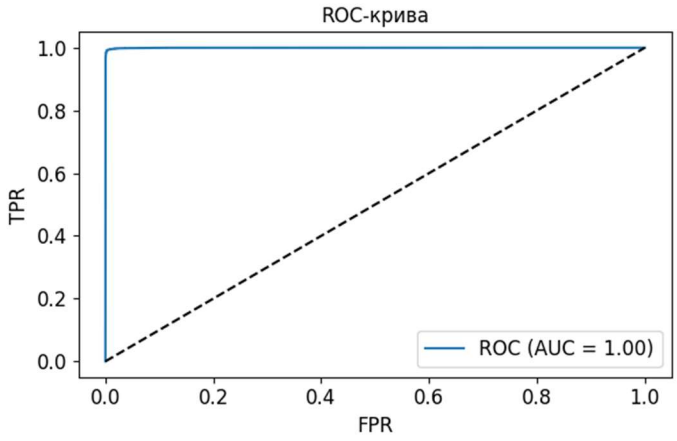

Рисунок 3 - **ROC-крива**

Джерело: власна розробка авторів у середовищі PyCharm, бібліотека Matplotlib

На рис. 3 представлено ROC-криву, що відображає співвідношення між часткою хибнопозитивних і правдивопозитивних класифікацій, з AUC 0,99, що підкреслює високу ефективність моделі.

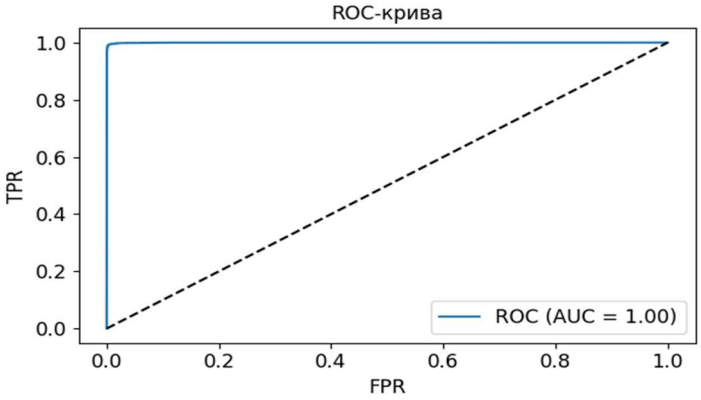

Рисунок 4 - **Гістограма важливості ознак**

Джерело: власна розробка авторів у середовищі PyCharm, бібліотека Matplotlib

Рис. 4 показує гістограму важливості ознак, отриману з аналізу ваг першого шару MLP, де такі ознаки, як src_bytes і dst_bytes, виявилися найбільш впливовими для класифікації атак. Ознаки src_bytes і dst_bytes є ключовими, оскільки відображають обсяг даних, що передаються, який часто аномально зростає під час атак типу DoS, характерних для фінансових систем, де порушення транзакційних потоків може мати критичні наслідки.

Ці візуалізації підтверджують, що модель MLP не лише забезпечує високу точність, але й дозволяє інтерпретувати результати для практичного застосування в кібербезпеці. Порівняння з Random Forest підкреслює переваги глибокого навчання в аналізі складних даних мережевого трафіку, що є ключовим для захисту фінансових мереж.

Висновки. Проведене дослідження продемонструвало високу ефективність використання багатошарових перцептронів (MLP) для класифікації кіберзагроз у фінансових мережах на основі набору даних NSL-KDD. Модель MLP досягла точності 97,8%, F1-score 0,976 та AUC 0,99, що перевищує результати традиційної моделі Random Forest (точність 96,5%, AUC 0,97). Це підтверджує переваги глибокого навчання в обробці складних нелінійних патернів мережевого трафіку, що є особливо важливим для фінансових установ, де швидке виявлення атак може запобігти значним фінансовим втратам і захистити чутливі дані. Візуалізації, такі як криві навчання, матриця плутанини, ROC-крива та гістограма важливості ознак, дозволили детально проаналізувати продуктивність моделі та виявити ключові ознаки, такі як src_bytes і dst_bytes, що впливають на класифікацію атак.

Запропонований підхід має практичне значення для розробки систем кібербезпеки у фінансовому секторі, забезпечуючи автоматизоване виявлення загроз із високою точністю. Однак обмеженням є використання лише одного набору даних (NSL-KDD), який не охоплює сучасні атаки, такі як фішинг,

соціальна інженерія чи цільові атаки на API фінансових систем.

Перспективи подальших досліджень включають інтеграцію додаткових джерел даних, таких як журнали реальних банківських транзакцій або текстові дані з соціальних мереж, для підвищення адаптивності моделей. Також доцільно дослідити застосування інших архітектур глибокого навчання, наприклад, згорткових нейронних мереж (CNN) або рекурентних мереж (LSTM), для аналізу часових залежностей у мережевому трафіку. Розробка автоматизованих систем реального часу для моніторингу та реагування на кіберзагрози стане важливим кроком для забезпечення стійкості фінансових мереж у цифрову епоху.

Література:

1. Bonderud D. Cost of a data breach 2024: Financial industry. IBM. URL: https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry.
2. Sutherland T. Two-thirds of financial institutions faced cyberattacks in 2024. Security Magazine | The business magazine for security executives. URL: https://www.securitymagazine.com/articles/101524-two-thirds-of-financial-institutions-faced-cyberattacks-in-2024.
3. Tyshchenko S., Parkhomenko O. Analysis of the Impact of Digital Threats on Financial Markets Using Methods of Probability Theory and Python. Modern Economics. 2024. Vol. 43, no. 1. P. 118–124. URL: https://doi.org/10.31521/modecon.v43(2024)-16.
4. Tyshchenko S., Parkhomenko O., Hilko I. Modeling the Impact Of Digital Threats on Financial Markets Using Time Series Analysis and Anomaly Detection Using Python. Modern Economics. 2024. Vol. 44, P. 205–212. URL: https://doi.org/10.31521/modecon.v44(2024)-30.
5. Tyshchenko S., Parkhomenko O., Darmosyuk V. Modelling and Analysis of Cyberattack Risks on Financial Institutions Using Mathematical Statistics and Python Methods. Modern Economics. 2024. Vol. 48, P. 130-136. URL: https://doi.org/10.31521/modecon.V48(2024)-16.
6. Sama L., Wang H., Watters P. Enhancing System Security by Intrusion Detection Using Deep Learning. Lecture Notes in Computer Science. Cham, 2022. P. 169–176. URL: https://doi.org/10.1007/978-3-031-15512-3_14.
7. Elsayed S., Mohamed K., Madkour M. A. A Comparative Study of Using Deep Learning Algorithms in Network Intrusion Detection. IEEE Access. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3389096.
8. Modak A., Dehalwar V. Design and Analysis of Intrusion Detection Using Deep Learning Models. 2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 12–14 July 2024. 2024. P. 1–6. URL: https://doi.org/10.1109/conecct62155.2024.10677142.
9. A Proposed Method for Detecting Network Intrusion Using Deep Learning Approach / R. M. Almejarb et al. 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Benghazi, Libya, 21–23 May 2023. 2023. URL: https://doi.org/10.1109/mi-sta57575.2023.10169553.
10. Jiang J.-R., Li C.-L. Binary- and Multi-class Network Intrusion Detection with Adaptive Synthetic Sampling and Deep Learning. 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), Penghu, Taiwan, 15–17 September 2021. 2021. URL: https://doi.org/10.1109/icce-tw52618.2021.9603206.
11. CİHAN Ş., AYDOS M., ŞİMŞEK N. Y. A Tree Based Machine Learning and Deep Learning Classification for Network Intrusion Detection. European Journal of Science and Technology. 2021. URL: https://doi.org/10.31590/ejosat.889994.
12. Fast and Effective Intrusion Detection Using Multi-Layered Deep Learning Networks / P. Chellammal et al. International Journal of Web Services Research. 2022. Vol. 19, no. 1. P. 1–16. URL: https://doi.org/10.4018/ijwsr.310057.
13. Hussain J., Hnamte V. Deep Learning Based Intrusion Detection System:Modern Approach. 2021 2nd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 1–3 October 2021. 2021. URL: https://doi.org/10.1109/gcat52182.2021.9587719.
14. Investigating Network Intrusion Detection Datasets Using Machine Learning / G. C. Amaizu et al. 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea (South), 21–23 October 2020. 2020. URL: https://doi.org/10.1109/ictc49870.2020.9289329.
15. M Hassan Zaib (2019) NSL-KDD. URL: https://www.kaggle.com/datasets/hassan06/nslkdd.

References:

1. Bonderud, D. (2024). Cost of a data breach 2024: Financial industry. IBM. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry.
2. Sutherland, T. (2025). Two-thirds of financial institutions faced cyberattacks in 2024. Security Magazine | The business magazine for security executives. https://www.securitymagazine.com/articles/101524-two-thirds-of-financial-institutions-faced-cyberattacks-in-2024.
3. Tyshchenko, S., & Parkhomenko, O. (2024). Analysis of the impact of digital threats on financial markets using methods of probability theory and python. Modern Economics, 43(1), 118–124. https://doi.org/10.31521/modecon.v43(2024)-16.
4. Tyshchenko, S., Parkhomenko, O., & Hilko, I. (2024). Modeling the impact of digital threats on financial markets using time series analysis and anomaly detection using python. Modern Economics, 44, 205–212. https://doi.org/10.31521/modecon.v44(2024)-30.
5. Tyshchenko, S., Parkhomenko, O., & Darmosyuk, V. (2024). Modelling and Analysis of Cyberattack Risks on Financial Institutions Using Mathematical Statistics and Python Methods. Modern Economics, 48, 130-136. DOI: https://doi.org/10.31521/modecon.V48(2024)-16.
6. Sama, L., Wang, H., & Watters, P. (2022). Enhancing System Security by Intrusion Detection Using Deep Learning, 169-176. https://doi.org/10.1007/978-3-031-15512-3_14.

7. Elsayed, S., Mohamed, K., & Madkour, M. (2024). A Comparative Study of Using Deep Learning Algorithms in Network Intrusion Detection. IEEE Access, 12, 58851-58870. https://doi.org/10.1109/ACCESS.2024.3389096.
8. Modak, A., & Dehalwar, V. (2024). Design and Analysis of Intrusion Detection Using Deep Learning Models. 2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), 1-6. https://doi.org/10.1109/CONECCT62155.2024.10677142.
9. Almejarb, R., Sallabi, O., Bushaala, F., Mohamed, A., Fawzi, A., & Adel, R. (2023). A Proposed Method for Detecting Network Intrusion Using Deep Learning Approach. 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), 83-88. https://doi.org/10.1109/MI-STA57575.2023.10169553.
10. Jiang, J., & Li, C. (2021). Binary- and Multi-class Network Intrusion Detection with Adaptive Synthetic Sampling and Deep Learning. 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 1-2. https://doi.org/10.1109/ICCE-TW52618.2021.9603206.
11. Cihan, S., Aydos, M., & Şimşek, N. (2021). A Tree Based Machine Learning and Deep Learning Classification for Network Intrusion Detection. European Journal of Science and Technology. https://doi.org/10.31590/ejosat.889994.
12. Chellammal, P., Kezia, S., Reka, K., & Raja, G. (2022). Fast and Effective Intrusion Detection Using Multi-Layered Deep Learning Networks. Int. J. Web Serv. Res, 19, 1-16. https://doi.org/10.4018/ijwsr.310057.
13. Hussain, J., & Hnamte, V. (2021). Deep Learning Based Intrusion Detection System:Modern Approach. 2021 2nd Global Conference for Advancement in Technology (GCAT), 1-6. https://doi.org/10.1109/GCAT52182.2021.9587719.
14. Amaizu, G., Nwakanma, C., Lee, J., & Kim, D. (2020). Investigating Network Intrusion Detection Datasets Using Machine Learning. 2020 International Conference on Information and Communication Technology Convergence (ICTC), 1325-1328. https://doi.org/10.1109/ICTC49870.2020.9289329.
15. M Hassan Zaib (2019). NSL-KDD. https://www.kaggle.com/datasets/hassan06/nslkdd.