DOI: 10.34185/1991-7848.itmm.2026.01.082

ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ

Малієнко С.Є.[1] [ORCID], Селівьорстова Т.В.[2] [ORCID]

[1]*Український державний університет науки і технологій, аспірант, Україна*

[2]*Український державний університет науки і технологій,*

к.т.н., доцент, Україна

Анотація. *У роботі досліджено ефективність методів машинного навчання для виявлення аномалій у мережевому трафіку. Проаналізовано основні підходи до побудови інтелектуальних систем виявлення вторгнень (IDS), зокрема сигнатурний аналіз та методи на основі машинного навчання. Виконано експериментальне порівняння алгоритмів Random Forest, Support Vector Machine, k-Nearest Neighbors та багатошарового перцептрона на датасеті NSL-KDD. Оцінку якості класифікації проведено за метриками Accuracy, Precision, Recall та F1-score. Результати показали, що метод Random Forest забезпечує найкращий баланс точності та швидкодії для задач виявлення мережевих аномалій у режимі реального часу. Визначено перспективи застосування ансамблевих методів та глибокого навчання для підвищення якості детектування кіберзагроз.*

Ключові слова: *машинне навчання, виявлення аномалій, мережевий трафік, кібербезпека, система виявлення вторгнень, Random Forest, класифікація, NSL-KDD.*

У сучасному цифровому середовищі кількість кібератак невпинно зростає, що створює критичну загрозу для інформаційної безпеки організацій та державних установ. За даними міжнародних звітів, щорічно фіксується понад 2 200 кібератак на день, причому значна частина з них залишається невиявленою протягом тривалого часу [1]. Традиційні сигнатурні методи виявлення вторгнень, що базуються на порівнянні мережевого трафіку з відомими шаблонами атак, виявляються неефективними проти нових типів загроз (zero-day атаки), оскільки не здатні ідентифікувати раніше невідомі патерни зловмисної активності.

Методи машинного навчання (ML) відкривають нові можливості для побудови інтелектуальних систем виявлення вторгнень (Intrusion Detection

System, IDS), здатних автоматично навчатися на прикладах нормального та аномального трафіку і виявляти відхилення навіть без попереднього знання про конкретний тип атаки [2]. Метою даної роботи є дослідження та порівняння ефективності методів машинного навчання — Random Forest (RF), Support Vector Machine (SVM), k-Nearest Neighbors (k-NN) та багатошарового перцептрона (MLP) — для задачі бінарної класифікації мережевого трафіку на нормальний та аномальний.

Задача виявлення аномалій у мережевому трафіку може бути формалізована як задача бінарної класифікації. Нехай кожне мережеве з'єднання описується вектором ознак $x = (x_1, x_2, ..., x_n)$, де ознаки характеризують тривалість з'єднання, тип протоколу, кількість переданих байтів, кількість пакетів, прапорці з'єднання тощо. Тоді задача полягає у побудові класифікатора $f: X \to \{0, 1\}$, де 0 відповідає нормальному трафіку, а 1 — аномальному.

Для оцінки якості класифікації використано стандартні метрики. Accuracy — частка правильно класифікованих зразків від загальної кількості (1). Precision — частка дійсно аномальних зразків серед усіх, класифікованих як аномальні (2). Recall — частка виявлених аномалій від загальної кількості реальних аномалій (3). F1-score — гармонічне середнє Precision та Recall, що забезпечує збалансовану оцінку (4):

$$Accuracy = (TP + TN) / (TP + TN + FP + FN), \quad (1)$$

$$Precision = TP / (TP + FP), \quad (2)$$

$$Recall = TP / (TP + FN), \quad (3)$$

$$F1 = 2 \cdot Precision \cdot Recall / (Precision + Recall), \quad (4)$$

де TP (True Positive) — кількість правильно виявлених аномалій, TN (True Negative) — правильно класифікований нормальний трафік, FP (False Positive) — хибно класифікований як аномальний нормальний трафік, FN (False Negative) — пропущені аномалії.

Для проведення експериментального дослідження обрано датасет NSL-KDD [3], який є вдосконаленою версією класичного KDD Cup'99 і широко використовується у дослідженнях з мережевої безпеки. Датасет містить записи мережевих з'єднань, кожне з яких описується 41 ознакою та класифіковане як

нормальне або як один з типів атак: DoS (відмова в обслуговуванні), Probe (сканування), R2L (віддалений доступ), U2R (підвищення привілеїв). Навчальна вибірка містить 125 973 записи, тестова — 22 544 записи. Для бінарної класифікації всі типи атак об'єднано в клас «аномалія».

У дослідженні порівняно чотири методи машинного навчання. Random Forest (RF) — ансамблевий метод, що будує множину дерев рішень та агрегує їх результати голосуванням, що забезпечує стійкість до перенавчання та високу точність на табличних даних. Support Vector Machine (SVM) — метод, що шукає оптимальну гіперплощину для розділення класів у просторі ознак із максимальним зазором. k-Nearest Neighbors (k-NN) — метод, що класифікує зразок за мажоритарним голосуванням k найближчих сусідів. Багатошаровий перцептрон (MLP) — нейронна мережа прямого поширення з одним або кількома прихованими шарами [4].

Препроцесинг даних включав нормалізацію числових ознак методом Min-Max scaling до діапазону [0, 1], one-hot кодування категоріальних ознак (protocol_type, service, flag) та розбиття на навчальну та тестову вибірки згідно стандартного поділу NSL-KDD. Результати експериментального порівняння наведено у табл. 1.

Таблиця 1

Результати класифікації мережевого трафіку

Метод	Accuracy	Precision	Recall	F1-score
Random Forest	0.9731	0.9685	0.9812	0.9748
SVM	0.9524	0.9478	0.9603	0.9540
k-NN	0.9412	0.9356	0.9501	0.9428
MLP	0.9658	0.9621	0.9724	0.9672

Як видно з табл. 1, метод Random Forest продемонстрував найвищі показники за всіма метриками: Accuracy = 0.9731, F1-score = 0.9748. Це пояснюється здатністю ансамблю дерев рішень ефективно обробляти гетерогенні ознаки мережевого трафіку та стійкістю до шуму в даних. Багатошаровий перцептрон показав другий за якістю результат (F1 = 0.9672),

однак потребує значно більшого часу на навчання. SVM забезпечив прийнятну точність, але масштабується гірше при зростанні обсягу даних. Метод k-NN показав найнижчі результати серед досліджених алгоритмів, що обумовлено чутливістю до вибору параметра k та високою розмірністю простору ознак.

Важливим аспектом є також швидкодія алгоритмів. Для систем реального часу критичним є час класифікації одного зразка. Random Forest забезпечує швидку класифікацію завдяки паралельній обробці дерев, тоді як SVM та MLP потребують більше обчислювальних ресурсів. Проблема дисбалансу класів у датасеті NSL-KDD, де нормальний трафік переважає над аномальним, частково компенсована використанням метрики F1-score, яка враховує як Precision, так і Recall.

Висновки

У роботі досліджено застосування методів машинного навчання для виявлення аномалій у мережевому трафіку. Експериментальне порівняння на датасеті NSL-KDD показало, що метод Random Forest забезпечує найкращий баланс точності (F1-score = 0.9748) та швидкодії серед розглянутих алгоритмів, що робить його найбільш придатним для застосування в інтелектуальних системах виявлення вторгнень реального часу. Перспективами подальших досліджень є застосування методів глибокого навчання (автоенкодерів, рекурентних нейронних мереж), ансамблевих підходів для підвищення якості детектування, а також адаптація моделей до потокових даних для роботи в умовах змінюваного характеру мережевого трафіку.

ЛІТЕРАТУРА / REFERENCE

1. Buczak A.L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials. 2016. Vol. 18, No. 2. P. 1153–1176. DOI: https://doi.org/10.1109/COMST.2015.2494502

2. Ahmad Z., Shahid Khan A., Wai Shiang C., Abdullah J., Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies. 2021. Vol. 32, No. 1. e4150. DOI: https://doi.org/10.1002/ett.4150

3. Tavallaee M., Bagheri E., Lu W., Ghorbani A.A. A Detailed Analysis of the KDD CUP 99 Data Set. Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA). 2009. P. 1–6. DOI: https://doi.org/10.1109/CISDA.2009.5356528

4. Mirsky Y., Doitshman T., Elovici Y., Shabtai A. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. Proceedings of the Network and Distributed System Security Symposium (NDSS). 2018. DOI: https://dx.doi.org/10.14722/ndss.2018.23204

APPLICATION OF MACHINE LEARNING METHODS FOR ANOMALY DETECTION IN NETWORK TRAFFIC

Stanislav Maliienko, Tetiana Selivorstova

Abstract. *This paper investigates the effectiveness of machine learning methods for anomaly detection in network traffic. The main approaches to building intelligent intrusion detection systems (IDS) are analyzed, including signature-based analysis and machine learning-based methods. An experimental comparison of Random Forest, Support Vector Machine, k-Nearest Neighbors, and Multilayer Perceptron algorithms was performed on the NSL-KDD dataset. Classification quality was assessed using Accuracy, Precision, Recall, and F1-score metrics. The results showed that the Random Forest method provides the best balance of accuracy and computational efficiency for real-time network anomaly detection tasks. The prospects of applying ensemble methods and deep learning for improving cyber threat detection quality are identified.*

Keywords: *machine learning, anomaly detection, network traffic, cybersecurity, intrusion detection system, Random Forest, classification, NSL-KDD.*