№ 2(56) 2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online
УДК 004.6:004.8
https://doi.org/10.52058/2786-6025-2026-2(56)-2136-2146

Рихва Володимир Ігорович аспірант кафедри кібербезпеки та інформаційних технологій Харківського національного економічного університету імені Семена Кузнеця, Харків, https://orcid.org/0009-0008-2711-547X

Солодовник Ганна Валеріївна кандидат технічних наук, доцент, доцент кафедри кібербезпеки та інформаційних технологій Харківського національного економічного університету імені Семена Кузнеця, Харків, https://orcid.org/0000-0001-6323-5083

ОПТИМІЗАЦІЯ КЛАСИФІКАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ НА ОСНОВІ LIGHTGBM ТА ВІДБОРУ ОЗНАК МЕТОДОМ SHAP

Анотація. У статті досліджено ефективність методу SHapley Additive exPlanations (SHAP) для відбору ознак при оптимізації класифікатора LightGBM у задачі виявлення мережевих вторгнень. Актуальність дослідження зумовлена необхідністю підвищення ефективності систем виявлення вторгнень в умовах зростання обсягів мережевого трафіку та кількості ознак, що потребують обробки. Метод SHAP, заснований на теорії кооперативних ігор, дозволяє обчислити справедливий внесок кожної ознаки у прогнозування моделі та відібрати найбільш інформативні, забезпечуючи при цьому локальну інтерпретованість рішень класифікатора. На відміну від традиційних методів відбору, що базуються на агрегованих метриках важливості, SHAP враховує взаємодію між ознаками та дозволяє ідентифікувати ознаки, схильні до перенавчання на специфічних шаблонах навчальної вибірки. У роботі проаналізовано вплив скорочення розмірності вхідного простору на якість класифікації та розпізнавання окремих класів атак. Експерименти проведено на чотирьох еталонних наборах даних мережевого трафіку: CIC-IDS2017, CIC-IDS2018, UNSW-NB15 та CICIoT2023, що відрізняються кількістю ознак, класів та ступенем дисбалансу. Для оцінки якості класифікації використано метрики Accuracy, Macro F1-score та Matthews Correlation Coefficient (MCC), що забезпечує об’єктивну оцінку навіть за значного дисбалансу класів. Досліджено вплив SHAP-відбору на розпізнавання рідкісних класів атак, що є критично важливим для практичного застосування систем виявлення вторгнень. Результати показали, що SHAP-відбір скорочує розмірність на 26–74% при збереженні або покращенні якості класифікації, а також суттєво підвищує розпізнавання міноритарних класів атак за рахунок усунення шумових ознак.

ISSN 2786-6025 Online

Практична значущість роботи полягає у можливості одночасного підвищення інтерпретованості моделі та оптимізації обчислювальних ресурсів.

Ключові слова: LightGBM, SHAP, відбір ознак, система виявлення вторгнень, класифікація мережевого трафіку, градієнтний бустинг, кібер-безпека.

Rykhva Volodymyr PhD student of the Department of Cybersecurity and Information Technologies, Simon Kuznets Kharkiv National Economic University, Kharkiv, https://orcid.org/0009-0008-2711-547X

Solodovnyk Ganna Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Cybersecurity and Information Technologies, Simon Kuznets Kharkiv National Economic University, Kharkiv, https://orcid.org/0000-0001-6323-5083

OPTIMIZATION OF NETWORK TRAFFIC CLASSIFICATION BASED ON LIGHTGBM AND SHAP FEATURE SELECTION

Abstract. This paper investigates the effectiveness of SHapley Additive exPlanations (SHAP) feature selection method for optimizing LightGBM classifier in network intrusion detection tasks. The relevance of the study is determined by the need to improve the efficiency of intrusion detection systems in conditions of growing network traffic volumes and the number of features that require processing. The SHAP method, based on cooperative game theory, allows calculating the fair contribution of each feature to the model prediction and selecting the most informative ones while providing local interpretability of classifier decisions. Unlike traditional selection methods based on aggregated importance metrics, SHAP accounts for feature interactions and enables identification of features prone to overfitting on training sample-specific patterns. In the article the impact of input dimensionality reduction on classification quality and recognition of individual attack classes is analyzed. Experiments were conducted on four benchmark network traffic datasets: CIC-IDS2017, CIC-IDS2018, UNSW-NB15, and CICIoT2023, which differ in the number of features, classes, and degree of imbalance. Accuracy, Macro F1-score, and Matthews Correlation Coefficient (MCC) metrics were used to evaluate classification quality, providing objective assessment even under significant class imbalance. The impact of SHAP selection on the recognition of rare attack classes, which is critical for practical application of intrusion detection systems, is investigated. Results showed that SHAP selection reduces dimensionality by 26–74% while maintaining or improving classification quality, and substantially improves

ISSN 2786-6025 Online

recognition of minority attack classes by eliminating noisy features. The practical significance of the work lies in the ability to simultaneously improve model interpretability and optimize computational resources.

Keywords: LightGBM, SHAP, feature selection, intrusion detection system, network traffic classification, gradient boosting, cybersecurity.

Постановка проблеми. Сучасні системи виявлення мережевих вторгнень (Intrusion Detection Systems, IDS) обробляють великі обсяги мережевого трафіку з десятками та сотнями ознак. Висока розмірність вхідних даних створює низку проблем: збільшення обчислювальних витрат на навчання та інференс, ризик перенавчання моделей на зашумлених ознаках, а також ускладнення інтерпретації прийнятих рішень [1]. Алгоритми градієнтного бустингу, зокрема LightGBM, демонструють високу ефективність на табличних даних мережевого трафіку [2], проте питання оптимального відбору ознак залишається актуальним для підвищення узагальнювальної здатності та швидкодії моделей.

Традиційні методи відбору ознак часто базуються на статистичних характеристиках або внутрішній важливості моделі, що не завжди відображає реальний внесок ознак у прогнозування [3]. Метод SHAP – це сучасний підхід на основі теорії кооперативних ігор (cooperative game theory), який обчислює справедливий внесок кожної ознаки у передбачення моделі для кожного зразка [4]. На відміну від глобальних агрегованих метрик важливості (global feature importance), SHAP забезпечує локальну інтерпретованість, що дозволяє ідентифікувати ознаки з високою дисперсією внеску та схильністю до перенавчання на специфічних шаблонах навчальної вибірки. Наукова проблема полягає у необхідності систематичного дослідження ефективності SHAP-відбору ознак для оптимізації класифікаторів мережевого трафіку на множині еталонних наборів даних із різними характеристиками: кількістю ознак, класів та ступенем дисбалансу.

Аналіз останніх досліджень і публікацій. Відбір ознак є важливим етапом побудови систем виявлення вторгнень. Комплексний огляд методів машинного навчання для IDS [1] показав, що зменшення розмірності вхідного простору дозволяє підвищити точність та швидкодію класифікаторів.

Дослідження ефективності LightGBM для виявлення мережевих атак [2] продемонструвало перевагу градієнтного бустингу над глибоким навчанням на табличних даних, проте питання оптимального набору ознак не розглядалося.

Гібридний метод відбору ознак IGRF-RFE для набору даних UNSW-NB15 [3] показав, що використання комбінації Information Gain та Random Forest Importance з рекурсивним виключенням дозволяє скоротити розмірність з 42 до 23 ознак при підвищенні точності класифікації. Проте цей підхід не

ISSN 2786-6025 Online

використовує SHAP. У роботі [5] показано ефективність SHAP для пояснення рішень моделей у медичних системах. Дослідження [6] підтвердило, що комбінація SHAP та Information Gain перевершує традиційні методи відбору для задач виявлення вторгнень.

Проведений аналіз наукових джерел засвідчив недостатню дослідженість питання впливу SHAP відбору ознак на ефективність класифікації мережевого трафіку, зокрема на розпізнавання міноритарних класів атак (minority class detection) в умовах незбалансованих наборів даних.

Мета статті полягає у дослідженні ефективності методу SHAP для відбору ознак в процесі оптимізації класифікатора LightGBM на чотирьох еталонних наборах даних мережевого трафіку та оцінці впливу скорочення розмірності на якість класифікації загалом та для окремих класів атак.

Виклад основного матеріалу. Дослідження проведено на чотирьох еталонних наборах даних мережевого трафіку (табл. 1), що відрізняються кількістю ознак, класів та ступенем дисбалансу.

Таблиця 1

Характеристики наборів даних

Набір даних	Ознак	Класів	Зразків (тис.)	Рік
CIC-IDS2017	78	7	2 830	2017
CIC-IDS2018	81	6	6 500	2018
UNSW-NB15	39	10	2 540	2015
CICIoT2023	46	8	~1 000	2023

Попередня обробка даних включала: видалення дублікатів та нескінченних значень, заповнення пропусків нулями, стандартизацію числових ознак (StandardScaler) з навчанням лише на тренувальній вибірці. Дані розділено на навчальну вибірку, яка складає 70% від всієї кількісті навчальних даних, валідаційну вибірку, яка складає 15%, та тестову вибірку, яка складає 15%. Наведені вибірки сформовано зі стратифікацією за класами (random_state=42).

Для базової класифікації використано алгоритм LightGBM, який демонструє високу ефективність для виявлення вторгнень у мережах IoT [7]. Параметри моделі: n_estimators=500, learning_rate=0.05, num_leaves=63, max_depth=-1, objective='multiclass'. Для врахування дисбалансу класів застосовано параметр class_weight='balanced'.

SHAP-аналіз проведено з використанням бібліотеки SHAP та TreeExplainer для моделей градієнтного бустингу. Для кожного набору даних обчислено середні абсолютні SHAP-значення по всіх зразках тестової вибірки.

ISSN 2786-6025 Online

На основі рейтингу важливості відібрано ознаки з найбільшим внеском, при цьому поріг відбору визначався емпірично для кожного набору даних.

Для оцінки якості класифікації використано наступні метрики: Accuracy, Macro F1-score та Matthews Correlation Coefficient (MCC). Метрика MCC має високу надійність у випадку незбалансованих даних, оскільки враховує всі чотири елементи матриці невідповідностей (confussion matrix) та забезпечує об'єктивну оцінку навіть за значного дисбалансу класів [11].

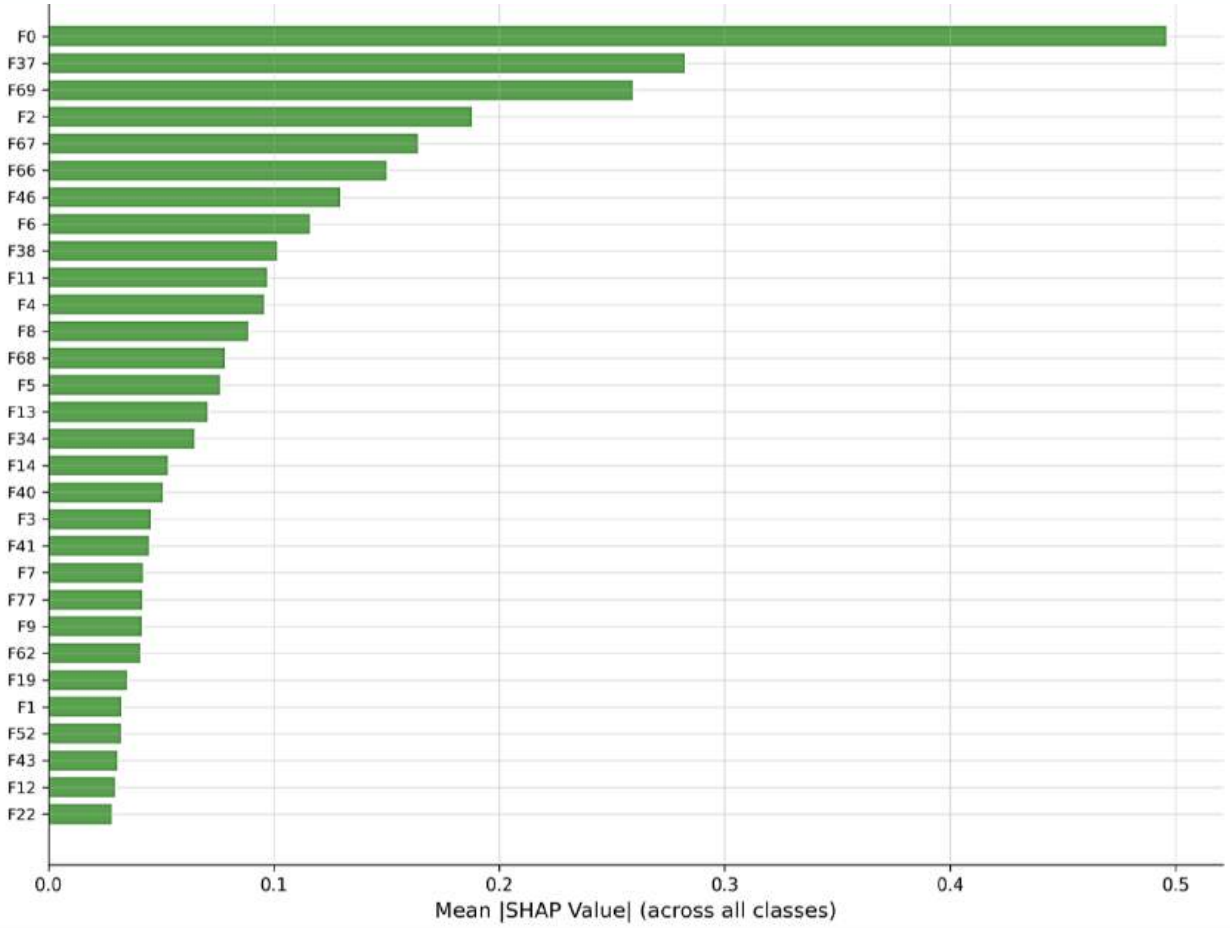

Рис. 1. Топ-30 ознак за SHAP-важливістю для CIC-IDS2017

На рисунку 1 представлено перелік з тридцяти ознак, які мають найвищу SHAP-важливість для набору даних CIC-IDS2017. Найбільший внесок у класифікацію мають ознаки Destination Port, Flow Duration, Fwd Packet Length Max та Bwd Packet Length Mean. Ці ознаки пов'язані з характеристиками мережевих потоків та дозволяють ефективно розрізняти типи атак.

Кількість відібраних SHAP-ознак для кожного набору даних визначалась на основі аналізу кумулятивного внеску та експериментальної валідації. Результати аналізу наведено у таблиці 2.

№ 2(56) 2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online

Таблиця 2

Результати SHAP-відбору ознак

Набір даних	Всього ознак	SHAP-відбір	Скорочення, %
CIC-IDS2017	78	50	35,9
CIC-IDS2018	81	60	25,9
UNSW-NB15	39	10	74,4
CICIoT2023	46	30	34,8

Графічний вигляд результатів аналізу представлено на рисунку 2.

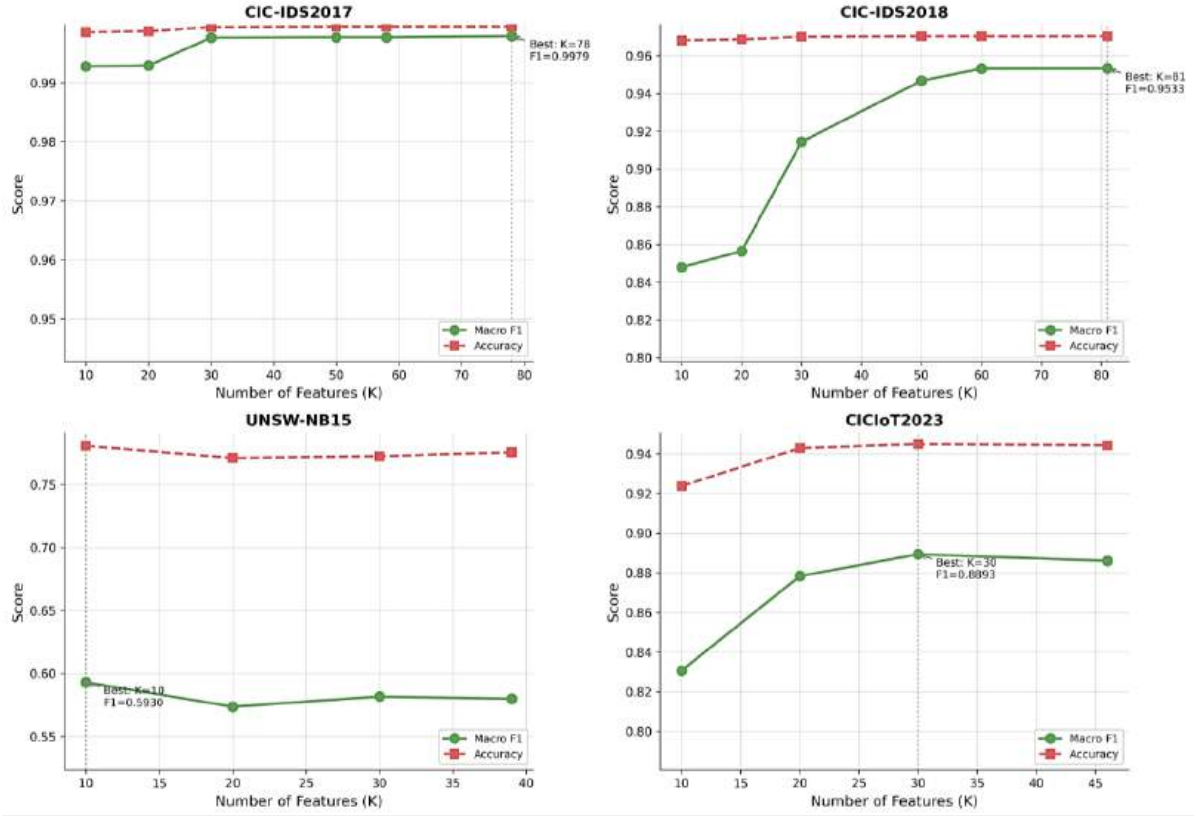

Рис. 2. Порівняння кількості ознак: повний набір і SHAP-відбір

Найбільше скорочення розмірності (74,4%) досягнуто для набору даних UNSW-NB15, за якого лише 10 ознак з 39 виявились найбільш інформативними. За набору даних CIC-IDS2018 скорочення виявилося мінімальним (25,9%), що свідчить про більшу інформативність повного набору ознак цього набору даних.

ISSN 2786-6025 Online

Результати порівняння моделі LightGBM з повним набором ознак та SHAP-оптимізованою версією цієї моделі на чотирьох наборах даних представлено в таблиці 3, а також на рисунку 3.

Табл. 3

Порівняння моделей LightGBM та LightGBM-SHAP

Набір даних	**Модель**	**Accuracy**	**Macro F1**	**MCC**
CIC-IDS2017	LightGBM	0,9995	0,9977	0,9994
CIC-IDS2017	LightGBM-SHAP	0,9995	0,9977	0,9994
CIC-IDS2018	LightGBM	0,9704	0,9583	0,9636
CIC-IDS2018	LightGBM-SHAP	0,9703	0,9532	0,9635
UNSW-NB15	LightGBM	0,7785	0,5778	0,7258
UNSW-NB15	LightGBM-SHAP	0,7808	0,5930	0,7315
CICIoT2023	LightGBM	0,9436	0,8850	0,9329
CICIoT2023	LightGBM-SHAP	0,9449	0,8893	0,9344

№ 2(56) 2026
НАУКА і ТЕХНІКА СЬОГОДНІ
ISSN 2786-6025 Online

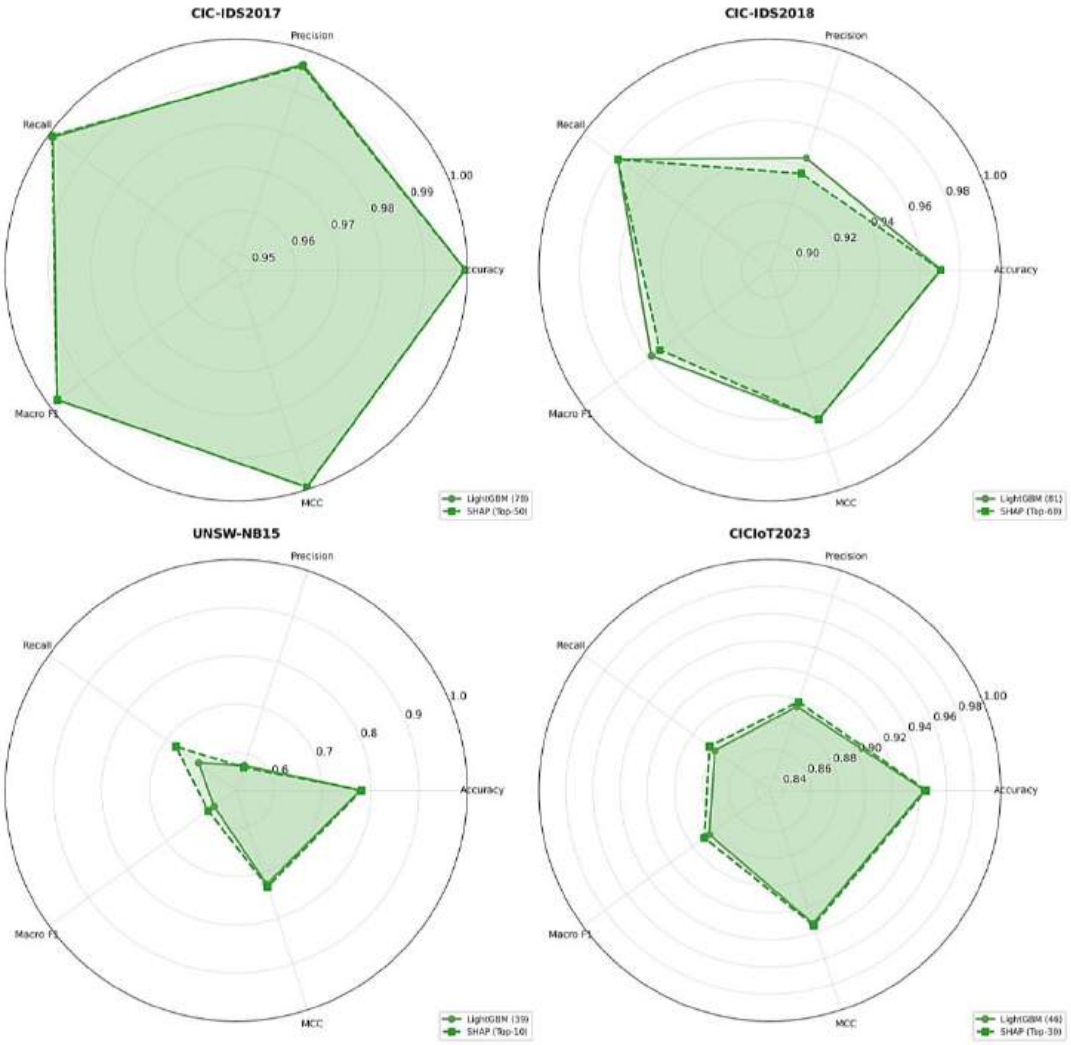

Рис. 3. Радарна діаграма порівняння LightGBM та LightGBM-SHAP за метриками

На наборі даних CIC-IDS2017 SHAP-оптимізована модель з використанням 50 ознак досягла практично ідентичних результатів порівняно з базовою моделлю, яка використовує 78 ознак: Macro F1 = 0,9977 для обох моделей. Це свідчить про те, що 28 виключених ознак не несли додаткової інформації для класифікації, тому їх видалення дозволяє скоротити обчислювальні витрати без втрати точності.

На наборі даних CIC-IDS2018 спостерігається незначне зниження показника Macro F1 з 0,9583 до 0,9532 (-0,5 п.п.) за скорочення ознак з 81 до 60. Основне погіршення пов'язане з класом WebAttack, для якого показник F1-score знизився з 0,897 до 0,867 (–3,0 п.п.).

Найбільш показовим є результат на наборі даних UNSW-NB15, за якого SHAP-відбір покращив показник Macro F1 з 0,5778 до 0,5930 (+2,6 п.п.) за

ISSN 2786-6025 Online

скорочення ознак з 39 до 10. Це свідчить про те, що 29 виключених ознак створювали шум, який погіршував загальну здатність моделі. Покращення особливо помітне для рідкісних класів атак представлених у таблиці 4, яка містить результати порівняння моделі LightGBM з повним набором ознак та SHAP-оптимізованою версією цієї моделі за показником Per-class F1-score для набору даних UNSW-NB15.

Таблиця 4

Результати порівняння моделей

Клас	LightGBM	LightGBM-SHAP	Δ F1
Analysis	0,075	0,124	+0,049
Backdoor	0,064	0,127	+0,063
DoS	0,376	0,469	+0,093
Exploits	0,676	0,660	-0,016
Fuzzers	0,676	0,663	-0,013
Generic	0,989	0,990	+0,001
Normal	0,905	0,889	-0,016
Reconnaissance	0,827	0,820	-0,007
Shellcode	0,656	0,569	-0,087
Worms	0,533	0,618	+0,085

Аналіз per-class метрик виявив, що SHAP-відбір значно покращує розпізнавання найрідкісніших класів: Worms (+15,9%), Backdoor (+98,4%), Analysis (+65,3%), DoS (+24,7%). Водночас спостерігається незначне погіршення для класу Shellcode (-13,3%). Такий результат пояснюється тим, що метод SHAP виключає ознаки, специфічні для навчальної вибірки, що покращує узагальнення на рідкісні класи, але може погіршити розпізнавання окремих категорій з унікальними патернами.

На наборі даних CICIoT2023 SHAP-оптимізована модель, побудована на 30 ознаках, покращила показник Macro F1 з 0,8850 до 0,8893 (+0,5 п.п.) при скороченні кількості ознак на 34,8%. Покращення спостерігається для всіх класів, зокрема BruteForce (+2,1 п.п.) та WebBased (+0,7 п.п.).

Висновки. У межах дослідження проведено комплексний аналіз ефективності методу SHAP для відбору ознак при оптимізації класифікатора LightGBM на чотирьох еталонних наборах даних мережевого трафіку. Основні результати:

ISSN 2786-6025 Online

1. Метод відбору SHAP дозволяє скоротити кількість ознак на 23–74% (залежно від набору даних) за збереження або покращення якості класифікації. На наборі даних CIC-IDS2017 модель з 50 ознаками досягла ідентичних результатів з повним набором, який налічує 78 ознак.

2. На наборі даних UNSW-NB15 SHAP-оптимізація покращила показник Macro F1 з 0,5778 до 0,5930 (+2,6%), що свідчить про усунення шумових ознак. Значного покращення досягнуто для рідкісних класів: Worms (+15,9%), Backdoor (+98,4%).

3. Аналіз per-class метрик виявив, що SHAP-відбір покращує розпізнавання рідкісних класів атак за рахунок усунення ознак, специфічних для навчальної вибірки.

4. Інтеграція SHAP-аналізу в IDS дозволяє одночасно підвищити інтерпретованість моделі та оптимізувати обчислювальні ресурси.

Перспективи подальших досліджень включають: адаптивний SHAP-відбір з динамічним порогом залежно від розподілу класів; порівняння метода SHAP з іншими методами (LIME, Permutation Importance) та застосування SHAP-відбору для ансамблевих моделей.

Література:

1. Momand A., Jan S. U., Ramzan N. A systematic and comprehensive survey of recent advances in intrusion detection systems using machine learning: Deep learning, datasets, and attack taxonomy. Journal of Sensors. 2023. DOI: 10.1155/2023/6048087.

2. Liu G., Zhao W., Wang Q. A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM. Computers & Security. 2021. Vol. 106. P. 102289. DOI: 10.1016/j.cose.2021.102289.

3. Yin Y., Jang-Jaccard J., Xu W., Singh A., Zhu J., Sabrina F., Kwak J. IGRF-RFE: A hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset. Journal of Big Data. 2023. Vol. 10, No. 1. P. 1-26. DOI: 10.1186/s40537-023-00694-8.

4. Ahmed U., Jiangbin Z., Almogren A., Khan I., Tariq A., Shorfuzzaman M. Hybrid bagging and boosting with SHAP based feature selection for enhanced predictive modeling in intrusion detection systems. Scientific Reports. 2024. Vol. 14. P. 30532. DOI: 10.1038/s41598-024-81151-1.

5. Nohara Y., Matsumoto K., Soejima H., Nakashima N. Explanation of machine learning models using shapley additive explanation and application for real data in hospital. Computer Methods and Programs in Biomedicine. 2022. Vol. 214. P. 106584. DOI: 10.1016/j.cmpb.2021.106584.

6. Wang D., Yang J., Cui B. A novel feature selection method based on SHAP and information gain for intrusion detection. IEEE Access. 2023. Vol. 11. P. 132892-132905. DOI: 10.1109/ACCESS.2023.3336127.

7. Singal H., Kumar A., Upreti K. Evolutionary LightGBM-based intrusion detection system for IoT networks. International Journal of Communication Systems. 2025. Vol. 38, No. 2. P. e70031. DOI: 10.1002/dac.70031.

8. Engelen G., Rimmer V., Joosen W. Troubleshooting an intrusion detection dataset: the CICIDS2017 case study. IEEE Security and Privacy Workshops (SPW). 2021. P. 102-109. DOI: 10.1109/SPW53761.2021.00009.

ISSN 2786-6025 Online

9. Neto E. C. P., Dadkhah S., Ferreira R., Zohourian A., Lu R., Ghorbani A. A. CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment. Sensors. 2023. Vol. 23, No. 13. P. 5941. DOI: 10.3390/s23135941.

10. Grinsztajn L., Oyallon E., Varoquaux G. Why do tree-based models still outperform deep learning on typical tabular data? Advances in Neural Information Processing Systems. 2022. Vol. 35. P. 507-520. DOI: 10.48550/arXiv.2207.08815.

11. Chicco D., Jurman G. The Matthews correlation coefficient (MCC) should replace the ROC AUC as the standard metric for assessing binary classification. BioData Mining. 2023. Vol. 16, No. 4. P. 1-23. DOI: 10.1186/s13040-023-00322-4.

References:

1. Momand, A., Jan, S. U., & Ramzan, N. (2023). A systematic and comprehensive survey of recent advances in intrusion detection systems using machine learning: Deep learning, datasets, and attack taxonomy. Journal of Sensors, 2023. https://doi.org/10.1155/2023/6048087

2. Liu, G., Zhao, W., & Wang, Q. (2021). A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM. Computers & Security, 106, 102289. https://doi.org/10.1016/j.cose.2021.102289

3. Yin, Y., Jang-Jaccard, J., Xu, W., Singh, A., Zhu, J., Sabrina, F., & Kwak, J. (2023). IGRF-RFE: A hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15dataset.Journal of Big Data,10(1),1-26. https://doi.org/10.1186/s40537-023-00694-8

4. Ahmed, U., Jiangbin, Z., Almogren, A., Khan, I., Tariq, A., & Shorfuzzaman, M. (2024). Hybrid bagging and boosting with SHAP based feature selection for enhanced predictive modeling in intrusion detect. sysm.Scientific Reports,14,30532. https://doi.org/10.1038/s41598-024-81151-1

5. Nohara, Y., Matsumoto, K., Soejima, H., & Nakashima, N. (2022). Explanation of machine learning models using shapley additive explanation and application for real data in hospital. Computer Methods and Programs in Biomedicine, 214, 106584. https://doi.org/10.1016/j.cmpb.2021.106584

6. Wang, D., Yang, J., & Cui, B. (2023). A novel feature selection method based on SHAP and information gain for intrusion detection. IEEE Access, 11, 132892-132905. https://doi.org/10.1109/ACCESS.2023.3336127

7. Singal, H., Kumar, A., & Upreti, K. (2025). Evolutionary LightGBM-based intrusion detection system for IoT networks. International Journal of Communication Systems, 38(2), e70031. https://doi.org/10.1002/dac.70031

8. Engelen, G., Rimmer, V., & Joosen, W. (2021). Troubleshooting an intrusion detection dataset: the CICIDS2017 case study. In IEEE Security and Privacy Workshops (SPW) (pp. 102-109). https://doi.org/10.1109/SPW53761.2021.00009

9. Neto, E. C. P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., & Ghorbani, A. A. (2023). CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment. Sensors, 23(13), 5941. https://doi.org/10.3390/s23135941

10. Grinsztajn, L., Oyallon, E., & Varoquaux, G. (2022). Why do tree-based models still outperform deep learning on typical tabular data? Advances in Neural Information Processing Systems, 35, 507-520. https://doi.org/10.48550/arXiv.2207.08815

11. Chicco, D., & Jurman, G. (2023). The Matthews correlation coefficient (MCC) should replace the ROC AUC as the standard metric for assessing binary classification. BioData Mining, 16(4), 1-23. https://doi.org/10.1186/s13040-023-00322-4

Дата першого надходження статті до видання: 11.02.2026
Дата прийняття статті до друку після рецензування: 24.02.2026