МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

# МІЖНАРОДНА КОНФЕРЕНЦІЯ

## *ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ*

## *(ПТІКІ'2026)*

**Одеса, Україна, 16 липня 2026 р.**

**Матеріали конференції**

**ОДЕСА**

**2026**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**МІЖНАРОДНИЙ УНІВЕРСИТЕТ**

# МІЖНАРОДНА КОНФЕРЕНЦІЯ

# «Передові технології в інформаційно-комунікаційній інженерії»

# (ПТІКІ'2026)

**Одеса, Україна, 16 липня 2026 р.**

**Матеріали конференції**

**Одеса**

**2026**

**УДК 004.9**
**ББК 32**

***Проведення заходу зареєстровано в Державній науковій установі «Український інститут науково-технічної експертизи та інформації» (Реєстраційний номер: 3326U000765 від 01-07-2026 р.).***

**Рецензенти:**
**Надія КАЗАКОВА** – д.т.н., професор, завідувач кафедри інформаційних технологій Одеського національного університету ім. І.І. Мечнікова
**Віктор СТРЕЛЬБИЦЬКИЙ** – к.т.н., доцент, доцент кафедри підйомно-транспортні машини та інжиніринг портового технологічного обладнання Одеського національного морського університету

**International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2026):** Conference Proceedings. Odesa: International university, 2026, 145 p**.**
DOI: https://doi.org/10.32837/11300.33747

**Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2026):** Матеріали конференції. Одеса: Міжнародний університет, 2026, 145 с.

У збірнику подано результати наукових досліджень, висвітлено обговорення актуальних проблем, викликів і тенденцій з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами у різних галузях народного господарства. Матеріали охоплюють інноваційні підходи, досвід упровадження сучасних рішень і приклади успішних практик трансформації різних галузях народного господарства .

Видання призначене для науково-педагогічних працівників, здобувачів освіти, науковців і фахівців ІТ галузі.



Відповідальні за випуск:
*к.т.н., доцент Пунченко Наталія,*
*к.т.н., доцент Розенвассер Денис.*

## ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

**Голова**

КІВАЛОВ С.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.

**Співголови**

ГРОМОВЕНКО К.В. – д.ю.н., проф., Міжнародний університет, м. Одеса, Україна.
ЛЕФТЕРОВ В.О. – д.п.н., проф., Міжнародний університет, Одеса, Україна
СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., НТУ України "КПІ імені Ігоря Сікорського", Київ, Україна.

**Члени організаційного комітету**

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ЙОНА Л.Г. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ВАКАРЧУК А.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРІБОВА В.В. – к.ф.-м.н., доц., Міжнародний університет, Одеса, Україна.

## РЕДАКЦІЙНИЙ КОМІТЕТ

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

## КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л. С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

## ВЧЕНИЙ СЕКРЕТАР

ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

## ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

**ЗМІСТ**

# СЕКЦІЯ 2.
# КОМП`ЮТЕРНІ НАУКИ

УДК 004.85:004.738.5

DOI: https://doi.org/10.32837/11300.33751

## КЛАСИФІКАЦІЯ ВЕБТРАФІКУ HTTP/HTTPS-ЗАПИТІВ

*Стрелковська І.В., д.т.н., професор,*
*Міжнародний університет,*
*i.strelkovskaya@mgu.edu.ua*
*Соловська І.М., к.т.н., доцент,*
*Міжнародний університет,*
*i.solovskaya@mgu.edu.ua,*
*Стрелковська Ю.О., к.ю.н., доцент*
*Worthing college*
*4800632s@gmail.com*

***Анотація.*** *Розглянуто задачу класифікації вебтрафіку до нормального (еталонного) або аномального (шкідливого) вебтрафіку HTTP/HTTPS-запитів. Встановлено, що для класифікації вебтрафіку доцільним є використання методів машинного навчання (ML-методів). Запропоновано використання для класифікації вебтрафіку методу k-найближчих сусідів KNN та Байєсівського методу. Отримані результати можуть бути використаними в системах моніторингу вебтрафіку та раннього попередження аномалій вебресурсів.*

Сучасний розвиток інформаційних технологій супроводжується стрімким зростанням обсягів вебтрафіку, класифікація якого зазвичай виконується за інтенсивністю трафіку, коли визначаються характеристики інтенсивності нормального та аномального трафіку. Особливої актуальності класифікація набуває в умовах зростання кількості DDoS-атак, спроб несанкціонованого доступу до вебресурсів, поширення шкідливого програмного забезпечення та інших аномалій. Використання методів машинного навчання Machine learning (ML) для класифікації вебтрафіку дозволяє виконувати обробку великих обсягів мережевих даних та гнучко адаптуватися до змін характеристик вебтрафіку, забезпечуючи точність класифікації та здатність до самонавчання.

На відміну від розглянутих в роботі [1-3] традиційних сигнатурних підходів до класифікації трафіку, коли використовуються відомі «сигнатури» трафіку – шаблони легітимного або шкідливого трафіку для порівняння та визначення аномалії, ML-методи класифікації здатні виявляти аномалії вебтрафіку на основі отриманих характеристик аналізу

трафіку, що є критично важливим для сучасних систем моніторингу та виявлення вторгнень.

Використання ML-методів для класифікації вебтрафіку розглянуто в роботах [4-7], авторами встановлено, що в умовах зростання обсягів вебтрафіку та відповідного зменшення ефективності традиційних методів, ML-методи мають перевагу. Однак, результати використання таких методів не завжди є придатними для практичної реалізації, коли метод класифікації визначається для заданого сервісу або додатку, тому в разі появи нового вебресурсу або вебсервісу, визначений алгоритм класифікації потребує зміни.

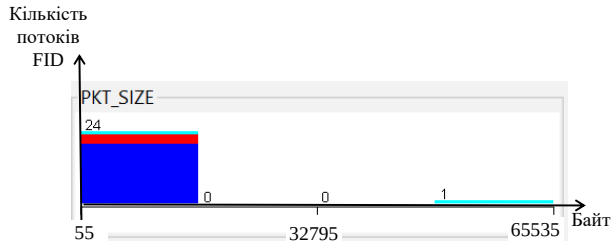
Метою даної роботи є використання методів машинного навчання для класифікації вебтрафіку HTTP/HTTPS-запитів з метою визначення аномалій трафіку спричинених DDoS-атаками.

Дослідження вебтрафіку виконано на базі датасету [8] з відкритого ресурсу https://www.kaggle.com результатів моніторингу трафіку, до яких віднесено інтенсивності HTTP/HTTPS-запитів (GET або POST), середній розмір HTTP/HTTPS-запитів та загальний обсяг переданих даних. Фрагмент вихідних даних датасету наведено **у** табл. 1.

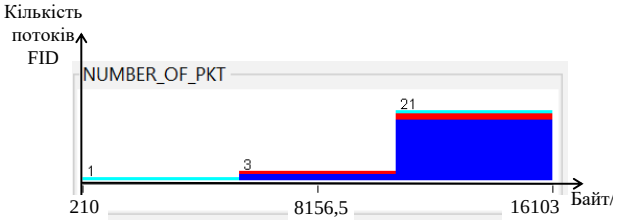
Таблиця 1 – Фрагмент даних датасету вебтрафіку HTTP/HTTPS-запитів

| Ідентифікатор мережевого потоку FID | Середній розмір HTTP/HTTPS-запитів PKT_SIZE, байт | Інтенсивність трафіку PKT_RATE, байт/с | Загальний обсяг переданих даних NUMBER_OF_BYTE, байт |
|---|---|---|---|
| FID 1 | 65535.0 | 1 519 660 | 13 762 400 |
| FID 2 | 55.0 | 18 056 | 1 770 010 |
| FID 3 | 797.5 | 261 790 | 25 665 105 |
| FID 4 | 797.5 | 261 772 | 25 665 105 |
| FID 5 | 1540.0 | 505 455 | 24 780 100 |

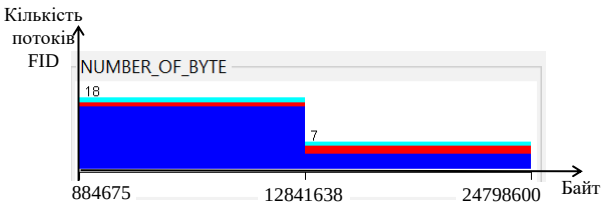
Для класифікації характеристик вебтрафіку, які задані в табл. 1, використано програмне середовище Weka 3.8.6 [9], результати аналізу характеристик вебтрафіку наведені на рис. 1. Аналіз значень інтенсивності трафіку PKT_RATE та BYTE_RATE та показника UTILIZATION дозволяє зробити висновки про наявність показових ознак, до яких відносяться пікові значення інтенсивності (наприклад, FID 1 та FID 5), створені HTTP/HTTPS-запитами.




а) середній розмір пакета PKT_SIZE




б) інтенсивність трафіку PKT_RATE




в) загальний обсяг переданих даних NUMBER_OF_BYTE

*Рисунок 1 – Результати аналізу вебтрафіку за допомогою Weka 3.8.6*

Для вирішення завдання класифікації вебтрафіку використаємо методи машинного навчання – метод k-найближчих сусідів kNN (k-nearest neighbour) та Байєсівський метод [10]. Метод k-найближчих сусідів виконує класифікацію для двох класів вебтрафіку, нормального та аномального, тоді множина класів має вигляд $H = \{H_0; H_1\}$, де $H_0$ – належність вебтрафіку до класу нормального (еталонного) трафіку HTTP/HTTPS-запитів, а $H_1$ – належність вебтрафіку до класу аномального (шкідливого) трафіку HTTP/HTTPS-запитів. Кожен зразок вебтрафіку описується вектором характеристик $a = (a_1, a_2, \ldots, a_n)$, де $N$ – кількість характеристик HTTP/HTTPS-запитів. Відстань $d(u,x_j)$ між тестовим зразком $u$ та $j$-тим навчальним зразком $x_j$ визначається як [10]:

$$d(u,a_j) = \sqrt{\sum_{i=1}^{N} (u_i - a_{j,i})^2},$$

(1)

де $u_i = (u_{1,i}, u_{2,i}, \ldots, u_{N,i})$ – $i$-та характеристика тестового зразка, $a_i = (a_{1,i}, a_{2,i}, \ldots, a_{N,i})$ – $i$-та характеристика $j$-того навчального зразка.

Клас, до якого належить тестовий зразок $u$, визначається за правилом зваженого голосування серед k-найближчих сусідів:

$$a(u) = \arg\min_{c \in C} \sum_{j \in N_k^c(u)} \omega(j,u)\ d(u,x_j), \qquad (2)$$

де $H$ – множина класів, $N_k^c(u)$ – множина k-найближчих сусідів класу $H$, $\omega(j,u)$ – вагова функція $j$-го сусіда, де $\omega(j,u)=[j \le k]$.

Байєсівський метод класифікації використовує формулу Байєса, яка дозволяє обчислити апостеріорну ймовірність належності трафіку до нормального (еталонного) або аномального (шкідливого) вебтрафіку HTTP/HTTPS-запитів за наявними характеристиками вебтрафіку [10]:

$$P(H_i / A) = \frac{P(H_i)P(A/H_i)}{\sum_{k=1}^{N} P(H_k)P(A/H_k)}, \; i = 1,2, \qquad (3)$$

де $H_i$ – гіпотеза про належність вебтрафіку до $i$-го класу, $i$ = 1,2; $N$ – кількість характеристик вебтрафіку; $a$ = ($a_1$, $a_2$, …, $a_N$) – вектор характеристик трафіку HTTP/HTTPS-запитів, який може включати інтенсивності трафіку, середній час затримки HTTP/HTTPS-запитів, загальну кількість HTTP/HTTPS-запитів, тощо; $P(H_i)$ – апріорна ймовірність класу вебтрафіку $H_i$, $i$=1,2, де $H_0$ – належність вебтрафіку до класу нормального (еталонного) трафіку HTTP/HTTPS-запитів, а $H_1$ – належність вебтрафіку до класу аномального (шкідливого) трафіку HTTP/HTTPS-запитів; $P(A/H_i)$ – умовна ймовірність спостереження вектора характеристик трафіку A за умови нормального чи аномального вебтрафіку за умови належності характеристикам трафіку до класу $H_i$; $P(H_i / A)$ – апостеріорна ймовірність належності вебтрафіку до класу $H_i$.

Для визначення класу трафіку використовується вираз:

$$\arg \max_i P(H_i / A), \qquad (4)$$

тобто, вебтрафік HTTP/HTTPS-запитів відноситься до того класу, для якого апостеріорна ймовірність є максимальна.

**Висновки.** Отримані значення класифікації вебтрафіку до нормального (еталонного) або аномального (шкідливого) вебтрафіку HTTP/HTTPS-запитів з використанням методу k-найближчих сусідів kNN (k-nearest neighbour) та Байєсівського методу дозволяють виконати оцінку похибок та бути використаними в системах моніторингу та раннього попередження аномалій, спричинених DDoS-атаками або мережевими аномаліями вебресурсів.

## Література


1. Стрелковська І.В., Соловська І.М., Стрелковська Ю.О. Детектування Flood-трафіку кібератак на Веб-сервери. Детектування Flood-трафіку кібератак на Веб-сервери. Measuring and computing devices in technological processes, 84(4), 203-210.
2. Strelkovskaya I., Solovskaya I., Strelkovska J. Detection of cyberattack flood traffic using spline approximation. Scientific achievements of contemporary society. Proceedings of the 4th International scientific and practical conference. Cognum Publishing House. London, United Kingdom. 2024. pp. 21-27.
3. Strelkovskaya I., Kivalov S. «Detection and prediction of DDoS cyber attacks using spline functions», IEEE TCSET 2022: 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, February 22-26, 2022. – P. 710-713.
4. Підгорний, П. (2024). Аналітичний огляд моделей і систем класифікації мережевого трафіку. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 155-169.
5. T. Radivilova, L. Kirichenko, O. Lemeshko and all, "Analysis of anomaly detection and identification methods in 5G traffic," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2021.
6. Петляк Н. Аналіз моделей виявлення аномалій трафіку в сучасних інформаційно-комунікаційних системах та мережах. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». – 2025. – Вип. 1, С. 180-186.
7. Ветлицька, О. С., Треньова, К. О. (2024). Виявлення атак у мережах Інтернету речей методами машинного навчання. Сучасний захист інформації, 1(57), 39–49.
8. Набори датасет для дослідження Kaggle: https://www.kaggle.com
9. Програмне забезпечення для машинного навчання Weka: https://ml.cms.waikato.ac.nz/weka/
10. Strelkovskaya I., Solovskaya I. and Strelkovska J. Comparative analysis of local positioning methods in Wi-Fi/Indoor networks. Proceedings of International Conference on Applied Innovations in IT (ICAIIT-2023), Vol. 11, Is. 1, Koethen, Germany, March, 9, 2023. – Anhalt University of Applied Sciences. – pp. 31-35.