МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ATICE'2025)

ОДЕСА, УКРАЇНА, 18 ЛИПНЯ 2025 Р.

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

ОДЕСА

2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

INTERNATIONAL HUMANITARIAN UNIVERSITY

INTERNATIONAL CONFERENCE

ADVANCED TECHNOLOGY IN INFORMATION AND COMMUNICATION ENGINEERING

(ATICE'2025)

ODESA, UKRAINE, JULY 18, 2025

CONFERENCE PROCEEDINGS

ODESA

2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

Одеса, Україна, 18 липня 2025 р.

Видавничий дім
«Гельветика»
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL HUMANITARIAN UNIVERSITY

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2025)

Odesa, Ukraine, July 18, 2025

Conference Proceedings

Видавничий дім
«Гельветика»
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025)

Одеса, Україна, 18 липня 2025 р.

Матеріали конференції

Видавничий дім
«Гельветика»
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings. Odesa : International humanitarian university, 2025, 123 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції. Міжнародний гуманітарний університет, 2025. – Одеса: Видавничий дім «Гельветика», 2025. – 123 с.

ISBN 978-617-554-582-9

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний 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

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний 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.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

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

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

РУСУ О.П. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.

ЙОНА Л.Г. – к.т.н., доц., Міжнародний гуманітарний університет, Одеса, Україна.

МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.

ПЕДЯШ В.В. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КУЧАЙ О.В. - д.п.н., проф., Національний університет біоресурсів і природокористування України.

ЖИГУЛІН О.А. – д.е.н., проф., Міжнародний гуманітарний університет, Одеса, Україна

ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

УДК 004.738.5:004.8

Стрелковська І.В., д.т.н., професор,
Міжнародний гуманітарний університет,
i.strelkovskaya@mgu.edu.ua
Соловська І.М., к.т.н., доцент,
Міжнародний гуманітарний університет,
i.solovskaya@mgu.edu.ua,
Стрелковська Ю.О., к.ю.н., доцент
Worthing college
4800632s@gmail.com
Костенко М.О., магістр 2 року навчання,
Міжнародний гуманітарний університет,
kostenko.web.dev@gmail.com

ДЕТЕКТУВАННЯ ТРАФІКУ DDoS-АТАКИ НА ВЕБ-СЕРВЕРИ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ

Анотація: *Розглянуто задачу детектування трафіку DDoS-атак (HTTP GET-flood, HTTP POST-flood), які спрямовані на суттєве перевантаження Веб-серверів. Встановлено, що для детектування трафіку DDoS-атак прикладного рівня L7 доцільним є використанням машинного навчання. Запропоновано використання сплайн-апроксимації на базі кубічних сплайнів для детектування сегментів з аномальними сплесками та коливаннями трафіку, з подальшою класифікацією легітимного та шкідливого DDoS-трафіку за допомогою методу k-найближчих сусідів KNN. Розроблений підхід дозволяє детектувати DDoS-трафік та прийняти рішення щодо зміни стратегії керування мережним трафіком в реальному часі.*

Ключові слова: детектування, DDoS-атака, DDoS-трафік, HTTP GET-flood, HTTP POST-flood, сплайн-апроксимація, машинне навчання, легітимний трафік, шкідливий трафік, метод k-найближчих сусідів KNN

Важливим завданням забезпечення безпеки функціональності Веб-серверів від атак відмови в обслуговуванні DDoS (Distributed Denial of Service Attack) є детектування початку DDoS-атаки, пов'язане зі зростанням інтенсивності запитів, наприклад, HTTP GET-flood та HTTP POST-flood, значним перевантаженням та неможливостями доступу до Веб-серверів. Відомо [1-2], що процес детектування трафіку DDoS-атаки може бути виконаний за допомогою аналізу «сигнатур» або аномалій шкідливого трафіку, використовуючи «сигнатури» шкідливого трафіку або визначаючи аномалії трафіку, які виникають за рахунок різкого збільшення інтенсивності надходження запитів відмінне від визначених порогових значень характеристик легітимного трафіку. Удосконалення механізмів та збільшення масштабів DDoS-атак часто ускладнює вищезазначені завдання та потребує пошуку нових підходів до детектування DDoS-трафіку. Таким рішенням може бути використання підходу на базі сплайн-апроксимації з використанням кубічних сплайнів для детектування сегментів з аномальними сплесками та коливаннями трафіку, з подальшою класифікацією легітимного та шкідливого DDoS-трафіку за допомогою методу k-найближчих сусідів KNN.

Використання сплайн-апроксимації для вирішення завдань оцінки характеристик трафіку запропоновано авторами в роботах [1-2], а підхід щодо класифікації трафіку на основі алгоритмів машинного навчання розглянуто в роботах [3-5], де автори пропонують

виявлення аномалій DDoS-трафіку на основі різних методів, таких як, логістична регресія, метод опорних векторів та дерева рішень, метод k-найближчих сусідів KNN. Такий підхід до класифікації дозволяє з різним ступенем точності класифікувати легітимний та шкідливий трафік, адаптуватися до змін у мережному трафіку і виявляти DDoS-атаки у реальному часі. Робота [6] присвячена порівнянню результатів використання машинного навчання для визначення аномалій DDoS-трафіку, встановлено, що доцільним є використання машинного навчання у поєднанні з іншими підходами, такими як нечітка логіка, статистичний аналіз, генетичні алгоритми та інші.

В даній роботі запропоновано альтернативне до вищерозглянутих рішень, яке базується на використанні сплайн-апроксимації для детектування DDoS-трафіку та дозволяє на першому етапі визначити сегменти з аномальними сплесками та коливаннями трафіку, а на другому, за допомогою методу класифікації k-найближчих сусідів KNN виконати класифікацію легітимного та шкідливого DDoS-трафіку.

Метою даної роботи є детектування DDoS-трафіку на Веб-сервери з використанням сплайн-апроксимації на базі кубічних сплайнів та подальшої класифікації легітимного та шкідливого трафіку за допомогою методу k-найближчих сусідів KNN.

Розглянемо перший етап детектування DDoS-атаки на прикладі HTTP GET-flood та HTTP POST-flood запитів до Веб-сервера. DDoS-атака HTTP-Flood прикладного рівня L7 моделі OSI спрямована безпосередньо на Веб-сервери та сервери Веб-додатків, яка виконує переповнення Веб-серверу значною кількістю HTTP-запитів, що робить його нездатним обробляти легітимні запити користувачів. Виконаємо детектування шкідливого HTTP GET-flood трафіку за допомогою сплайн-апроксимації на базі кубічних сплайн-функцій, використовуючи [7], передбачаючи, що завданням детектування є виявлення аномалій та коливань трафіку. В якості вихідного легітимного та шкідливого Flood-трафіку використаємо DataSet трафіку HTTP GET-flood [8], що показано на рис. 1. Використаємо кубічний сплайн для HTTP GET-flood трафіку, показаного на рис. 1 на проміжку [1000;1500].

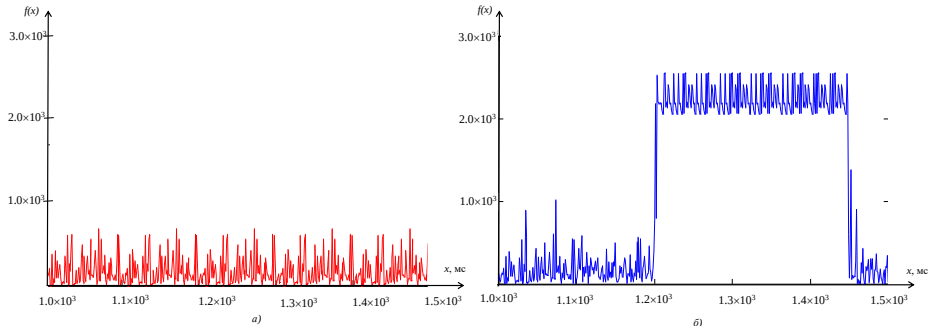

Рисунок 1 – Легітимний трафік (*а*) та шкідливий HTTP GET-flood трафік DDoS-атаки (*б*)

Нехай на відрізку [0;T] задані значення Flood-трафіку DDoS-атаки *f*(*x*). Розіб'ємо цей відрізок [0;T] точками Δ: $0 = x_0 < x_1 < ... < x_N = T$ на проміжки [x_i; x_{i+1}], $i = \overline{0, N-1}$, на кожному з яких побудуємо кубічний сплайн $S_3(f;x)$, який задовольняє умовам [9]

$$S_3(f;x_i) = f_i,\ i = 0,\ 1\ \ ...\ \ N,\ \ S''(f;0) = f''(0),\ S''(f;T) = f''(T). \qquad (1)$$

Згідно [9], інтерполяційний кубічний сплайн *S*3(*f*; *x*) відповідає умовам:

$$S_3(x_i) = S_i,\ S_3(x_{i+1}) = S_{i+1},\ i = \overline{0, N-1}, \tag{2}$$

де на кожному з відрізків $[x_i; x_{i+1}]$, $i = \overline{0, N-1}$ є многочленом третього ступеня, причому на відрізку [0;T] $S_3(f; x)$ має неперервність других похідних. Позначимо $S_3''(x_i) = M_i,\ S_3''(x_{i+1}) = M_{i+1},\ S_3''(x_0) = M_0,\ S_3''(x_1) = M_1$.

Тоді кубічний сплайн $S_3(f; x)$ має вигляд:

$$S_3(f; x) = f_i(1-t) + f_{i+1}t - \frac{h_i^2}{6}t(1-t)\left[(2-t)M_i + (1+t)M_{i+1}\right],\ x \in [x_i, x_{i+1}],\ i = \overline{0, N-1}, \tag{3}$$

де $h_i = x_{i+1} - x_i,\ t = (x - x_i)/h_i$.

Розглянемо трафік на проміжку [1000;1500] мс (рис. 1), задавши рівномірну сітку розбиття та крок детектування Δ = 10 мс. Легітимний трафік має вигляд рис. 1,*а*, трафік DDoS-атаки HTTP GET-flood показаний трасою рис. 1,*б*, на проміжку [1200;1210] мс відбувся різкий сплеск інтенсивності HTTP GET запитів, кількість яких є понад 2.5×10^3, при цьому така аномальність зберігається на проміжку часу [1200;1450] мс.

Для детектування використовуємо сплайн-апроксимацію на базі кубічних сплайн-функцій, яка дозволяє на першому етапі визначити аномалії інтенсивності надходження шкідливих HTTP GET-запитів у заданих вузлах інтерполяції. Легітимний трафік HTTP GET-запитів, показано на рис. 1,*а*, має рівномірну структуру та помірні сплески інтенсивності запитів, які становлять від 0.3×10^3 до 0.9×10^3. На першому етапі детектування, використовуючи кубічний сплайн вигляду (3) та умови (1-2), отримаємо сплайн-апроксимацію на базі кубічної сплайн-функції детектування трафіку HTTP GET-flood, фрагмент якої показано на рис. 2.

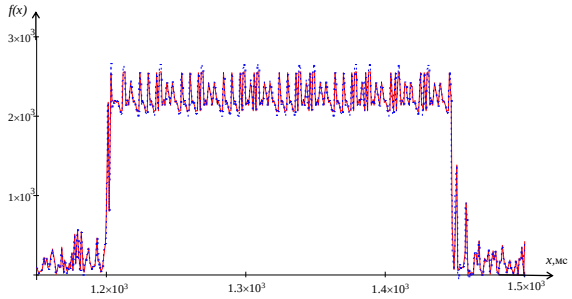

Рисунок 2 – Сплайн-апроксимація HTTP GET DDoS-трафіку на відрізку [1200;1500] мс

Другий етап детектування відбувається шляхом класифікації трафіку, як легітимного та шкідливого трафіку, за допомогою методу k-найближчих сусідів [10], який використовується для пошуку подібності між наявними значеннями легітимного та шкідливого DDoS-трафіку на базі метрики Евкліда, відстані $d_{Euclidean}$ між заданими значеннями легітимного та шкідливого трафіку:

$$d_{Euclidean} = \sqrt{\sum_{i=1}^{n}(x_{i,j} - y_{i,j})^2}, \tag{4}$$

де $x_{i,j}$ – поточне значення інтенсивності легітимного трафіку, $y_{i,j}$ – значення інтенсивності шкідливого трафіку HTTP GET-запитів, n – кількість вимірів.

Для класифікації використано програмне забезпечення машинного навчання Weka 3.8.6 [11] в якому проведено навчання, валідація та тестування методу k-найближчих сусідів для класифікації DDoS-трафіку. Отримані результати зведено в табл. 1.

Таблиця 1– Результати класифікації легітимного та шкідливого трафіку на основі методу k-найближчих сусідів

Метод	Коефіцієнт кореляції	Середня абсолютна похибка	Середньоквадратична помилка	Відносно-абсолютна похибка	Відносно-квадратична помилка кореня
k-найближчих сусідів	0,968	186,75	227,27	23,94 %	32,75 %

Для визначення точності результатів класифікації трафіку використаємо значення середньої абсолютної похибки MSE (Mean Squared Error) [10]:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\sqrt{(x_{est} - x_{real})^2 + (y_{est} - y_{real})^2}, \quad (5)$$

де x_{est}, y_{est} – значення інтенсивності шкідливого трафіку HTTP GET-запитів, визначені в ході експерименту; x_{real}, y_{real} – значення інтенсивностей легітимного трафіку, L – кількість значень.

Отримані результати розрахунку середньої абсолютної похибки MSE класифікації трафіку зведені в табл. 2.

Таблиця 2 – Визначення середньої абсолютної похибки MAPE класифікації трафіку

Значення середньої абсолютної похибки MSE	Legal traffic	HTTP GET
Класифікатор k-найближчих сусідів	43,2%	52,3%

Висновки

1. Розглянуто трафік DDoS-атаки на базі Flood-трафіку (HTTP GET-flood, HTTP POST-flood), який спрямовано на суттєве перевантаження Веб-ресурсів. Встановлено, що для детектування трафіку DDoS-атак доцільним є використання методів машинного навчання.

2. Запропоновано використання сплайн-апроксимації на базі кубічних сплайнів для детектування сегментів з аномальними сплесками та коливаннями трафіку з подальшою класифікацією легітимного та шкідливого DDoS-трафіку за допомогою методу k-найближчих сусідів KNN.

3. Розроблений підхід дозволяє детектувати DDoS-трафік та прийняти рішення щодо зміни стратегії керування мережним трафіком в реальному часі.

Література

1. 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.

2. 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.

3. Ветлицька, О. С., Треньова, К. О. (2024). Виявлення атак у мережах Інтернету речей методами машинного навчання. Сучасний захист інформації, 1(57), 39–49.

4. P.D. Bojovi, I. Basicevi, S. Ocovaj, M. Popovic (2019) A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method. Computers & Electrical Engineering 73 (2019): 84-96.

5. Imran, Jamil F., Kim D. An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments. Sustainability. – 2021. – Vol. 13, no. 10057.

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. Strelkovskaya I., Solovskaya I., Strelkovska J. Spline-Approximпation and Spline-Extrapolation Methods in Telecommunication Problems, Current Trends in Communication and Information Technologies. IPF 2020. Lecture Notes in Networks and Systems. Vol. 212, Springer, Cham, 2021, P. 3-22.

8. https://www.kaggle.com

9. Ahlberg J.H., Nilson E.N., Walsh J.L. The Theory of Splines and Their Applications, Academic Press, New York, 1967.

10. Strelkovskaya I., Solovskaya I., Strelkovskaya J., Paskalenko V. Complex spline approximation in positioning problems. Radioelectronics and Communications Systems. 2022. Vol. 65 (7). P. 376–385.

11. https://ml.cms.waikato.ac.nz/weka/

УДК 004.942

Стрелковська І.В., д.т.н., професор,
Міжнародний гуманітарний університет,
i.strelkovskaya@mgu.edu.ua
Соловська І.М., к.т.н., доцент,
Міжнародний гуманітарний університет,
i.solovskaya@mgu.edu.ua,
Стрелковська Ю.О., к.ю.н., доцент
Worthing college
4800632s@gmail.com
Кольцов В.В., магістр 2 року навчання,
Міжнародний гуманітарний університет,
vladkoltsov@ukr.net

СПЛАЙН-АПРОКСИМАЦІЯ В ЗАДАЧАХ ВІЗУАЛІЗАЦІЇ ТА РЕНДЕРИНГУ 3D-ОБ'ЄКТІВ

Анотація: *Розглянуто задачу підвищення точності візуалізації та рендерингу 3D-об'єктів за допомогою сплайн-апроксимації. Запропоновано використання інтерполяційного параметричного сплайну в процесі моделювання кривих та поверхонь 3D-об'єкту у процедурі візуалізації та рендерингу. Встановлено, що застосування інтерполяційного параметричного кубічного сплайну забезпечує зниження обчислювальної складності, масштабованість рішень і суттєво спрощує процес моделювання.*

Ключові слова: сплайн-апроксимація, 3D-моделювання, 3D-модель, візуалізація, рендеринг, інтерполяційний параметричний сплайн, точність, похибка