https://doi.org/10.31891/2219-9365-2025-84-22
УДК 004.946:519.65

СТРЕЛКОВСЬКА Ірина
Міжнародний гуманітарний університет
https://orcid.org/0000-0002-1813-0554
e-mail: i.strelkovskaya@mgu.edu.ua
СОЛОВСЬКА Ірина
Міжнародний гуманітарний університет
https://orcid.org/0000-0002-9904-5692
e-mail: i.solovskaya@mgu.edu.ua
СТРЕЛКОВСЬКА Юлія
Worthing college
https://orcid.org/0000-0002-9835-0222
e-mail: 4800632s@gmail.com

ДЕТЕКТУВАННЯ ТРАФІКУ DDoS-АТАК НА ВЕБ-СЕРВЕРИ

Розглянуто задачу детектування DDoS-атаки на базі Flood-трафіку (SYN-Flood, UDP-Flood та HTTP-flood), яка спрямована на суттєве перевантаження Веб-ресурсів. Встановлено, що для детектування трафіку DDoS-атаки є доцільним використання результатів моніторингу та аналізу трафіку пошуком аномалій спричинених шкідливим трафіком. Запропоновано детектування шкідливого Flood-трафіку DDoS-атак за допомогою сплайн-апроксимації на базі кубічних сплайн-функцій з подальшою класифікацією легітимного та шкідливого трафіку за допомогою методу машинного навчання k-найближчих сусідів. Розроблений підхід дозволяє детектувати Flood-трафік та прийняти рішення щодо зміни стратегії керування мережним трафіком Веб-ресурсів під час DDoS-атаки.

Ключові слова: детектування, Веб-ресурс, Flood-трафік, DDoS-атака, SYN-Flood, UDP-Flood, HTPP-Flood, сплайн-апроксимація, кубічна сплайн-функція, методи машинного навчання, метод k-найближчих сусідів

STRELKOVSKAYA Irina, SOLOVSKAYA Irina
International Humanitarian University
STRELKOVSKA Juliya
Worthing college

DETECTION OF DDoS ATTACK TRAFFIC ON WEB SERVERS

The paper addresses the problem of detecting DDoS (Distributed Denial of Service) attacks based on Flood traffic, including SYN-Flood, UDP-Flood, and HTTP-Flood types, which aim to overload and disable web resources. It is established that efficient DDoS detection can be achieved through continuous traffic monitoring and anomaly analysis caused by malicious flows. A novel approach is proposed for detecting harmful Flood traffic using spline approximation based on cubic spline functions, followed by the classification of legitimate and malicious traffic via the k-nearest neighbors (k-NN) machine learning algorithm. This method allows accurate detection of the onset of DDoS attacks and supports timely decision-making to modify network traffic control strategies during an attack.

The study analyzes HTTP(S) GET-Flood attacks at the application (L7) layer, which overwhelm web servers with numerous HTTP requests, making them unable to process legitimate user connections. Using cubic spline interpolation, traffic anomalies are detected through intensity spikes within specific time intervals. The proposed spline-based approximation identifies abrupt traffic surges corresponding to the start of DDoS activity. The subsequent classification stage, implemented in the Weka 3.8.6 environment using k-NN, achieves a correlation coefficient of 0.88, with mean absolute and root mean square errors confirming high detection accuracy.

Experimental results show that the mean absolute error (MSE) of classification equals 21.7% for legitimate traffic and 14.7% for malicious HTTP GET requests, proving the efficiency of the proposed two-stage detection model. The spline-based DDoS detection combined with k-NN classification provides an effective and computationally efficient mechanism for real-time recognition of Flood-based cyberattacks and enhances network resilience by supporting adaptive traffic management strategies.

Keywords: detection, web resource, Flood traffic, DDoS attack, SYN-Flood, UDP-Flood, HTTP-Flood, spline approximation, cubic spline function, machine learning, k-nearest neighbors.

Стаття надійшла до редакції / Received 07.11.2025
Прийнята до друку / Accepted 02.12.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Важливим завданням забезпечення безпеки мережної інфраструктури від різного виду кібератак є підтримка функціональності Веб-ресурсів та захист даних. Серед кібератак, слід виділити атаки, що призводять до відмови в обслуговуванні DDoS (Distributed Denial of Service Attack) та характеризуються відправкою потоку запитів SYN-Flood, UDP-Flood, TCP-Flood та HTTP-Flood до Веб-серверів та Веб-ресурсів, що призводить до перевантаження та неможливості досупу користувачів до Веб-ресурсу. В такому випадку важливим питанням є визначення моменту початку DDoS-атаки та зміни стратегії щодо керування мережним

трафіком.

В цілому, DDoS-атаки різних різновидів флудів SYN-Flood, UDP-Flood, TCP-Flood та HTTP-Flood характеризуються різким зростанням інтенсивності трафіку, збільшенням кількості запитів різного виду та значним перевантаженням Веб-ресурсів мережі (рис. 1). Частіше DDoS-атаки відбуваються на рівнях L3, L4 та L7 моделі OSI (Open Systems Interconnection), причому на канальному рівні – UDP-Flood, ICMP-Flood переважно генерують значний обсяг трафіку, на транспортному рівні – атаки на протоколи SYN-Flood та Ping of Death, DDoS-атаки на прикладному рівні – HTTP-Flood та Slowloris зазвичай складно ідентифікуються та є найбільш руйнівними [1-2].

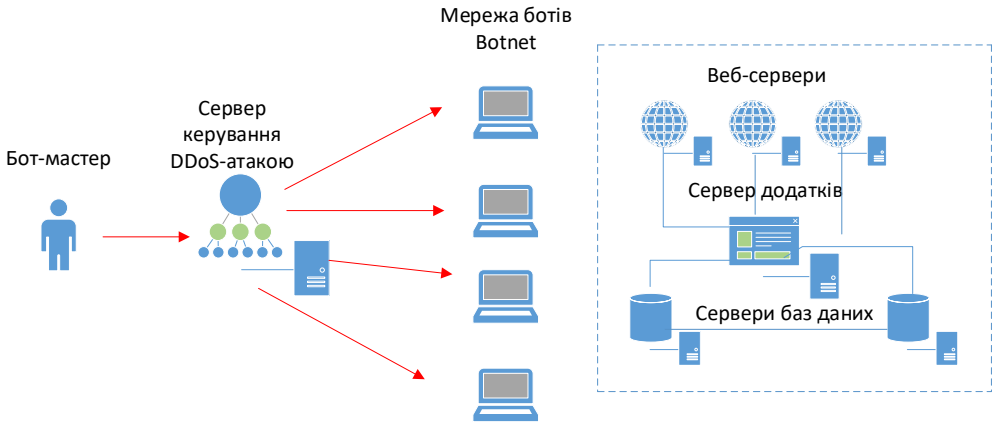

Рис. 1. Кібератака DDoS – відмова в обслуговуванні

Забезпечення безпеки мережної інфраструктури від DDoS-атак канального L3 та транспортного L4 рівнів може виконуватися в залежності від хостингу Веб-ресурсів, налаштувань брандмауера та його відкритих портів, політик міжмережних екранів фільтрування трафіку та налаштувань щодо списків доступу з врахуванням адрес відправників, протоколів та сервісів.

Важливим завданням щодо протидії DDoS-атак є своєчасність виявлення Flood-трафіку засобами моніторингу мережі та впровадження стратегії керування мережим трафіком, балансування навантаження та фільтрування трафіку, використання системи виявлення вторгнень і брандмауерів Веб-додатків.

Шкідливий трафік DDoS-атаки прикладного L7 рівня зазвичай важче відрізнити від легітимного через їхню подібність, окрім того поява нових різновидів таких атак теж ускладнює цю задачу.

Відомо [1-2], що процес детектування аномалій Flood-трафіку DDoS-атаки може бути виконаний за допомогою двох підходів. Перший – ґрунтується на аналізі «сигнатур» трафіку, шаблонів легітимного або шкідливого Flood-трафіку, які визначають DDoS-атаку, шляхом порівняння досліджених характеристик легітимного трафіку з характеристиками шкідливого Flood-трафіку. Однак, такий підхід потребує наявності бази даних «сигнатур» шкідливого Flood-трафіку, а виявлення Flood-трафіку може бути зовсім неефективним при виявленні нових або модифікованих типів DDoS-атак. Іншим підходом до детектування аномалій Flood-трафіку DDoS-атаки є виявлення шкідливого Flood-трафіку на основі аномалій, коли поточний стан обслуговування трафіку фіксує аномалію характеристик трафіку, наприклад, різке збільшення інтенсивності трафіку. В такому випадку детектування передбачає визначення поточних характеристик легітимного трафіку з подальшим пошуком аномалій у його структурі. Алгоритм детектування Flood-трафіка DDoS-атаки з визначенням аномалій показано на рис. 2.

Удосконалення механізмів та збільшення масштабів DDoS-атак часто ускладнює завдання визначення аномалій Flood-трафіку та потребує пошуку нових підходів до детектування шкідливого трафіку. З огляду на те, що системи моніторингу та аналізу трафіку використовують підхід заснований на аналізі характеристик трафіку та виявленні його аномалій, дослідження характеристик Flood-трафіку з детектуванням моменту початку DDoS-атаки та визначенням шкідливого трафіку, є актуальним.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою даної роботи є детектування шкідливого Flood-трафіку кібератаки DDoS за допомогою сплайн-апроксимації з використанням кубічних сплайн-функцій з подальшою класифікацією трафіку методом машинного навчання k-найближчих сусідів для підвищення точності визначення початку кібератаки.

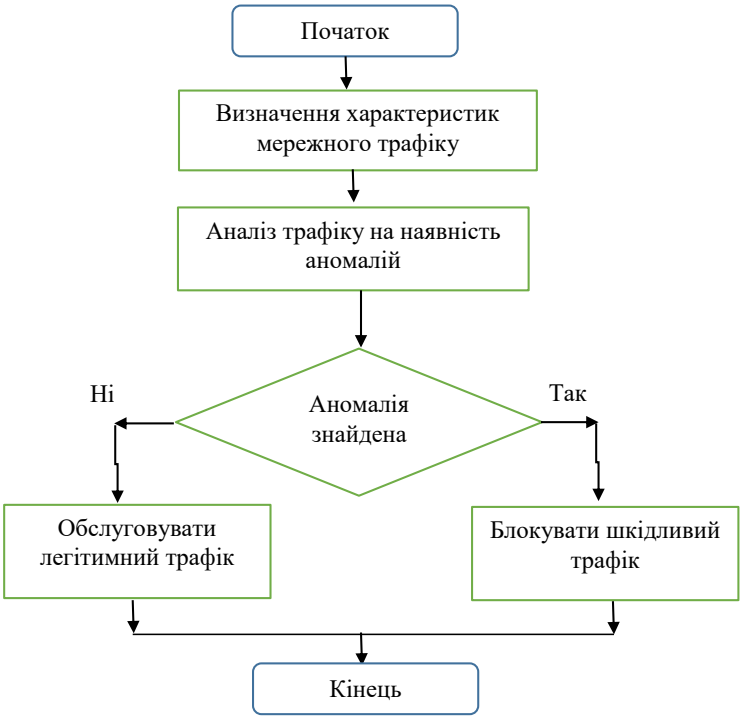

Рис. 2. Алгоритм виявлення аномалій Flood-трафіку DDoS-атак

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Дослідження аномалій Flood-трафіку розглянуто в роботах багатьох авторів, зокрема, в роботі [4] для визначення аномалій Flood-трафіку запропоновано використання статистичних методів дослідження, шляхом визначення коефіцієнта Херста, коефіцієнта авторегресії та коефіцієнта варіації, які формують метрики DDoS-атаки на часовому відрізку. Перевагою використання таких метрик є відповідна точність, простота в обчисленні та реалізації в програмному забезпеченні. В роботі [5] авторами запропоновано використання класифікаторів для детектування аномалій мережного трафіку, що пов'язані з DDoS-атаками, використання методу ковзних середніх, показане в роботі [6], дозволяє детектувати Flood-трафік в моменти максимальних значень швидкості зміни значення ковзного середнього, що відповідає початку та закінченню DDoS-атаки. Використання методів нейронних мереж в роботі [7] дозволяє за допомогою згорткових та рекурентних моделей значно підвищивши точність виявлення аномалій шкідливого DDoS-трафіку. Автори в роботі [8] пропонують модель виявлення аномалій на основі поєднання автоматизованого машинного навчання з алгоритмами фільтра Калмана, шляхом пошуку архітектури нейронної мережі для створення моделей глибокого навчання, що дозволяє адаптуватися до змін у мережному трафіку і виявляти DDoS-атаки у реальному часі. Робота [9] присвячена порівнянню методів машинного навчання для визначення аномалій трафіку DDoS-атак, доведено, що доцільним є використання машинного навчання у поєднанні з іншими підходами, такими як нечітка логіка, сигнатурний аналіз, генетичні алгоритми та автокодери.

Альтернативним до вищерозглянутих рішень є отримані раніше авторами в роботах [1-2] та [10-11] результати вирішення завдань оцінки характеристик та оцінки станів даних, сигналів та трафіку за допомогою сплайн-апроксимації. Використання сплайн-апроксимації для детектування Flood-трафіку DDoS-атак дозволить на першому етапі виконати визначення моменту початку DDoS-атаки із необхідною точністю, а на другому етапі за допомогою методу машинного навчання k-найближчих сусідів виконати класифікацію легітимного та шкідливого трафіку.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Розглянемо детектування моменту початку DDoS-атаки на Веб-ресурси на прикладі HTTP-Flood за допомогою сплайн-апроксимації з використанням кубічних сплайн-функцій.

DDoS-атака HTTP-Flood прикладного рівня L7 спрямована безпосередньо на Веб-сервери та сервери Веб-додатків (рис. 3) та виконує переповнення Веб-серверу величезною кількістю HTTP-запитів, що робить його нездатним обробляти легітимні запити користувачів. DDoS-атака на Веб-додаток, що допускає шифрування, може бути запущена поверх трафіку, зашифрованого SSL/TLS, що створює певні труднощі щодо її ідентифікації.

Більшість технологій протидії DoS атакам не здійснюють реальної перевірки трафіку SSL, оскільки це вимагає розшифрування зашифрованих даних. Веб-сервери взаємодіють з клієнтами на прикладному рівні

протоколом HTTP, який використовує простий текстовий формат та визначає спеціальну структуру для запиту і відповіді.

Відрізняють два види DDoS-атак HTTP-Flood [12]:

– HTTP(S) GET-flood, DDoS-атака прикладного рівня L7 моделі OSI, яка передбачає надсилання GET-запиту даних на Веб-сервері (файл, сторінку або скрипт) для відображення у Веб-браузері. При цьому мета HTTP(S) GET-flood переповнити Веб-сервер GET-запитами та унеможливити його функціонування.

– HTTP(S) POST-flood, DDoS-атака, яка передбачає розміщення даних в тілі POST-запиту для подальшої обробки на Веб-сервері. POST-запит кодує інформацію і відправляє на Веб-сервер, коли кількість POST-запитів переповнює Веб-сервер, що спричиняє аварійну зупинку сервера.

DDoS-атака виконується на базі мережі скомпрометованих систем – ботнетів. Керує мережею зловмисник, який ховається за кількома рівнями ботів, степінгстоунів, які приховують ідентифікацію. Зловмисник ініціює процес DDoS-атаки, розповсюджуючи HTTP(S) GET-flood або HTTP(S) POST-flood, які перевантажують пропускну спроможність Веб-серверу або Веб-ресурсу.

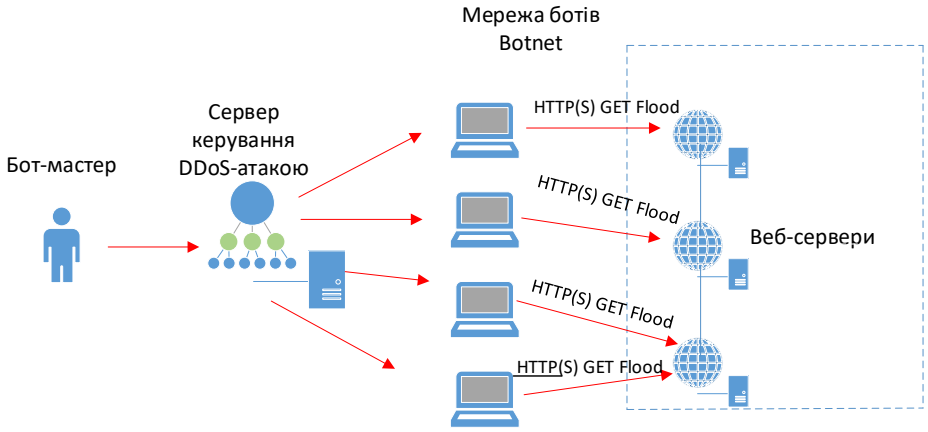

Рис. 3. DDoS-атака HTTP(S) GET-flood

Для обладнання захисту відрізнити зловмисні HTTP запити від легітимних є надзвичайно складною задачею, невірні методи чи налаштування призводять до великої кількості помилкових спрацювань.

В багатокроковому процесі захисту Веб-ресурсу, першим етапом є визначення моменту надходження початку DDoS-атаки HTTP(S) GET-flood в реальному масштабі часу. Для детектування тарфіку DDoS-атаки HTTP(S) GET-flood, яка надходить до Веб-серверу, виконуються наступні дії:

– аналіз інтенсивності потоку трафіку HTTP(S)-запитів;

– формування трас легітимного та HTTP(S) GET-flood трафіку DDoS-атаки;

– детектування аномалій трафіку HTTP(S)-запитів.

Розглянемо детектування шкідливого HTTP(S) GET-flood DDoS-атаки за допомогою сплайн-апроксимації на базі кубічних сплайн-функцій, використовуючи [10-11], передбачаючи, що завданням детектування буде виявлення аномалії трафіку. В якості вихідного легітимного та шкідливого Flood-трафіку використаємо трафік HTTP(S) GET-flood, який розміщено в Dataset/ddos-attack-network [13] та показано на рис. 4.

Розглянемо використання сплайн-апроксимації на базі кубічних сплайн-функцій. Використаємо кубічний сплайн $S_3(t)$ для детектування аномалій HTTP(S) GET-flood трафіку, показаного на рис. 4 на проміжку [1000;1500].

Нехай на відрізку [0;T] задані значення Flood-трафіку DDoS-атаки, а саме кількість N – запитів HTTP(S) GET-flood. Дані HTTP(S) GET-flood трафіку DDoS-атаки задані за допомогою Dataset/ddos-attack-network [13] та показані на рис. 4.

Розіб'ємо цей відрізок [0;T] точками Δ: $0 = t_0 < t_1 < \ldots < t_N = T$ на проміжки $[t_i; t_{i+1}]$, $i = \overline{0, N-1}$, на кожному з яких побудуємо многочлен третього ступеню [14]. В якості такого многочлену використаємо кубічну сплайн-функцію та отримаємо на проміжку [0;T] кусково-неперервну функцію, яка і буде визначати кубічний сплайн. Нехай на відрізку [0;T] у вузлах сітки Δ: задані значення функції $s_i = s(t_i), \quad i = \overline{0, N}$.

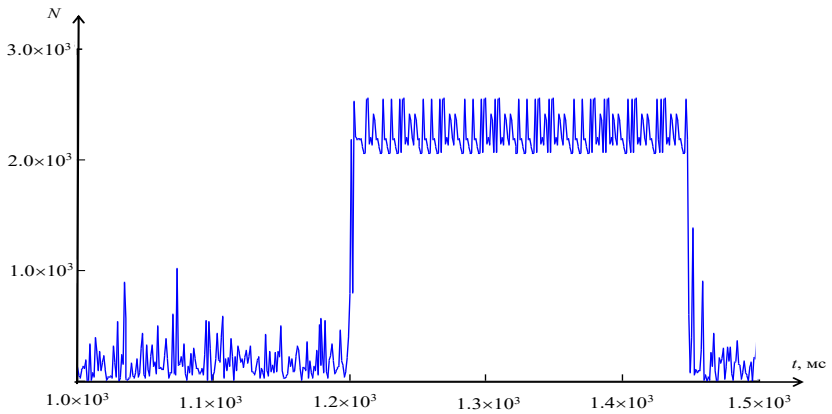

Рис. 4. HTTP(S) GET-flood трафік DDoS-атаки, отриманий за допомогою Dataset/ddos-attack-network [13]

Згідно [14], інтерполяційний кубічний сплайн $S_3(t_i)$ відповідає умовам:

$$S_3(t_i) = S_i, , i = \overline{0, N-1}, \quad (1)$$

– на кожному з відрізків $[t_i; t_{i+1}]$, $i = \overline{0, N-1}$ він є многочленом третього ступеню,

– на всьому відрізку [0;T] має неперервність других похідних $S_3''(t_i) = M_i$, $S_3''(t_{i+1}) = M_{i+1}, S_3''(t_0) = M_0 S_3''(t_1) = M_1$.

Тоді для $S_3(t)$:

$$S_3(t) = f_i(1-t) + f_{i+1}t - \frac{h_i^2}{6}t(1-t)[(2-t)M_i + (1+t)M_{i+1}], t \in [t_i, t_{i+1}], i = \overline{0, N-1}. \quad (2)$$

Розглянемо трафік на проміжку [1000;1500] мс (рис. 5), задавши рівномірну сітку розбиття та крок детектування Δ = 10 мс. Легітимний трафік має трасу вигляду рис. 5, *а*, трафік DDoS-атаки HTTP(S) GET-flood показаний трасою рис. 5, *б*, на проміжку [1200;1210] мс відбувся різкий сплеск інтенсивності HTTP(S) GET запитів, кількість яких становила понад 2.5×10^3.

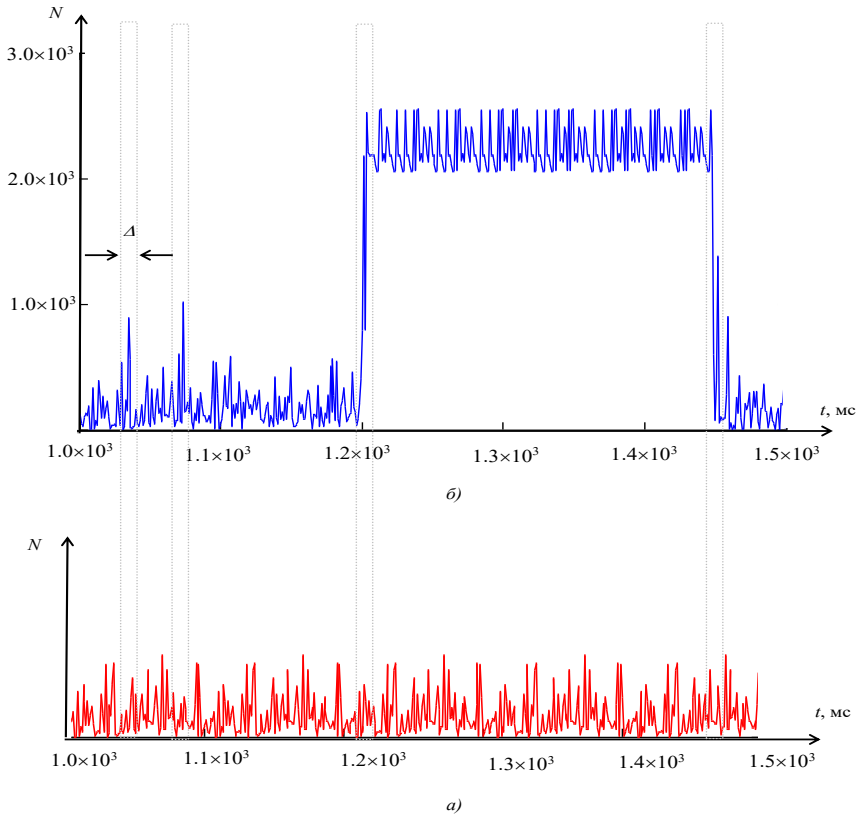

Рис. 5. Легітимний трафік (а) та HTTP(S) GET-flood трафік DDoS-атаки (б)

Для детектування використовуємо сплайн-апроксимацію на базі кубічних сплайн-функцій, яка дозволяє на першому етапі визначити аномалії інтенсивності надходження шкідливих HTTP(S) GET-запитів у заданих вузлах інтерполяції. Легітимний трафік HTTP(S) GET-запитів, показаний на рис. 5, *а*, має рівномірну структуру та помірні сплески інтенсивності запитів, які становлять $0.3\times10^3 – 0.9\times10^3$.

Шкідливий трафік HTTP(S) GET-flood має аномальний сплеск інтенсивності до 2.5×10^3 запитів, при цьому така аномальність зберігається протягом визначеного проміжку часу на проміжку [1200;1450] мс.

На першому етапі детектування, використовуючи кубічний сплайн вигляду (2) та умови (1), отримаємо сплайн-апроксимацію на базі кубічної сплайн-функції детектування трафіку HTTP(S) GET-flood, фрагмент якої показаний на рис. 6.

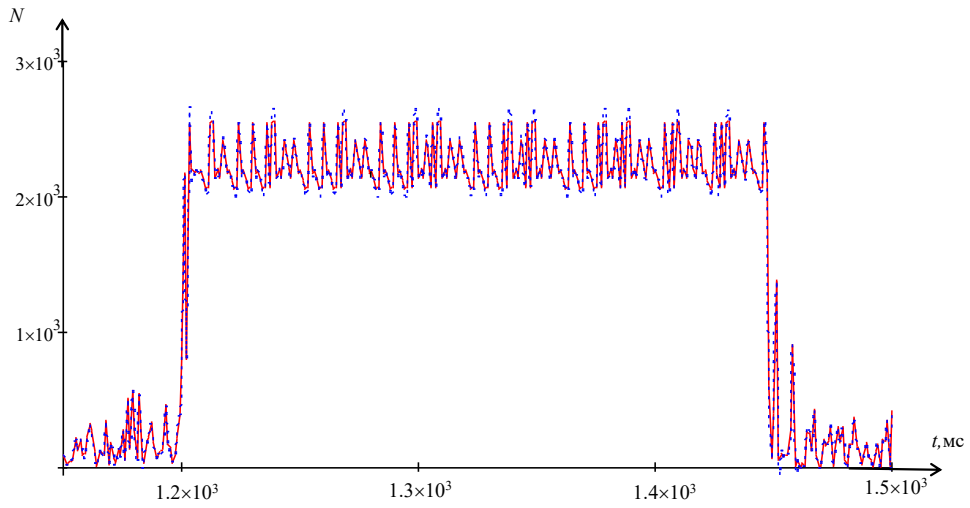

Рис. 6. Сплайн-апроксимація HTTP(S) GET-flood трафіку DDoS-атаки на базі кубічного сплайну на відрізку [1200; 1500] мс

Другий етап детектування відбувається шляхом класифікації трафіку, як легітимного та шкідливого трафіку, за допомогою методу k-найближчих сусідів [15], 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 [15]:

$$d_{Ecl} = \sqrt{\sum_{i=1}^{k}(x_{i,j} - y_{i,j})^2}, \tag{3}$$

де $x_{i,j}$ – поточне значення інтенсивності легітимного трафіку HTTP(S) GET-запитів,

$y_{i,j}$ – значення інтенсивності шкідливого трафіку HTTP(S) GET-запитів,

k – кількість кластерів.

Для класифікації легітимного та шкідливого трафіку, розглянутого на відрізку [1200;1500] мс (рис. 5) використано програмне забезпечення машинного навчання Weka 3.8.6 [17] в якому проведено навчання, валідація та тестування трафіку на базі методу k-найближчих сусідів. 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	Середньо квадратична помилка	Відносно-абсолютна похибка	Відносно-квадратична помилка кореня
k-найближчих сусідів	0,88	106,71	77,23	15,49 %	19,15 %

Отримані результати класифікації легітимного та шкідливого трафіку на основі методу k-найближчих сусідів дозволяють зробити висновок про те, що:

– значення коефіцієнту кореляції становить 0,88 та дозволяє стверджувати, що класифікація відображає характеристики легітимного та шкідливого трафіку;

– значення середньої абсолютної похибки та середньоквадратичної помилки є відносно невеликими та підтверджують достатню точність класифікації;

– підвищення точності класифікації можливо досягти за рахунок вибору значення k-кількості сусідів, вибору метрики відстані та попередньої обробки даних.

Для визначення точності результатів класифікації трафіку використаємо значенням середньої абсолютної похибки MSE (Mean Squared Error) [15-16]:

$$MSE = \frac{1}{L}\sum_{i=1}^{L}\sqrt{(x_{est} - x_{real})^2 + (y_{est} - y_{real})^2}\ , \qquad (4)$$

де x_{est}, y_{est} – значення інтенсивності шкідливого трафіку HTTP(S) 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	Легітимний трафік	Шкідливий трафік, HTTP GET
Класифікатор k-найближчих сусідів	21,7%	14,7%

Згідно результатам розрахунку середньої абсолютної похибки MSE класифікації трафіку отримані значення похибок дозволяють стверджувати, що для легітимного трафіку середня абсолютна похибка становить 21,7 %, а для шкідливого HTTP GET-запитів – 14,7 %, що дозволяє використовувати метод класифікації саме для цього типу трафіку. Підвищення точності можливо отримати з використанням інших методів машинного навчання, таких як – метод опорних векторів, дерева рішень або Байєсівський метод.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

1. DDoS-атаки на базі Flood-трафіку (SYN-Flood, UDP-Flood та HTPP-Flood), яка спрямована на суттєве перевантаження Веб-ресурсів. Встановлено, що детектування аномалій Flood-трафіку доцільно виконувати шляхом аналізу шкідливого та легітимного трафіку.

2. Запропоновано використання сплайн-апроксимації на базі кубічних сплайнів для детектування шкідливого трафіку HTTP(S) GET-flood з подальшою класифікацією трафіку методом машинного навчання k-найближчих сусідів.

3. Проведений експеримент для трафіку HTTP(S) GET-flood DDoS-атаки дозволяє визначити аномалію трафіку в реальному часі та визначити характеристики шкідливого трафіку HTTP(S) GET-flood. Підвищення точності детектування трафіку DDoS-атаки на Веб-сервери можливо за допомогою різних методів машинного навчання, таких як – метод опорних векторів, дерева рішень або Байєсівський метод.

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. T. Radivilova, L. Kirichenko, O. Lemeshko, D. Ageyev, O. Mulesa and A. Ilkov, "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)*, Cracow, Poland, 2021, pp. 1108-1113, https://doi.org/10.1109/IDAACS53288.2021.9660920

4. Hajtmanek, R., Kontšek, M., Smieško, J., & Uramová, J. (2022). One-Parameter Statistical Methods to Recognize DDoS Attacks. *Symmetry*, *14*(11), 2388. https://doi.org/10.3390/sym14112388

5. Ветлицька, О. С., Треньова, К. О. (2024). Виявлення атак у мережах Інтернету речей методами машинного навчання. Сучасний захист інформації, 1(57), 39–49. https://doi.org/10.31673/2409-7292.2024.010005

6. 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. https://doi.org/10.1016/j.compeleceng.2018.11.004

7. Майор Є. Виявлення шкідливих пакетів та Ddos-атак у мережевому трафіку за допомогою глибоких згорткових нейронних мереж. Measuring and computing devices in technological processes, 2024 (1), 303 -311. https://doi.org/10.31891/2219-9365-2024-77-41

8. Imran, Jamil, F., & Kim, D. (2021). An Ensemble of Prediction and Learning Mechanism for Improving Accuracy of Anomaly Detection in Network Intrusion Environments. *Sustainability*, *13*(18), 10057. https://doi.org/10.3390/su131810057

9. ПЕТЛЯК, Н. (2025). АНАЛІЗ МОДЕЛЕЙ ВИЯВЛЕННЯ АНОМАЛІЙ ТРАФІКУ В СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES*, (1), 180–186. https://doi.org/10.31891/2219-9365-2025-81-21

10. 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. https://doi.org/10.1007/978-3-030-76343-5_1

11. Strelkovskaya I., Solovskaya I., Strelkovska J. Methods of spline functions in solving problems of telecommunication and information technologies Proceedings of the International Conference on Applied Innovations in IT 2023, 11(2), pp. 11-18. https://doi.org/10.25673/112989

12. Connect, protect, and build everywhere. [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/ (дата звернення 06.11.2025).

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

14. Level up with the largest AI & ML community. [Електронний ресурс]. – Режим доступу: https://www.kaggle.com (дата звернення 06.11.2025)

15. 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. https://doi.org/10.3103/s0735272722100028

16. Popovsky V.V., Strelkovskaya I.V. Accuracy of procedures for filtering, extrapolating and interpolating random processes. Telecommunication problems, 1(3), 2011. P. 3-10.

17. The Weka Workbench. [Електронний ресурс]. – Режим доступу: https://ml.cms.waikato.ac.nz/weka/ (дата звернення 06.11.2025).

References

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. T. Radivilova, L. Kirichenko, O. Lemeshko, D. Ageyev, O. Mulesa and A. Ilkov, "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)*, Cracow, Poland, 2021, pp. 1108-1113, https://doi.org/10.1109/IDAACS53288.2021.9660920

4. Hajtmanek, R., Kontšek, M., Smieško, J., & Uramová, J. (2022). One-Parameter Statistical Methods to Recognize DDoS Attacks. *Symmetry*, *14*(11), 2388. https://doi.org/10.3390/sym14112388

5. Vetlytska, O. S., Trenova, K. O. (2024). Vyiavlennia atak u merezakh Internetu rechei metodamy mashynnoho navchannia. Suchasnyi zakhyst informatsii, 1(57), 39–49. https://doi.org/10.31673/2409-7292.2024.010005

6. 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. https://doi.org/10.1016/j.compeleceng.2018.11.004

7. Maior, Ye. (2024). Vyiavlennia shkidlyvykh paketiv ta DDoS-atak u merezhevomu trafiku za dopomohoiu hlybokykh zhvortkovykh neironnykh merezh. Measuring and Computing Devices in Technological Processes, 1, 303–311. https://doi.org/10.31891/2219-9365-2024-77-41

8. Imran, Jamil, F., & Kim, D. (2021). An Ensemble of Prediction and Learning Mechanism for Improving Accuracy of Anomaly Detection in Network Intrusion Environments. *Sustainability*, *13*(18), 10057. https://doi.org/10.3390/su131810057

9. PETLIAK H. (2025). ANALYSIS OF TRAFFIC ANOMALY DETECTION MODELS IN MODERN INFORMATION AND COMMUNICATION SYSTEMS AND NETWORKS. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES*, (1), 180–186. https://doi.org/10.31891/2219-9365-2025-81-21

10. 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. https://doi.org/10.1007/978-3-030-76343-5_1

11. Strelkovskaya I., Solovskaya I., Strelkovska J. Methods of spline functions in solving problems of telecommunication and information technologies Proceedings of the International Conference on Applied Innovations in IT 2023, 11(2), pp. 11-18. https://doi.org/10.25673/112989

12. Connect, protect, and build everywhere. [Electronic resource]. – Access mode: https://www.cloudflare.com/ (accessed date 06.11.2025).

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

14. Level up with the largest AI & ML community. [Electronic resource]. – Access mode: https://www.kaggle.com (accessed date 06.11.2025)

15. 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. https://doi.org/10.3103/s0735272722100028

16. Popovsky V.V., Strelkovskaya I.V. Accuracy of procedures for filtering, extrapolating and interpolating random processes. Telecommunication problems, 1(3), 2011. P. 3-10.

17. The Weka Workbench. [Electronic resource]. – Access mode: https://ml.cms.waikato.ac.nz/weka/ (accessed date 06.11.2025).