Упередження повільних DDoS-атак на хмарні сервіси

УДК 004.056 (043.2)

Ігор Аверічев[1], Петро Поночовний[2]

Державний університет інформаційно-комунікаційних технологій,
[1]iaverichev19@gmail.com, [2]petja9186@gmail.com

Повільні (low-and-slow) DDoS-атаки є одним із найнебезпечніших видів кіберзагроз для сучасних хмарних сервісів. На відміну від традиційних об'ємних (volumetric) атак, які генерують величезний трафік, повільні атаки імітують поведінку легітимних користувачів, надсилаючи мінімальну кількість даних протягом тривалого часу. Це дозволяє їм ефективно вичерпувати серверні ресурси — кількість одночасних з'єднань, робочі потоки, пам'ять та процесор — без створення помітного мережевого навантаження [1, 2, 3].

Найпоширенішими прикладами таких атак є:

- Slowloris — відкриває багато HTTP-з'єднань і повільно надсилає заголовки, не завершуючи запити;
- R.U.D.Y. (R U Dead Yet?) — повільно передає тіло POST-запиту;
- Slow HTTP POST / Slow Read — інші варіанти, що тримають з'єднання відкритими максимально довго.

Хмарні середовища (AWS, Microsoft Azure, Google Cloud) забезпечують автоматичне масштабування, але залишаються вразливими до атак на рівні додатків (Layer 7). Базові мережеві засоби захисту (Layer 3/4) часто не виявляють такі загрози, оскільки трафік виглядає нормальним. Атака з однієї машини може вивести з ладу веб-сервер, вичерпавши пул з'єднань Apache, Nginx чи інших серверів [4, 8].

Таблиця 1

Порівняння характеристик різних типів DDoS-атак

Тип атаки	Рівень OSI	Обсяг трафіку	Складність виявлення	Основна мета	Приклади
Volumetric	3–4	Дуже високий	Низька	Перевантаження каналу	UDP Flood, DNS Amplification
Protocol	3–4	Середній	Середня	Виснаження стеку протоколів	SYN Flood, Ping of Death
Application (Low-and-Slow)	7	Низький	Висока	Виснаження ресурсів сервера	Slowloris, RUDY

Таблиця 2

Оцінка ефективності методів захисту
від повільних DDoS-атак (умовні бали, 1–100)

Метод захисту	Вияв лення	Блокув ання	Вплив на легітимний трафік	Масштабованіс ть у хмарі	Вартість впровад ження
Традиційний firewall / IPS	40–55	50–65	Низький	Низька	Низька

CDN + WAF (Cloudflare, Imperva)	80–90	85–95	Низький	Висока	Середня
Behavioral analysis + ML/AI	90–95	92–97	Середній	Висока	Середня / Висока
Rate limiting + dynamic timeouts	75–85	80–90	Низький	Висока	Низька
Хмарний scrubbing (AWS Shield, Radware)	85–93	90–96	Низький	Дуже висока	Висока

Ефективне упередження вимагає багаторівневого (defense-in-depth) підходу. Основними елементами є:

- Always-on моніторинг параметрів з'єднань (тривалість сесії, швидкість передачі даних, частота запитів, поведінкові профілі);
- Адаптивне обмеження швидкості (rate limiting) та динамічне керування таймаутами;
- Reverse proxy та CDN (Cloudflare, AWS CloudFront, Akamai), які фільтрують шкідливий трафік на краю мережі ще до потрапляння на origin-сервер;
- Web Application Firewall (WAF) з правилами для виявлення slow HTTP аномалій;
- Машинне навчання для аналізу поведінки та виявлення відхилень у реальному часі [2, 9].

Узагальнену класифікацію методів показано на рисунку 1.

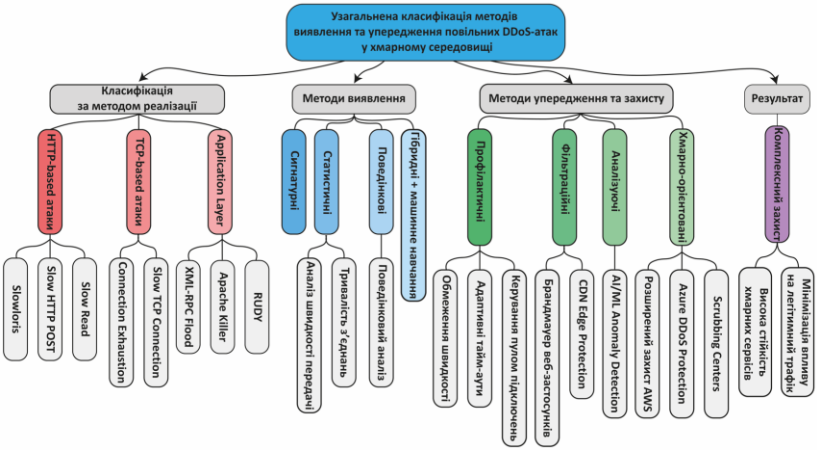

Рис.1. Узагальнена класифікація методів виявлення та упередження повільних DDoS-атак у хмарному середовищі

Математична модель оцінки ризику вичерпання ресурсів може бути представлена формулою:

$$R = \frac{N \cdot T \cdot C \cdot K}{M \cdot S} \quad (1)$$

де N – кількість підозрілих з'єднань, T – середня тривалість з'єднання, C – споживання ресурсів на з'єднання, K – коефіцієнт аномальності, M – доступні ресурси, S – коефіцієнт масштабування хмарного середовища.

Для практичної реалізації рекомендується:

- впровадження CDN та edge-захисту;
- використання штучного інтелекту для аналізу поведінки користувачів;
- динамічне керування таймаутами та обмеженнями;
- регулярне тестування систем навантаженням з імітацією slow-атак;
- інтеграція з професійними хмарними сервісами захисту [5, 6, 7, 10].

Запропонований комплексний підхід дозволяє суттєво підвищити стійкість хмарних сервісів до повільних DDoS-атак і забезпечити високу доступність критичних інформаційних систем.

Перехід до проактивних систем захисту з використанням штучного інтелекту дозволяє не лише реагувати на атаки, але й прогнозувати їх. Комбінація edge-обчислень, поведінкового аналізу та хмарних scrubbing-центрів забезпечує високу стійкість критичних сервісів до повільних DDoS-загроз.

Запропоновані методи та рекомендації дозволяють суттєво знизити ймовірність успішної реалізації повільних атак, забезпечити високу доступність та надійність хмарних сервісів у сучасному кіберпросторі.

1. Cloudflare. What is a low and slow DDoS attack? URL: https://www.cloudflare.com/learning/ddos/ddos-low-and-slow-attack/
2. NETSCOUT. Low and Slow DDoS Attacks Explained. URL: https://www.netscout.com/what-is-ddos/low-slow-attack
3. Imperva. Slowloris DDoS Attack. URL: https://www.imperva.com/learn/ddos/slowloris/
4. AWS. AWS Shield Advanced. URL: https://aws.amazon.com/shield/
5. Венгерський П.С., Вишневська Н.С., Хохлачова Ю.Є. Кількісна оцінка кіберзахищеності інформації // Захист інформації. – 2023. – Т. 25, №2. – С. 53-61.
6. Radware. Low and Slow Attacks: Detection and Mitigation. 2024.
7. OWASP. Denial of Service Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/Denial_of_Service_Cheat_Sheet.html
8. Поночовний П.М., Пепа Ю.В. Реалізація системи захисту серверів з урахуванням аномалій в пакетах // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2025. – № 1. – С. 44–51. URL: https://vottp.khmnu.edu.ua/index.php/vottp/article/view/459/426
9. Поночовний П.М. Модель упередження низькошвидкісних HTTP

DDoS атак на кінцевого користувача // Кібербезпека: освіта, наука, техніка. – 2024. – № 2 (26). – С. 291–304. URL: https://doi.org/10.28925/2663-4023.2024.26.695

10. Аверічев І.М., Роженко А.С., Кихтенко Є.М. Інноваційні підходи до підвищення рівня кібербезпеки корпоративних мереж при використанні хмарних технологій // Кібербезпека: освіта, наука, техніка. – 2025. – № 1 (29). – С. 732–747. https://doi.org/10.28925/2663-4023.2025.29.934

Вплив характеристик навчального набору на коректність виявлення дипфейкових зображень моделлю ResNetSECBAM

УДК 004.056.5:004.93

Дмитро Азарний[1], Анатолій Давиденко[2], Олена Висоцька[3]

[1]Київський національний університет імені Тараса Шевченка, dazarny@gmail.com,
[2]Державний університет інформаційно-комунікаційних технологій, davidenkoan@gmail.com,
[3]Державний університет «Київський авіаційний інститут», Lek_Vys@ukr.net

Стрімкий розвиток генеративних моделей призвів до поширення дипфейкових зображень, що становлять загрозу інформаційній безпеці, цифровій ідентичності та довірі до мультимедійного контенту. Практика показує, що навіть високоточні детектори можуть істотно знижувати ймовірність коректної класифікації при переході до даних, відмінних від навчального набору. Тому актуальним є дослідження міждатасетного переносу моделей виявлення дипфейків для реального застосування систем комп'ютерного зору.

Метою роботи є дослідження впливу характеристик навчального набору даних на коректність виявлення дипфейкових зображень моделлю ResNetSECBAM. Наукова новизна полягає у двосторонньому порівнянні переносу між DFFD [1] та HiDF [2], а також у перевірці впливу їх об'єднання. Модель побудовано на базі ResNet-50 з механізмом уваги CBAM [3], що посилює інформативні канальні та просторові ознаки.

Було проведено три експерименти: навчання на DFFD з тестуванням на HiDF, навчання на HiDF з тестуванням на DFFD та навчання на об'єднаному наборі DFFD+HiDF. За підсумковим розбиттям використано 62 260 зображень DFFD (50 638 навчальних, 5 626 валідаційних, 5 996 тестових) та 69 828 зображень HiDF (48 879 навчальних, 6 982 валідаційних, 13 967 тестових), тобто 132 088 зображень загалом. У третьому експерименті навчальна вибірка становила 99 517 зображень (50 638 DFFD і 48 879 HiDF), валідаційна — 12 608 (5 626 DFFD і 6 982 HiDF), а тестова — 19 963 (5 996 DFFD і 13 967 HiDF); усі тестові зображення були відкладеними і не використовувалися під час навчання. Оцінювання проводилося за метриками Accuracy, Precision, Recall, F1-міра та AUC.