УДК 004.056

М. В. Боднар

С. М. Захарченко

АНАЛІЗ МЕРЕЖЕВИХ АТАК ТА СИСТЕМ ЗАХИСТУ ХОСТИНГОВИХ СЕРВЕРІВ

Вінницький національний технічний університет

Анотація

У роботі проведено аналіз природи мережевих атак та типів хостингових архітектур. Розглянуто загальну класифікацію загроз та проаналізовано динаміку розподілу типів атак протягом 2025 року, яка виявила тенденцію до суттєвого зростання відсотка атак рівня застосунків (L7). Описано комплексні методи детектування аномалій, включаючи вейвлет-аналіз, моніторинг системних журналів та механізм автентифікації виклик-відповідь для захисту серверної інфраструктури.

Ключові слова: DDoS-атаки, хостинг-сервери, Ados, модель OSI, вейвлет-аналіз, аналіз логів, автентифікація «виклик-відповідь», мережева безпека.

Abstract

The paper analyzes the nature of network attacks and types of hosting architectures. The general threat classification is considered and the dynamics of attack type distribution throughout 2025 is analyzed, revealing a trend of significant increase in the percentage of application-layer (L7) attacks. Comprehensive anomaly detection methods are described, including Wavelet analysis, system log monitoring, and the challenge-response authentication mechanism for protecting server infrastructure.

Keywords: DDoS attacks, hosting servers, Ados, OSI model, Wavelet analysis, log analysis, challenge-response authentication, network security.

Вступ

Забезпечення доступності веб-ресурсів у 2026 році вимагає глибокого розуміння структури мережевих атак та особливостей серверної інфраструктури. Стрімке зростання кількості інцидентів відмови в обслуговуванні (DDoS) зумовлює необхідність впровадження інтелектуальних систем захисту, адаптованих під різні типи хостингу.

Результати дослідження

Мережеві атаки можна класифікувати за декількома фундаментальними ознаками [2]. За характером впливу виділяють пасивні та активні атаки [3]. За метою впливу загрози поділяють на порушення конфіденційності, цілісності та доступності. Важливим є поділ за рівнями моделі OSI: від фізичного рівня до прикладного (L7), де атаки імітують дії легітимних додатків. Також атаки розрізняють за

наявністю зворотного зв’язку, умовами початку та розташуванням атакуючого об’єкта щодо цілі(рис. 1).

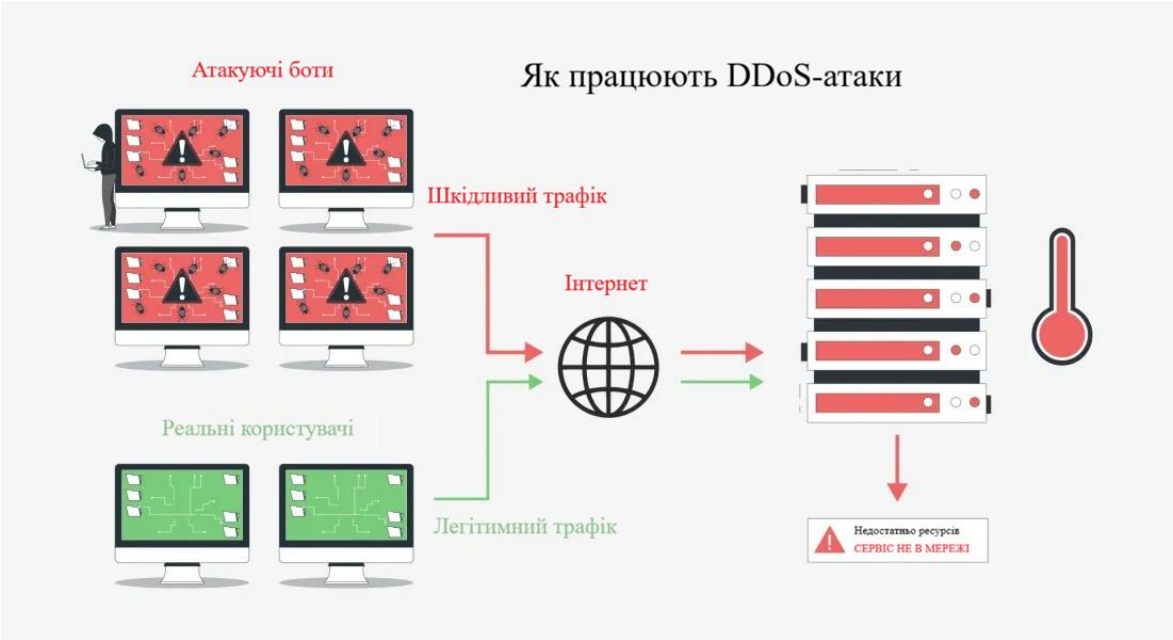

Рисунок 1 — Загальна схема реалізації DDoS-атаки на веб-ресурс

2025 рік відзначився масштабним сплеском DDoS-активності: загальна кількість атак зросла більш ніж удвічі, досягнувши неймовірного показника у 47,1 мільйона інцидентів. Протягом 2023–2025 рр. спостерігалося стрімке зростання кількості атак на 236%. За даними Cloudflare(рис. 2), у 2025 році в середньому ліквідовували 5 376 DDoS-атак щогодини, з яких 3 925 припадало на мережевий рівень, а 1 451 — на рівень HTTP [4].

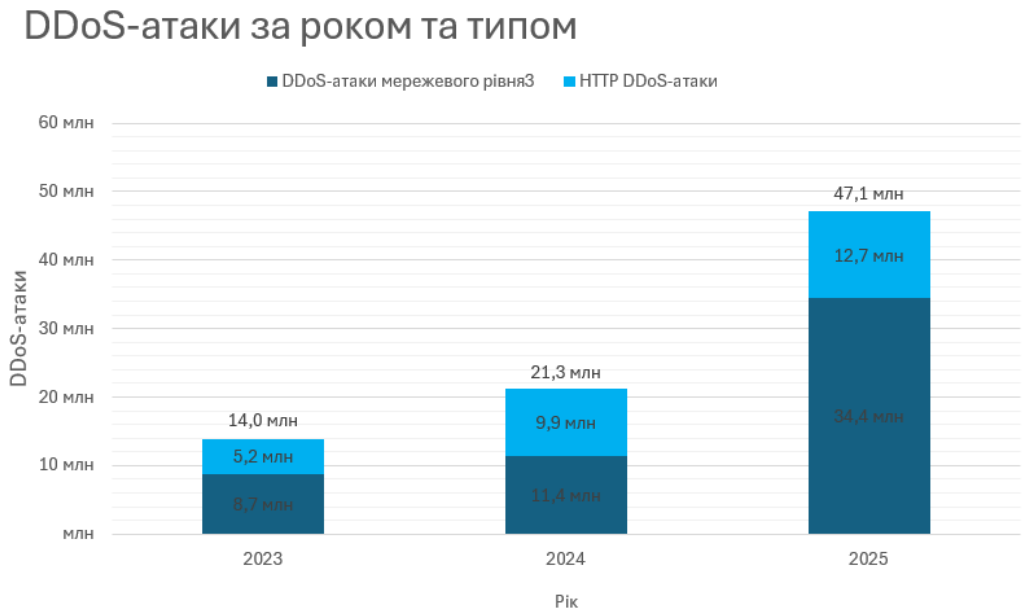

Рисунок 2 — Динаміка кількості DDoS-атак у 2023–2025 рр. (за даними Cloudflare)

Окрему та найбільш руйнівну категорію становлять атаки типу DoS та DDoS, спрямовані на порушення доступності сервісів [3]. Їхня ефективність безпосередньо залежить від обраної моделі хостингу. На віртуальному хостингу (Shared) клієнти ділять спільні ресурси та IP-адресу, що робить їх вразливими до атак на «сусідів» [2]. Віртуальні виділені сервери (VPS) забезпечують кращу ізоляцію через віртуалізацію, дозволяючи встановлювати локальні засоби моніторингу, тоді як виділені сервери (Dedicated) надають повний контроль над фізичним обладнанням для побудови ешелонованих систем захисту [3].

Аналіз статистики за перший квартал 2025 року (Q1) на основі даних Cloudflare Radar(рис. 3) свідчить про безпрецедентну ескалацію DDoS-загроз. У цей період загальна кількість атак сягнула рекордного показника у 20,5 млн інцидентів за квартал. Найбільшу активність продемонстрували мережеві DDoS-атаки — 16,8 млн випадків, що значно перевищує показники наступних періодів. Проте аналіз динаміки розподілу типів атак протягом усього 2025 року виявив тенденцію до суттєвого зростання відсотка атак рівня застосунків (L7). Така динаміка свідчить про поступове зміщення вектора зловмисників у бік складніших методів впливу, що вимагає більш інтелектуальних методів детектування [4].

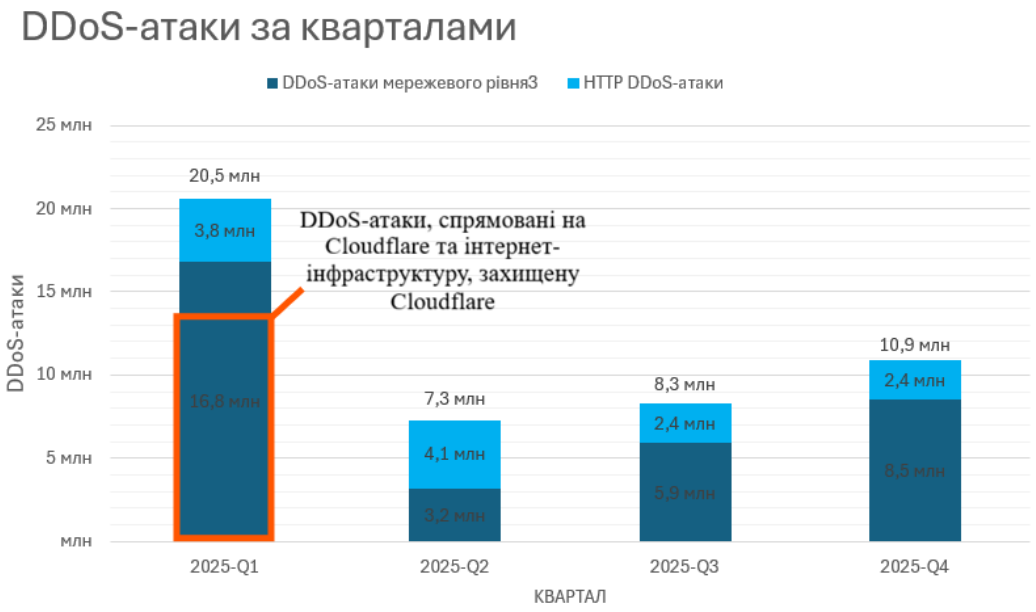

Рисунок 3 — Статистика DDoS-атак за кварталами 2025 року (за даними Cloudflare)

Для ефективного детектування аномалій пропонується поєднання декількох взаємодоповнюючих методів аналізу, що дозволяє забезпечити багаторівневий захист хостингових ресурсів. Зокрема, Вейвлет-аналіз (Wavelet Analysis) дає змогу виявляти атаки на ранніх стадіях через частотне розкладання мережевого трафіку, що підсвічує короткочасні сплески та аномальні коливання, які зазвичай маскуються під природні флуктуації запитів [5]. Паралельно з мережевим моніторингом, аналіз логів (Log Analysis) за допомогою SIEM-систем допомагає ідентифікувати загрози рівня застосунків (L7), детально аналізуючи журнали веб-серверів на предмет підозрілих послідовностей запитів [6]. Механізм автентифікації виклик-відповідь (Challenge-Response) виступає надійним бар'єром проти сучасних ботнетів, таких як Aisuru-Kimwolf, оскільки вимагає від клієнта успішного проходження динамічної перевірки, яку практично неможливо автоматизувати без значних обчислювальних витрат з боку атакуючого [1]. Локальна система Ados суттєво посилює цей комплекс захисту, виконуючи динамічну фільтрацію пакетів на основі математичного розрахунку «ваги» запитів за формулою:

$$rate = \frac{\sum_{i=1}^{n}(C_i \cdot W_i)}{track\_period}$$

де C_i— кількість запитів, а W_i — їх встановлена вага. Перевищення порогу автоматично переміщує IP-адресу джерела до бан-листа. У разі перевищення встановленого порогу система в реальному часі ідентифікує загрозу та автоматично переміщує IP-адресу джерела до бан-листа, забезпечуючи стабільну роботу веб-ресурсу для легітимних користувачів [2].

Висновки

Дослідження показало, що побудова надійного захисту хостингових систем вимагає переходу від загальної класифікації атак до впровадження спеціалізованих інструментів протидії DDoS. Проаналізована динаміка розподілу типів атак протягом 2025 року вказує на стійку тенденцію до зростання відсотка атак рівня застосунків (L7). Інтеграція вейвлет-аналізу, глибокого моніторингу системних журналів та механізмів автентифікації клієнтів дозволяє створити стійку інфраструктуру, здатну витримувати масштабні мережеві навантаження.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Автентифікація виклик-відповідь : Глосарій MDN / Mozilla Developer Network. URL: https://developer.mozilla.org/uk/docs/Glossary/Challenge (дата звернення: 14.03.2026).
2. Класифікація DDoS-атак : Мережеві DoS та DDoS-атаки. URL: https://studwood.net/1654202/informatika/klasifikatsiya_ddos_atak (дата звернення: 14.03.2026).
3. Cisco ScanSafe. Denial of Service Attacks. URL: https://www.sei.cmu.edu/documents/527/1997_019_001_496601.pdf (дата звернення: 14.03.2026).
4. Cloudflare Radar. DDoS threat report for 2025 Q4. URL: https://radar.cloudflare.com/reports/ddos-2025-q4 (дата звернення: 14.03.2026).
5. Torrence C., Compo G. P. A Practical Guide to Wavelet Analysis. *Bulletin of the American Meteorological Society*. 1998. Vol. 79, No. 1. P. 61–78. URL: https://paos.colorado.edu/research/wavelets/bams_79_01_0061.pdf (дата звернення: 14.03.2026).
6. Kent K., Souppaya M. Guide to Computer Security Log Management. NIST Special Publication 800-92. 2006. 72 p. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf (дата звернення: 14.03.2026).

Боднар Михайло Володимирович *— студент гр. 2КІ-22б, факультет інформаційних та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: mihajlobodnar8@gmail.com.*

Науковий керівник: Захарченко Сергій Михайлович *— к.т.н., професор кафедри обчислювальної техніки, Вінницький національний технічний університет, м. Вінниця.*

Bodnar Mykhailo Volodymyrovych *— student of Faculty of Information and Computer Engineering, Vinnytsia National Technical University.*

Supervisor: Zakharchenko Serhii *— PhD in Technical Sciences, Professor of Computer Engineering Department, Vinnytsia National Technical University.*