

МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ЦИФРОВИХ АКТИВІВ ВЕБЗАСТОСУНКІВ В УМОВАХ DDoS-АТАКИ

Шестопал Д.О., Балагура Д.С., Смірнов А.О.

Харківський національний університет радіоелектроніки, Харків, Україна

В умовах сучасного цифрового світу, веб-додатки є основними платформами для надання послуг та взаємодії з користувачами. Проте зростання їхньої популярності супроводжується зростанням кількості кіберзагроз, серед яких особливе місце займають DDoS-атаки (Distributed Deny of Service): різновид атак, які відрізняються збільшеною складністю у виявленні та відбитті у порівнянні з класичними DoS-атаками [1, 2]. Ці атаки спрямовані на перевантаження серверів і призводять до недоступності послуг, втрати прибутку та репутаційних ризиків.

У даній доповіді розглянуто сучасні методи та технології захисту цифрових активів веб-додатків від DDoS-атак. Разом з цим було проаналізовано варіанти простих атак з використанням сучасних видів захисту.

Метою доповіді є моделювання DDoS атаки, аналіз існуючих рішень, надання рекомендацій та впровадження ефективних захисних механізмів та заходів для забезпечення стабільної роботи веб-додатків, що атакуються, безпосередньо під час DDoS атаки.

В доповіді проведено огляд та класифікацію DDoS-атак, розглянуто основні механізми їх реалізації та існуючі методи захисту. Крім того проаналізовано архітектурні рішення та мережеві технології, що можуть бути використані для мінімізації впливу DdoS-атак, а також зроблено висновки щодо їх ефективності.

В практичній частині роботи створено тестовий полігон та проведено аналіз вразливостей веб-додатку, впроваджено захисні заходи та проведено моніторинг їх ефективності. Результати дослідження можуть бути використані для покращення захисту веб-додатків від DDoS-атак.

Для захисту від DDoS-атак перспективним напрямом є використання машинного навчання.

Ці технології дозволяють виявляти аномалії в мережевому трафіку на ранніх етапах та класифікувати типи атак із високою точністю.

Список літератури

1. Бірюков А.А. Інформаційна безпека: захист та напад. – видавництво ДМК-ПРЕСС. – 2016. – 434 с.
2. Северінов О.В., Шевцов В.О., Сокол-Кутиловська А.С. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка 1 (2017): 65-68.
3. Kavetskyi M.S., Sievierinov O.V., Gvozdev R.Y., Smirnov A.O. (2024). Використання машинного навчання для класифікації атак типу DOS/DDOS. *Radiotekhnika*, (217), 55-63.