WEB-ДОДАТОК З ВІДСТЕЖЕННЯ ТА БЛОКУВАННЯ DDoS-АТАК

Коломицев А.Р., Наконечний М.В., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У наш час веб-додатки та сайти стали ключовим інструментом для бізнесу, комунікацій та обслуговування клієнтів. Однак розвиток цифрових технологій також супроводжується збільшенням кіберзагроз.

Метою доповіді є розгляд однієї з найпоширеніших атак – атаки на відмову в обслуговуванні (Distributed Denial of Service, DDoS). Її метою є перевантаження серверів і обмеження доступу до ресурсу легітимним користувачам. Захист веб-додатків від таких загроз є критично важливим завданням [1]. DDoS-атаки полягають у масовому надсиланні запитів до сервера з різних джерел, що призводить до перевантаження мережі та відмови у її функціонуванні. Різновиди таких атак включають UDP-флудинг, SYN-флудинг, HTTP-флудинг та інші.

У доповіді розглядається створення веб-додатку, що дозволяє відстежувати та блокувати DDoS-атаки на веб-сайті. Основними функціями такого додатку є моніторинг трафіку, виявлення підозрілих активностей та оперативна реакція на можливі загрози шляхом блокування атакуючих IP-адрес або інших заходів [2].

Основні етапи створення веб-додатку з функціями захисту від DDoS-атак:

1. Моніторинг мережевого трафіку. Збір даних про запити до сервера в реальному часі. Це включає відстеження таких параметрів, як частота запитів, обсяги трафіку та географічне розташування джерел запитів.

2. Виявлення аномалій. Використання алгоритмів аналізу для визначення нетипової активності.

3. Реалізація механізмів блокування. Забезпечення можливості блокування підозрілих IP-адрес або обмеження доступу на певний проміжок часу. Реалізація функції автоматичного блокування на основі налаштованих правил.

4. Інтеграція системи оповіщення. Додаток повинен забезпечувати своєчасне інформування адміністраторів про можливі загрози через електронну пошту, повідомлення або інші засоби комунікації.

5. Візуалізація даних. Надання візуальної інформації для зручного аналізу роботи системи та виявлення тенденцій у мережевому трафіку.

Результатом реалізації такого веб-додатку є зменшення ризиків збоїв у роботі сайту через DDoS-атаки, підвищення надійності інформаційної системи та захист даних користувачів.

Список літератури

1. Cloudflare. DDoS Protection. URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

2. Д'якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних веб-ресурсів, НТУ «ХПІ»,. – 2022.