Хімічук О. В., магістрант
Фальковський І. Г., старший викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ ТА ВПРОВАДЖЕННЯ СУЧАСНИХ МЕТОДІВ ДЛЯ ПОБУДОВИ КОМПЛЕКСНОГО ЗАХИСТУ ВЕБ-ДОДАТКІВ ВІД DDOS-АТАК

DDoS-атаки (розподілені атаки відмови в обслуговуванні) становлять серйозну загрозу стабільній роботі веб-додатків і мереж, оскільки спрямовані на перевантаження системи, що може призвести до її відключення. Щороку ці атаки ускладнюються й масштабуються, що потребує адаптивних захисних технологій для протидії новим загрозам. Під загрозою опиняються не лише великі підприємства, а й середні та малі бізнеси. Основна мета атак – вивести веб-сервіси з ладу, що спричиняє фінансові втрати та шкодить репутації компаній. Це дослідження спрямоване на аналіз методів та отримання оптимальних узагальнених алгоритмів, які забезпечують адаптивний захист веб-додатків від DDoS-атак та їх наслідків.

DDoS-атаки поділяються на різні типи залежно від рівня, на якому вони діють. Найпоширеніші з них – атаки на рівні мережі та на рівні додатків. Атаки на мережевому рівні передбачають флудинг пакетами для виснаження мережевих ресурсів, тоді як атаки на рівні додатків можуть включати HTTP-флудинг, тобто надсилання численних запитів до сервера, або інші техніки виснаження ресурсів, які найчастіше реалізуються за допомогою ботнетів – мереж заражених пристроїв, що координуються зловмисниками. Оскільки кожен з цих методів має свої унікальні механізми, протидія їм вимагає різноманітних підходів.[1]

Сучасні методи захисту від DDoS-атак базуються на багаторівневих технологіях і рішеннях. Один із ключових елементів – фільтрація трафіку на рівні мережі, реалізована через фаєрволи та системи виявлення й запобігання вторгнень (IDS/IPS). Вони дозволяють відсіяти шкідливі пакети до проникнення в систему, забезпечуючи ранній захист. Для протидії великим обсягам трафіку використовуються масштабовані рішення, такі як Anycast, що розподіляють трафік між точками доступу, знижуючи навантаження на сервери. Інші методи включають капчу, автентифікацію для обмеження доступу ботів і розподілені мережі доставки контенту (CDN) для зниження ризиків атак на рівні додатків. Застосування машинного навчання й штучного інтелекту для виявлення аномалій у мережі також стало ключовим у протидії атакам, дозволяючи реагувати на загрози в реальному часі. [2]

Захист веб-додатків також вимагає постійного моніторингу та аналізу трафіку для виявлення аномальних активностей. Системи моніторингу дозволяють відстежувати незвичайні сплески трафіку, що може свідчити про підготовку до атаки. Рекомендується використовувати хмарні рішення, як-от Cloudflare та Amazon Shield, які надають комплексний захист від DDoS та інструменти для швидкого реагування. Крім того, для мінімізації наслідків успішної атаки важливо створювати резервні копії даних та мати можливість швидкого відновлення роботи сервісу.

Для тестування і вдосконалення систем захисту існує низка корисних інструментів, зокрема LOIC, Slowloris та Wireshark, які дозволяють аналізувати мережевий трафік, виявляти аномалії та перевіряти систему на стійкість до атак. Існують також інструменти, що сприяють підвищенню безпеки в реальних умовах, такі як Fail2ban для блокування підозрілих IP, Snort та Suricata як додаткові IDS/IPS засоби для мережевої фільтрації. OWASP також надає набір рекомендацій та інструментів для забезпечення безпеки веб-додатків.

Таким чином, з метою підвищення ефективності дії системи захисту веб-додатків від DDoS-атак рекомендується комплексний підхід, що включає використання багаторівневих заходів безпеки, таких як фаєрволи, IDS/IPS, CDN та механізми аутентифікації. Важливим також є підтримка безпеки шляхом постійного навчання співробітників, регулярного оновлення інструментів та впровадження стандартів інформаційної безпеки, таких як ISO/IEC 27001 [3]. Оскільки методи атак постійно змінюються, організаціям слід інвестувати у сучасні технології для забезпечення високого рівня стійкості веб-додатків перед кіберзагрозами.

Список використаних джерел

1. Що таке DDoS-атака? Microsoft URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-ddos-attack

2. Distributed Denial of Service Attacks - The Internet Protocol Journal - Volume 7, Number 4/ Cisco – URL: https://web.archive.org/web/20190826143507/https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html

3. Як стандарт ISO/IEC 27001 допомагає розвиватися сучасному бізнесу / IT Specialist. – URL: https://my-itspecialist.com/standard-iso/iec-27001-for-business