ЗАХИСТ ВЕБ-СЕРВІСУ ОБМІНУ ПОВІДОМЛЕННЯМИ ВІД СПАМУ ТА BRUTE-FORCE АТАК

Кот А.В., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Веб-сервіси обміну повідомленнями широко використовуються для організації комунікації в режимі реального часу, однак вони є вразливими до кіберзагроз, зокрема спам-активності та атак типу brute-force. Недостатній рівень захисту може призводити до перевантаження системи, зниження продуктивності та несанкціонованого доступу до облікових записів.

Відповідно до міжнародних стандартів інформаційної безпеки, захист веб-сервісів повинен включати механізми автентифікації, контролю доступу і моніторингу подій [1]. Особливу роль відіграє обмеження кількості спроб входу, що дозволяє зменшити ефективність brute-force атак [2].

Метою роботи є розробка системи захисту веб-сервісу обміну повідомленнями від спам-активності та brute-force атак. У роботі реалізовано веб-сервіс обміну повідомленнями з механізмами захисту, зокрема:

- обмеження частоти запитів (rate limiting);
- виявлення повторюваних повідомлень;
- обмеження кількості невдалих спроб автентифікації;
- журналювання подій безпеки;
- інформування адміністратора про інциденти.

Механізм обмеження частоти запитів базується на аналізі активності користувача у визначеному часовому інтервалі, що дозволяє запобігти надмірному навантаженню системи. Виявлення підозрілої активності здійснюється шляхом аналізу поведінки користувачів. Використання журналювання подій відповідає рекомендаціям щодо моніторингу безпеки веб-додатків і дозволяє своєчасно виявляти інциденти [3, 4]. Запропонований підхід забезпечує підвищення рівня захисту веб-сервісу та зменшує ризик реалізації атак.

Список літератури

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. 3rd ed. [Чинний від 2022-10]. Вид. офіц. Geneva: ISO/IEC, 2022. 19 с.

2. NIST SP 800-63B-4. Digital Identity Guidelines: Authentication and Authenticator Management/ D. Temoshok, J. L. Fenton, Y. Y. Choong, N. Lefkovitz, A. Regenscheid, R. Galluzzo, J. P. Richer. [Чинний від 2025-07]. Вид. офіц. Gaithersburg, MD: NIST, 2025. 118 с.

3. OWASP Top 10:2025. URL: https://owasp.org/Top10/2025/ (дата звернення: 01.04.2026).

4. Дорофєєва, К., Сєвєрінов, О., Сидоренко, З., & Сухотеплий, В. (2025). Застосування інструмента аналізу безпеки для виявлення критичних вразливостей у веб-додатках. *Вісник Херсонського національного технічного університету*, *3*(4 (95)), 62-68.