УДК 004.056.5:004.77

Пунько Х.М., студент
Вовк Р.Б., к.т.н., доцент
Івано-Франківський національний технічний університет нафти і газу

МЕТОДОЛОГІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВЕБОРІЄНТОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

На сучасному етапі розвитку інформаційних технологій вебсторінки та вебзастосунки є домінуючим інструментарієм взаємодії користувачів із розподіленими масивами даних. Протягом останніх років спостерігається суттєве ускладнення архітектури вебсистем, зумовлене інтенсивним впровадженням методів автоматизації та мікросервісних підходів. Паралельно з еволюцією вебтехнологій відбувається експоненціальне зростання кількості кіберзагроз, спрямованих на несанкціоноване отримання доступу до конфіденційної інформації або дестабілізацію функціонування інформаційних систем. Відповідно, проектування та розробка захищених систем стає одним із пріоритетних напрямів сучасної інженерії програмного забезпечення.

Для системного оцінювання та гарантування безпеки вебрішень доцільно застосовувати спеціалізовані моделі зрілості, зокрема OWASP SAMM (Software Assurance Maturity Model) та DSOMM (DevSecOps Maturity Model). Зазначені моделі пропонують комплексний методологічний підхід до інтеграції практик безпеки у життєвий цикл розробки програмного забезпечення та детермінують методи протидії релевантним загрозам. До найбільш критичних категорій уразливостей належать порушення механізмів контролю доступу, дефекти криптографічного захисту, а також атаки типу «ін'єкція» [1].

Однією з найбільш деструктивних проблем безпеки є порушення контролю доступу (Broken Access Control). Експлуатація даної уразливості дозволяє суб'єктам загрози отримати доступ до облікових записів, адміністративних панелей або баз даних, що створює умови для несанкціонованого підвищення привілеїв, модифікації або знищення інформаційних активів. Для нівелювання зазначених ризиків фахівці OWASP рекомендують впроваджувати рольові механізми автентифікації (RBAC), обмежувати доступ до функціональних модулів на рівні сервера та виключати можливість зберігання конфіденційних об'єктів у відкритих директоріях вебсервера [2].

Криптографічні збої посідають чільне місце в ієрархії загроз, оскільки призводять до експозиції конфіденційних даних. Забезпечення цілісності та конфіденційності інформації потребує впровадження стійких алгоритмів шифрування як для даних у стані спокою (Data at Rest), так і для даних, що передаються мережею (Data in Transit), з використанням актуальних протоколів безпеки [3]. Окрему групу

поширених атак становлять ін’єкції, що виникають внаслідок некоректної валідації вхідних параметрів. Це дозволяє зловмиснику маніпулювати SQL-запитами до бази даних, оскільки вебзастосунок не здатний диференціювати користувацьке введення від системних команд. Аналогічно, атаки типу XSS (Cross-Site Scripting) дозволяють здійснювати впровадження шкідливого коду у вебсторінки, що призводить до компрометації сесій користувачів у середовищі браузера. Превентивні заходи включають:

- використання параметризованих запитів;
- сувору типізацію та фільтрацію вхідних даних;
- регулярне проведення сканувань на наявність уразливостей.

Вибір архітектурного паттерну системи (монолітного або мікросервісного) безпосередньо детермінує стратегію забезпечення безпеки. У монолітній архітектурі централізація компонентів спрощує реалізацію контролю доступу. Натомість у мікросервісних системах критично важливу роль відіграє API Gateway, який функціонує як єдина точка входу, забезпечуючи автентифікацію, фільтрацію запитів та розмежування прав доступу до внутрішніх сервісів. Незалежно від обраної архітектури, фундаментальним аспектом є інтеграція сучасних стандартів автентифікації та авторизації, зокрема використання JSON Web Tokens у синергії з механізмами багатофакторної перевірки [3].

Таким чином, проектування захищених веборієнтованих систем є комплексним завданням, що потребує системного підходу до вибору архітектурних рішень та методів захисту. Застосування сучасних криптографічних протоколів, суворих механізмів контролю доступу та методів валідації даних дозволяє мінімізувати ймовірність успішної реалізації кібератак та гарантувати стійкість інформаційних систем.

Список використаних джерел

1. OWASP Top 10:2025 – The Ten Most Critical Web Application Security Risks [Електронний ресурс]. OWASP Foundation. 2025. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 16.03.2026).

2. OWASP Top 10 Web Application Security Risks [Електронний ресурс]. URL: https://surl.li/sxijuh (дата звернення: 16.03.2026).

3. Almeida M., Canedo E. Authentication and Authorization in Microservices Architecture: A Systematic Literature Review. Applied Sciences. 2022. Vol. 12, No. 6. URL: https://www.mdpi.com/2076-3417/12/6/3023 (дата звернення: 16.03.2026).