УДК 004.4

Царук К.А., здобувачка,
Чижмотря О.В., ст. викладач
Державний університет «Житомирська політехніка»

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВЕБПЛАТФОРМИ ДЛЯ ОРГАНІЗАЦІЇ ВОЛОНТЕРСЬКОЇ ДІЯЛЬНОСТІ

Перехід волонтерської діяльності в цифрове середовище супроводжується широким використанням вебплатформ, які забезпечують координацію допомоги, взаємодію учасників та обробку інформації. У таких системах акумулюються персональні дані користувачів, інформація про заходи та результати діяльності, що підвищує вимоги до їх захисту.

Особливістю волонтерських платформ є робота з чутливими даними, зокрема контактною інформацією, відомостями про місцезнаходження та запитами на допомогу. Порушення безпеки в цьому випадку може спричинити не лише витік даних, а й негативно вплинути на організацію самої діяльності. З огляду на вимоги законодавства щодо захисту персональних даних [1], такі системи повинні відповідати встановленим нормам безпеки.

Дослідження сучасних вебзастосунків свідчить, що одними з найбільш поширених проблем залишаються недостатній рівень контролю доступу до облікових записів, вразливості при взаємодії з базами даних та відсутність належного захисту від типових кіберзагроз. Серед них особливу небезпеку становлять SQL-ін’єкції, що дають змогу отримати несанкціонований доступ до даних, а також XSS-атаки, спрямовані на виконання шкідливого коду в браузері користувача [2].

У процесі розробки вебплатформи передбачено застосування комплексу технічних засобів захисту. Зокрема, передача даних здійснюється із використанням протоколу HTTPS, що забезпечує їх шифрування. Паролі користувачів зберігаються у вигляді хешів із застосуванням сучасних алгоритмів, що унеможливлює їх відновлення у відкритому вигляді навіть у разі доступу до бази даних.

Крім того, реалізовано механізми автентифікації та розподілу прав доступу залежно від ролі користувача. Це дозволяє обмежити доступ до функцій системи та запобігти виконанню несанкціонованих дій. Для підвищення рівня захисту також передбачено обмеження кількості спроб входу, що зменшує ефективність атак перебором.

Перевірка введених користувачем даних є ще одним важливим елементом безпеки. Валідація здійснюється як на клієнтській, так і на

серверній стороні, що знижує ризик виконання шкідливого коду та забезпечує захист від XSS-атак і різних типів ін'єкцій.

У системі реалізовано ведення журналу подій, який фіксує ключові дії користувачів. Це дає змогу аналізувати активність, виявляти підозрілі операції та своєчасно реагувати на можливі загрози.

Додатковим рівнем захисту є використання багатофакторної автентифікації, яка передбачає підтвердження особи користувача за допомогою додаткових засобів. Незважаючи на певне ускладнення процесу входу, такий підхід значно підвищує безпеку доступу до системи.

Важливим напрямом є також забезпечення захисту даних на рівні бази даних. Передбачено розмежування доступу не лише за ролями користувачів, а й за операціями, що виконуються над даними. Це дозволяє обмежити можливість їх перегляду або зміни лише уповноваженими особами.

Крім того, передбачено резервне копіювання даних, що дає змогу відновити інформацію у разі технічних збоїв або кібератак. Регулярне створення резервних копій забезпечує збереження даних і стабільність функціонування системи.

Контроль цілісності даних також має важливе значення. Використання відповідних перевірок у базі даних дозволяє запобігти появі помилкової або неповної інформації, що є критично важливим для волонтерських платформ.

Окрему увагу приділено застосуванню принципу мінімальних привілеїв, відповідно до якого кожен користувач отримує лише необхідний рівень доступу. Це дозволяє обмежити можливі наслідки компрометації облікового запису.

Отже, забезпечення інформаційної безпеки вебплатформи для організації волонтерської діяльності потребує комплексного підходу, який враховує як технічні, так і організаційні аспекти. Реалізація таких рішень дозволяє підвищити стійкість системи до сучасних загроз і забезпечити її стабільну роботу [3].

Список використаних джерел:

1. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI.

2. Євсеєв С. П., Ткачов А. М., Алексієв В. О., Рябуха Ю. М. Кібербезпека: WEB-технології : навчально-довідковий посібник. – Львів: Новий Світ-2000, 2026. – 390 с.

3. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній. – Київ: Сідкон, 2022. – 372 с.