УДК 004.056.5

Нечипорук М.В., здобувач,
Саган Б.В., здобувач,
Скальська А.Р., здобувач,
Чешун В.М., к.т.н., доцент,
Хмельницький національний університет

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ІНТЕРНЕТ-ПРОВАЙДЕРА

Інформаційна безпека в умовах стрімкого розвитку цифрових технологій та зростаючих загроз у кіберпросторі є однією з пріоритетних задач [1]. Надійна система захисту інформаційних ресурсів має гарантувати безперервну роботу сервісів [2], захист персональних даних користувачів [3], а також здатність своєчасно виявляти та нейтралізовувати потенційні атаки [4].

В межах проведених робіт вирішувалось завдання проєктування, реалізації та тестування інформаційної системи інтернет-провайдера, що здатна виявляти та протидіяти базовим видам кіберзагроз.

На першому етапі проведено ґрунтовний теоретичний аналіз стану проблеми, визначено основні види шкідливого програмного забезпечення (віруси, трояни, скриптові ін’єкції, програми-шпигуни тощо) та проаналізовано сучасні підходи до побудови систем захисту на рівні прикладного програмного забезпечення, баз даних і мережевої інфраструктури. Особливу увагу приділено аналізу відкритих вразливостей, таких як SQL-ін’єкції, XSS-атаки, обхід автентифікації та підміна запитів.

На другому етапі спроєктовано структуру бази даних для обліку користувачів та супутніх дій, яка містить такі компоненти:

- основна таблиця users для зберігання облікових записів;
- logs для фіксації усіх дій користувачів (входів, помилок, спроб доступу);
- alerts для зберігання зафіксованих інцидентів безпеки;
- access_tokens для управління авторизаційними сесіями;
- roles і user_roles для реалізації рольової моделі доступу;
- security_settings як механізм конфігурації параметрів безпеки без втручання в код.

Реалізація бази даних здійснювалася за допомогою середовища phpMyAdmin, а логіка обробки даних – за допомогою мови PHP. Застосовано алгоритм хешування SHA-256 для паролів користувачів, що гарантує незворотність та захист від компрометації облікових даних. Для захисту персональної інформації реалізовано шифрування поля full_name з використанням симетричного алгоритму AES-256, що

забезпечує конфіденційність у випадку несанкціонованого доступу до бази даних.

Окремо розглянуто реалізацію фільтрації вхідних даних користувача. Запити, які містять шкідливі патерни (наприклад, SQL-ін'єкцію або XSS), розпізнаються засобами регулярних виразів і не обробляються, а їхній вміст автоматично записується у таблицю alerts. Це дозволяє фіксувати всі підозрілі дії та потенційні загрози для подальшого аналізу.

Також реалізовано рівневе управління доступом: користувачам можуть бути призначені різні ролі, що обмежують або розширюють їхні можливості в системі. Такий підхід відповідає принципу мінімальних привілеїв та забезпечує сегментацію доступу до критично важливих компонентів.

Система успішно протестована за допомогою низки імітаційних сценаріїв, у тому числі – моделювання входу користувача, шкідливих запитів, перевищення дозволених спроб входу та завершення сесій. Під час тестування підтверджено:

- правильність обробки персональних даних;
- коректність дій системи при виявленні атак;
- стабільність при багаторазовому доступі;
- працездатність функціоналу автоматичного логування та шифрування;
- гнучкість системи налаштувань безпеки.

Результати показали, що реалізована система відповідає сучасним вимогам до інформаційної безпеки для веб-застосунків та може слугувати прототипом для впровадження у провайдерських середовищах, корпоративних мережах та малих IT-інфраструктурах.

Список використаних джерел:

1. Зубок В.Ю., Мохор В.В. Кібербезпека топології INTERNET : монографія. К. : ІПМЕ ім. Г.Є.Пухова, 2022. 191 с.

2. Геєць В.М. Соціальна реальність у цифровому просторі. Економіка України. 2022. №1. С. 3-28. DOI: https://doi.org/10.15407/economyukr.2022.01.003

3. Бакаєв О.О., Суський Г.В. Методи захисту персональної інформації в інформаційних системах Телекомунікаційні та інформаційні технології. 2024. №2(83). С. 68-77. DOI: 10.31673/2412-4338.2024.028190

4. Шторгін Б. Дослідження та програмна реалізація системи надання доступу до мережі Internet сервіс провайдера. Збірник праць молодих науковців ЦНТУ. 2024. Вип.14. С. 318-328.