Секція 1

БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ ВЕБ-ЗАСТОСУНКІВ

Желтухіна І. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Желтухін О. В.

Актуальність. В сучасному цифровому ландшафті, де веб-застосунки стають необхідною та незамінною складовою повсякденного життя, а активність онлайн зростає, актуальність забезпечення безпеки персональних даних користувачів стає критичною. З ростом технологічного прогресу збільшується ймовірність кіберзагроз, таких як хакерські атаки, фішинг, розкрадання даних, які можуть призвести до витоку конфіденційної інформації користувачів в веб-застосунках. Велика кількість людей використовує веб-застосунки для різноманітних цілей, включаючи фінансові операції «Mono Bank», покупки «Rozetka», обмін особистою інформацій. Це робить їх привабливою мішенню для кіберзлочинців. Законодавчі органи України впроваджують нові норми і стандарти щодо захисту особистої інформації [1]. Це вимагає від компаній та веб-застосунків дотримуватися строгих правил, що підсилює необхідність надійного захисту даних. Також були великі інциденти, такі як витоки даних у великих корпораціях, привертають значну увагу громадськості та підкреслюють необхідність покращення безпеки веб-застосунків. Забезпечення безпеки даних впливає на психологічний аспект споживачів. Користувачі виявляють більшу довіру та впевненість в використанні веб-сервісів, де їх данні належним чином захищені. Отже, розгляд та розробка стратегій для забезпечення безпеки персональних даних у веб-сервісах стає необхідністю для збереження довіри споживачів, стабільності онлайн-середовища та успішного функціонування цифрового суспільства.

Мета роботи полягає в тому що потрібно всебічно розглянути проблему несанкціонованого доступу до персональних даних та розробка стратегій для ефективного захисту цих персональних даних користувачів у веб-застосунках. Робота спрямована на аналіз існуючих загроз, визначення ключових принципів захисту даних, і розробку рекомендацій для забезпечення стабільності та конфіденційності в онлайн-сервісах.

Основні положення. В роботі встановлюються фундаментальні принципи та стратегії для ефективного захисту персональних даних в веб-застосунках. Враховуючи технічні та соціальні аспекти безпеки, щоб створити комплексний підхід для забезпечення безпеки. Приклад 1: Аналіз та дослідження останніх випадків атак на веб-застосунки, таких як атаки типу SQL ін’єкції, крос-сайтового сценаріювання (XSS) або викрадення

індентифікаторів сесій [2]. Приклад 2: Розгляд принципів енкрипції даних в покої, аутентифікації двофакторного типу, та систем моніторингу, таких як системи реєстрації подій, для виявлення непередбачуваних активностей. Приклад 3: Визначення конкретних процедур та політик безпеки, встановлення регулярних аудитів безпеки коду, підтримка систем патчінгу та імплементація функцій контролю доступу. Приклад 4: Створення веб-сайту або розділу в додатку, де користувачі можуть дізнатися про методи забезпечення своїх персональних даних та взаємодіяти з питаннями безпеки [3].

Висновки. В результаті проведеного аналізу вказують на важливість та актуальність заходів забезпечення безпеки персональних даних у веб-застосунках. Розроблені рекомендації та стратегії мають на меті сприяти створенню надійних та безпечних онлайн-сервісів для користувачів.

Список літератури

1. Політика безпеки персональних даних в Україні для веб-застосунків *Vlasne*. URL: https://www.vlasneua.com/policy (дата звернення 14.11.2023);
2. Найвідоміші вразливості веб-застосунків *XSS* та *SQL* ін'єкції, вразливості автентифікації. *DOU UA*. URL: https://dou.ua/forums/topic/40613/ (дата звернення 14.11.2023);
3. Забезпечення конфіденційності у компанії Apple. *Apple*. URL: https://support.apple.com/uk-ua/HT202303 (дата звернення 14.11.2023).

Відомості про авторів

Желтухіна Ірина Олександрівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.o.zheltukhina@student.csn.khai.edu
Желтухін Олександр Васильович, старший викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.zheltukhin@csn.khai.edu