

АНАЛІЗ ТЕХНОЛОГІЙ ЗАХИСТУ ВЕБ САЙТІВ**ANALYSIS OF WEB SITE PROTECTION TECHNOLOGIES**

Веб-сайти є основою сучасного цифрового середовища, об'єднуючи бізнес, науку, освіту, розваги та інші сфери діяльності. Зі зростанням значення цифрової присутності для компаній і організацій, удосконалення веб-сайтів стало ключовим завданням для забезпечення їх ефективності, доступності та безпеки. Інформаційні технології (ІТ) виступають рушійною силою цих змін, забезпечуючи інструменти для всебічного аналізу, оптимізації та захисту веб-ресурсів.

Зростання кількості атак на веб-сайти, спрямованих на викрадення даних, злам систем або виведення ресурсів із ладу, вимагає впровадження сучасних рішень для забезпечення безпеки. Системи WAF (Web Application Firewall) дозволяють блокувати підозрілі запити в реальному часі, запобігаючи SQL-ін'єкціям, XSS-атакам та іншим загрозам. Використання SSL/TLS забезпечує шифрування даних, що передаються між сервером і клієнтом, запобігаючи їх перехопленню [1].

Одним із найбільш ефективних способів захисту користувачів веб-сайту – є впровадження багатофакторної автентифікації. Наприклад, користувач під час входу на сайт вводить свій логін і пароль, після чого система запитує одноразовий код, згенерований додатком Google Authenticator. У разі компрометації пароля злоумисник не зможе отримати доступ без цього додаткового коду [2].

Впровадження штучного інтелекту в системи кібербезпеки відкриває нові можливості для захисту веб-ресурсів. Алгоритми машинного навчання дозволяють виявляти нові типи загроз, аналізуючи поведінку трафіку та патерни атак. Наприклад, технології Deep Packet Inspection, що застосовуються у продуктах компаній, таких як Palo Alto Networks, здатні розпізнавати складні кіберзагрози [3].

Удосконалення захисту веб-сайтів за допомогою сучасних інформаційних технологій є основою їхньої стабільної роботи та довіри користувачів. Використання автоматизованих систем, машинного навчання, регулярний аудит і навчання персоналу забезпечують багаторівневий підхід до безпеки, що дозволяє запобігти більшості сучасних загроз. Тільки комплексні заходи зможуть гарантувати ефективність, надійність і захист веб-ресурсів у цифрову епоху.

Література

1. Гришина І. П., Коваленко А. С. «Сучасні методи забезпечення безпеки веб-додатків: теоретичний аналіз і практичні рекомендації». [Електронний ресурс]: journals.dut.edu.ua/index.php/dataprotect. Доступ: 05.12.2024. У статті розглядаються основні технології, включаючи SSL/TLS та WAF, як ефективні інструменти для запобігання сучасним кіберзагрозам
2. Добринін І.С., Пшеничних С.В. «Аналіз методів автентифікації для вебзастосунків та реалізація системи автентифікації». [Електронний ресурс]: ITSSI Journal. Доступ: 05.12.2024. У статті досліджуються сучасні технології багатофакторної автентифікації, включаючи Google Authenticator.
3. Савченко В. А., Шаповаленко О. Д. «Основні напрями застосування технологій штучного інтелекту у кібербезпеці». [Електронний ресурс]: journals.dut.edu.ua/index.php/sciencenotes. Доступ: 05.12.2024.