# ПРОБЛЕМАТИКА ЗАХИСТУ ІНФОРМАЦІЇ У ВЕБ-СЕРВІСАХ

Малярова Д.М., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

Веб-сервіси стали ключовими інструментами обміну даними, організації бізнес-процесів і комунікації. Разом із цим зростає кількість кіберзагроз, що спрямовані на несанкціонований доступ до інформації, її модифікацію чи знищення. Надійний захист даних у веб-сервісах є критично важливим аспектом кібербезпеки.

Сучасні веб-сервіси обробляють значний обсяг персональних, фінансових та корпоративних даних, що робить їх привабливою мішенню для кіберзлочинців. Найпоширенішими атаками залишаються SQL-ін'єкції, міжсайтовий скриптинг (XSS), підробка міжсайтових запитів (CSRF), MITM, атаки грубої сили, DDoS-атаки, а також Broken Authentication [1, 2].

Основними причинами існування вразливостей є нехтування принципами безпечної розробки, відсутність тестування, застарілі бібліотеки, слабке шифрування та контроль доступу.

Враховуючи вищесказане, для безпеки веб-сервісів необхідно [3]:

– застосовувати тестування SAST, DAST і Fuzzing;

– впроваджувати багатофакторну автентифікацію, TLS, HMAC;

– перевіряти налаштування серверів та середовища, регулярно оновлювати ПЗ, використовувати сканери (Burp Suite, OWASP ZAP);

– використовувати контроль доступу (RBAC), WAF;

– навчати персонал цифровій безпеці та реагуванню на інциденти.

Через еволюцію загроз, адаптування зловмисників та вдосконалення методів атак, ефективний захист веб-додатка вимагає комплексного підходу. В доповіді надані результати аналізу та оцінки ефективності існуючих захисних механізмів, рекомендації щодо поліпшення безпеки веб-сервісів.

У підсумку, безпека веб-сервісів – це технічне і організаційне питання, де поєднуються технології управління ризиками, освітні практики та постійний моніторинг нових загроз. Такий підхід забезпечує безпеку веб-сервісів, зменшує ризик кіберзагроз та підвищує довіру користувачів.

**Список літератури**

1. Васильченко Д.І., Лавровський І.М. Огляд типових уразливостей web-сайтів організацій у 2019-2020 році. Сучасний захист інформації. 2021. №1(45). С. 41-46.

2. Lysakov V., Sievierinov O., Taran I. Security of Web Applications Using AWS Cloud Provider // Computer and Information Systems and Technologies (2021).

3. Кравчук Н. В., Коробейнікова Т.І. Огляд проблематики захищеного доступу до вебсерверів. Вісник Львівського державного університету безпеки життєдіяльності. 2024. № 30. С. 78-89.