

С.О. Заболотна
Д.Г. Шевченко
О.В. Городецький
М.К. Прокопович
В.В. Войтко
О.В. Романюк

БЕЗПЕКА ВЕБПЛАТФОРМИ: СУЧАСНІ ПІДХОДИ ДО ЗАХИСТУ ДАНИХ КОРИСТУВАЧІВ ТА ЇХ ВПЛИВ НА КОРИСТУВАЧІВ

Вінницький національний технічний університет

Анотація: у статті аналізуються сучасні підходи до захисту даних вебплатформ, серед яких шифрування, двофакторна аутентифікація (2FA), логування подій, захист від DDoS-атак та регулярні оновлення програмного забезпечення. Особлива увага приділяється обробці помилок, щоб уникнути витоку конфіденційної інформації, а також важливості оновлення компонентів програмного забезпечення для мінімізації вразливостей. Також аналізується вплив технологій безпеки на довіру користувачів, підкреслюючи важливість прозорості та дотримання вимог конфіденційності.

Ключові слова: безпека даних, шифрування, двофакторна аутентифікація (2FA), захист персональних даних, довіра користувачів.

Abstract: The article analyzes modern approaches to data protection on web platforms, including encryption, two-factor authentication (2FA), event logging, protection against DDoS attacks, and regular software updates. Particular attention is given to error handling to prevent the leakage of confidential information, as well as the importance of updating software components to minimize vulnerabilities. The impact of security technologies on user trust is also examined, emphasizing the importance of transparency and compliance with privacy requirements.

Keywords: data security, encryption, two-factor authentication (2FA), personal data protection, user trust.

Вступ

У сучасному цифровому середовищі захист персональних даних користувачів є важливою частиною будь-якої онлайн-платформи. Оскільки кіберзагрози зростають, необхідно вживати ефективні заходи безпеки для забезпечення конфіденційності та цілісності даних. скільки кіберзагрози зростають, необхідно вживати ефективні заходи безпеки для забезпечення конфіденційності та цілісності даних. Згідно зі звітом IBM за 2023 рік, середня вартість витоку даних становила 4,5 мільйона доларів США, що на 2,3% більше порівняно з 2022 роком. Крім того, у 2024 році кількість кіберінцидентів зросла на 400%, що підкреслює необхідність посилення заходів безпеки. Використовуючи різні методи захисту цих даних, комплексний підхід до безпеки допоможе зменшити ризик і підвищити довіру користувачів [1].

Сучасні підходи до захисту даних користувачів вебплатформ

Вебплатформи можуть стати привабливими цілями для хакерів, оскільки користувачі вводять особисту інформацію, включаючи дані для оплати. Тому важливо впровадити ефективні заходи захисту, для убезпечення даних користувачів.

Одним з ключових методів захисту є шифрування даних, яке забезпечує конфіденційність, цілісність та безпеку інформації. Завдяки шифруванню лише власник і одержувач можуть читати дані. Також воно допомагає запобігти витоку інформації та зловмисним атакам, таким як перехоплення трафіку [2]. Для захисту вебресурсів широко використовується протокол HTTPS, який шифрує дані, що передаються, і забезпечує безпеку під час взаємодії користувача з вебсервером.

Ще одним методом захисту облікових даних є двофакторна аутентифікація (2FA). Це додатковий рівень безпеки, який доповнює пароль або PIN-код, забезпечуючи надійніший захист облікового запису. У разі підозрілої активності, наприклад повторних невдалих спроб входу, обліковий запис може бути автоматично заблоковано. Основними перевагами 2FA є підвищена безпека, захист від крадіжки пароля та надійне просте впровадження, що робить цей метод ефективним засобом попередження несанкціонованого доступу до облікових записів [3].

Важливим заходом безпеки є логування подій, яке дозволяє здійснювати моніторинг та запис усіх ключових дій, таких як входи в обліковий запис, зміни в налаштуваннях та спроби доступу до особистих даних. У разі виявлення підозрілої активності система може автоматично надсилати повідомлення адміністраторам, що дає змогу оперативно реагувати на загрози та запобігати нелегальному доступу [4].

Для захисту від DDoS-атаки, тобто атаки коли система отримує великий потік даних, що перевантажує її ресурси та може спричинити збій, застосовуються різні методи. Одним із ефективних способів є обмеження кількості запитів з однієї IP-адреси (rate limiting). Додатково можна використовувати WAF (Web Application Firewall), який аналізує вхідний трафік і блокує шкідливі запити, зменшуючи ризики атак і забезпечуючи стабільну роботу веб-ресурсу [5].

Підтримка актуальності всіх використаних бібліотек, фреймворків та серверного програмного забезпечення є основним заходом безпеки. Оновлення допомагають усувати вразливості, які можуть бути використані зловмисниками, адже розробники постійно вдосконалюють свої продукти та впроваджують нові механізми захисту. Регулярні системні оновлення забезпечують її стабільність і мінімізують ризики атак.

Обробка помилок є великим аспектом безпеки вебплатформи, оскільки неправильне їх відображення може спричинити витік конфіденційної інформації. Для захисту внутрішньої структури програми помилки слід відобразити у спрощеному вигляді, без технічних деталей. Рекомендується створювати спеціальні HTML-шаблони для кожної помилки, які відповідають зрозумілим повідомленням для користувачів і задаються за типом головної сторінки чи інших розділів сайту, не розкриваючи важливої інформації про систему [6].

Захист конфіденційності є важливою частиною безпеки вебплатформи, особливо ті, які обробляють особисті дані користувачів. Варто лише збирати дані, необхідні для виконання певної дії, наприклад покупки. Це дозволяє знизити ризик витоку персональних даних або несанкціонованого доступу. Крім того, вебсайт повинен відповідати вимогам Загального регламенту захисту даних (GDPR), зокрема щодо згоди користувача, обробки та захисту даних.

Вплив технологій безпеки даних на довіру користувачів до онлайн-сервісів

Технології безпеки даних значною мірою впливають на довіру користувачів до вебсервісів. Користувачі довіряють вебсайтам, які забезпечують надійний захист їхніх особистих і фінансових даних за допомогою методів шифрування, двофакторної аутентифікації та перегляду політики конфіденційності. Впровадження сучасних стандартів безпеки, таких як GDPR, допоможе зміцнити репутацію вашого бренду та забезпечити відповідність міжнародним вимогам. Швидке реагування на інциденти безпеки також є важливим для збереження довіри. Сервіси, які надають користувачам чіткі інструкції щодо обробки даних і можливість контролювати їхні персональні дані, мають вищий рівень довіри. Загалом, захист даних є ключовим фактором у формуванні позитивного іміджу сервісу та його успішності на ринку.

Крім того, користувачі більше довіряють сервісам, які пропонують можливість видалення або анонімізації їхніх даних за запитом. Це дозволяє їм відчувати контроль над власною інформацією та зменшує побоювання щодо її несанкціонованого використання. Також важливим аспектом є реалізація механізмів захисту від витоків даних, наприклад, автоматичне блокування облікових записів у разі підозрілої активності або повідомлення користувачів про потенційні загрози. Довіра зростає, якщо платформи впроваджують багаторівневий захист, включаючи поведінкову аналітику та біометричну автентифікацію. Крім того, користувачі надають перевагу сервісам, які прозоро звітують про випадки порушень безпеки та вжиті заходи для їх усунення. Впровадження функцій самостійного керування налаштуваннями конфіденційності підвищує рівень довіри до компанії та сприяє довготривалим відносинам із клієнтами. У результаті, високий рівень безпеки не лише мінімізує ризики кібератак, а й

формує конкурентну перевагу онлайн-платформ, які прагнуть залучити й утримати клієнтів, забезпечуючи їм безпечний і комфортний користувацький досвід.

Висновки

Забезпечення безпеки даних є важливою складовою будь-якої онлайн-платформи. Від правильного впровадження цих технологій залежить не тільки захист даних, але й загальна репутація компанії, її здатність конвертувати користувачів та підтримувати стабільність роботи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cyber Diges [Електронний ресурс]. – Режим доступу: https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/2023/Cyber%20digest_July_2023_UA.pdf? (дата звернення: 08.03.2025).
2. Що таке шифрування та як воно працює?. [Електронний ресурс]. – Режим доступу: <https://www.kingston.com/ua/blog/data-security/what-is-encryption> (дата звернення: 08.03.2025).
3. Що таке двофакторна аутентифікація (2FA) і як вона працює? [Електронний ресурс]. – Режим доступу: <https://blog.whitebit.com/uk/what-is-two-factor-authentication/#heading-text-7-0> (дата звернення: 08.03.2025).
4. Логуювання: поняття, вимоги, рівні. [Електронний ресурс]. – Режим доступу: <https://training.qateslab.com/blog/technical-articles/logging-in-concepts-requirements-levels/> (дата звернення: 08.03.2025).
5. DDoS атаки і захист від них. [Електронний ресурс]. – Режим доступу: https://www.ukraine.com.ua/blog/hosting_ukraine/ddos-ataki-i-zashchita-ot-nih.html (дата звернення: 08.03.2025).
6. Як показувати повідомлення про помилки. [Електронний ресурс]. – Режим доступу: <https://blog.ithillel.ua/articles/khiuston-u-nas-problemy-abo-yak-pokazuvaty-povidomlennia-pro-pomylyky> (дата звернення: 08.03.2025).

Заболотна Софія Олексіївна – студентка групи 4ПІ-236, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: zbltnsonia2005@gmail.com.

Шевченко Дар'я Григорівна – студентка групи 4ПІ-236, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: dash37979@gmail.com.

Городецький Олександр Васильович – студент групи 4ПІ-236, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: ikorka.vn@gmail.com.

Прокопович Максим Костянтинович – студент групи 4ПІ-236, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: prokopovych2006@gmail.com.

Романюк Оксана Володимирівна – кандидат технічних наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: romaniukoksana@gmail.com.

Науковий керівник: **Войтко Вікторія Володимирівна** – кандидат технічних наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: voitko@vntu.edu.ua.

Zabolotna Sofiia Oleksiivna – student of group 4PI-23b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: zbltnsonia2005@gmail.com.

Shevchenko Daria Hryhorivna – student of group 4PI-23b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dash37979@gmail.com.

Horodetskyi Oleksandr Vasylovych – student of group 4PI-23b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: ikorka.vn@gmail.com.

Prokopovych Maksym Kostiantynovych – student of group 4PI-23b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: prokopovych2006@gmail.com.

Romaniuk Oksana Volodymyrivna – Ph.D., Associate Professor of Software Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: romaniukoksana@gmail.com.

Scientific Supervisor: **Voitko Viktoriia Volodymyrivna** – Ph.D., Associate Professor of Software Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: voitko@vntu.edu.ua.