8. Калакура Я. Українська архівна наука у викликах війни та цифровізації інформаційних ресурсів архівів. *Архіви України*. 2022. Вип. 4(333). С. 126–141. URL: https://au.archives.gov.ua (дата звернення: 05.03.2025).

9. Хромов А. Портал «Архіви Європи» та репрезентація України в європейському просторі оцифрованого культурного надбання. *Архіви України*. 2020. Вип. 2(323). С. 70–80. URL: https://au.archives.gov.ua/ (дата звернення: 05.03.2025)

10. Ковальська Л., Яворська Т., Ковальський Г. Документно-інформаційні ресурси архівів, бібліотек і музеїв: цифрові трансформації та виклики війни. *Бібліотечний вісник.* 2024. № 4. С. 3–18.

УДК 004.056.53:004.738.1

БЕЗПЕКА САЙТА: КОМПЛЕКСНИЙ ПІДХІД ДО ЗАХИСТУ ВІД ЗАГРОЗ

О. В. Черніхевич, О. В. Зелінська

Анотація. У статті розглянуто комплексний підхід до забезпечення безпеки сайта, зокрема захист від хакерських атак, витоку даних та шкідливого програмного забезпечення. Досліджено основні кіберзагрози, як-от SQL-ін'єкції, XSS-атаки. Застосовано методи аналізу вразливостей, оцінки ризиків та впровадження найкращих практик кіберзахисту, включно з багаторівневою аутентифікацією, шифруванням та системами виявлення вторгнень. Основні результати демонструють ефективність комбінованого підходу до захисту вебресурсів, що значно знижує ймовірність атак та забезпечує безпеку даних користувачів.

Ключові слова: безпека сайта, хакерські атаки, витік даних, кіберзагрози, шифрування.

Вступ. У сучасному цифровому світі, де ризики витоку даних та кібератаки набирають усе більшої поширеності, безпека вебресурсів стає критично важливим питанням. Незалежно від того, чи ви є власником бізнесу, веброзробником або адміністратором сайта, дотримання передових заходів кіберзахисту є ключовим для збереження конфіденційності інформації та довіри користувачів. Важливо впроваджувати комплексні стратегії безпеки, щоб гарантувати надійний захист онлайн-платформи від потенційних загроз.

З розвитком інформаційних технологій вебсайти стали невіддільною частиною будь-якого підприємства чи організації. Захист вебресурсу – це не лише питання конфіденційності, а й важливий аспект підтримки репутації компанії та забезпечення безпечного користувацького досвіду. Розглянемо основні методи та підходи, які допоможуть ефективно убезпечити вебсайт [1].

Основна частина. Вразливість вебресурсів та загрози, які з цим пов'язані, стосуються не лише окремих власників сайтів, а й усього інтернет-простору. За статистикою, понад 90 % заражень персональних комп'ютерів відбувається саме через взаємодію з ураженими вебсторінками. Кіберзлочинці постійно шукають слабкі місця в безпеці сайтів, використовуючи їх для поширення шкідливого програмного забезпечення, що може призвести до значних фінансових та репутаційних втрат.

Зараження пристроїв користувачів зазвичай відбувається через впровадження зловмисного коду у вебсторінки. Хакери активно експлуатують вразливості в браузерних компонентах, як-от JavaScript-інтерпретатори, плагіни для відтворення Flash, перегляду PDF-файлів або виконання Java-додатків. Якщо виникає необхідність відкрити потенційно небезпечний сайт, але немає можливості скористатися його безпечною версією, рекомендується тимчасово вимкнути ці компоненти під час перегляду. Це значно знизить ризик зараження шкідливим кодом та допоможе уникнути потенційних загроз.

Таблиця 1

Класифікація загроз

Назва	Загроза	Розповсюдження	Складність захисту	Об'єкт атаки
Code injection	Найвища	Низька	Низька	Скрипт(з привілеями вебсервера)
SQL Injection	Висока	Середня	Середня	База даних
XSS	Середня	Висока	Висока	Кінцевий користувач

Основні типи загроз:

1. Загрози конфіденційності – несанкціонований доступ до даних.

2. Загрози цілісності – несанкціоноване спотворення або знищення даних.
3. Загрози доступності – обмеження або блокування доступу до даних [2].
Відсотковий розподіл загроз вебсайтам наведений на рис. 1.

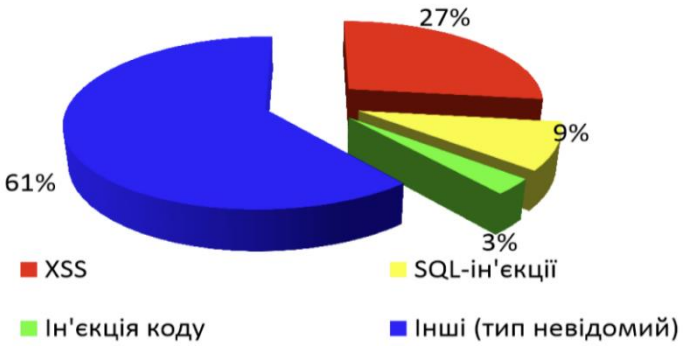

Рис. 1. Відсотковий розподіл загроз вебсайтів

Атаки SQL-ін'єкцій

Одним із найбільш небезпечних видів атак на вебдодатки є SQL-ін'єкції. Ці атаки реалізуються шляхом внесення шкідливих SQL-операторів у введені користувачем дані, які передаються через форми зворотного зв'язку, коментарі, параметри запитів чи інші поля взаємодії. Хакери використовують цю техніку для отримання конфіденційної інформації або внесення змін у базу даних, зокрема додавання нових записів, видалення таблиць чи маніпуляції з правами доступу. Часто зловмисники застосовують цю методику, щоб створити акаунти з розширеними привілеями або підвищити рівень доступу вже наявних користувачів [3]. Приклад вразливого коду SQL, який вразливий для SQL-ін'єкції, представлено на рис. 2.

```
<?php
$username = $_POST[“username”];
$password = $_POST[“password”];

$query = “SELECT * FROM users WHERE username = ‘$username’ AND password = ‘$password’”;
$result = mysqli_query mysqli_query($connection, $query);

if (mysqli_num_rows mysqli_num_rows($result) > 0) {
// вхід в систему пройшов успішно
} else {
// помилка входу в систему
}
?>
```

Рис. 2. Приклад вразливого коду SQL

SQL-ін'єкції становлять значну загрозу для вебсайтів, особливо якщо вони працюють із великими масивами персональних даних. Основна причина появи таких вразливостей – відсутність належної перевірки введених користувачем даних. Наслідки таких атак можуть бути критичними – від викрадення інформації до повного порушення роботи системи, що призводить до фінансових втрат та втрати довіри користувачів.

Щоб ефективно захиститися від SQL-ін'єкцій, необхідно використовувати комплексний підхід, що включає:

– усвідомлення принципів роботи SQL-атак і типових вразливостей;
– використання сучасних інструментів для запобігання виконанню шкідливого коду;
– регулярний аудит безпеки коду та навчання розробників основ кіберзахисту [4].

Міжсайтовий скриптинг (XSS)

XSS-атаки використовують вразливості вебдодатків для впровадження зловмисного скриптового коду, зазвичай на основі JavaScript. Якщо вебресурс не перевіряє та не фільтрує введені користувачем дані, атакуючі можуть інтегрувати шкідливі скрипти через параметри запитів або форми. Коли такий код виконується у браузері жертви, він може перехоплювати конфіденційні дані або змінювати вміст сторінки [5].

Хоча деякі XSS-атаки мають обмежений вплив, у складних сценаріях вони можуть використовуватися для довготривалих атак або як частина ланцюгових атак. Оскільки сучасні вебдодатки на JavaScript працюють не тільки в браузері, але й на серверній стороні (наприклад, у середовищі Node.js), наслідки таких атак можуть бути значно серйознішими.

Для ефективного захисту від XSS важливо:

1. Впроваджувати безпечні методи кодування.
2. Фільтрувати введені користувачем дані та блокувати потенційно небезпечний код. Використовувати політику безпеки контенту (Content Security Policy), що обмежує джерела виконання скриптів.

Автоматизовані інструменти, як-от Invicti DAST, дають змогу ідентифікувати та перевіряти різні види XSS-вразливостей, включаючи відображені, збережені (persistent) та DOM-based атаки [6].

DDoS-атаки

Distributed Denial-of-Service, або розподілена відмова в обслуговуванні – це спрямований вплив на сервер з метою вичерпання його ресурсів та виведення з робочого стану. Основний механізм такої атаки полягає у масовій генерації запитів, які перевантажують сервер, що призводить до його недоступності для звичайних користувачів.

Під час обробки кожного запиту сервер виконує певну послідовність дій: обробляє програмний код вебсторінки, витягує необхідні дані з бази, генерує HTML-документ та надсилає його клієнту. Час, який витрачається на ці процеси, називається серверним часом відповіді. Його тривалість залежить від кількох факторів, серед яких якість коду, оптимізація бази даних та апаратні характеристики серверного обладнання. Два ключові параметри процесора – тактова частота (що визначає швидкість обчислень) і кількість ядер (яка впливає на можливість паралельного виконання операцій) – суттєво впливають на стійкість сервера до навантаження.

DDoS-атаки можуть здійснюватися як автоматизованими бот-мережами, так і реальними користувачами. Використання ботів є менш затратним, однак атаки за участю людей є складнішими для виявлення та блокування, тому можуть бути значно ефективнішими. Водночас навіть високоякісна атака, реалізована ботами, потребує значних фінансових витрат.

Цікаво, що сервери можуть зазнавати значного навантаження не лише через цілеспрямовані атаки, а і внаслідок неправильно спроєктованих алгоритмів. Наприклад, неефективний парсинг вебсторінок без контролю частоти звернень може створити ефект, подібний до DDoS-атаки. Також значний трафік можуть генерувати пошукові роботи, тому власники великих сайтів часто обмежують їх активність для зменшення навантаження на сервер [7–8].

Щоб ефективно протидіяти DDoS-атакам, застосовуються три основні підходи до захисту:

– Програмні рішення – це найбільш поширений спосіб захисту, який передбачає використання спеціалізованих засобів фільтрації трафіка. Такі інструменти розробляються на основі досвіду спеціалістів із кібербезпеки та дають змогу блокувати менш складні атаки, як-от вандалізм або надмірний запит трафіка [9].

– Апаратні рішення – ці методи передбачають створення розподіленої інфраструктури з великим запасом пропускної здатності. Вони широко використовуються у масштабних мережах, зокрема в дата-центрах, великих провайдерів інтернет-послуг та вузлах обміну трафіком.

– Хмарні технології – такі рішення базуються на мережах із високою пропускною здатністю, де інтегровані сервери для автоматичного відсіювання шкідливого трафіка. Цей підхід дає змогу поступово фільтрувати потік даних, мінімізуючи кількість загрозливих запитів та знижуючи ризик перевантаження серверів.

Використання цих методів у комплексі дає змогу значно знизити ймовірність успішного здійснення DDoS-атаки, забезпечуючи стабільність роботи вебресурсу та захист даних користувачів [10–11].

Висновки. Безпека вебсайтів у сучасному цифровому середовищі є критично важливим складником, оскільки кіберзагрози постійно розвиваються, а наслідки атак можуть бути катастрофічними для власників сайтів і їх користувачів. Основні типи загроз, як-от SQL-ін’єкції, XSS-атаки, DDoS-атаки та порушення конфіденційності даних, потребують комплексного підходу до захисту.

Ефективна стратегія безпеки вебресурсів включає в себе правильну обробку введених даних, використання сучасних методів шифрування, впровадження багаторівневої автентифікації, постійний моніторинг активності та регулярні оновлення програмного забезпечення. Також важливо застосовувати надійні механізми захисту від атак, зокрема апаратні та хмарні рішення, що здатні мінімізувати ризики компрометації даних.

Захист вебсайтів є безперервним процесом, який потребує не лише технічних заходів, а й підвищення рівня обізнаності розробників та користувачів. Лише дотримання найкращих практик кібербезпеки дозволяє забезпечити стабільну та безпечну роботу вебресурсів, зберігаючи довіру користувачів і захищаючи критично важливі дані від зловмисників.

Abstract. The article discusses a comprehensive approach to website security, including protection against hacker attacks, data leakage, and malware. The main cyber threats, such as SQL injections, XSS attacks, DDoS attacks, and zero-day exploits, are investigated. Methods of vulnerability analysis, risk assessment, and implementation of cybersecurity best practices, including multi-level authentication, encryption, and intrusion detection systems, are applied. The main results demonstrate the effectiveness of a combined approach to protecting web resources, which significantly reduces the likelihood of attacks and ensures the security of user data.

Keywords: website security, hacker attacks, data leakage, cyber threats, encryption.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Найкращі методи створення безпечних веб-сайтів. *Whileweb.* 01.08.2023. URL: Найкращі методи створення безпечних веб-сайтів | While Web Production (дата звернення: 06.03.2025).

2. Шакуров Є. О. Шляхи захисту змістової частини Web-сайту. *Безпека соціально-економічних процесів в кіберпросторі:* матеріали Всеукр. наук.-практ. конф. (Київ, 27 берез. 2019 р.). Київ: Київ. нац. торг.-екон. ун-т, 2019. С. 130–131. URL: 250dafc576ffd3c6a92546eebacc834d.pdf (дата звернення: 06.03.2025).

3. Найпоширеніші атаки ін'єкцій – CoreWin. *CoreWin.* 29.10.2024. URL: Найпоширеніші атаки ін'єкцій – CoreWin (дата звернення: 07.03.2025).

4. How To Prevent SQL Injection Attacks? Best Practices. *GlobalDots.* 30.06.2023. URL: https://www.globaldots.com/resources/blog/how-to-prevent-sql-injection-attacks/ (дата звернення: 08.03.2025).

5. Jatana N., Agrawal A., Sobti K. Post XSS Exploitation: Advanced Attacks and Remedies. P. 9.

6. Безпека та захист сайту. Як не втратити свій сайт. WEB ROOM. URL: Безпека та захист сайту. Як не втратити свій сайт? (дата звернення: 09.03.2025).

7. Шпінталь М. Я., Орловський Н. М. Методи захисту робочих станцій від DDoS-атак. *ACIT'2014.* Тернопіль (16–17 травня 2014). С. 230–231. URL: Шпінталь М.Я., Орловський Н.М..pdf (дата звернення: 09.03.2025).

8. Reddick C. G. Public administration in the digital age: A review of research and practice. International *Journal of Public Administration.* 2013. Vol. 36(2). P. 77–90.

9. Pigarev Yu., Kosteniuk N. Digitalization of public administration as a factor of digital transformation of Ukraine. Actual problems of public administration. 2021. Vol. 2. P. 92–96. URL: http://uran.oridu.odessa.ua/article/view/237257 (Accessed 01 June 2023).

10. Денисюк В. В., Зелінська О. В. Важливість кібербезпеки в сучасному світі. *Комп'ютерні технології обробки даних:* матеріали II Всеукраїнської науково-практичної конференції (м. Вінниця, 10 грудня 2021 р.). Вінниця: ДонНУ імені Василя Стуса. URL: https://jktod.donnu.edu.ua/article/view/11614

11. Зелінська О. В., Колосова К. К. Огляд методів UX-досліджень під час створення IT-продуктів. *Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса.* 2022. Вип. 14, т. 1. С. 267–270. URL: https://jvestnik-sss.donnu.edu.ua/article/view/12827

УДК 004.738.5:651.7

СТРАТЕГІЇ ЕФЕКТИВНОЇ ЕЛЕКТРОННОЇ КОМУНІКАЦІЇ ДЛЯ УНИКНЕННЯ СПАМУ

І. С. Шпикуляк, О. В. Прігунов

Анотація. У статті розглядаються ефективні стратегії запобігання потраплянню електронних листів до папки «Спам». Описуються технічні аспекти, зокрема налаштування записів SPF, DKIM та DMARC, а також важливість ретельного оформлення тексту листів і врахування поведінки одержувачів. Визначено ключові стратегії, як-от використання релевантних тем, оновлення списків розсилки, налаштування процедури відписки, а також використання онлайн-сервісів для перевірки листів на ризик потрапляння до спаму. Підкреслюється важливість постійної адаптації стратегій електронної комунікації з огляду на еволюцію методів спам-фільтрації.

Ключові слова: спам-фільтрація, репутація відправника, персоналізація листів, онлайн-сервіси для перевірки email.