© Onyshchuk O. SEO and cyberattacks: investigation of web resource security and methods for protecting search engine optimization positions // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 30-31. © This is an open access article under the CC BY 4.0 International license.*

DOI: 10.18372/2225-5036.32.21655

SEO ТА КІБЕРАТАКИ: ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ ВЕБ РЕСУРСІВ І МЕТОДИ ЗАХИСТУ SEO-ПОЗИЦІЙ

Оксана Онищук

Волинський національний університет імені Лесі Українки, Україна



ОНИЩУК Оксана Олександрівна, к.т.н.
Рік та місце народження: 1985 рік, м. Львів, Україна.
Освіта: Державний університет "Житомирська Політехніка", 2024 рік. Луцький національний технічний університет, 2007 рік
Посада: доцент кафедри комп'ютерних наук та кібербезпеки з 2022 року.
Наукові інтереси: технології та методів захисту інформації, обробки даних, проектування мережевої та хмарної безпеки я.
Публікації: більше 80 наукових публікацій, серед яких монографія, наукові статті, матеріали та тези доповідей на конференціях.
E-mail: onyshchuk.oksana@vnu.edu.ua
Orcid: https://orcid.org/0000-0002-8342-3011

Анотація. *У статті досліджено взаємозв'язок між кібербезпекою вебресурсів і забезпеченням стабільності їхніх SEO-позицій у пошукових системах. Актуальність дослідження зумовлена постійним зростанням кількості кібератак, спрямованих не лише на компрометацію інформаційних ресурсів, а й на маніпулювання результатами пошуку, зниження органічного трафіку та погіршення репутації веб сайтів. Проаналізовано сучасні наукові праці, міжнародні стандарти та рекомендації OWASP, Google Search Essentials і NIST щодо захисту веб застосунків та підтримки їхньої пошукової видимості.Практичну частину дослідження виконано на тестовому веб ресурсів із застосуванням автоматизованих та ручних методів тестування. Для оцінювання рівня захищеності використано інструменти OWASP ZAP, SQLMap, Nikto, Google Search Console та Screaming Frog SEO Spider. Проведено тестування на наявність SQL-ін'єкцій, міжсайтового скриптингу (Stored XSS і Reflected XSS), відкритих директорій, відсутності механізмів Rate Limiting, а також виконано аналіз можливостей реалізації SEO spam, SEO poisoning і автоматизованого скрейпінгу контенту.За результатами дослідження встановлено, що найбільшу загрозу для пошукової видимості веб ресурсів становлять SQL-ін'єкції та Stored XSS, які можуть використовуватися для впровадження прихованого контенту, зовнішніх посилань і шкідливого програмного коду. Також підтверджено негативний вплив відсутності захисних HTTP-заголовків, Web Application Firewall, серверної валідації даних та механізмів обмеження частоти запитів на загальний рівень кібербезпеки та SEO-показники ресурсу.Запропоновано комплекс практичних рекомендацій щодо підвищення рівня захищеності веб ресурсів без погіршення їхніх технічних SEO-характеристик. Повторне тестування після впровадження запропонованих заходів підтвердило усунення критичних вразливостей, зменшення рівня SEO-ризиків та збереження коректної індексації веб ресурсу пошуковими системами. Практичне значення роботи полягає у формуванні комплексного підходу до інтеграції методів кіберзахисту та пошукової оптимізації під час розроблення й експлуатації сучасних веб ресурсів.*

Ключові слова: *кібербезпека, SEO, веб ресурс, SQL Injection, XSS, SEO poisoning, SEO spam, OWASP ZAP, Google Search Console, Web Application Firewall.*

Вступ

У сучасному цифровому середовищі веб ресурси є основним інструментом комунікації, електронної комерції та надання інформаційних послуг. Одним із ключових факторів успішного функціонування веб сайтів є їхня видимість у пошукових системах, що забезпечується завдяки пошуковій оптимізації (SEO) [1, 5]. Проте зростання конкуренції в мережі супроводжується збільшенням кількості кібератак, які спрямовані не лише на отримання несанкціонованого доступу до інформації, а й на погіршення позицій сайтів у результатах пошуку [2].

Особливу небезпеку становлять атаки, що поєднують технічні вразливості веб додатків із маніпуляціями пошуковими алгоритмами. До таких загроз належать SQL-ін'єкції, міжсайтовий скриптинг (XSS), SEO spam, SEO poisoning, Negative SEO, контентний скрейпінг та інші способи компрометації веб ресурсів [1–3]. Наслідком їх реалізації можуть бути втрата органічного трафіку, зниження довіри пошукових систем, погіршення репутації ресурсу та накладення санкцій з боку пошукових сервісів [5, 6]. Саме тому дослідження взаємозв'язку між кібербезпекою та SEO є актуальним як для веб розробників, так і для спеціалістів із пошукової оптимізації.

Аналіз існуючих досліджень

Проблема забезпечення безпеки веб ресурсів та збереження їхньої пошукової видимості останніми роками стала предметом активних наукових досліджень. Сучасні роботи демонструють, що кібербезпека веб додатків і пошукова оптимізація є взаємопов'язаними напрямами, оскільки успішні атаки можуть негативно впливати як на функціонування веб ресурсу, так і на його позиції у результатах пошуку [2, 3].

Одним із найбільш актуальних напрямів є дослідження явища SEO poisoning. У роботі Le D. T., Le Dinh T. та Wizee Mungus. [1] проаналізовано механізми використання пошукової оптимізації для поширення шкідливого програмного забезпечення та перенаправлення користувачів на скомпрометовані веб ресурси. Автори підкреслюють необхідність комплексного підходу до захисту веб ресурсів, який поєднує моніторинг SEO-показників,

контроль цілісності контенту та використання сучасних засобів кіберзахисту.

У дослідженні Huang H.-C., Zhang Z.-K., Cheng H.-W. та Shieh S. [2] розглянуто основні загрози безпеці веб застосунків, серед яких SQL-ін'єкції, XSS та CSRF. Автори доводять, що використання параметризованих SQL-запитів, серверної перевірки введених даних і сучасних механізмів автентифікації значно знижує ризик компрометації веб ресурсів.

Систематичний аналіз методів тестування безпеки веб застосунків виконано Aydos M., Aldan Ç., Coşkun E. та Soydan A. [3]. Дослідники порівняли статичний, динамічний і ручний аналіз безпеки та дійшли висновку, що найбільш ефективним є їх комплексне застосування, оскільки воно забезпечує більш повне виявлення потенційних вразливостей.

У роботі Aktas O. та Can A. B. [4] досліджено особливості аналізу веб ресурсів, що активно використовують JavaScript. Запропонований авторами підхід дозволяє підвищити ефективність роботи автоматизованих сканерів і покращити виявлення прихованих загроз, які можуть бути непомітними для традиційних засобів тестування.

Практичні рекомендації щодо підтримки технічного стану веб ресурсів наведено в документації Google Search Essentials [5] та Google Search Console [8]. Методичні матеріали OWASP Top 10 [6] і Web Security Testing Guide [7] визначають перелік найкритичніших вразливостей вебзастосунків та описують сучасні підходи до їх виявлення й усунення.

Аналіз літературних джерел показав, що більшість наукових праць досліджує питання інформаційної безпеки або пошукової оптимізації окремо. Комплексний аналіз впливу кібератак на SEO-показники веб ресурсів залишається недостатньо висвітленим, що обумовлює актуальність проведеного дослідження.

Метою дослідження є аналіз впливу кібератак на SEO-показники веб ресурсів, оцінювання рівня їх захищеності та розроблення рекомендацій щодо мінімізації ризиків втрати пошукових позицій.

Основна частина дослідження

Методи дослідження

Для досягнення поставленої мети використано комплекс теоретичних і практичних методів дослідження. Теоретична частина базувалася на аналізі сучасних наукових публікацій, міжнародних стандартів та рекомендацій щодо кібербезпеки і пошукової оптимізації [1–7].

Практичне дослідження виконувалося на тестовому вебресурсі. Оцінювання рівня його захищеності здійснювалося за допомогою OWASP ZAP, SQLMap, Nikto, Google Search Console та Screaming Frog SEO Spider [5–8]. Проводилося автоматизоване та ручне тестування веб форм, аналіз механізмів автентифікації, перевірка можливості реалізації SQL-ін'єкцій, XSS, SEO spam і контентного скрейпінгу відповідно до рекомендацій OWASP та NIST [6, 7, 10].

Результати дослідження

Практичне дослідження захищеності веб ресурсу виконувалося відповідно до методології OWASP Web Security Testing Guide v4.2 із застосуванням автоматизованих та ручних методів тестування [6, 7]. Перевірка проводилася на спеціально створеному тестовому веб ресурсі в контрольованому середовищі без використання реальних користувацьких даних. Під час дослідження було виконано збір інформації про ресурс, тестування поширених вразливостей веб застосунків, аналіз можливостей реалізації SEO-атак та оцінювання стійкості ресурсу до автоматизованого копіювання контенту.

Результати автоматизованого сканування за допомогою OWASP ZAP підтвердили наявність критичних та середніх вразливостей, серед яких SQL Injection, Stored XSS, Reflected XSS, відсутність захисних HTTP-заголовків і механізмів обмеження частоти запитів (Rate Limiting). Загальний результат сканування наведено на рис. 1.

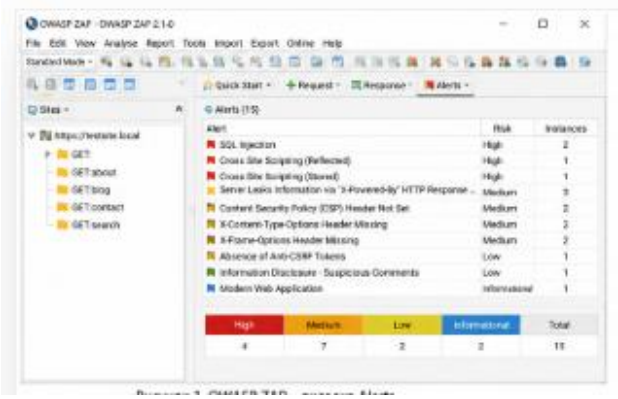


Рис. 1. Результати автоматизованого сканування вебресурсу в OWASP ZAP

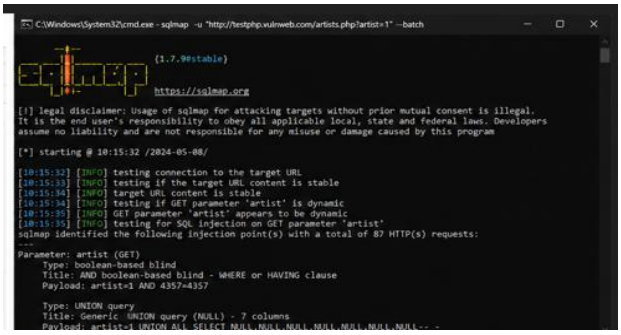


Рис. 2. Результат тестування SQLMap

Під час перевірки SQLMap було встановлено, що форма пошуку є вразливою до SQL-ін'єкцій типу Union-based SQL Injection, що підтверджує можливість отримання несанкціонованого доступу до бази даних та модифікації її вмісту. За шкалою CVSS 3.1 рівень критичності цієї вразливості становить 9,8 бала, що відповідає критичному рівню ризику [2]. Перевірка веб форм також виявила наявність двох різновидів межсайтового скриптингу: Reflected XSS у полі пошуку та Stored XSS у формі коментарів. Найбільшу загрозу становить Stored XSS, оскільки він дозволяє впроваджувати прихований

HTML-код і зовнішні посилання безпосередньо до сторінок сайту, що може бути використано для реалізації SEO spam та погіршення репутації ресурсу. Результати тестування основних вразливостей наведено в табл. 1.

Таблиця 1

Результати тестування веб ресурсу на вразливості

Вразливість	Місце виявлення	CVSS	Потенційний вплив на SEO
SQL Injection	Форма пошуку	9,8	Впровадження прихованого SEO-контенту та посилань у базу даних
Stored XSS	Форма коментарів	8,8	Додавання SEO-spam на сторінки сайту
Reflected XSS	Поле пошуку	6,1	Фішингові атаки, погіршення репутації ресурсу
Open Directory	Каталог */uploads/*	5,3	Полегшення скрейпінгу та розкриття структури сайту
Відсутність Rate Limiting	Веб Форми	5,3	Автоматизований збір контенту, brute-force атаки

Окремим етапом дослідження став аналіз можливостей реалізації SEO spam. Було встановлено, що експлуатація SQL Injection дозволяє змінювати вміст бази даних шляхом додавання прихованого тексту та зовнішніх посилань, які можуть бути проіндексовані пошуковими системами. Крім того, використання Stored XSS створює можливість автоматичного розміщення прихованих рекламних або шкідливих посилань без відома адміністратора сайту. Відсутність перевірки User-Agent також дозволяє реалізувати елементи клоакінгу, коли пошуковим роботам демонструється інший контент, ніж звичайним користувачам [1, 5].

Для оцінювання стійкості веб ресурсу до автоматизованого копіювання інформації було проведено тестування із застосуванням Python-скриптів (Requests, BeautifulSoup4) та фреймворку Scrapy. Результати показали, що весь відкритий контент сайту може бути автоматично скопійований менш ніж за дві хвилини через відсутність механізмів Rate Limiting, CAPTCHA та інших засобів протидії скрейпінгу (рис. 3).

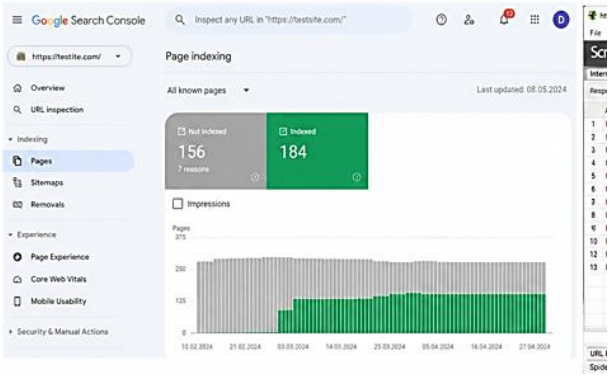


Рис. 3. Результат тестування веб ресурсу на стійкість до scraping

Під час SEO-аудиту за допомогою Google Search Console та Screaming Frog SEO Spider було також виявлено окремі технічні недоліки, що можуть негативно впливати на індексацію ресурсу, зокрема дубльовані метадані, сторінки з кодом відповіді 404 та недостатню оптимізацію структури внутрішніх посилань (рис.4). Узагальнення результатів дослідження показало, що найбільшу небезпеку для SEO-показників веб ресурсу становлять SQL Injection та Stored XSS, які можуть використовуватися для впровадження прихованого SEO-контенту та зовнішніх посилань.

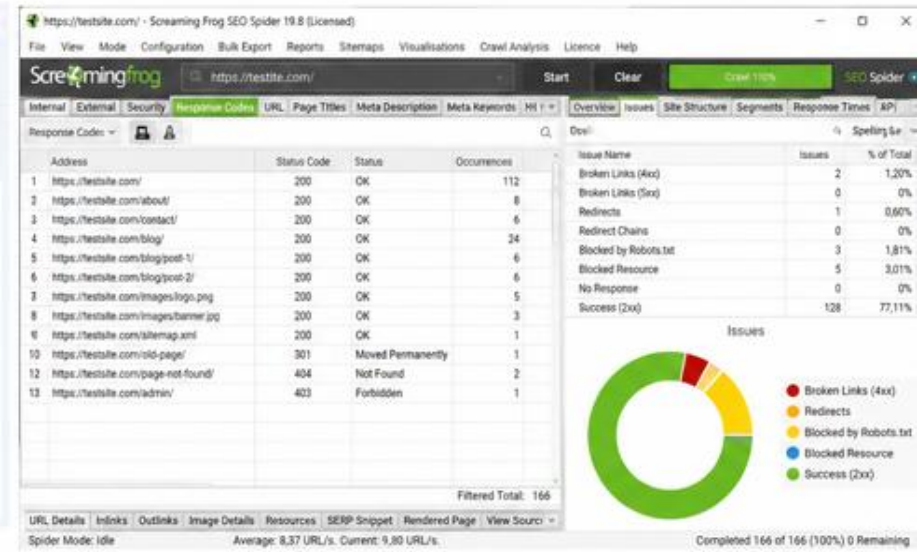


Рис. 4. Результати SEO-аудиту вебресурсу

© Onyshchuk O. SEO and cyberattacks: investigation of web resource security and methods for protecting search engine optimization positions // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 30-31. © This is an open access article under the CC BY 4.0 International license.*

Відсутність механізмів захисту від автоматизованого збору інформації створює додаткові ризики дублювання контенту та втрати його унікальності. За умови експлуатації виявлених вразливостей можливими наслідками є погіршення позицій сайту в результатах пошуку, потрапляння до переліку небезпечних ресурсів Google Safe Browsing та суттєве зменшення органічного трафіку [1, 5, 6].

На основі проведеного дослідження рекомендовано впровадити параметризовані SQL-запити, серверну валідацію введених даних, політику Content Security Policy (CSP), механізми Rate Limiting, Web Application Firewall (WAF), а також здійснювати регулярний моніторинг стану веб ресурсу засобами Google Search Console та періодичний аудит безпеки відповідно до рекомендацій OWASP. Оцінювання ефективності запропонованих заходів захисту. На основі результатів проведеного тестування було сформовано інтегрований перелік основних проблем, які впливають як на рівень кібербезпеки веб ресурсу, так і на його SEO-показники. Аналіз показав, що найбільш критичними є SQL-ін'єкції, Stored XSS, відсутність серверної валідації вхідних даних, механізмів обмеження частоти запитів (Rate Limiting), необхідних HTTP-заголовків безпеки та регулярного моніторингу змін контенту [2, 6, 7].

З метою усунення виявлених недоліків було запропоновано комплекс організаційних і технічних заходів, які включають використання параметризованих SQL-запитів (Prepared Statements), політики Content Security Policy (CSP), Web Application Firewall (WAF), серверної валідації введених даних, двофакторної автентифікації для адміністративної панелі, налаштування захисних HTTP-заголовків, механізмів Rate Limiting та регулярного моніторингу стану веб ресурсу за допомогою Google Search Console [5–10].

Для оцінювання ефективності запропонованих заходів було виконано повторне тестування веб ресурсу після їх впровадження. Отримані результати наведено в табл. 2.

Повторний аудит засвідчив, що впровадження рекомендованих заходів дозволило повністю усунути критичні вразливості та суттєво зменшити кількість потенційних шляхів реалізації SEO-атак. Під час повторного сканування OWASP ZAP не було виявлено критичних попереджень, а SQLMap не підтвердив можливості експлуатації SQL-ін'єкцій.

Крім підвищення рівня інформаційної безпеки, проведений аналіз показав відсутність негативного впливу запропонованих заходів на технічні SEO-показники веб ресурсу. Після впровадження механізмів захисту швидкість відповіді сервера, коректність індексації сторінок і доступність ресурсу для пошукових роботів залишилися на належному рівні, а використання Google Search Console не виявило нових проблем із безпекою чи індексацією.

Отримані результати підтверджують, що сучасні механізми кіберзахисту можуть бути інтегровані у веб ресурс без погіршення його пошукової оптимізації. Навпаки, своєчасне усунення технічних вразливостей сприяє підвищенню довіри пошукових систем, збереженню стабільних SEO-позицій і зменшенню ризику втрати органічного трафіку, що узгоджується з рекомендаціями OWASP, Google Search Essentials та результатами сучасних наукових досліджень [1–7].

Таблиця 2

Порівняння стану безпеки веб ресурсу до та після впровадження заходів захисту

Показник	До впровадження	Після впровадження	Результат
SQL Injection	Вразливий (CVSS 9,8)	Не виявлено	Усунуто
Stored XSS	Вразливий (CVSS 8,8)	Не виявлено	Усунуто
Reflected XSS	Вразливий (CVSS 6,1)	Не виявлено	Усунуто
HTTP Security Headers	Відсутні	Налаштовані	Покращено
Rate Limiting	Відсутній	Активний (10 апитів/с)	Додано
Web Application Firewall	Відсутній	Активний (OWASP RS)	Додано
Захист від scraping	Відсутній	Частково реалізований	Покращено
Загальний рівень SEO-ризику	Високий	Низький	Знижено

У результаті проведеного дослідження встановлено, що наявність технічних вразливостей безпосередньо впливає на пошукову ефективність веб ресурсу. Виявлено потенційні ризики реалізації SQL-ін'єкцій, міжсайтового скриптингу, SEO spam та несанкціонованого копіювання контенту, що узгоджується з результатами сучасних досліджень [2, 3].

Аналіз показав, що успішна експлуатація зазначених вразливостей може призводити до появи прихованих посилань, модифікації HTML-коду сторінок, поширення шкідливого програмного забезпечення та порушення процесу індексації веб ресурсу [1, 2]. Як наслідок, сайт може втрачати органічний трафік, знижувати свої позиції у результатах пошуку або бути позначеним Google як потенційно небезпечний [5, 8].

На основі отриманих результатів запропоновано комплекс заходів щодо підвищення рівня захисту веб ресурсів, який включає використання параметризованих SQL-запитів, серверної перевірки введених даних, політики Content Security Policy (CSP), Web Application Firewall (WAF), механізмів Rate Limiting, регулярного аудиту безпеки та моніторингу SEO-показників [2, 6, 7, 9, 10].

Висновки

Проведене дослідження підтвердило, що забезпечення кібербезпеки є необхідною умовою підтримання стабільної пошукової видимості сучасних веб ресурсів. На відміну від традиційного підходу, за якого інформаційна безпека та SEO розглядаються окремо, результати роботи демонструють їх тісний взаємозв'язок. Експлуатація технічних вразливостей здатна призвести не лише до компрометації інформації, а й до погіршення індексації, втрати органічного трафіку, появи прихованого контенту, накладення санкцій пошуковими системами та зниження довіри користувачів. Практичне тестування тестового веб ресурсу із застосуванням OWASP ZAP, SQLMap, Nikto, Google Search Console та Screaming Frog SEO Spider дозволило виявити критичні вразливості, серед яких SQL Injection, Stored XSS, Reflected XSS, відсутність механізмів Rate Limiting і необхідних HTTP-заголовків безпеки. Отримані результати підтвердили можливість реалізації SEO spam, SEO poisoning, контентного скрейпінгу та інших атак, які негативно впливають на пошукові позиції вебресурсів.

Запропонований комплекс заходів захисту, що включає використання Prepared Statements, Content Security Policy, Web Application Firewall, серверної валідації введених даних, механізмів Rate Limiting, багатофакторної автентифікації та введених даних, механізмів Rate Limiting, багатофакторної автентифікації та постійного моніторингу засобами Google Search Console, забезпечив повне усунення критичних вразливостей під час повторного тестування. При цьому не було зафіксовано негативного впливу на технічні SEO-показники, що підтверджує можливість інтеграції сучасних механізмів кіберзахисту без зниження ефективності пошукової оптимізації.

Наукова новизна роботи полягає у комплексному дослідженні взаємозв'язку між кіберзахистом вебресурсів і стабільністю SEO-позицій із використанням сучасних інструментів тестування безпеки та SEO-аудиту. Практичне значення полягає у розробленні рекомендацій, які можуть бути використані веб розробником, адміністраторами інформаційних систем і фахівцями з пошукової оптимізації для підвищення рівня інформаційної безпеки та забезпечення довгострокової пошукової видимості веб ресурсів.

Перспективами подальших досліджень є розроблення інтелектуальних систем раннього виявлення SEO-атак із використанням методів машинного навчання, автоматизований аналіз змін пошукових алгоритмів та інтеграція засобів безперервного моніторингу безпеки у DevSecOps-процеси.

Література

[1] T., Le Dinh T., Uwizeyemungu S. *Search Engine Optimization Poisoning: A Cybersecurity Threat Analysis and Mitigation Strategies for Small and Medium-Sized Enterprises*. Technology in Society. 2024. Vol. 76. DOI: 10.1016/j.techsoc.2024.102470.

[2] Huang H.-C., Zhang Z.-K., Cheng H.-W., Shieh S. *Web Application Security: Threats, Countermeasures, and Pitfalls*. Computer. 2017. Vol. 50(6). P. 81–85. DOI: 10.1109/MC.2017.183.

[3] Aydos M., Aldan Ç., Coşkun E., Soydan A. *Security Testing of Web Applications: A Systematic Mapping of the Literature*. Journal of King Saud University – Computer and Information Sciences. 2022. Vol. 34(9). P. 6775–6792. DOI: 10.1016/j.jksuci.2021.09.018.

[4] Aktas O., Can A. B. *Making JavaScript Render Decisions to Optimize Security-Oriented Crawler Process*. IEEE Access. 2024. Vol. 12. P. 161688–161696. DOI: 10.1109/ACCESS.2024.3481646.

[5] Google. *Google Search Essentials*. https://developers.google.com/search/docs/fundamentals/seo-starter-guide

[6] OWASP Foundation. *OWASP Top 10: The Ten Most Critical Web Application Security Risks*. https://owasp.org/www-project-top-ten/

[7] OWASP Foundation. *Web Security Testing Guide (WSTG)*. https://owasp.org/www-project-web-security-testing-guide/

[8] Google. *Google Search Console Help*. https://support.google.com/webmasters/

[9] Mozilla Developer Network. *Content Security Policy (CSP)*. https://developer.mozilla.org/docs/Web/HTTP/CSP

[10] National Institute of Standards and Technology (NIST). *Cybersecurity Framework 2.0*. https://www.nist.gov/cyberframework

УДК 004.056:004.738.5:004.774

Onyshchuk O. SEO and cyberattacks: investigation of web resource security and methods for protecting search engine optimization positions

Abstract. *The paper investigates the relationship between web application cybersecurity and the preservation of search engine optimisation (SEO) performance. The growing number of cyberattacks targeting not only information assets but also search engine rankings, website reputation and organic traffic determines the relevance of this research. Current scientific publications, OWASP recommendations, Google Search Essentials and NIST cybersecurity guidelines are analysed to identify effective approaches for protecting web resources while maintaining search visibility. The experimental study was carried out using a dedicated test web application. Security assessment combined automated and manual testing techniques employing OWASP ZAP, SQLMap, Nikto, Google Search Console and Screaming Frog SEO Spider. The testing process included detection of SQL Injection vulnerabilities, Stored and Reflected Cross-Site Scripting (XSS), insecure directory exposure, missing HTTP security headers, insufficient rate limiting and weaknesses enabling SEO spam, SEO poisoning and automated content scraping. The obtained results demonstrate that SQL Injection and Stored XSS represent the most critical threats to website SEO because they enable attackers to inject hidden content, malicious hyperlinks and harmful scripts that may subsequently be indexed by search engines. The study also confirms that inadequate server-side validation, missing Web Application Firewall protection, absent Content Security Policy and poor monitoring significantly increase both cybersecurity and SEO-related risks. Based on the identified vulnerabilities, a comprehensive protection framework is proposed, including prepared SQL statements, Content Security Policy, Web Application Firewall deployment, server-side input validation, rate limiting,*

security headers and continuous monitoring using Google Search Console. Repeated security testing confirmed the elimination of critical vulnerabilities, a significant reduction in SEO risks and preservation of website indexing quality without degrading technical SEO performance. The proposed approach may be applied during the development and maintenance of secure web applications requiring stable search engine visibility.
Keywords: *cybersecurity, search engine optimization, web application security, SQL Injection, XSS, SEO poisoning, SEO spam, OWASP ZAP, Google Search Console, Web Application Firewall.*

ОНИЩУК Оксана Олександрівна*, к.т.н. доцент кафедри комп'ютерних наук та кібербезпеки, Волинський національний університет імені Лесі Українки.*
ONYSHCHUK Oksana Oleksandrivna*, Ph.D., Associate Professor, Department of Information Technology And Cybersecurity, Lesya Ukrainka Volyn National University.*

Дата надходження:	Дата прийняття:	Дата публікації:
29.07.2026	13.08.2026	21.08.2026