УДК 004.056 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.127

# ТЕОРІЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В WORDPRESS

Кутя Б.С.
Науковий керівник – доц. Скорик Ю.В.
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна
email: bohdan.kutia@nure.ua

Information security risk theory is a key aspect in managing the security of WordPress websites. This abstract explores the theoretical framework of risk management in the context of WordPress, one of the most widely used content management systems worldwide. The abstract highlights key risk factors such as vulnerabilities in WordPress core software, themes, and plugins. In addition, it discusses strategies to prevent and mitigate risks, including regular software updates, strong password policies, and implementing security plugins like Wordfence. By understanding and effectively applying information security risk theory, WordPress site owners and administrators can increase the resilience and integrity of their online platforms in the face of emerging cybersecurity challenges.

Ключові слова: WordPress, веб-сайт, плагін, теми.

WordPress — це відкрите програмне забезпечення для створення та керування веб-сайтами та блогами. Як основа для програмного забезпечення PHP і розробників баз даних MySQL. Та для відтворення контенту використовується HTML, CSS, Javascript. WordPress починався як платформа для створення простих веб-сайтів, без особливо складного функціоналу, але з роками перетворився на потужний інструмент для створення веб-сайтів будь-якого типу, включаючи корпоративні сайти, онлайн-магазини, фотогалереї тощо. З можливістю відтворення будь-якого функціоналу.

Однією з основних переваг WordPress є його простота в установці та використанні. Людина без особливих знань може створити свій веб-сайт та розмістити його в інтернеті, для будь-якої задачі. Він має інтуїтивно зрозумілий і легкий у використанні інтерфейс, який дозволяє користувачам без технічних навичок створювати, редагувати та опубліковувати контент на своєму веб-сайті. Крім того, для WordPress існує велика кількість безкоштовних та платних тем і плагінів, що дозволяє розширювати функціональність сайту за допомогою додаткових модулів. Також є можливість використовування білдерів. Для створення одразу візуального вигляду веб-сайту, та функціоналу, але для специфічного функціоналу потрібно мати навички з програмування.

WordPress також відомий своєю гнучкістю та налаштовуваністю. Він дозволяє користувачам створювати унікальний дизайн для свого сайту, використовуючи теми та кастомізуючи їх з використанням власного CSS і HTML. Крім того, завдяки широким можливостям налаштування та плагінам, WordPress може бути адаптований під різні потреби користувачів.

Але з таким різноманітними платними, безплатними темами, плагінами відкривається проблеми з безпекою в Wordpress:

1. Будь-яке програмне забезпечення, WordPress має потенціал до уразливості, які можуть бути використані зловмисниками для злому сайту або отримання несанкціонованого доступу до інформації.
2. Важливо регулярно оновлювати ядро WordPress, теми та плагіни, оскільки це допомагає уникнути використання вразливостей зловмисниками.
3. Слабкі або легко вгадувані паролі можуть бути скомпрометовані зловмисниками, що може призвести до порушення безпеки.
4. Недостатньо не захищені або оброблені запити до бази даних можуть призвести до SQL-ін'єкцій, що може дати зловмисникам виконувати шкідливі запити до бази даних.
5. Не правильно налаштовані права доступу можуть призвести до несанкціонованого доступу до важливої інформації або можливості редагування вмісту.
6. Некоректне налаштування веб-сервера може призвести до потенційних загроз безпеці.
7. Неправильне організування регулярних резервних копій може ускладнити відновлення сайту

Для захисту веб-сайту потрібно не робити ці всі правила, та використовувати провіренні плагині та теми. Та дотримуватися всіх правил, які були перераховані.

Наприклад для захисту веб-сайту можна використовувати плагін Wordfence. Він закриває більшість проблем з безпекою в Wordpress. Можливості Wordfence:

1. Блокує шкідливий трафік: Wordfence аналізує весь трафік на веб-сайті в реальному часі і блокує будь-які спроби несанкціонованого доступу, DDoS-атаки, спамерів і ботів.
2. Виявляє вразливості: автоматично перевіряє веб-сайт на наявність вразливостей в темах, плагінах та ядрі WordPress.
3. Блокує атак на паролі: має функцію блокування авторизації за неправильними паролями, що допомагає уникнути атак перебору паролів.
4. Відшукує віруси та шкідливі програми: сканує веб-сайт на наявність вірусів, шкідливих програм та інших загроз і надає детальний звіт про виявлені проблеми.
5. Оновлює безпеку: автоматично оновлює важливі безпекові скрипти та файли, щоб забезпечити веб-сайт останніми захистами.
6. Фаервол: має вбудований веб-фаервол з додатковими правилами, які допомагають захистити веб-сайт від різних атак.

Список використаних джерел:

1. https://wordpress.org/documentation/
2. https://www.wordfence.com/
3. Hope P., Walther B. Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast. O'Reilly Media, 2008.