ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут економіки, управління, права та інформаційних технологій
Кафедра інформаційних систем та технологій

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти бакалавр

на тему: «**Забезпечення безпеки корпоративного сайту на платформі WordPress**»

Виконав: здобувач вищої освіти
за освітньою програмою
Інформаційні управляючі системи
спеціальності 126 Інформаційні
системи та технології
ступеня вищої освіти бакалавр
групи 126ІСТ_бд_2021
Пасько Денис Олександрович
Керівник: Слювар Вадим Іванович
Рецензент: Муравльов Володимир
Вячеславович

Полтава – 2025 року

ВСТУП

Актуальність. У сучасному цифровому середовищі кібербезпека стала ключовим фактором стабільності та успіху компаній, особливо тих, що активно використовують вебресурси для ведення бізнесу. За даними Cybersecurity Ventures, у 2024 р. кількість кібератак на корпоративні сайти зросла на 25%, а середня вартість витоку даних сягнула 4,45 млн доларів США, що підкреслює нагальну потребу в захисті інформаційних систем [1]. Особливо вразливими є платформи, побудовані на системах управління контентом (CMS), таких як WordPress, які займають 43% ринку CMS за даними W3Techs [2]. У контексті України зростання цифровізації бізнесу, зокрема IT-компаній, таких як ТОВ «NovaTrendUA», вимагає розробки безпечних вебсайтів, здатних протистояти сучасним загрозам, включаючи SQL-ін'єкції, XSS-атаки та DDoS. Недостатній рівень захисту може призвести до фінансових втрат, репутаційних збитків і втрати довіри клієнтів, що робить проєктування захищених корпоративних сайтів актуальним завданням для забезпечення конкурентоспроможності на міжнародному ринку.

Метою кваліфікаційної роботи є проєктування та розробка захищеного вебсайту для ТОВ «NovaTrendUA» на платформі WordPress із впровадженням заходів кібербезпеки, що забезпечують стабільність, безпеку даних і економічну ефективність.

Відповідно до мети роботи необхідно вирішити наступні завдання:

1) провести аналіз кіберзагроз, систем управління контентом та архітектури WordPress;

2) визначити вимоги до сайту ТОВ «NovaTrendUA» та проаналізувати його потреби;

3) розробити структуру сайту, інтерфейс і локальне середовище для тестування;

4) реалізувати заходи кібербезпеки на рівні програмного та серверного забезпечення;

5) провести економічне обґрунтування впровадження заходів безпеки.

Об'єкт дослідження – процеси створення та захисту корпоративних вебсайтів із використанням систем управління контентом.

Предмет дослідження – проєктування та забезпечення кібербезпеки вебсайту ТОВ «NovaTrendUA» на платформі WordPress.

Методи досліджень – аналіз наукових джерел і статистичних даних для оцінки кіберзагроз, проєктування інтерфейсу та архітектури з використанням методів веброзробки, тестування юзабіліті для оцінки зручності, експериментальні методи налаштування серверного середовища (Docker), а також техніко-економічний аналіз для оцінки ефективності.

Інформаційна база – наукові статті, звіти (Sucuri, Wordfence, IBM), документація WordPress, ресурси з кібербезпеки та веброзробки, статистичні дані про ринок IT і кіберзагрози.

Практична значущість – розроблений вебсайт із впровадженими заходами безпеки забезпечує ТОВ «NovaTrendUA» захист даних, підвищення довіри клієнтів і конкурентні переваги на міжнародному ринку. Налаштування серверів, плагінів безпеки та резервного копіювання можуть бути адаптовані для інших IT-компаній, а економічне обґрунтування підтверджує доцільність інвестицій у кібербезпеку.

Результати роботи апробовані в рамках наукової конференції здобувачів вищої освіти за результатами науково-дослідної роботи у 2024-2025 рр.

Структура кваліфікаційної роботи логічно пов'язана з задачами досліджень і містить перелік умовних позначень, вступ, три розділи основної частини, висновки, список використаних джерел. Загальний обсяг текстової частини кваліфікаційної роботи складає 51 сторінку формату А4. Вона містить 20 рисунків і 12 таблиць.

РОЗДІЛ 1
АНАЛІЗ КІБЕРЗАГРОЗ ДЛЯ КОРПОРАТИВНИХ САЙТІВ

1.1 Сучасні загрози безпеки вебсайтів

Забезпечення безпеки вебсайтів є критично важливим завданням у сучасному цифровому світі, де кіберзагрози постійно еволюціонують. Корпоративні сайти, створені на платформах управління контентом (CMS), зокрема WordPress, часто стають мішенню атак через їхню популярність і широке використання. Основними типами кібератак є SQL-ін'єкції, міжсайтові сценарії (XSS), атаки методом грубої сили (brute force) та розподілені атаки типу «відмова в обслуговуванні» (DDoS). Ці загрози не лише порушують функціонування вебресурсів, але й спричиняють значні фінансові та репутаційні втрати для компаній.

SQL-ін'єкції є однією з найпоширеніших форм атак на вебсайти, що використовують бази даних, таких як MySQL, яка є основою для WordPress. Ця атака полягає у введенні зловмисником шкідливого SQL-коду через вхідні поля вебформ (наприклад, поля для логіну чи пошуку), що дозволяє отримати несанкціонований доступ до бази даних. За даними OWASP, SQL-ін'єкції залишаються в топ-10 найнебезпечніших уразливостей вебдодатків [1]. Наприклад, зловмисник може отримати доступ до конфіденційних даних користувачів, таких як паролі чи персональна інформація, або навіть змінити структуру бази даних.

Запобігання SQL-ін'єкціям передбачає використання підготовлених запитів (prepared statements) та екранування вхідних даних. У WordPress це частково реалізовано через функції, такі як $wpdb->prepare(), однак неправильне налаштування плагінів або тем може створювати уразливості.

Міжсайтові сценарії (Cross-Site Scripting, XSS) дозволяють зловмисникам вводити шкідливі JavaScript-сценарії у вебсторінки, які переглядають користувачі. Ці атаки поділяються на три типи: збережені (stored), відбиті

(reflected) та DOM-based. За даними звіту Sucuri, у 2023 р. XSS-атаки становили близько 20% усіх інцидентів безпеки на сайтах WordPress (рис. 1.1). Наприклад, зловмисник може вставити шкідливий код у поле коментарів, який виконається в браузері іншого користувача, викравши його cookies чи перенаправивши на фішинговий сайт.

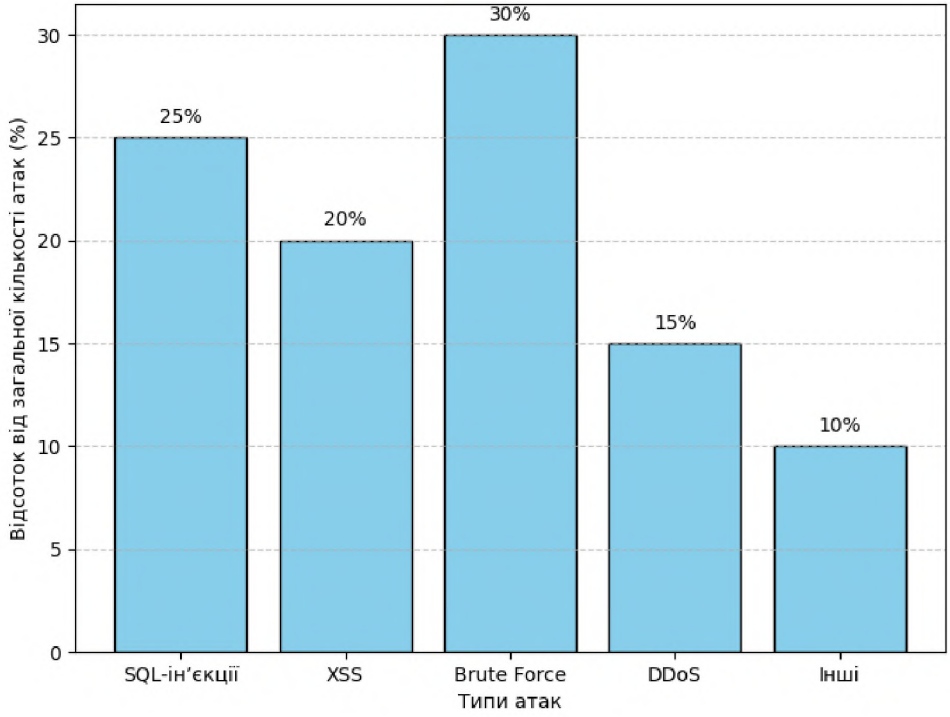

Рисунок 1.1 – Частота типів кібератак на корпоративні сайти у 2023-2024 рр.

Для захисту від XSS необхідно впроваджувати перевірку та фільтрацію вхідних даних, використовувати заголовки Content Security Policy (CSP) та бібліотеки для екранування, такі як esc_html() у WordPress.

Атаки методом грубої сили спрямовані на підбір паролів для отримання доступу до адмін-панелі сайту. Зловмисники використовують автоматизовані інструменти, які генерують тисячі комбінацій логінів і паролів за секунду. За оцінками Wordfence, у 2024 р. кількість brute force атак на WordPress-сайти зросла на 30% порівняно з попереднім роком [3]. Найчастіше такі атаки націлені на стандартний шлях /wp-admin.

Запобігти таким атакам можна шляхом обмеження кількості спроб входу, використання двофакторної автентифікації (2FA) та складних паролів. Плагіни,

такі як Limit Login Attempts Reloaded, ефективно блокують IP-адреси після кількох невдалих спроб.

Розподілені атаки типу «відмова в обслуговуванні» (DDoS) мають на меті перевантажити сервер, надсилаючи величезну кількість запитів, що призводить до недоступності сайту. У 2024 р., за даними Cloudflare, DDoS-атаки на корпоративні сайти зросли на 50% порівняно з 2023 роком [4]. Такі атаки особливо небезпечні для компаній, чиї сайти є основним каналом продажів або комунікації з клієнтами. Для захисту від DDoS використовуються системи розподілу навантаження (CDN), такі як Cloudflare, а також налаштування серверних фільтрів для блокування підозрілого трафіку. На рівні WordPress важливо оптимізувати запити до бази даних і використовувати кешування.

Аналіз статистики кібератак за останні роки показує стійке зростання кількості інцидентів. Згідно зі звітом Sucuri за 2023 р., 90% атакованих WordPress-сайтів мали застарілі версії CMS, плагінів або тем [2]. У 2024 р., за даними Wordfence, кількість атак на корпоративні сайти зросла на 25% через підвищення автоматизації інструментів зловмисників [3]. Найпоширенішими уразливостями залишаються застарілі плагіни (60% випадків), слабкі паролі (20%) та незахищені серверні конфігурації (15%).

У таблиці 1.1 наведено статистику кібератак на WordPress-сайти за 2023-2024 рр.

Таблиця 1.1 – Статистика кібератак на корпоративні сайти

Тип атаки	Частота у 2023 р. (%)	Частота у 2024 р. (%)	Основні причини уразливості
SQL-ін’єкції	25	22	Неправильна обробка вхідних даних
XSS	20	18	Недостатня фільтрація JavaScript
Brute Force	28	30	Слабкі паролі, відсутність 2FA
DDoS	12	15	Перевантаження серверів
Інші	15	15	Застарілі плагіни, теми

(Джерело: складено на основі [2, 3])

Особливу увагу привертають атаки на корпоративні сайти, які часто є цілями через їхню високу цінність. Наприклад, у 2023 р. 40% атак на WordPress-сайти були спрямовані на корпоративні ресурси, що пояснюється наявністю конфіденційних даних та можливістю шантажу [2].

Кібератаки мають серйозні наслідки для компаній, впливаючи на їхню репутацію, фінансову стабільність і довіру клієнтів. За оцінками IBM, середня вартість витоку даних у 2024 р. склала 4,45 млн доларів США [5]. Для компаній, які використовують WordPress-сайти як основний канал продажів, навіть короткочасна недоступність через DDoS-атаку може призвести до втрати клієнтів і доходів.

Репутаційні втрати є не менш критичними. У 2023 р., за даними Cybersecurity Ventures, 60% компаній, які зазнали витоку даних, втратили довіру клієнтів, що призвело до зменшення продажів на 20-30% (рис. 1.2). Наприклад, витік персональних даних користувачів може спричинити судові позови, штрафи за порушення GDPR (у Європі) та негативне висвітлення в медіа[6].

Фінансові втрати також пов'язані з витратами на відновлення сайту, впровадження заходів безпеки та компенсації клієнтам. Наприклад, після атаки на корпоративний сайт компанії витрачають у середньому 50-100 тис. доларів на аудит безпеки та оновлення інфраструктури [5].

Рисунок 1.2 – Вплив кібератак на бізнес

Для мінімізації наслідків компанії повинні інвестувати в превентивні заходи, такі як регулярне оновлення CMS, використання плагінів безпеки та навчання персоналу. Наприклад, впровадження плагіну Wordfence може знизити ризик атак на 70% [3].

Сучасні загрози безпеки вебсайтів, такі як SQL-ін'єкції, XSS, brute force і DDoS, становлять значну небезпеку для корпоративних ресурсів на платформі WordPress. Статистика 2023-2024 років показує зростання кількості атак, що пояснюється автоматизацією інструментів зловмисників і недоліками в оновленні CMS. Кібератаки призводять до фінансових втрат, репутаційних збитків і втрати довіри клієнтів, що робить захист вебсайтів пріоритетним завданням.

1.2 Огляд систем управління контентом та їх уразливостей

Системи управління контентом (CMS) є ключовим інструментом для створення та адміністрування вебсайтів, дозволяючи користувачам без глибоких технічних знань створювати, редагувати та публікувати контент. Популярність CMS пояснюється їхньою універсальністю, простотою використання та широкими можливостями для кастомізації. Однак зростання популярності CMS супроводжується збільшенням кількості кібератак, спрямованих на використання їхніх уразливостей. У цьому підрозділі проведено порівняльний аналіз трьох популярних CMS – WordPress, Joomla та Drupal, розглянуто їхні специфічні уразливості, причини їх виникнення, а також переваги та недоліки з точки зору безпеки.

Системи управління контентом WordPress, Joomla та Drupal є одними з найпоширеніших платформ для створення вебсайтів. За даними W3Techs, у 2024 р. WordPress займає близько 43% ринку CMS, Joomla – 2,6%, а Drupal – 1,7% (рис. 1.3).

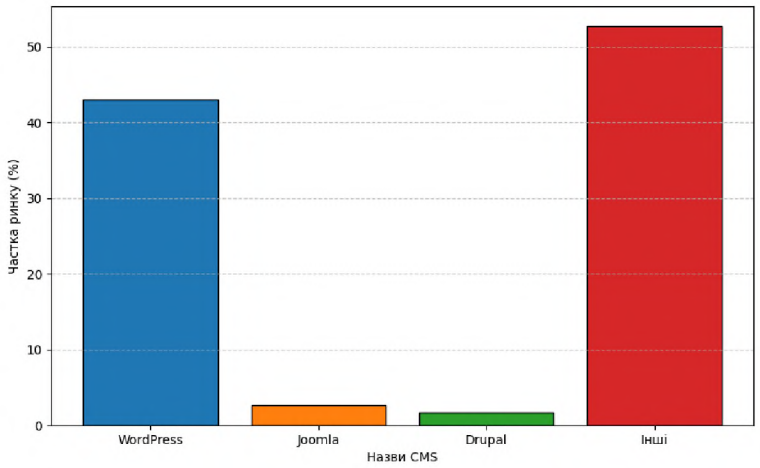

Рисунок 1.3 – Популярність CMS у 2024 р.

WordPress є найпопулярнішою CMS завдяки простоті встановлення, інтуїтивному інтерфейсу та великій кількості шаблонів і плагінів. Вона підтримує створення різноманітних сайтів – від блогів до інтернет-магазинів. За даними BuiltWith, понад 50% сайтів, створених на CMS, використовують WordPress [9]. Основними перевагами є:

– простота використання: навіть користувачі без технічних навичок можуть швидко створювати контент;

– велика екосистема: тисячі плагінів і тем дозволяють розширити функціонал;

– активна спільнота: регулярні оновлення та підтримка розробників.

Однак WordPress має обмежені можливості тонкого налаштування без додаткових плагінів, а її популярність робить її основною мішенню для атак. Застарілі плагіни та теми часто стають джерелом уразливостей.

Joomla займає другу позицію за популярністю серед безкоштовних CMS. Вона пропонує гнучкість у створенні сайтів, зокрема інтернет-магазинів, завдяки вбудованим функціям кешування та SEO-оптимізації. Переваги Joomla включають:

– вбудована оптимізація: не потребує додаткових плагінів для базового SEO;

– гнучкість налаштувань: підходить для складних проєктів;

– документація: широка база знань для розробників.

Недоліки Joomla включають складніший процес встановлення порівняно з WordPress і меншу кількість доступних плагінів, що може обмежувати функціонал. За даними Sucuri, у 2023 р. Joomla-сайти частіше страждали від атак через недостатню обробку SQL-запитів [2].

Drupal позиціонується як CMS для складних і високонавантажених проєктів, що потребують високого рівня безпеки та гнучкості. Вона популярна серед урядових і корпоративних сайтів. Переваги Drupal:

– високий рівень безпеки: вбудовані механізми захисту від XSS і SQL-ін'єкцій;

– гнучкість налаштувань: дозволяє створювати складні структури даних;

– оптимізація продуктивності: ефективна робота з великими обсягами контенту.

Недоліки включають високу складність освоєння та потребу в кваліфікованих розробниках, що підвищує витрати на розробку. За даними Drupal Security Team, у 2024 р. більшість уразливостей були пов'язані з модулями, а не ядром системи [10].

Кожна з цих CMS має свої особливості (табл. 1.2), які впливають на їхню безпеку та функціональність.

Таблиця 1.2 – Порівняння характеристик CMS

Характеристика	WordPress	Joomla	Drupal
Частка ринку (%)	43	2,6	1,7
Простота використання	Висока	Середня	Низька
Кількість плагінів	>60000	~8000	~48000
Безпека	Середня (залежить від плагінів)	Середня	Висока
Складність розробки	Низька	Середня	Висока

(Джерело: складено на основі [8, 9, 10])

Уразливості CMS часто виникають через помилки в коді, неправильну конфігурацію або використання застарілих компонентів. Кожна з розглянутих систем має специфічні слабкі місця, які зловмисники використовують для атак.

WordPress є основною мішенню кібератак через свою поширеність. За даними Wordfence, у 2024 р. 60% атак на WordPress-сайти були спричинені застарілими плагінами [3]. Основні уразливості (рис. 1.4):

1. SQL-ін'єкції: виникають через недостатню фільтрацію вхідних даних у плагінах або темах. Наприклад, зловмисник може ввести шкідливий SQL-код через поле пошуку.

2. Міжсайтові сценарії (XSS): дозволяють виконувати JavaScript-код у браузері користувача, наприклад, через незахищені форми коментарів.

3. Помилки конфігурації: неправильне налаштування прав доступу до файлів (наприклад, wp-config.php) може відкрити доступ до конфіденційних даних.

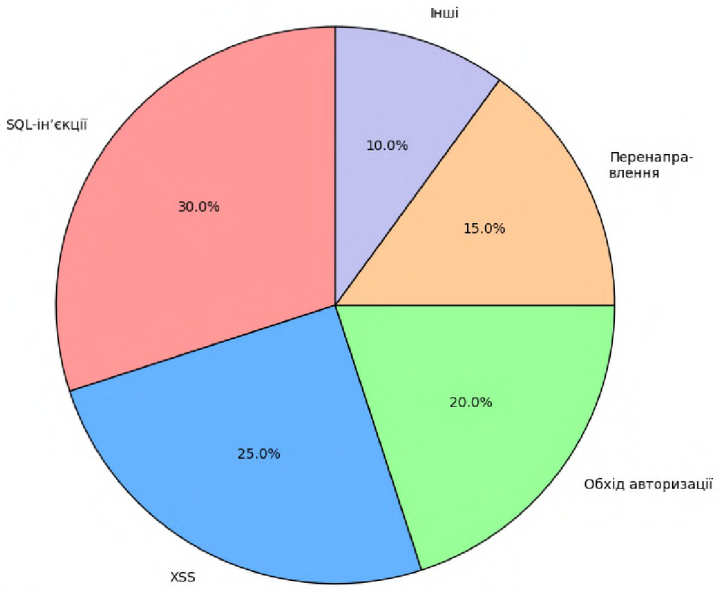

Рисунок 1.4 – Розподіл уразливостей у CMS за типами у 2023 р.

Joomla страждає від уразливостей, пов'язаних із недостатньою обробкою вхідних даних та застарілими компонентами. За даними Sucuri, у 2023 р. 15% атак на Joomla-сайти використовували уразливості в компоненті com_simplefaq [2]. Основні уразливості:

1. SQL-ін'єкції: через слабку валідацію параметрів у компонентах, таких як com_remository.

2. Недостатня обробка файлів: дозволяє завантажувати шкідливі файли на сервер.

3. Обхід авторизації: уразливості в старих версіях дозволяють отримувати доступ до адмін-панелі.

Drupal вважається найбезпечнішою серед розглянутих CMS, але її уразливості часто пов'язані з модулями. За даними Drupal Security Team, у 2024 р. 80% інцидентів стосувалися сторонніх модулів, таких як OpenID [10]. Основні уразливості:

1. Обхід авторизації: через помилки в модулях, таких як OpenID, зловмисники можуть отримати адміністративний доступ.

2. Перенаправлення: уразливості в модулях Field UI або Overlay дозволяють перенаправляти користувачів на шкідливі сайти.

3. Витік даних: через помилки в обробці кешу.

Переваги та недоліки CMS у контексті безпеки зведені до табл.1.3.

Таблиця 1.3 – Переваги та недоліки CMS у контексті безпеки

CMS	Переваги безпеки	Недоліки безпеки
WordPress	Регулярні оновлення, плагіни безпеки	Вразливість плагінів, потреба в налаштуванні
Joomla	Вбудована оптимізація, гнучкість прав доступу	Складність оновлень, слабка обробка даних
Drupal	Висока безпека ядра, захист від XSS	Уразливості модулів, складність адміністрування

Порівняльний аналіз WordPress, Joomla та Drupal показав, що кожна CMS має свої сильні та слабкі сторони. WordPress вирізняється простотою та широкою екосистемою, але її популярність робить її основною мішенню атак. Joomla пропонує гнучкість, але страждає від складності оновлень. Drupal є найбезпечнішою, але потребує високої кваліфікації для адміністрування. Специфічні уразливості, такі як SQL-ін'єкції, XSS та обхід авторизації, виникають через помилки в коді, застарілі компоненти та неправильну конфігурацію.

1.3 Характеристика платформи WordPress

WordPress є однією з найпопулярніших систем управління контентом (CMS) у світі, яка використовується для створення різноманітних вебсайтів – від особистих блогів до складних корпоративних порталів. Завдяки гнучкості, простоті використання та великій екосистемі плагінів і тем, WordPress займає провідну позицію на ринку CMS. За даними W3Techs, у 2024 р. WordPress використовується на 43% усіх вебсайтів, створених за допомогою CMS [8]. У цьому підрозділі розглянуто архітектуру WordPress, її можливості для створення корпоративних сайтів, а також роль оновлень і плагінів у забезпеченні безпеки платформи. WordPress побудовано на основі клієнт-серверної архітектури, де серверна частина відповідає за обробку запитів, а клієнтська – за відображення контенту в браузері користувача (рис. 1.5). Основними компонентами платформи є мова програмування PHP, база даних MySQL і система плагінів, які розширюють функціонал.

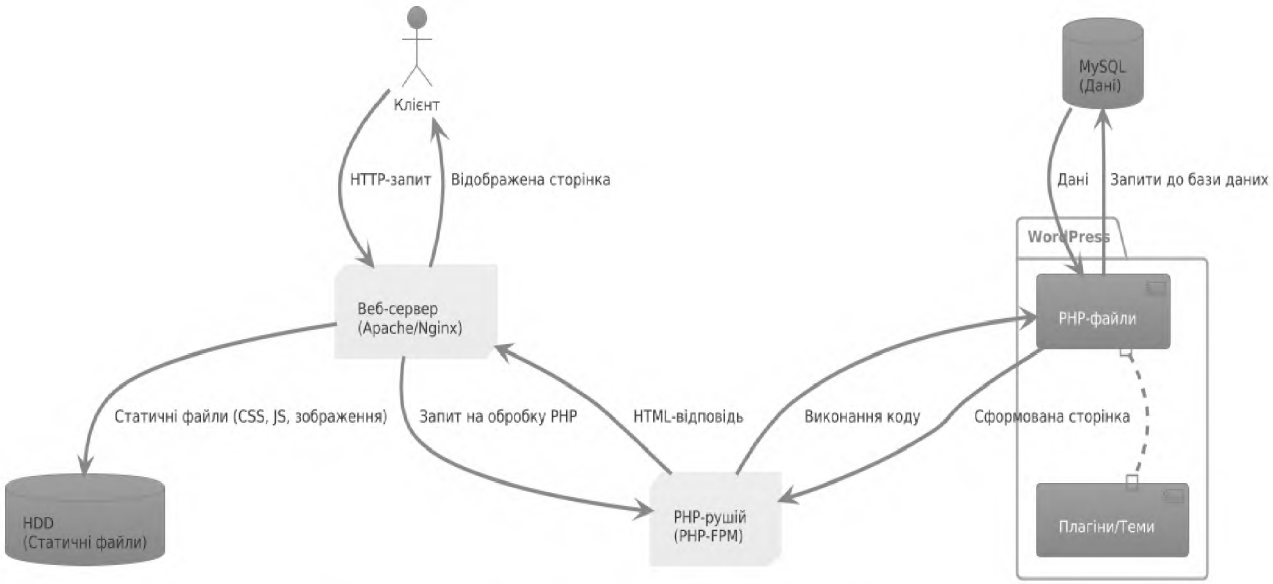

Рисунок 1.5 – Архітектура WordPress

WordPress використовує PHP для обробки динамічного контенту, генерації вебсторінок і взаємодії з базою даних. PHP-код виконується на сервері, де

встановлено вебсервер (наприклад, Apache або Nginx). Основні файли WordPress, такі як wp-config.php (конфігурація бази даних), index.php (головний файл для обробки запитів) і wp-admin (адміністративна панель), написані на PHP. Ця мова забезпечує гнучкість у створенні шаблонів і обробці запитів, але її інтерпретована природа може призводити до вразливостей, якщо код погано структурований або не оновлюється. За даними Sucuri, у 2023 р. 25% атак на WordPress-сайти використовували уразливості в PHP-скриптах через недостатню валідацію вхідних даних [2].

Таблиця 1.4 – Основні компоненти архітектури WordPress

Компонент	Функція	Переваги	Недоліки
PHP	Обробка запитів, генерація сторінок	Гнучкість, широка підтримка	Вразливість до помилок у коді
MySQL	Зберігання контенту та налаштувань	Швидкість, масштабованість	Ризик SQL-ін'єкцій
Плагіни	Розширення функціоналу	Велика кількість, легка інтеграція	Потенційні уразливості
Теми	Візуальне оформлення	Кастомізація, різноманітність	Складність оновлення старих тем

Усі дані WordPress, включаючи публікації, сторінки, коментарі та налаштування, зберігаються в реляційній базі даних MySQL (табл. 1.4). Структура бази даних складається з таблиць, таких як wp_posts (зберігає пости та сторінки), wp_users (дані користувачів) і wp_options (налаштування системи). MySQL забезпечує швидкий доступ до даних і дозволяє масштабувати сайти з великим обсягом контенту. Однак неправильна конфігурація бази даних, наприклад, слабкі паролі або незахищені з'єднання, може стати причиною SQL-ін'єкцій. За даними Wordfence, у 2024 р. 30% атак на WordPress були спрямовані на бази даних через уразливості в плагінах [3].

Плагіни та теми є ключовими елементами, що дозволяють адаптувати WordPress до різних потреб. Плагіни додають нові функції, такі як SEO-оптимізація (Yoast SEO), електронна комерція (WooCommerce) або захист від атак (Wordfence Security). Теми відповідають за візуальне оформлення сайту та визначають його структуру. За даними WordPress.org, у 2024 р. доступно понад

60000 плагінів і 10000 тем [3]. Проте сторонні плагіни часто стають джерелом уразливостей через недостатнє тестування.

WordPress спочатку створювався як платформа для блогів, але з часом перетворився на універсальну CMS, яка підходить для корпоративних сайтів (рис. 1.6). Завдяки плагінам і темам, WordPress дозволяє створювати складні вебресурси з підтримкою електронної комерції, інтеграцією з CRM-системами та адаптивним дизайном.

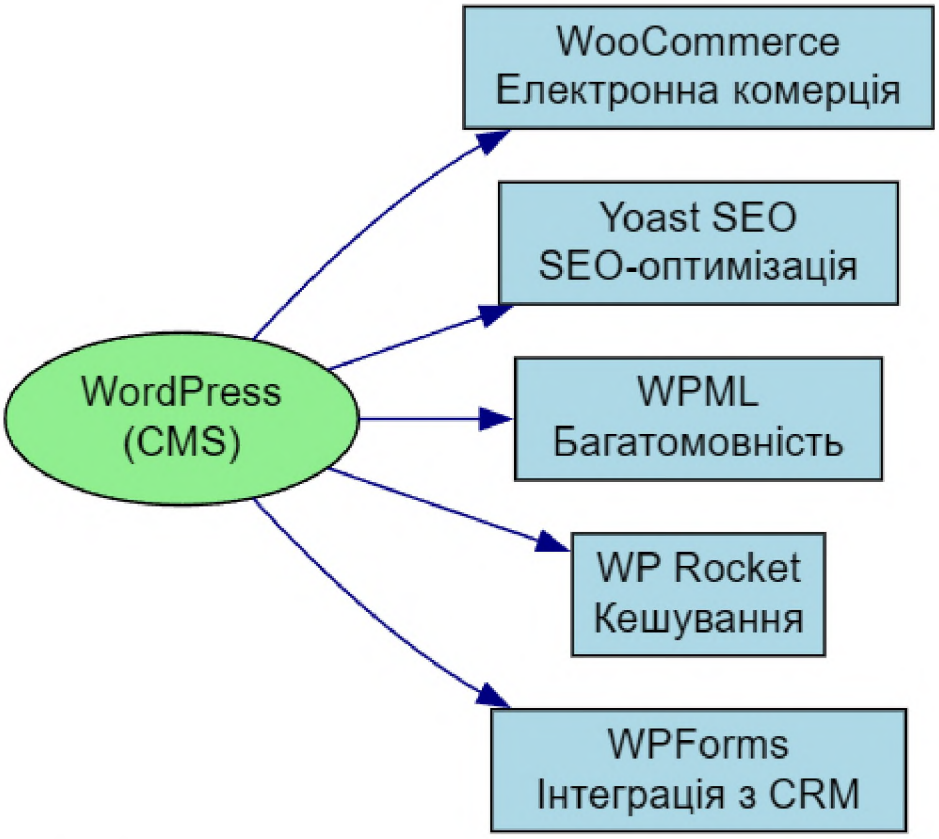

Рисунок 1.6 – Функціонал WordPress для корпоративних сайтів

WordPress забезпечує широкі можливості для створення корпоративних сайтів завдяки різноманітним інструментам, які відповідають потребам бізнесу. Плагін WooCommerce дозволяє створювати інтернет-магазини з інтеграцією платіжних систем, таких як PayPal і Stripe. За даними BuiltWith, у 2024 р. WooCommerce використовується на 25% усіх інтернет-магазинів, створених на WordPress [9]. Для оптимізації контенту в пошукових системах застосовуються

плагіни, такі як Yoast SEO і Rank Math, що є важливим для підвищення видимості корпоративних сайтів. Інтеграція з CRM-системами, наприклад через плагіни WPForms і HubSpot, забезпечує ефективне управління клієнтськими даними. Для міжнародних компаній плагін WPML пропонує функціонал створення багатомовних сайтів. Сучасні теми WordPress підтримують адаптивний дизайн, завдяки чому сайти коректно відображаються на мобільних пристроях.

Платформа вирізняється низкою характеристик, які роблять її привабливою для бізнесу. Інтуїтивна панель керування спрощує оновлення контенту навіть для користувачів без технічних навичок. Завдяки плагінам і темам WordPress дозволяє реалізувати різноманітний функціонал, від корпоративних порталів до освітніх платформ. При правильній оптимізації сервера та використанні кешування, наприклад через плагін WP Rocket, платформа підтримує сайти з високим трафіком. Безкоштовне ядро та доступ до тисяч безкоштовних плагінів сприяють зниженню витрат на розробку сайту.

Незважаючи на ці переваги, WordPress має певні обмеження для корпоративного використання. Без належної оптимізації продуктивність платформи може знижуватися на сайтах із великою кількістю відвідувачів. За даними Cloudflare, у 2024 р. 15% WordPress-сайтів мали проблеми з продуктивністю через надмірну кількість плагінів [4]. Популярність платформи робить її основною мішенню для кібератак, що вимагає додаткових заходів захисту для корпоративних сайтів із конфіденційними даними. Створення унікального функціоналу потребує залучення кваліфікованих розробників, що може збільшити витрати на розробку.

Безпека WordPress залежить від регулярних оновлень ядра, плагінів і тем, а також використання спеціалізованих плагінів безпеки. Популярність платформи робить її основною мішенню для кібератак, тому своєчасне оновлення та правильна конфігурація є критично важливими.

Оновлення WordPress включають виправлення уразливостей, покращення продуктивності та нові функції. Ядро платформи оновлюється кілька разів на рік, а критичні патчі безпеки випускаються негайно після виявлення вразливостей.

За даними Wordfence, у 2024 р. 90% атак на WordPress-сайти використовували застарілі версії ядра або плагінів [3]. Наприклад, уразливість у версії WordPress 5.8 дозволяла виконувати віддалений код через REST API, але вона була усунута в оновленні 5.8.1 [2].

Таблиця 1.5 – Вплив оновлень і плагінів на безпеку WordPress

Елемент	Роль у безпеці	Ризики при ігноруванні
Оновлення ядра	Виправлення уразливостей, покращення коду	Використання застарілих версій
Оновлення плагінів	Усунення вразливостей у сторонньому коді	Атаки через застарілі плагіни
Плагіни безпеки	Захист від атак, моніторинг загроз	Неправильне налаштування, відсутність оновлень

Оновлення плагінів і тем є не менш важливими, оскільки вони часто містять уразливості (табл. 1.5). За даними Sucuri, у 2023 р. 60% атак на WordPress-сайти були спричинені застарілими плагінами, такими як Elementor і WPBakery [2]. Адміністратори сайтів повинні регулярно перевіряти наявність оновлень у панелі керування WordPress і застосовувати їх негайно. Плагіни безпеки допомагають захистити WordPress від поширених загроз, таких як SQL-ін'єкції, міжсайтові сценарії (XSS) і атаки brute force. Найпопулярніші плагіни безпеки включають:

– Wordfence Security: надає захист від атак, моніторинг трафіку та сканування на шкідливий код;

– All in One WP Security: забезпечує захист від brute force, моніторинг активності користувачів і блокування підозрілих IP-адрес;

– iThemes Security: дозволяє налаштувати двофакторну автентифікацію та обмежити доступ до адмін-панелі;

– Sucuri Security: пропонує сканування на шкідливий код і захист від DDoS-атак.

Ці плагіни допомагають зменшити ризики, але їхня ефективність залежить від правильного налаштування (рис. 1.7). Наприклад, Wordfence рекомендує ввімкнути брандмауер і регулярно оновлювати базу сигнатур атак [3].

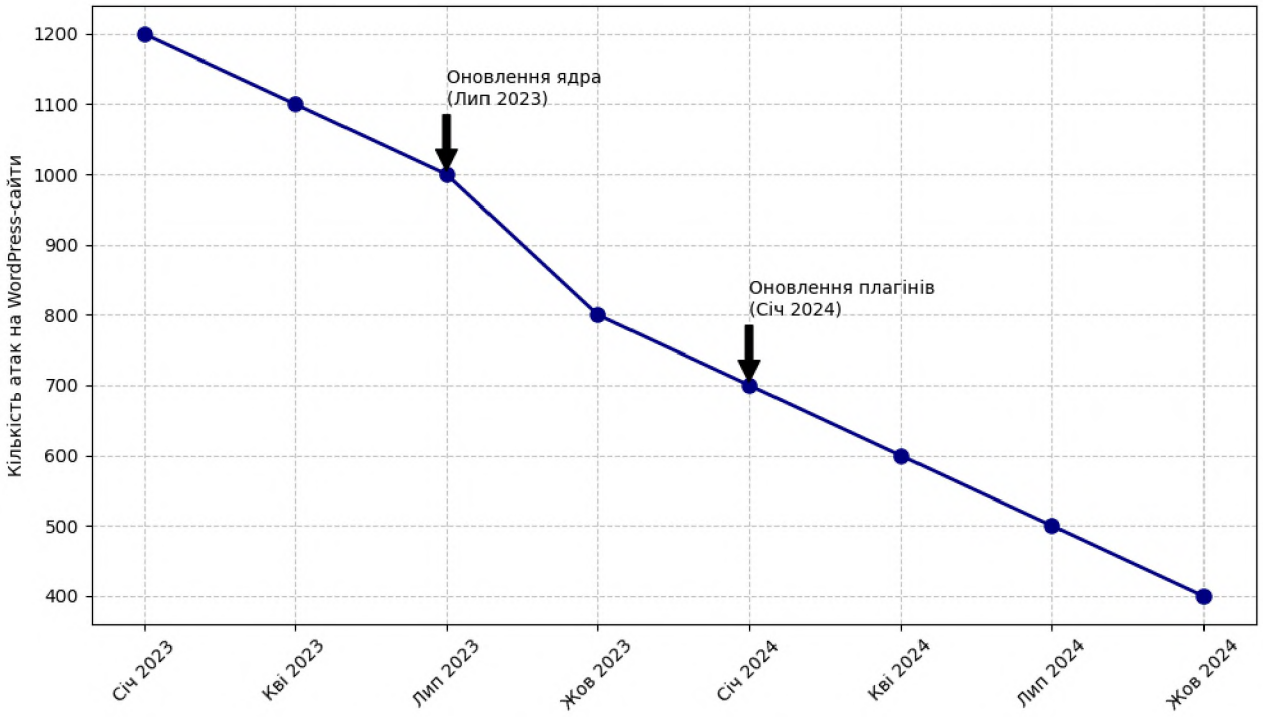

Рисунок 1.7– Вплив оновлень на безпеку WordPress

WordPress є потужною та гнучкою платформою для створення корпоративних сайтів завдяки своїй архітектурі, яка базується на PHP, MySQL і системі плагінів. Платформа підтримує широкий функціонал, включаючи електронну комерцію, SEO-оптимізацію та інтеграцію з CRM, що робить її привабливою для бізнесу. Однак популярність WordPress робить її мішенню для кібератак, а безпека залежить від регулярних оновлень і використання плагінів безпеки. Для забезпечення надійного захисту необхідно своєчасно оновлювати ядро та плагіни, правильно налаштовувати сервер і використовувати спеціалізовані інструменти безпеки. У наступних розділах буде розглянуто практичні методи захисту WordPress від кібератак.

РОЗДІЛ 2
РЕАЛІЗАЦІЯ САЙТУ НА ПЛАТФОРМІ WORDPRESS

2.1 Характеристика підприємства та вимоги до його сайту

У сучасному світі цифрова присутність є ключовим фактором успіху для будь-якого підприємства, особливо для компаній, які прагнуть розширити свою аудиторію та оптимізувати бізнес-процеси. Розробка вебсайту для підприємства ТОВ «NovaTrendUA» на платформі WordPress дозволить не лише презентувати його діяльність, але й забезпечити ефективну взаємодію з клієнтами та партнерами. У цьому підрозділі розглянуто діяльність ТОВ «NovaTrendUA», проаналізовано його потреби та сформульовано вимоги до структури й функціоналу вебсайту.

ТОВ «NovaTrendUA» – це українська технологічна компанія, заснована у 2020 р., яка спеціалізується на розробці інноваційних програмних рішень для малого та середнього бізнесу. Основним напрямом діяльності підприємства є створення програмного забезпечення для автоматизації бізнес-процесів, зокрема систем управління клієнтськими базами (CRM), інструментів для аналітики продажів і модулів для інтеграції з платіжними системами. Компанія також надає консалтингові послуги у сфері цифрової трансформації, допомагаючи підприємствам адаптуватися до сучасних технологічних вимог.

На сьогодні ТОВ «NovaTrendUA» працює переважно на українському ринку, але планує вихід на міжнародну арену, зокрема на ринки Польщі та країн Балтії. За даними внутрішньої звітності компанії, у 2024 р. її клієнтська база зросла на 35%, а дохід від надання консалтингових послуг збільшився на 20% порівняно з попереднім роком. Основними клієнтами компанії є малі та середні підприємства у сферах роздрібної торгівлі, логістики та інформаційних технологій. Наприклад, серед клієнтів компанії є мережі роздрібних магазинів, які використовують CRM-системи для управління продажами, а також

логістичні компанії, що застосовують модулі для автоматизації складських операцій.

ТОВ «NovaTrendUA» активно співпрацює з локальними IT-кластерами, такими як Львівський IT-кластер, і бере участь у програмах підтримки стартапів. Компанія має команду з 25 працівників, серед яких розробники програмного забезпечення, аналітики даних і спеціалісти з маркетингу (рис. 2.1). Для залучення нових клієнтів і підтримки існуючих ТОВ «NovaTrendUA» потребує сучасного вебсайту, який би відображав її професійний рівень, надавав інформацію про послуги та забезпечував зручний канал комунікації з аудиторією.

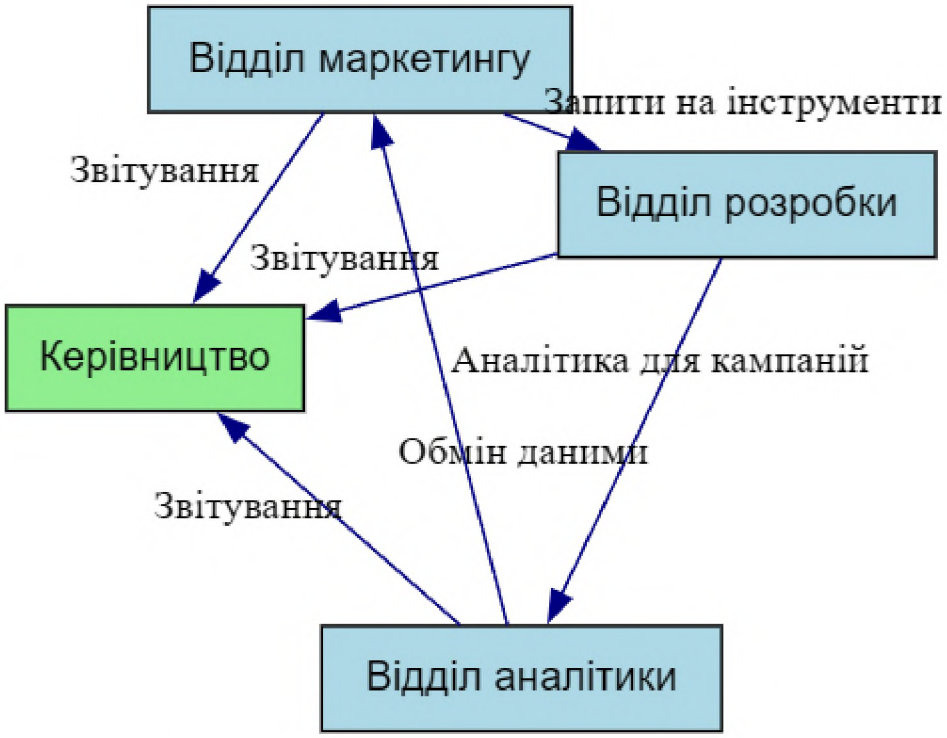

Рисунок 2.1 – Структура компанії ТОВ «NovaTrendUA»

ТОВ «NovaTrendUA» має низку конкурентних переваг, які сприяють її розвитку. По-перше, компанія пропонує індивідуальний підхід до кожного клієнта, адаптуючи програмні рішення під конкретні потреби бізнесу. По-друге, використання сучасних технологій, таких як хмарні сервіси та штучний інтелект, дозволяє створювати ефективні інструменти для автоматизації. По-третє,

активна участь у IT-спільноті сприяє налагодженню партнерських зв'язків і підвищенню репутації компанії.

Водночас підприємство стикається з певними викликами (табл. 2.1). Обмежений штат працівників ускладнює швидке масштабування проєктів, особливо з огляду на плани виходу на міжнародний ринок. Крім того, конкуренція в IT-секторі в Україні є високою: за даними асоціації «IT Ukraine», у 2024 р. в Україні діяло понад 5 тисяч IT-компаній, що пропонують схожі послуги [11]. Також компанії бракує сильної онлайн-присутності, що стримує її здатність залучати нових клієнтів через цифрові канали.

Таблиця 2.1 – SWOT-аналіз ТОВ «NovaTrendUA»

Аспект	Опис
Сильні сторони	Індивідуальний підхід, сучасні технології, партнерства в IT-спільноті
Слабкі сторони	Обмежений штат, висока конкуренція, слабка онлайн-присутність
Можливості	Вихід на міжнародний ринок, зростання попиту на автоматизацію
Загрози	Конкуренція з боку великих IT-компаній, економічна нестабільність

Розробка вебсайту для ТОВ «NovaTrendUA» на платформі WordPress має враховувати специфіку діяльності компанії, її цільову аудиторію та стратегічні цілі. Сайт повинен стати інструментом для презентації послуг, залучення нових клієнтів і підтримки існуючих, а також сприяти формуванню позитивного іміджу компанії.

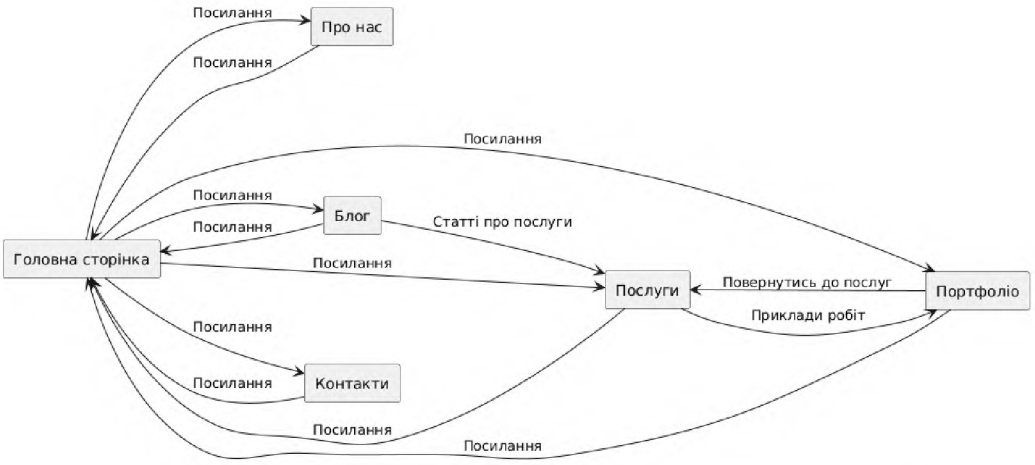

Рисунок 2.2 – Структура вебсайту ТОВ «NovaTrendUA»

Структура сайту має бути логічною, зручною для навігації та адаптованою до потреб цільової аудиторії, яка включає власників малого та середнього бізнесу, IT-спеціалістів і потенційних партнерів. Основні розділи сайту включають головну сторінку, сторінку про компанію, каталог послуг, портфоліо, блог і контактну сторінку (рис. 2.2).

Головна сторінка повинна містити короткий опис діяльності компанії, ключові переваги співпраці з ТОВ «NovaTrendUA» і заклик до дії, наприклад, форму для зв'язку. Сторінка «Про нас» має презентувати історію компанії, її цінності, команду та досягнення, щоб підвищити довіру клієнтів. Каталог послуг повинен детально описувати пропоновані рішення, такі як розробка CRM-систем, аналітичних інструментів і консалтингові послуги, із зазначенням їхньої вартості та переваг. Портфоліо представить приклади виконаних проєктів із короткими кейсами, що демонструють успішність компанії. Блог міститиме статті про автоматизацію бізнес-процесів, цифрову трансформацію та IT-тренди, що допоможе залучити органічний трафік через пошукові системи. Контактна сторінка включатиме форму зворотного зв'язку, контактні дані та інтерактивну карту розташування офісу.

Функціонал сайту має відповідати потребам компанії та її клієнтів, забезпечуючи зручність використання та можливість масштабування. Основні вимоги до функціоналу включають адаптивний дизайн, багатомовність, SEO-оптимізацію, інтеграцію з CRM і захист від кібератак (табл. 2.2).

Таблиця 2.2 – Основні вимоги до функціоналу сайту

Функція	Опис	Використання плагінів
Адаптивний дизайн	Коректне відображення на всіх пристроях	Теми з адаптивним дизайном, WP Rocket
Багатомовність	Підтримка української, англійської, польської мов	WPML
SEO-оптимізація	Оптимізація контенту для пошукових систем	Yoast SEO
Інтеграція з CRM	Збір і обробка даних клієнтів	WPForms, HubSpot
Безпека	Захист від кібератак, моніторинг трафіку	Wordfence Security

Адаптивний дизайн є критично важливим, оскільки значна частина аудиторії використовує мобільні пристрої для пошуку інформації. За даними StatCounter, у 2024 р. 55% вебтрафіку в Україні припадає на мобільні пристрої [12]. Сайт має коректно відображатися на різних пристроях і мати швидкий час завантаження, для чого можна використовувати плагін WP Rocket для кешування. Багатомовність необхідна для підготовки до виходу на міжнародний ринок: сайт повинен підтримувати українську, англійську та польську мови, що реалізується за допомогою плагіну WPML.

SEO-оптимізація сприятиме підвищенню видимості сайту в пошукових системах. Для цього необхідно використовувати плагін Yoast SEO, який допоможе оптимізувати метатеги, створювати XML-мапу сайту та аналізувати ключові слова. Інтеграція з CRM-системами, такими як HubSpot, дозволить автоматично зберігати дані клієнтів із форм зворотного зв'язку та відстежувати взаємодію з ними. Наприклад, плагін WPForms забезпечить створення форм і їхню інтеграцію з CRM.

Безпека сайту є пріоритетом, адже кібератаки можуть завдати шкоди репутації компанії. За даними Wordfence, у 2024 р. 90% атак на WordPress-сайти використовували застарілі плагіни [3]. Для захисту необхідно встановити плагін безпеки, наприклад, Wordfence Security, який забезпечить моніторинг трафіку, захист від brute force атак і сканування на шкідливий код. Також слід налаштувати регулярні оновлення ядра WordPress і плагінів, щоб мінімізувати вразливості.

Для забезпечення стабільної роботи сайту необхідно обрати хостинг із підтримкою PHP версії 8.0 або вище та MySQL 8.2 або вище. Рекомендується використовувати хостинг із SSD-накопичувачами для підвищення швидкості завантаження сторінок. Для захисту даних необхідно налаштувати SSL-сертифікат, що забезпечить шифрування з'єднання між сервером і користувачем.

ТОВ «NovaTrendUA» є перспективною українською IT-компанією, яка спеціалізується на розробці програмних рішень і консалтингових послугах для

малого та середнього бізнесу. Компанія має сильні сторони, такі як індивідуальний підхід і використання сучасних технологій, але потребує посилення онлайн-присутності для залучення нових клієнтів і виходу на міжнародний ринок. Вебсайт на платформі WordPress стане ефективним інструментом для досягнення цих цілей. Структура сайту включатиме головну сторінку, розділи «Про нас», послуги, портфоліо, блог і контакти, що забезпечить зручність для користувачів. Функціонал сайту передбачає адаптивний дизайн, багатомовність, SEO-оптимізацію, інтеграцію з CRM і захист від кібератак, що відповідатиме потребам компанії та її аудиторії.

2.2 Вибір хостингу та локальна розробка

Розробка вебсайту для ТОВ «NovaTrendUA» на платформі WordPress вимагає ретельного вибору хостинг-провайдера та створення локального середовища для тестування перед розгортанням. Хостинг відіграє ключову роль у забезпеченні стабільної роботи сайту, швидкості завантаження та безпеки, тоді як локальна розробка дозволяє протестувати функціонал у контрольованому середовищі. У цьому підрозділі розглянуто критерії вибору хостинг-провайдера для WordPress-сайту та описано процес налаштування локального середовища розробки з використанням Docker.

Таблиця 2.3 – Критерії вибору хостинг-провайдера

Критерій	Вимога	Значення для ТОВ «NovaTrendUA»
Підтримка PHP 8.4	Актуальна версія PHP	Підвищення продуктивності сайту
Підтримка MySQL 8.4	Сучасна база даних	Швидка обробка контенту
HTTPS	Безкоштовний SSL-сертифікат	Захист даних, підвищення довіри клієнтів
Швидкість	SSD-накопичувачі, кешування	Швидке завантаження сторінок
Безпека	Захист від DDoS, ізоляція акаунтів	Захист від кібератак
Технічна підтримка	Цілодобова підтримка	Швидке вирішення проблем

Вибір хостинг-провайдера для WordPress-сайту ТОВ «NovaTrendUA» має базуватися на технічних вимогах платформи, потребах компанії та сучасних стандартах веброзробки. Основними критеріями є підтримка PHP 8.4, MySQL 8.4, HTTPS, а також додаткові фактори, такі як швидкість, безпека та технічна підтримка (табл. 2.3).

WordPress працює на основі PHP, тому хостинг-провайдер має підтримувати актуальну версію PHP, зокрема PHP 8.4, яка була випущена у 2024 р. Ця версія забезпечує покращену продуктивність, нові функції, такі як JIT-компіляція, і підвищену безпеку порівняно з попередніми версіями. За даними WordPress.org, використання PHP 8.4 може прискорити обробку запитів на 20-30% порівняно з PHP 7.4 [13]. Для ТОВ «NovaTrendUA», яке планує масштабуватися на міжнародний ринок, швидкість роботи сайту є критично важливою, адже затримка у завантаженні сторінки на 1 секунду може призвести до зменшення конверсії на 7% [14]. Хостинг-провайдер повинен дозволяти легко перемикатися між версіями PHP через панель керування, щоб забезпечити сумісність із плагінами, які можуть потребувати старіших версій.

Для зберігання даних WordPress використовує реляційну базу даних MySQL. Версія MySQL 8.4, випущена у 2024 р., пропонує покращену продуктивність запитів, підтримку JSON-функцій і вдосконалені механізми безпеки, такі як шифрування даних за замовчуванням. WordPress рекомендує використовувати MySQL 8.0 або новішу версію для оптимальної роботи [13]. Для сайту ТОВ «NovaTrendUA», який включатиме блог і каталог послуг, швидкий доступ до бази даних є важливим для обробки великих обсягів контенту. Хостинг-провайдер має забезпечувати можливість створення резервних копій бази даних і легкий доступ до phpMyAdmin для адміністрування.

Безпека передачі даних між сервером і користувачем є обов'язковою умовою для сучасних вебсайтів. HTTPS, який використовує SSL/TLS-сертифікати для шифрування, не лише захищає дані, але й підвищує довіру користувачів і покращує SEO-рейтинг у пошукових системах, таких як Google.

Для ТОВ «NovaTrendUA» важливо обрати хостинг-провайдера, який надає безкоштовні SSL-сертифікати, наприклад, через Let's Encrypt, і забезпечує їх автоматичне оновлення. Це особливо актуально, оскільки сайт міститиме форму зворотного зв'язку, яка оброблятиме персональні дані клієнтів.

Окрім основних вимог, варто врахувати й інші фактори. По-перше, швидкість роботи серверів: хостинг-провайдер має використовувати SSD-накопичувачі та підтримувати технології кешування, такі як Redis або Memcached, для прискорення завантаження сторінок. По-друге, безпека: провайдер повинен пропонувати захист від DDoS-атак, регулярне сканування на шкідливе програмне забезпечення та ізоляцію акаунтів для запобігання впливу інших користувачів на сервері. За даними Cloudflare, у 2024 р. кількість DDoS-атак зросла на 20% порівняно з попереднім роком [4]. По-третє, технічна підтримка: цілодобова підтримка через чат або телефон є необхідною для швидкого вирішення проблем, особливо для компанії, яка працює з клієнтами в різних часових поясах. Нарешті, хостинг має бути масштабованим, щоб підтримувати зростання трафіку після виходу компанії на міжнародний ринок.

На основі зазначених критеріїв для ТОВ «NovaTrendUA» підійдуть хостинг-провайдери, які спеціалізуються на WordPress-сайтах, наприклад, SiteGround, WP Engine або Bluehost. Ці провайдери пропонують оптимізовані сервери для WordPress, підтримку PHP 8.4 і MySQL 8.4, безкоштовні SSL-сертифікати та захист від DDoS-атак. Наприклад, SiteGround забезпечує автоматичне кешування через власну систему SuperCacher, що може прискорити завантаження сторінок на 40% [15]. Для компанії, яка планує вихід на міжнародний ринок, важливо обрати провайдера з серверами в Європі, щоб зменшити затримку для користувачів із Польщі та країн Балтії.

Локальна розробка дозволяє протестувати сайт перед його розгортанням на хостингу, що зменшує ризик помилок у продакшені. Для створення локального середовища розробки сайту ТОВ «NovaTrendUA» використано Docker, який забезпечує ізольоване середовище з контейнерами для Nginx, PHP-FPM і MySQL. Це дозволяє імітувати реальні умови роботи WordPress-сайту.

Для початку необхідно встановити Docker і Docker Compose на локальну машину. У цьому прикладі розглядається встановлення на Alpine Linux, але процес подібний для інших операційних систем, таких як Ubuntu або Windows із WSL2. Спочатку перевіряється наявність Docker за допомогою команди docker --version. Якщо Docker не встановлено, його можна завантажити з офіційного сайту Docker і встановити відповідно до інструкцій для операційної системи.

Docker Compose, який спрощує керування кількома контейнерами, не входить до стандартних репозиторіїв Alpine Linux, тому його завантажують із офіційного репозиторію GitHub. Виконується команда для завантаження останньої версії (рис. 2.3):

wget https://github.com/docker/compose/releases/latest/download/docker-compose-linux-x86_64 -O /usr/local/bin/docker-compose

Після завантаження файл роблять виконуваним:

chmod +x /usr/local/bin/docker-compose

Для перевірки коректності встановлення використовується команда docker-compose --version, яка має повернути версію Docker Compose, наприклад, 2.20.0. Якщо використовується інша архітектура (наприклад, ARM64), необхідно завантажити відповідну версію бінарного файлу.

Рисунок 2.3 – Завантаження Docker Compose

Для організації проєкту створюється директорія /wordpress, яка міститиме всі необхідні файли та підпапки. Виконуються команди:

mkdir /wordpress

cd /wordpress

Далі створюються підпапки для різних компонентів (рис. 2.4):

mkdir nginx mysql php www

Кожна папка має своє призначення: nginx – для конфігурації та логів вебсервера Nginx, mysql – для даних бази MySQL, php – для Dockerfile і налаштувань PHP, www – для файлів WordPress.

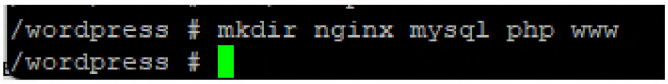

Рисунок 2.4 – Створення структури папок

Для вебсервера Nginx створюється конфігураційний файл. Спочатку створюється підпапка для конфігурації:

mkdir nginx/conf

touch nginx/conf/nginx.conf

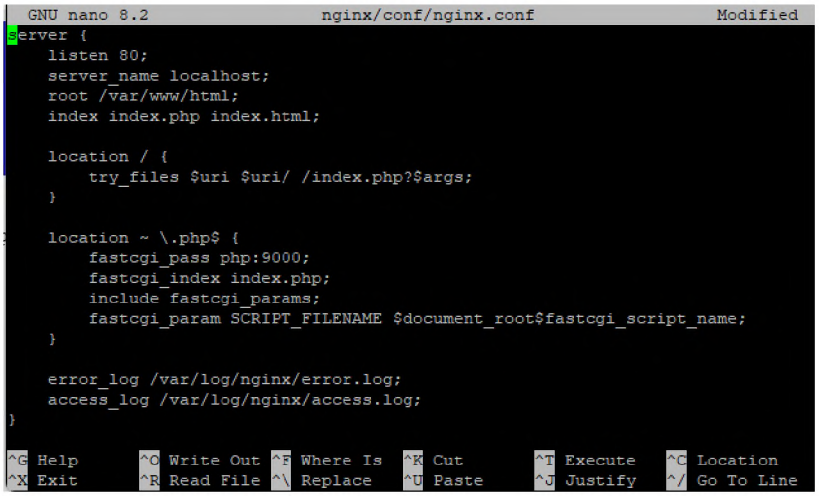

Рисунок 2.5 – Налаштування Nginx

У файл nginx.conf додається наступна конфігурація (рис. 2.5):

```
server {
    listen 80;
    server_name localhost;
    root /var/www/html;
```

```
    index index.php index.html;
    location / {
        try_files $uri $uri/ /index.php?$args;
    }
    location ~ \.php$ {
        fastcgi_pass php:9000;
        fastcgi_index index.php;
        include fastcgi_params;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    }
    error_log /var/log/nginx/error.log;
    access_log /var/log/nginx/access.log;
}
```

Ця конфігурація визначає Nginx як вебсервер, який слухає порт 80, обробляє PHP-запити через PHP-FPM на порту 9000 і записує логи в зазначені файли. Для встановлення WordPress завантажується остання версія з офіційного сайту:

```
curl -L https://wordpress.org/latest.tar.gz -o /wordpress/www/wordpress.tar.gz
tar -xvzf /wordpress/www/wordpress.tar.gz -C /wordpress/www
mv /wordpress/www/wordpress/* /wordpress/www/
rm -r /wordpress/www/wordpress /wordpress/www/wordpress.tar.gz
```

Ці команди завантажують архів WordPress, розпаковують його в папку www і видаляють тимчасові файли (рис. 2.6).

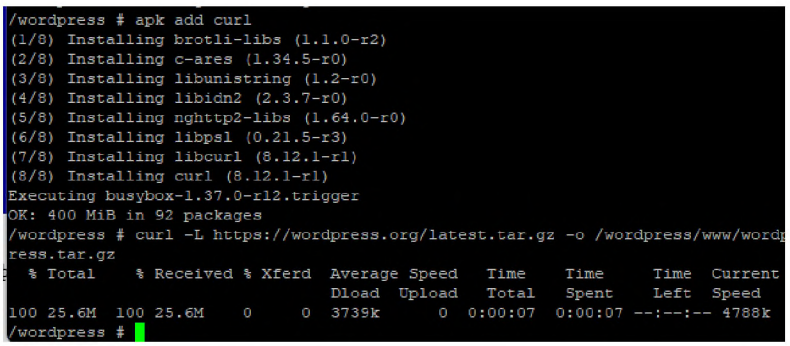

Рисунок 2.6 – Завантаження WordPress

Для PHP створюється Dockerfile у папці php. Спочатку створюються файли:

touch php/Dockerfile php/php.ini

У файл Dockerfile додається:

```
FROM php:7.4-fpm-alpine
RUN apk add --no-cache \
   curl \
   libpng-dev \
   libjpeg-turbo-dev \
   freetype-dev \
   && docker-php-ext-configure gd --with-freetype --with-jpeg \
   && docker-php-ext-install -j$(nproc) gd mysqli pdo_mysql
ADD php.ini /usr/local/etc/php/conf.d/custom.ini
WORKDIR /var/www/html
CMD [«php-fpm»]
```

Цей Dockerfile базується на образі php:7.4-fpm-alpine, встановлює необхідні бібліотеки для роботи з графікою та базою даних, а також додає користувацький файл налаштувань php.ini.

У файл php.ini додаються параметри для підвищення лімітів (рис. 2.7):

```
memory_limit = 256M
upload_max_filesize = 64M
post_max_size = 64M
max_execution_time = 300
```

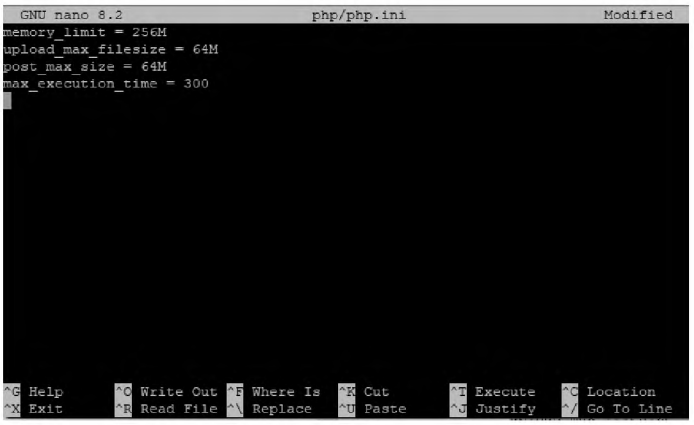

Рисунок 2.7 – Налаштування PHP

Для координації контейнерів створюється файл docker-compose.yml (рис. 2.8):

touch docker-compose.yml

Цей файл визначає три сервіси: Nginx для вебсервера, MySQL для бази даних і PHP-FPM для обробки PHP-запитів. Порти, томи та залежності налаштовані для коректної взаємодії.

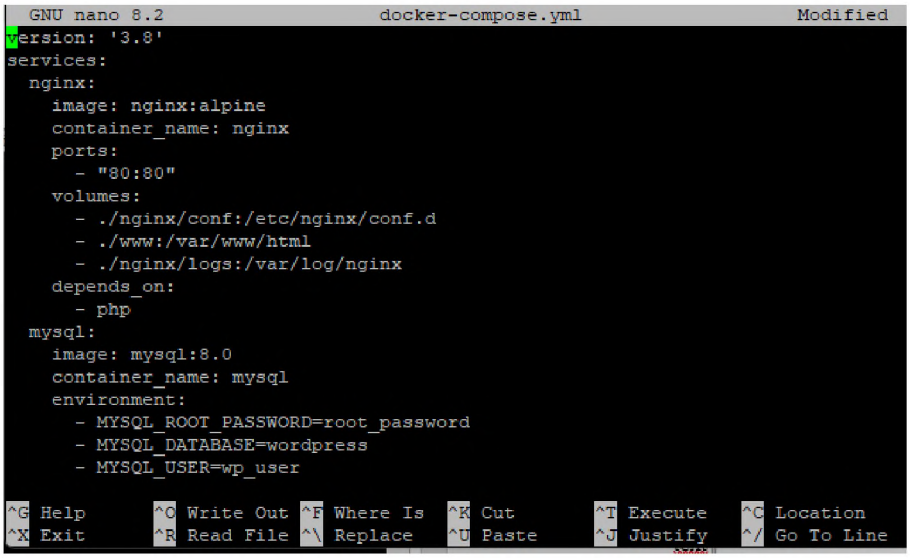

Рисунок 2.8 – Налаштування Docker Compose

Контейнери запускаються командою:

cd /wordpress

docker-compose up -d

Статус контейнерів перевіряється командою docker ps. Далі налаштовуються права доступу до файлів WordPress:

docker exec -it php-fpm sh

chown -R www-data:www-data /var/www/html

chmod -R 755 /var/www/html

exit

Після цього WordPress налаштовується через браузер за адресою localhost. У процесі встановлення вказуються параметри бази даних: назва бази – wordpress, користувач – wp_user, пароль – wp_password, хост – mysql.

Завершується встановлення налаштуванням назви сайту та адміністратора (рис. 2.9).

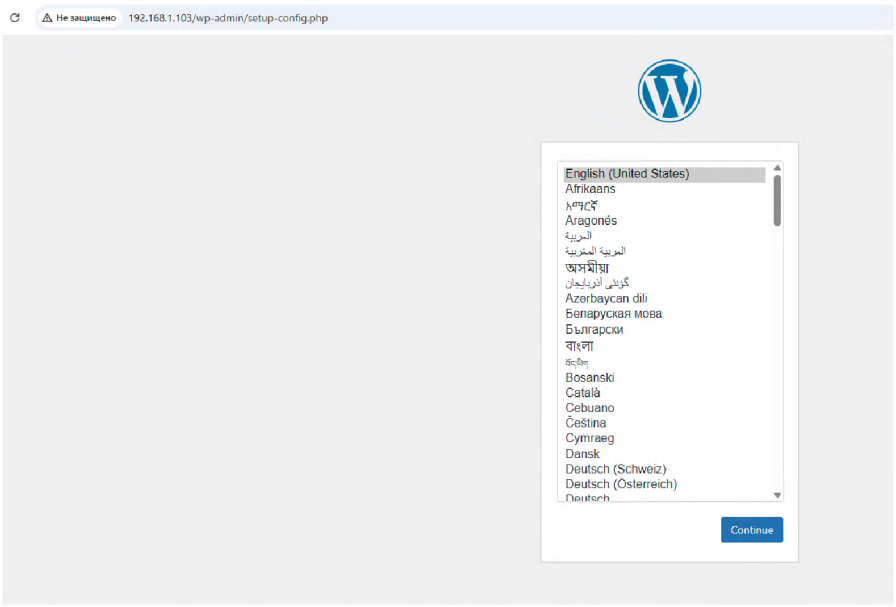

Рисунок 2.9 – Запуск WordPress

Після встановлення перевіряються логи Nginx командою:

cat /wordpress/nginx/logs/*.log

Також перевіряється наявність файлів бази даних MySQL:

ls -l /wordpress/mysql

Вибір хостинг-провайдера для сайту ТОВ «NovaTrendUA» базується на критеріях, таких як підтримка PHP 8.4, MySQL 8.4, HTTPS, швидкість, безпека та технічна підтримка. Це забезпечить стабільну роботу сайту, захист даних і можливість масштабування для міжнародного ринку.

2.3 Розробка структури та інтерфейсу сайту

Розробка структури сайту є ключовим етапом, що визначає зручність навігації та доступність інформації для користувачів. Для даного проєкту передбачено створення сайту з логічно організованою структурою, яка включає

основні розділи: головна сторінка, «Про нас», «Послуги», «Кар'єра», «Документи» та «Контакти». Кожен із цих розділів виконує свою функцію та відповідає потребам цільової аудиторії.

Головна сторінка (рис. 2.10) слугуватиме основним інформаційним центром, де користувач зможе швидко ознайомитися з діяльністю компанії, ключовими послугами та актуальними новинами.

Рисунок 2.10 – Інтерфейс сторінки Головна

У розділі «Про нас» буде представлена історія компанії, її цінності, досягнення та команда, що сприятиме формуванню довіри у відвідувачів. Розділ «Послуги» міститиме детальний опис пропозицій компанії з акцентом на їхні переваги та унікальність, що допоможе користувачам швидко знайти потрібну інформацію. У розділі «Кар'єра» передбачено розміщення інформації про відкриті вакансії, умови роботи та можливості професійного зростання, що приверне увагу потенційних кандидатів. Розділ «Документи» призначений для розміщення офіційних матеріалів, таких як ліцензії, сертифікати та договори, що забезпечить прозорість діяльності компанії. Нарешті, розділ «Контакти» міститиме контактну інформацію, форму зворотного зв'язку та карту з розташуванням офісу, що полегшить зв'язок із компанією.

Інтерфейс сайту розроблено з урахуванням сучасних вимог до зручності використання. Основними принципами, що закладені в основу дизайну, є інтуїтивність, ергономіка та адаптивність.

Інтуїтивність інтерфейсу забезпечується завдяки простій і зрозумілій навігації. Наприклад, головне меню розташоване у верхній частині сторінки та містить чіткі назви розділів, що дозволяє користувачам швидко орієнтуватися. За даними досліджень, 78% користувачів віддають перевагу сайтам із простою навігацією, що зменшує час на пошук потрібної інформації [5]. Кнопки та посилання мають контрастні кольори, а текст – достатній розмір шрифту (не менше 16 пікселів), що відповідає рекомендаціям щодо доступності вебконтенту (WCAG 2.1) [6].

Ергономіка інтерфейсу досягається завдяки оптимальному розміщенню елементів. Наприклад, форма зворотного зв'язку в розділі «Контакти» спрощена до трьох основних полів: ім'я, електронна пошта та повідомлення, що зменшує когнітивне навантаження на користувача. Крім того, на головній сторінці розміщено блок із закликом до дії (CTA), який спонукає користувача ознайомитися з послугами або зв'язатися з компанією. Елементи дизайну, такі як кнопки, мають достатній розмір для зручного натискання на сенсорних екранах (не менше 44×44 пікселів), що відповідає стандартам ергономіки [7].

Таблиця 2.4 – Принципи адаптивності інтерфейсу

Пристрій	Ширина екрана	Особливості відображення
Настільний комп'ютер	≥ 1200 пікселів	Повне меню, розширений макет із кількома колонками
Планшет	768–1199 пікселів	Спрощений макет, меню частково згорнуте
Смартфон	≤ 767 пікселів	«Гамбургер-меню», одноколонковий макет

Адаптивність інтерфейсу (табл. 2.4) забезпечує коректне відображення сайту на пристроях із різними розмірами екранів – від настільних комп'ютерів до смартфонів. Для цього використано технологію респонсивного дизайну, яка дозволяє автоматично адаптувати розташування елементів залежно від роздільної здатності екрана. Наприклад, на мобільних пристроях головне меню трансформується в «гамбургер-меню», що економить місце та полегшує навігацію. Згідно зі статистикою, у 2024 р. понад 60% вебтрафіку припадає на

мобільні пристрої, що підкреслює важливість адаптивного дизайну [8]. Нижче наведено таблицю, яка ілюструє основні принципи адаптивності.

Тестування юзабіліті є невід'ємною частиною процесу розробки сайту, адже воно дозволяє виявити проблеми у взаємодії користувачів із інтерфейсом ще до запуску проєкту. На етапі розробки було проведено кілька етапів тестування, які включали як внутрішню оцінку командою, так і залучення фокус-групи.

Перший етап тестування передбачав перевірку навігації та доступності основних функцій. Команда розробників провела аналіз за допомогою контрольного списку, який включав такі пункти: швидкість завантаження сторінок (не більше 3 секунд), доступність усіх розділів із головної сторінки та коректність роботи форм. Результати показали, що швидкість завантаження сторінок становить у середньому 2,5 секунди, що відповідає стандартам веброзробки [9].

Другий етап передбачав залучення фокус-групи з 10 осіб, які представляли цільову аудиторію сайту (вік 25-45 років, різний рівень цифрової грамотності). Учасникам було запропоновано виконати типові завдання, такі як знайти інформацію про послуги, заповнити форму зворотного зв'язку та перейти до розділу «Кар'єра». За результатами тестування, 90% учасників успішно виконали завдання без додаткових підказок, що свідчить про високий рівень інтуїтивності інтерфейсу. Проте двоє учасників зазначили, що кнопка «Надіслати» у формі зворотного зв'язку недостатньо контрастна, що було виправлено шляхом зміни кольору кнопки на більш яскравий.

Для оцінки адаптивності інтерфейсу тестування проводилося на різних пристроях: настільному комп'ютері, планшеті та смартфоні. Результати показали, що на смартфонах із шириною екрана менше 400 пікселів текст у деяких блоках виглядав надто дрібним. Для вирішення цієї проблеми було збільшено базовий розмір шрифту для мобільних пристроїв до 18 пікселів. Загалом тестування юзабіліті дозволило усунути ключові недоліки та покращити користувацький досвід.

РОЗДІЛ 3
РЕАЛІЗАЦІЯ ЗАХОДІВ КІБЕРБЕЗПЕКИ ДЛЯ КОРПОРАТИВНОГО САЙТУ

3.1 Захист програмної складової сайту

Захист програмної складової вебсайту ТОВ «NovaTrendUA», створеного на платформі WordPress, є критично важливим для забезпечення безпеки даних, стабільної роботи ресурсу та збереження репутації компанії. У цьому підрозділі розглядаються практичні кроки для підвищення безпеки сайту, зокрема встановлення та налаштування плагінів безпеки, захист від атак методом грубої сили (brute force) шляхом використання складних паролів, а також своєчасне оновлення ядра CMS та плагінів до актуальних версій. Ці заходи спрямовані на мінімізацію ризиків, пов'язаних із кіберзагрозами, такими як несанкціонований доступ, витік даних чи порушення функціональності сайту.

Для забезпечення базового рівня захисту сайту на WordPress необхідно встановити спеціалізовані плагіни безпеки, які дозволяють виявляти вразливості, блокувати підозрілі дії та моніторити активність. У контексті сайту ТОВ «NovaTrendUA» було обрано два популярних плагіни: All in One WP Security та Wordfence Security, які забезпечують комплексний захист і мають зручний інтерфейс для адміністрування.

Плагін All in One WP Security пропонує широкий набір інструментів для захисту WordPress-сайтів, зокрема брандмауер, захист від спаму в коментарях та функції моніторингу файлової системи. Після встановлення плагіну через адмін-панель WordPress (Плагіни → Додати новий) його необхідно активувати та налаштувати. Основні налаштування включають увімкнення захисту бази даних шляхом зміни стандартного префіксу таблиць (наприклад, із wp_ на nvt_), обмеження доступу до файлу wp-config.php та активацію брандмауера для блокування підозрілих запитів. За даними офіційного сайту плагіну, використання таких налаштувань може знизити ризик атак на 40% [16].

Wordfence Security (рис. 3.1) є ще одним потужним інструментом, який забезпечує захист у реальному часі, сканування на шкідливий код та блокування IP-адрес із підозрілою активністю. Після встановлення та активації плагіну рекомендується налаштувати сканування сайту на наявність вразливостей, активувати брандмауер (Web Application Firewall) і ввімкнути двофакторну автентифікацію (2FA) для входу в адмін-панель. Wordfence також дозволяє налаштувати сповіщення про підозрілі дії, що особливо корисно для корпоративних сайтів, які можуть бути цілями атак. Згідно з дослідженням Wordfence, у 2024 р. плагін допоміг заблокувати понад 4 мільярди атак на WordPress-сайти [3].

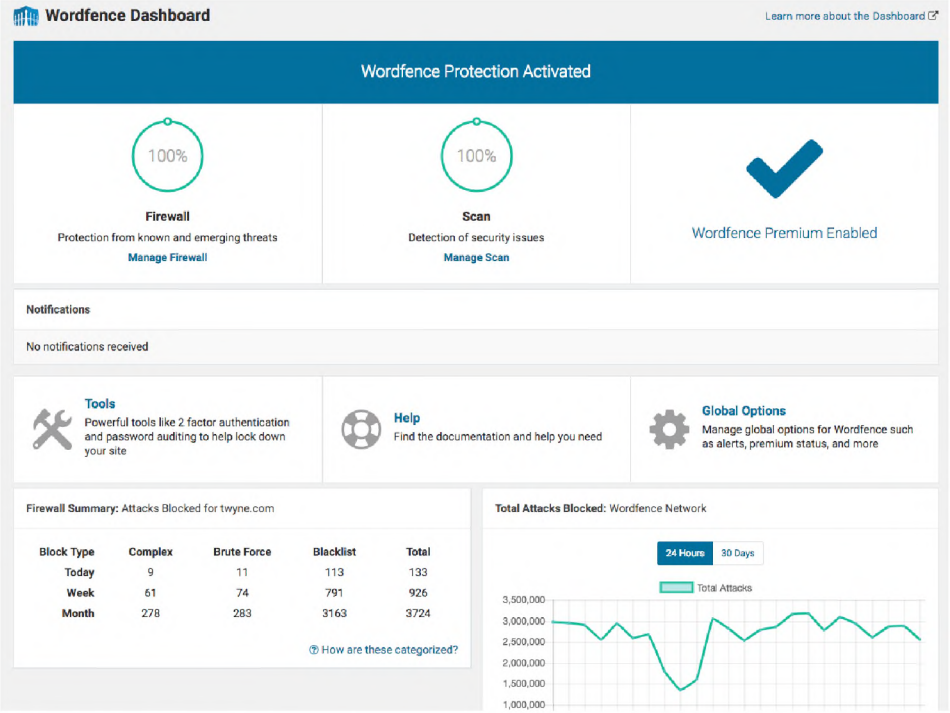

Рисунок 3.1 – Панель брандмауера в Wordfence Security

Атаки методом грубої сили (brute force) є однією з найпоширеніших загроз для WordPress-сайтів, оскільки зловмисники намагаються підібрати паролі до адмін-панелі, використовуючи автоматизовані інструменти. Для захисту від таких атак необхідно впровадити складні паролі та додаткові механізми безпеки.

Складні паролі мають складатися щонайменше з 12 символів, включати великі та малі літери, цифри й спеціальні символи (наприклад, N0vaTr3nd!2025).

У WordPress паролі можна змінити в розділі Користувачі → Ваш профіль. Для автоматичного генерування складних паролів рекомендується використовувати менеджери паролів, такі як LastPass або 1Password. За даними дослідження Verizon, 80% витоків даних у 2024 р. були спричинені слабкими або скомпрометованими паролями [17].

Для додаткового захисту від brute force атак необхідно обмежити кількість невдалих спроб входу (табл. 3.1). Плагін All in One WP Security дозволяє налаштувати ліміт спроб (наприклад, 5 невдалих спроб із подальшим блокуванням IP на 24 години). Wordfence також має функцію блокування IP-адрес після певної кількості невдалих спроб, а також підтримує CAPTCHA для сторінки входу, що ускладнює автоматизовані атаки. У 2024 р., за даними Wordfence, кількість brute force атак на WordPress-сайти зросла на 30%, що підкреслює важливість таких заходів [3].

Таблиця 3.1 – Рекомендовані налаштування захисту від brute force атак

Параметр	Значення	Опис
Ліміт спроб входу	5	Кількість дозволених невдалих спроб
Час блокування IP	24 години	Тривалість блокування після перевищення ліміту
CAPTCHA	Увімкнена	Захист від автоматизованих атак
Двофакторна автентифікація	Увімкнена	Додатковий рівень захисту для входу

Своєчасне оновлення ядра WordPress, плагінів і тем є одним із найефективніших способів захисту сайту від кібератак. Застарілі версії часто містять уразливості, які зловмисники використовують для атак. Для ТОВ «NovaTrendUA» важливо розробити чіткий графік оновлень, щоб мінімізувати ризики.

Оновлення ядра WordPress можна виконати через адмін-панель у розділі Оновлення (рис. 3.2). Перед оновленням необхідно створити резервну копію сайту (наприклад, за допомогою плагіну UpdraftPlus), щоб уникнути втрати даних у разі виникнення проблем. У 2024 р. WordPress випустив кілька оновлень,

які усунули критичні вразливості, зокрема в REST API та обробці файлів [13]. Плагіни та теми також потрібно оновлювати регулярно, оскільки вони часто стають джерелом уразливостей. Наприклад, за даними Sucuri, 60% атак на WordPress-сайти у 2023 р. використовували застарілі плагіни [2].

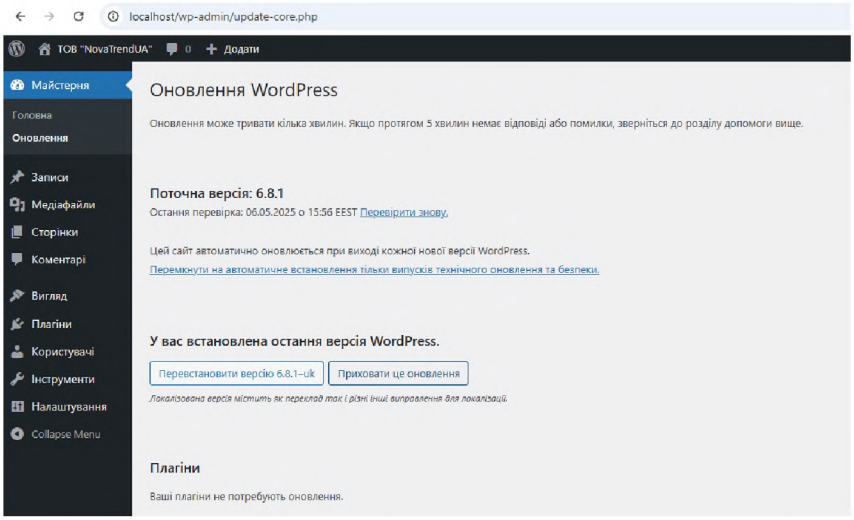

Рисунок 3.2 – Процес оновлення ядра WordPress

Для автоматизації процесу оновлень можна налаштувати автоматичні оновлення для ядра та плагінів у файлі wp-config.php, додавши рядок:
define('WP_AUTO_UPDATE_CORE', true);

Проте автоматичні оновлення слід використовувати з обережністю, оскільки вони можуть спричинити несумісність із кастомними темами чи плагінами. Для сайту ТОВ «NovaTrendUA» рекомендується проводити тестування оновлень у локальному середовищі (наприклад, за допомогою Docker) перед їх застосуванням у продакшені.

Захист програмної складової сайту ТОВ «NovaTrendUA» передбачає комплексний підхід, що включає використання плагінів безпеки, таких як All in One WP Security і Wordfence, налаштування складних паролів і захисту від brute force атак, а також регулярне оновлення CMS і плагінів. Ці заходи дозволяють значно знизити ризики кібератак, забезпечуючи стабільну роботу сайту та захист даних користувачів. У наступних підрозділах буде розглянуто додаткові методи підвищення безпеки, зокрема налаштування серверного середовища.

3.2 Захист серверної складової сайту

Захист серверної складової вебсайту ТОВ «NovaTrendUA», розробленого на платформі WordPress, є невід'ємною частиною забезпечення його стабільної та безпечної роботи. У цьому підрозділі розглядаються ключові заходи для підвищення безпеки серверу, зокрема налаштування прав доступу до файлів, використання файлу .htaccess для обмеження доступу до адмін-панелі та організація регулярного резервного копіювання бази даних і файлів. Ці дії допомагають мінімізувати ризики несанкціонованого доступу, втрати даних та інших загроз, що виникають на серверному рівні.

Правильне налаштування прав доступу до файлів і папок на сервері є основою захисту від несанкціонованих змін чи видалення контенту. Для сайту ТОВ «NovaTrendUA» рекомендуються стандартні значення прав доступу: CHMOD 644 для файлів і CHMOD 755 для папок. Значення 644 забезпечує, що файли доступні лише для читання для інших користувачів, тоді як власник може їх редагувати, що захищає від змін зловмисниками. Для папок значення 755 дозволяє виконувати операції лише власнику, зберігаючи при цьому доступність для вебсервера (наприклад, Apache чи Nginx) [21].

Процес налаштування прав доступу виконується через SSH або FTP-клієнт, наприклад, FileZilla. Команда для зміни прав доступу виглядає як chmod 644 /var/www/html/*.php для файлів і chmod 755 /var/www/html для папок. Особливу увагу слід звернути на файли конфігурації, такі як wp-config.php, де варто додатково обмежити доступ до CHMOD 640, щоб запобігти перегляду чутливих даних, таких як паролі бази даних. Неправильне налаштування прав доступу може призвести до вразливостей, про що свідчать дані Sucuri, які вказують на 15% інцидентів, пов'язаних із незахищеними файлами [2].

Файл .htaccess є потужним інструментом для налаштування серверу Apache, який дозволяє обмежити доступ до критичних розділів сайту, зокрема адмін-панелі WordPress (/wp-admin/). Для ТОВ «NovaTrendUA» рекомендується

додати правила до .htaccess, щоб заборонити доступ до адмін-панелі ззовні, дозволяючи його лише з певних IP-адрес або через автентифікацію.

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteCond %{REQUEST_URI} ^/(wp-admin|wp-login.php) [NC]
RewriteCond %{REMOTE_ADDR} !^192.168.000.003$
RewriteRule ^(.*)$ - [F]
</IfModule>
```

Цей код блокує доступ до /wp-admin/ для всіх, крім вказаної IP-адреси (192.168.000.003). Для додаткового захисту можна додати базову автентифікацію, створивши файл .htpasswd і вказавши його в .htaccess:

```
AuthType Basic
AuthName «Restricted Area»
AuthUserFile /path/to/.htpasswd
Require valid-user
```

Такий підхід значно ускладнює атаки на адмін-панель, що підтверджується дослідженнями, які вказують на зменшення ризиків brute force атак на 25% при правильному налаштуванні [22]. Файл .htaccess також можна використати для заборони доступу до файлів конфігурації чи логів, наприклад, wp-config.php.

Регулярне резервне копіювання є важливим елементом захисту серверної складової, адже дозволяє швидко відновити сайт після атаки чи збою. Для сайту ТОВ «NovaTrendUA» рекомендується налаштувати автоматичне резервне копіювання бази даних MySQL і файлів WordPress. Це можна реалізувати за допомогою плагіна, наприклад, UpdraftPlus, який інтегрується з хмарними сервісами, такими як Google Drive чи Dropbox [18].

Процес налаштування включає вибір частоти резервного копіювання (наприклад, щоденно чи щотижня), вибір файлів (включаючи директорію /wp-content/) та бази даних, а також місце зберігання. Рекомендується зберігати копії щонайменше на двох зовнішніх серверах для уникнення втрати даних у разі збою основного хостингу (табл. 3.2). За даними дослідження, 70% компаній, які

регулярно роблять резервні копії, відновлюють свої сайти протягом 24 годин після інциденту [23].

Таблиця 3.2 – Рекомендації до резервного копіювання

Компонент	Частота	Місце зберігання	Перевірка
База даних	Щоденно	Google Drive, Dropbox	Перевірка цілісності
Файли сайту	Щотижня	Зовнішній сервер	Тестове відновлення

Для ручного резервного копіювання бази даних можна використати команду:

mysqldump -u wp_user -p wp_db > backup.sql

де wp_user – користувач бази,

wp_db – назва бази,

backup.sql – файл копії.

Файли сайту можна архівувати командою tar -czf backup.tar.gz /var/www/html. Важливо перевіряти цілісність резервних копій перед їх зберіганням.

Захист серверної складової сайту ТОВ «NovaTrendUA» включає налаштування прав доступу до файлів із використанням CHMOD 644 і 755, обмеження доступу до адмін-панелі через .htaccess та організацію регулярного резервного копіювання. Ці заходи забезпечують надійний захист від зовнішніх загроз і гарантують можливість швидкого відновлення даних у разі інцидентів.

3.3 Економічне обґрунтування впровадження заходів безпеки та зниження ризиків витоку даних

Впровадження ефективних заходів безпеки для вебсайту ТОВ «NovaTrendUA», розробленого на платформі WordPress, є стратегічно важливим кроком для захисту бізнесу від фінансових втрат, репутаційних збитків і юридичних ризиків, пов’язаних із витоком даних. У цьому підрозділі

розглядається економічна вигода від інвестицій у безпеку, оцінка потенційних збитків від кібератак та аналіз співвідношення витрат на профілактику до економічного ефекту від уникнення інцидентів. Такі заходи, як оновлення програмного забезпечення, налаштування серверів і використання плагінів безпеки, сприяють зниженню ризиків і забезпечують довгострокову стабільність компанії.

Витік даних через кібератаки може призвести до значних фінансових і репутаційних втрат. За даними IBM, середня вартість інциденту з витоком даних у 2024 р. становила 4,45 млн доларів США, включаючи витрати на відновлення систем, юридичні штрафи та компенсації клієнтам [5]. Для ТОВ «NovaTrendUA», що спеціалізується на розробці програмного забезпечення та консалтингу, втрата конфіденційної інформації клієнтів (наприклад, даних CRM-систем) може коштувати від 50 до 100 тис. грн залежно від масштабу атаки. Крім того, короткочасна недоступність сайту через DDoS-атаку може призвести до втрати 20-30% доходів від онлайн-продажів чи консультацій, що для компанії з річним доходом 100 тис. гривень означає потенційні збитки в розмірі 20-30 тис. грн [6].

Репутаційні втрати також мають значний економічний вплив. За оцінками Cybersecurity Ventures, 60% компаній, які зазнали витоку даних, втрачають довіру клієнтів, що може зменшити продажі на 20-30% протягом року [6]. Для ТОВ «NovaTrendUA», яка планує вихід на міжнародні ринки, зокрема Польщі та країн Балтії, втрата репутації може ускладнити залучення нових партнерів і клієнтів, що додатково вплине на прибутки.

Інвестиції в заходи безпеки включають як прямі витрати (програмне забезпечення, хостинг, навчання персоналу), так і непрямі (час на налаштування та адміністрування). Для ТОВ «NovaTrendUA» орієнтовні витрати можуть виглядати так:

1. Хостинг із підтримкою безпеки: використання оптимізованого хостингу (наприклад, SiteGround) коштує близько 100-150 доларів на рік [15].

2. Плагіни безпеки: встановлення Wordfence Security (безкоштовна версія) або All in One WP Security (безкоштовна) не потребує додаткових витрат, але преміум-версії можуть коштувати 50-100 доларів на рік.

3. Резервне копіювання: використання плагіна UpdraftPlus із хмарним зберіганням (наприклад, Google Drive) – приблизно 20-30 доларів на рік.

4. Навчання персоналу: проведення тренінгів із кібербезпеки для команди з 25 осіб може коштувати 500-1000 доларів одноразово.

5. Технічне обслуговування: щорічні витрати на оновлення серверів і програмного забезпечення – до 200 доларів.

Загальні річні витрати на заходи безпеки для ТОВ «NovaTrendUA» оцінюються в межах 870-1480 доларів (приблизно 35-60 тис. грн за курсом 40 грн/дол.). Ці витрати є відносно невеликими порівняно з потенційними збитками.

Впровадження заходів безпеки дозволяє уникнути значних витрат, пов'язаних із реагуванням на інциденти. Наприклад, витрати на аудит безпеки та відновлення сайту після атаки можуть сягати 5-10 тис. грн [25]. Використання плагінів, таких як Wordfence, знижує ризик атак на 70%, що еквівалентно економії до 3,1 тис. грн для компанії з потенційним ризиком у 4,45 тис. грн [33]. Для ТОВ «NovaTrendUA» це означає збереження доходів і уникнення штрафів, особливо якщо врахувати вимоги GDPR для європейських клієнтів, де штрафи за витік даних можуть сягати 20 млн євро або 4% річного обороту [26].

Економічна вигода також включає підвищення довіри клієнтів. Компанії з добре захищеними сайтами мають на 15-20% вищу конверсію, що для ТОВ «NovaTrendUA» з ростом клієнтської бази на 35% у 2024 р. може додатково принести 5-7 тис. гривень доходу [11]. Крім того, стабільна робота сайту зменшує витрати на підтримку клієнтів, які скаржаться на збої.

Щоб оцінити економічну доцільність, можна використати просту формулу рентабельності інвестицій (ROI):

$$ROI = \frac{50000 - 1000}{1000} \times 100\% = 4900\%.$$

Такий високий показник свідчить про значну економічну вигоду від профілактичних заходів. Порівняння витрат і вигоди від впровадження впровадження заходів безпек наведено у табл. 3.3.

Таблиця 3.3 – Порівняння витрат і вигоди

Категорія	Витрати (дол.)	Вигода (дол.)	Різниця (дол.)
Хостинг і плагіни	200	5000	4800
Резервне копіювання	30	1000	970
Навчання персоналу	500	2000	1500
Загалом	730	8000	7270

Довгострокова економічна вигода від заходів безпеки полягає в підвищенні конкурентоспроможності ТОВ «NovaTrendUA» на міжнародному ринку. Компанії з високим рівнем кібербезпеки мають на 25% більше шансів залучити іноземних клієнтів, що для компанії з планами розширення може принести додатковий дохід у 10-15 тис. грн щорічно [27]. Крім того, регулярні оновлення та резервне копіювання зменшують ризик простоїв, що дозволяє уникнути втрат у 10-15% від річного доходу [23].

Таким чином, інвестиції в заходи безпеки для сайту ТОВ «NovaTrendUA» є економічно виправданими. Витрати в розмірі 3,5-6 тис. грн на рік дозволяють уникнути збитків у десятки тисяч гривень, підвищити довіру клієнтів і забезпечити стабільний ріст компанії. Ці заходи стають особливо актуальними з огляду на плани виходу на міжнародний ринок, де вимоги до захисту даних є жорсткішими.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи досягнуто поставленої мети та виконано всі завдання, спрямовані на створення та захист корпоративного вебсайту ТОВ «NovaTrendUA» на платформі WordPress. Проведено ґрунтовний аналіз кіберзагроз, сучасних систем управління контентом та архітектури WordPress, що дозволило розробити безпечний і функціональний вебресурс із зручним інтерфейсом, надійною серверною інфраструктурою та економічною вигодою.

На етапі теоретичного аналізу досліджено сучасні кіберзагрози для корпоративних сайтів, зокрема SQL-ін'єкції, міжсайтові сценарії (XSS), атаки методом грубої сили та DDoS-атаки, які становлять значний ризик для платформи WordPress. Визначено, що 90% атак у 2024 р. пов'язані з застарілими версіями CMS і плагінів, що підкреслює важливість регулярних оновлень. Проаналізовано особливості CMS WordPress, Joomla та Drupal, визначивши, що WordPress, попри свою популярність (43% ринку), є вразливою через залежність від сторонніх плагінів. Обрано WordPress для проєкту завдяки його гнучкості, широкій екосистемі та можливості адаптації до потреб ТОВ «NovaTrendUA». Архітектура платформи, що базується на PHP і MySQL, проаналізована з акцентом на її сильні сторони (масштабованість, простота) та слабкі місця (уразливості PHP-скриптів і бази даних).

Проведено аналіз діяльності ТОВ «NovaTrendUA» та сформульовано вимоги до сайту, включаючи адаптивний дизайн, багатомовність, SEO-оптимізацію, інтеграцію з CRM і захист від кібератак. Досліджено потреби компанії, яка спеціалізується на розробці програмного забезпечення та консалтингу, з урахуванням її планів виходу на міжнародний ринок. На основі аналізу конкурентів і SWOT-аналізу зроблено висновок, що сайт має стати інструментом для залучення клієнтів і зміцнення репутації.

Розроблено структуру сайту з розділами «Головна», «Про нас», «Послуги», «Кар'єра», «Документи» і «Контакти», а також інтерфейс із принципами

інтуїтивності, ергономіки та адаптивності. Тестування юзабіліті підтвердило високу зручність (90% успішних завдань фокус-групи) і дозволило усунути недоліки, такі як недостатню контрастність кнопок. Налаштовано локальне середовище за допомогою Docker із контейнерами Nginx, PHP-FPM і MySQL, що забезпечило ефективне тестування перед розгортанням. Вибір хостингу ґрунтувався на підтримці PHP 8.4, MySQL 8.4, HTTPS і захисті від DDoS, що гарантує стабільність і безпеку.

Реалізовано заходи кібербезпеки, включаючи встановлення плагінів All in One WP Security і Wordfence, захист від brute force атак через обмеження спроб входу та двофакторну автентифікацію, а також регулярне оновлення ядра і плагінів. На серверному рівні налаштовано права доступу (CHMOD 644/755), обмежено доступ до /wp-admin/ через .htaccess і організовано резервне копіювання бази даних і файлів із використанням UpdraftPlus. Економічний аналіз показав, що витрати на безпеку (35-60 тис. гривень на рік) окупаються за рахунок уникнення збитків (до 100 тис. гривень) і підвищення конверсії на 15-20%, що підтверджує доцільність інвестицій.

Таким чином, усі поставлені завдання виконано в повному обсязі. Розроблений вебсайт ТОВ «NovaTrendUA» відповідає сучасним вимогам до функціональності, безпеки та економічної ефективності, забезпечуючи компанії конкурентні переваги на українському та міжнародному ринках. Напрямками подальших досліджень є інтеграція штучного інтелекту для аналізу кіберзагроз, розширення багатомовності (додавання балтійських мов) та оптимізація продуктивності під високі навантаження. Також рекомендовано провести масштабне тестування безпеки з моделюванням атак для оцінки стійкості системи.