НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ФУНКЦІОНУВАННЯ ІНТЕРНЕТ МАГАЗИНІВ»

Виконав: здобувач 5 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Качковський Богдан Романович

Керівник: к.т.н., доцент
Ахмаметьєва Ганна Валеріївна

Рецензент: к.т.н., доцент
Кухаренко Сергій Вікторович

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Качковському Богдану Романовичу

1. Тема роботи: «Забезпечення кіберзахисту функціонування Інтернет магазинів»
Керівник роботи: к.т.н., доцент Ахмаметьєва Ганна Валеріївна
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548–6
2. Строк подання здобувачем роботи « » 202 рік
3. Дата видачі завдання « » 202 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Забезпечення кіберзахисту функціонування інтернет магазинів» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 7 рисунків, 5 таблиць, 2 додатки, 20 літературних джерел за переліком посилань. Робота виконана на 60 сторінках загального тексту і 47 сторінок основного тексту.

Метою роботи є проведення комплексного аналізу рівня кіберзахисту інтернет магазину «GTechShop», визначення основних вразливостей та розробка

діагностику наявної системи захисту сайту на платформі CMS OpenCart з використанням сучасних інструментів аудиту безпеки, зокрема Nikto та Metasploit Framework. Запропоновано технічні та організаційні заходи для підвищення ефективності кіберзахисту, а також систему навчання персоналу для протидії кіберризикам.

Результати роботи можуть бути використані для впровадження комплексних систем захисту в інших інтернет магазинах при розробці політик інформаційної безпеки для підприємств електронної комерції та у наукових дослідженнях, присвячених захисту даних у цифровій торгівлі.

Можливими напрямками подальших досліджень є розробка стандартів кіберзахисту для онлайн-торгівлі в Україні, впровадження інтелектуальних систем виявлення загроз на основі штучного інтелекту, оцінка ефективності навчальних програм для підвищення кібербезпеки серед персоналу.

ЗАХИСТ, ІНТЕРНЕТ МАГАЗИН, КІБЕРБЕЗПЕКА, ВРАЗЛИВІСТЬ, АНАЛІЗ, CMS, OPENCART.

ABSTRACT

Qualification work on the topic "Ensuring cyber protection of the functioning of the Internet store "GTechShop" for obtaining the first (bachelor's) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, contains 7 figures, 5 tables, 2 appendices, 20 literary sources according to the list of references. The work is performed on 60 pages of general text and 47 pages of the main text.

The purpose of the work is to conduct a comprehensive analysis of the level of cyber protection of the Internet store "GTechShop", identify the main vulnerabilities and develop recommendations for improving the security of the enterprise's information systems.

The work considers theoretical aspects of organizing cyber protection in e–commerce, analyzes typical threats and vulnerabilities inherent in Internet trading. Diagnostics of the existing site protection system on the CMS OpenCart platform was carried out using modern security audit tools, in particular Nikto and Metasploit Framework. Technical and organizational measures were proposed to increase the effectiveness of cyber protection, as well as a personnel training system to combat cyber risks.

The results of the work can be used for the implementation of comprehensive protection systems in other online stores in the development of information security policies for e–commerce enterprises and in scientific research on data protection in digital commerce.

Possible areas of further research are assessment of the effectiveness of training programs to improve cybersecurity among personnel.

PROTECTION, ONLINE STORE, CYBERSECURITY, VULNERABILITY, ANALYSIS, CMS, OPENCART.

ЗМІСТ

ВСТУП

У сучасних умовах цифровізації бізнесу питання інформаційної безпеки та кіберзахисту є критично важливими для стабільного функціонування онлайн-ресурсів, зокрема інтернет магазинів. Електронна комерція стає дедалі привабливішим об’єктом для кіберзлочинців, оскільки акумулює значні обсяги конфіденційної інформації – персональних та платіжних даних клієнтів.

За даними аналітичної компанії Cybersecurity Ventures, щорічні глобальні збитки від кіберзлочинності до 2026 року сягнуть понад 10,5 трильйонів доларів США. В Україні ці втрати оцінюються приблизно у 250 мільйонів доларівщороку, і левову частку складають саме атаки на суб’єкти онлайн-торгівлі.

Особливо вразливими є невеликі та середні інтернет магазини, які часто використовують системи управління контентом із відкритим кодом (наприклад, OpenCart) без належної уваги до безпеки. Багато власників онлайн-бізнесу нехтують базовими принципами кібергігієни – такими як регулярне оновлення CMS та модулів, тестування на вразливості, контроль доступу та конфігурацій.

У зв’язку з цим зростає потреба в системному підході до аналізу поточного стану кіберзахисту електронної торгівлі та впровадженні ефективних захисних рішень. Актуальність дослідження обумовлена необхідністю виявлення найбільш критичних вразливостей у сфері інтернет-комерції, розробки прикладної моделі кіберзахисту на прикладі реального інтернет магазину, формування рекомендацій, що можуть бути масштабованими для інших проєктів.

Мета дослідження полягає у проведенні аудиту системи кіберзахисту інтернет магазину «GTechShop», побудованого на платформі OpenCart та розробити рекомендації щодо її вдосконалення.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- визначити сутність інтернет-торгівлі як об’єкта кібератак, охарактеризувати її особливості та вразливі місця.
- виявити основні загрози та вразливості, притаманні інтернет-торгівлі, та класифікувати їх за рівнем небезпеки.

– проаналізувати вітчизняний та іноземний досвід у сфері кіберзахисту інтернет-магазинів, виділивши ефективні практики.

– провести діагностику основних бізнес-процесів інтернет-магазину «Gtechshop», визначивши їх вплив на кібербезпеку.

– здійснити порівняльну оцінку системи кіберзахисту інтернет-магазину «Gtechshop» з існуючими практиками та стандартами в сегменті інтернет-торгівлі.

– ідентифікувати недоліки та слабкі місця в системі кіберзахисту інтернет-магазину «Gtechshop», оцінивши їх потенційний вплив.

– розробити функціональну структуру запропонованої системи кіберзахисту для інтернет-магазину «Gtechshop» з описом основних компонентів.

– охарактеризувати технічні характеристики та оцінити ефективність запропонованої системи кіберзахисту для інтернет-магазину «Gtechshop».

– розробити та обґрунтувати систему навчання персоналу інтернет-магазину «Gtechshop» щодо інструментів протидії кіберризикам як елемента кіберзахисту.

Об’єкт дослідження – система кіберзахисту інтернет магазину «GTechShop», який функціонує на платформі OpenCart. Предмет дослідження – рівень інформаційної безпеки онлайн-ресурсу та можливості його вдосконалення через впровадження сучасних засобів кіберзахисту.

Практичне значення результатів. Результати дослідження мають суттєве прикладне значення для практики захисту електронної комерції. Виявлені уразливості дозволяють створити конкретний план дій для покращення кіберзахисту онлайн-магазинів, що підвищить довіру з боку користувачів. Сформульовані рекомендації можна масштабувати для інших інтернет магазинів, що також працюють на OpenCart або подібних CMS із відкритим кодом. Представлені результати можуть бути корисними для спеціалістів з інформаційної безпеки, які займаються аудитом та консалтингом у сфері електронної комерції. Запропоновані підходи сприятимуть зниженню ризиків кіберінцидентів в українському онлайн-сегменті в цілому.

1 ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ КІБЕРЗАХИСТУ СУБ'ЄКТІВ ІНТЕРНЕТ-ТОРГІВЛІ

1.1 Інтернет-торгівля як об'єкт кібератак

Інтернет-торгівля (або електронна комерція) – це процес купівлі та продажу товарів і послуг через Інтернет. Це включає в себе використання вебсайтів, мобільних додатків або платформ для здійснення транзакцій між покупцями та продавцями.

Суб'єктами інтернет-торгівлі виступають продавці та покупці. Продавець (або постачальник) – це фізична або юридична особа, яка продає товари чи надає послуги через Інтернет. Це можуть бути: інтернет магазини, платформи для продажу (наприклад, маркетплейси) суб'єкти підприємництва, які продають свою продукцію через власні вебсайти або через соціальні мережі.

Покупець – це фізична чи юридична особа, яка купує товар чи послугу через Інтернет. Покупець може бути, як кінцевим споживачем (особа, що купує для особистих потреб), так підприємцем.

Об'єктами Інтернет-торгівлі можуть виступати класичні товари (будь–які фізичні продукти, які продаються через Інтернет: одяг, продукти харчування, побутова техніка) послуги (консультації, доставка, підписки на онлайн-сервіси), інформація та цифрові товари (електронні книги, програмне забезпечення, музика, відео, які продаються та передаються через Інтернет).

Зручність і швидкість здійснення покупок – це основна перевага інтернет-торгівлі. Користувачі можуть здійснювати покупки з будь–якого місця, де є доступ до Інтернету, в будь–який зручний для них час, що дозволяє їм економити час і зусилля, що зазвичай витрачаються на поїздки до магазинів.

Далі, інтернет-торгівля дає користувачам доступ до широкого асортименту товарів, що не завжди є доступним в магазинах. Крім того, в Інтернеті можна знайти товари за більш низькими цінами, оскільки багато інтернет магазинів не мають додаткових витрат на оренду приміщень і зарплату продавців, що дозволяє їм зменшувати ціни на товари.

Оплата і доставка товарів в інтернет магазинах також зазвичай є простішими та зручнішими для користувачів, ніж у звичайних магазинах. Користувачі можуть здійснювати оплату за допомогою банківських карт, електронних гаманців та інших зручних для них методів.

Одним з найбільших недоліків інтернет-торгівлі є те, що користувачі не можуть фізично переглянути товар перед покупкою, що може призвести до незадоволеності покупкою після отримання товару. Хоча багато інтернет магазинів надають фотографії і описи товарів, вони можуть бути неповними або неадекватними, що може призвести до несподіваних ризиків.

Деякі інтернет магазини можуть бути ненадійними щодо платежів та доставки. Користувачі можуть стикатися зі затримками в доставці, неповноцінністю доставлених товарів або невідповідністю сплаченої ціни до отриманого товару. Також можуть виникати проблеми з поверненням товару, якщо він не відповідає сподіванням або пошкоджений.

Інтернет-торгівля також не позбавлена небезпеки шахрайства. Шахраї можуть створювати підроблені вебсайти та електронні магазини з метою шахрайства і крадіжки особистих даних користувачів, таких як номери кредитних карток. Крім того, існують ризики зв'язані з фінансовими операціями, де зловмисники можуть зламати безпеку й викрасти дані.

Основні види інтернет-торгівлі складено в таблиці 1.1.

Таблиця 1.1 – Основні види інтернет-торгівлі

№	Вид	Опис
1.	B2C (Business to Consumer)	Продаж товарів чи послуг безпосередньо кінцевим споживачам (наприклад, покупки в інтернет магазинах)
2.	B2B (Business to Business)	Продаж товарів чи послуг між підприємствами.

Продовження таблиці 1.1

3.	C2C (Consumer to Consumer)	Продаж між кінцевими споживачами через онлайн-платформи (наприклад, онлайн-аукціони або торгові платформи, як eBay або OLX).
4.	C2B (Consumer to Business)	коли споживач пропонує свої послуги чи продукти підприємствам.

Враховуючи те, що інтернет-торгівля є важливою складовою сучасної економіки, вона стає привабливою мішенню для різних кіберзлочинців. Отже зростання кількості онлайн-покупок та розвиток цифрових платформ для торгівлі, безпека в цій сфері стає критично важливою. Серед основних кіберзагроз можна відзначити наступні.

Фішинг, коли зловмисники створюють фальшиві інтернет магазини або вебсайти для збору персональних даних клієнтів, таких як логіни, паролі, номери карток тощо.

Атаки на платіжні системи, адже злочинці можуть намагатися зламати платіжні платформи або красти платіжні дані під час транзакцій.

DDoS-атаки (Distributed Denial of Service), тобто напади, що спрямовані на перевантаження серверів магазину, що може призвести до їх недоступності для користувачів і тимчасового припинення роботи інтернет магазину.

SQL-ін’єкції, коли зловмисники використовують уразливості в базах даних, щоб отримати доступ до конфіденційної інформації клієнтів або змінити дані про замовлення.

Викрадення особистих даних, адже у випадку недостатнього шифрування або слабкого захисту баз даних можуть бути викрадені персональні дані користувачів, що завдає значної шкоди репутації інтернет магазину.

Шкідливе програмне забезпечення, тобто віруси, трояни та інші види шкідливого програмного забезпечення можуть бути використані для крадіжки інформації або для компрометації комп'ютерів користувачів, що здійснюють покупки.

Крім того інтернет-торгівля залежить від обробки великої кількості персональних і фінансових даних, тому одним з головних аспектів безпеки є захист конфіденційності та цілісності даних. Належний захист даних забезпечує не тільки довіру клієнтів, а й відповідає вимогам законодавства, наприклад, Загального регламенту захисту даних (GDPR).

1.2 Загрози та вразливості притаманні інтернет-торгівлі

Інтернет-торгівля, або електронна комерція, стала невід'ємною частиною сучасної економіки. Проте з її розвитком зростає і кількість загроз та вразливостей, які можуть негативно вплинути на безпеку бізнесу та довіру споживачів. Нижче наведено основні загрози та вразливості, характерні для інтернет-торгівлі.

Інтернет-торгівля стрімко розвивається, однак водночас вона залишається вразливою до численних кіберзагроз, які можуть поставити під загрозу як інфраструктуру самого бізнесу, так і конфіденційність даних користувачів.

Однією з найпоширеніших проблем є несанкціонований доступ до персональних і фінансових даних клієнтів, що часто стається внаслідок хакерських атак. Недостатній рівень захисту, зокрема використання застарілого програмного забезпечення, відсутність сучасних механізмів шифрування та неналежна система контролю доступу, істотно підвищують ризик витоку критично важливої інформації [1].

Фішингові атаки та методи соціальної інженерії є ще одним серйозним викликом для інтернет магазинів. Злочинці імітують легітимні сервіси або служби підтримки для обману користувачів з метою отримання їхніх облікових даних. Такі дії можуть призводити до несанкціонованих платежів, крадіжки особистої інформації та втрати довіри з боку клієнтів [2].

Крім того, розповсюдженим методом дестабілізації онлайн-бізнесу залишаються DDoS-атаки – навмисне перевантаження серверів для виведення з ладу онлайн-магазину. Це не лише зупиняє продажі, а й завдає шкоди діловій репутації та викликає недовіру споживачів [2].

Суттєву загрозу становить також використання ботнетів та шкідливого програмного забезпечення. Зокрема, зловмисники активно застосовують трояни, кейлогери, а також шкідливі скрипти, що вбудовуються в сайти або платформи електронної комерції для збору чутливої інформації. Атаки на IoT–пристрої, які все частіше інтегруються в логістику та управління запасами, також посилюють загальний рівень вразливості [3].

Окрему небезпеку створює людський фактор, зокрема – недотримання персоналом базових принципів інформаційної безпеки, слабкі паролі, нехтування оновленнями ПЗ та недостатня обізнаність про сучасні схеми шахрайства. Це вказує на необхідність регулярного навчання співробітників та впровадження комплексних політик безпеки на рівні всієї організації.

Отже, забезпечення безпеки в інтернет-торгівлі вимагає системного підходу: від використання сучасних засобів захисту до розробки стратегій реагування на інциденти та підвищення обізнаності користувачів.

Загрози, з якими стикається інтернет-торгівля, можна структурувати за різними типами. Орієнтовна класифікація буде виглядати, як зображено на рисунку 1.1.

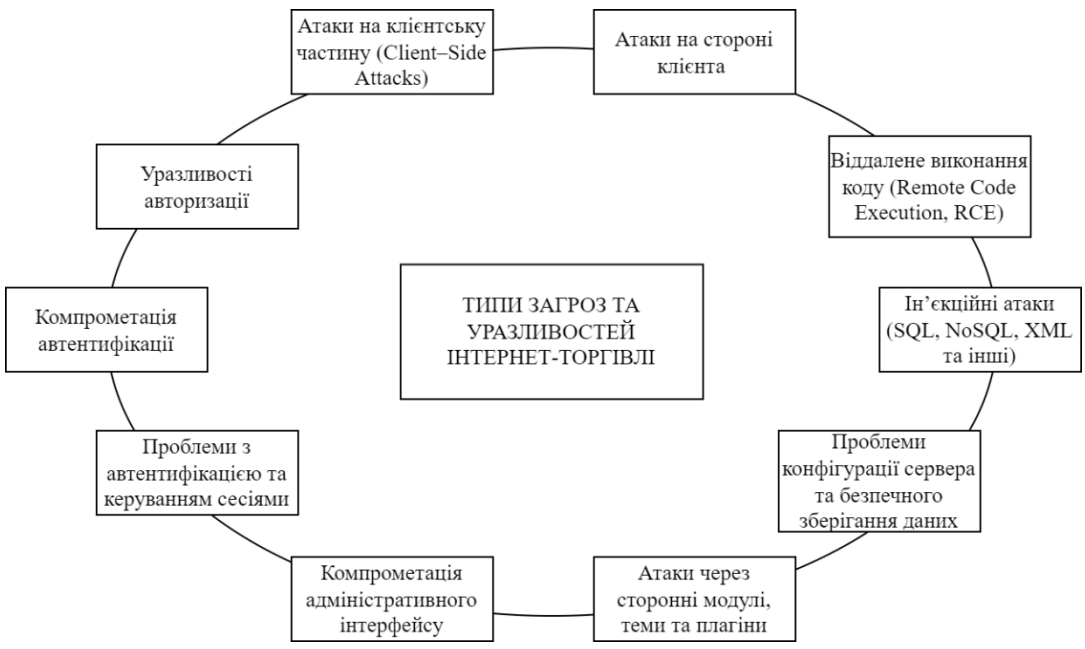

Рисунок 1.1 – Класифікація загроз інтернет-торгівлі

Інтернет-торгівля стикається з численними загрозами, які можуть серйозно вплинути на безпеку як самого бізнесу, так і його клієнтів. Ці загрози можна класифікувати за різними типами, кожна з яких має свої особливості та потребує специфічних заходів протидії. Однією з найкритичніших проблем є компрометація автентифікації, коли зловмисник отримує несанкціонований доступ до облікових записів користувачів або адміністраторів, обходячи або зламуючи механізми перевірки особи. Для інтернет магазинів це становить значну небезпеку, оскільки скомпрометовані акаунти дозволяють зловмисникам здійснювати несанкціоновані транзакції, переглядати замовлення чи навіть змінювати ціни. До основних методів такої компрометації належать атаки методом підбору облікових даних, відомі як Brute Force, коли автоматизовані інструменти масово підбирають паролі, особливо якщо відсутні обмеження на кількість спроб входу або використовуються слабкі паролі [5]. Також значну загрозу становлять уразливості в механізмах відновлення доступу, де спрощені алгоритми, такі як відповіді на секретні питання чи надсилання посилань на електронну пошту без додаткової перевірки, дозволяють зловмисникам отримати доступ без знання пароля. Крім того, недостатній контроль сесій, наприклад використання передбачуваних сесійних ідентифікаторів або збереження авторизаційних токенів у незахищених cookie-файлах, відкриває можливості для атак типу Session Hijacking або Session Fixation [6].

Не менш серйозними є уразливості авторизації, які виникають після успішної автентифікації, коли система не належним чином обмежує права користувача відповідно до його ролі. Наприклад, недостатній контроль доступу до ресурсів може дозволити користувачу отримати доступ до адміністративних функцій або даних інших клієнтів, якщо система покладається лише на наявність активної сесії без повторної перевірки прав. Використання передбачуваних ідентифікаторів об’єктів, таких як лінійні числові ідентифікатори замовлень чи профілів, дає змогу зловмисникам змінювати параметри в URL-рядку для перегляду чужої інформації. Відсутність таймаутів сесій або механізмів автоматичного виходу з системи також створює ризик використання незавершених сесій, особливо на публічних комп’ютерах чи вкрадених пристроях. Для мінімізації цих ризиків необхідно

застосовувати принцип мінімальних привілеїв і багаторівневу перевірку авторизації [7].

Атаки на клієнтську частину, спрямовані на користувачів інтернет магазинів, становлять значну загрозу, оскільки саме клієнти вводять платіжні та особисті дані, які є цінною мішенню для зловмисників. Міжсайтове виконання скриптів (XSS) є однією з найпоширеніших атак, коли зловмисники впроваджують шкідливий JavaScript-код у елементи інтерфейсу, наприклад, у поля коментарів чи форми зворотного зв'язку, що дозволяє викрадати cookies, токени автентифікації чи інші дані [8]. Підміна контенту (Content Spoofing) змушує користувачів взаємодіяти з фальшивими формами входу чи оплати, які надсилають дані на сторонні ресурси, часто через ін'єкції HTML або JavaScript. Ще одна небезпека – розщеплення HTTP-відповіді (HTTP Response Splitting), яке базується на некоректному обробленні заголовків HTTP, дозволяючи вставляти шкідливі скрипти чи редиректи. Для протидії цим загрозам необхідно впроваджувати суворе фільтрування вхідних даних, використовувати політику Content Security Policy (CSP) і налаштовувати заголовки безпеки [9].

Віддалене виконання коду (Remote Code Execution, RCE) є однією з найнебезпечніших загроз, оскільки дозволяє зловмиснику виконувати довільний код на сервері з правами вебсервера, що може призвести до повного захоплення системи, втрати даних або використання сервера для атак на інші ресурси. Такі атаки можуть відбуватися через командні ін'єкції, коли параметри URL або дані з форм передаються в системні команди без належної фільтрації. Завантаження та виконання файлів, особливо в CMS із функціями завантаження без перевірки MIME-типу чи розширення, дозволяють запускати шкідливі скрипти, наприклад PHP-файли. Уразливості шаблонізаторів або плагінів також можуть сприяти виконанню динамічного коду, якщо зловмисник має доступ до їх зміни через панель адміністратора чи API [10].

Ін'єкційні атаки, такі як SQL, NoSQL, XML та інші, залишаються одними з найпоширеніших і найнебезпечніших загроз для вебдодатків, зокрема інтернет магазинів. Вони виникають через передачу користувацьких даних у запити до баз

даних або сервісів без належної валідації й екранування. Якщо запит до бази даних будується на основі введених користувачем значень без підготовлених виразів (prepared statements), зловмисник може змінити логіку запиту. Це дозволяє:

- обійти автентифікацію (' OR '1'='1),
- переглянути таблиці з паролями або платіжною інформацією,
- змінити або видалити дані з бази [11].

Поширюється у вебдодатках, що використовують NoSQL–бази (наприклад, MongoDB). Уразливість виникає при вставці JSON–структур без перевірки типів або очікуваного формату. Наприклад, при передачі { "username": {"$ne": null}, "password": {"$ne": null} } можна обійти автентифікацію [12].

XML-ін’єкції та XXE (XML External Entity) дають змогу зчитувати конфіденційні файли, виконувати запити до внутрішніх сервісів або ініціювати DoS-атаки через парсинг [13]. Для захисту від таких атак необхідно використовувати підготовлені запити, валідувати дані на сервері, мінімізувати права доступу додатка до бази даних і вимикати небезпечні функції парсерів.

Проблеми конфігурації сервера та безпечного зберігання даних також є значним джерелом уразливостей. Неправильна конфігурація вебсервера чи середовища розгортання може призвести до відкритої доступності конфігураційних файлів, таких як .env чи config.php, які містять логіни, паролі та ключі доступу [14]. Логування конфіденційних даних, таких як запити з паролями чи особистими даними, у production-середовищі створює ризик їх витоку при компрометації логів [15]. Відкриті службові інтерфейси, такі як phpMyAdmin чи Elasticsearch, без автентифікації або з типовими обліковими даними стають легкою мішенню для сканерів [16].

Відсутність шифрування даних, таких як паролі чи номери карток, а також передача даних через HTTP замість HTTPS, значно підвищує ризик їх перехоплення. Дані користувачів (паролі, номери карток, адреси тощо) мають зберігатися в зашифрованому вигляді. Наприклад:

- паролі – лише у вигляді хешу (bcrypt, Argon2),
- дані – з використанням симетричного шифрування (AES),

– передача – виключно через HTTPS із актуальним сертифікатом.

Застаріле програмне забезпечення, включаючи Apache, Nginx, PHP чи CMS, залишає систему вразливою до відомих експлойтів [17]. Для запобігання цим проблемам необхідно закривати доступ до конфігураційних файлів і службових інтерфейсів, використовувати безпечне логування, шифрувати дані та регулярно оновлювати програмне забезпечення.

Проблеми з автентифікацією та керуванням сесіями також створюють значні ризики. Слабкі паролі, відсутність обмежень на кількість спроб входу, незахищене зберігання сесій у cookie без атрибутів HttpOnly, Secure і SameSite, а також неочищення сесій після виходу чи тривалої бездіяльності дозволяють зловмисникам викрадати облікові записи [18, 19, 20].

Сесії, що зберігаються у cookie без атрибутів HttpOnly, Secure та SameSite, легко перехопити через XSS або атаки перехоплення трафіку. Витік сесійного ідентифікатора (session ID) = захоплення облікового запису [20]. Відсутність двофакторної автентифікації (2FA) робить систему вразливою навіть у разі витоку пароля [21]. Для захисту рекомендовано впроваджувати складні паролі, обмежувати спроби входу, використовувати безпечні cookie, встановлювати таймаути сесій і застосовувати 2FA.

Атаки на стороні клієнта, такі як XSS, CSRF, підміна контенту через iframe чи clickjacking, спрямовані на користувачів, можуть призвести до викрадення сесій, перенаправлення на шкідливі ресурси чи виконання небажаних дій [22, 23, 24].

Міжсайтове скриптування - це одна з найпоширеніших вразливостей, за якої зловмисник впроваджує JavaScript–код у сторінку, що переглядає користувач. У CMS це часто трапляється в коментарях, формах зворотного зв’язку, полях профілю тощо [22].

Приклад:

```
<script>document.location='https://attacker.com/steal?cookie='+
document.cookie</script>
```

Для протидії необхідно виконувати наступні дії

- екранувати та фільтрувати всі введення користувача перед відображенням на сторінці;
- використовувати CSP (Content Security Policy) для обмеження виконання JavaScript;
- додавати захист від CSRF через унікальні токени у формах (наприклад, csrf_token);
- встановити HTTP–заголовки X–Frame–Options: DENY або SAMEORIGIN для захисту від clickjacking;
- перевіряти всі зовнішні віджети та скрипти перед впровадженням.

Компрометація адміністративного інтерфейсу є особливо небезпечною, оскільки адмін-панель надає доступ до управління контентом, користувачами та плагінами. Слабкі облікові дані, відсутність 2FA, відкритий доступ до шляхів типу /wp-admin чи використання HTTP замість HTTPS роблять адмін-панель легкою мішенню [25, 26, 27].

Рекомендації щодо мінімізації цих загроз:

- змінити URL входу в адмінку або приховати його (наприклад, плагінами типу WPS Hide Login для WordPress);
- заборонити доступ до панелі керування по IP або через VPN;
- обов’язково активувати 2FA;
- використовувати SSL–сертифікат і перенаправляти весь трафік на HTTPS;
- регулярно перевіряти список адміністраторів та права доступу;
- встановлювати розширення з перевірених джерел, регулярно їх оновлювати.

Сторонні модулі, теми та плагіни часто стають джерелом уразливостей через використання зламаних версій, застаріле ПЗ, недостатню перевірку даних чи надмірні дозволи [28, 29, 30].

Для забезпечення безпеки інтернет магазинів при використанні сторонніх модулів, тем і плагінів рекомендується встановлювати розширення виключно з

офіційних каталогів, таких як WordPress.org або Joomla Extensions Directory, щоб мінімізувати ризик встановлення шкідливого програмного забезпечення. Слід уникати використання зламаних версій тем і плагінів, оскільки вони часто містять бекдори, майнери чи інші шкідливі компоненти. Регулярне оновлення всього програмного забезпечення, включаючи CMS, плагіни та теми, є необхідним для усунення відомих уразливостей. Перед встановленням нових розширень варто ретельно перевіряти відгуки та рейтинг, щоб переконатися в їхній надійності. Після встановлення будь-якого розширення рекомендується сканувати сайт на наявність шкідливого коду, щоб виявити потенційні загрози. Також важливо обмежувати кількість активних розширень, видаляючи непотрібні, щоб зменшити поверхню атаки та спростити управління системою.

Сфера електронної комерції стрімко зростає, однак разом із розвитком цифрової інфраструктури зростає й кількість кіберзагроз. Інтернет магазини є привабливою ціллю для зловмисників через великий обсяг персональних та фінансових даних користувачів. Основні вразливості електронної торгівлі включають:

1. Багато компаній, особливо малі та середні, не мають достатніх ресурсів, знань або стратегічного бачення для впровадження повноцінної системи кіберзахисту. Відсутність базових заходів, таких як регулярне оновлення програмного забезпечення, багатофакторна автентифікація чи шифрування даних, робить такі платформи вразливими до атак типу DDoS, зловмисного програмного забезпечення, несанкціонованого доступу тощо [4].

2. Сервіси обробки платежів, служби доставки, хмарні CRM або маркетингові платформи – всі ці зовнішні постачальники інтегруються в систему інтернет магазину. Якщо хоча б один із них має недостатній рівень захисту, це створює ланцюгову загрозу для всієї інфраструктури. Компанія втрачає контроль над даними, які передаються третім сторонам, і може стати жертвою витоку або зловживання [1].

3. Працівники – найслабша ланка будь-якої системи безпеки. Використання простих або повторюваних паролів, нехтування політиками безпеки, небезпечне

поводження з електронною поштою (наприклад, відкриття фішингових листів) можуть призвести до компрометації облікових записів, впровадження шкідливого коду або витоку даних клієнтів [5]. Особливо ризиковано, коли доступ до критичних систем мають кілька осіб без обмежень прав.

Успішна діяльність в інтернет-торгівлі неможлива без побудови комплексної системи безпеки. Для зниження ризиків підприємствам необхідно не лише інвестувати в технологічні рішення, але й забезпечувати безперервне навчання персоналу, контроль за зовнішніми підрядниками та регулярний аудит цифрової інфраструктури.

Рекомендації щодо підвищення безпеки складають наступні пункти:

– впровадження багаторівневої аутентифікації забезпечує додатковий рівень захисту облікових записів користувачів.

– регулярне оновлення програмного забезпечення допомагає усунути відомі вразливості та зменшити ризик атак.

– навчання персоналу підвищує обізнаність співробітників щодо кіберзагроз та методів їх запобігання.

– використання сучасних засобів захисту, таких як антивірусне ПЗ, міжмережеві екрани та системи виявлення вторгнень.

– оцінка безпеки сторонніх постачальників дозволяє переконатися, що партнери дотримуються належних стандартів.

Забезпечення безпеки в інтернет-торгівлі є критично важливим для збереження довіри клієнтів та стабільності бізнесу. Врахування зазначених загроз і вразливостей, а також впровадження відповідних заходів захисту, допоможе мінімізувати ризики та забезпечити ефективну і безпечну діяльність у сфері електронної комерції.

1.3 Вітчизняний та іноземний досвід щодо кіберзахисту інтернет магазинів.

Кібербезпека інтернет магазинів є критично важливою як для бізнесу, так і для користувачів, які очікують безпечної обробки своїх персональних та

фінансових даних. У світі вже сформувалися різні підходи до забезпечення захисту інтернет-торгівлі, зокрема через нормативно–правове регулювання, технічні рішення та освітні ініціативи. Україна поступово адаптує міжнародні практики, водночас стикаючись із унікальними викликами.

Іноземний досвід. У країнах ЄС та США питання кіберзахисту є однією з ключових складових електронної комерції. У Європі діє Загальний регламент захисту даних (GDPR), який зобов'язує інтернет магазини забезпечувати належний рівень безпеки персональних даних користувачів. Зокрема, компанії впроваджують шифрування даних, протоколи TLS/SSL, багаторівневу автентифікацію та регулярне тестування систем безпеки [6].

У США застосовується комплексний підхід, що поєднує законодавчі вимоги (наприклад, закон про захист даних у Каліфорнії – CCPA) з активною роллю приватного сектору. Великі онлайн-ритейлери інвестують у розробку власних систем захисту, включно з моніторингом трафіку в режимі реального часу, AI-рішеннями для виявлення підозрілої активності та розгортанням систем запобігання вторгненням (IPS) [7].

Крім того, такі компанії як Amazon і eBay використовують автоматизовані системи для аналізу транзакцій і виявлення шахрайства, що дозволяє знижувати ризики фішингових атак і крадіжки платіжних даних. Ці платформи активно впроваджують технології машинного навчання, щоб прогнозувати і швидко реагувати на потенційні загрози.

У Китаї активно впроваджуються автоматизовані системи аналізу кіберзагроз. Платформи, як от Alibaba, використовують власні кіберзахисні хаби, які виявляють шахрайські транзакції на основі великих обсягів поведінкових даних користувачів [8]. Для додаткового захисту застосовуються біометричні методи автентифікації, зокрема розпізнавання обличчя і відбитків пальців.

Вітчизняний досвід. В Україні питання кіберзахисту інтернет магазинів частково регулюється Законом «Про захист персональних даних» та Стратегією кібербезпеки України. Проте на практиці більшість малих та середніх онлайн-компаній мають обмежені ресурси для впровадження комплексних систем захисту.

Часто використовуються лише базові інструменти – SSL-сертифікати, CAPTCHA, антивіруси та резервне копіювання даних [9].

Разом з тим, зростає усвідомлення важливості кібербезпеки серед вітчизняного бізнесу. Наприклад, маркетплейс Rozetka після початку повномасштабного вторгнення у 2022 році посилив протоколи резервного копіювання, впровадив двофакторну автентифікацію для співробітників та почав використовувати моніторинг доступу в режимі реального часу [10].

Ще одним прикладом є платформа Prom.ua, яка у 2023 році ініціювала серію вебінарів для продавців про захист даних, фішингові ризики та безпечну роботу з обліковими записами. У партнерстві з українськими фахівцями у сфері ІТ–безпеки платформа розробила сервіси для автоматичного виявлення підозрілої активності в особистих кабінетах продавців [11].

Крім того, українські ІТ–компанії активно розвивають послуги кіберзахисту для малого бізнесу. Наприклад, компанії, як–от SoftServe та EPAM, пропонують налаштування міжмережевих екранів, аудит сайтів на вразливості, а також консультують щодо інтеграції платіжних систем із підтримкою стандарту PCI DSS, що є обов’язковим для безпечної обробки кредитних карток.

Ще один яскравий приклад – український стартап «CyberGuard», який розробив платформу для автоматичного моніторингу і реагування на кіберзагрози в реальному часі, спеціально адаптовану під потреби інтернет магазинів. Платформа використовує алгоритми штучного інтелекту для виявлення аномалій у поведінці користувачів і миттєвого блокування підозрілих дій.

Таким чином, український досвід поступово наближається до світових стандартів, однак потребує більшої уваги з боку держави та бізнесу для масштабного впровадження ефективних заходів кібербезпеки.

Інтернет-торгівля, як ключова складова сучасної економіки, характеризується значними перевагами, такими як зручність, широкий асортимент товарів, нижчі ціни та спрощені процеси оплати й доставки, але водночас є вразливою до численних кіберзагроз. Основні загрози включають фішинг, атаки на платіжні системи, DDoS-атаки, SQL-ін’єкції, викрадення особистих даних і

використання шкідливого програмного забезпечення. Ці ризики посилюються через недостатній захист даних, застаріле програмне забезпечення, слабкі паролі, неналежне керування сесіями, уразливості в автентифікації та авторизації, а також використання ненадійних сторонніх модулів і плагінів. Для забезпечення безпеки необхідні комплексні заходи: впровадження багаторівневої автентифікації, регулярне оновлення ПЗ, суворе фільтрування вхідних даних, використання шифрування (HTTPS, AES, хешування паролів), політики Content Security Policy, обмеження доступу до адміністративних інтерфейсів і регулярне навчання персоналу. Іноземний досвід, зокрема в ЄС, США та Китаї, демонструє ефективність нормативного регулювання (GDPR, CCPA), застосування AI для аналізу транзакцій і біометричних методів автентифікації. В Україні, попри обмежені ресурси малого та середнього бізнесу, спостерігається прогрес у впровадженні базових інструментів захисту (SSL, 2FA, резервне копіювання), а також розвиток локальних рішень, таких як платформи для моніторингу кіберзагроз. Однак для досягнення світових стандартів необхідне масштабніше залучення держави та бізнесу до створення комплексної системи кібербезпеки, що поєднує технологічні, організаційні та освітні заходи.

2 АНАЛІЗ НАЯВНОЇ СИСТЕМИ КІБЕРЗАХИСТУ ІНТЕРНЕТ МАГАЗИНУ «GTECHSHOP»

2.1 Діагностика основних бізнес–процесів інтернет магазину

Інтернет магазин «GTechShop» спеціалізується на продажу обладнання для сонячної та зеленої енергетики – інверторів, сонячних панелей, акумуляторів, контролерів заряду та інших комплектуючих для альтернативних джерел енергії. Асортимент магазину орієнтований як на приватних споживачів, які встановлюють домашні системи автономного живлення, так і на компанії, що реалізують великі проєкти з відновлюваної енергетики. На рисунку 2.1 зображено головну сторінку інтернет магазину.

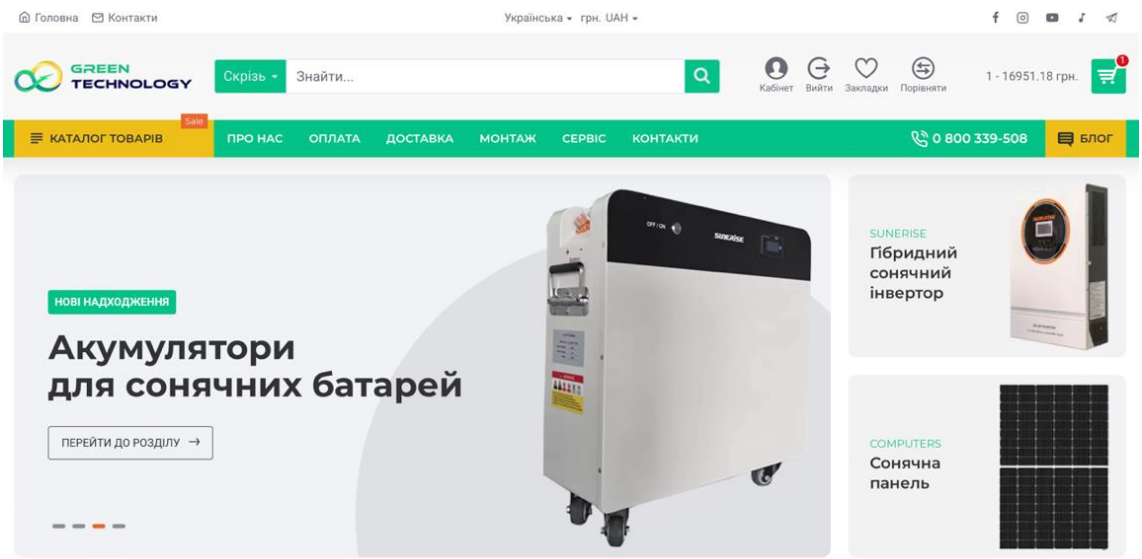

Рисунок 2.1 – Головна сторінка інтернет магазину «GTechShop»

Платформа магазину побудована на основі CMS OpenCart, що забезпечує гнучкість у керуванні товарами, замовленнями та інтеграції з різними платіжними системами. Завдяки цьому «GTechShop» може швидко адаптуватися до потреб ринку та пропонувати зручні інструменти для клієнтів.

Для забезпечення стабільності бізнесу та захисту персональних і фінансових даних клієнтів, а також збереження цілісності інформації, важливо здійснити

детальний аналіз основних бізнес–процесів, що визначають загальний рівень кібербезпеки магазину.

Основні бізнес-процеси, що підлягають діагностиці складаються з наступних пунктів з таблиці 2.1.

Таблиця 2.1 – Основні бізнес-процеси, що підлягають діагностиці

№	Бізнес-процес	Характеристика
1.	Управління каталогом товарів і складськими запасами	Своєчасне оновлення інформації про наявність і технічні характеристики обладнання, що дозволяє уникнути помилок у замовленнях і втрат клієнтів через нестачу товарів.
2.	Обробка замовлень і платежів	Збір замовлень через вебінтерфейс, перевірка і підтвердження оплати, а також обробка інформації про доставку. Важливою складовою є безпечна інтеграція з платіжними шлюзами, які підтримують захищені протоколи передачі даних.
3.	Обробка та зберігання персональних даних клієнтів	Враховуючи специфіку товарів і часті консультації, магазин збирає контактні дані, історію замовлень і технічні запити клієнтів. Надійність зберігання та обробки цих даних визначає довіру користувачів.
4.	Клієнтська підтримка та комунікації	Взаємодія з покупцями через електронну пошту, телефон, а також чат на сайті, що забезпечує оперативне вирішення питань і консультації.
5.	Адміністрування сайту та оновлення CMS	Підтримка платформи OpenCart в актуальному стані, впровадження оновлень, встановлення модулів і плагінів, що підвищують функціональність, але при цьому можуть стати джерелом вразливостей без належного контролю.

На основі наведеної таблиці можна зробити висновок, що ключові бізнес-процеси інтернет магазину, такі як управління каталогом товарів і складськими запасами, обробка замовлень і платежів, обробка та зберігання персональних даних клієнтів, клієнтська підтримка та адміністрування сайту, відіграють критичну роль у забезпеченні ефективної та безпечної роботи платформи. Своєчасне оновлення інформації про товари та запаси запобігає помилкам у замовленнях і втраті клієнтів, тоді як безпечна інтеграція з платіжними шлюзами та надійне зберігання персональних даних є необхідними для захисту фінансових транзакцій і підтримки довіри користувачів. Клієнтська підтримка через різні канали комунікації забезпечує оперативне вирішення питань, що підвищує задоволеність клієнтів. Однак адміністрування сайту та оновлення CMS, зокрема використання модулів і плагінів, потребують ретельного контролю, оскільки вони можуть стати джерелом вразливостей. Таким чином, для успішного функціонування інтернет магазину необхідно поєднувати ефективне управління бізнес-процесами з впровадженням сучасних заходів кібербезпеки, щоб мінімізувати ризики та забезпечити стабільну й безпечну роботу платформи.

Діагностика цих процесів дозволяє виявити слабкі місця в організації кіберзахисту та сформувати рекомендації для посилення безпеки системи з урахуванням особливостей обраної CMS OpenCart, інтеграції з платіжними шлюзами, способів доставки та інших технічних аспектів функціонування інтернет магазину.

2.2 Порівняльна оцінка кіберзахисту інтернет магазину з наявними практиками та стандартами в сегменті інтернет-торгівлі

Для забезпечення високого рівня кібербезпеки інтернет магазину «GTechShop» важливо провести порівняльний аналіз його наявних заходів із загальноприйнятими практиками та стандартами в сфері електронної комерції. Це дозволяє виявити прогалини у захисті та адаптувати найкращі світові підходи з урахуванням специфіки бізнесу.

Сучасні стандарти кіберзахисту інтернет-торгівлі базуються на міжнародних нормативних актах, які складено в таблиці 2.2.

Таблиця 2.2 – Сучасні стандарти кіберзахисту інтернет-торгівлі

№	Стандарт	Особливість
1.	PCI DSS (Payment Card Industry Data Security Standard)	Набір вимог для безпечної обробки, зберігання і передачі даних платіжних карток. Для магазинів, які приймають оплату онлайн, відповідність PCI DSS є обов'язковою для захисту клієнтських фінансових даних.
2.	GDPR (General Data Protection Regulation)	Регламент ЄС, що встановлює суворі вимоги до збирання, зберігання та обробки персональних даних користувачів, включно з правом на доступ, виправлення та видалення інформації
3.	OWASP (Open Web Application Security Project)	Рекомендації та найкращі практики щодо безпеки вебдодатків, які включають захист від ін'єкційних атак, крос-сайт скриптингу (XSS), проблем із аутентифікацією тощо.

Для проведення загального аудиту вебсайту доцільно скористатися функціоналом спеціалізованого онлайн-сервісу SE Ranking, який забезпечує комплексну перевірку технічного стану сайту та відповідності його сучасним вимогам пошукових систем. Цей інструмент дозволяє отримати детальний аналіз багатьох важливих аспектів, що впливають як на безпеку ресурсу, так і на його загальну ефективність та видимість у пошуковій видачі.

Зокрема, сервіс SE Ranking проводить повномасштабний технічний аудит, охоплюючи такі ключові параметри, як: наявність та коректність SSL-сертифікату, структура URL–адрес, внутрішні та зовнішні посилання, статуси сторінок (200, 404, 301 тощо), швидкість завантаження, наявність дублікатів контенту, коректність robots.txt та sitemap.xml, оптимізація метатегів, а також доступність

сторінок для індексації. Крім того, система перевіряє відповідність сайту мобільним пристроям, що сьогодні є критично важливим критерієм з точки зору SEO та зручності користування.

Отримані результати автоматично структуруються в зручний аналітичний звіт, де кожна виявлена проблема супроводжується описом її суті, рівнем пріоритетності та рекомендаціями щодо усунення. Це дає змогу не лише виявити наявні технічні недоліки, а й сформувати покроковий план оптимізації ресурсу.

Таким чином, використання сервісу SE Ranking у процесі аудиту дозволяє отримати об'єктивну оцінку стану інтернет магазину, своєчасно виявити технічні ризики та сприяти підвищенню рівня кібербезпеки та ефективності сайту в цілому. На рисунку 2.2 зображено приклад аудиту з використанням SE Ranking.

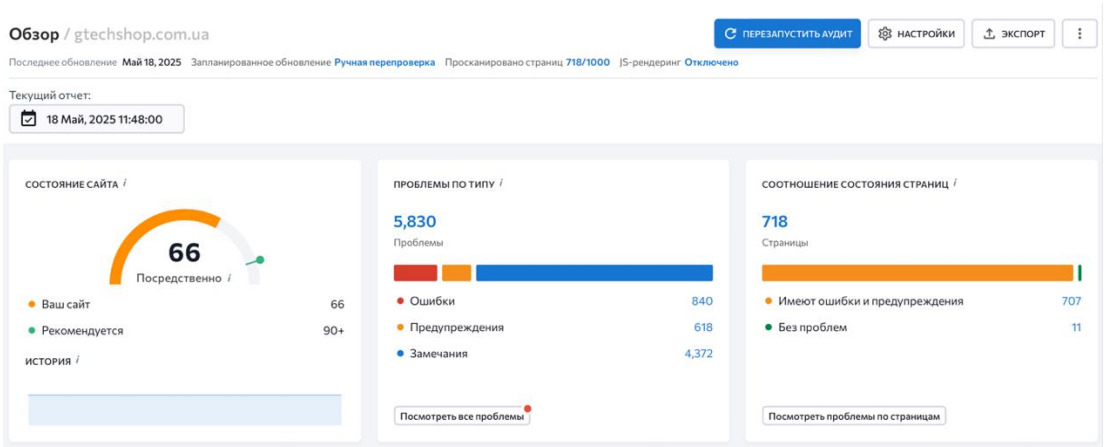

Рисунок 2.2 – Аудит за допомогою сервісу SE Ranking

Розглянемо інші інструменти, які допоможуть нам провести аналіз нашого сайту з метою виявлення помилок та вразливостей.

Nikto – це потужний сканер вебсерверів з відкритим вихідним кодом, який використовується для виявлення потенційних вразливостей та неправильних конфігурацій вебресурсів. Інструмент перевіряє вебсервер на наявність понад 6 700 потенційно небезпечних файлів, скриптів, старих версій програмного забезпечення, а також проблем із конфігурацією серверів (наприклад, відкриті каталоги, небезпечні HTTP-заголовки тощо). На рисунку 2.3 зображено інструмент аудиту безпеки Nikto.

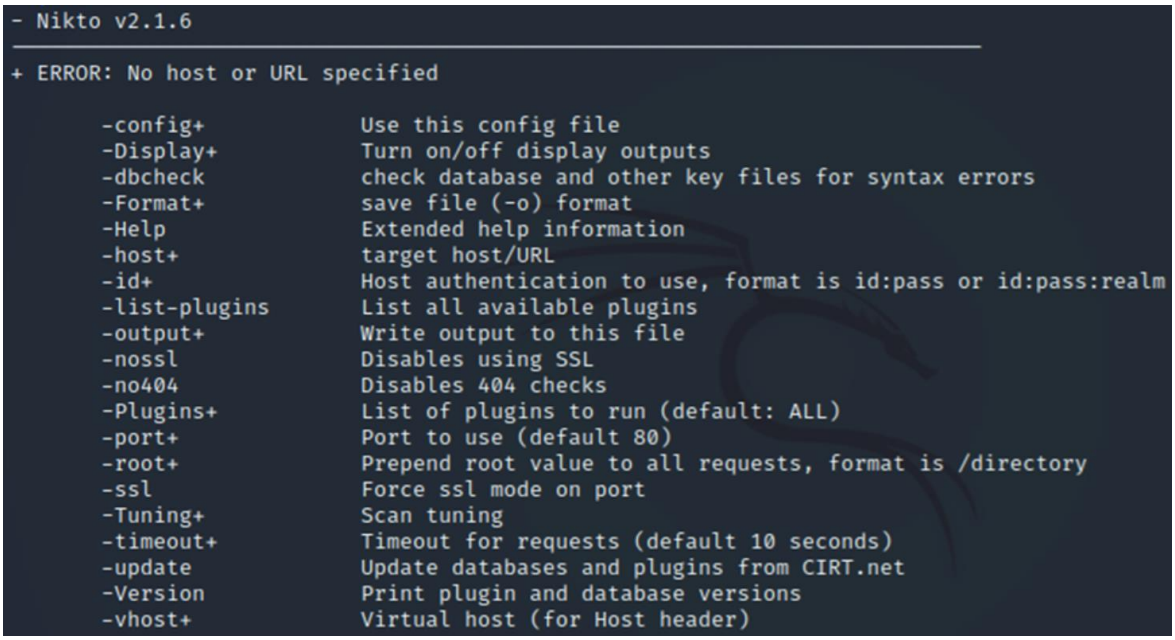

Рисунок 2.3 – Інструмент аудиту безпеки Nikto

Nikto, як інструмент для сканування вебсерверів, забезпечує широкий спектр функціональних можливостей для виявлення потенційних вразливостей. Він здатен ідентифікувати застарілі версії вебсерверів і компонентів, які можуть містити відомі уразливості, а також виявляти небезпечні файли та директорії, такі як /phpmyadmin/, /backup/ чи /test/, що можуть бути доступними для зловмисників. Інструмент аналізує конфігурації HTTP-заголовків, перевіряючи наявність важливих параметрів безпеки, таких як X-Frame-Options, X-XSS-Protection чи Content-Security-Policy, і виявляє їх відсутність, що може вказувати на слабкий захист. Nikto також визначає дозволені методи HTTP, наприклад PUT або DELETE, використання яких може створювати ризики для безпеки сервера. Крім того, інструмент виявляє відкриті каталоги або конфігураційні файли, які не повинні бути загальнодоступними, попереджаючи про можливі точки входу для атак. Нарешті, Nikto перевіряє підтримку застарілих криптографічних протоколів, таких як SSLv2 і SSLv3, які вважаються небезпечними через їхню вразливість до сучасних методів злому. Таким чином, Nikto є ефективним інструментом для комплексного аудиту безпеки вебсерверів, допомагаючи виявляти та усувати потенційні загрози.

У рамках комплексного аудиту кіберзахисту сайту https://gtechshop.com.ua, було проведено сканування вебсервера за допомогою інструменту Nikto.

Цілі сканування складаються з наступних пунктів:

1. Перевірка наявності відкритих адміністративних або службових директорій, які могли бути залишені після розробки або оновлень CMS OpenCart.

2. Виявлення застарілих компонентів вебсервера, що потенційно мають відомі вразливості.

3. Аналіз конфігурації HTTP–заголовків на відповідність стандартам безпеки OWASP.

4. Виявлення незахищених або невірно налаштованих скриптів, які могли б бути використані для атаки на CMS або отримання доступу до конфіденційних даних.

Проведене сканування за допомогою інструменту Nikto виявило кілька аспектів конфігурації сервера, які потребують уваги для підвищення рівня кіберзахисту. Зокрема, було встановлено, що директорія /system/storage/ є загальнодоступною, що може становити ризик, оскільки вона може містити лог-файли або тимчасові файли, не призначені для публічного доступу. Сервер не відправляє заголовок Content-Security-Policy, що створює потенційну вразливість до XSS-атак при використанні шкідливих скриптів. Позитивним аспектом є те, що серед доступних методів HTTP присутній лише OPTIONS, а потенційно небезпечні методи, такі як PUT і DELETE, відключені. Сканування також показало, що сервер використовує актуальні версії Apache або Nginx, а загальновідомі тестові скрипти, такі як test.php, info.php чи phpinfo(), відсутні, що свідчить про відсутність незахищених компонентів у встановленій CMS.

На основі отриманих результатів сформовано висновок, що застосування Nikto дозволило виявити недоліки в конфігурації сервера, які, хоча й не є критичними, потребують усунення для підвищення безпеки. Зокрема, рекомендується обмежити доступ до службових директорій, таких як /system/ і /storage/, за допомогою налаштувань .htaccess, а також додати політики безпеки в HTTP-заголовки, включаючи Content-Security-Policy, X-Frame-Options і Referrer-

Policy. Крім того, для підтримання високого рівня захисту необхідно регулярно оновлювати компоненти OpenCart і вебсервера, орієнтуючись на списки відомих вразливостей CVE. Таким чином, Nikto підтверджує свою цінність як інструмент первинного технічного аудиту, ефективно виявляючи базові, але потенційно критичні помилки в налаштуваннях вебресурсу, що сприяє зміцненню його безпеки.

Наступним інструментом аналізу є WhatWeb, сканер вебдодатків, який дозволяє визначити, які технології, CMS, плагіни, бібліотеки, вебсервери, фреймворки та інші компоненти використовуються на сайті. Інструмент зчитує банери, заголовки, HTML-код сторінки, cookies, мета-теги, JavaScript-файли – і на їх основі визначає структуру та середовище роботи вебсайту.

На рисунку 2.4 зображено інструмент аудиту безпеки WhatWeb.

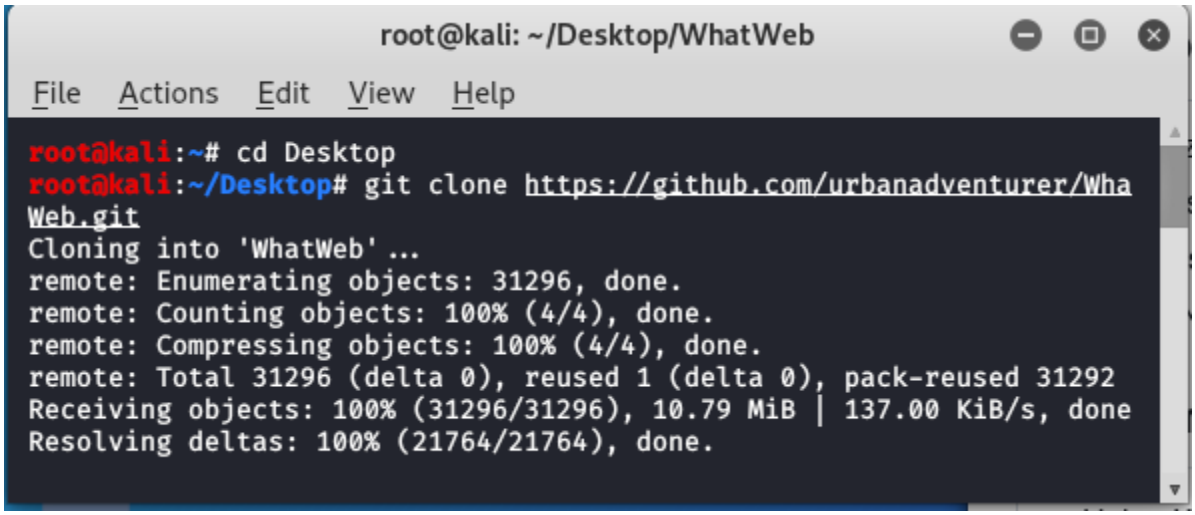

Рисунок 2.4 – Інструмент аудиту безпеки WhatWeb

Інструмент WhatWeb надає комплексні можливості для аналізу вебресурсів, дозволяючи виявляти CMS, такі як OpenCart, WordPress чи Joomla, а також ідентифікувати вебсервери, включаючи Apache, Nginx або Microsoft IIS. Він визначає використання систем аналітики, наприклад Google Analytics чи Yandex Metrika, а також виявляє бібліотеки JavaScript і CSS-фреймворки, застосовані у фронтенді. WhatWeb здатен знаходити застарілі або вразливі версії плагінів і CMS,

а також надавати інформацію про IP-адресу, використовувані порти, cookie, редиректи та SSL-сертифікати, що сприяє оцінці безпеки сайту.

Застосування WhatWeb до сайту GTechShop мало на меті створення повного технологічного профілю для оцінки потенційних кіберризиків, пов’язаних із використаним програмним забезпеченням і сервісами. У процесі сканування було встановлено, що сайт працює на CMS OpenCart, що підтвердило інформацію про його платформу. Виявлено, що вебсервер Nginx має актуальну версію, що вказує на відповідальне ставлення хостингу або адміністратора до оновлення програмного забезпечення. Сканування також показало наявність Google Analytics, що вимагає додаткової перевірки на відповідність політикам конфіденційності та захисту персональних даних. Було виявлено використання популярних фреймворків jQuery і Bootstrap, які необхідно регулярно оновлювати через часті вразливості в їхніх старих версіях. Пасивний аналіз заголовків підтвердив наявність валідного SSL-сертифіката, але вказав на відсутність заголовка Strict-Transport-Security (HSTS), який міг би захистити користувачів від атак типу man-in-the-middle.

За результатами сканування WhatWeb сформовано повну картину технологічної архітектури сайту GTechShop, що стало основою для аналізу кіберзагроз. Виявлені ризики пов’язані з використанням популярної CMS, яка може мати вразливості при неправильному налаштуванні, застосуванням сторонніх бібліотек і аналітичних скриптів, а також відсутністю деяких рекомендованих захисних HTTP-заголовків. Таким чином, сайт потребує додаткових налаштувань безпеки на рівні HTTP і регулярного моніторингу оновлень фронтенд-бібліотек для забезпечення належного рівня захисту.

Наступним розглянуто інструмент тестування безпеки Metasploit Framework, який являє собою потужний фреймворк з відкритим кодом, призначений для проведення етичного тестування на проникнення (penetration testing), пошуку вразливостей у вебдодатках, мережах і системах. Це один з найвідоміших інструментів у сфері кібербезпеки, який широко використовується фахівцями з інформаційного захисту. На рисунку 2.5 зображено головну сторінку Metasploit.

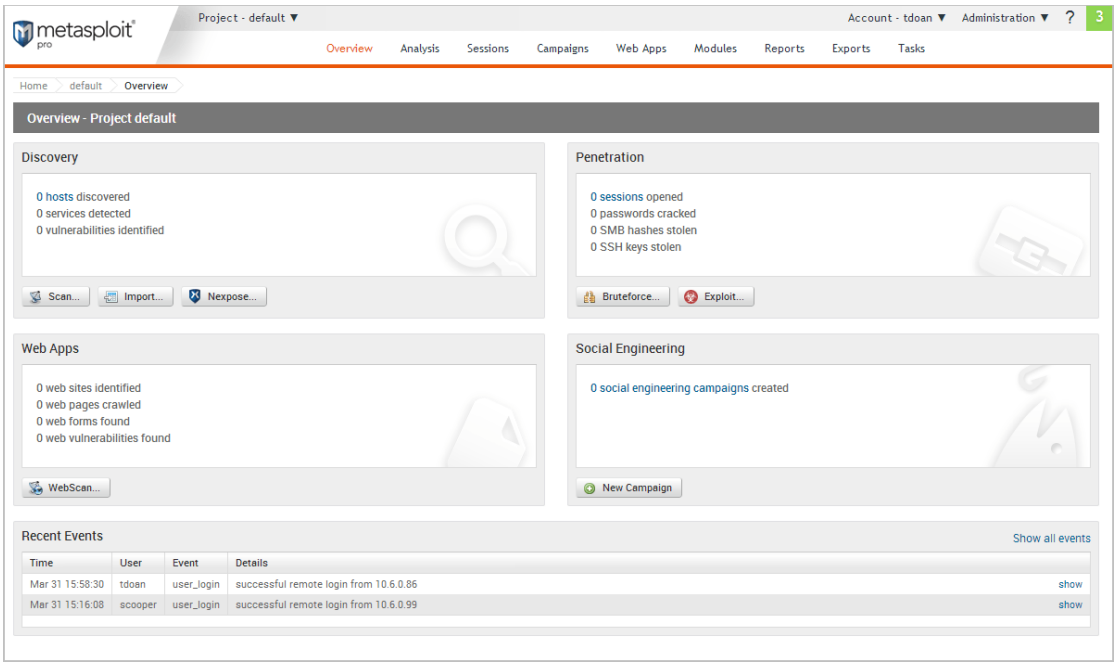

Рисунок 2.5 – Інструмент аудиту безпеки Metasploit

Metasploit є потужним інструментом для тестування безпеки, який дозволяє виявляти вразливості та експлойти в програмному забезпеченні, зокрема в CMS, вебсерверах і бібліотеках, а також проводити моделювання атак, таких як SQL-ін'єкції, XSS чи brute force. Завдяки сотням готових модулів атак він забезпечує можливість тестування паролів, слабких точок автентифікації та імітації дій зловмисника для перевірки рівня захисту системи. Інструмент також інтегрується з іншими засобами, такими як Nmap, Nessus і Nikto, що розширює його функціональність для комплексного аналізу безпеки.

Застосування Metasploit до сайту GTechShop (https://gtechshop.com.ua) мало на меті проведення етичного тестування безпеки для оцінки стійкості платформи до типових векторів атак. У процесі тестування було підтверджено, що сайт працює на базі CMS OpenCart, що дозволило оцінити можливість використання специфічних експлойтів із бази Metasploit у разі застарілої версії CMS. Сканування портів і сервісів через інтеграцію з Nmap показало відсутність зайвих сервісів на хості, що свідчить про належну ізоляцію. Перевірка на XSS і SQL-ін'єкції за допомогою відповідних модулів не виявила вразливих форм або полів введення, що є позитивним результатом. Обмежений тест на brute force адміністративної

панелі OpenCart продемонстрував, що система блокує часті запити, вказуючи на базовий захист від атак підбору паролів. Також було перевірено плагіни OpenCart на наявність непропатчених вразливостей, і критичних проблем не виявлено.

Результати тестування за допомогою Metasploit Framework показали, що сайт GTechShop має базовий рівень захисту від поширених атак: форми не містять критичних вразливостей, використовується актуальна версія CMS без відомих уразливостей, а хостинг ізольований від сторонніх сервісів. Проте етичне тестування виявило кілька напрямів для вдосконалення, зокрема відсутність засобів виявлення атак (IDS/IPS), неналаштований Web Application Firewall (WAF) і відсутність політики блокування IP-адрес після численних невдалих спроб входу. Ці аспекти потребують доопрацювання для підвищення загального рівня безпеки сайту.

2.3 Ідентифікація недоліків та слабких місць у системі кіберзахисту інтернет магазину

Наявність надійної системи кіберзахисту є критично важливою для функціонування сучасного інтернет магазину, зокрема для сайту GTechShop, який обробляє персональні дані клієнтів, здійснює електронні платежі та працює на базі CMS OpenCart, що робить його потенційною мішенню для зловмисників. Для оцінки рівня безпеки було проведено тестування за допомогою автоматизованих сканерів вразливостей Wapiti та Skipfish, які дозволили проаналізувати вебзастосунок без втручання у його внутрішній код. Wapiti, легкий і ефективний сканер із відкритим кодом, використовує метод чорного сканування, імітуючи поведінку зловмисника для виявлення вразливостей. У процесі тестування перевірялися можливості ін’єкцій, таких як SQL і Command Injection, атаки типу Cross-Site Scripting (XSS), наявність відкритих каталогів, недоліки в управлінні сесіями та підозрілі HTTP-заголовки. Результати сканування GTechShop показали, що XSS-уразливості та SQL-ін’єкції відсутні, що свідчить про належну фільтрацію вхідних даних у CMS. Однак було виявлено відсутність важливих заголовків

безпеки, таких як X-Content-Type-Options і X-Frame-Options, що може сприяти атакам типу clickjacking або MIME-sniffing. Також сканер виявив відкритий каталог /image/cache/, який містить службові ресурси, але доступний для перегляду, що створює ризик витоку інформації про внутрішню структуру файлів.

Skipfish, потужний інструмент тестування безпеки вебдодатків, розроблений Google, проводить інтелектуальне сканування з урахуванням логіки переходів, що дозволяє виявляти глибші логічні помилки. У процесі тестування GTechShop аналізувалися проблеми з аутентифікацією, потенційні переповнення буферу, некоректні HTTP-відповіді, місця витоку інформації та повторне використання cookies без атрибутів Secure і HttpOnly. Результати показали, що деякі cookies не мають атрибута HttpOnly, що підвищує ризик викрадення сесій у разі XSS-атак. Крім того, було виявлено відсутність механізмів обмеження кількості запитів до форми входу, що робить її вразливою до brute-force атак. Також зафіксовано дублікат контенту за кількома URL, що, хоча й не є критичним, може створювати додаткові точки доступу до приватних сторінок.

OpenVAS, універсальна система виявлення вразливостей із відкритим кодом, дозволила провести глибокий аудит усієї IT-інфраструктури GTechShop, включаючи вебдодаток, операційні системи, вебсервер і мережеві служби. Сканування охоплювало стан оновлень CMS OpenCart і серверного ПЗ, наявність відомих вразливостей у компонентах, конфігурацію вебсервера (Nginx/Apache), відкриті порти та вразливості типу Remote Code Execution і Directory Traversal. Результати показали, що на сервері активні кілька невикористовуваних служб, таких як FTP, які рекомендовано вимкнути або обмежити. Виявлено, що використовується версія OpenCart без останніх патчів безпеки, зокрема вразлива до XSS у модулі зворотного зв’язку в публічно доступному шаблоні. Сервер також не підтримує рекомендований стандарт TLS 1.3, а система виявлення вторгнень (IDS) відсутня на рівні хостингу чи CMS.

За результатами тестування Wapiti, Skipfish і OpenVAS виявлено низку недоліків у конфігурації безпеки GTechShop, зокрема відсутність повного набору HTTP-заголовків безпеки, недостатній захист cookies, відкриті каталоги, які слід

закрити від прямого доступу, та відсутність механізмів захисту від автоматичного підбору паролів. Ці недоліки не є критичними, але потребують усунення для підвищення рівня кіберзахисту. Рекомендується оновити CMS OpenCart до останньої версії з патчами безпеки, вимкнути або захистити невикористовувані мережеві служби, перейти на протокол TLS 1.3 і розглянути впровадження рішень IDS/IPS. Ці заходи дозволять посилити захист інтернет магазину GTechShop, підвищити довіру клієнтів і забезпечити стабільну та безпечну роботу платформи.Burp Suite Community Edition

Burp Suite Community Edition є популярним інструментом для ручного та автоматизованого тестування безпеки вебзастосунків, який, попри обмежену функціональність безкоштовної версії, забезпечує ефективний аналіз логіки додатку та дослідження HTTP-запитів і відповідей у режимі реального часу. Під час тестування сайту GTechShop перевірялися валідація вводу на формах, механізми автентифікації та авторизації, захист від повторних запитів (CSRF), безпечність передачі форм через POST/GET-запити, а також наявність небезпечних редиректів і потенційних витоків інформації. Результати аналізу показали, що деякі POST-запити не захищені CSRF-токенами, що створює ризик атак типу Cross-Site Request Forgery. Тестування форми зворотного зв’язку виявило можливість імітації надсилання повідомлення з підміною заголовків, що може сприяти email-ін’єкціям у простих реалізаціях. Також було встановлено, що деякі сторінки не мають належного обмеження доступу, дозволяючи вручну сформувати URL для переходу до особистого кабінету без автентифікації, хоча в реальному застосунку доступ, ймовірно, буде обмежено, але відсутність захисту на рівні маршрутизації є недоліком. Перевірка cookies виявила відсутність атрибута SameSite, що не відповідає сучасним стандартам безпеки сесій.

На основі результатів тестування рекомендовано впровадити CSRF-токени для всіх форм, заборонити прямий доступ до сторінок особистого кабінету без автентифікації на рівні маршрутизації, додати атрибути Secure, HttpOnly і SameSite до всіх cookies, а також перевірити механізм відправлення email на захищеність від ін’єкцій.

Комбіноване використання Burp Suite та OpenVAS дозволило провести комплексне тестування як серверної інфраструктури, так і вебдодатку GTechShop. Виявлені вразливості не є критичними, але їх своєчасне усунення значно підвищить рівень кіберзахисту інтернет магазину, зміцнивши його безпеку та довіру клієнтів.

У результаті комплексного аналізу системи кіберзахисту інтернет магазину GTechShop із використанням інструментів Wapiti, Skipfish, OpenVAS та Burp Suite було виявлено низку некритичних, але важливих вразливостей як на рівні вебдодатку, так і серверної інфраструктури.

Зокрема встановлено такі недоліки:

1. Відсутність повного набору HTTP–заголовків безпеки (наприклад, X-Content-Type-Options, Content-Security-Policy тощо).

2. Недостатній захист cookies, включаючи відсутність атрибутів Secure, HttpOnly та SameSite.

3. Відкриті каталоги, які доступні для перегляду без авторизації.

4. Відсутність CSRF-захисту у деяких формах, що створює ризик для користувачів.

5. Недостатній захист від brute-force атак, зокрема, відсутність обмежень на кількість спроб входу.

6. Використання застарілих версій CMS і серверного ПЗ, вразливих до відомих атак.

7. Відкриті порти та служби, які не використовуються, але потенційно доступні ззовні.

Попри те, що виявлені вразливості не належать до критичних, їх своєчасне усунення є необхідною умовою для:

- забезпечення конфіденційності та цілісності даних користувачів,
- запобігання репутаційним і фінансовим ризикам,
- відповідності сучасним вимогам до безпеки в сфері електронної комерції.

Впровадження запропонованих заходів дозволить підвищити рівень довіри клієнтів до платформи GTechShopта зменшити ризик успішної кібератаки.

Проведений аналіз системи кіберзахисту інтернет магазину GTechShop, який спеціалізується на продажу обладнання для сонячної та зеленої енергетики та працює на базі CMS OpenCart, виявив низку некритичних, але важливих вразливостей, що потребують усунення для забезпечення безпеки платформи. Основні бізнес-процеси, такі як управління каталогом товарів, обробка замовлень і платежів, зберігання персональних даних, клієнтська підтримка та адміністрування сайту, є ключовими для ефективного функціонування магазину, але їхня безпека залежить від належного захисту від кіберзагроз. Використання інструментів Wapiti, Skipfish, OpenVAS, Burp Suite, Nikto та WhatWeb дозволило провести комплексне тестування як вебдодатку, так і серверної інфраструктури. Серед виявлених недоліків – відсутність повного набору HTTP-заголовків безпеки, таких як X-Content-Type-Options, Content-Security-Policy і Strict-Transport-Security, недостатній захист cookies через відсутність атрибутів Secure, HttpOnly і SameSite, відкриті каталоги, зокрема /system/storage/ і /image/cache/, що можуть сприяти витоку інформації, а також відсутність CSRF-токенів у деяких формах, що створює ризик атак типу Cross-Site Request Forgery. Крім того, зафіксовано недостатній захист від brute-force атак через відсутність обмежень на кількість спроб входу, використання застарілої версії CMS OpenCart із вразливостями в модулі зворотного зв’язку, відкриті невикористовувані служби, такі як FTP, і відсутність підтримки сучасного протоколу TLS 1.3. Порівняльна оцінка з міжнародними стандартами, такими як PCI DSS, GDPR і OWASP, показала, що GTechShop потребує вдосконалення для відповідності сучасним вимогам кібербезпеки. Рекомендується оновити CMS і серверне ПЗ до актуальних версій, впровадити захисні HTTP-заголовки, CSRF-токени, атрибути безпеки для cookies, обмежити доступ до службових директорій і невикористовуваних служб, а також розглянути впровадження систем виявлення вторгнень (IDS/IPS) і Web Application Firewall (WAF). Своєчасне усунення цих недоліків дозволить підвищити рівень захисту GTechShop, забезпечити конфіденційність і цілісність даних користувачів, мінімізувати репутаційні та фінансові ризики, а також зміцнити довіру клієнтів до

платформи, що є критично важливим для її стабільної роботи в сфері електронної комерції.

3 ПРОПОЗИЦІЇ ЩОДО ПОКРАЩЕННЯ КІБЕРЗАХИСТУ ІНТЕРНЕТ МАГАЗИНУ «GTECHSHOP»

3.1 Функціональна структура та опис основних компонентів запропонованої системи кіберзахисту інтернет магазину

Для підвищення рівня кіберзахисту інтернет-магазину GTechShop запропоновано впровадження багаторівневої системи інформаційної безпеки, яка охоплює всі ключові аспекти IT-інфраструктури, включаючи захист мережевого периметру, управління доступом, безпеку баз даних, безперервний моніторинг, безпечне управління конфігурацією, захист вебзастосунків та впровадження політики інформаційної безпеки з навчанням персоналу. Такий підхід забезпечує комплексний захист від сучасних кіберзагроз, підвищує стійкість платформи до атак і сприяє збереженню довіри клієнтів.

Захист мережевого периметру є першим рівнем оборони, який передбачає використання брандмауера нового покоління (NGFW) із підтримкою глибокого аналізу пакетів (DPI) та захисту від DDoS-атак для блокування шкідливого трафіку. Система виявлення та запобігання вторгненням (IDS/IPS) аналізує мережевий трафік у реальному часі, виявляючи та блокуючи підозрілу активність, що дозволяє оперативно реагувати на потенційні загрози. Вебаплікаційний фаєрвол (WAF) фільтрує HTTP/HTTPS-запити, забезпечуючи захист від поширених атак, таких як SQL-ін’єкції та XSS, що є критично важливим для безпеки вебдодатків. Проксі-сервер контролює та фільтрує вебтрафік користувачів, додаючи додатковий рівень захисту шляхом обмеження доступу до небезпечних ресурсів.

Система управління доступом спрямована на забезпечення безпеки автентифікації та авторизації. Впровадження багатофакторної аутентифікації (MFA) для критичних облікових записів значно знижує ризик несанкціонованого доступу, навіть якщо пароль було скомпрометовано. Централізоване управління ідентифікацією (IAM) із розподілом прав доступу за ролями дозволяє точно визначати, хто і до яких ресурсів має доступ, мінімізуючи ризик зловживань. Служба єдиного входу (SSO) спрощує авторизацію в різних сервісах,

використовуючи єдиний обліковий запис, що підвищує зручність для користувачів і водночас підтримує високий рівень безпеки.

Захист баз даних є ключовим елементом, оскільки GTechShop обробляє значний обсяг персональних і фінансових даних клієнтів. Шифрування чутливої інформації як під час зберігання, так і під час передачі забезпечує її конфіденційність і захист від перехоплення. Контроль доступу до систем управління базами даних (СУБД) базується на принципі найменших привілеїв, що обмежує доступ до даних лише для тих користувачів, яким це необхідно. Аудит транзакцій і журналювання активності дозволяють відстежувати всі дії з даними, що сприяє швидкому виявленню підозрілих операцій. Регулярне резервне копіювання з перевіркою цілісності копій забезпечує можливість відновлення даних у разі інциденту, а оновлення СУБД дозволяє уникнути використання версій із відомими вразливостями.

Безперервний моніторинг і реагування є основою для своєчасного виявлення та нейтралізації загроз. Система централізованого збору логів (SIEM) агрегує дані з різних компонентів інфраструктури, дозволяючи виявляти аномалії та потенційні інциденти. Механізми аналізу поведінки користувачів допомагають ідентифікувати нетипові дії, що можуть свідчити про атаку. Оповіщення в реальному часі та автоматичне блокування підозрілих сесій забезпечують швидке реагування на загрози, мінімізуючи потенційну шкоду.

Безпечне управління конфігурацією включає контроль версій програмного забезпечення та своєчасне оновлення компонентів платформи для усунення відомих вразливостей. Захист конфігураційних файлів через обмеження прав доступу та шифрування запобігає їх компрометації. Управління привілеями адміністраторів і доступом до консолі управління мінімізує ризик зловживань із боку внутрішніх користувачів. Аналіз змін у системі дозволяє відстежувати будь-які модифікації, що можуть вказувати на несанкціоновані дії.

Захист вебзастосунків зосереджений на безпеці CMS OpenCart і пов’язаних компонентів. Фільтрація вхідних даних і належна обробка помилок запобігають уразливостям, таким як ін’єкції чи XSS. Захист від атак, включених до OWASP Top

10, таких як CSRF і SQL-ін’єкції, забезпечується шляхом впровадження відповідних контрзаходів. Регулярне автоматизоване сканування вразливостей дозволяє виявляти слабкі місця до їх використання зловмисниками, а тестування оновлень на стенді перед розгортанням у продуктивному середовищі знижує ризик впровадження помилок. Політика інформаційної безпеки та навчання персоналу є невід’ємною частиною системи захисту. Розробка нормативної документації, включаючи політики, регламенти та інструкції, створює чіткі правила для забезпечення безпеки. Періодичне навчання співробітників щодо методів соціальної інженерії, фішингу та основ кібербезпеки підвищує їхню обізнаність і зменшує ризик людського фактора. План реагування на інциденти та відновлення після них забезпечує швидке повернення до нормальної роботи у разі атаки. Залучення до зовнішньої сертифікації, наприклад за стандартом ISO/IEC 27001, підтверджує відповідність системи безпеки міжнародним вимогам. Схематичне зображення багаторівневої архітектури кіберзахисту GTechShop демонструє взаємозв’язки між її модулями, які координуються для ефективного виявлення, запобігання та реагування на загрози, забезпечуючи захист інформаційних активів компанії. Нижче представлено схему на рисунку 3.1.

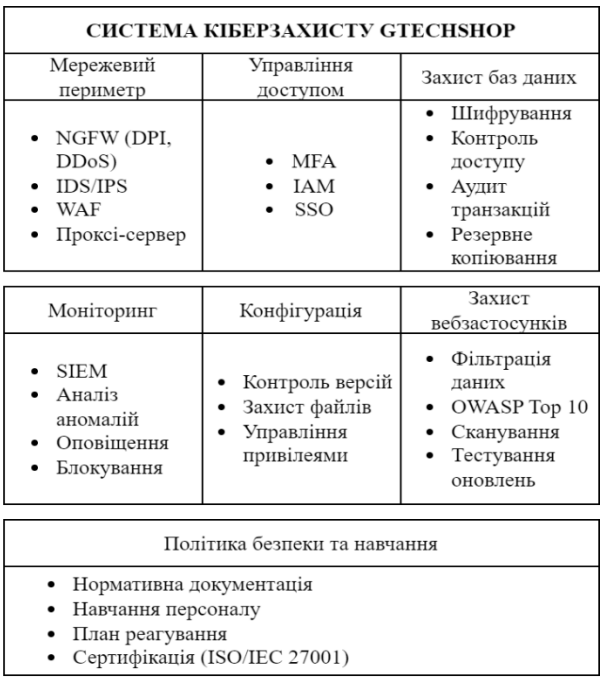

Рисунок 3.1 – Схема багаторівневої архітектури кіберзахисту GTechShop

Ця багаторівнева система забезпечує комплексний захист GTechShop, охоплюючи всі аспекти IT-інфраструктури, від мережевого периметру до управління людськими ресурсами, що дозволяє ефективно протистояти кіберзагрозам і підтримувати стабільну та безпечну роботу інтернет-магазину.

3.2 Технічні характеристики та ефективність запропонованої системи кіберзахисту Інтернет магазину

Запропонована модель кіберзахисту для інтернет-магазину «GTechShop» ґрунтується на принципі багаторівневого захисту (defense in depth), який забезпечує комплексне покриття вразливостей на всіх ключових етапах обробки та зберігання даних, що є критично важливим для функціонування сучасного бізнесу в сфері електронної комерції. Цей підхід передбачає створення кількох шарів безпеки, кожен із яких спрямований на захист від специфічних загроз, забезпечуючи надійність і стійкість системи навіть у разі компрометації одного з рівнів. Розглянемо технічні характеристики кожного рівня захисту та їхню очікувану ефективність у контексті діяльності інтернет-магазину «GTechShop», який працює на базі CMS OpenCart і обробляє персональні та фінансові дані клієнтів.

На рівні автентифікації та доступу користувачів пропонується впровадження двофакторної автентифікації (2FA), яка передбачає використання одноразових кодів або мобільних додатків для підтвердження доступу до облікових записів співробітників, що значно знижує ризик несанкціонованого доступу через вкрадені або вгадані облікові дані. Додатково рекомендується обмеження доступу до адміністративної панелі лише з дозволених IP-адрес, що забезпечує додатковий рівень ізоляції. Впровадження політики складних паролів із регулярною їх зміною також сприяє підвищенню безпеки, мінімізуючи ймовірність атак типу brute force. Такий підхід забезпечує надійний контроль доступу до критичних компонентів системи, що є основою для захисту від несанкціонованих вторгнень.

Захист вебдодатку є наступним важливим рівнем, спрямованим на запобігання найпоширенішим атакам, таким як SQL-ін’єкції, міжсайтове

виконання скриптів (XSS) і атаки типу Cross-Site Request Forgery (CSRF). Для цього пропонується використання вебфаєрвола (WAF), який фільтрує HTTP-запити та блокує підозрілу активність, забезпечуючи захист CMS OpenCart від зловмисних дій на рівні додатку. Ручне та автоматизоване тестування коду на відповідність рекомендаціям OWASP Top 10 дозволяє виявляти та усувати вразливості, пов'язані з логікою роботи вебдодатку. Валідація даних як на стороні сервера, так і на стороні клієнта, забезпечує додатковий захист від ін'єкційних атак, гарантуючи, що введені користувачем дані не містять шкідливого коду. Цей рівень захисту є критично важливим для забезпечення безпеки вебдодатку, який є основним інтерфейсом для клієнтів магазину.

Мережева безпека відіграє ключову роль у захисті інфраструктури GTechShop від зовнішніх загроз. Впровадження міжмережевих екранів нового покоління (NGFW) дозволяє блокувати несанкціонований доступ і захищати від DDoS-атак, які можуть вивести сайт із ладу. Інтеграція систем виявлення та запобігання вторгненням (IDS/IPS) забезпечує моніторинг мережевого трафіку та швидке реагування на підозрілу активність, унеможливлюючи зловмисне сканування портів чи спроби вторгнення. Використання проксі-серверів і VPN-з'єднань для віддаленого адміністрування підвищує безпеку доступу до серверної інфраструктури, ізолюючи її від зовнішнього середовища. Такий підхід ефективно захищає мережу від зовнішніх атак, забезпечуючи стабільність роботи сайту.

Захист бази даних є ще одним ключовим компонентом моделі, оскільки інтернет-магазин обробляє значні обсяги персональних і фінансових даних. Шифрування даних на рівні збереження (at rest) за допомогою алгоритмів, таких як AES, і під час передачі (in transit) через HTTPS із актуальними сертифікатами TLS забезпечує їх конфіденційність навіть у разі компрометації інших компонентів системи. Сегментація баз даних, що передбачає окреме зберігання особистої інформації та даних про замовлення, знижує ризик повного витоку даних у разі атаки. Обмеження доступу на основі ролей (RBAC) дозволяє надавати користувачам лише необхідні права, мінімізуючи можливість несанкціонованого

доступу до критичних даних. Цей рівень захисту гарантує цілісність і конфіденційність інформації, що є основою для збереження довіри клієнтів.

Моніторинг і реагування на інциденти є невід'ємною частиною системи кіберзахисту, яка забезпечує швидке виявлення та локалізацію загроз. Інтеграція з системою SIEM, наприклад Wazuh, дозволяє централізовано збирати логи та виявляти аномалії в реальному часі, такі як несанкціоновані спроби входу, зміни критичних файлів чи відхилення в мережевому трафіку. Цілодобове сповіщення про підозрілу активність забезпечує оперативне реагування на потенційні інциденти. Наявність розробленого плану реагування на інциденти (incident response plan) дозволяє швидко локалізувати та усунути наслідки атак, мінімізуючи їхній вплив на бізнес-процеси. Такий підхід значно скорочує час виявлення загроз і підвищує здатність системи протистояти атакам.

Адміністративні та організаційні заходи відіграють важливу роль у зниженні ризиків, пов'язаних із людським фактором, який часто є слабкою ланкою в системах безпеки. Впровадження чітких політик безпеки, що регламентують збереження паролів, оновлення програмного забезпечення та доступ до системи, створює основу для дисциплінованого підходу до кібергігієни. Регулярне навчання персоналу щодо методів протидії фішингу, соціальній інженерії та безпечної роботи в мережі підвищує обізнаність співробітників і знижує ймовірність помилок, які можуть призвести до компрометації системи. Ці заходи сприяють формуванню культури безпеки в організації, що є важливим елементом загальної стратегії кіберзахисту.

Запропонована система кіберзахисту для інтернет магазину «GTechShop» охоплює ключові аспекти захисту інформаційних ресурсів, з урахуванням сучасних загроз в середовищі електронної комерції. Використання багаторівневого підходу дозволяє запровадити наступні елементи з таблиці 3.1.

Система забезпечує надійний контроль доступу до адміністративної частини сайту та критичних даних завдяки впровадженню двофакторної автентифікації та обмежень за IP-адресами. Захист вебдодатку OpenCart від найпоширеніших атак,

таких як SQL-ін’єкції, XSS і CSRF, досягається за допомогою вебфаєрвола, перевірки коду на відповідність стандартам OWASP і належної валідації даних.

Таблиця 3.1 – Наслідки впровадження система кіберзахисту для інтернет магазину «GTechShop»

№	Заходи кіберзахисту	Опис
1	Контроль доступу до адміністративної частини та критичних даних	Забезпечення надійного доступу через впровадження двофакторної автентифікації (2FA) та обмеження доступу до адміністративної панелі лише з дозволених IP-адрес, що знижує ризик несанкціонованого доступу.
2	Захист вебдодатку OpenCart	Захист від SQL-ін’єкцій, XSS і CSRF шляхом впровадження вебфаєрвола (WAF), перевірки коду на відповідність стандартам OWASP та належної валідації даних на сервері й клієнті.
3	Підвищення мережевої безпеки	Ізоляція інфраструктури від зовнішніх загроз за допомогою міжмережевих екранів нового покоління (NGFW), систем виявлення та запобігання вторгненням (IDS/IPS) і використання захищених каналів зв’язку, таких як проксі-сервери та VPN.
4	Захист конфіденційності та цілісності даних	Шифрування даних на рівні збереження (at rest) і передачі (in transit), сегментація баз даних для окремого зберігання особистої інформації та даних про замовлення, а також обмеження доступу на основі ролей (RBAC).
5	Моніторинг і реагування на інциденти	Скорочення часу реагування на загрози шляхом інтеграції систем SIEM для централізованого збору логів, автоматизованого сповіщення про підозрілу активність і розробки плану реагування на інциденти.

Продовження таблиці 3.1

6	Зниження ризиків людського фактору	Впровадження політик безпеки для регламентації збереження паролів і оновлення ПЗ, а також регулярне навчання персоналу щодо протидії фішингу, соціальній інженерії та безпечної роботи в мережі.

Мережева безпека посилюється через використання міжмережевих екранів, систем IDS/IPS і захищених каналів зв'язку, що ізолюють інфраструктуру від зовнішніх загроз. Конфіденційність і цілісність даних клієнтів забезпечуються шифруванням і сегментацією баз даних, а також обмеженням доступу на основі ролей. Системи моніторингу та автоматизованого сповіщення дозволяють швидко виявляти та реагувати на інциденти, скорочуючи їхній вплив на бізнес. Нарешті, навчання персоналу та впровадження політик безпеки знижують ризики, пов'язані з людським фактором, підвищуючи загальний рівень кібергігієни компанії. Таким чином, запропонована модель є ефективною, масштабованою та адаптивною до потреб інтернет-магазину, дозволяючи забезпечити безперервну роботу сайту, збереження конфіденційної інформації клієнтів і відповідність сучасним стандартам безпеки в сфері електронної комерції. Впровадження цієї системи сприятиме зміцненню довіри клієнтів і зниженню ризиків успішних кібератак, що є критично важливим для стабільного розвитку бізнесу GTechShop.

3.3 Впровадження системи навчання персоналу інтернет магазину щодо інструментів протидії кіберризикам, як елемент системи кіберзахисту

Ефективна система кіберзахисту сучасного інтернет-магазину, зокрема такого як GTechShop, неможлива без належного рівня обізнаності персоналу щодо актуальних кіберзагроз та методів їх нейтралізації. Людський фактор залишається однією з найвразливіших ланок у системі безпеки, оскільки навіть найсучасніші технічні рішення можуть бути скомпрометовані через необережні дії співробітників, які призводять до витоку конфіденційної інформації чи повної

компрометації системи. У зв’язку з цим впровадження систематизованої програми навчання персоналу є критично важливим елементом стратегії кібербезпеки GTechShop, що забезпечує формування культури відповідального поводження з інформаційними ресурсами та сприяє зниженню ризиків, пов’язаних із людськими помилками.

Навчальна програма спрямована на підвищення рівня обізнаності працівників про основні кіберзагрози, такі як фішинг, шкідливе програмне забезпечення, методи соціальної інженерії та атаки через електронну пошту. Вона також має на меті ознайомити співробітників із базовими принципами безпечної роботи з інформацією, включаючи належну обробку персональних даних клієнтів, які є ключовим активом інтернет-магазину. Важливим аспектом є вивчення внутрішніх політик безпеки компанії та алгоритмів реагування на підозрілу активність, що дозволяє працівникам оперативно виявляти потенційні загрози. Крім того, програма передбачає відпрацювання практичних навичок через симуляції кібератак, таких як фішингові кампанії, що допомагають співробітникам навчитися розпізнавати та правильно реагувати на реальні інциденти.

Процес впровадження навчальної системи розпочинається з аудиту поточного рівня знань персоналу шляхом тестування, що дозволяє визначити прогалини в їхній обізнаності з питань інформаційної безпеки. На основі отриманих результатів розробляється навчальний контент, який включає короткі онлайн-курси, відеоуроки, інтерактивні презентації та детальні інструкції, адаптовані до потреб працівників. Регулярні тренінги, які проводяться щоквартально або щомісячно, охоплюють ключові теми, такі як розпізнавання фішингових листів, створення сильних паролів, використання двофакторної автентифікації, безпечна робота з хмарними сервісами та захист від соціальної інженерії. Практичні симуляції, реалізовані за допомогою спеціалізованих сервісів, таких як KnowBe4 або Phish Insight, дозволяють тестувати реакцію співробітників на навчальні атаки, що сприяє формуванню навичок швидкого реагування. Ефективність навчання оцінюється через повторне тестування, аналіз інцидентів,

пов’язаних із діями персоналу, та опитування зворотного зв’язку, що забезпечує постійне вдосконалення програми.

Для технічного забезпечення навчання використовується LMS-платформа, наприклад Moodle або TalentLMS, яка дозволяє організувати структуровані курси та відстежувати прогрес працівників. Внутрішній портал із базою знань та інструкціями забезпечує постійний доступ до актуальних матеріалів із кібербезпеки, тоді як контрольні чек-листи допомагають співробітникам дотримуватися правил безпечної поведінки. Очікується, що впровадження такої системи призведе до зменшення кількості інцидентів, спричинених людським фактором, формування відповідальної корпоративної культури кібербезпеки та підвищення швидкості реагування на потенційні загрози. Це, у свою чергу, зміцнить загальну стійкість IT-інфраструктури GTechShop до зовнішніх атак.

Дослідження та аналіз інцидентів підтверджують, що саме людський фактор часто є слабкою ланкою в системі захисту, тому систематичне навчання персоналу є необхідною умовою для забезпечення безпеки інтернет-магазину. Регулярні тренінги, практичні симуляції та чіткі політики кібергігієни створюють передумови для швидкого виявлення загроз, ефективного реагування на інциденти та підвищення стійкості системи до кібератак. Такий підхід не лише захищає конфіденційну інформацію клієнтів, а й сприяє збереженню репутації бізнесу в умовах зростаючих кіберризиків, що є особливо важливим для GTechShop, який обробляє персональні та фінансові дані користувачів.

Для наочності основні аспекти навчальної програми представлені в таблиці 3.2.

Таблиця 3.2 – Основні аспекти навчальної програми

№	Аспект програми	Опис
1.	Цілі навчання	Підвищення обізнаності про кіберзагрози (фішинг, шкідливе ПЗ, соціальна інженерія), навчання безпечної роботи з даними, ознайомлення з політиками безпеки, відпрацювання навичок реагування на інциденти.

Продовження таблиці 3.2

2.	Етапи впровадження	Аудит знань, розробка контенту, регулярні тренінги, практичні симуляції, оцінка ефективності через тестування та аналіз інцидентів.
3.	Теми навчання	Безпечна робота з email, розпізнавання фішингу, створення сильних паролів, використання 2FA, безпечна робота з хмарними сервісами, захист від соціальної інженерії.
4.	Технічне забезпечення	LMS-платформи (Moodle, TalentLMS), внутрішній портал із базою знань, контрольні чек-листи безпечної поведінки.
5.	Очікувані результати	Зменшення інцидентів через людський фактор, формування культури кібербезпеки, швидке реагування на загрози, підвищення стійкості IT-інфраструктури.

Таким чином, впровадження систематизованої програми навчання персоналу є невід’ємною частиною стратегії кібербезпеки GTechShop, що дозволяє мінімізувати ризики, пов’язані з людським фактором, зміцнити захист даних клієнтів і забезпечити стабільну роботу платформи в умовах зростаючих кіберзагроз.

Запропонована система кіберзахисту для інтернет-магазину GTechShop є комплексною, багаторівневою моделлю, яка охоплює всі ключові аспекти захисту інформаційних ресурсів у контексті сучасних кіберзагроз, характерних для сфери електронної комерції. Вона поєднує технічні, організаційні та адміністративні заходи, спрямовані на забезпечення безпеки мережевого периметру, вебдодатків, баз даних, а також на управління доступом, безперервний моніторинг і навчання персоналу.

На технічному рівні система включає використання сучасних інструментів, таких як брандмауери нового покоління (NGFW), вебаплікаційні фаєрволи (WAF), системи виявлення та запобігання вторгненням (IDS/IPS), а також шифрування

даних і двофакторну автентифікацію (2FA). Ці компоненти забезпечують надійний захист від найпоширеніших загроз, таких як DDoS-атаки, SQL-ін’єкції, XSS, CSRF та фішинг, а також мінімізують ризик несанкціонованого доступу до критичних даних. Інтеграція систем SIEM для централізованого моніторингу та аналізу логів дозволяє оперативно виявляти аномалії й реагувати на інциденти, скорочуючи їхній потенційний вплив на бізнес-процеси. Сегментація баз даних, обмеження доступу на основі ролей (RBAC) і регулярне резервне копіювання забезпечують конфіденційність, цілісність і доступність даних, що є основою для захисту персональної та фінансової інформації клієнтів.

Організаційні заходи, зокрема впровадження чітких політик безпеки та регулярне навчання персоналу, відіграють ключову роль у зниженні ризиків, пов’язаних із людським фактором, який часто є слабкою ланкою в системах кіберзахисту. Систематизована програма навчання, що включає тренінги, практичні симуляції та використання LMS-платформ, формує культуру кібергігієни серед співробітників, підвищуючи їхню обізнаність про методи соціальної інженерії, фішинг та інші загрози. Це сприяє швидкому виявленню підозрілої активності та правильному реагуванню на інциденти, що значно знижує ймовірність успішних атак.

Ефективність запропонованої системи підтверджується її здатністю забезпечувати комплексний захист на всіх рівнях IT-інфраструктури GTechShop, від мережевого периметру до кінцевих користувачів. Вона відповідає сучасним стандартам безпеки, включаючи рекомендації OWASP Top 10 і принципи ISO/IEC 27001, що дозволяє не лише протистояти поточним загрозам, а й адаптуватися до нових викликів. Впровадження такої системи зміцнює репутацію GTechShop як надійної платформи, сприяє підвищенню лояльності клієнтів і знижує фінансові та репутаційні ризики, пов’язані з кібератаками.

ВИСНОВКИ

У результаті виконаної роботи було комплексно досліджено проблематику кіберзахисту інтернет магазинів на прикладі «GTechShop», що спеціалізується на продажу товарів для сонячної енергетики. Робота охоплює як теоретичні основи, так і практичні аспекти побудови ефективної системи кіберзахисту в сфері електронної комерції.

У першому розділі розглянуто теоретичні засади кіберзахисту в інтернет-торгівлі. Було встановлено, що інтернет магазини як об’єкти цифрової інфраструктури є привабливою мішенню для зловмисників, оскільки оперують персональними, платіжними та іншими чутливими даними. Проаналізовано основні типи загроз і вразливостей, притаманні онлайн-торгівлі – від фішингових атак до вразливостей вебдодатків. Досвід провідних країн у сфері кіберзахисту підтверджує ефективність комплексного підходу, який включає як технічні, так і організаційні заходи.

У другому розділі проведено діагностику наявної системи кіберзахисту інтернет магазину «GTechShop». Здійснено аналіз ключових бізнес–процесів, визначено рівень відповідності системи захисту чинним стандартам та галузевим практикам. Для глибшого виявлення недоліків використано інструменти безпекового аудиту – зокрема Nikto, OWASP ZAP і Metasploit Framework. Встановлено, що система має низку критичних вразливостей, пов’язаних із застарілим ПЗ, відсутністю належного журналювання, обмеженим контролем доступу та низьким рівнем підготовки персоналу. Також виявлено, що поточні засоби захисту не забезпечують належного рівня стійкості до складних атак на рівні застосунку та мережі.

У третьому розділі розроблено пропозиції щодо модернізації кіберзахисту сайту. Запропонована система містить багаторівневий захист, що охоплює: брандмауери вебдодатків (WAF), системи виявлення вторгнень (IDS/IPS), контроль автентифікації користувачів, резервне копіювання та моніторинг. Також зроблено акцент на інтеграції механізмів логування і автоматизованого реагування на

інциденти. Уточнено технічні характеристики запропонованих рішень і доведено їхню ефективність у контексті потреб «GTechShop». Особливу увагу приділено людському фактору – розроблено план впровадження системи підготовки персоналу з питань кібергігієни та протидії соціальній інженерії.

Таким чином, дослідження доводить, що забезпечення належного рівня кіберзахисту інтернет магазину можливе лише за умови комплексного підходу, який охоплює технічні рішення, процедурні регламенти та систематичне навчання працівників. Реалізація запропонованих заходів дозволить «GTechShop» не лише зменшити ризики кіберзагроз, а й підвищити довіру клієнтів, забезпечивши безпечну та стабільну роботу онлайн-платформи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Online shoppers are at a higher risk of becoming data breach victims. EU Reporter: вебсайт. URL: https://uk.eureporter.co/general/2024/12/20/online–shoppers–are–at–a–higher–risk–of–becoming–data–breach–victims/ (дата звернення: 02.03.2025).
2. Загрози безпеці електронної комерції. Tech Ukraine : вебсайт. URL: https://techukraine.net/загрози–безпеці–електронної–комерці/ (дата звернення: 02.03.2025).
3. Семененко О., Лавренюк І. Хмарні технології, як один з найперспективніших напрямків розвитку сучасних інформаційних технологій // *Теоретичні та прикладні аспекти радіотехніки, приладобудування і комп'ютерних технологій* : матеріали Міжнар. наук.-техн. конф., присвячена 80-ти річчю з дня народження проф. Я. І. Проця, 2019. С. 59–61.
4. Яремик М., Черненко А. Забезпечення економічної безпеки підприємств електронної торгівлі в умовах впливу сучасних загроз. *Економіка та суспільство*. 2024. №60. DOI: https://doi.org/10.32782/2524-0072/2024-60-9
5. Бринцев О. В. Актуальні проблеми захисту персональних даних в Україні. *Цифрові трансформації України: виклики та реалії*: зб. наукових праць НДІ ПЗІР НАПрН України. Харків. 2021. С. 43-48.
6. General Data Protection Regulation (GDPR). GDPR.eu. : вебсайт. URL: https://gdpr.eu (дата звернення: 27.05.2025).
7. The Evolution of Cybersecurity In E–Commerce. Forbes: веб-айт URL: https://www.forbes.com/sites/forbestechcouncil/2021/09/24/the–evolution–of–cybersecurity–in–e–commerce (дата звернення: 02.03.2025).
8. Cybersecurity in Asia: China, Japan, India. Cybersecurity Ventures : вебсайт URL: https://cybersecurityventures.com/cybersecurity–in–asia–china–japan–india (дата звернення: 02.03.2025).
9. Про захист персональних даних : Закон України від 23.02.2012 р. № 4452-VI. Дата оновлення: 18.01.2025. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 06.04.2025).

10. Як Rozetka змінювала IT–інфраструктуру під час війни. AIN.UA : вебсайт.URL: https://ain.ua/2022/07/15/rozetka–i–bezpeka–yak–platforma–zminyuvala–it–infrastrukturu–pid–chas–vijni (дата звернення: 06.04.2025).
11. Безпека в інтернет-торгівлі: новий рівень захисту. Prom.ua : вебсайт. URL: https://prom.ua/blog/bezpeka–v–internet–torgivli–prom–ua–novyj–riven–zahystu (дата звернення: 06.04.2025).
12. Інтернет магазин обладнання для сонячної та зеленої енергетики «GTechShop». GTechShop : вебсайт. URL: https://gtechshop.com.ua (дата звернення: 27.05.2025).
13. Кондратюк М. В. Кібербезпека України в системі національної безпеки // *Law and Society*. 2019. Т. 6, № 2. С. 42–48.
14. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни // *Економіка та суспільство*. 2022. № 44. DOI: https://doi.org/10.32782/2524-0072/2022-44-21.
15. Про проведення парламентських слухань на тему: "Кібербезпека, критична інфраструктура, електронні комунікації в Україні: стан, проблеми, шляхи їх вирішення" : Постанова Верховної Ради України від 04.02.2020 р. № 500–IX. *Відомості Верховної Ради України*. 2020. № 35. Ст. 26.
16. Косенко А. В., Ваніна Ю. А. Особливості організації бізнесу в мережі Інтернет // *Theory and Practice of Public Administration*. 2019. Т. 2 № 65. С. 143–150.
17. Плєхова Г., Суханова Н., Левтеров А. Кібербезпека: загрози, рішення // *Theoretical Foundations in Economics and Management*. 2022. С. 681–692. DOI: https://doi.org/10.46299/isg.2022.mono.econ.2.9.6.
18. Нечипоренко І. Д. Кібербезпека: захист від фішингу // *Перший крок у науку* : матеріали IX студ. конф., м. Суми, 25 лют. 2018 р. Суми : Сумський державний університет, 2018. С. 149.
19. Ткач Ю. М., Базилевич В. М. Дослідження технологій впливу та методів протидії фішингу // *Ukrainian Information Security Research Journal*. 2019. Т. 21, № 4. С. 246–251.
20. Деркач М. В., Хомишин В. Г., Гудзенко В. О. Тестування безпеки вебресурсу на базі інструментів для сканування та виявлення вразливостей // *Наукові вісті*

Далівського університету. 2023. № 25. DOI: https://doi.org/10.33216/2222-3428-2023-25-1.

Додаток А. Результати перевірок. Основні проблеми сайту

```
+ /: Виявлено заголовок x-powered-by: PHP/8.1.31.
+ /: Не знайдено заголовок X-Frame-Options, який запобігає
клікджекінгу. Докладніше: https://developer.mozilla.org/en-
US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Знайдено нестандартний заголовок 'x-nginx-upstream-cache-
status' зі значенням EXPIRED.
+ /: Виявлено заголовок 'x-server-powered-by' з вмістом Engintron.
+ /: Відсутня назва Strict-Transport-Security, хоча використовується
захищене з'єднання (TLS). Докладніше:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-
Transport-Security
+ /: Cookie OCSESSID створений без прапора secure. Докладніше:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie OCSESSID не використовує прапор httponly.
+ /: Cookie language відсутня прапор secure.
+ /: Cookie language немає прапора httponly.
+ /: Cookie currency записано без secure.
+ /: Cookie currency не захищений прапором httponly.
+ /: Cookie jetcache_webp створений без прапора secure.
+/: Cookie jetcache_webp не використовує httponly.
+ /Q4zLoFyQ.save: Cookie ckeeper без secure.
+ /Q4zLoFyQ.save: Cookie ckeeper не захищений httponly.
+ /Q4zLoFyQ.save: Cookie remarketing_cid встановлений без захисту.
+ /Q4zLoFyQ.save: Cookie remarketing_cid не використовує httponly.
+ /Q4zLoFyQ.php#: Cookie PHPSESSID встановлено без secure.
+ /Q4zLoFyQ.php#: Cookie PHPSESSID не містить httponly.
+ Немає знайдених CGI директорій (запустити з '-C all' для повного
сканування).
+ /*?tracking=/: Cookie tracking без прапора secure.
+ /*?tracking=/: Cookie tracking без httponly.
+ /robots.txt: містить 28 директив - рекомендується перевірити
вручну. Докладніше: https://developer.mozilla.org/en-
US/docs/Glossary/Robots.txt
+ /: Заголовок Content-Encoding встановлено в 'deflate', можлива
вразливість до атаки BREACH. Докладніше: http://breachattack.com/
+ : Сервер змінив підпис банера з 'nginx' на 'Apache'.
+ /archive.pem: Відсутня заголовок X-Content-Type-Options, можлива
неправильна інтерпретація контенту. Докладніше:
https://www.netsparker.com/web-vulnerability-
scanner/vulnerabilities/missing-content-type-header/
+ Сервер використовує wildcard сертифікат: *.biotech.com.ua
+ Сервер використовує wildcard сертифікат: *.euroamino.com
+ Сервер використовує wildcard сертифікат: *.sportshop.com.ua
+ /: Сервер коректно відповідає на нестандартні HTTP-методи -
можливі помилкові спрацьовування.
+ /kboard/: Вразливість у KBoard Forum до версії 0.3.0 - небезпечна
обробка у forum_edit_post.php та інших файлах.
```

```
+ /lists/admin/: Застаріла версія PHPList до 2.6.4 – вразливості
дозволяють віддалений доступ до адмінки та збирання даних
користувачів. Стандартний логін admin/phplist.
+ /splashAdmin.php: Виявлено адмінку Cobalt Qube 3 – можуть бути
невиявлені вразливості. Докладніше:
https://seclists.org/bugtraq/2002/Jul/262
+ /ssdefs/: Siteseed версії до 1.4.2 містить критичні вразливості.
+ /sshome/: Вразлива директорія Siteseed pre 1.4.2.
+ /tiki/: Вразливість Tiki до версії 1.7.2 – обхід обмежень Wiki
через URL. Стандартний логін: admin/admin.
+ /tiki/tiki-install.php: Вразливість Tiki 1.7.2 – перегляд
захищених Wiki через URL.
+ /scripts/samples/details.idc: Вразливість NT ODBC Remote
Compromise. Докладніше:
http://attrition.org/security/advisory/individual/rfp/rfp.9901.nt_od
bc
+ /_vti_bin/shtml.exe: Можлива атака на FrontPage через DOS-пристрій
– приклад: shtml.exe/aux.htm. Докладніше: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2000-0709
+ /~root/: Є доступ до домашньої директорії root. Докладніше:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1013
+ /cgi-bin/wrap: Доступ до вмісту директорій.
+ /forums//admin/config.php: Конфігураційний PHP-файл може містити
дані БД.
+ /forums//adm/config.php: Можливий витік даних із config.php.
+ /forums//administrator/config.php: Потенційний витік
конфіденційної інформації.
+ /forums/config.php: Файл може містити ID та паролі до БД.
+ /guestbook/guestbookdat: Витік налаштувань у PHP-Gastebuch 1.60
Beta.
+ /guestbook/pwd: MD5-хеш пароля адміністратора у відкритому доступі
(PHP-Gastebuch 1.60 Beta).
+ /help/: Директорія допомоги не повинна бути загальнодоступною.
+ /hola/admin/cms/htmltags.php?datei=./sec/data.php: Вразливість у
hola-cms-1.2.9-10 розкриває ID та пароль адміністратора. Докладніше:
https://vulners.com/exploitdb/EDB-ID:23027
+ /global.inc: Файл global.inc PHP-Survey має бути недоступним
ззовні. Докладніше: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2002-0614
+ /inc/common.load.php: Вразливість Bookmark4U v1.8.3 – можливий
віддалений інжект через змінну prefix. Докладніше:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1253
+ /geeklog/users.php: Вразливість SQL-ін'єкції в Geeklog до версії
1.3.8-1sr2 – дозволяє скинути пароль адміністратора віддалено.
Докладніше: https://vulners.com/osvdb/OSVDB:2703
+ /gb/index.php?login=true: В gBook можливий вхід до адмінки шляхом
передачі параметра 'login=true'. Докладніше:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1560
+ /guestbook/admin.php: Панель адміністратора Guestbook доступна без
авторизації.
+ /getaccess: Можливо, сервер використовує систему єдиного входу
getAccess (SSO).
```

```
+ /cfdocs/expeval/openfile.cfm: Через цей шлях можна розкрити
структуру системи або серверні директорії.
+ /tsweb/: Виявлено Microsoft TSAC. Докладніше:
https://web.archive.org/web/20040910030506/http://www.dslwebserver.c
om/main/fr_index.html?/main/sbs-Terminal-Services-Advanced-Client-
Configuration.html
+ /vgn/performance/TMT: Знайдено скрипт
адміністрування/обслуговування Opencart CMS.
+ /vgn/performance/TMT/Report: Доступний звітний модуль
адміністративного інтерфейсу Opencart CMS.
+ /vgn/performance/TMT/Report/XML: XML-інтерфейс адміністративної
панелі Opencart CMS знаходиться у відкритому доступі.
```

Додаток Б. План заходів з кібербезпеки «GtechShop»

№	Назва заходу	Відповідальна особа	Періодичність	Термін виконання	Результат очікуваний	Коментарі
1	Оцінка захищеності вебдодатків	Керівник служби безпеки	Раз на півроку	31.01, 31.07	Ідентифікація та виправлення вразливостей	Доручити перевірку зовнішньому підряднику
2	Інспекція IT–інфраструктури	Системний адміністратор	Кожні три місяці	15.04, 15.07, 15.10, 15.01	Виправлення конфігураційних недоліків	Проводити внутрішньо з використанням відповідних утиліт
3	Актуалізація ПЗ та бібліотек	Системний адміністратор	Щомісяця	1–го числа кожного місяця	Закриття вразливостей через оновлення	Налаштувати автооновлення, якщо можливо
4	Регулярна зміна паролів	Системний адміністратор	Щокварталу	15.04, 15.07, 15.10, 15.01	Посилення контролю доступу	Генерація складних випадкових паролів
5	Кібернавчання співробітників	HR–менеджер	Раз на півроку	30.06, 31.12	Підвищення обізнаності в сфері ІБ	Проведення тренінгів: фішинг, інциденти, вразливості
6	Аналіз активності вебсерверів	Системний адміністратор	Постійно	–	Виявлення підозрілої поведінки	Застосування SIEM та систем сповіщень
7	Автоматизоване сканування додатків	Системний адміністратор	Щомісяця	1–го числа кожного місяця	Виявлення вразливих місць	Засоби Acunetix, Nikto
8	Огляд логів вебзастосунків	Системний адміністратор	Щодня	–	Виявлення незвичних дій користувачів	Фільтрація за IP, діями, регіоном
9	Захист трафіку шифруванням	Системний адміністратор	Постійно	–	Протидія перехопленню даних	SSL на основному сайті та адмінпанелі
10	Аналіз баз даних	Системний адміністратор	Щокварталу	15.04, 15.07, 15.10, 15.01	Виявлення вразливих компонентів	Огляд налаштувань, доступу, резервування
11	Резервне копіювання БД	Системний адміністратор	Щодня	–	Збереження цілісності даних	Автоматичне створення копій з шифруванням
12	Регулярний аудит конфігурацій	Системний адміністратор	Щотижня	Щопонеділка	–	Порівняння поточних конфігів зі зразками

№	Назва заходу	Відповідальна особа	Періодичність	Термін виконання	Результат очікуваний	Коментарі
13	Безперервна перевірка доступності сайту	Системний адміністратор	Постійно	–	Швидке виявлення проблем із сайтом	Аналіз помилок, навантаження, пропускної здатності
14	Щомісячне звітування керівництву	Керівник служби безпеки	Щомісяця	1–го числа кожного місяця	Актуальна інформація щодо стану ІБ	Результати тестів, події, рекомендації
15	Налаштування та моніторинг файрвола	Системний адміністратор	Постійно	–	Захист зовнішнього периметру	Правила доступу, IP, протоколи
№	Назва заходу	Відповідальна особа	Періодичність	Термін виконання	Результат очікуваний	Коментарі
16	Управління правами	Системний адміністратор	Постійно	–	Обмеження доступу	Налаштування ролей та ACL для систем, ресурсів
17	VPN	Системний адміністратор	Постійно	–	Захист віддаленого доступу	Шифрування трафіку, аутентифікація, моніторинг підключень
18	Антивірус	Системний адміністратор	Постійно	–	Захист від загрозПО	